THÈSE DE DOCTORAT
UNIVERSITÉ PARIS 6

Spécialité
Mathématiques

Présentée par
Guillaume Aubrun

Pour obtenir le grade de
Docteur de l'Université Paris 6

Sujet de la thèse
Convexité en grande dimension, matrices aléatoires et théorie quantique de l'information

Soutenue le 15 décembre 2005 devant le jury composé de

MM.	Philippe Biane	Examinateur
	Bernard Maurey	Examinateur
	Alain Pajor	Rapporteur
	Gilles Pisier	Examinateur
	Mark Rudelson	Rapporteur
	Stanisław Szarek	Directeur de thèse

Je tiens à remercier Staszek Szarek pour avoir encadré ma thèse. Il a su me guider au travers de mathématiques variées et passionnantes. La confiance qu'il a placée en moi, au même titre que sa constante bonne humeur, ont contribué à rendre ces années agréables. Malgré la distance, il a toujours répondu à mes questions avec précision et patience.

Alain Pajor et Mark Rudelson ont accepté de rapporter ce travail, et ce en un délai très bref. Je leur en suis très reconnaissant. Je remercie également Alain pour les nombreuses discussions que nous avons eues au cours de la dernière année, qui ont joué un rôle prépondérant dans ce travail.

Merci aussi à Philippe Biane, Bernard Maurey et Gilles Pisier de me faire l'honneur de participer à mon jury.

J'ai eu la chance au cours de ces années d'effectuer plusieurs séjours à l'étranger. Je veux exprimer ici toute ma gratitude envers tous ceux qui ont rendu possibles ces voyages. Merci encore à Staszek et Margaretmary pour leur accueil. À Apostolos dont la générosité fut sans égale je dirai simplement : ευχαριστώ πολύ.

Cette thèse a été effectuée au sein de l'Équipe d'Analyse Fonctionnelle, je tiens à en remercier vivement tous les membres. Merci en particulier à Olivier Guédon qui a répondu à mes nombreuses interrogations. Ma formation mathématique doit aussi beaucoup aux groupes de travail organisés à Marne-la-Vallée, dont je remercie tous les participants, notamment Matthieu Fradelizi avec qui j'ai eu grand plaisir à travailler. Je remercie également Elisabeth Werner pour les longues discussions que nous avons eues.

Je suis toujours heureux de parler de mathématiques avec des amis ; je voudrais notamment citer Yves Cornulier et Romain Tessera avec qui j'ai de fortes interactions mathématiques. Merci aussi à tous les autres amis avec qui j'ai eu des fortes interactions non nécessairement mathématiques.

Merci enfin à Aurélie.

Table des matières

Introduction

Cette thèse s'inscrit dans le cadre de l'Analyse Géométrique Asymptotique, domaine en pleine expansion dont le but est l'étude des propriétés géométriques des corps convexes, ou des espaces normés, de dimension finie mais très grande. Cette discipline a émergé d'une branche de l'Analyse, la théorie locale des espaces de Banach, qui vise à étudier les espaces de Banach de dimension infinie à travers leurs sous-espaces de dimension finie. L'investigation du comportement de diverses quantités lorsque la dimension, ou tout autre paramètre pertinent, tend vers l'infini (ou vers 0, selon le contexte), est un thème central dans de nombreux domaines des mathématiques. Par exemple, une large branche de la théorie des Probabilités étudie de telles problématiques. Mais les résultats-limites sont parfois peu efficaces lorsqu'ils ne sont pas quantifiés, et cette étape de quantification est souvent d'une difficulté supérieure. Plusieurs exemples viennent de la théorie des matrices aléatoires. Leur utilité pour l'Analyse Géométrique Asymptotique n'est plus à démontrer. Il est en effet connu depuis E. Gluskin que des méthodes probabilistes permettent d'exhiber des corps convexes dont les propriétés géométriques sont, en un certain sens, extrémales, tandis que les exemples explicites ou déterministes construits jusqu'ici sont très loin de posséder de telles propriétés. Ces techniques nécessitent de contrôler la norme (ou d'autres paramètres) d'opérateurs aléatoires.

Le modèle le plus simple de matrices aléatoires est l'Ensemble Gaussien Unitaire, objet paradigmatique qui reflète les propriétés asymptotiques d'une plus large classe d'ensembles matriciels. Il consiste en la donnée d'une matrice hermitienne de taille $n \times n$ dont les coefficients sont des variables aléatoires gaussiennes complexes (essentiellement) indépendantes. La norme d'une telle matrice, ainsi que sa plus grande valeur propre $\lambda_{\max}$, sous la normalisation adéquate, tendent presque sûrement vers une limite finie ℓ quand la dimension n tend vers l'infini. La phénomène de concentration de la mesure (dans notre cadre, pour la mesure gaussienne), outil fondamental utilisé notamment par V. Milman pour démontrer le théorème de Dvoretzky, nous permet d'écrire une inégalité de déviations pour $\lambda_{\max}$. Cette inégalité décrit bien la décroissance gaussienne dans le régime des grandes déviations. Cependant, elle passe à côté d'un autre phénomène, plus subtil, découvert par C. Tracy et H. Widom : $\lambda_{\max}$ fluctue autour de sa limite à l'échelle $n^{-2/3}$, nettement en deçà de l'échelle $n^{-1/2}$ usuelle dans le cadre gaussien. Cependant, le résultat de Tracy–Widom est un théorème-limite et peut difficilement être utilisé pour l'étude de matrices d'une taille donnée. Nous y remédions à travers l'inégalité suivante, qui constitue une version quantifiée du phénomène découvert par Tracy–Widom : pour toute dimension n et pour tout $\varepsilon > 0$

$$\mathbf{P}(\lambda_{\max} \geqslant \ell + \varepsilon) \leqslant C \exp\left(-cn \max(\varepsilon^{3/2}, \varepsilon^2)\right),$$

C et c étant des constantes universelles. Le régime $\varepsilon^{3/2}$ correspond aux petites déviations et le régime ε^2 aux grandes déviations, de type gaussien. Ce résultat a été obtenu indépendamment par M. Ledoux. Notre preuve, exposée dans le chapitre 1, utilise la méthode des polynômes orthogonaux (dans ce cas les polynômes de Hermite), qui repose sur la propriété d'invariance du modèle par conjugaison unitaire. La démonstration redonne également le théorème-limite de Tracy–Widom.

D'autres ensembles de matrices aléatoires ne jouissent pas des mêmes symétries et l'étude de leur spectre est plus délicate. Par exemple, fixons une variable aléatoire Z de loi ν, centrée et suffisamment régulière, et considérons une matrice dont les coefficients sont des copies indépendantes de Z. Le cas où Z est une gaussienne est relativement proche du cas décrit précédemment. Une telle matrice, à N lignes et n colonnes ($N \geqslant n$), peut être vue comme un opérateur de plongement de ℓ_2^n dans ℓ_2^N. Par un résultat de Z. Bai et Y. Yin, la distorsion (ou le nombre de conditionnement) de ce plongement, c'est-à-dire la manière dont la norme euclidienne est déformée, est contrôlée asymptotiquement (lorsque la dimension tend vers l'infini) par le rapport n/N. Il s'agit encore une fois d'un résultat-limite, sans analogue quantifié. Un problème géométrique équivalent est le suivant : soit N vecteurs aléatoires indépendamment distribués selon la mesure-produit $\nu^{\otimes n}$, est-ce que l'ellipsoïde d'inertie de la mesure $\nu^{\otimes n}$ est loin de l'ellipsoïde d'inertie empirique reconstitué à partir des N échantillons ? Il n'y a aucune raison de se restreindre à des mesures-produits pour ce problème d'échantillonnage. En termes de matrices aléatoires, cette généralisation revient à considérer des matrices dont seulement les lignes sont indépendantes, en autorisant des dépendances parmi les coefficients d'une même ligne. On sort ainsi de la théorie classique des matrices aléatoires. Le problème de l'approximation de la matrice d'inertie a été étudié dans le cas de la mesure uniforme sur un corps convexe, suite aux travaux de R. Kannan, L. Lovász et M. Simonovits en géométrie algorithmique : leur motivation était d'approcher efficacement la position isotrope d'un corps convexe. Des améliorations ont ensuite été obtenues par J. Bourgain ainsi que M. Rudelson. Jusqu'à présent, les seuls exemples connus de convexes dont l'ellipsoïde d'inertie est uniformément approximable avec un nombre d'échantillons proportionnel à la dimension (on ne peut espérer mieux) étaient les convexes dont toutes les marginales sont uniformément sous-gaussiennes, classe fort restreinte. Nous montrons qu'il en est de même pour la boule-unité de ℓ_1^n, corps convexe très différent de ces exemples. Notre preuve utilise un résultat de représentation de la mesure uniforme sur les boules-unités des espaces ℓ_p^n afin de se ramener au cas d'une matrice à coefficients indépendants, ainsi qu'un argument de concentration de la mesure pour rendre utilisable le résultat-limite de Bai–Yin. Cette idée a l'inconvénient d'être spécifique aux cas des espaces ℓ_p^n, aussi nous développons une autre approche. La preuve de Bai–Yin repose sur la combinatoire de la méthode des moments ; en relaxant cette combinatoire, on peut englober la classe des mesures log-concaves inconditionnelles sur $\mathbf{R}^n$. Pour ces mesures nous obtenons une conclusion plus faible : l'approximation *isomorphe*, et non plus *quasi-isométrique*. En contrepartie, le nombre d'échantillons nécessaire est réduit de manière spectaculaire à ρn, où $\rho > 1$ est un facteur arbitraire. Ce résultat est prouvé dans le chapitre 2.

Une autre idée centrale en Analyse Géométrique Asymptotique est la suivante : les corps convexes de grande dimension présentent des symétries cachées (ou tout au moins des symétries approximatives) qui ne sont décelables que lorsqu'on les regarde à travers une structure euclidienne adaptée. Autrement dit, étant donné un corps convexe, on cherche parmi toutes ses images affines la position la mieux équilibrée. Le choix d'une « bonne » position dépend du problème considéré : citons ainsi la M-position, la ℓ-position, ou bien la position isotrope évoquée précédemment. Nous illustrons ce principe à l'aide d'un nouvel exemple venu de la théorie quantique de l'information. Un problème fondamental dans ce domaine est la quantification du phénomène de l'intrication quantique. Cette problématique peut se reformuler en termes de géométrie convexe : l'ensemble $\mathcal{D}$ des états mélangés d'un système quantique est un corps convexe dans un espace de matrices, et le sous-ensemble $\mathcal{S}$ des états séparables (non-intriqués) est un corps convexe de même dimension. Récemment, S. Szarek a introduit des outils de l'Analyse Géométrique Asymptotique pour l'étude des relations géométriques (volumes, distances, etc) entre $\mathcal{D}$ et $\mathcal{S}$ dans le cadre des qubits. Nous poursuivons cette étude pour des particules quantiques plus complexes. L'une de nos principales découvertes est l'importance du rôle joué par la structure euclidienne induite par l'ellipsoïde de Löwner de $\mathcal{S}$. Cette structure, qui se combine agréablement avec le produit tensoriel projectif de corps convexes, objet que nous introduisons, permet par exemple d'obtenir un ordre de grandeur étonnant et asymptotiquement exact pour le volume de l'ensemble $\mathcal{S}$. Qui plus est, nous utilisons cette structure originale pour déduire des informations — asymptotiquement exactes, ici aussi — sur la géométrie de $\mathcal{S}$ vis-à-vis d'une structure euclidienne plus standard, celle induite par la norme de Hilbert–Schmidt, une question récemment étudiée dans une série d'articles de Gurvits et Barnum. Ces outils et ces résultats sont présentés dans le chapitre 3.

Les différents chapitres sont indépendants, les notations communes sont expliquées ci-après. Les trois chapitres ont une architecture similaire : la première partie est une introduction en français, qui motive et énonce les résultats. La seconde partie en anglais, qui contient les preuves des théorèmes, est un article de recherche, à des modifications mineures près. Ainsi, la partie

1.2 est publiée dans *Séminaire de Probabilités* [Aub1]. Les parties 3.2 (travail en collaboration avec S. Szarek) et 2.2 sont soumises à des revues internationales. Enfin, le chapitre 3 contient également quelques appendices dont le premier est un travail en collaboration avec S. Szarek et E. Werner.

On pourra trouver des versions ultérieures de ce manuscrit à l'adresse `http://www.institut.math.jussieu.fr/~aubrun/`

This Ph.D. thesis lies within the framework of Asymptotic Geometric Analysis, an expanding field dealing with the study of geometric properties of convex bodies, or of normed spaces, of large but finite dimension. This subject branched out from the local theory of Banach spaces, a subfield of Analysis aiming at studying infinite-dimensional Banach spaces through their finite-dimensional subspaces. Investigation of the behavior of various quantities when the dimension, or other relevant parameter, tends to infinity (or to 0, as appropriate) is a central theme in many areas of mathematics. For example, a major branch of Probability theory deals with such questions. However, limit results may be not-too-useful when non-quantified, and this quantification step is often of higher complexity. Several examples arise from random matrix theory. One hardly need to show today how useful random matrices are for Asymptotic Geometric Analysis: it is known since E. Gluskin that probabilistic methods allow to exhibit convex bodies having, in some sense, extremal geometric properties, a feature which rarely was achieved via explicit/deterministic examples. These techniques often require controlling norms (or other parameters) of random operators.

The simplest model of random matrices is the Gaussian Unitary Example, a central object reflecting asymptotic properties of a wider class of matrix ensembles. This model is the data of a complex $n \times n$ Hermitian matrix with entries being random Gaussian variables (essentially) independent. Under proper normalization, the norm of such a matrix, as well as its largest eigenvalue $\lambda_{\max}$, tend almost surely to a finite limit ℓ when the dimension n tends to infinity. The concentration of measure phenomenon (applied here for the Gaussian measure), a fundamental tool introduced by V. Milman in his proof of Dvoretzky's theorem, allows us to write a deviation inequality for $\lambda_{\max}$. This inequality provides a good description of Gaussian decay in the large deviation regime. However, it misses another phenomenon, more subtle, discovered by C. Tracy and H. Widom: $\lambda_{\max}$ fluctuates around its limit on the scale $n^{-2/3}$, clearly below the scale $n^{-1/2}$ usual in the Gaussian framework. However, the Tracy-Widom result was a limit statement, not very efficient when studying matrices of a particular size. We fill this gap with the following inequality, which constitutes a quantified version of the Tracy-Widom phenomenon: for any dimension n and any $\varepsilon > 0$,

$$\mathbf{P}(\lambda_{\max} \geqslant \ell + \varepsilon) \leqslant C \exp\left(-cn \max(\varepsilon^{3/2}, \varepsilon^2)\right),$$

C and c being universal constants. The rate $\varepsilon^{3/2}$ corresponds to small deviations whereas the rate ε^2 to large Gaussian-type deviations. This result has been independently obtained by M. Ledoux. Our proof, presented in chapter 1, uses orthogonal polynomials technique (in this case the Hermite polynomials), which depends on the invariance property of the model under unitary conjugation. In addition, our argument allows to reprove the limit theorems of Tracy and Widom.

Other random matrix ensembles have less symmetries than the Gaussian ensemble and the study of their spectrum is more tricky. Fix for example a random variable Z with law ν, centered and regular enough. Consider a matrix with independent copies of Z as entries. If Z is Gaussian, this is quite close to the previous model. Such a matrix, with N rows and n columns, can be thought of as an embedding operator from ℓ_2^n into ℓ_2^N. By a result of Z. Bai and Y. Yin, the distortion (or the condition number) of this embedding, which is the way the Euclidean norm is deformed, is asymptotically controlled (when sizes increase to infinity) by the ratio n/N. Here again this is a limit result, without quantified version available. An equivalent geometric problem is the following: given N independent random vectors distributed according to the product measure $\nu^{\otimes n}$, is the inertia ellipsoid of the measure $\nu^{\otimes n}$ far from the empirical inertia ellipsoid built from the N sample points? There is actually no reason for restricting oneself to product measures for this sampling problem. In the language of random matrices, this amounts to considering matrices with independent rows, but allowing dependencies within a single row. This setting goes beyond the classical random matrix theory. The sampling problem for the inertia matrix has been studied for the uniform measures on convex bodies, following the work of R. Kannan, L. Lovász and M. Simonovits in algorithmic geometry: their motivation was to efficiently approximate the isotropic position of a convex body. Improvements were then achieved by J. Bourgain, and M. Rudelson. The only known (to date) examples of convex bodies for which the inertia ellipsoid can be approximated using sample points whose number is linear in the dimension (we cannot hope for better) are those whose all marginals are uniformly sub-Gaussian, which is a very narrow class. We show that the same holds for the unit ball of ℓ_1^n, a body very far from those examples. Our proof uses a result on representation of the uniform measure on unit ball on ℓ_p^n spaces to get back a matrix with independent entries, as well as a concentration of measure argument which make usable the limit result of Bai–Yin. The drawback of this idea is its specificity to the ℓ_p^n spaces, therefore we develop another approach. The proof by Bai–Yin is based on the moment method; by generalizing the combinatorics involved there to a less restrictive setting we can encompass the wider class of all log-concave unconditional measures on $\mathbf{R}^n$. For these measures we obtain a weaker conclusion: *isomorphic* approximation instead of *almost isometric*. On the other hand, the number of sample points required dramatically reduces to ρn, where $\rho > 1$ is an arbitrary number. This result is proved in chapter 2.

Another central idea in Asymptotic Geometric Analysis is the following: high-dimensional convex bodies possess hidden symmetries (or at least approximate symmetries), which can only be revealed by introducing a proper Euclidean structure. To find it, for a given convex body, we have to seek among its affine images for the appropriately balanced position. The choice of a "good" position may depend on the problem: it could be for example the M-position, the ℓ-position, or the previously mentioned isotropic position. We illustrate this principle with a new example coming from quantum information theory. One fundamental question in that field is to quantify the phenomenon of quantum entanglement, which can be phrased as a convex geometry problem. Namely, the set $\mathcal{D}$ of mixed states of a quantum system is a convex body in a matrix space, and its subset, the set $\mathcal{S}$ of separable (non-entangled) states is also a convex body of the same dimension. Recently, S. Szarek introduced the methods of Asymptotic Geometric Analysis to the study of geometric relationships (such as volumes, distances etc.) between $\mathcal{D}$ and $\mathcal{S}$ in the case of qubits. We carry on this investigation to more complex quantum particles. One of our main discoveries is the significance of the Euclidean structure induced by the Löwner ellipsoid of $\mathcal{S}$. This structure nicely interplays with the projective tensor product of convex bodies, a notion which we introduce. It also enables us to obtain the order of magnitude of the volume of the set $\mathcal{S}$, a surprising and asymptotically sharp result. Moreover, we use this Euclidean structure to obtain information — also asymptotically sharp — on the geometry of $\mathcal{S}$ with respect to the more standard Euclidean structure induced by the Hilbert–Schmidt norm, the theme that has been recently studied in a series of papers by Gurvits and Barnum. All these results and concepts are presented in chapter 3.

Notations

Dans toute la thèse, les symboles $C, c, C', c', C_0, \ldots$ désigneront des constantes, dont la valeur peut varier librement d'une occurrence à l'autre. Par constante on entend constante universelle, strictement positive et finie, ne dépendant d'aucun paramètre. Les dépendances seront toujours précisées.

Lorsque l'on travaille dans l'espace euclidien $\mathbf{R}^n$, les coordonnées d'un vecteur x sont notées $(x_1, \ldots, x_n)$. Le produit scalaire est noté $\langle \cdot, \cdot \rangle$ et la norme euclidienne associée est notée $|\cdot|$. La boule-unité est $B_2^n = \{x \in \mathbf{R}^n;\ |x| \leqslant 1\}$ et la sphère-unité est $S^{n-1} = \{x \in S^{n-1}, |x| = 1\}$. La mesure de Lebesgue sur $\mathbf{R}^n$ est notée $\mathrm{vol}(\cdot)$. Si A et B sont des parties de $\mathbf{R}^n$, et α un réel, on utilise les notations

$$\alpha A = \{\alpha a;\ a \in A\},$$

$$A + B = \{a + b;\ a \in A, b \in B\}.$$

Un *corps convexe* dans $\mathbf{R}^n$ est une partie convexe compacte d'intérieur non vide. Un corps convexe K est dit *symétrique* s'il est symétrique par rapport à l'origine, c'est-à-dire si $K = -K$. Un corps convexe de $\mathbf{R}^n$ est dit *inconditionnel* s'il est symétrique par rapport aux hyperplans de coordonnées, c'est-à-dire si pour tout choix de signes $(\varepsilon_i) \in \{-1, 1\}^n$, on a

$$(x_1, \ldots, x_n) \in K \Longleftrightarrow (\varepsilon_1 x_1, \ldots, \varepsilon_n x_n) \in K.$$

De même, une mesure μ sur $\mathbf{R}^n$ est dite inconditionnelle si elle vérifie pour toute partie borélienne B et pour tout choix de signes $(\varepsilon_i) \in \{-1, 1\}^n$

$$\mu(B) = \mu\left(\{(\varepsilon_1 x_1, \ldots, \varepsilon_n x_n);\ x \in B\}\right).$$

Pour $1 \leqslant p < +\infty$, on définit la norme ℓ_p sur $\mathbf{R}^n$ par

$$\|(x_1, \ldots, x_n)\|_p = \left(\sum_{i=1}^n |x_i|^p\right)^{1/p}.$$

Cette définition s'étend au cas $p = +\infty$ en posant

$$\|(x_1, \ldots, x_n)\|_\infty = \max_{1 \leqslant i \leqslant n} |x_i|.$$

La boule-unité associée est définie par

$$B_p^n = \{x \in \mathbf{R}^n;\ \|x\|_p \leqslant 1\}.$$

Les boules B_p^n sont des exemples de corps convexes inconditionnels. On note $\mathrm{conv}(A)$ l'enveloppe convexe d'un ensemble $A \subset \mathbf{R}^n$ et $\mathrm{ext}(K)$ l'ensemble des points extrémaux d'un convexe K.

Toutes les variables aléatoires que nous considérerons seront définies sur un espace probabilisé $(\Omega, \mathcal{A}, \mathbf{P})$ suffisamment gros. On note $\mathbf{E}$ l'espérance associée à $\mathbf{P}$. Si X est une variable aléatoire de loi μ, on écrit $X \overset{\mathscr{L}}{\sim} \mu$. On fera communément l'abus de langage d'identifier une variable aléatoire et sa loi. On désigne par δ_x la masse de Dirac au point x. L'abréviation i.i.d. signifie « indépendantes et identiquement distribuées ». On désigne par $N(0, \sigma^2)$ la mesure de probabilité gaussienne sur $\mathbf{R}$ de variance σ^2, donnée par la densité

$$\frac{dN(0,\sigma^2)}{dx} = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{x^2}{2\sigma^2}\right).$$

Un vecteur gaussien est un vecteur aléatoire $(X_1, \dots, X_n)$ tel que toute combinaison linéaire des (X_i) est une variable aléatoire gaussienne. Un exemple de vecteur gaussien sur $\mathbf{R}^n$ est le vecteur gaussien *standard*, noté $G_{\mathbf{R}^n}$ et dont les coordonnées, dans n'importe quelle base orthonormale, sont des variables gaussiennes $N(0,1)$ indépendantes. On dit d'une variable aléatoire complexe X qu'elle suit la loi $N_{\mathbf{C}}(0, 2\sigma^2)$ si elle se décompose en $X = Y + \imath Z$, où Y et Z sont des variables i.i.d. $N(0, \sigma^2)$. On dit d'une suite (μ_n) de mesures boréliennes sur un espace métrique T qu'elle converge étroitement vers μ si pour toute fonction f continue bornée sur T, on a

$$\lim_{n\to\infty} \int_T f d\mu_n = \int_T f d\mu.$$

Si X est une variable aléatoire, et $\alpha \in [1,2]$, la norme Ψ_α de X est donnée par

$$\|X\|_{\Psi_\alpha} = \inf\{t > 0;\ \mathbf{E}\exp(|X/t|^\alpha) \leqslant 2\}.$$

Si $\|X\|_{\Psi_\alpha} \leqslant C < \infty$, on dit que X est Ψ_α avec constante C. Le lemme suivant est classique

Lemme 1. *Il existe des constantes universelles c, C telles que pour tout $\alpha \in [1,2]$ et pour toute variable aléatoire X telle que $\|X\|_{\Psi_\alpha} < \infty$, on ait*

$$c\|X\|_{\Psi_\alpha} \leqslant \sup_{p \geqslant 1} \frac{(\mathbf{E}|X|^p)^{1/p}}{p^{1/\alpha}} \leqslant C\|X\|_{\Psi_\alpha}.$$

Démonstration. On peut supposer par homogénéité que $\|X\|_{\Psi_\alpha} = 1$, c'est-à-dire $\mathbf{E}\exp(|X|^\alpha) = 2$. L'inégalité de droite est une conséquence de l'inégalité de Markov : on obtient pour tout $u > 0$

$$\mathbf{P}(|X| \geqslant u) \leqslant 2\exp(-u^\alpha).$$

L'inégalité de gauche s'obtient en développant $\exp(|X|^\alpha)$ en série entière. $\square$

Dans ce paragraphe, le corps $\mathbf{K}$ désignera toujours $\mathbf{R}$ ou $\mathbf{C}$. On note $\mathcal{B}(E)$ l'espace des endomorphismes d'un $\mathbf{K}$-espace vectoriel E ; $\mathcal{B}(\mathbf{K}^n)$ est aussi l'espace des matrices carrées de taille n. On note Id la matrice identité. Les coefficients d'une matrice $A \in \mathcal{B}(\mathbf{K}^n)$ dans la base canonique sont notés $(a_{ij})_{1 \leqslant i,j \leqslant n}$. Si A est une matrice complexe, $A^\dagger$ désigne la transconjuguée de A. Dans le cas où A est une matrice réelle, $A^\dagger$ est simplement la transposée de A. Une matrice A telle que $A = A^\dagger$ est autoadjointe ; on note $\mathcal{B}_{sa}(E)$ l'ensemble des éléments autoadjoints de $\mathcal{B}(E)$. On note $\mathcal{U}(\mathbf{C}^n)$ ou $\mathcal{U}_n$ le groupe unitaire. Si une matrice A est autoadjointe, ses valeurs propres sont réelles et on les range dans l'ordre croissant (en les comptant avec multiplicité) :

$$\lambda_{\min}(A) = \lambda_n(A) \leqslant \cdots \leqslant \lambda_1(A) = \lambda_{\max}(A).$$

Si A et B sont des matrices autoadjointes, la notation $A \leqslant B$ signifie que la matrice $B - A$ est positive (c'est-à-dire $\lambda_{\min}(B - A) \geqslant 0$). Si A est une matrice $p \times n$, avec $p \geqslant n$, les *valeurs singulières* de A sont, par définition, les racines carrées des valeurs propres de $A^\dagger A$

$$0 \leqslant s_{\min(A)} = \sqrt{\lambda_{\min}(A^\dagger A)} \leqslant \cdots \leqslant s_{\max}(A) = \sqrt{\lambda_{\max}(A^\dagger A)}.$$

L'espace $\mathcal{B}(\mathbf{K}^n)$, (ainsi que ses sous-espaces) est muni d'une mesure de Lebesgue (notée dA) induite par le produit scalaire de Hilbert–Schmidt

$$\langle A, B \rangle_{HS} = \mathrm{tr} A^\dagger B.$$

La norme associée à ce produit scalaire, appelée norme de Hilbert–Schmidt, s'écrit

$$\|A\|_{HS} = \left(\sum_{i=1}^{n} s_i(A)^2 \right)^{1/2} = \left(\sum_{i,j=1}^{n} |a_{ij}|^2 \right)^{1/2}.$$

Si E et F sont des $\mathbf{K}$-espaces vectoriels, $E \otimes F$ est le produit tensoriel de E par F. Dans le cas où E et F sont munis d'un produit scalaire, on peut construire naturellement un produit scalaire sur $E \otimes F$, en posant pour $x, x' \in E$ et $y, y' \in F$

$$\langle x \otimes y, x' \otimes y' \rangle = \langle x \otimes x' \rangle_E \langle y \otimes y' \rangle_F,$$

qui se prolonge bilinéairement de manière unique à l'espace tout entier. L'espace $E \otimes F$, muni de ce produit scalaire, est noté $E \otimes_2 F$; c'est le *produit tensoriel hilbertien* de E et F. Tout ceci se généralise immédiatement à des produits tensoriels de plus de deux facteurs. Si $x \in \mathbf{K}^n$ et $y \in \mathbf{K}^m$, on désigne par $|x\rangle\langle y|$ l'opérateur de rang 1 de $\mathbf{K}^m$ dans $\mathbf{K}^n$ défini par

$$\forall z \in \mathbf{K}^m, \quad |x\rangle\langle y|(z) = \langle y, z \rangle x.$$

Si (T, d) est un espace métrique compact et $\varepsilon > 0$, un ε-réseau de T est une partie finie $\mathcal{N} \subset T$ telle que tout point de T est à distance au plus ε d'au moins un point de $\mathcal{N}$. On utilisera le résultat suivant, prouvé classiquement par un argument volumique (cf [Pis], Lemma 4.10)

Lemme 2. *Pour tout $\varepsilon > 0$ et pour tout entier n, il existe un ε-réseau de S^{n-1} (pour la distance euclidienne) de cardinal inférieur à $(1 + 2/\varepsilon)^n$.*

Pour les notations qui ne seraient expliquées ici, nous renvoyons aux références standard en Analyse Géométrique Asymptotique [Pis, Tom, MS, LQ].

Chapitre 1

Petites déviations pour la norme d'une matrice aléatoire

1.1 Introduction et présentation des résultats

Un objet central dans la théorie des matrices aléatoires est l'Ensemble Gaussien Unitaire (GUE). Une description en est la suivante : il s'agit, pour chaque dimension n, d'une mesure de probabilité $\mathbf{P}_n$ sur l'espace $\mathcal{B}_{sa}(\mathbf{C}^n)$ donnée par la densité :

$$d\mathbf{P}_n = \frac{1}{c_n} \exp\left(-\frac{n}{2}\mathrm{tr}A^2\right) dA.$$

Ici c_n est une constante de normalisation. La mesure $\mathbf{P}_n$ est invariante par conjugaison unitaire. Elle peut être caractérisée par la construction alternative suivante : soit $B \in \mathcal{B}(\mathbf{C}^n)$ une matrice aléatoire dont les n^2 coefficients sont des variables aléatoires gaussiennes complexes de loi $N_{\mathbf{C}}(0, 1/n)$. Soit A la partie autoadjointe de B, définie par $A = \frac{1}{2}(B + B^\dagger)$. Alors A est distribuée selon la mesure $\mathbf{P}_n$. En particulier, aux contraintes de symétrie près, les coefficients d'une matrice du GUE sont des variables aléatoires indépendantes. Ceci est même une caractérisation du GUE : toute mesure de probabilité sur $\mathcal{B}_{sa}(\mathbf{C}^n)$ invariante par conjugaison unitaire et telle que les variables aléatoires $(a_{ij})_{1 \leqslant i \leqslant j \leqslant n}$ sont indépendantes se déduit de $\mathbf{P}_n$ par une transformation affine (voir [Meh], livre auquel nous renvoyons systématiquement pour tout ce qui suit). Cette propriété fait du GUE un objet modèle, dont on conjecture que les propriétés asymptotiques (quand la dimension n tend vers $+\infty$) sont universelles, c'est-à-dire qu'elles sont communes à une large famille d'ensembles matriciels de construction similaire.

Si A est une matrice de $\mathcal{B}_{sa}(\mathbf{C}^n)$, on note μ_A la mesure spectrale empirique associée à A, définie par

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

Si B est un borélien de $\mathbf{R}$, $\mu_A(B)$ est la proportion de valeurs propres de la matrice A qui appartiennent à l'ensemble B. Lorsque A est un élément du GUE (c'est-à-dire une matrice aléatoire distribuée selon $\mathbf{P}_n$), la mesure μ_A est une mesure de probabilité aléatoire sur $\mathbf{R}$. Un résultat célèbre de Wigner précise le comportement asymptotique de cette mesure : elle converge vers une mesure déterministe dont la densité a la forme d'un demi-cercle. Plus précisément, si pour chaque dimension n, $A^{(n)}$ est une matrice aléatoire distribuée selon $\mathbf{P}_n$, alors, presque sûrement, la suite de mesures empiriques $(\mu_{A^{(n)}})$ converge étroitement vers la mesure μ_c, de support l'intervalle $[-2, 2]$ et donnée par la densité

$$d\mu_c := \frac{1}{2\pi} 1_{[-2,2]} \sqrt{4 - x^2} dx.$$

Ce résultat précise le comportement global du spectre de la matrice ; on dit qu'il s'agit du *régime global*. On ne peut rien en déduire sur le comportement asymptotique de la plus grande valeur propre de la matrice A. Néanmoins, le *régime local* aux extrémités du spectre est également connu (voir [Bai]) : presque sûrement, les valeurs propres extrêmes convergent vers le bord du support de la mesure-limite

$$\lim_{n\to\infty} \lambda_{\max}(A^{(n)}) = 2 \quad \text{et} \quad \lim_{n\to\infty} \lambda_{\min}(A^{(n)}) = -2.$$

Bien évidemment, grâce aux symétries de la mesure $\mathbf{P}_n$, il est complètement équivalent de travailler sur $\lambda_{\max}$ ou sur $\lambda_{\min}$. Notons également que ces résultats de convergence presque sûrs sont valables dans un contexte beaucoup plus général que celui du GUE (voir par exemple [Bai]).

Un problème plus délicat est celui des fluctuations de la plus grande valeur propre autour de sa limite ; Tracy et Widom ([TW1]) ont montré que l'ordre de grandeur de ces fluctuations est de $n^{-2/3}$, ce qui peut paraître surprenant car très différent de la situation « habituelle », comme dans le théorème central limite, où les fluctuations sont en $n^{-1/2}$. Plus précisément, Tracy et Widom ont montré la convergence en distribution

$$\lim_{n\to\infty} n^{2/3}(\lambda_{\max}(A^{(n)}) - 2) \to TW.$$

où la variable aléatoire TW est distribuée selon une loi de probabilité explicite, mais dont la description demeure compliquée (on trouvera plus de détails dans la partie 1.2.3). Cette même distribution-limite apparaît aussi dans le calcul des fluctuations pour d'autres quantités : par exemple pour la plus grande sous-suite croissante d'une permutation aléatoire des n premiers entiers (voir [Led3] pour plus de précisions, et d'autres exemples où cette loi-limite apparaît). La queue (positive) de la distribution TW vérifie l'encadrement

$$\forall x \geqslant 0, \quad c' \exp(-C' x^{3/2}) \leqslant \mathbf{P}(TW \geqslant x) \leqslant c \exp(-C x^{3/2}).$$

Cette estimation peut être déduite à partir d'une description de la loi TW en termes de fonctions de Painlevé obtenue dans [TW1] ; cependant la preuve de cette description est délicate. Dans la partie 1.2.5, nous donnons une preuve à l'aide de la représentation déterminantale, qui est un outil plus standard.

En analyse géométrique asymptotique, il est important de disposer d'inégalités valides en toute dimension, plutôt que de résultats-limites dont l'utilité pratique est souvent limitée. On aimerait ainsi une borne supérieure pour la probabilité

$$\mathbf{P}(\lambda_{\max}(A^{(n)}) \geqslant 2 + \varepsilon),$$

qui reflète le comportement découvert par Tracy et Widom. De telles inégalités de déviations peuvent parfois être démontrées par des principes généraux de concentration (voir [Led1]). L'inégalité de concentration gaussienne est valable pour n'importe quelle fonction lipschitzienne d'un vecteur gaussien dans $\mathbf{R}^N$. En identifiant $\mathcal{B}_{sa}(\mathbf{C}^n)$ à $\mathbf{R}^{n^2}$, la plus grande valeur propre entre dans ce cadre. Comme par ailleurs l'inégalité $\mathbf{E}\lambda_{\max}(A^{(n)}) \leqslant 2$ est connue (voir [Sza]), cela donne

$$\forall \varepsilon > 0,\ \mathbf{P}(\lambda_{\max}(A^{(n)}) \geqslant 2 + \varepsilon) \leqslant \exp(-n\varepsilon^2/2). \tag{1.1}$$

Cette inégalité est valable en toute dimension ; cependant elle n'est pas asymptotiquement optimale pour des petites valeurs de ε. Prenons par exemple $\varepsilon = tn^{-2/3}$ pour t fixé. Lorsque la dimension n tend vers l'infini, le membre de gauche de (1.1) tend vers une limite $l \in]0,1[$, tandis que le membre de droite tend vers 1 ; et pour t petit on a $l \ll 1$. De fait, l'inégalité (1.1) est une inégalité de grandes déviations. Il est en fait possible de quantifier le théorème de Tracy–Widom et nous obtenons ainsi le résultat suivant, qui est exact pour le régime des petites déviations

Proposition 1.1 : *Il existe des constantes universelles C et c telles que pour tout $t \geqslant 0$ et tout entier n, on ait*

$$\mathbf{P}_n(\lambda_1(A^{(n)}) \geqslant 2 + t) \leqslant C \exp(-cnt^{3/2}).$$

Comme $\|A\| = \max(\lambda_{\max}(A), -\lambda_{\min}(A))$, on a aussi une inégalité similaire pour la norme de $A^{(n)}$. Notons que le même résultat a été obtenu indépendamment par M. Ledoux ([Led2]), par une approche différente. Le plan de notre preuve est simple : suivre pas à pas la preuve de Tracy et Widom en prenant soin à chaque étape de contrôler les différentes quantités impliquées de manière uniforme. Cela nécessite en particulier d'utiliser certaines estimations sur des fonctions spéciales. La preuve du résultat est présentée dans la section suivante, où les outils nécessaires sont également introduits. Nous obtenons en réalité un résultat formellement plus fort que la proposition 1.1 : la convergence $n^{2/3}(\lambda_{\max}(A^{(n)}) - 2) \to TW$ a lieu au sens d'une distance de Wasserstein sur $\mathbf{R}$ associée à un coût adapté au problème ; nous renvoyons à la section 1.2.1 pour plus de détails.

1.2 A sharp small deviation inequality for the largest eigenvalue of a random matrix

We prove that the convergence of the largest eigenvalue λ_1 of a $n \times n$ random matrix from the Gaussian Unitary Ensemble to its Tracy–Widom limit holds in a strong sense, specifically with respect to an appropriate Wasserstein-like distance. This unifying approach allows us both to recover the limiting behavior and to derive the inequality $\mathbf{P}(\lambda_1 \geqslant 2 + t) \leqslant C \exp(-cnt^{3/2})$, valid uniformly for all n and t. This inequality is sharp for "small deviations" and complements the usual "large deviation" inequality obtained from the Gaussian concentration principle. Following the approach by Tracy and Widom, the proof analyses several integral operators, which converge in the appropriate sense to an operator whose determinant can be estimated.

Introduction

Let $\mathcal{H}_n$ be the set of n-dimensional (complex) Hermitian matrices. The general element of $\mathcal{H}_n$ is denoted $A^{(n)}$, and its entries are denoted $(a_{ij}^{(n)})$.

We exclusively focus on the Gaussian Unitary Ensemble GUE, which can be defined by the data of a probability measure $\mathbf{P}_n$ on $\mathcal{H}_n$ which fulfills the following conditions

1. The n^2 random variables $(a_{ii}^{(n)}), (\Re a_{ij}^{(n)})_{i<j}, (\Im a_{ij}^{(n)})_{i<j}$ are independent,
2. $\forall i, a_{ii}^{(n)}$ follows the Gaussian law $N(0, 1/n)$,
3. $\forall i < j, \Re a_{ij}^{(n)}$ and $\Im a_{ij}^{(n)}$ follow the Gaussian law $N(0, 1/2n)$.

The measure $\mathbf{P}_n$ is uniquely determined by these three conditions because of the extra symmetry constraint $a_{ij} = \overline{a_{ji}}$; it can also be made explicit. $\mathcal{H}_n$ is a vector space on which the scalar product $\langle u, v \rangle := \operatorname{tr}(uv)$ induces an Euclidean structure, hence a Lebesgue measure. The probability measure $\mathbf{P}_n$ has a density with respect to this Lebesgue measure, which can be shown to equal

$$d\mathbf{P}_n := \frac{1}{c_n} \exp(-\frac{n}{2} \operatorname{tr} M^2) dM,$$

where c_n is a normalization constant.

The GUE has the wonderful property of invariance under rotation : indeed the measure $\mathbf{P}_n$ is invariant under the conjugation action of the unitary group. This makes calculations easier and is very useful for the study of eigenvalues, which are also invariant under the same action.

From now on, "random matrix" means "element of $(\mathcal{H}_n, \mathbf{P}_n)$" seen as a probability space. Let $(\Omega, \mathbf{P})$ denote the product of all these probability spaces $\prod_{i=n}^{\infty}(\mathcal{H}_n, \mathbf{P}_n)$; an element of Ω is a sequence of random matrices, the nth matrix being of size n. However, for all the questions we shall consider, the relationships between the $\mathcal{H}_n$'s for different n's are immaterial.

For more background, we refer the reader to the monograph [Meh]. Let $\lambda_1(A^{(n)}) \geqslant \lambda_2(A^{(n)}) \geqslant \cdots \geqslant \lambda_n(A^{(n)})$ be the ordered eigenvalues of a random matrix $A^{(n)}$. The global asymptotic behavior of these eigenvalues is well-known. The most famous result in this topic is the semi-circle law, which can be stated as follows : let $N(A^{(n)})$ be the probability measure on $\mathbb{R}$ derived from the random matrix $A^{(n)}$ in the following way (δ_x denotes the Dirac mass at point x)

$$N(A^{(n)}) := \sum_{k=1}^{n} \delta_{\lambda_k(A^{(n)})}.$$

Then, $\mathbf{P}$-almost surely, the sequence of probabilities $(N(A^{(n)}))$ converges weakly to a deterministic measure μ_c, with a density with respect to Lebesgue measure given by

$$d\mu_c := \frac{1}{2\pi} 1_{[-2,2]} \sqrt{4 - x^2} dx.$$

We are interested here in the asymptotic behavior of the largest eigenvalue $\lambda_1(A^{(n)})$, which is a so-called local problem. Classical results (see e.g. [DS], also for precise references to the original articles) claim that

$$\lim_{n \to \infty} \lambda_1(A^{(n)}) = 2 \quad \mathbf{P}\text{-almost surely.}$$

The asymptotic behavior of $\lambda_1(A^{(n)})$ was further clarified by Tracy and Widom, who proved the following result : there exists a continuous decreasing function ψ_{TW} from $\mathbb{R}$ onto $(0, 1)$ such that

$$\lim_{n \to \infty} \mathbf{P}_n(\lambda_1(A^{(n)}) \geqslant 2 + xn^{-2/3}) = \psi_{\mathrm{TW}}(x). \tag{1.2}$$

This function ψ_{TW} naturally arises as a determinant linked to the so-called "Airy kernel", which will be defined later. The most difficult point of Tracy and Widom's work was to show that this function ψ_{TW} can be written in terms of a Painlevé function (see [TW1]). From this point one can deduce the asymptotic behavior of ψ_{TW} around $+\infty$ and find universal positive constants C, c, C', c' such that for x large enough

$$c' \exp(-C'x^{3/2}) \leqslant \psi_{\mathrm{TW}}(x) \leqslant c \exp(-Cx^{3/2}). \tag{1.3}$$

The remainder of this article is organized as follows : in section 1.2.1, we define an appropriate Wasserstein distance and state our main theorem which asserts that Tracy–Widom convergence holds in this strong distance. In section 1.2.2, we derive from this theorem the small deviation inequality and compare it with the classical one. Section 1.2.3 introduces the needed framework of determinantal kernels, which are classical in this field, and section 1.2.4 contains the proof of the main theorem. Finally, section 1.2.5 contains an alternative simple deviation of upper bounds (1.3) for Tracy–Widom distribution.

1.2.1 Convergence in terms of a Wasserstein distance

We call tail function of a measure μ on $\mathbb{R}$ the function $\psi_\mu : \mathbb{R} \to [0,1]$ defined by $\psi_\mu(x) := \mu((x,+\infty))$. Such a function is decreasing, left-continuous, tends to 1 at $-\infty$ and to 0 at $+\infty$. The tail function just equals 1 minus the cumulative distribution function. The function appearing in the r.h.s. of (1.2) is the tail function of the Tracy–Widom distribution on $\mathbb{R}$ (we denote this distribution by TW).

We want to prove that the law of the rescaled largest eigenvalue tends to the Tracy–Widom law in a strong sense. As we only focus on the upper tail, we can consider truncated laws, supported on an interval $[a,+\infty)$ for some real a. Let Λ_n^a be the probability measure with tail function defined by

$$\psi_{\Lambda_n^a}(x) = \begin{cases} \mathbf{P}_n(\lambda_1(A^{(n)}) \geqslant 2 + xn^{-2/3}) & \text{if } x \geqslant a \\ 1 & \text{if } x < a \end{cases} .$$

Similarly, let TW^a be the truncated Tracy–Widom law defined by

$$\psi_{\mathrm{TW}^a}(x) = \begin{cases} \psi_{\mathrm{TW}}(x) & \text{if } x \geqslant a \\ 1 & \text{if } x < a \end{cases} .$$

We are going to show that for any a, Λ_n^a tends to TW^a with respect to the distance defined through a mass transportation problem in its Monge–Kantorovich formulation (see [RR]).

A mass transportation problem is the question of optimizing the transshipment from a measure to another with respect to to a given cost. More precisely, let μ and ν be two probability measures on the same space X, and $c : X \times X \to \mathbb{R}_+$ a symmetric function vanishing on the diagonal ($c(x,y)$ represent the price to pay to transfer a unit of mass from x to y). Ways to carry μ onto ν are represented through probability measures π on the square space $X \times X$ having μ and ν as marginals (this means that for any measurable subset A of X, $\pi(A \times X) = \mu(A)$ and $\pi(X \times A) = \nu(A)$). We denote by $\Pi(\mu,\nu)$ the space of such π.

The Wasserstein distance associated with the problem is the "minimum cost to pay", defined by

$$d(\mu,\nu) = \inf_{\pi\in\Pi(\mu,\nu)} \int_{X^2} c(x,y)d\pi(x,y).$$

We are going to consider a very special case of this problem. Let us suppose that $X = \mathbb{R}$ and that the cost c is defined as follows

$$c(x,y) := \left| \int_x^y w(t)dt \right|, \tag{1.4}$$

where w is a positive function.

We can now state the main result of this note

Theorem 1.1. *Let $w(x) := \exp(\gamma x^{3/2})$ and let d be the Wasserstein distance associated with the cost induced by w via the formula (1.4). Then, for any fixed $a \in \mathbb{R}$, if $\gamma > 0$ is small enough, Λ_n^a tends to TW^a for the distance d*

$$\lim_{n\to\infty} d(\Lambda_n^a, TW^a) = 0.$$

1.2.2 The small deviation inequality

The simplest idea to get concentration inequalities for the largest eigenvalue of a GUE random matrix is to use Gaussian concentration ; it is a straightforward consequence of the measure concentration phenomenon in the Gaussian space (see [DS]) that

$$\forall t > 0, \forall n, \mathbf{P}_n(\lambda_1(A^{(n)}) \geqslant M_n + t) < \exp(-nt^2/2), \tag{1.5}$$

where M_n is the median of $\lambda_1(A^{(n)})$ with respect to the probability measure $\mathbf{P}_n$. One has the same upper estimate is the median M_n is replaced by the expected value $\mathbb{E}_n\lambda_1(A^{(n)})$.

The value of M_n can be controlled : for example we have $M_n \leqslant 2+c/\sqrt{n}$. This will be for example a consequence of our Proposition. Plugging this into the equation (1.5), we get the following result, where C is a universal constant

$$\forall t > 0, \forall n, \mathbf{P}_n(\lambda_1(A^{(n)}) \geqslant 2 + t) < C\exp(-nt^2/2). \tag{1.6}$$

It has been proved after the redaction of this note in [Sza] (Appendix F) that $\mathbb{E}_n\lambda_1(A^{(n)}) \leqslant 2$. This was done using the Harer–Zagier recurrence formula for the expected moments of the empirical measure. Note that the situation for the GOE (Gaussian Orthogonal Ensemble), an ensemble of real symmetric matrices defined in a similar way as GUE (see [Meh] for a precise definition), is much simpler since we can use standard comparison techniques for (real) Gaussian vectors, such as Slepian's lemma. The proof can be found in [DS], it is very similar to the ideas presented in Appendix 3.3.4 in a different context. Note also that since the function λ_1 is convex, its median with respect to $\mathbf{P}_n$ does not exceed its expected value ([Kwa]). This implies that one can choose $C = 1$ in the inequality (1.6). There are similar though not as simple results for $\mathbf{P}_n(\lambda_1(A^{(n)}) \leqslant 2 - t)$, but in this paper we will concentrate on the "upper tail" estimates.

The result of Tracy and Widom (1.2) shows that the majoration (1.6) is not optimal for very small values of t. If for example t is equal to $xn^{-2/3}$ for a fixed x, then the right-hand side in concentration inequality (1.6) tends to 1 when n grows to ∞, whereas the left-hand side tends to $\psi_{\mathrm{TW}}(x)$, which can be very small.

We would like to derive from our Theorem a deviation inequality which would improve the inequality (1.6) for small values of t. For this purpose, the uniform convergence in (1.2) (which, by Dini's theorem, follows formally form the pointwise convergence) is not enough. But we will prove in this section that our Theorem implies the following Proposition :

Proposition 1.1. *There exist positive universal constants C and c such that for every positive t and any integer n*

$$\mathbf{P}_n(\lambda_1(A^{(n)}) \geqslant 2 + t) \leqslant C \exp(-cnt^{3/2}). \tag{1.7}$$

Of course, by symmetry of the law $\mathbf{P}_n$, similar results are true for the smallest eigenvalue $\lambda_n(A^{(n)})$

$$\mathbf{P}_n(\lambda_n(A^{(n)}) \leqslant -2 - t) \leqslant C \exp(-cnt^{3/2}). \tag{1.8}$$

Using the fact that for a Hermitian matrix A, the norm equals the maximum absolute value of an eigenvalue, we get a similar estimate for $||A^{(n)}||$

$$\mathbf{P}_n(||A^{(n)}|| \geqslant 2 + t) \leqslant C \exp(-cnt^{3/2}). \tag{1.9}$$

We need the following lemma to prove the proposition, which will help us to explicitly compute Wasserstein distance

Lemma 3. *Suppose that the measures μ and ν are defined on $\mathbb{R}$, and that the cost c is defined by an integral, as in (1.4). If μ and ν are regular enough,* *for example if ψ_μ and ψ_ν are piecewise C^1, then the Wasserstein distance for the cost c equals*

$$d(\mu,\nu)=\int_{-\infty}^{\infty} w(t)|\psi_\mu(t)-\psi_\nu(t)|dx. \tag{1.10}$$

Proof. In fact, this transportation problem is explicitly solvable. For a one-dimensional problem with a cost satisfying the Monge condition (which is always the case when the cost is defined using an integral as in (1.4)), the optimal transshipment is achieved through the map T defined as follows (see [RR], chapter 3.1)

$$\int_{-\infty}^{x} d\mu=\int_{-\infty}^{T(x)} d\nu.$$

Thus, we can compute the value of $d(\mu,\nu)$

$$d(\mu,\nu)=\int_0^1 c(\psi_\mu^{-1}(u),\psi_\nu^{-1}(u))du.$$

Let us consider first the particular case when $\psi_\mu \leqslant \psi_\nu$. This allows us to drop the absolute values in the definition of c (see (1.4)) and unfold the calculations. Using the appropriate changes of variables, we come to the equality (1.10).

For general μ and ν, define $\mu\wedge\nu$ and $\mu\vee\nu$ using their tail functions

$$\psi_{\mu\wedge\nu}(x)=\min(\psi_\mu(x),\psi_\nu(x)) \quad \text{and} \quad \psi_{\mu\vee\nu}(x)=\max(\psi_\mu(x),\psi_\nu(x)).$$

We easily check that $\psi_{\mu\wedge\nu}\leqslant\psi_{\mu\vee\nu}$, $d(\psi_\mu,\psi_\nu)=d(\psi_{\mu\wedge\nu},\psi_{\mu\vee\nu})$ and that the value of the r.h.s. of (1.10) does not change if we replace ψ_μ and ψ_ν by $\psi_{\mu\wedge\nu}$ and $\psi_{\mu\vee\nu}$. This yields the conclusion for the general case. □

Using this lemma, we get from our theorem (with $a=0$), using the upper bound (1.3) for ψ_{TW}, the uniform estimate

$$\int_0^{\infty} w(x)\mathbf{P}_n(\lambda_1(A^{(n)})\geqslant 2+xn^{-2/3})\,dx\leqslant C,$$

which implies immediately for $x\geqslant 1$ (keep in mind that ψ_n is decreasing)

$$\psi_n(x)\leqslant C\exp(-\gamma(x-1)^{3/2})\leqslant C'\exp(-\gamma' x^{3/2}). \tag{1.11}$$

This is, up to the rescaling $t=xn^{-2/3}$, the content of the proposition.

Now we can also easily show that our theorem implies the Tracy–Widom limit (1.2) : using the uniform bound (1.11) and Lebesgue's convergence theorem, we get from the Theorem that ψ_{TW} is the pointwise limit of the ψ_n's on $[a, +\infty)$, and thus on the whole real line if we let a go to $-\infty$.

It should be emphasized that recently (independently from and slightly preceding this work), this small deviations result has been proved by Ledoux in [Led2] using an argument based on the Harer–Zagier recurrence formula (see [HT] for a simple proof of this formula). The same paper by Ledoux contains another proof based on hypercontractivity which gives the result up to a polynomial factor ; this method works also for the Laguerre Unitary Ensemble (see [Led2] for the definition). However, the existence of a Tracy–Widom limit does not follow from this approach. More generally, many contributions to this and related topics either address the limit behavior or provide dimension-free bounds, rarely combining the two. Our technique captures both phenomena in a single "stroke".

1.2.3 Relation to determinants

The remainder of this note is devoted to the proof of the main theorem. For simplicity, we will prove only the case $a = 0$, and drop all the superscripts. The proof for a general a requires only routine modifications.

We are first going to express all involved quantities in terms of determinants of certain operators. This is quite classical work due to Gaudin and Mehta (see [Meh]). Part of the calculations done here are present, at least implicitly, in the paper by Tracy and Widom ([TW1]).

We need new notation. Let (H_n) be the Hermite polynomials, which are defined by

$$H_n(t) := (-1)^n \exp(t^2)(\frac{d}{dt})^n \exp(-t^2).$$

They are orthogonal for the measure on $\mathbb{R}$ of density $\exp(-x^2)$ with respect to Lebesgue measure. Then we note

$$\phi_n(t) := \frac{1}{\sqrt{d_n}} H_n(t) \exp(-t^2/2), \tag{1.12}$$

where $d_n := \int_{\mathbb{R}} H_n(x)^2 dx = 2^n n! \sqrt{\pi}$. The family (ϕ_n) is therefore orthonormal in $L^2(\mathbb{R})$. We introduce

$$k_n(x, y) := \sum_{j=0}^{n-1} \phi_j(x)\phi_j(y).$$

We can associate to k_n an integral operator K_n acting on the Hilbert space $L^2(\mathbb{R})$ in the following way

$$(K_n f)(x) := \int_{\mathbb{R}} k_n(x,y) f(y) dy. \tag{1.13}$$

This operator K_n is nothing but the orthogonal projection in $L^2(\mathbb{R})$ onto the subspace spanned by $(\phi_j)_{1 \leqslant j \leqslant n}$.

This is a very general setting : if we have a measure space (X, μ) and a "kernel" $k \in L^2(X \times X)$, we can define an operator K on $L^2(X)$ using a formula similar to (1.13). From now on, all kernels are assumed to belong to $L^2(X \times X)$ and are denoted by small letters ; associated integral operators are denoted by the corresponding capital letter.

It is straightforward to prove that Hilbert–Schmidt operators on $L^2(X)$ are exactly integral operators with a L^2 kernel. Moreover, the Hilbert–Schmidt norm of the operator and the L^2 norm of the kernel coincide. This fact is proved in [GG], which is a good reference for a reader who wants more detail on integral operators. Let us just quote the formula for compositions of operators : if k and l are two kernels on the same space (X, μ), then the operator KL is an integral operator with kernel :

$$(kl)(x,y) = \int_X k(x,z) l(z,y) d\mu(z). \tag{1.14}$$

The tail function of $\lambda_1(A^{(n)})$ can now be expressed using the kernel k_n. The key formula is the following (see [Meh])

$$\forall t \in \mathbb{R}, \mathbf{P}_n \left(\frac{\sqrt{n}}{\sqrt{2}} \lambda_1(A^{(n)}) \leqslant t \right) = \det_{[t,\infty)} (\mathrm{Id} - K_n). \tag{1.15}$$

In the formula (1.15), the right-hand side must be understood as the determinant of the operator K_n acting on the space $L^2([t,\infty))$ (or equivalently of the operator with kernel equal to is the restriction of k_n to $[t,\infty)^2$). This restricted operator is denoted $K_n^{[t]}$.

It may not be immediately obvious how to define such a determinant, as the operator involved acts on an infinite-dimensional space. However, the operator K_n that we consider here has a finite rank, hence we can define its determinant as if it were acting on a finite-dimensional space.

A problem will arise when we want to consider limits of such operators, which might fail to have a finite rank. Fortunately, a whole theory of determinants (and traces) of integral operators exists (so-called "Fredholm" determinants). In fact, there are several possible ways to extend these concepts to the infinite-dimensional case. We will focus on a more algebraic approach, due to Grothendieck (see [GGK] or [Sim] for a complete exposition), which defines determinants of a nuclear (= trace class) perturbation of identity in terms of traces of its exterior powers (here N is a nuclear operator, for which trace is well-defined).

$$\det(\mathrm{Id} + N) := 1 + \sum_{k=1}^{\infty} \operatorname{tr}(\Lambda^k(N)).$$

Of course, this definition coincides with the usual one in the finite-dimensional case.

The presence of the factor $\sqrt{n}/\sqrt{2}$ in equation (1.15) requires an explanation. It arose because there are several normalizations possible. We chose to define the GUE so that the first eigenvalue is about 2, while other authors, as Tracy and Widom in [TW1], prefer to locate it around $\sqrt{2n}$ (there are still other normalizations but an exhaustive list would be too long). As we kept their notation for the kernels k_n, a scaling factor will appear when we pass from a normalization to the other one.

To get a nontrivial limit, we must replace the t in formula (1.15) by the following rescaling, as for the Tracy–Widom limit (1.2)

$$t = \tau_n(x) := \frac{\sqrt{n}}{\sqrt{2}}(2 + \frac{x}{n^{2/3}}).$$

Let also $\tilde{k}_n$ be the rescaled kernel

$$\tilde{k}_n(x, y) := \frac{1}{\sqrt{2}n^{1/6}} k_n(\tau_n(x), \tau_n(y)).$$

We can see using a change of variable that $\tilde{K}_n^{[x]}$ and $K_n^{[\tau_n(x)]}$ have the same eigenvalues. More precisely, if f is a eigenfunction of $\tilde{K}_n^{[x]}$, then $f \circ \tau_n^{-1}$ is a eigenfunction of $K_n^{[\tau_n(x)]}$, with the same eigenvalue.

Plugging these renormalizations into the formula (1.15), we obtain

$$\mathbf{P}_n(\lambda_1(A^{(n)}) \leqslant 2 + xn^{-2/3}) = \det_{[x,+\infty)}(\mathrm{Id} - \tilde{K}_n). \tag{1.16}$$

Using the previous definition for the tail function ψ_n, we can write for a positive s

$$\psi_n(s) = 1 - \det(\mathrm{Id} - \tilde{K}_n^{[s]}).$$

The following result was known before Tracy and Widom's work (see for example [For])

$$\lim_{n \to \infty} \tilde{k}_n(x, y) = k(x, y), \tag{1.17}$$

uniformly on compact subsets in x and y.

Here k is the kernel, often called Airy kernel, defined by

$$k(x,y) := \frac{\mathrm{Ai}(x)\mathrm{Ai}'(y) - \mathrm{Ai}'(x)\mathrm{Ai}(y)}{x-y}. \tag{1.18}$$

The kernel k is extended by continuity to the diagonal. The function Ai is called the Airy function. It is very useful in physics and can be defined by several means. One of them is the following integral representation

$$\mathrm{Ai}(z) := \frac{1}{2\pi}\int_{-\infty}^{\infty} \exp(\mathrm{i}(zt + t^3/3))dt.$$

It can also be written as a combination of Bessel functions. It satisfies the Airy ODE

$$\frac{\partial^2}{\partial x^2} y(x) = xy(x). \tag{1.19}$$

The asymptotic behavior of Ai is well-known, for example [Sze] contains the following formula, valid when x tends to $+\infty$

$$\mathrm{Ai}(x) \sim \frac{1}{2} 3^{-1/4}\sqrt{\pi} x^{-1/4} \exp(-\frac{2}{3^{3/2}} x^{3/2}). \tag{1.20}$$

The function ψ_{TW} can be defined using this Airy kernel

$$\psi_{\mathrm{TW}}(x) := 1 - \det(\mathrm{Id} - K^{[x]}). \tag{1.21}$$

In [TW1] Tracy and Widom found another expression for ψ_{TW}. Let q be the solution of the Painlevé II ODE

$$\frac{\partial^2}{\partial x^2} q(x) = xq(x) + 2q(x)^3,$$

which is determined by the asymptotics $q(x) \sim \mathrm{Ai}(x)$ for x close to $+\infty$. Then we have the representation

$$\psi_{\mathrm{TW}}(x) = 1 - \exp(-\int_x^{\infty} (t-x)q(t)^2 dt). \tag{1.22}$$

It is easy to get from (1.20) and (1.22) the bounds (1.3) for the asymptotic behavior of ψ_{TW}. However, as we do not really need all the depth of Tracy and Widom's results and connections to Painlevé functions, we will reprove this fact in a more elementary way at the end of this note.

1.2.4 Convergence of the operators

The convergence in (1.17) as determined in the existing literature is rather weak ; in particular, it does not imply convergence of the associated integral operators in the Hilbert–Schmidt norm or even in the operator norm on L^2. In particular, we are not *a priori* allowed to exchange limit and determinant in (1.16) when n tends to infinity.

Our main step will be to show that $\tilde{K}_n$ tends to K with respect to the nuclear (trace class) norm. To that end we need several lemmas.

Lemma 4. *The following equality holds*

$$\left(\frac{\partial}{\partial x}+\frac{\partial}{\partial y}\right)k_n(x,y)=-\sqrt{\frac{n}{2}}\left(\phi_n(x)\phi_{n-1}(y)+\phi_{n-1}(x)\phi_n(y)\right).$$

Proof. We start with the Christoffel–Darboux formula (see [Sze])

$$k_n(x,y)=\sqrt{\frac{n}{2}}\frac{\phi_n(x)\phi_{n-1}(y)-\phi_{n-1}(x)\phi_n(y)}{x-y}.$$

Then we apply the operator $\frac{\partial}{\partial x}+\frac{\partial}{\partial y}$ to each term. We use the formula (1.12) and the following identities (those which are not obvious are shown in [Sze])

$$\phi_n'(x)=-\frac{\exp(-x^2/2)}{\sqrt{d_n}}(H_n'(x)-xH_n(x)).$$

$$H_{n-1}'(x)=2xH_{n-1}(x)-H_n(x).$$

$$H_n'(x)=2nH_{n-1}(x).$$

We obtain exactly the expected result. □

Lemma 5. *The following integral representation holds*

$$\begin{aligned}\tilde{k}_n(x,y) &= \frac{n^{1/6}}{2\sqrt{2}}\int_0^\infty \phi_n(\tau_n(x+z))\phi_{n-1}(\tau_n(y+z)) \\ &+ \phi_{n-1}(\tau_n(x+z))\phi_n(\tau_n(y+z))dz.\end{aligned}\tag{1.23}$$

Proof. If we apply the operator $\frac{\partial}{\partial x} + \frac{\partial}{\partial y}$ to the right-hand side of (1.23) (there is no trouble with interchanging the operations "$\frac{\partial}{\partial x} + \frac{\partial}{\partial y}$" and "$\int_0^\infty$" since all the functions involved are Schwartz functions), we get after standard calculations

$$\frac{n^{1/6}}{2\sqrt{2}}(\phi_n(\tau_n(x))\phi_{n-1}(\tau_n(y)) + \phi_{n-1}(\tau_n(x))\phi_n(\tau_n(y))).$$

Lemma 4 asserts that we obtain exactly the same expression when we apply the operator $\frac{\partial}{\partial x} + \frac{\partial}{\partial y}$ to the left member of (1.23). Thus, the two members of the equation are equal modulo a function (say, α) which only depends on $x-y$. But both members tend to zero when x et y tend to infinity in an independent way. Therefore the function α has to vanish identically and the lemma is proved. □

Let us introduce extra notation. The following kernels are defined on $[s, +\infty)^2$, where s is any positive number

$$a_n^{[s]}(x, y) := \frac{n^{1/12}}{2^{1/4}}\phi_n(\tau_n(x + y - s)).$$

$$b_n^{[s]}(x, y) := \frac{n^{1/12}}{2^{1/4}}\phi_{n-1}(\tau_n(x + y - s)).$$

$$a^{[s]}(x, y) := \mathrm{Ai}(x + y - s).$$

The equality (1.23) can be translated in terms of operators (this is just a consequence of the formula (1.14) for the composition of kernels)

$$\tilde{K}_n^{[s]} = \frac{1}{2}(A_n^{[s]}B_n^{[s]} + B_n^{[s]}A_n^{[s]}). \tag{1.24}$$

A similar equality for the operator K is proved (exactly in the same way) in [TW1]

$$K^{[s]} = (A^{[s]})^2. \tag{1.25}$$

We shall subsequently show that (for a fixed s) the operators $A_n^{[s]}$ and $B_n^{[s]}$ tend to $A^{[s]}$ with respect to the Hilbert–Schmidt norm. To that end, we need estimates for ϕ_n contained in two lemmas that follow.

Lemma 6. *The functions ϕ_n, after rescaling, converge to* Ai*, uniformly on compact subsets in y :*

$$\phi_n(\tau_n(y))2^{-1/4}n^{1/12} \to \mathrm{Ai}(y) \quad \text{and} \quad \phi_{n-1}(\tau_n(y))2^{-1/4}n^{1/12} \to \mathrm{Ai}(y). \tag{1.26}$$

Proof. This is an immediate consequence of the following asymptotic formulae for Hermite polynomials due to Plancherel and Rotach. They can be found, in a slightly different presentation, in the book by Szegö ([Sze])

$$\text{If } x = \sqrt{2n+1} + \frac{y}{\sqrt{2}n^{1/6}}, \text{ then } \phi_n(x) = 2^{1/4}n^{-1/12}(\mathrm{Ai}(y) + O(n^{-3/4})).$$

The O holds when n tends to $+\infty$, uniformly in y on compact subsets. □

Lemma 7. *We have a bound for ϕ_n which is uniform in n : there exists a positive constant c such that for any $y > 0$ and any integer n*

$$\begin{cases} n^{1/12}\phi_n(\tau_n(y)) \leqslant C\exp(-cy^{3/2}) \\ n^{1/12}\phi_n(\tau_{n-1}(y)) \leqslant C\exp(-cy^{3/2}) \end{cases}. \tag{1.27}$$

Proof. Let us sketch a proof of the first inequality in (1.27). We will use the following result, which is an exercise at page 403 in [Olv]. It is valid for $x \geqslant 1$

$$H_n(\nu x) \leqslant 1.13\sqrt{2\pi}\exp(-\nu^2/4)\nu^{(3\nu^2-1)/6}\exp(\nu^2x^2/2)\left(\frac{\zeta}{x^2-1}\right)^{1/4}\mathrm{Ai}(\nu^{4/3}\zeta).$$

where $\nu := \sqrt{2n+1}$ and

$$\zeta := \left(\frac{3}{4}x\sqrt{x^2-1} - \frac{3}{4}\mathrm{Argch}x\right)^{2/3}.$$

Using the definition of ϕ_n given in formula (1.12) and Stirling's formula to estimate d_n, we obtain

$$n^{1/12}\phi_n(\nu x) \leqslant C\left(\frac{\zeta}{x^2-1}\right)^{1/4}\mathrm{Ai}(\nu^{4/3}\zeta).$$

We deduce from (1.20) a bound for Ai, and we also use the inequality $\zeta \geqslant c(x-1)$ to get

$$n^{1/12}\phi_n(\sqrt{2n+1}x) \leqslant Cn^{-1/6}\frac{1}{(x-1)^{1/4}}\exp(-c(2n+1)(x-1)^{3/2}). \tag{1.28}$$

We now return to our notation through the change of variable

$$\sqrt{2n+1}\,x = \tau_n(y).$$

We can estimate x in the following way

$$x \geqslant 1 - \frac{c}{n} + \frac{y}{\sqrt{2}n^{1/6}\sqrt{2n+1}}.$$

For y large enough, we even have

$$x \geqslant 1 + c\frac{y}{n^{2/3}}. \tag{1.29}$$

Combining (1.28) and (1.29) yields

$$n^{1/12}\phi_n(\tau_n(y)) \leqslant C\frac{1}{y^{1/4}}\exp(-cy^{3/2}).$$

The factor $y^{-1/4}$ can be deleted if c is made small enough. This inequality is only true for y large enough, but we keep in mind that convergence in (1.26) was uniform on compact subsets, so we can extend it to all positive y, and the inequality is proved. The same scheme of demonstration works for the second inequality, with τ_{n-1} instead of τ_n. □

We are now ready to prove our main theorem

Proof. We denote by $||.||_{HS}$ the Hilbert–Schmidt norm and by ν the nuclear norm.

We are first going to estimate the quantity $|\psi_n(s) - \psi_{\text{TW}}(s)| = |\det(\mathrm{Id} - \tilde{K}_n^{[s]}) - \det(\mathrm{Id} - K^{[s]})|$. To reach this goal, we will use the following majoration (see [GGK]), valid for any two nuclear operators A and B

$$|\det(\mathrm{Id} + A) - \det(\mathrm{Id} + B)| \leqslant \nu(A - B)\mathbf{E}^{1+\nu(A)+\nu(B)}. \tag{1.30}$$

It will be useful to notice that lemma 7 implies in particular the following remark : there is a positive C such that for any $s \geqslant 0$ and any integer n, all the quantities $||A_n^{[s]}||_{HS}$, $||B_n^{[s]}||_{HS}$ and $||A^{[s]}||_{HS}$ are bounded by C (remember that the Hilbert–Schmidt norm is just the L^2-norm of the kernel). Using inequalities (1.24), (1.25) and the non-commutative Hölder inequality, we get that $\nu(K^{[s]})$ and $\nu(\tilde{K}_n^{[s]})$ are also bounded by the constant. Hence we can drop the exponential factor in formula (1.30)

$$|\psi_n(s) - \psi_{\text{TW}}(s)| \leqslant C\nu(\tilde{K}_n^{[s]} - K^{[s]}).$$

We need to estimate the quantity $\nu(\tilde{K}_n^{[s]} - K^{[s]})$. The key to do this is to use the equalities (1.24) et (1.25) to get

$$\begin{aligned}\tilde{K}_n^{[s]} - K^{[s]} &= \frac{1}{4}\Big((A_n^{[s]} - A^{[s]})(B_n^{[s]} + A^{[s]}) + (A_n^{[s]} + A^{[s]})(B_n^{[s]} - A^{[s]}) \\ &+ (B_n^{[s]} + A^{[s]})(A_n^{[s]} - A^{[s]}) + (B_n^{[s]} - A^{[s]})(A_n^{[s]} + A^{[s]})\Big).\end{aligned}$$

The non-commutative Hölder inequality yields

$$\begin{aligned} \nu(\tilde{K}_n^{[s]} - K^{[s]}) &\leqslant \frac{1}{2}||A_n^{[s]} - A^{[s]}||_{HS}||B_n^{[s]} + A^{[s]}||_{HS} \\ &+ \frac{1}{2}||A_n^{[s]} + A^{[s]}||_{HS}||B_n^{[s]} - A^{[s]}||_{HS}. \end{aligned} \tag{1.31}$$

The factors with a "+" are easy to get rid of : we can use the triangle inequality to write $||A_n^{[s]} + A^{[s]}||_{HS} \leqslant ||A_n^{[s]}||_{HS} + ||A^{[s]}||_{HS}$, which is uniformly bounded according to the remark following formula (1.30). We obtain

$$\nu(\tilde{K}_n^{[s]} - K^{[s]}) \leqslant C(||A_n^{[s]} - A^{[s]}||_{HS} + ||B_n^{[s]} - A^{[s]}||_{HS}).$$

We can now calculate the Wasserstein distance from Λ_n to TW, using the expression given by lemma 3

$$\begin{aligned} d(\Lambda_n, TW) &= \int_0^\infty \exp(\gamma s^{3/2})|\psi_n(s) - \psi_{\mathrm{TW}}(s)|ds \\ &\leqslant C\int_0^\infty \exp(\gamma s^{3/2})(||A_n^{[s]} - A^{[s]}||_{HS} + ||B_n^{[s]} - A^{[s]}||_{HS})ds. \end{aligned}$$

First deal with the term $||A_n^{[s]} - A^{[s]}||_{HS}$. Using the definition of $A_n^{[s]}$ and $A^{[s]}$ we get

$$\begin{aligned} &\int_0^\infty \exp(\gamma s^{3/2})||A_n^{[s]} - A^{[s]}||_{HS} ds \\ = \ &\sqrt{2}\int_0^\infty \exp(\gamma s^{3/2}) \left(\int_0^\infty z\left((\frac{n^{1/12}}{2^{1/4}}\phi_n \circ \tau_n - \mathrm{Ai})(z+s) \right)^2 dz \right)^{1/2} ds. \end{aligned} \tag{1.32}$$

Fix an $\varepsilon > 0$ and use the uniform bound of lemma 7 : we get that for γ small enough, S large enough and any n

$$\sqrt{2}\int_S^\infty \exp(\gamma s^{3/2}) \left(\int_0^\infty z\left((\frac{n^{1/12}}{2^{1/4}}\phi_n \circ \tau_n - \mathrm{Ai})(z+s) \right)^2 dz \right)^{1/2} ds \leqslant \varepsilon.$$

Similarly, for Z large enough, any s smaller than S and any n

$$\left(\int_Z^\infty z\left((\frac{n^{1/12}}{2^{1/4}}\phi_n \circ \tau_n - \mathrm{Ai})(z+s) \right)^2 dz \right)^{1/2} \leqslant \frac{\varepsilon}{\sqrt{2}S\exp(S^{3/2})}.$$

Now we can split the integral in (1.32) into three terms to get (remember than convergence in lemma 6 was uniform on compact subsets)

$$\int_0^\infty \exp(\gamma s^{3/2})||A_n^{[s]} - A^{[s]}||_{HS} ds \leqslant 3\varepsilon \qquad \text{for } n \text{ large enough.}$$

We can write a similar estimate with B_n instead of A_n. We finally deduce that, for n large enough, $d(\Lambda_n, TW) \leqslant 6C\varepsilon$. Hence Λ_n tends to TW in the Wasserstein sense. This is the announced result. □

1.2.5 An elementary proof of asymptotics for ψ_{TW}

To prove our theorem, we needed the upper asymptotics (1.3) for ψ_{TW}. It is possible to derive them from the representation (1.22) : keeping in mind that $q \sim \text{Ai}$, we get from (1.20)

$$\int_x^\infty (t-x)q^2(t)dt \leqslant C\exp(-cx^{3/2}).$$

Hence, (1.22) yields

$$\psi_{\text{TW}}(x) \leqslant 1 - \exp(-C\exp(-cx^{3/2})) \leqslant C'\exp(-cx^{3/2}).$$

However, for sake of completeness, we are going to derive in this section this last result in a more elementary way, i.e. without using the Painlevé representation. To do this, we need some facts about integral operators. Of course, a general integral operator can fail to be nuclear (for example, any Hilbert–Schmidt operator from $L^2(X)$ into itself can be written as an integral operator). Nevertheless, there exist several "nuclearity tests", criteria ensuring that under some conditions, kernels generate nuclear operators ([GG],[GGK]). The main result in this topic is Mercer's theorem, which enables us to expand a continuous self-adjoint kernel (i.e. the associated operator is self-adjoint) as a series of eigenfunctions of the operator. Unfortunately, these results are usually stated when dealing with a compact space of finite measure, and we have to consider half-infinite intervals $[s, +\infty)$. However, the standard proofs work also in this setting with only slight modifications.

A result which fits the present context is the following

Lemma 8. *Let $X = [s, +\infty)$, equipped with the Lebesgue measure, and k be a kernel on $X \times X$ which satisfies the following conditions*

1. $k \in L^2(X \times X)$,

2. *k is jointly continuous,*
3. *K is positive self-adjoint as an operator on $L^2(X)$,*
4. *There exists a continuous positive function ϱ in $L^2(X)$ such that*

$$|k(x,y)| \leqslant \varrho(x)\varrho(y)$$

   for every x, y in X.

Then the operator K is nuclear and the trace formula holds

$$\operatorname{tr}(K) = \int_s^\infty k(x,x)dx. \tag{1.33}$$

Proof. We are going to derive our result from the classical finite-measure case using a change of density trick. Let μ be the measure on X with density ϱ^2 with respect to Lebesgue measure ; we have $\mu(X) < \infty$. If we (isometrically) identify $L^2(X, dx)$ with $L^2(X, \mu)$ sending f to f/ϱ, the integral operator K viewed from $L^2(X, \mu)$ into itself has kernel $k(x, y)/\varrho(x)\varrho(y)$. To get the result we simply apply to the new kernel the following version of Mercer's theorem (it can proved adapting straightforward the classical proof from [Smi]) : if μ is a finite Borel measure on X and k a continuous bounded positive self-adjoint kernel, then the associated operator K is nuclear and its trace is equal to the integral of the kernel along the diagonal. □

Lemma 9. *The following estimation holds*

$$\exists C, c > 0, \forall s > 0, \quad \psi_{\text{TW}}(s) \leqslant C \exp(-cs^{3/2}).$$

Proof. By definition (see [Sim]), we have

$$\psi_{\text{TW}}(s) = \sum_{k=1}^{\infty} (-1)^{k-1} \operatorname{tr}(\Lambda^k(K^{[s]})).$$

Using the fact that $\operatorname{tr}(\Lambda^k(K^{[s]})) \leqslant \operatorname{tr}(K^{[s]})^k/k!$, we get

$$|\psi_{\text{TW}}(s)| \leqslant \exp(\operatorname{tr}K^{[s]}) - 1.$$

Actually, formula (1.21) shows that ψ_{TW} is positive since we have $0 \leqslant K^{[s]} \leqslant 1$. In the end, the convexity of the exponential function on $[0, \operatorname{tr}K^{[0]}]$ yields for $s \geqslant 0$

$$\psi_{TW}(s) \leqslant C \operatorname{tr}K^{[s]}.$$

It is not hard to check that the kernel $k^{[s]}$ satisfies the hypotheses of lemma 8 ; to check condition 4 we can cook up a function ϱ using Ai and its derivative.

Thus we can rewrite the trace of $K^{[s]}$ as an integral

$$\psi_{TW}(s) \leqslant C \int_s^\infty \big((\mathrm{Ai}'(x))^2 - x\mathrm{Ai}(x)\big)\, dx. \tag{1.34}$$

The value of K on the diagonal comes from (1.18) and the Airy ODE (1.19).

Using (1.20), we can write

$$\exists C, c > 0 \quad \forall s \geqslant 0 \quad \mathrm{Ai}(s) \leqslant C \exp(-cs^{3/2}). \tag{1.35}$$

A similar majoration holds for Ai' : we only need to write $\mathrm{Ai}'(s) = \int_s^\infty \mathrm{Ai}''(x)dx$ and to use formulae (1.19) and (1.35)

$$\exists C, c > 0 \quad \forall s \geqslant 0 \quad \mathrm{Ai}'(s) \leqslant C \exp(-cs^{3/2}). \tag{1.36}$$

The conclusion comes when combining formulae (1.34), (1.35) and (1.36). □

Possible Generalizations

Of course, we expect the inequalities analogous to (1.7) to be true in a much more general setting. Basically, each time a Tracy–Widom-like behavior has been proved or is suspected, we can ask whether such an uniform estimate holds.

The most natural extension would be the setting of general Wigner matrices, for which universality of Tracy–Widom limit has been proved by Soshnikov ([Sos]). However, the bounds on moments he obtained are not enough to derive the small deviations inequality.

Tracy and Widom proved results similar to (1.2), involving a different limit law, for the matrix ensembles GOE and GSE (the real orthogonal and the symplectic cases) in [TW2].

Several authors investigated the behavior of the largest s-number (also called singular value) of a rectangular $m \times n$ matrix with independent entries, when the ratio m/n tends to a limit in $(0, 1)$. The paper [Joh] contains an result analogous to (1.2) for the Gaussian case (the so-called Wishart ensemble). There is strong numerical evidence indicating that a convergence on the scale $n^{-2/3}$ as in Tracy–Widom behavior occurs also universally in this case, for the largest s-number, but also for the smallest one.

Another quantity of interest is the norm of a $n \times m$ random matrix when considered as a operator from ℓ_p^n to ℓ_q^m. Concentration results have been recently obtain in this case by Meckes (cf [Mec]).

In all these cases, we know concentration inequalities similar to (1.6), it would be interesting to prove the corresponding small deviation result.

Acknowledgements

I would like to express my sincere thanks and appreciation to my supervisor, Prof. Stanislaw J. Szarek, for our inspiring discussion and for his ongoing support. I would also like to thank Charles-Antoine Louët for his assiduous proofreading.

Chapitre 2

Échantillonnage de corps convexes : approximation de la matrice d'inertie

2.1 Introduction et présentation des résultats

2.1.1 Notations et position du problème

Dans tout ce chapitre, μ désigne une mesure de probabilité sur $\mathbf{R}^n$, décroissement suffisamment vite à l'infini pour que nous n'ayons pas à nous préoccuper des problèmes de convergesce. Un cas particulier que nous considérerons est celui de la mesure uniforme sur un corps convexe K, notée μ_K et définie pour toute partie mesurable B de $\mathbf{R}^n$ par

$$\mu_K(B) = \frac{\mathrm{vol}(K \cap B)}{\mathrm{vol}(K)}.$$

Si μ est centrée, c'est-à-dire si elle vérifie $\int_{\mathbf{R}^n} x d\mu(x) = 0$, sa *matrice d'inertie* A_μ est une matrice carrée symétrique, de taille n, définie par

$$(A_\mu)_{ij} = \int_{\mathbf{R}^n} x_i x_j d\mu(x_1, \ldots, x_n).$$

Alternativement, l'opérateur correspondant est

$$A_\mu = \int_{\mathbf{R}^n} |x\rangle\langle x| d\mu(x).$$

Cette matrice est positive ; elle est définie positive si et seulement si le support de μ n'est pas contenu dans un hyperplan. Dans le cas où A_μ est la matrice identité, on dit que la mesure μ est *isotrope*. Un convexe K est dit isotrope si la mesure μ_K l'est.

Si μ est une mesure sur $\mathbf{R}^n$ et $T : \mathbf{R}^n \to \mathbf{R}^n$ est une application linéaire inversible, notons $T_*\mu$ la mesure-image de μ par T, définie pour tout borélien B de $\mathbf{R}^n$ par

$$T_*\mu(B) = \mu(T^{-1}B).$$

Dans le cas d'une mesure uniforme sur un convexe, on a la relation

$$T_*\mu_K = \mu_{TK}.$$

Les matrices d'inertie de μ et de $T_*\mu$ sont liées par l'égalité

$$A_{T_*\mu} = T A_\mu T^\dagger. \tag{2.1}$$

Par conséquent, dès lors que la matrice A_μ est inversible, il existe une transformation affine T telle que $T_*\mu$ est isotrope.

On peut aussi définir l'*ellipsoïde d'inertie* d'une mesure μ comme étant l'unique ellipsoïde $\mathcal{E}$ tel que μ et $\mu_{\mathcal{E}}$ aient la même matrice d'inertie. Cet ellipsoïde est connu en mécanique sous le nom d'ellipsoïde de Legendre (voir [MiPa1]).

Pour certaines applications, notamment algorithmiques (cf [KLS]), il est important de pouvoir déterminer la matrice d'inertie de μ à partir d'un petit nombre d'échantillons. Plus précisément, si (X_i) sont des vecteurs aléatoires indépendants et identiquement distribués de loi μ, l'approximation empirique de la mesure μ avec N échantillons est donnée par

$$\mu_N = \frac{1}{N}\sum_{i=1}^{N}\delta_{X_i}.$$

La suite de mesures (μ_N) est une approximation aléatoire de la mesure μ. Le théorème de Varadarajan ([Dud]), parfois appelé théorème fondamental de la statistique, nous dit que presque sûrement, la suite (μ_N) converge étroitement vers μ lorsque N tend vers $+\infty$. Cependant, le nombre N d'échantillons nécessaires pour avoir une bonne approximation avec grande probabilité est en général exponentiel en la dimension (voir [GM] pour une question proche dans le cas d'un corps convexe). Si l'on cherche à n'approximer que la matrice d'inertie, ce nombre peut être choisi beaucoup plus petit. On sait que la suite (A_{μ_N}) converge vers A_μ presque sûrement et on cherche à quantifier cette convergence : étant donnée une tolérance $\varepsilon > 0$, quel nombre N d'échantillons faut-il prendre pour qu'avec grande probabilité

$$(1-\varepsilon)A_{\mu_N} \leqslant A_\mu \leqslant (1+\varepsilon)A_{\mu_N}? \tag{2.2}$$

Lorsque l'on a (2.2), on dit que l'on a *ε-approximation de la matrice d'inertie avec N échantillons.*

Si μ est une mesure sur $\mathbf{R}^n$ et $T : \mathbf{R}^n \to \mathbf{R}^n$ est une application linéaire inversible, les matrices d'inertie empiriques de μ et $T_*\mu$ vérifient

$$A_{(T_*\mu)_N} \overset{\mathscr{L}}{\sim} T A_{\mu_N} T^\dagger. \tag{2.3}$$

Par (2.1) et (2.3), on peut supposer que la mesure à échantillonner est isotrope, ce n'est nullement une restriction. Dans le cas d'une mesure isotrope, (2.2) s'écrit plus simplement

$$\|A_{\mu_N} - \mathrm{Id}\|_{op} \leqslant \varepsilon. \tag{2.4}$$

L'inégalité (2.4) est équivalente à

$$\forall \theta \in S^{n-1},\ \ 1-\varepsilon \leqslant |A_{\mu_N}\theta| \leqslant 1+\varepsilon,$$

ou encore, comme $A_{\mu_N} = \frac{1}{N} \sum |X_i\rangle\langle X_i|$, à

$$\forall \theta \in S^{n-1}, \ \ 1-\varepsilon \leqslant \frac{1}{N}\sum_{i=1}^{N} \langle X_i, \theta\rangle^2 \leqslant 1+\varepsilon.$$

On peut par ailleurs construire des mesures sur $\mathbf{R}^n$ qui sont aussi mal approximables que l'on veut. Par exemple, si a est dans l'intervalle $]0,1]$ et (e_i) est la base canonique de $\mathbf{R}^n$, considérons la mesure $\bar{\mu}_a$ définie par

$$\bar{\mu}_a = (1-a)\delta_0 + \frac{a}{2n}\sum_{i=1}^{n}\left(\delta_{\sqrt{\frac{n}{a}}e_i} + \delta_{-\sqrt{\frac{n}{a}}e_i}\right). \tag{2.5}$$

Cette mesure est bien isotrope. Si $(X_1, \dots, X_N)$ sont indépendants et identiquement distribués de loi $\bar{\mu}_a$, alors avec probabilité $(1-a)^N$ les X_i sont tous nuls, et donc la matrice d'inertie empirique est la matrice nulle ! Pour a suffisamment petit, ces mesures sont donc très mal approximables par les mesures empiriques.

Le problème de savoir combien d'échantillons sont nécessaires pour obtenir l'ε-approximation de la matrice d'inertie d'un corps convexe avec grande probabilité a été posé pour la première fois dans [KLS]. Un certain nombre de résultats sur le sujet ont été obtenus depuis ; nous ne nous intéressons pas ici à la dépendance en ε.

Tout d'abord, Kannán, Lovász et Simonovits ont montré que $N \geqslant C(\varepsilon)n^2$ échantillons garantissent l'ε-approximation avec probabilité supérieure à $1-\varepsilon$. Bourgain ([Bou]) a ensuite amélioré la borne pour obtenir $N \geqslant C(\varepsilon) n \log^3 n$. Il a ensuite été montré par Giannopoulos et Milman ([GM]) qu'une petite modification de la preuve de Bourgain permettait d'obtenir $N \geqslant C(\varepsilon) n \log^2 n$. Ce même résultat a aussi été obtenu par Rudelson, qui a en fait montré l'inégalité générale suivante : si μ est une mesure isotrope et X un vecteur aléatoire de loi μ, alors

$$\mathbf{E}\|A_{\mu_N} - \mathrm{Id}\|_{op} \leqslant C\sqrt{\frac{\log n}{N}} \left(\mathbf{E}|X|^{\log N}\right)^{1/\log N} \tag{2.6}$$

dès lors que le membre de droite est inférieur à 1. L'approche de Rudelson utilisait à l'origine le théorème des mesures majorantes de Fernique–Talagrand ; une preuve plus simple, basée sur les inégalités de Khintchine non commutatives de Lust-Piquard–Pisier, a ensuite été obtenue par Pisier. Pour utiliser l'inégalité (2.6), il est nécessaire de contrôler la quantité $(\mathbf{E}|X|^{\log N})^{1/\log N}$. Pour $N \geqslant e^2$, elle est toujours supérieure à $(\mathbf{E}|X|^2)^{1/2}$, qui vaut $\sqrt{n}$ par la condition d'isotropie. Dans les meilleurs cas, on a aussi une inégalité inverse du type

$$(\mathbf{E}|X|^{\log N})^{1/\log N} \leqslant C\sqrt{n}. \tag{2.7}$$

C'est par exemple le cas pour les convexes inconditionnels (voir le lemme 11 ci-après), pour lesquels Giannopoulos, Hartzoulaki et Tsolomitis ont ainsi montré que $N \geqslant C(\varepsilon) n \log n$ échantillons suffisent à obtenir l'ε-approximation de la matrice d'inertie avec probabilité supérieure à $1-\varepsilon$. Il est conjecturé (voir [Pao]) que l'on peut toujours obtenir une inégalité inverse du type (2.7), mais le résultat n'est connu que pour les convexes inconditionnels et les boules-unités des classes de Schatten (voir [BN1, GP]). Pour conclure dans le cas d'un convexe général, Rudelson utilise le lemme 10.3 ci-après qui fait intervenir un facteur logarithmique supplémentaire.

Ainsi, l'inégalité (2.6) est un outil puissant, mais qui ne permet pas d'espérer obtenir l'approximation de la matrice d'inertie avec moins de $Cn \log n$ échantillons. Il était d'ailleurs conjecturé (la conjecture apparaît explicitement dans [GHT]) que l'estimation $N \geqslant C(\varepsilon) n \log n$ est optimale pour un convexe général. Il est simple de voir que cette borne est optimale pour des exemples discrets. Considérons par exemple la mesure $\bar{\mu}_1$ définie par (2.5), qui n'est autre que la mesure uniforme sur les sommets de la boule $\sqrt{n} B_1^n$, on obtient en utilisant (2.6) l'inégalité

$$\mathbf{E} \| A_{(\bar{\mu}_1)_N} - A_{\bar{\mu}_1} \| \leqslant \varepsilon,$$

dès lors que $N \geqslant Cn \log n / \varepsilon^2$. Mais si X est distribué selon $\bar{\mu}_1$, l'opérateur $|X\rangle\langle X|$ est la projection orthogonale sur une coordonnée aléatoire. Ainsi la matrice $A_{(\bar{\mu}_1)_N}$ est diagonale, et ses coefficients diagonaux sont distribués selon $(p_1, \ldots, p_n)$, où p_i est le nombre de boules que contient l'urne numéro i lorsque l'on place aléatoirement, uniformément et indépendamment N boules dans n urnes. Ce problème, connu sous le nom d'allocation aléatoire, a été longuement étudié ([KSC]), et il est nécessaire de prendre $N \geqslant C(\varepsilon) n \log n$ boules afin d'avoir

$$(1-\varepsilon) N/n \leqslant \min(p_i) \leqslant \max(p_i) \leqslant (1+\varepsilon) N/n.$$

Pour conclure, l'inégalité (2.6) de Rudelson s'applique dans un cadre général (n'importe quelle mesure isotrope sur $\mathbf{R}^n$) et elle est optimale en toute généralité. Néanmoins, il est possible qu'en utilisant des outils spécifiques au cadre des corps convexe on puisse obtenir des améliorations.

2.1.2 Convexes et mesures log-concaves isotropes

Rappelons qu'un convexe K est dit *isotrope* si la mesure μ_K l'est, c'est-à-dire si sa matrice d'inertie est la matrice identité. Notons que cette définition est légèrement différente de celle utilisée habituellement en analyse géométrique asymptotique, où la normalisation est obtenue en imposant

$\mathrm{vol}(K) = 1$. Avec notre définition, contrôler le volume d'un convexe isotrope est équivalent à la conjecture de l'hyperplan (cf [MiPa1]). Introduisons maintenant la notion de mesure log-concave

Définition : *Une mesure positive μ sur $\mathbf{R}^n$ est dite logarithmiquement concave (ou plus simplement : log-concave) si pour toutes parties A, B mesurables de R^n et pour tout θ dans $]0,1[$, on a*

$$\mu^*(\theta A + (1-\theta)B) \geqslant \mu(A)^\theta \mu(B)^{1-\theta}.$$

Il se peut que $A+B$ ne soit pas mesurable même si A et B le sont (voir [Sie]), d'où la nécessité d'introduire la mesure extérieure μ^*. Alternativement, on pourrait se restreindre aux parties compactes. Borell a obtenu une caractérisation des mesures log-concaves particulièrement remarquable [Bor] : une mesure est log-concave si et seulement si elle a une densité par rapport à la mesure de Lebesgue sur l'espace affine engendré par son support, et si le logarithme de cette densité est une fonction concave (on autorise ici la valeur $-\infty$ pour les fonctions concaves). Un exemple de mesure log-concave est donné par les mesures μ_K définies précédemment ; en effet la fonction $-\log(\mathbf{1}_K)$ est concave si K est un ensemble convexe.

La classe des mesures log-concaves jouit de certaines propriétés de stabilité : ainsi les marginales de mesures log-concaves sont encore log-concaves. Plus précisément, soit μ une mesure log-concave sur $\mathbf{R}^n$ et E un sous-espace vectoriel. On identifie $\mathbf{R}^n$ à $E \times E^\perp$. La mesure marginale $\mu|E$, définie pour $B \subset E$ borélien par

$$(\mu|E)(B) = \mu(B \times E^\perp),$$

est aussi log-concave. C'est une conséquence de l'inégalité de Prékopa–Leindler (cf [Pré]). Ainsi, les marginales de mesures uniformes sur des convexes sont log-concaves. Réciproquement, si μ est une mesure log-concave sur $\mathbf{R}^k$, on peut construire une suite $(K_n)_{n \geqslant k}$ de convexes, $K_n \subset \mathbf{R}^n$, tels que la suite des mesures marginales

$$(\mu_{K_n}|\mathbf{R}^k)_{n \geqslant k}$$

converge étroitement vers μ (voir par exemple [AKM]). La classe des mesures de probabilité log-concaves isotropes est une classe de mesures dont les matrices d'inertie sont bien approximables ; avant de développer ce point, listons-en quelques propriétés qui nous seront utiles.

Lemme 10. *1. Il existe une constante universelle C telle que si X est un vecteur aléatoire dans $\mathbf{R}^n$ distribué selon une loi log-concave isotrope, et si $\theta \in S^{n-1}$ est une direction, alors la variable aléatoire $\langle X, \theta \rangle$ est Ψ_1 avec constante C.*

2. *Il existe des constantes universelles c, C telles que si μ est une mesure de probabilité log-concave isotrope sur $\mathbf{R}^n$, de densité f par rapport à la mesure de Lebesgue, alors pour toute direction $\theta \in S^{n-1}$, on a*

$$c \leqslant \int_{\theta^\perp} f(x)dx \leqslant C,$$

dx désignant ici la mesure de Lebesgue sur l'hyperplan $\theta^\perp$.

3. *Il existe une constante universelle C telle que pour tout convexe isotrope $K \subset \mathbf{R}^n$, si X est un vecteur aléatoire de loi μ_K, alors la norme euclidienne de X est une variable aléatoire qui est Ψ_2 avec constante $C\sqrt{n}$.*
4. *Il existe une constante universelle c telle que pour toute mesure de probabilité log-concave isotrope* **inconditionnelle** *μ, et pour tous nombres positifs $(\alpha_1, \dots, \alpha_n)$, on a*

$$\mu(\{(x_1, \dots, x_n) \text{ tq } |x_1| \geqslant \alpha_1, \dots, |x_n| \geqslant \alpha_n\}) \leqslant e^{-c(\alpha_1 + \cdots + \alpha_n)}.$$

On peut trouver la preuve de l'ensemble de ces résultats dans les notes [Gia]. Le fait 1 est dû à Borell et le fait 2 à Hensley ([Hen]). Leur preuve repose sur des inégalités valables pour des fonctions log-concaves de $\mathbf{R}$ dans $\mathbf{R}$, en effet $\langle X, \theta \rangle$ est une marginale de X, et est donc également log-concave. Le fait 3 est dû à Alesker ([Ale]), il est d'autant plus remarquable qu'il ne se généralise pas à toutes les mesures log-concaves (considérer par exemple, en dimension 1, une variable exponentielle). Le fait 4 a été prouvé par Bobkov et Nazarov ([BN1]). Le lemme suivant en est une conséquence

Lemme 11. *Il existe une constante universelle C tel que pour tout vecteur aléatoire $X = (x_1, \dots, x_n)$ de loi isotrope inconditionnelle log-concave et pour toute partie $I \subset \{1, \dots, n\}$, on a*

$$\mathbf{E} \prod_{i \in I} x_i^2 \leqslant C^{\# I}.$$

Démonstration. Soit z une variable aléatoire symétrique telle que $\mathbf{P}(|z| > t) = e^{-ct}$ pour tout $t > 0$. Soit $Z = (z_1, \dots, z_n)$ un n-uplet de copies indépendantes de z. Le lemme 10.4 se reformule alors comme suit

$$\mathbf{P}(\{|x_1| \geqslant \alpha_1, \dots, |x_n| \geqslant \alpha_n\}) \leqslant \mathbf{P}(\{|z_1| \geqslant \alpha_1, \dots, |z_n| \geqslant \alpha_n\}).$$

La version intégrée de cette inégalité (qui s'obtient comme dans le cas d'un convexe inconditionnel traité dans [BN2]) s'écrit alors ainsi : pour toute mesure π positive sur $(\mathbf{R}^+)^n$, la fonction $F : (\mathbf{R}^+)^n \to \mathbf{R}$ définie par

$$F(x_1, \dots, x_n) = \pi([0, x_1] \times \cdots \times [0, x_n])$$

vérifie l'inégalité

$$\mathbf{E}F(X) \leqslant \mathbf{E}F(Z).$$

La fonction $F_I(x_1, \dots, x_n) = \prod_{i \in I} x_i^2$ entre dans ce cadre et le lemme découle du fait que $\mathbf{E}F_I(Z)$ se calcule facilement (les coordonnées de Z sont indépendantes) et vaut $(2/c^2)^{\#I}$. □

Les techniques présentées auparavant ne permettent pas d'obtenir l'approximation de la matrice d'inertie avec moins de $Cn \log n$ échantillons. Il existe cependant certaines mesures pour lesquelles on sait que l'on peut faire mieux. Introduisons la définition suivante

Définition : *Si μ est une mesure de probabilité isotrope dans $\mathbf{R}^n$, sa norme Ψ_2, notée $\Psi_2(\mu)$ est définie par*

$$\Psi_2(\mu) = \sup_{\theta \in S^{n-1}} \|\langle X, \theta \rangle\|_{\Psi_2},$$

où X est un vecteur aléatoire de loi μ. On écrit aussi $\Psi_2(K)$ pour $\Psi_2(\mu_K)$

Pour les mesures dont on contrôle la norme Ψ_2, il est possible d'approximer la matrice d'inertie avec un nombre de points proportionnel à la dimension. Plus précisément, on a la proposition suivante

Proposition 2.1. *Il existe une constante universelle C telle que, si μ est une mesure de probabilité centrée sur $\mathbf{R}^n$, si $0 \leqslant \varepsilon \leqslant 1/2$ et si $N \geqslant C\Psi_2(\mu)^4 log(1/\varepsilon)/\varepsilon^2$, alors avec probabilité supérieure à $1 - \varepsilon$, on a ε-approximation de la matrice d'inertie de μ avec N échantillons :*

$$(1 - \varepsilon)A_\mu \leqslant A_{\mu_N} \leqslant (1 + \varepsilon)A_\mu. \tag{2.8}$$

Démonstration. Cette proposition est très similaire aux résultats de [GM], néanmoins elle n'y figure pas sous cette forme. La preuve utilise la forme suivante des inégalités de Bernstein, que l'on peut trouver par exemple dans [BLM]

Lemme 12. *Si (X_i) est une suite de variables aléatoires indépendantes, d'espérance nulle, telle que pour tout i, $\|X_i\|_{\Psi_1} \leqslant A$, alors pour tout $0 < \varepsilon < 4A$ et pour tout $n \geqslant 1$*

$$\mathbf{P}\left(\left|\sum_{i=1}^n X_i\right| \geqslant \varepsilon n\right) \leqslant 2\exp(-\varepsilon^2 n/16A^2). \tag{2.9}$$

On peut tout d'abord supposer que la mesure μ est isotrope, dans ce cas (2.8) est équivalent à

$$\forall x \in S^{n-1}, \quad 1-\varepsilon \leqslant \langle A_{\mu_N} x, x\rangle \leqslant 1+\varepsilon. \tag{2.10}$$

On va utiliser un argument de réseau. Fixons d'abord une direction $\theta \in S^{n-1}$, et soit (X_i) des vecteurs aléatoires i.i.d. de loi μ. On a alors

$$\|\langle X_i, \theta\rangle^2\|_{\Psi_1} = \|\langle X_i, \theta\rangle\|_{\Psi_2}^2 \leqslant \Psi_2(\mu)^2.$$

Et, comme $\mathbf{E}\langle X_i, \theta\rangle^2 = 1$

$$\|\langle X_i, \theta\rangle^2 - 1\|_{\Psi_1} \leqslant 2\Psi_2(\mu)^2.$$

Par les inégalités de Bernstein (lemme 12), pour tout $\alpha \leqslant 1$

$$\mathbf{P}\left(\frac{1}{N}\left|\sum_{i=1}^{N}(\langle X_i, \theta\rangle^2 - 1)\right| \geqslant \alpha\right) \leqslant 2\exp\left(-\frac{\alpha^2 N}{64\Psi_2(\mu)^4}\right).$$

Autrement dit,

$$\forall \theta \in S^{n-1}, \quad \mathbf{P}(1-\alpha \leqslant \langle A_{\mu_N}\theta, \theta\rangle \leqslant 1+\alpha) \geqslant 1 - 2\exp\left(-\frac{\alpha^2 N}{64\Psi_2(\mu)^4}\right).$$

Soit maintenant $\mathcal{N}$ un α-réseau de S^{n-1} de cardinal inférieur à $(3/\alpha)^n$. En utilisant la propriété d'approximation du réseau, on obtient

$$\|A_{\mu_N}\| = \sup_{x \in S^{n-1}} \langle A_{\mu_N} x, x\rangle \leqslant \sup_{\theta \in \mathcal{N}} \langle A_{\mu_N}\theta, \theta\rangle + 2\alpha\|A_{\mu_N}\|,$$

$$\inf_{x \in S^{n-1}} \langle A_{\mu_N} x, x\rangle \geqslant \inf_{\theta \in \mathcal{N}} \langle A_{\mu_N}\theta, \theta\rangle - 2\alpha\|A_{\mu_N}\|.$$

Soit E l'événement « $\forall \theta \in \mathcal{N}, \;\; 1-\alpha \leqslant \langle A_{\mu_N}\theta, \theta\rangle \leqslant 1+\alpha$ », qui implique

$$\forall x \in S^{n-1}, \quad \frac{1-5\alpha}{1-2\alpha} \leqslant \langle A_{\mu_N} x, x\rangle \leqslant \frac{1+\alpha}{1-2\alpha}.$$

Lorsque $\alpha \leqslant 1/8$, on a les inégalités $(1+\alpha)/(1-2\alpha) \leqslant 1+4\alpha$ et $(1-5\alpha)/(1-2\alpha) \geqslant 1-4\alpha$. En choisissant $\alpha = \varepsilon/4$, on obtient donc (2.10) dès que E est vrai. Or, on a l'estimation

$$\mathbf{P}(E) \geqslant 1 - 2\left(\frac{12}{\varepsilon}\right)^n \exp\left(-\frac{\varepsilon^2 N}{1024\Psi_2(\mu)^4}\right).$$

La proposition est donc prouvée, en choisissant la constante C suffisamment grande. □

La classe des convexes isotropes K tels que $\Psi_2(K)$ soit borné indépendamment de la dimension est assez restreinte, elle contient par exemple les boules B_p^n pour $p \geqslant 2$. Il est naturel de se demander si, pour des corps convexes (ou des mesures log-concaves) pour lesquels la quantité $\Psi_2(\cdot)$ n'est pas bornée par une constante indépendante de la dimension, il est néanmoins possible d'avoir ε-approximation de la matrice d'inertie avec un nombre d'échantillons proportionnel à la dimension. Le premier exemple qui vient à l'esprit est celui de la boule B_1^n, car cet exemple est en quelque sorte à l'opposé des corps convexes pour lesquels $\Psi_2(\cdot)$ est borné. Nous verrons que l'approche via la théorie des matrices aléatoires permet de répondre positivement à cette question.

2.1.3 Matrices aléatoires et échantillonnage

Dans cette section, nous allons faire le lien entre les matrices aléatoires telles qu'elles ont été introduites auparavant et le problème de l'échantillonnage. Prenons le cas d'une mesure μ isotrope. La première remarque à faire est la suivante : la matrice d'inertie empirique, définie comme

$$A_{\mu_N} = \frac{1}{N} \sum_{i=1}^{N} |X_i\rangle\langle X_i|,$$

peut aussi être vue comme le produit matriciel $\Gamma_N^\dagger \Gamma_N$, où Γ_N est la matrice suivante, formée de N lignes et n colonnes

$$\Gamma_N = \frac{1}{\sqrt{N}} \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_N \end{pmatrix}. \tag{2.11}$$

L'inégalité d'approximation de la matrice d'inertie $\|A_{\mu_N} - \mathrm{Id}\| \leqslant \varepsilon$ se traduit sur la matrice Γ_N en

$$\sqrt{1-\varepsilon} \leqslant s_{\min}(\Gamma_N) \leqslant s_{\max}(\Gamma_N) \leqslant \sqrt{1+\varepsilon}.$$

Cette approche a été introduite par exemple dans [MePa]. Les lignes de la matrice Γ sont indépendantes, mais les colonnes ne le sont pas (sauf si la mesure μ échantillonnée peut s'écrire comme une mesure-produit $\mu_1 \otimes \cdots \otimes \mu_n$). C'est ici un point fondamental : en effet le comportement des valeurs singulières de matrices aléatoires dont les coefficients sont des variables aléatoires indépendantes est un sujet très étudié. On a par exemple les résultats suivants, dans le régime global et dans le régime local :

Théorèmes. *Fixons une loi μ, d'espérance nulle, de variance 1 et possédant un moment d'ordre 4. Soit pour chaque couple d'entiers (n, N), $N \geqslant n$, une matrice aléatoire $\Gamma = \Gamma_{n,N}$, de taille $n \times N$, dont les coefficients sont des variables aléatoires i.i.d. de loi μ. La mesure empirique associée aux valeurs singulières de $\frac{1}{\sqrt{N}}\Gamma$ est définie par*

$$\mu_\Gamma = \frac{1}{n} \sum_{i=1}^{n} \delta_{s_i(\Gamma)/\sqrt{N}}.$$

On considère une suite de couples (n, N) tendant vers l'infini de telle manière que le rapport n/N tende vers une limite $\beta \in]0, 1[$. On a alors les théorèmes-limites suivants

– **Marčenko–Pastur [MaPa] :** *Presque sûrement, la suite $(\mu_{\Gamma_{n,N}})$ converge étroitement vers la mesure déterministe μ_β, supportée par l'intervalle $[1 - \sqrt{\beta}, 1 + \sqrt{\beta}]$, donnée par la densité*

$$\frac{d\mu_\beta}{dx} = \frac{1}{\pi \beta x} \sqrt{((1 + \sqrt{\beta})^2 - x^2)(x^2 - (1 - \sqrt{\beta}))^2}.$$

– **Bai–Yin [BY] :** *Presque sûrement, on a les convergences :*

$$\lim_{(n,N)\to\infty} \frac{1}{\sqrt{N}} s_{\min}(\Gamma_{n,N}) = 1 - \sqrt{\beta},$$

$$\lim_{(n,N)\to\infty} \frac{1}{\sqrt{N}} s_{\max}(\Gamma_{n,N}) = 1 + \sqrt{\beta}.$$

Le résultat le plus intéressant pour le problème de l'échantillonnage est le théorème de Bai–Yin : on cherche en effet à contrôler les valeurs singulières extrémales. Il y *a priori* deux obstacles majeurs qui nous empêchent d'appliquer ce théorème :

1. C'est seulement un résultat limite alors que l'on a en vue un résultat valide en toute dimension.
2. Les coefficients de la matrice Γ_N ne sont pas en général indépendants.

Le problème posé par le point 1 est très similaire aux travaux présentés dans le chapitre 1 : il faut raffiner la preuve d'un résultat-limite pour obtenir un résultat *uniforme*, c'est-à-dire valable en toute dimension. C'est vraisemblablement une tâche ardue, mais nous verrons que des résultats de concentration permettent ici de contourner le problème et de travailler directement à partir du résultat-limite.

Le point 2 est en revanche beaucoup plus fondamental : en effet la propriété d'indépendance des coefficients est utilisée de façon cruciale dans [BY].

Nous parvenons cependant à des résultats satisfaisants dans certains cas particuliers. Un résultat dû à Barthe, Guédon, Mendelson et Naor permet de décrire la mesure uniforme sur les boules B_p^n par des opérations élémentaires à partir de composantes 1-dimensionnelles ; cela permet de se ramener au cas où les coefficients sont indépendants et d'appliquer les théorèmes évoqués précédemment pour obtenir

Théorème 2.3 : *Fixons $1 \leqslant p \leqslant +\infty$. Pour chaque couple (n, N), $N \geqslant n$, soit Γ_N la matrice définie par (2.11), les (X_i) étant uniformément distribués sur l'image homothétique isotrope de la boule B_p^n. Soit $\mu_\Gamma = 1/n \sum_{i=1}^n \delta_{s_i(\Gamma)}$ la mesure spectrale empirique associée. Alors, si on considère une suite de couples (n, N) tendant vers l'infini de telle manière que le rapport n/N tende vers une limite $\beta \in]0, 1[$, presque sûrement, la suite $(\mu_{\Gamma_{n,N}})$ converge étroitement vers la distribution de Marchenko–Pastur μ_β.*

De même, à partir du théorème de Bai–Yin, on peut obtenir le théorème suivant :

Théorème 2.1 : *Pour tout $\varepsilon > 0$ et pour tout $1 \leqslant p \leqslant \infty$, il existe une constante $K = K(\varepsilon, p)$ telle que, si $(X_1, \ldots, X_N)$ sont i.i.d. uniformément sur l'image homothétique isotrope de la boule B_p^n et $N \geqslant Kn$, alors avec probabilité supérieure à $1 - \varepsilon$, on a*

$$\left\| \frac{1}{N} \sum_{i=1}^{N} |X_i\rangle\langle X_i| - \mathrm{Id} \right\| \leqslant \varepsilon.$$

Cela répond positivement à la question posée dans la section précédente : il est possible d'obtenir l'ε-approximation de la matrice d'inertie de la boule B_1^n avec un nombre d'échantillons qui est proportionnel à la dimension. à notre connaissance, c'est le premier exemple d'une famille de convexes (dans toutes les dimensions) dont la quantité $\Psi_2(\cdot)$ n'est pas bornée, pour laquelle un tel résultat d'approximation est prouvé.

Il y a très peu d'espoir d'obtenir une description de la mesure uniforme sur un convexe général aussi sympathique que dans le cas de la mesure uniforme sur B_p^n. Pour aller plus loin il est nécessaire de pénétrer dans la mécanique de la preuve du théorème de Bai–Yin ([BY]) et d'en adapter les rouages à notre contexte. Ceci est possible si l'on s'autorise une plus grande marge de manœuvre[1]. Si l'approximation presque isométrique de la matrice d'inertie nécessite un contrôle total de toutes les erreurs, ce n'est pas le cas l'approxi-

[1] J'ai pu en fait démontrer la version forte — l'approximation quasi-isométrique — après la rédaction du manuscrit. Voir l'appendice 2.3.1.

mation isomorphe, où l'on cherche à obtenir une inégalité du type

$$\frac{1}{C} A_\mu \leqslant A_{\mu_N} \leqslant C A_\mu,$$

la constante C pouvant être choisie arbitrairement grande. Il est alors possible d'obtenir un résultat d'approximation, uniformément sur toute la classe des mesures log-concaves inconditionnelles :

Théorème 2.2 : *Pour tout $\rho > 1$ il existe des constantes $C(\rho), c(\rho)$, telles que, pour toute mesure log-concave isotrope inconditionnelle μ sur $\mathbf{R}^n$, si $(X_1, \ldots, X_N)$ sont i.i.d. de loi μ avec $N \geqslant \rho n$, alors avec probabilité supérieure à $1 - \exp(-c(\rho) n^{1/11})$, on a*

$$\|A_{\mu_N}\| \leqslant C(\rho) \text{ et } \|A_{\mu_N}^{-1}\| \leqslant C(\rho),$$

ou en d'autres termes, pour tout θ dans S^{n-1}

$$\frac{1}{C(\rho)} \leqslant \frac{1}{N} \sum_{i=1}^{N} \langle X_i, \theta \rangle^2 \leqslant C(\rho).$$

Il est frappant de remarquer que le facteur $\rho > 1$ peut être choisi aussi petit que possible. Par exemple, seulement $[1.1n]$ échantillons suffisent à déterminer, avec une erreur contrôlée et une grande probabilité, la matrice d'inertie d'un convexe inconditionnel ! Ce phénomène ne semble pas avoir été observé précédemment. Il est bien sûr tentant de conjecturer qu'un résultat similaire reste vrai pour des convexes généraux ; répondre à cette question nécessiterait vraisemblablement de nouveaux outils car notre preuve utilise la propriété d'inconditionnalité de manière centrale.

2.2 Sampling convex bodies: the random matrix approach

We adapt results and techniques from the classical Random Matrix Theory (where matrices have independent entries) to the framework of matrices with independent rows. We prove that the inertia ellipsoid of a log-concave unconditional measure in $\mathbf{R}^n$ can be isomorphically approximated by cn sample points, for any $c > 1$. For ℓ_p^n balls we also obtain almost isometric approximation.

2.2.1 Introduction

The following notation will be kept throughout the paper: $C, c, C', \ldots$ denote absolute constants whose value may change from line to another. By μ we denote a probability measure on $\mathbf{R}^n$ which is isotropic, i.e. for any direction θ in the unit sphere S^{n-1}, $\int_{\mathbf{R}^n} \langle x, \theta\rangle d\mu = 0$ and $\int_{\mathbf{R}^n} \langle x, \theta\rangle^2 d\mu = 1$. The random vectors $X_1, \ldots, X_N$ are i.i.d. according to μ. The matrix $\Gamma = \Gamma_N$ and $A = A_N$ denote respectively

$$\Gamma_N = \frac{1}{\sqrt{N}} \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_N \end{pmatrix} \tag{2.12}$$

$$A_N = \Gamma_N^\dagger \Gamma_N = \frac{1}{N} \sum_{i=1}^N |X_i\rangle\langle X_i| \tag{2.13}$$

The matrix A must be thought of as the empirical approximation to the inertia matrix of μ, which equals the identity matrix because of the isotropy condition ($\mathbf{E}|X\rangle\langle X| = \mathrm{Id}$). In this situation we say that Γ and A sample the measure μ (with N sample points). A natural question asked in [KLS] is then: how large the number N of sample points should be to ensure that the empirical inertia matrix A is, with high probability, $(1+\varepsilon)$-close to the identity, in the sense that

$$\mathbf{P}\left(\left\| \frac{1}{N} \sum_{i=1}^N |X_i\rangle\langle X_i| - \mathrm{Id} \right\| \geqslant \varepsilon \right) \leqslant \varepsilon \tag{2.14}$$

Note for future reference that $\|A\| = \|\Gamma\|^2 = s_1(\Gamma)^2$ and $\|A^{-1}\| = s_n(\Gamma)^{-2}$, where $s_1(\Gamma)$ (resp. $s_n(\Gamma)$) denotes the largest (resp. smallest) singular value of Γ. Of course N must also depend on the error ε allowed; however here we are interested in asymptotics when the dimension n tends to infinity. A general result in this direction was obtained by Rudelson, who proved in [Rud] the following result valid for any isotropic random vector X in $\mathbf{R}^n$ (X_i being i.i.d. copies of X)

$$\mathbf{E}\left\|\frac{1}{N}\sum_{i=1}^{N}|X_i\rangle\langle X_i| - \mathrm{Id}\right\| \leqslant C\sqrt{\frac{\log n}{N}}(\mathbf{E}\|X\|_2^{\log N})^{1/\log N} \tag{2.15}$$

provided that the r.h.s. is smaller that 1, $\|\cdot\|_2$ being the Euclidean norm on $\mathbf{R}^n$.

To get any result using this inequality it is clear that one must take N at least $c(\varepsilon)n\log n$, since the parenthesis in the r.h.s. is always larger than $(\mathbf{E}\|X\|_2^2)^{1/2} = \sqrt{n}$. In some cases this is sharp: consider for example the isotropic probability measure which assigns a mass $1/2n$ to the points $\pm\sqrt{n}e_i$, where (e_i) is the canonical basis of $\mathbf{R}^n$. This case is fairly simple to analyze, and is equivalent to the following probabilistic experiment: put randomly, uniformly and independently N balls into n urns. How large should be N such that, with high probability, all urns contain between $(1+\varepsilon)N/n$ balls and $(1+\varepsilon)^{-1}N/n$ balls ? This is a classical problem and the answer is of order $N \approx c(\varepsilon)n\log n$ ([KSC]), the bound obtained using (2.15). This example is the simplest example of a frame, which are studied in [Ver].

We are interested here in the case when μ has a log-concave density, and more specially when it is the uniform measure μ_K on a convex body K. We say that K is isotropic if μ_K is isotropic; note that this definition is slightly different from the usual one in asymptotic convex geometry, where normalization is achieved by setting $\mathrm{vol}(K) = 1$. A special class of measures with extra symmetry properties is the class of unconditional measures: they are the measures μ which are invariant under reflections into coordinate hyperplanes, i.e. for any Borel set $A \subset \mathbf{R}^n$ and η in $\{-1,1\}^n$, we have $\mu(A) = \mu(S_\eta A)$, where S_η is the linear map defined by $S_\eta(x_1,\dots,x_n) = (\eta_1 x_1,\dots,\eta_n x_n)$. We similarly say that K is unconditional if μ_K is unconditional.

In the case of an isotropic convex body, it was proved by Kannan, Lovász and Simonovits ([KLS]) that (2.14) holds when $N \geqslant C(\varepsilon)n^2$, where $C(\varepsilon)$ is a constant; we are not interested in the dependence in ε here. This was improved later to $N \geqslant C(\varepsilon)n\log^3 n$ by Bourgain ([Bou]) and to $N \geqslant C(\varepsilon)n\log^2 n$ by Rudelson as a consequence of (2.15). As noted in [GM], a slight modification of Bourgain's argument also gives $N \geqslant C(\varepsilon)n\log^2 n$. In some special cases it is possible to use Rudelson's technique with full strength: for unconditional bodies $N \geqslant C(\varepsilon)n\log n$ points are enough, as shown by Giannopoulos, Hartzoulaki and Tsolomitis ([GHT]).

Let us introduce now some useful terminology: for $\alpha \in [1,2]$, the Ψ_α

norm of a random variable f is defined by

$$\|f\|_{\Psi_\alpha} = \inf\{t > 0 \text{ s.t. } \mathbf{E}\exp((f/t)^\alpha) \leqslant 2\} \tag{2.16}$$

This is a Orlicz norm. Moreover, (2.16) implies the moments and tail estimates (C is an absolute constant)

$$\forall p \leqslant 1, \mathbf{E}|f|^p \leqslant (Cp\|f\|_{\Psi_\alpha})^{p/\alpha} \tag{2.17}$$

$$\forall t > 0, \mathbf{P}(|f| \geqslant t) \leqslant 2\exp(-(f/\|f\|_{\Psi_\alpha})^\alpha) \tag{2.18}$$

An isotropic random vector X in $\mathbf{R}^n$ is said to be Ψ_α (with constant κ) is all its marginals are uniformly Ψ_α:

$$\forall \theta \in S^{n-1}, \|\langle X, \theta\rangle\|_{\Psi_\alpha} \leqslant \kappa$$

If a random vector is Ψ_2 with constant κ, then the number of points in the approximation problem can be chosen to be proportional to the dimension: for every ε, there is a constant C depending on ε and on κ such that, if $N \geqslant C(\varepsilon, \kappa)n$ and A defined as (2.13), then with probability larger than ε, $\|A - \mathrm{Id}\| \leqslant \varepsilon$. This was previously shown in proposition 2.1. Much more can actually be proved for Ψ_2 random vectors; see [MPT]. Examples of Ψ_2 random vectors are vectors uniformly distributed on (the isotropic image of) the ℓ_p^n ball for p larger than 2 (see [BGMN]).

On the other hand, there is a very different class of measures for which, at least asymptotically, we can do better and take N proportional to n: the class of product measures. If $\mu = \nu^{\otimes n}$, where ν is a probability measure on $\mathbf{R}$, the entries of Γ are i.i.d. random variables, and this enters the setting of the following result of Bai and Yin ([BY]). The notation $[\cdot]$ stands for integer part.

Theorem (Bai–Yin): *Fix a real number $\beta \in (0,1)$ and a measure ν on $\mathbf{R}$ with mean zero, variance one and finite fourth moment. For each n, let $B^{(n)}$ be a $n \times N$ random matrix with entries i.i.d. according to ν, with $N = [n/\beta]$. Then, almost surely,*

$$\lim_{n\to+\infty} s_1\left(\frac{1}{\sqrt{N}}B^{(n)}\right) = 1 + \sqrt{\beta} \text{ and } \lim_{n\to+\infty} s_n\left(\frac{1}{\sqrt{N}}B^{(n)}\right) = 1 - \sqrt{\beta} \tag{2.19}$$

The matrices $B^{(n)}$ satisfying the hypotheses of the Bai–Yin theorem are sometimes called Wishart matrices. This theorem is a typical limit theorem from random matrix theory, and the drawback is that there is no quantitative estimate on the speed of convergence and no information for fixed n.

In this note we try to adapt results and techniques from Random Matrix Theory to the case of an isotropic measure uniformly distributed on a convex body. We show here that a proportional number of sample points is enough to obtain almost isometric approximation for ℓ_p^n balls, and to obtain isomorphic approximation for unconditional log-concave measures.

Theorem 2.1. *For every $\varepsilon > 0$ and $1 \leqslant p \leqslant \infty$, there is a constant $K = K(\varepsilon, p)$ such that if $(X_1, \ldots, X_N)$ are i.i.d. uniformly distributed on the isotropic image of the unit ball of ℓ_p^n with $N \geqslant Kn$, then with probability larger than $1 - \varepsilon$, we have*

$$\left\| \frac{1}{N} \sum_{i=1}^{N} |X_i\rangle\langle X_i| - \mathrm{Id} \right\| \leqslant \varepsilon$$

Theorem 2.2. *For any $\rho > 1$ there are constants $C(\rho), c(\rho)$, such that for any isotropic unconditional log-concave measure μ on $\mathbf{R}^n$, if $(X_1, \ldots, X_N)$ are i.i.d. according to μ with $N \geqslant \rho n$, if A is defined as (2.13), then with probability larger than $1 - \exp(-c(\rho) n^{1/11})$ we have*

$$\|A\| \leqslant C(\rho) \text{ and } \|A^{-1}\| \leqslant C(\rho)$$

or, in other words, for every θ in S^{n-1}

$$\frac{1}{C(\rho)} \leqslant \frac{1}{N} \sum_{i=1}^{N} \langle X_i, \theta \rangle^2 \leqslant C(\rho)$$

I am not able to prove than the constant $C(\rho)$ tends to 1 when ρ tends to infinity[2]. On the other hand, we can take ρ close to 1. For example, only $1.1n$ sample points determine isomorphically the inertia ellipsoid of a n-dimensional unconditional log-concave measure.

Acknowledgement: I want to thank Alain Pajor and Olivier Guédon for many fruitful discussions and ideas.

2.2.2 The case of the unit ball of ℓ_p^n

For $1 \leqslant p < +\infty$, we write B_p^n for the unit ball of ℓ_p^n, i.e. $B_p^n = \{(x_1, \ldots, x_n) \in \mathbf{R}^n \text{ s.t. } \sum |x_i|^p \leqslant 1\}$. There exists a unique positive real $\lambda_{n,p}$ such that $\lambda_{n,p} B_p^n$ is isotropic, and we write $\tilde{B}_p^n = \lambda_{n,p} B_p^n$. We will use the following representation of the uniform measure on B_p^n by Barthe, Guédon, Mendelson and Naor in order to transfer results from the case with independent entries.

[2] I was actually able, after the manuscript was submitted. See Appendix 2.3.1.

Theorem ([BGMN]). *Let (Y_i) be a n-tuple of i.i.d. random variables distributed according to the probability ν_p with density $1/(2\Gamma(1+1/p))e^{-|t|^p}$ ($t \in \mathbf{R}$). We write $Y = (Y_1, \ldots, Y_n)$. Let also Z be an exponential random variable independent from Y (i.e. the density of Z is $e^{-t}, t \geqslant 0$). Then the random vector*

$$\frac{Y}{(\sum_{i=1}^n |Y_i|^p + Z)^{1/p}} \tag{2.20}$$

generates the normalized Lebesgue measure on B_p^n.

The following lemma will enable us to transfer the results from the independent case to the B_p^n case.

Lemma 13. *Let Γ be a $N \times n$ matrix whose rows are i.i.d. random vectors distributed according to the Lebesgue measure on $\tilde{B}_p^n$. Let $B = (b_{ij})$ be a $N \times n$ random matrix whose entries are independent and distributed according to ν_p. Let Δ be a $N \times N$ diagonal matrix with entries $\delta_{jj} = (\sum_{i=1}^n |b_{ij}|^p + Z_j)^{-1/p}$, where Z_j are i.i.d. exponential random variables independent from B. Then the random matrices Γ and $\lambda_{n,p}\Delta \cdot B$ have the same distribution (here $\cdot$ is the usual matrix product).*

Proof. It is a direct application of the representation theorem. □

Using this trick, results on Wishart matrices can be transferred to the case of random matrices sampling $\tilde{B}_p^n$, since the diagonal matrix Δ will be very close to the identity matrix. It is actually quite easy to get from lemma 13 a limit theorem holding almost surely using the result of Bai and Yin. It is here possible using concentration properties to derive from the almost sure result a result holding for all n (or for all n large enough). The following lemma will be useful

Lemma 14. *For fixed n and fixed probability measure μ on $\mathbf{R}^n$, if (Y_i) are i.i.d. random vectors distributed according to μ, then*

$$\mathbf{E}\lambda_{max}\left(\frac{1}{N}\sum_{i=1}^N |Y_i\rangle\langle Y_i|\right)$$

is a decreasing function of N, whereas

$$\mathbf{E}\lambda_{min}\left(\frac{1}{N}\sum_{i=1}^N |Y_i\rangle\langle Y_i|\right)$$

is an increasing function of N.

Proof. Let $N_1 \geqslant N_2$. Let also I be a random subset of cardinality N_2 of $\{1,\ldots,N_1\}$, uniformly chosen. We write $\mathbf{E}'$ for the expectation with respect to I, this is just a short way to write a finite sum. It follows from the convexity of the function λ_{max} on the set of self-adjoint matrices that

$$\begin{aligned}
\mathbf{E}\lambda_{max}\left(\frac{1}{N_1}\sum_{i=1}^{N_1}|X_i\rangle\langle X_i|\right) &= \mathbf{E}\lambda_{max}\left(\frac{1}{N_2}\mathbf{E}'\sum_{i\in I}|X_i\rangle\langle X_i|\right)\\
&\leqslant \mathbf{E}\mathbf{E}'\lambda_{max}\left(\frac{1}{N_2}\sum_{i\in I}|X_i\rangle\langle X_i|\right)\\
&= \mathbf{E}\lambda_{max}\left(\frac{1}{N_2}\sum_{i=1}^{N_2}|X_i\rangle\langle X_i|\right)
\end{aligned}$$

The second statement follows similarly from the concavity of the function λ_{min}. □

We fix $p \in [1,\infty]$. Given $\varepsilon > 0$, we choose ρ such that $1 + 1/\sqrt{\rho} \leqslant (1+\varepsilon)^{1/3} - \varepsilon/6$ and $1 - 1/\sqrt{\rho} \geqslant (1-\varepsilon)^{1/3} + \varepsilon/6$. For each n and N, consider the matrix Γ sampling the uniform measure on $\tilde{B}_p^n$ with N sample points, defined as (2.12). We will rather consider the matrix $\tilde{\Gamma} = \frac{\lambda_{n,p}}{\sqrt{N}}\Delta \cdot B$, where B and Δ are defined as in lemma 13; hence Γ and $\tilde{\Gamma}$ are identically distributed. We may write $\Gamma^{(n)}$, $B^{(n)}$, ... to insist on the dependence in n. We write r for the normalization factor $(\mathbf{E}b_{11}^2)^{-1/2}$, so that the matrix $rB^{(n)}$ has i.i.d. entries with mean 0 and variance 1. We will prove the following lemmas about the matrices B and Δ appearing in the decomposition

Lemma 15. *There is an integer n_0 (depending only on ε and p) such that for any $n \geqslant n_0$ and $N \geqslant \rho n$, we have with probability larger that $1 - \varepsilon/2$, if B is an $N \times n$ matrix with entries i.i.d. according to ν_p*

$$(1-\varepsilon)^{1/3}\sqrt{N} \leqslant s_n(rB) \leqslant s_1(rB) \leqslant (1+\varepsilon)^{1/3}\sqrt{N} \tag{2.21}$$

Proof. We use here concentration of measure: it is known that the measures ν_p satisfies a Poincaré inequality on $\mathbf{R}$ (see [Led1]). This implies concentration for the product measures: for any $k \geqslant 1$ and any function $f : \mathbf{R}^k \to \mathbf{R}$ which is 1-Lipschitz with respect to the Euclidean distance on $\mathbf{R}^k$

$$\nu_p^{\otimes k}(\{(v_1,\ldots,v_k) \text{ s.t. } |f(v_1,\ldots,v_k) - \mathbf{E}_{\nu_p^{\otimes k}} f| > t\}) \leqslant C_p \exp(-c_p t) \tag{2.22}$$

This can be applied to the largest (resp. smallest) singular value of a matrix, which is a 1-Lipschitz function of the entries of the matrix with respect to the

Hilbert–Schmidt distance, as can be seen from the min-max characterization (where M is a $N \times n$ matrix)

$$s_1(M) = \max_{x \in S^{n-1}} \max_{y \in S^{N-1}} \langle Mx, y \rangle$$

$$s_n(M) = \min_{x \in S^{n-1}} \max_{y \in S^{N-1}} \langle Mx, y \rangle$$

In our context, (2.22) gives

$$\mathbf{P}(|s_1(rB^{(n)}) - \mathbf{E}s_1(rB^{(n)})| \geqslant t) \leqslant C_p \exp(-c_p t/r) \tag{2.23}$$

$$\mathbf{P}(|s_n(rB^{(n)}) - \mathbf{E}s_n(rB^{(n)})| \geqslant t) \leqslant C_p \exp(-c_p t/r) \tag{2.24}$$

The matrix $rB^{(n)}$ has i.i.d. entries with mean 0 and variance 1, therefore it enters the setting of Wishart matrices and the Bai–Yin theorem (2.19) holds: if $N = [\rho n]$, this gives that almost surely, $\lim_{n\to\infty} s_1(rB^{(n)})/\sqrt{N} = 1 + 1/\sqrt{\rho}$ and $\lim_{n\to\infty} s_n(rB^{(n)})/\sqrt{N} = 1 - 1/\sqrt{\rho}$. A first consequence is that for any $\theta > 0$ there is a integer $n_1 = n_1(\varepsilon, p, \theta)$ such that for $n \geqslant n_1$ and $N = [\rho n]$:

$$1 - 1/\sqrt{\rho} - \theta \leqslant \mathbf{E}s_n(rB)/\sqrt{N} \leqslant \mathbf{E}s_1(rB)/\sqrt{N} \leqslant 1 + 1/\sqrt{\rho} + \theta \tag{2.25}$$

Indeed, if for example the right inequality was false, then using (2.23) we get that for n large enough, $\mathbf{P}(s_1(rB)/\sqrt{N} \geqslant 1 + 1/\sqrt{\rho} + \theta/2) \geqslant 1/2$, and this contradicts the almost sure convergence. The other inequality is handled similarly. In order to use lemma 14, we would prefer a statement about the second moment rather that the expectation. This can be done using concentration; another consequence of (2.23) and (2.24) is that

$$\mathbf{E}(s_1(rB))^2 - (\mathbf{E}s_1(rB))^2 = \int_0^\infty \mathbf{P}(|s_1(rB) - \mathbf{E}s_1(rB)|^2 > t)dt \leqslant \frac{2Cr^2}{c^2} \tag{2.26}$$

and similarly for s_n. Together with (2.25), this gives the existence of an integer $n_2 = n_2(\varepsilon, p, \theta)$ such that for $n \geqslant n_2$ and $N = [\rho n]$

$$\begin{aligned}(1 - 1/\sqrt{\rho} - 2\theta)^2 \quad &\leqslant \mathbf{E}(s_n(rB)/\sqrt{N})^2 \leqslant \\ &\leqslant \mathbf{E}(s_1(rB)/\sqrt{N})^2 \leqslant \quad (1 + 1/\sqrt{\rho} + 2\theta)^2\end{aligned}$$

Lemma 14 allows to extend automatically these inequalities to all $N \geqslant \rho n$. Using again (2.26) to come back to expectations, this gives a rank $n_3 = n_3(\varepsilon, p, \theta)$ such that if $n \geqslant n_3$ and $N \geqslant \rho n$

$$1 - 1/\sqrt{\rho} - 3\theta \leqslant \mathbf{E}s_n(rB)/\sqrt{N} \leqslant \mathbf{E}s_1(rB)/\sqrt{N} \leqslant 1 + 1/\sqrt{\rho} + 3\theta$$

Using again concentration inequalities (2.23) and (2.24), this gives for $n \geqslant n_4(\varepsilon, p, \theta)$ and $N \geqslant \rho n$, with probability larger that $1 - \varepsilon/2$:

$$1 - 1/\sqrt{\rho} - 4\theta \leqslant s_n(rB)/\sqrt{N} \leqslant s_1(rB)/\sqrt{N} \leqslant 1 + 1/\sqrt{\rho} + 4\theta$$

It remains to choose $\theta = \varepsilon/24$ to prove the lemma. $\square$

Lemma 16. *There is an integer n_0' and a constant β (depending only on ε and $p \leqslant 2$) such that for any $n \geqslant n_0'$ and $N \leqslant \exp(\beta n)$, if Δ is a $N \times N$ diagonal matrix with entries $\delta_{jj} = (\sum_{i=1}^n |b_{ij}|^p + Z_j)^{-1/p}$, with (b_{ij}) i.i.d. according to ν_p and (Z_j) i.i.d. according to ν_1, then with probability larger than $1 - \varepsilon/2$,*

$$(1-\varepsilon)^{1/3}(n\mathbf{E}|b_{11}|^p)^{-1/p} \leqslant s_n(\Delta) \leqslant s_1(\Delta) \leqslant (1+\varepsilon)^{1/3}(n\mathbf{E}|b_{11}|^p)^{-1/p} \quad (2.27)$$

Proof. Since $p \leqslant 2$, the random variables $|b_{ij}|^p$ and Z_j are Ψ_1 with constant depending on p, and the same is true for their centered versions $|b_{ij}|^p - \mathbf{E}|b_{11}|^p$ and $Z_j - \mathbf{E}Z_j$. Applying Bernstein's inequality (lemma 12), we get for any $\theta \leqslant C$ and any $1 \leqslant j \leqslant N$

$$\mathbf{P}\left(\left|\sum_{i=1}^N |b_{ij}|^p + Z_j - n\mathbf{E}|b_{ij}|^p\right| \geqslant \theta n + 1\right) \leqslant 2\exp(-c_p\theta^2 n)$$

By choosing θ small enough (depending on ε), we get for any fixed j, with probability larger than $1 - \exp(-c(\varepsilon, p)n)$

$$(1-\varepsilon)^{1/3}(n\mathbf{E}|b_{11}|)^{-1/p} \leqslant \delta_{jj} \leqslant (1+\varepsilon)^{1/3}(n\mathbf{E}|b_{11}|)^{-1/p}$$

For n large enough, the conclusion of the lemma holds since $s_n(\Delta) = \min(\delta_{jj})$ and $s_1(\Delta) = \max(\delta_{jj})$. $\square$

Proof of theorem 2.1: For $p \geqslant 2$, a random vector uniformly distributed on the $\tilde{B}_p^n$ ball is Ψ_2 (see [BGMN]). Since for Ψ_2 random vectors it is known that one can always take a proportional number of sample points (proposition 2.1), we can assume that $p \leqslant 2$.

The constant $\lambda_{n,p}$ can be calculated using the representation theorem, or by direct calculation:

$$\lambda_{n,p} = \left(\frac{1}{\mathrm{vol}(B_p^n)}\int_{B_p^n} x_1^2 dx_1 \ldots dx_n\right)^{-1/2} \sim_{n\to\infty} \frac{n^{1/p}(\mathbf{E}|b_{11}|^p)^{1/p}}{(\mathbf{E}b_{11}^2)^{1/2}} \quad (2.28)$$

And so for n bigger than some n_1,

$$(1-\varepsilon)^{1/3}\frac{(n\mathbf{E}|b_{11}|^p)^{1/p}}{(\mathbf{E}b_{11}^2)^{1/2}} \leqslant \lambda_{n,p} \leqslant (1+\varepsilon)^{1/3}\frac{(n\mathbf{E}|b_{11}|^p)^{1/p}}{(\mathbf{E}b_{11}^2)^{1/2}} \quad (2.29)$$

Let now n bigger than $\max(n_0, n_0', n_1)$, where n_0 and n_0' appear in lemmas 15 and 16. Then the statements (2.21), (2.27) and (2.29) hold simultaneously with probability larger than $1-\varepsilon$. Using the inequalities $s_1(\Delta \cdot B) \leqslant s_1(\Delta)s_1(B)$ and $s_n(\Delta \cdot B) \geqslant s_n(\Delta)s_n(B)$, this implies $s_1(\Gamma) \leqslant 1+\varepsilon$ and $s_n(\Gamma) \geqslant 1-\varepsilon$, provided $n \geqslant \max(n_0, n_0', n_1)$ and $\rho n \leqslant N \leqslant \exp(\beta n)$. We now by previous results ([Rud] for example) than the same conclusion holds true if $N \geqslant C(\varepsilon) n \log^2 n$. If we define $\bar{n}$ to be the smallest number so that $\bar{n} \geqslant \max(n_0, n_0', n_1)$ and $C(\varepsilon)\bar{n}\log^2 \bar{n} \leqslant \exp(\beta \bar{n})$, this proves the theorem with $K(\varepsilon, p) = \rho$ and for n larger than $\bar{n}$. This latter condition can be removed by enlarging the constant $K(\varepsilon, p)$ to $K'(\varepsilon, p) = \max(\rho, C(\varepsilon)\log^2 \bar{n})$. □

Remark: We used here the theorem of Bai–Yin as a “black box”. This has several serious drawbacks: for example we have no information of the behavior of the function $C(\varepsilon)$ in theorem 2.1, it may even depend on p. The right thing to do to avoid these problems should be to prove an analogue of Bai–Yin theorem valid for all dimensions n, with deviations estimates depending on the moments of the entries. Such a localized version was obtained by Sodin ([Sod]) in the case of ± 1 random variables where he could use special properties of the entries to simplify the calculations.

The same trick allows us to transfer available results for the so-called global regime:

Theorem 2.3. *Fix $1 \leqslant p \leqslant +\infty$. For any n, let Γ be defined as usual, using $N = [n/\beta]$ sample points according to the uniform measure on $\tilde{B}_p^n$. Let $s_n(\Gamma) \leqslant \cdots \leqslant s_1(\Gamma)$ be the singular values of Γ, and $\mu_\Gamma = 1/n \sum_{i=1}^n \delta_{s_i(\Gamma)}$ be the empirical spectral measure: for every Borel set $B \subset \mathbf{R}$, $\mu_\Gamma(B)$ is the proportion of singular values which fall in B. Then, almost surely, the sequence (μ_Γ) converges weakly to the Marčenko–Pastur distribution μ_β supported on the interval $[1-\sqrt{\beta}, 1+\sqrt{\beta}]$ and with density*

$$\frac{d\mu_\beta}{dx} = \frac{1}{\pi \beta x}\sqrt{((1+\sqrt{\beta})^2 - x^2)(x^2 - (1-\sqrt{\beta}))^2}$$

Proof. As in the previous proof, we use the alternative representation from lemma 13: $\tilde{\Gamma} = \frac{\lambda_{n,p}}{\sqrt{N}}\Delta \cdot B = \Delta' \cdot B'$ with $\Delta' = \lambda_{n,p}(\mathbf{E} b_{11}^2)^{1/2}\Delta$ and $B' = \frac{1}{\sqrt{N}(\mathbf{E}b_{11}^2)^{1/2}} B$. The matrix B' has i.i.d. entries with mean 0 and variance $1/\sqrt{N}$. Let $s_n(B') \leqslant \cdots \leqslant s_1(B')$ be its singular values, and $\mu_{B'} = 1/n \sum_{i=1}^n \delta_{s_i(B')}$ be its empirical spectral measure. By the classical Marčenko–Pastur theorem (see [MaPa, OP]), almost surely, the sequence $(\mu_{B'})$ converges weakly to μ_β when n tends to infinity. We want to prove that the same holds for (μ_Γ). Define δ to be the smallest number so that $\|\Delta'\| \leqslant 1+\delta$ and $\|\Delta'^{-1}\| \leqslant 1+\delta$. By repeating the proof of lemma 16 and using (2.28), we obtain that the random variable δ tends almost surely to 0 when n tends to infinity.

Note that for every $k \leqslant n$, $(1+\delta_n)^{-1}s_k(\Gamma) \leqslant s_k(B') \leqslant (1+\delta_n)s_k(\Gamma)$. This implies in particular than for any $a < b$.

$$\mu_{B'}([(1+\delta_n)a,(1+\delta_n)^{-1}b]) \leqslant \mu_\Gamma([a,b]) \leqslant \mu_{B'}([(1+\delta_n)^{-1}a,(1+\delta_n)b])$$

Consequently, we obtain that, almost surely,

$$\lim_{n\to\infty} \mu_\Gamma^{(n)}([a,b]) = \lim_{n\to\infty} \mu_{B'}^{(n)}([a,b]) = \mu_\beta([a,b])$$

Since it is enough to check the weak convergence on intervals with rational endpoints, this proves the theorem. □

Remark: The result of Theorem 2.3 was obtained independently by Pajor and Pastur ([PP]) using the Stieltjes transform method.

2.2.3 The case of unconditional log-concave measures: proof of theorem 2.2

We are first going to give a proof, based on the moments method, for the assertion on the norm of A. We work with the matrix Γ rather than with A. We denote the entries of Γ by (x_{ij}), i.e. x_{ij} is the jth coordinate of the vector X_i. We can also assume that N is not too large, for example $N \leqslant n^2$, since for larger values of N we can conclude using known results ([GHT] for example). We want to give an upper bound for $\mathbf{E}\|\Gamma\|^{2k}$ for an integer k as large as possible. We first need a truncation argument. Let E denote the event: "All entries of the matrix Γ have absolute value smaller than t_0", where the truncation level t_0, depending on k and n, will be determined later. By lemma 10.1, the one-dimensional marginals of an isotropic log-concave measure are uniformly Ψ_1: there are absolute constants c, C such that for any i, j ,

$$\mathbf{P}(|x_{ij}| > t) \leqslant C\exp(-ct)$$

Therefore $\mathbf{P}(E^c) \leqslant CnN\exp(-ct_0) \leqslant Cn^3\exp(-ct_0)$. We then write

$$\mathbf{E}\|\Gamma\|^{2k} = \mathbf{E}(\|\Gamma\|^{2k}\mathbf{1}_E) + \mathbf{E}(\|\Gamma\|^{2k}\mathbf{1}_{E^c})$$

On the small set E^c we can afford bad bounds. Denoting by $\|\cdot\|_{HS}$ the Hilbert–Schmidt norm (Euclidean norm of the entries),

$$\mathbf{E}(\|\Gamma\|^{2k}\mathbf{1}_{E^c}) \leqslant \sqrt{\mathbf{E}(\|\Gamma\|^{4k})}\sqrt{\mathbf{P}(E^c)} \leqslant \sqrt{\mathbf{E}\|\Gamma\|_{HS}^{4k}}\sqrt{C}n^{3/2}\exp(-ct_0/2)$$

Writing $\mathbf{E}\|\Gamma\|_{HS}^{4k}$ as $1/N^{2k}\mathbf{E}(\sum x_{ij}^2)^{2k}$ and expanding the sum, we obtain $(nN)^{2k}$ terms of the form $\mathbf{E}\prod_{r=1}^{2k} x_{i_r j_r}$. We bound each of them by

$$\prod_{r=1}^{2k}(\mathbf{E}x_{i_r j_r}^{4k})^{1/2k}$$

by Hölder inequality, and use the moment version (2.18) of the Ψ_1 property of the entries of Γ to get for an absolute constant C

$$\mathbf{E}\|\Gamma\|_{HS}^{4k} \leqslant n^{2k}(Ck)^{4k}$$

Putting all estimates together, we obtain

$$\mathbf{E}(\|\Gamma\|^{2k}\mathbf{1}_{E^c}) \leqslant n^{k+3/2}(Ck)^{2k}\sqrt{C}\exp(-ct_0/2)$$

We now set $t_0 = C_1 k \log n$, where the absolute constant C_1 is chosen so that $\mathbf{E}(\|\Gamma\|^{2k}\mathbf{1}_{E^c}) \leqslant 1$ (we will later choose k smaller than n).

It now remains to study $\mathbf{E}(\|\Gamma\|\mathbf{1}_E)$. We bound the operator norm, which is the ℓ_∞^n norm of singular values, by the Schatten norm $\|A\|_k = (\sum s_i(\Gamma)^k)^{1/k}$.

$$\|\Gamma\|^{2k} \leqslant \|A\|_k^k = \mathrm{tr}(A^k)$$

We get by expanding the trace that

$$\mathbf{E}\mathrm{tr}(A^k)\mathbf{1}_E = \frac{1}{N^k}\sum \mathbf{E}x_{i_1j_1}x_{i_1j_2}x_{i_2j_2}\dots x_{i_kj_k}x_{i_kj_1}\mathbf{1}_E,$$

where the sum is taken over all indices $i_1,\dots,i_k$ in $\{1,\dots,N\}$ and $j_1,\dots,j_k$ in $\{1,\dots,n\}$. Since the rows of Γ are independent, the expectation can be factorized as the product of N factors of the form

$$\mathbf{E}x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}\mathbf{1}_F \tag{2.30}$$

for some integers $\alpha_1,\dots,\alpha_n$, where $X = (x_1,\dots,x_n)$ is a random vector distributed according to the sampled measure, and F is the event: "all coordinates of X have absolute value smaller than t_0". Since the vector X, as well as its truncated variant $X\mathbf{1}_F$, are unconditional, there are invariant under sign operators S_η, and this shows that the expectation (2.30) is zero when at least one of the α_i is odd. Now the arguments follows essentially the classical combinatorial techniques of [Gem, YBK], which for the reader's convenience we repeat here. We are lead to the following inequality

$$\mathbf{E}\|\Gamma\|^{2k}\mathbf{1}_E \leqslant \frac{1}{N^k}\sum_{[(r_1,s_1),\dots,(r_{2k},s_{2k})]\ \text{V-graph}} \mathbf{E}x_{r_1s_1}\dots x_{r_{2k}s_{2k}}\mathbf{1}_E$$

where a V-graph is a $2k$-uple of couples $(r_i,s_i)\in\{1,\dots,N\}\times\{1,\dots,n\}$ such that

1. $r_{2p} = r_{2p-1}$
2. $s_{2p+1} = s_{2p}$ (and $s_1 = s_{2p}$)
3. Each couple (r_i, s_i) appears an even number of times.

Now we use the following strategy: if some x_{ij} appears 4 times or more, we bound it by t_0, and after this, since the event E has played its role, we also use $\mathbf{1}_E \leqslant 1$. Thus there only remain squared coefficients, which are treated by lemma 11 : for any $I \subset \{1, \ldots, n\}$, we have

$$\mathbf{E} \prod_{i \in I} x_i^2 \leqslant C^{\#I}.$$

Call two V-graphs $G = [(r_i, s_i)]$ and $G' = [(r_i', s_i')]$ isomorphic if there exist permutations $\sigma \in \mathfrak{S}_N$ and $\tau \in \mathfrak{S}_n$ such that $r_i' = \sigma(r_i)$ and $s_i' = \tau(s_i)$. For a V-graph $G = [(r_1, r_1), \ldots, (r_{2k}, r_{2k})]$, we define the invariant ℓ by $\ell(G) := \#\{r_i\} + \#\{s_i\}$. It the number of different indices that appear in G; note that $2 \leqslant \ell(G) \leqslant k + 1$. Also, the isomorphism class of G contains no more than $N^{\ell(G)}$ elements (recall that $n \leqslant N$).

Let $n_2(G)$ be the number of indices i such that the couple (r_i, s_i) appears exactly 2 times in G and $n_+(G)$ be the number of indices i such that the couple (r_i, s_i) appears 4 times or more in G. Since there are at least $\ell(G) - 1$ different couples (r_i, s_i) in G, we get the relations $\ell(G) - 1 \leqslant \frac{1}{2} n_2 + \frac{1}{4} n_+$ and $n_2 + n_+ = 2k$, which imply that n_+ is smaller that $4(k - \ell(G) + 1)$. Applying the strategy described before to bound the expectations, and gathering V-graphs with the same ℓ, we get:

$$\mathbf{E} \|\Gamma\|^{2k} \mathbf{1}_E \leqslant \left(\frac{C}{N} \right)^k \sum_{l=2}^{k+1} N^l t_0^{4(k-l)+2} \gamma_l \tag{2.31}$$

where γ_l is the number of isomorphism classes of V-graphs G for which $\ell(G) = l$. To each V-graph $[(r_1, r_1), \ldots, (r_{2k}, r_{2k})]$, we associate its type sequence, which is a sequence $(\tau_1, \ldots, \tau_{2k})$ of elements of $\{\mathrm{T}_1, \mathrm{T}_{3a}, \mathrm{T}_{3u}, \mathrm{T}_4\}$ defined as follows

- $\tau_i = \mathrm{T}_1$ when (r_i, s_i) is an innovation, i.e. either r_i is not in the set $\{r_j, j < i\}$ (row innovation), or s_i is not in the set $\{s_j, j < i\}$ (column innovation). The first element is always an innovation. Also, row innovations can only occur when i is odd and column innovations when i is even.

- $\tau_i = \mathrm{T}_{3a}$ or T_{3u} if (r_i, s_i) is the first repetition of an innovation, i.e. there exists $i_0 < i$ such that $(r_{i_0}, s_{i_0}) = (r_i, s_i)$, and for every k such that $i_0 < k < i$, $(r_k, s_k) \neq (r_i, s_i)$. If this repetition is ambiguous, i.e. if there exist an other unmatched innovation which is in the row/column in which (r_i, s_i) must lie, then we set $\tau_i = \mathrm{T}_{3a}$. If not, the repetition is unambiguous and we set $\tau_i = \mathrm{T}_{3u}$.

- $\tau_i = \mathrm{T}_4$ in the other cases.

The type sequence is an invariant of V-graph isomorphism. Moreover, there are at most $4^{2k} = 16^k$ possible type sequence (this is very rough, but here we do not claim at optimality of constants). Also, there are exactly $\ell(G) - 1$ innovations in a V-graph G, and consequently exactly $\ell(G) - 1$ first repetitions of these innovations. Consequently, there are exactly $2(k - \ell(G) + 1)$ type T_4 elements. The nice fact is that when ℓ becomes large, there are rather few isomorphism classes of V-graphs which have a given type sequence; this compensates for the fact that each individual isomorphism class is large. To check this fact, in each isomorphism class of V-graphs, we single out a element, called canonical V-graph, by the properties

- The first element is $(1, 1)$

- Each time a new index r_i (resp. s_i) appears, it is the smallest available one (i.e. the smallest number which is not in $\{r_j, j < i\}$ (resp. $\{s_j, j < i\}$))

Note that in any canonical V-graph, all indices all smaller than k (they are even smaller than $\ell - 1$). Now if we try to reconstruct a canonical V-graph from its type sequence starting from $(1, 1)$, some steps are unambiguous: when $\tau_i = \mathrm{T}_1$ (since the V-graph is canonical we must go to the next free row/column) and when $\tau_i = \mathrm{T}_{3u}$. The other steps ($\tau_i = \mathrm{T}_{3a}$ and $\tau_i = \mathrm{T}_4$) are ambiguous, but for each of them there are at most k possible choices by the previous remark. The main lemma is now the following

Lemma 17 ([Gem],[YBK]). *The number of ambiguous repetitions ($\tau_i = \mathrm{T}_{3a}$) in a V-graph is no more than twice the number of T_4 elements ($\tau_i = \mathrm{T}_4$).*

Proof. We give a very sketchy proof and refer to [Gem, YBK] for more details. We write n_4 for the number of type T_4 elements. If $\tau_i = \mathrm{T}_{3a}$, then $\tau_{i-1} \neq \mathrm{T}_1$, otherwise there could not be ambiguity. If $\tau_{i-1} = \mathrm{T}_{3a}$ or $\tau_{i-1} = \mathrm{T}_{3u}$, this means that at time $i - 2$ there must have been 3 unmatched innovations in the corresponding row/column. One can check that only type T_4 elements can create such a situation, so this can occur at most n_4 times (this is the delicate point). Also, it can happen that $\tau_{i-1} = \mathrm{T}_4$, but only at most n_4 times. This proves the lemma. $\square$

The preceding discussion, together with lemma 17, gives

$$\gamma_l \leqslant 16^k k^{6(k-l+1)} \tag{2.32}$$

Plugging (2.32) into (2.31), we obtain

$$\mathbf{E}(\|\Gamma\|^{2k}\mathbf{1}_E) \leqslant C^k k^6 t_0^2 \sum_{l=2}^{k+1} \left(\frac{t_0^4 k^6}{N}\right)^{k-l}$$

Recall that $t_0 = C_1 k \log n$ and choose now $k = [n^{1/11}]$, so that for n large enough the parenthesis is smaller that 1, and the r.h.s. is bounded by C'^k for an absolute constant C'. Together with the estimate for E^c, this gives

$$\text{For } n \geqslant n_0 \text{ and } k = [n^{1/11}], \mathbf{E}\|\Gamma\|^k \leqslant C'^k$$

By Markov inequality, we obtain immediately that

$$\mathbf{P}(\|\Gamma\| \geqslant 2C') \leqslant \mathbf{E}\|\Gamma\|^k/(2C')^k \leqslant 1/2^k$$

and this proves the assertion on $\|A\| = \|\Gamma\|^2$. It remains to show that $s_n(\Gamma)$ is bounded away from 0. We are going actually to prove a more general result, from which the theorem follows immediately.

Proposition 2.2. *For every $C_0 > 0$ and $\rho > 1$ there are constants $K = K(C_0, \rho), \kappa = \kappa(C_0, \rho)$ such that, for every isotropic log-concave measure μ, the matrix A sampling μ with $N \geqslant \rho n$ sample points, defined as (2.13), automatically satisfies*

$$\mathbf{P}(\|A^{-1}\| > K) \leqslant \mathbf{P}(\|A\| > C_0) + \exp(-\kappa n)$$

Remark: Usually in random matrix theory, it is substantially harder to deal with the smallest eigenvalue than with the largest, hence the above proposition may surprise. We emphasize that it is only an isomorphic result.

Proof. The proof is similar to the proof of the main theorem in [LPRT], but here the log-concavity makes things much easier. We will rather work with the matrix Γ, seen as a linear operator from ℓ_2^n to ℓ_2^N, and we write $|\cdot|$ for the Euclidean norm in $\mathbf{R}^n$ or $\mathbf{R}^N$. Note that $\|A^{-1}\| \geqslant K$ is equivalent to the fact that there exists x in the sphere S^{n-1} such that $|\Gamma x| \leqslant 1/\sqrt{K}$. Let now be $\mathcal{N}$ be a ε-net in S^{n-1} with cardinality smaller that $(3/\varepsilon)^n$ (see lemma 2). Set also $t = \varepsilon/\sqrt{C_0}$. Let $\bar{\Omega}$ be the set of events ω such that $\|\Gamma(\omega)\| \leqslant \sqrt{C_0}$. By the standard approximation argument, the event

$$\bar{\Omega} \cap \{\exists x \in S^{n-1} \text{ s.t. } |\Gamma x| \leqslant t\}$$

is contained in the event

$$\bar{\Omega} \cap \{\exists x \in \mathcal{N} \text{ s.t. } |\Gamma x| \leqslant 2t\}$$

Consequently,

$$\mathbf{P}(s_n(\Gamma) \leqslant t) \leqslant \mathbf{P}(\bar{\Omega}^c) + \#(\mathcal{N}) \max_{x \in S^{n-1}} \mathbf{P}(|\Gamma x| \leqslant 2t)$$

For fixed x in the sphere S^{n-1} and j between 1 and N, let f_j be the random variable $\langle X_j, x\rangle$. This is a marginal of μ. By lemma 10.2, when μ is a log-concave isotropic measure on $\mathbf{R}^n$, the $(n-1)$-dimensional measure of hyperplane sections is controlled up to universal constant: $\forall \theta \in S^{n-1}$ and $t \in \mathbf{R}$, we have $\int_{\theta^\perp + t\theta} d\mu \leqslant C$ for a universal constant C. This integral must be understood as $\int_{\theta^\perp + t\theta} g(x)dx$, where g is the density of μ with respect to the Lebesgue measure on $\mathbf{R}^n$. Consequently, there is an absolute constant C such that, for every $s \geqslant 0$, $\mathbf{P}(|f_j| \leqslant s) \leqslant Cs$ Calculations are now straightforward:

$$\begin{aligned}
\mathbf{P}(|\Gamma x| \leqslant 2t) &= \mathbf{P}(\sum_{j=1}^N f_j^2 \leqslant 4t^2 N) \\
&= \mathbf{P}(N - \sum_{j=1}^N f_j^2/4t^2 \geqslant 0) \\
&\leqslant \mathbf{E}\exp(N - \sum_{j=1}^N f_j^2/4t^2) \\
&= (e\mathbf{E}\exp(-f_1^2/4t^2))^N \\
&= e^N \left(\int_0^1 \mathbf{P}(\exp(-f_1^2/4t^2) > s) ds \right)^N \\
&= e^N \left(\int_0^1 \mathbf{P}(f_1 \leqslant 2t\sqrt{\log(1/s)}) ds \right)^N \\
&\leqslant e^N \left(2Ct \int_0^1 \sqrt{\log(1/s)} ds \right)^N \\
&= (Ce\sqrt{\pi}t)^N
\end{aligned}$$

And consequently

$$\mathbf{P}(s_n(\Gamma) \leqslant t) \leqslant \mathbf{P}(\|A\| \geqslant C_0) + \left(\frac{3\sqrt{C_0}}{t}\right)^n (Ce\sqrt{\pi}t)^N$$

and thus for any ρ, we can choose t and such that the conclusion of the proposition holds. $\square$

2.3 Appendice

2.3.1 Version quasi-isométrique du théorème 2.2

J'ai pu démontrer le résultat suivant, après la rédaction et la soumission d'une version préliminaire du manuscrit.

Théorème. *Pour tout $\varepsilon > 0$, il existe des constantes $C(\varepsilon), c(\varepsilon) > 0$ telles que si μ est une mesure log-concave isotrope inconditionnelle sur $\mathbf{R}^n$ et $X_1, \ldots, X_N$ sont i.i.d. de loi μ avec $N \geqslant C(\varepsilon)n$, alors avec probabilité supérieure à $1 - \exp(-c(\varepsilon)n^{1/11})$ on a ε-approximation de la matrice d'inertie de μ :*

$$\left\| \frac{1}{N} \sum_{i=1}^{N} |X_i\rangle\langle X_i| - \mathrm{Id} \right\| \leqslant \varepsilon$$

Le lecteur est renvoyé à [Aub2] pour une preuve.

Chapitre 3

Problèmes géométriques en théorie quantique de l'information

3.1 Introduction et présentation des résultats

3.1.1 Motivations et principales définitions

L'intrication quantique est un phénomène de la mécanique quantique dans lequel deux systèmes physiques (ou un plus grand nombre) ne peuvent pas être décrits séparément, bien qu'ils puissent être spatialement éloignés. Cela implique que les propriétés observables des différents systèmes sont corrélées. Il est par exemple possible de préparer deux particules de telle manière qu'en observant successivement chacune d'entre elles, on observe toujours qu'elles se trouvent dans le même état, mais qu'il demeure néanmoins impossible de prédire le résultat de la première observation. Lorsque deux systèmes quantiques sont ainsi intriqués, une mesure effectuée sur un des systèmes semble influencer instantanément l'état de l'autre système. L'intrication est un des phénomènes sur lesquels reposent, par exemple, la théorie quantique de l'information et la cryptographie quantique ; pour plus de détails sur ce sujet on pourra consulter [NC] ou [CG].

Rappelons brièvement le formalisme de la mécanique quantique qui nous sera utile. Un système quantique S est décrit par son espace d'états $\mathcal{H} = \mathcal{H}_S$, qui est un espace de Hilbert complexe. Un *état pur* du système S est un vecteur unitaire ψ de $\mathcal{H}$. Il est impossible de distinguer par une mesure l'état ψ de l'état $\alpha\psi$, où α est un nombre complexe de module 1, il est donc plus juste d'identifier l'ensemble des états à l'espace projectif sur $\mathcal{H}$, ceci sera précisé ultérieurement. On ne considérera ici que des espaces d'états de dimension finie ; l'espace $\mathcal{H}_S$ est alors identifié à $\mathbf{C}^D$, pour un entier D. Le système quantique le plus simple correspond à un espace d'états de dimension 2 ; un tel système est appelé un *qubit*. En théorie quantique de l'information, c'est l'unité minimale d'information, l'analogue du bit en théorie classique de l'information. Concrètement, un qubit peut par exemple être réalisé par le spin d'un photon. On appelle parfois *qudit* un système dont l'espace d'états associé est $\mathbf{C}^D, D > 2$.

Si $S_1, \ldots, S_N$ sont des systèmes quantiques (disjoints) d'espaces d'états respectifs $\mathcal{H}_1, \ldots, \mathcal{H}_N$, le système S formé de la réunion $S_1 \cup \cdots \cup S_N$ est complètement décrit par l'espace d'états obtenu par le produit tensoriel hilbertien des espaces d'états :

$$\mathcal{H}_S = \mathcal{H}_1 \otimes_2 \cdots \otimes_2 \mathcal{H}_N$$

On écrira généralement $\otimes$ au lieu de $\otimes_2$ pour alléger les notations. Un état pur ψ du système S est dit *pur séparable* si c'est un tenseur pur, c'est-à-dire s'il peut s'écrire sous la forme $\psi = \psi_1 \otimes \cdots \otimes \psi_N$, où pour i variant de 1 à N, ψ_i est un état pur du système S_i. Cela correspond au cas où il n'y a pas d'interaction entre les sous-systèmes de S. Un état pur qui n'est pas pur séparable est dit *pur intriqué*.

En réalité, un système quantique n'est pas en général dans un seul état, mais dans une superposition (un *mélange*) de plusieurs états purs $\psi_1, \dots, \psi_k$, la probabilité d'observer le système dans l'état ψ_i étant donnée par un nombre réel positif λ_i. On a bien évidemment $\lambda_1 + \cdots + \lambda_k = 1$. Appelons ρ cet état superposé. Ce phénomène peut être formalisé à l'aide des opérateurs de densité. Un état pur ψ est identifié à $|\psi\rangle\langle\psi|$, qui est le projecteur orthogonal sur la droite complexe engendrée par ψ. Ainsi, l'état mélangé ρ décrit précédemment s'écrit comme

$$\rho = \sum_{i=1}^{k} \lambda_i |\psi_i\rangle\langle\psi_i| \tag{3.1}$$

L'ensemble des états mélangés sur un espace d'états $\mathcal{H}$, noté $\mathcal{D}(\mathcal{H})$ ou plus simplement $\mathcal{D}$ lorsqu'il n'y a pas d'ambiguïté, est ainsi défini par

$$\mathcal{D}(\mathcal{H}) = \operatorname{conv}\{|\psi\rangle\langle\psi|, \psi \in \mathcal{H}, |\psi| = 1\}$$

Désormais, le mot *état* sous-entendra toujours état mélangé, et les états purs seront toujours identifiés aux états mélangés de rang 1. Les éléments de $\mathcal{D}$ sont des opérateurs autoadjoints, positifs, de trace 1 ; réciproquement ces trois conditions sont suffisantes pour pouvoir écrire une décomposition du type (3.1). On a donc la description alternative

$$\mathcal{D}(\mathcal{H}) = \{\rho \in \mathcal{B}_{sa}(\mathcal{H}), \rho \geqslant 0, \operatorname{tr}\rho = 1\}$$

Remarquons que l'ensemble des points extrémaux de $\mathcal{D}$ coïncide avec l'ensemble des états purs. L'ensemble $\mathcal{D}$ est convexe, l'espace affine qu'il engendre est l'hyperplan des matrices de trace 1, noté $\mathcal{T}_1$. Ainsi, la dimension de $\mathcal{D}(\mathcal{H})$ égale $d^2 - 1$, où d est la dimension complexe de $\mathcal{H}$. Notons également que $|\psi\rangle\langle\psi| = |\phi\rangle\langle\phi|$ si et seulement s'il existe un scalaire α de module 1 tel que $\psi = \alpha\phi$; rappelons que dans ce cas les états ψ et ϕ ne peuvent pas être physiquement différenciés par une observation.

Revenons au cas d'un système formé de plusieurs sous-systèmes, c'est-à-dire d'un espace d'états de la forme $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$. Notons d la dimension de $\mathcal{H}$. Si pour i entre 1 et N, ρ_i est un état sur $\mathcal{H}_i$, alors l'opérateur $\rho_1 \otimes \cdots \otimes \rho_N$ est un état sur $\mathcal{H}$; un tel état est appelé *état produit*. Si un état produit est un état pur, c'est nécessairement un produit d'états purs (car si $\rho_1 \otimes \cdots \otimes \rho_N$ est de rang 1, alors ρ_i est de rang 1 pour tout i).

La notion de séparabilité s'étend naturellement aux états mélangés. Un état est dit *séparable* s'il peut s'écrire comme un mélange d'états produits. Ainsi, l'espace des états séparables est

$$\mathcal{S}(\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N) = \operatorname{conv}\{\rho_1 \otimes \cdots \otimes \rho_N, \rho_i \in \mathcal{D}(\mathcal{H}_i)\}$$

On écrira $\mathcal{S}(\mathcal{H})$ ou $\mathcal{S}$ pour alléger les notations, cette écriture est a priori ambiguë car $\mathcal{S}(\mathcal{H})$ dépend de la décomposition tensorielle de $\mathcal{H}$; cependant le contexte sera toujours clair. Un état sera dit *intriqué* s'il n'est pas séparable. On a l'identification canonique

$$\mathcal{B}_{sa}(\mathcal{H}_1) \otimes \cdots \otimes \mathcal{B}_{sa}(\mathcal{H}_N) \simeq \mathcal{B}_{sa}(\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N)$$

L'espace de gauche se plonge naturellement dans l'espace de droite, et ce plongement est surjectif car on a pris soin de considérer des espaces de Hilbert complexes ; il n'est pas injectif dans le cadre réel. Cette identification permet de voir $\mathcal{S}$ comme un sous-ensemble de $\mathcal{D}$. De plus $\mathcal{S}$ et $\mathcal{D}$ ont la même dimension (encore une fois, ce ne serait pas vrai dans le cadre d'espaces de Hilbert réels). Cela peut par exemple se déduire du résultat général suivant : si $\dot{\otimes}$ désigne le produit tensoriel ponctuel, c'est-à-dire

$$K_1 \dot{\otimes} \cdots \dot{\otimes} K_N = \{x_1 \otimes \cdots \otimes x_N ;\ x_i \in K_i\},$$

on a

$$\mathrm{vect}(K_1 \dot{\otimes} \cdots \dot{\otimes} K_N) = \mathrm{vect}(K_1) \otimes \cdots \otimes \mathrm{vect}(K_N)$$

Si ρ est séparable, il peut s'écrire comme un mélange d'états produits, mais aussi, en écrivant chaque facteur sous la forme (3.1), comme un mélange d'états produits purs. Comme on a l'identité

$$|\psi_1\rangle\langle\psi_1| \otimes \cdots \otimes |\psi_N\rangle\langle\psi_N| = |\psi_1 \otimes \cdots \otimes \psi_N\rangle\langle\psi_1 \otimes \cdots \otimes \psi_N|$$

on en déduit la description alternative de $\mathcal{S}$

$$\mathcal{S}(\mathcal{H}) = \mathrm{conv}\{|\psi\rangle\langle\psi|, \psi \text{ état pur séparable sur } \mathcal{H}\}$$

L'ensemble $\mathcal{D}$ est invariant par conjugaison unitaire :

$$\forall U \in \mathcal{U}(\mathcal{H}), \forall A \in \mathcal{D}(\mathcal{H}), \text{ on a } UAU^\dagger \in \mathcal{D}(\mathcal{H})$$

Restreinte à l'hyperplan $\mathcal{T}_1$, cette action est irréductible. En particulier, le point Id/d, où d est la dimension complexe de $\mathcal{H}$, est le seul point fixé par toutes les isométries de $\mathcal{D}$, c'est donc par exemple le centre de gravité de $\mathcal{D}$. Cet état central est appelé *état mélangé maximal*. L'ensemble $\mathcal{S}$ a moins d'isométries ; si $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$, $\mathcal{S}(\mathcal{H})$ est invariant par conjugaison unitaire locale, c'est-à-dire par conjugaison par des matrices unitaires de la forme $U_1 \otimes \cdots \otimes U_N$, où U_i est un élément de $\mathcal{U}(\mathcal{H}_i)$. Il peut y avoir d'autres isométries de $\mathcal{S}$ (par exemple, si $\mathcal{H} = \mathbf{C}^D \otimes \mathbf{C}^D$, l'opération d'échange $\rho_1 \otimes \rho_2 \longrightarrow \rho_2 \otimes \rho_1$), mais l'action du groupe d'isométries de $\mathcal{S}$ n'est pas irréductible en général. On a néanmoins le résultat suivant :

Lemme 18. *Le seul point fixé par toutes les isométries de $\mathcal{S}$ est l'état mélangé maximal* Id/d*. C'est donc en particulier le centre de gravité de* $\mathcal{S}$*.*

Démonstration. Soit un état ρ fixé par toutes les isométries de $\mathcal{S}$, en particulier par conjugaison par toutes les matrices unitaires locales. On peut décomposer ρ comme

$$\rho = \sum_{j=1}^{k} \lambda_j \rho_1^j \otimes \cdots \otimes \rho_N^j$$

où ρ_i^j est un état sur $\mathcal{H}_i$. Soit U une matrice unitaire locale aléatoire, c'est-à-dire de la forme $U = U_1 \otimes \cdots \otimes U_N$, où U_i est distribuée selon la mesure de Haar sur $\mathcal{U}(\mathcal{H}_i)$. Moyennons ρ sous la conjugaison par U :

$$\begin{aligned}
\mathbf{E}_U U \rho U^\dagger &= \sum_{j=1}^{k} \lambda_j \mathbf{E}_{U_1,\ldots,U_N} (U_1 \rho_1^j U_1^\dagger) \otimes \cdots \otimes (U_N \rho_N^j U_N^\dagger) \\
&= \sum_{j=1}^{k} \lambda_j (\mathbf{E}_{U_1} U_1 \rho_1^j U_1^\dagger) \otimes \cdots \otimes (\mathbf{E}_{U_N} U_N \rho_N^j U_N^\dagger) \\
&= \mathrm{Id}/d
\end{aligned}$$

Pour obtenir la dernière égalité, on a utilisé le fait que $\mathbf{E}_{U_i} U_i A U_i^\dagger = \mathrm{tr}(A)\mathrm{Id}/d_i$ pour toute matrice A de $\mathcal{B}(\mathcal{H}_i)$, où d_i est la dimension de $\mathcal{H}_i$. Cette formule découle de l'observation suivante : comme la mesure de Haar est invariante par translation, l'application $A \to \mathbf{E}_{U_i} U_i A U_i$ est invariante par conjugaison unitaire et donc $\mathbf{E}_{U_i} U_i A U_i$ est toujours un multiple de l'identité. Le coefficient multiplicatif est obtenu en remarquant que la conjugaison unitaire préserve la trace.

□

3.1.2 Estimation de certains paramètres géométriques liés à la séparabilité et à l'intrication

Il est important de savoir lequel des deux phénomènes prévaut : séparabilité ou intrication ? D'un point de vue géométrique, cette question peut prendre plusieurs formes, parmi lesquelles

(a) Calculer la distance géométrique entre $\mathcal{D}$ et $\mathcal{S}$, c'est-à-dire déterminer le plus petit nombre K tel que

$$\mathcal{D} - \mathrm{Id}/d \subset K(\mathcal{S} - \mathrm{Id}/d)$$

Comme $\mathcal{D}$ et $\mathcal{S}$ ont même dimension, un tel nombre K existe nécessairement.

(b) Déterminer le rayon r de la plus grande boule contenue dans $\mathcal{S}$, au sens de la norme Hilbert–Schmidt. Par le lemme 18, une telle boule peut être choisie centrée en l'état mélangé maximal Id/d. Le nombre r est appelé *rayon interne* de $\mathcal{S}$.

(c) Comparer le volume de $\mathcal{S}$ et de $\mathcal{D}$, le volume étant mesuré au sens de la mesure de Lebesgue induite par le produit scalaire de Hilbert–Schmidt.

Ces trois questions ont été posées à plusieurs reprises dans des articles de théorie quantique de l'information, par exemple [HHH2, GB1, GB2, GB3, RMNDMC]. Quelques résultats étaient connus avant nos travaux. Dans le cas d'un système homogène, formé de N particules de dimension D, l'espace d'états est $\mathcal{H} = (\mathbf{C}^D)^{\otimes N}$ et sa dimension est notée $d = D^N$

(a) En ce qui concerne la distance géométrique, on a les estimations suivantes [RMNDMC, GB3]

$$D^{N-1} \leqslant K \leqslant D^{N/2+1}(2D-1)^{N/2-1}$$

Même dans le cas le plus simple, celui des qubits ($D = 2$), la borne supérieure et la borne inférieure ne sont pas du même ordre de grandeur :

$$\frac{1}{2}d \leqslant K_{\text{qubits}} \leqslant \frac{2}{3}6^{N/2} = \frac{2}{3}d^{1.292\ldots}$$

(b) Barnum et Gurvits ont montré dans [GB3] que

$$r \geqslant \frac{1}{D^{N/2+1}(2D-1)^{N/2-1}}$$

Dans le cas des qubits, ils ont également obtenu une légère amélioration :

$$r_{\text{qubits}} \geqslant \tau_N 6^{-N/2} = \tau_N d^{-1.292\ldots}$$

pour une suite (τ_N) explicite vérifiant $1 < \tau_N < \sqrt{3}$ et $\lim_{N\to\infty} \tau_N = \sqrt{3}$.

(c) Essentiellement rien n'était su à propos du volume.

Tout d'abord, nous montrons qu'il est possible de simplifier l'approche de Gurvits et Barnum dans le cas des qubits et de remplacer τ_N par $\sqrt{3}$.

Théorème 3.1. *L'ensemble $\mathcal{S}((\mathbf{C}^2)^{\otimes N})$ contient une boule Hilbert–Schmidt de rayon $\sqrt{3}\,6^{-N/2}$, centrée en l'état mélangé maximal* $\mathrm{Id}/2^n$. *Ce résultat est donc une minoration du rayon interne de $\mathcal{S}$*

$$r_{\text{qubits}} \geqslant \sqrt{3}\,6^{-N/2} = \sqrt{3}\,d^{-1.292\ldots}$$

La preuve du théorème est donnée dans l'appendice 3.3.1. En appliquant des idées de géométrie des convexes, notamment une procédure de symétrisation et l'introduction de la largeur moyenne, qui dans ce cas peut être estimée, nous obtenons également les résultats ci-après, qui prennent tout leur sens lorsque l'on considère des systèmes suffisamment grands. En ce qui concerne le volume, la situation est sensiblement différente selon que l'on considère un système formé d'un petit nombre de gros sous-systèmes, ou d'un grand nombre de petits sous-systèmes. Le fait remarquable est que dans le second cas, il est nécessaire de changer de structure euclidienne pour pouvoir obtenir l'ordre de grandeur du volume. Plus précisément, on a les théorèmes suivants :

Théorème 3.2 (Petit nombre de gros sous-systèmes). *Il existe des constantes universelles $C, c > 0$ telles que, pour tout $D, N \geqslant 2$,*

$$\frac{c^N}{d^{1/2-1/2N}} \leqslant \left(\frac{\mathrm{vol}(\mathcal{S})}{\mathrm{vol}(\mathcal{D})}\right)^{1/n} \leqslant \frac{C(N\log N)^{1/2}}{d^{1/2-1/2N}}$$

Théorème 3.3 (Grand nombre de petits sous-systèmes). *Il existe des constantes universelles $C', c' > 0$ telles que, pour tout $D, N \geqslant 2$,*

$$\frac{c'}{d^{1/2+\alpha_D}} \leqslant \left(\frac{\mathrm{vol}(\mathcal{S})}{\mathrm{vol}(\mathcal{D})}\right)^{1/n} \leqslant \frac{C'(DN\log N)^{1/2}}{d^{1/2+\alpha_D}}$$

où

$$\alpha_D := \frac{1}{2}\log_D(1+\frac{1}{D}) - \frac{1}{2D^2}\log_D(D+1)$$

Le cas des qubits ($D = 2$) a été obtenu par Szarek dans un article antérieur ([Sza]). Nos preuves se trouvent dans la partie suivante. Le théorème 3.3 est celui qui est le plus intéressant du point de vue de l'informatique quantique. Par exemple, dans le cas des qubits cela donne

$$\frac{c'}{d^{0.594\ldots}} \leqslant \left(\frac{\mathrm{vol}(\mathcal{S})}{\mathrm{vol}(\mathcal{D})}\right)^{1/n} \leqslant \frac{C'\sqrt{\log d \log\log d}}{d^{0.594\ldots}} \tag{3.2}$$

La double inégalité ainsi obtenue est précise à l'échelle des puissances de d ; les facteurs logarithmiques parasites étant négligeables (la méthode utilisée rend inévitable l'apparition de tels facteurs). Il est de plus possible d'avoir des estimations raisonnables concernant les différentes constantes impliquées dans ces théorèmes.

Il est possible de déduire directement de la borne supérieure de (3.2) une borne supérieure pour le rayon interne de $\mathcal{S}$. En effet le rayon interne de $\mathcal{S}$ est majoré par la quantité

$$\left(\frac{\mathrm{vol}(\mathcal{S})}{\mathrm{vol}(B_{HS})}\right)^{1/n}$$

appelée *rayon volumique* de $\mathcal{S}$. Le volume de $\mathcal{D}$ est connu (une formule exacte est obtenue dans [ŻS], et il peut aussi être estimé par des moyens plus élémentaires, voir la formule (3.8) dans la partie suivante), et le rayon volumique de $\mathcal{D}$ est de l'ordre de $1/\sqrt{d}$. Cela donne

$$r_{\text{qubits}} \leqslant \frac{C \log d \log\log d}{d^{1.094\ldots}}$$

C'est un résultat intéressant car aucune borne supérieure sur le rayon interne n'était connue auparavant ; cependant la borne obtenue ne coïncide pas avec la borne inférieure du théorème 3.1. Il est en fait possible de démontrer un résultat plus précis :

Théorème 3.4 (Borne supérieure précise sur le rayon interne de $\mathcal{S}$). *Il existe une constante universelle $C_0 > 0$ telle que, pour tout N, l'ensemble $\mathcal{S}((\mathbf{C}^2)^{\otimes N})$, ne contient pas de boule Hilbert–Schmidt de rayon*

$$C_0\sqrt{N\log N}\; 6^{-N/2}.$$

Rappelons que le théorème 3.1 dit exactement que $\mathcal{S}((\mathbf{C}^2)^{\otimes N})$ contient une boule Hilbert–Schmidt de rayon $\sqrt{3}\, 6^{-N/2}$. Le rayon interne de l'ensemble des états séparables est donc connu, à un facteur logarithmique près, dans le cas des qubits. Il est possible d'en déduire directement un résultat analogue pour des qudits ($D > 2$), mais dans ce cas la borne supérieure ne coïncide pas avec la borne inférieure de Gurvits et Barnum ([GB3])

Théorème 3.4'. *Il existe une constante universelle $C_0 > 0$ telle que, pour tout N et pour tout $D \geqslant 2$, l'ensemble $\mathcal{S}((\mathbf{C}^D)^{\otimes N})$ ne contient pas de boule Hilbert–Schmidt de rayon*

$$C_0\sqrt{N\log N}\left(\frac{3}{2}D^2\right)^{-N/2}$$

La preuve de ce corollaire se trouve dans l'appendice 3.3.2.

3.1.3 Faiblesse asymptotique du critère de Peres

Le théorème 3.2 est un résultat global, au sens où il ne permet pas de dire quelque chose sur un état particulier. Or il est important de pouvoir déterminer si un état donné est séparable ou intriqué, et cette question est en général complexe. Dans le cas d'un système bipartite, il existe néanmoins un critère simple, appelé critère de Peres, qui est une condition nécessaire de séparabilité. Fixons un espace d'états $\mathcal{H} = \mathbf{C}^D \otimes \mathbf{C}^D$, ainsi qu'une base de $\mathbf{C}^D$. Si un élément A de $\mathcal{B}_{sa}(\mathcal{H})$ peut s'écrire comme un opérateur produit $A_1 \otimes A_2$, avec $A_i \in \mathcal{B}_{sa}(\mathbf{C}^D)$, on définit la transposition partielle de A (par rapport au premier sous-système) par

$$T(A) = A_1^t \otimes A_2,$$

où $A \to A^t$ est l'opération de transposition dans $\mathcal{B}_{sa}(\mathbf{C}^D)$, pour la base choisie. L'opérateur T, défini uniquement pour les tenseurs purs, peut s'étendre de manière unique en un opérateur linéaire défini sur tout $\mathcal{B}_{sa}(\mathcal{H})$. Si ρ est un état, alors $T\rho$ est un opérateur autoadjoint de trace 1. Si de plus $T\rho$ est positif (c'est-à-dire si $T\rho$ est un état), on dit que ρ est p.p.t. (transposé partiel positif). Remarquons que si $T\rho$ dépend du choix de la base, ce n'est pas le cas de ses valeurs propres, et la notion de p.p.t. est donc intrinsèque. On peut aussi définir la transposition partielle par rapport au deuxième sous-système, mais la notion de p.p.t. obtenue est encore la même. L'observation de Peres est simplement le fait que tout état séparable est p.p.t.. Si l'on note PPT l'ensemble des états p.p.t., on a les inclusions

$$\mathcal{S} \subset \mathrm{PPT} \subset \mathcal{D}$$

On sait, d'après le théorème 3.2, que l'ensemble $\mathcal{S}$ a un volume asymptotiquement beaucoup plus petit que celui de $\mathcal{D}$. Qu'en est-il de l'ensemble PPT ? La réponse est donnée par le théorème suivant :

Théorème 3.5 (Faiblesse asymptotique du critère de Peres). *Il existe une constante universelle $c_0 > 0$ telle que pour tout système bipartite ($\mathcal{H} = \mathbf{C}^D \otimes \mathbf{C}^D$),*

$$c_0 \leqslant \left(\frac{\mathrm{vol}(\mathrm{PPT})}{\mathrm{vol}(\mathcal{D})} \right)^{1/n}$$

Ainsi, lorsque D est suffisamment grand, le volume de PPT est très proche de celui de $\mathcal{D}$, et donc beaucoup plus grand que celui de $\mathcal{S}$. Pour deux gros systèmes, un état p.p.t. typique est en fait intriqué ! Le critère de Peres devient de moins en moins efficace pour détecter la séparabilité lorsque la dimension augmente.

3.2 Tensor product of convex sets and the volume of separable states on N qudits

This note deals with estimating the volume of the set of separable mixed quantum states when the dimension of the state space grows to infinity. This has been studied recently for qubits; here we consider larger particles. We also show that the partial transpose criterion becomes weaker when the dimension increases, and that the lower bound $6^{-N/2}$ on the (Hilbert–Schmidt) inradius of the set of separable states on N qubits obtained recently by Gurvits and Barnum is essentially optimal. We employ standard tools of classical convexity, high-dimensional probability and geometry of Banach spaces. One relatively novel point is a formal introduction of the concept of projective tensor products of convex bodies, and an initial study of this concept.

3.2.1 Introduction and summary of results

An important problem in quantum information theory is to estimate quantitatively some parameters related to *entanglement*. This phenomenon is thought to be at the heart of quantum information processing while, on the other hand, its experimental creation and handling are still challenging. The question of determining the volume of the set of separable states has been asked for example in [ŻHSL, HHH2],where we refer the reader for background and motivation. In this paper we obtain estimates which are meaningful when the dimension of the state space is "not too small," and which are asymptotically tight as that dimension tends to infinity. The effective radius in the sense of volume (that is, the radius of the Euclidean ball of the same volume, also referred to as *volume radius*) of the set of separable states for qubits has been determined (precisely on the scale of powers of the dimension) in [Sza]. Here we apply the same techniques from asymptotic convex geometry to deal with more general particles.

We now recall the mathematical framework and introduce some notation. The state space is a complex Hilbert space $\mathcal{H} = \mathbf{C}^{D_1} \otimes \cdots \otimes \mathbf{C}^{D_N}$. We write $d = D_1 \ldots D_N$ for the dimension of $\mathcal{H}$. This Hilbert space allows to describe quantum interactions between N particles; $D_j = 2$ corresponds to qubits and $D_j = 3$ to qutrits. We write $\mathcal{B}(\mathcal{H})$ for the space (or C^*-algebra) of linear maps from $\mathcal{H}$ into itself, and $\mathcal{B}_{sa}(\mathcal{H})$ for the (real linear) subspace of self-adjoint operators. The space $\mathcal{B}(\mathcal{H})$ is endowed with the Hilbert–Schmidt, or Frobenius, scalar product defined by $\langle A, B\rangle_{HS} := \mathrm{tr} A^\dagger B$ $(= \sum_{i,j=1}^d \overline{A_{ij}} B_{ij}$ if A and B are represented as matrices). A state on $\mathcal{B}(\mathcal{H})$ (which we will abbreviate to "a state on $\mathcal{H}$") can be represented as a positive (semi-definite) trace one element of $\mathcal{B}_{sa}(\mathcal{H})$. A state is said to be *separable* if it can be written as a convex combination of tensor products of N states, otherwise it is called *entangled*. That is, the set of states (also called in this context density operators or density matrices) is

$$\mathcal{D} = \mathcal{D}(\mathcal{H}) := \{\rho \in \mathcal{B}_{sa}(\mathcal{H}), \rho \geqslant 0, \mathrm{tr}\rho = 1\},$$

and the set of separable states is

$$\mathcal{S} = \mathcal{S}(\mathcal{H}) := \mathrm{conv}\{\rho_1 \otimes \cdots \otimes \rho_N, \rho_j \in \mathcal{D}(\mathbf{C}^{D_j})\}.$$

The notation $\mathcal{S}(\mathcal{H})$ is in principle ambiguous: separability of a state on $\mathcal{B}(\mathcal{H})$ is not an intrinsic property of the Hilbert space $\mathcal{H}$ or of the algebra $\mathcal{B}(\mathcal{H})$; it depends on the particular decomposition of $\mathcal{H}$ as a tensor product of (smaller) Hilbert spaces. However, this will not be an issue here since our study focuses on fixed decompositions.

$\mathcal{D}$ and $\mathcal{S}$ are convex subsets of $\mathcal{B}_{sa}(\mathcal{H})$ of (real) dimension $n := d^2-1$. We write $\mathcal{T}_1$ for the affine subspace generated by $\mathcal{D}$ (or $\mathcal{S}$); it is the hyperplane of trace one matrices. The space $\mathcal{B}_{sa}(\mathcal{H})$ inherits a (real) Euclidean structure from the scalar product $\langle\cdot,\cdot\rangle_{HS}$. The corresponding unit ball will be denoted by B_{HS} (or B_{HS}^d). We denote by vol the corresponding d^2-dimensional Lebesgue volume on $\mathcal{B}_{sa}(\mathcal{H})$; we will also write vol for the n-dimensional volume induced on $\mathcal{T}_1$.

We shall concentrate on the special case when all the subsystems are identical, i.e., $D_1 = \cdots = D_N = D$. Our techniques also apply to general state spaces, but formulae which fit all the situations would be more cumbersome than for this "homogeneous" case. If $\mathcal{H} = (\mathbf{C}^D)^{\otimes N}$, there are two "regular" ways to make its dimension tend to infinity: either $N \geqslant 2$ is fixed and D tends to infinity, or $D \geqslant 2$ is fixed and N goes to infinity (as in [Sza] for $D = 2$). Surprisingly, it turns out that in the latter case the natural Euclidean structure is not the one given by the Hilbert–Schmidt scalar product, but rather a mixture of that product with a Killing-type form. Our goal is to prove the following theorems (recall that we work with $\mathcal{H} = (\mathbf{C}^D)^{\otimes N}$ and that $d = \dim\mathcal{H} = D^N$, $N = \log_D d$ and $n = \dim\mathcal{D} = d^2-1 = D^{2N}-1$).

Theorem 3.2 (Small number of large subsystems). *There exist universal constants $C, c > 0$ such that, for all $D, N \geqslant 2$,*

$$\frac{c^N}{d^{1/2-1/2N}} \leqslant \left(\frac{\mathrm{vol}(\mathcal{S})}{\mathrm{vol}(\mathcal{D})}\right)^{1/n} \leqslant \frac{C(N\log N)^{1/2}}{d^{1/2-1/2N}}$$

We point out that considering the nth root of the ratio of volumes is natural from the geometric point of view: if the two sets had been Euclidean balls, we would have obtained the ratio of their radii, and so we are comparing the volume radii of $\mathcal{S}$ and $\mathcal{D}$ (see section 3.2.2 for additional geometric background).

Theorem 3.3 (Large number of small subsystems). *There exist universal constants $C', c' > 0$ such that, for all $D, N \geqslant 2$,*

$$\frac{c'}{d^{1/2+\alpha_D}} \leqslant \left(\frac{\mathrm{vol}(\mathcal{S})}{\mathrm{vol}(\mathcal{D})}\right)^{1/n} \leqslant \frac{C'(DN\log N)^{1/2}}{d^{1/2+\alpha_D}}$$

where

$$\alpha_D := \frac{1}{2}\log_D(1+\frac{1}{D}) - \frac{1}{2D^2}\log_D(D+1)$$

For illustration, we list approximate values of α_D for small D's: $\alpha_2 \approx 0.09436, \alpha_3 \approx 0.06083, \alpha_4 \approx 0.04420$. Note that α_D is a positive decreasing function of D, asymptotically equivalent to $1/(2D\log D)$.

Theorem 3.2 asserts that, as $D \to \infty$, the *ratio of the volume radii* of $\mathcal{S}$ and $\mathcal{D}$ is of order $d^{-(1/2-1/2N)} = D^{-(N-1)/2}$ (up to a multiplicative constant depending only on N). Theorem 3.3 is slightly less definite: while, for fixed D, the ratio in question is determined precisely on the scale of the powers of d, there are some (possibly parasitic) logarithmic factors. [We recall again that $N = \log_D d = \log d/\log D$.] We point out that, apart from the value of the numerical constant, the upper estimate in Theorem 3.3 is always sharper than that in Theorem 3.2. However, the gain α_D in the exponent is negligible if N is fixed and $D \to \infty$.

It is possible to give reasonable estimates on the constants appearing in both theorems. One can, for example, take $c = 1/\sqrt{6}$, $c' = 0.3$ and $C = C' = 6$. It is also possible to establish a tighter asymptotic behavior of these constants (relevant if one is only interested in large values of d): one can have C and C' tending to $\sqrt{2}\,e^{1/4}$ and c' tending to $e^{3/4}/\sqrt{2\pi}$ as D or N tend to infinity. Finally, sharper estimates for specific dimensions can be obtained by using known results on, among others, efficient spherical codes; see Appendix G of [Sza] for an example of such calculation.

The case $D = 2$ of Theorem 3.3 was treated in detail in [Sza]. In this note we present additional ingredients required to deal with the general case. We point out that the (relatively) easy part is the estimation of $\mathrm{vol}(\mathcal{D})$, which of course does not depend on the tensor structure of $\mathcal{H}$. It has been shown in [ŻS] that

$$\mathrm{vol}(\mathcal{D}) = \sqrt{d}\,(2\pi)^{d(d-1)/2}\frac{\Gamma(1)\dots\Gamma(d)}{\Gamma(d^2)} \tag{3.3}$$

A direct calculation then yields that the volume radius of $\mathcal{D}$ behaves as $e^{-1/4}d^{-1/2}(1+O(1/d))$ as $d \to \infty$. It is also possible (and easy) to estimate the volume radius of $\mathcal{D}$ using techniques with the same flavor as the ones presented here. For example, it was shown in [Sza] that for any value of d that radius is contained between $d^{-1/2}/2$ and $2d^{-1/2}$ (see section 3.2.2 below). Finally, the fact that the volume radius in question is of order $d^{-1/2}$ as $d \to \infty$ follows from an early paper [ST].

The ratio of Euclidean volumes is not the only geometric parameter which is of interest here. An arguably more relevant parameter would be its analogue for the so-called *Bures volume*, which may be a more appropriate measure of size in the present context (see [BC]). Another quantity with physical significance is the largest number $\varepsilon = \varepsilon(\mathcal{H})$ below which the mixture $(1-\varepsilon)\mathrm{Id}/d + \varepsilon\rho$ is separable for any state ρ. Of course it is possible to derive from volume estimates an upper bound on this $\varepsilon(\mathcal{H})$, but this bound is weaker that what is already known ([RMNDMC, GB2, GB3]). Still, the knowledge of the volume radii yields additional information also in this context: for $\varepsilon \gg (\mathrm{vol}(\mathcal{S})/\mathrm{vol}(\mathcal{D}))^{1/\dim\mathcal{D}}$, the mixture $(1-\varepsilon)\mathrm{Id}/d+\varepsilon\rho$ is entangled for "most of" $\rho \in \mathcal{D}$, and not just for very special states as those constructed in [RMNDMC, GB2, GB3]. Another quantity that has been studied in [GB1, GB2, GB3] is the inradius of $\mathcal{S}$, which is the radius of the inscribed Euclidean ball in $\mathcal{S}$ (here we assume that the balls are centered at Id/d, which is the natural center of both $\mathcal{S}$ and $\mathcal{D}$). It seems that, prior to results on qubits in [Sza], the only upper bound which was known on the inradius of $\mathcal{S}$ was the inradius of $\mathcal{D}$, or $1/\sqrt{d(d-1)}$. [A remarkable fact discovered in [GB1] is that the two inradii coincide when $N=2$.] Theorem 3.3 improves on this for large N giving, up to logarithmic factors, the upper bound $1/d^{1+\alpha_D}$. Moreover, the techniques developed in [Sza] and in the present paper allow to tighten this bound substantially. We present the following sample result.

Theorem 3.4 (Tight upper bounds on the inradii of $\mathcal{S}$ and Σ). *There exists an absolute constant $C_0 > 0$ such that, for any N, the set $\Sigma((\mathbf{C}^2)^{\otimes N})$, and hence also $\mathcal{S}((\mathbf{C}^2)^{\otimes N})$, does not contain any Hilbert–Schmidt ball of radius $C_0\sqrt{N\log N}\, 6^{-N/2}$.*

For comparison, let us cite the lower bound of $6^{-N/2}$ on the inradius of the set Σ noted in [Sza], Appendix H, and a similar lower bound on the *a priori* smaller inradius of $\mathcal{S}$ shown subsequently in [GB3]. This means that, at least for N qubits, the inradii of $\mathcal{S}$ and of Σ have been determined up to a multiplicative factor which is logarithmic in the dimension of the state space. The argument we present can be generalized to other values of D, leading to an upper bound for the inradii of $\Sigma((\mathbf{C}^D)^{\otimes N})$ and $\mathcal{S}((\mathbf{C}^D)^{\otimes N})$ which is $(D(D+1))^{-N/2}$ (again, up to a logarithmic factor). For the inradius of the set Σ this bound is essentially sharp. However, for $D > 2$, the value $(D(D+1))^{-N/2}$ does not coincide with the lower bound for the inradius of $\mathcal{S}((\mathbf{C}^2)^{\otimes N})$ that was found in [GB3] and which is of the form $O((D(2D-1))^{-N/2})$. As was noticed in [GB3], a better upper bound for $D > 2$ is derived from our upper bound for $D = 2$ and is (up to a logarithmic factor) of the form $(1.5 \times D^2)^{-N/2}$. However, this still leaves a gap between the upper and lower estimates which is exponential in N (as $N \to \infty$). A similar discussion of the bilateral case ($N = 2, D \to \infty$) can be found in the Remark at the end of section 3.2.3.

Theorem 3.2 above means that *typical* (as measured by the standard volume) high-dimensional bipartite states are entangled. This statement is of global nature, and is therefore not helpful when one faces a given state and has to decide about its separability. In turn, *lower* bounds for the inradii of sets Σ, or for the quantity $\varepsilon(\mathcal{H})$ mentioned above provide a *sufficient* condition for separability which, while very useful in some contexts, is conclusive for only a very small fraction of separable states. A very simple and efficient (at least in small dimensions) *necessary* condition is the so-called *Peres partial transpose criterion* ([Per]). We briefly recall what partial transposition is, say when the state space is $\mathcal{H} = \mathbf{C}^D \otimes \mathbf{C}^D$. Fix a basis $(e_1, \dots, e_D)$ of $\mathbf{C}^D$, for example the canonical basis. Any state ρ on $\mathcal{H}$ can be uniquely expressed as

$$\rho = \sum_{i,j,\alpha,\beta=1}^{D} \rho_{i\alpha,j\beta} |e_i \otimes e_\alpha\rangle\langle e_j \otimes e_\beta|$$

We then consider $T\rho$, the partial transpose of ρ (with respect to the first subsystem), defined by the formula

$$(T\rho)_{i\alpha,j\beta} = \rho_{j\alpha,i\beta}$$

One checks that $T\rho$ is also an Hermitian operator of trace one which, however, is not necessarily positive. Following [HHH2], we write PPT (Positive Partial Transpose) for the set of states ρ for which $T\rho$ is also positive. Note that while $T\rho$ depends on the choice of the basis, its eigenvalues do not; so the set PPT is basis-independent. The Peres criterion simply reads: *any separable state has a positive partial transpose.* In other words, we have the inclusions $\mathcal{S} \subset \text{PPT} \subset \mathcal{D}$. An natural question (asked for example in [HHH2]) is then: what is the volume of PPT? Is it close to the volume of $\mathcal{S}$, or rather to the volume of $\mathcal{D}$? The following theorem answers the latter question.

Theorem 3.5 (Asymptotic weakness of PPT criterion). *There exists an absolute constant* $c_0 > 0$ *such that for any bipartite system* ($\mathcal{H} = \mathbf{C}^D \otimes \mathbf{C}^D$)

$$c_0 \leqslant \left(\frac{\mathrm{vol}(\mathrm{PPT})}{\mathrm{vol}(\mathcal{D})} \right)^{1/n}$$

An immediate corollary to Theorems 3.2 and 3.5 is that, for large D, the volume of PPT states is much bigger than the volume of separable states. This means that a typical high-dimensional PPT state is entangled, and thus that Peres criterion becomes weaker and weaker as the dimension increases. Theorem 3.5 is just a sample result; similar analysis may be performed for other bipartite and multipartite systems. On the other hand, it is quite conceivable that the quantity from Theorem 3.5 admits a nontrivial (i.e., < 1, independent of D) upper bound, even in the case of bipartite systems.

3.2.2 Preliminaries about convex bodies

In this section we list some known (or elementary) facts from convexity theory that will be needed in the sequel. A *convex body* is a convex compact subset of $\mathbf{R}^n$ (or of $\mathbf{C}^m$ identified with $\mathbf{R}^{2m}$, or of an *affine* subspace of $\mathbf{R}^n$) with nonempty interior. We will say that a convex body K is *symmetric* if it is symmetric with respect to the origin (i.e., $K = -K$). To a convex body $K \subset \mathbf{R}^n$ containing the origin in its interior one can canonically associate $\|\cdot\|_K$, the *gauge of* K, by setting, for $x \in \mathbf{R}^n$, $\|x\|_K := \inf\{\lambda \ : \ x \in \lambda K\}$. If K is symmetric, $\|\cdot\|_K$ is the norm for which K is the unit ball. If K and L are two convex bodies in $\mathbf{R}^n$ which contain the origin in their interior, we define the *geometric distance* between K and L as the product $\alpha\beta$, where α (resp. β) is the smallest number for which $K \subset \alpha L$ (resp. $L \subset \beta K$). This quantifies how the shapes of K and L differ.

The Urysohn inequality

Let $K \subset \mathbf{R}^n$ be a convex body and $u \in S^{n-1}$ be a unit vector. The *width of* K in the direction u is

$$w(K, u) := \max_{x \in K} \langle u, x \rangle$$

Geometrically, $w(K, u)$ is the distance from the origin to the hyperplane tangent to K in the direction u. The *mean width of* K is simply the mean of the widths in all directions:

$$w(K) := \int_{S^{n-1}} w(K, u) d\sigma(u)$$

where σ is the Lebesgue measure on the sphere, normalized so that $\sigma(S^{n-1}) = 1$. The classical *Urysohn inequality*, which is of isoperimetric flavor, states that among all convex bodies of given volume, the Euclidean ball has the minimal mean width. It can be written as follows (see, e.g., Appendix A of [Sza] for a proof)

$$\left(\frac{\mathrm{vol}(K)}{\mathrm{vol}(B_n^2)}\right)^{\frac{1}{n}} \leqslant w(K),$$

where B_2^n is the n-dimensional Euclidean unit ball. The quantity on the left-hand side equals the radius of the Euclidean ball which has the same volume as K and, as we mentioned earlier, is sometimes called the *volume radius* of K; we will denote it $\mathrm{vrad}(K)$. We will use the Urysohn inequality to estimate, among others, the volume radius of Σ, which is the quantity we are interested in. It is often more convenient to rewrite the inequality above by expressing the mean width via a Gaussian integral (rather than an integral over the sphere):

$$\mathrm{vrad}(K) \leqslant \frac{1}{\gamma_n}\mathbf{E}\max_{x\in K}\langle x, G\rangle,$$

where G is a $\mathcal{N}(0, \mathrm{Id}_n)$ Gaussian vector, $\mathbf{E}$ is the expectation with respect to G and $\gamma_n := \sqrt{2}\Gamma(\frac{n+1}{2})/\Gamma(\frac{n}{2})$ is a constant which is close to $\sqrt{n}$. The identity $w(K) = \gamma_n^{-1}\mathbf{E}\max_{x\in K}\langle x, G\rangle$ is checked by passing to polar coordinates. We will occasionally call $\mathbf{E}\max_{x\in K}\langle x, G\rangle$ the *Gaussian mean width* of K and denote it $w_G(K)$.

A special situation is when the body K is a polytope with v vertices on the unit sphere. In this case it is well-known (see Proposition 1.1.3. in [Tal] for a nice proof) that the expectation $w_G(K)$ is smaller than $\sqrt{2\log v}$. A somewhat more complicated argument based on another proof ([Fer], Lemme 0.6.2) and supplemented by numerics shows that the same estimate works for a *symmetric* polytope with $2v$ vertices on the unit sphere (or just in the unit ball) provided $v > 1$ (see Appendix 3.3.3). We eventually obtain that, for $v > 1$ points $(x_i)_{i=1}^v$ in the unit ball,

$$\mathrm{vrad}(\mathrm{conv}\{\pm x_i\}_{i=1}^v) \leqslant w(\mathrm{conv}\{\pm x_i\}_{i=1}^v) < \frac{1}{\gamma_n}\sqrt{2\log v}. \tag{3.4}$$

Note that since $\gamma_n = w_G(B_2^n) \sim \sqrt{n}$, the quantity on the right will be small as long as $\log v \ll n$.

Symmetrization and the Rogers–Shephard inequality

Let H be an affine hyperplane in $\mathbf{R}^{n+1}$, not containing the origin, and let W be a convex body in H. Consider the symmetrization Ω of W, defined by $\Omega := \mathrm{conv}(W \cup -W)$. This procedure is quite natural in the framework of convex bodies, since much more information is available about centrally symmetric convex bodies as opposed to general ones. In particular, Ω is the unit ball with respect to the norm $\|.\|_\Omega$. If $h > 0$ is the distance between H and the origin, then we have the following inequalities

$$2h\,\mathrm{vol}(W) \leqslant \mathrm{vol}(\Omega) \leqslant 2h\,\frac{2^n}{n+1}\mathrm{vol}(W). \tag{3.5}$$

The left hand inequality is an immediate consequence of the *Brunn–Minkowski inequality* ([Gar]), and is an equality if the body W is centrally symmetric. The right hand inequality is the *Rogers–Shephard inequality* ([RS]) and equality is achieved when W is a simplex. The factor $\frac{2^n}{n+1}$ may appear large, but we point out that its nth root, which is more relevant here, is smaller than 2.

We now consider symmetric versions of $\mathcal{D}$ and $\mathcal{S}$, namely $\Delta := \mathrm{conv}(\mathcal{D} \cup -\mathcal{D})$ and $\Sigma := \mathrm{conv}(\mathcal{S} \cup -\mathcal{S})$; then $n = d^2 - 1$. The set Δ is just the Hermitian part of the unit ball of the usual Schatten class of trace class operators. In other words $\Delta = \{A \in \mathcal{B}_{sa}(\mathcal{H}), \|A\|_1 \leqslant 1\}$, where $\|A\|_1$ is the *trace class norm*, i.e., the sum of singular values of A or, in our Hermitian setting, of the absolute values of the eigenvalues of A. [See section 3.2.2 for the functional-analytic interpretation of Σ.] The inequalities (3.5) imply now

$$\frac{1}{2}\left(\frac{\mathrm{vol}(\Sigma)}{\mathrm{vol}(\Delta)}\right)^{1/n} \leqslant \left(\frac{\mathrm{vol}(\mathcal{S})}{\mathrm{vol}(\mathcal{D})}\right)^{1/n} \leqslant 2\left(\frac{\mathrm{vol}(\Sigma)}{\mathrm{vol}(\Delta)}\right)^{1/n} \tag{3.6}$$

Therefore, we lose only a factor of 2 when passing from the ratio of the volume radii of $\mathcal{S}$ and $\mathcal{D}$ to the ratio of the volume radii of Σ and Δ. To be precise, the exponent obtained for the symmetrized bodies is $1/n$ whereas it should be $1/d^2$ (which is the reciprocal of the dimension of Δ and Σ), but this is not at all an issue. First, we can *a posteriori* change the exponent, this will at most slightly affect the constants. Second, the extra $n+1$ in (3.5) ensures that no modification of the constants is actually needed (see [Sza], Appendix C, for a precise general statement in this direction).

For future reference we recall here the estimates from [Sza] for the volume radius of $\mathcal{D}$ (cited in the Introduction), for the volume radius of Δ, and for the mean widths of these sets.

$$\frac{1}{\sqrt{d}} \leqslant \mathrm{vrad}(\Delta) = \left(\frac{\mathrm{vol}(\Delta)}{\mathrm{vol}(B_2^{d^2})}\right)^{1/d^2} \leqslant w(\Delta) \leqslant \frac{2}{\sqrt{d}} \tag{3.7}$$

$$\frac{1}{2\sqrt{d}} \leqslant \mathrm{vrad}(\mathcal{D}) \leqslant w(\mathcal{D}) \leqslant \frac{2}{\sqrt{d}} \tag{3.8}$$

While, as we mentioned in the Introduction, both a closed expression for $\mathrm{vrad}(\mathcal{D})$ and its precise asymptotic behavior (as the dimension increases) are known, and while presumably similar information about $\mathrm{vrad}(\Delta)$ may be obtained via the methods of [ŻS], the compact and transparent inequalities from (3.7) and (3.8) are sufficient for our asymptotic results. Moreover, having upper bounds for the *larger* parameter $w(\cdot)$ will provide us with additional flexibility.

Ellipsoids associated to convex bodies

An ellipsoid is an affine image of the unit ball B_2^n. There is a one-to-one correspondence between symmetric ellipsoids and scalar products (or Euclidean structures). Indeed, if $\mathcal{E} = TB_2^n$, with T a linear map, then $\mathcal{E}$ is the unit ball associated to the scalar product $\langle x, y\rangle_{\mathcal{E}} := \langle T^{-1}x, T^{-1}y\rangle$. If K is a convex body in $\mathbf{R}^n$, its *polar body*, denoted K°, is defined by $K^\circ = \{x \in \mathbf{R}^n, \forall y \in K, \langle x, y\rangle \leqslant 1\}$. If 0 belongs to the interior of K, K° is also a convex body (if not, it fails to be bounded). We point out that $\|x\|_{K^\circ} = \max_{y\in K}\langle x, y\rangle$ and that the restriction of the gauge $\|\cdot\|_{K^\circ}$ to the sphere coincides with $w(K, \cdot)$, the width function of K defined in section 3.2.2. We further note that the polar of a symmetric ellipsoid is again a symmetric ellipsoid. The following definition is useful for our purposes.

Definition: If K is a convex body in $\mathbf{R}^n$, a *John resolution of identity* associated to K is a finite family $(x_i, c_i)_{i\in I}$, where x_i belong to $\partial K \cap S^{n-1}$ (if $K \subset B_2^n$ or $B_2^n \subset K$, these are contact points of K with the sphere) and c_i are positive numbers, such that

1. $\sum c_i x_i = 0$
2. $\forall y \in \mathbf{R}^n, y = \sum c_i \langle x_i, y\rangle x_i$

Condition 2 can be rephrased using Dirac notation as $\sum c_i |x_i\rangle\langle x_i| = \mathrm{Id}_n$. Taking trace both sides, we see that necessarily $\sum c_i = n$. We recall the following result due to John

Proposition 3.1 (John's theorem). *Let K be a convex body in $\mathbf{R}^n$. Then there exists a unique ellipsoid of minimal volume containing K, called Löwner ellipsoid, which we denote* $\mathrm{L\ddot{o}w}(K)$*. Similarly, there exists a unique ellipsoid of maximal volume contained in K, called John ellipsoid, which we denote* $\mathrm{John}(K)$*. Moreover, the equality* $\mathrm{L\ddot{o}w}(K) = B_2^n$ *holds if and only if $K \subset B_2^n$ and there exists a John resolution of identity associated to K. Similarly, the equality* $\mathrm{John}(K) = B_2^n$ *holds if and only if $B_2^n \subset K$ and there exists a John resolution of identity associated to K.*

For a proof of this theorem, see [Bal]. These ellipsoids are affine invariants: for any affine map T, we have $\text{John}(TK) = T\text{John}(K)$ and $\text{Löw}(TK) = T\text{Löw}(K)$. In the symmetric case (the one we mostly deal with in the sequel), John and Löwner ellipsoids are also symmetric and dual to each other with respect to polarity. More precisely, if K is symmetric, we have $\text{John}(K^\circ) = \text{Löw}(K)^\circ$ and $\text{Löw}(K^\circ) = \text{John}(K)^\circ$; this is a consequence of the fact that for any symmetric ellipsoid $\mathcal{E}$, we have $\text{vol}(\mathcal{E}^\circ) = \text{vol}(B_2^n)^2/\text{vol}(\mathcal{E})$. It is therefore immediate to pass from the statement about John ellipsoid to the statement about Löwner ellipsoid (actually the theorem is usually stated for the John ellipsoid only).

Tensor products of convex bodies

If K and K' are convex bodies, respectively in $\mathbf{R}^n$ and $\mathbf{R}^{n'}$, their *projective tensor product* is the convex body $K \hat{\otimes} K'$ in $\mathbf{R}^n \otimes \mathbf{R}^{n'} \sim \mathbf{R}^{nn'}$ defined as follows

$$K \hat{\otimes} K' = \text{conv}\{x \otimes x', x \in K, x' \in K'\}.$$

This terminology is motivated by the fact that when K and K' are unit balls with respect to some norms, the set $K \hat{\otimes} K'$ is the unit ball of the corresponding projective tensor product norm on $\mathbf{R}^n \otimes \mathbf{R}^{n'}$. The relevance of the notion to our discussion is obvious: the set of separable states is the projective tensor product of sets of states on factor spaces; more precisely, if $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, then $\mathcal{S}(\mathcal{H}) = \mathcal{D}(\mathcal{H}_1) \hat{\otimes} \mathcal{D}(\mathcal{H}_2)$. It is easy to see that the operation $\hat{\otimes}$ commutes with symmetrizations: if $\tilde{K} = \text{conv}(K \cup -K)$ and $\tilde{K}' = \text{conv}(K' \cup -K')$, then $\text{conv}(K \hat{\otimes} K', -K \hat{\otimes} K') = \tilde{K} \hat{\otimes} \tilde{K}'$. It follows that, in our notation, $\Sigma(\mathcal{H}) = \Delta(\mathcal{H}_1) \hat{\otimes} \Delta(\mathcal{H}_2)$. Since, as was pointed out in section 3.2.2, Δ is the unit ball in the trace class norm, $\Sigma(\mathcal{H})$ is the unit ball of the projective tensor product of the spaces $\mathcal{B}_{sa}(\mathcal{H}_k)$, $k = 1, 2$, each endowed with the trace class norm.

The definition of $K \hat{\otimes} K'$ — similarly as other definitions, comments and lemmas of this section — immediately generalizes to tensor products of any finite number of factors. However, for the sake of transparency, we shall concentrate in this section on the case of two bodies. We also point out that while the definition appears to be well-adapted to 0-symmetric sets, cones and linear maps as morphisms (this is used in the proof of Lemma 19 below and, later, in the first paragraph of section 5), the projective tensor product *is not* invariant under affine maps. We refer to [Sve], Chapter 2, for a discussion of related categorical issues.

If $\mathcal{E} = SB_2^n$ and $\mathcal{E}' = S'B_2^{n'}$ are two ellipsoids, respectively in $\mathbf{R}^n$ and $\mathbf{R}^{n'}$, their Hilbertian tensor product is the ellipsoid $\mathcal{E} \otimes_2 \mathcal{E}' := (S \otimes S')B_2^{nn'}$.

This definition does not depend on the choice of S and S'. It turns out that Löwner ellipsoids behave well with respect to projective tensor product, as the following lemma shows (note that the analogous statement *does not* hold for the John ellipsoid).

Lemma 19. *Let $K \subset \mathbf{R}^n$ and $K' \subset \mathbf{R}^{n'}$ be two convex bodies. Then the Löwner ellipsoid of their projective tensor product is the Hilbertian tensor product of the respective Löwner ellipsoids.*

In terms of scalar products, for every x, y in $\mathbf{R}^n$ and x', y' in $\mathbf{R}^{n'}$, we have

$$\langle x \otimes x', y \otimes y' \rangle_{\text{Löw}(K\hat{\otimes}K')} = \langle x, y \rangle_{\text{Löw}(K)} \langle x', y' \rangle_{\text{Löw}(K')}$$

Proof. First suppose that $\text{Löw}(K) = B_2^n$ and $\text{Löw}(K') = B_2^{n'}$. By John's theorem, there exist John resolutions of identity for K and K', respectively $(x_i, c_i)_{1 \leqslant i \leqslant k}$ and $(x'_j, c'_j)_{1 \leqslant j \leqslant k'}$. We easily check that $K \hat{\otimes} K' \subset B_2^{nn'} = B_2^n \otimes_2 B_2^{n'}$. Moreover, $(x_i \otimes x'_j, c_i c'_j)_{1 \leqslant i \leqslant k, 1 \leqslant j \leqslant k'}$ is also a John resolution of identity for $K \hat{\otimes} K'$. It is enough to check this on pure tensors: take $y \in \mathbf{R}^n$ and $y' \in \mathbf{R}^{n'}$ and verify the two conditions

1. $\sum_{i=1}^k \sum_{j=1}^{k'} c_i c'_j x_i \otimes x'_j = (\sum_{i=1}^k c_i x_i) \otimes (\sum_{j=1}^{k'} c'_j x'_j) = 0$
2. $\sum_{i=1}^k \sum_{j=1}^{k'} c_i c'_j \langle x_i \otimes x'_j, y \otimes y' \rangle x_i \otimes x'_j =$
   $(\sum_{i=1}^k c_i \langle x_i, y \rangle x_i) \otimes (\sum_{j=1}^{k'} c'_j \langle x'_j, y' \rangle x'_j) = y \otimes y'$

For the general case, let T and T' be linear maps such that $T\text{Löw}(K) = B_2^n$ and $T'\text{Löw}(K') = B_2^{n'}$. Using the elementary identities $\text{Löw}(TK) = T\text{Löw}(K)$ and $(T \otimes T')(K \hat{\otimes} K') = (TK) \hat{\otimes} (T'K')$, the result follows from the previous particular case. $\square$

The next "Chevet–Gordon type" lemma relates the mean widths of convex sets to that of their projective tensor product. It is most conveniently stated for the mean *Gaussian* width $w_G(\cdot)$ defined in section 3.2.2.

Lemma 20. *Let $K \subset B_2^n \subset \mathbf{R}^n$ and $K' \subset B_2^{n'} \subset \mathbf{R}^{n'}$ be convex bodies, one of which is the convex hull of a subset of the corresponding unit sphere. Then*

$$w_G(K \hat{\otimes} K') \leqslant w_G(K) + w_G(K').$$

Restating the assertion of the Lemma in terms of the standard mean width gives

$$w(K \hat{\otimes} K') \leqslant \frac{\gamma_n}{\gamma_{nn'}} w(K) + \frac{\gamma_{n'}}{\gamma_{nn'}} w(K') \leqslant \frac{w(K)}{\sqrt{n'}} + \frac{w(K')}{\sqrt{n}},$$

The second inequality follows from the fact that the sequence $(\gamma_k/\sqrt{k})$ is increasing (which can be deduced from inequalities proved in [Luk]; the fact that the coefficients on the right hand side are *approximately* $1/\sqrt{n'}$ and $1/\sqrt{n}$ follows from the simpler relationship $\gamma_k \approx \sqrt{k}$.) We thus get seemingly strong upper bounds for mean widths and, *a fortiori*, for volume radii of projective tensor products of convex bodies. However, in spite of its elegance, Lemma 20 will play only rather limited role in our arguments. This is because, when iterated, it yields asymptotically worse dependence on the number of factors than the techniques employed in subsequent sections. Accordingly, its main use will be in considerations involving few factors and in ameliorating the numerical constants which appear in the statements of the Theorems. The Lemma can be shown by an argument very similar to that of section 2c of [DS], we postpone the proof to appendix 3.3.4.

Finally, let us note that if K and K' are circled convex bodies in respective complex vector spaces (a convex body $K \subset \mathbf{C}^n$ is said to be circled if $K = e^{i\theta}K$ for all real θ), then $K\hat{\otimes}K'$ is circled; as was the case for symmetrizations, the operation absconv (the absolute convex hull) commutes with the projective tensor product.

3.2.3 Proof of Theorem 3.2: Small number of large subsystems

The upper bound can be obtained through a standard discretization argument. Recall that, for $\delta > 0$, a δ-net of a set K is a subset $\mathcal{N} \subset K$ such that for each $x \in K$ there exists $y \in \mathcal{N}$ whose distance to x is smaller than δ. If $\mathcal{N} \subset \mathbf{C}^D$, we write $P(\mathcal{N})$ for the polytope $\text{conv}\{\pm|x\rangle\langle x|\}_{x\in\mathcal{N}} \subset \mathcal{B}_{sa}(\mathbf{C}^D)$. The following elementary lemma shows that if $\mathcal{N}$ is a net of the unit sphere of $\mathbf{C}^D$ — which may be identified with S^{2D-1} as a metric space — then $P(\mathcal{N})$ is a good approximation of $\Delta(\mathbf{C}^D)$.

Lemma 21. *Let $\delta < \sqrt{2-\sqrt{2}} \approx 0.765$ and let $\mathcal{N}$ be a δ-net of the unit sphere of $\mathbf{C}^D$. Then*

$$(1 - 2\delta^2 + \delta^4/2)\Delta(\mathbf{C}^D) \subset P(\mathcal{N}) \subset \Delta(\mathbf{C}^D)$$

Proof. The second inclusion is trivial. Let us check the first one through the corresponding dual (polar) norms

$$\|A\|_{P(\mathcal{N})^\circ} = \max_{y\in\mathcal{N}} |\langle y|A|y\rangle|$$

$$\|A\|_{\Delta(\mathbf{C}^D)^\circ} = \|A\|_{op} = \max_{x\in\mathbf{C}^D, \|x\|=1} |\langle x|A|x\rangle| = \max_{\lambda\in\sigma(A)} |\lambda|,$$

where $\|\cdot\|_{op}$ is the operator norm and $\sigma(\cdot)$ is the spectrum (recall that we consider only Hermitian matrices here). We need to show that $\|A\|_{P(\mathcal{N})^\circ} \geq (1-2\delta^2+\delta^4/2)\|A\|_{op}$. To this end, let $A \in \mathcal{B}_{sa}(\mathbf{C}^D)$ be such that $\|A\|_{op}$ and the largest eigenvalue of A are both equal to 1, and let $x \in \mathbf{C}^D$ be a norm one vector such that $Ax = x$. Choose $y_0 \in \mathcal{N}$ verifying $\|x - y_0\| \leqslant \delta$. We claim that $\langle y_0|A|y_0\rangle \geq 1 - 2\delta^2 + \delta^4/2$; the inequality between the norms follows then by homogeneity. The claim is easily established by writing $y_0 = y_1 + y_2$ with $y_1 = \langle y_0|x\rangle x$ and noting that $\langle y_1|A|y_1\rangle \geq |\langle y_0|x\rangle|^2 \geq (1-\delta^2/2)^2$, $|\langle y_2|A|y_2\rangle| \leq \|y_2\|^2 \leq \delta^2(1-\delta^2/4)$ and $\langle y_1|A|y_2\rangle = 0$. □

Tensoring the conclusion of the preceding lemma and recalling that $\Delta(\mathbf{C}^D)^{\hat{\otimes} N} = \Sigma(\mathcal{H})$ yields an inclusion $(1-2\delta^2+\delta^4/2)^N \Sigma(\mathcal{H}) \subset P(\mathcal{N})^{\hat{\otimes} N}$. Observe that $P(\mathcal{N})^{\hat{\otimes} N}$ is another symmetric polytope with at most $2(\#\mathcal{N})^N$ vertices. It is well-known (lemma 2) that for $\delta \leqslant 1$ we can find δ-nets in S^{2D-1} of cardinality not exceeding $\leqslant (1+2/\delta)^{2D}$. We thus get a bound on the volume of the polytope using the estimation (3.4).

We note for future reference that the above discussion can be carried out using other Euclidean structures, the only constraint being that the vertices of the polytope are of norm not exceeding 1. Thus, if $\mathcal{E}$ is any ellipsoid containing $\Sigma(\mathcal{H})$, we obtain

$$\left(\frac{\mathrm{vol}(\Sigma(\mathcal{H}))}{\mathrm{vol}(\mathcal{E})}\right)^{1/d^2} \leqslant \inf_{0<\delta<\sqrt{2-\sqrt{2}}} \frac{\sqrt{2\log\left((1+2/\delta)^{2DN}\right)}}{\gamma_{d^2}(1-2\delta^2+\delta^4/2)^N} \tag{3.9}$$

Using $\mathcal{E} = B_{HS}$ and, say, $\delta = 1/\sqrt{N\log 2N}$ leads to an estimate

$$\mathrm{vrad}(\Sigma(\mathcal{H})) = O((DN\log N)^{1/2}/d)$$

[Indeed, for large d we have then $\gamma_{d^2} \sim d$, $(1-2\delta^2+\delta^4/2)^N \sim 1$ and $\log\left((1+2/\delta)^{2DN}\right) \sim DN\log N$.] We obtain the upper bound announced in Theorem 3.2 by combining this with the *lower* bound on $\mathrm{vrad}(\Delta(\mathcal{H}))$ given by (3.7) and with (3.6).

The lower estimate will be proved by showing that $\Sigma(\mathcal{H})$ contains a Euclidean ball of appropriately large volume. We start with the following lemma

Lemma 22. *Let $K := (B_2^D)^{\hat{\otimes} m}$ be the projective tensor product of m copies of the D-dimensional Euclidean ball (real or complex). Then K contains the following multiple of the Euclidean ball in $(\mathbf{C}^D)^{\otimes m}$ (resp., $(\mathbf{R}^D)^{\otimes m}$)*

$$\frac{1}{D^{(m-1)/2}} B_2^{D^m} \subset K.$$

Proof. Let $(e_1, \dots, e_D)$ be the canonical basis of $\mathbf{C}^D$. We write an element A of $(\mathbf{C}^D)^{\otimes m}$ as a generalized matrix: $A = (a_{i_1 \dots i_m})$ stands for

$$A = \sum_{i_1, \dots, i_m = 1}^{D} a_{i_1 \dots i_m} e_{i_1} \otimes \dots \otimes e_{i_m}$$

The norm dual to $\| \cdot \|_K$ is

$$\|A\|_{K^\circ} = \max_{x^1, \dots, x^m \in B_2^D} \left| \sum_{i_1, \dots, i_m = 1}^{D} a_{i_1 \dots i_m} x^1_{i_1} \dots x^m_{i_m} \right| \tag{3.10}$$

Let us write $\|A\|_2$ for the Euclidean norm of A, i.e., $\|A\|_2^2 = \sum |a_{i_1 \dots i_m}|^2$. We want to show that $\forall A \in (\mathbf{C}^D)^{\otimes m}$ we have $D^{-(m-1)/2}\|A\|_2 \leqslant \|A\|_{K^\circ}$. By homogeneity, we can assume that $\|A\|_2 = 1$. Now choose $x^1, \dots, x^{m-1}$ randomly and independently to be uniformly distributed on the unit sphere of $\mathbf{C}^D$. We write $\mathbf{E}$ for the corresponding expectation. Let X_k, $k = 1, \dots, D$, be the random variable obtained by summing only on the kth "hyper-slice," that is

$$X_k = X_k(x^1, \dots, x^{m-1}) := \sum_{i_1, \dots, i_{m-1} = 1}^{D} a_{i_1 \dots i_{m-1} k} x^1_{i_1} \dots x^{m-1}_{i_{m-1}}$$

We can easily calculate $\mathbf{E}|X_k|^2$ since many cancellations come from the fact that $\mathbf{E}(x^k_i \overline{x^l_j}) = \frac{1}{D}\delta_{kl}\delta_{ij}$. We obtain

$$\mathbf{E}|X_k|^2 = \frac{1}{D^{m-1}} \sum_{i_1, \dots, i_{m-1} = 1}^{D} \left| a_{i_1 \dots i_{n-1} k} \right|^2$$

Therefore, $\mathbf{E}(\sum_{k=1}^{D} |X_k|^2) = \frac{1}{D^{m-1}}$. This implies the existence of unit vectors $x^1, \dots, x^{m-1}$ such that denoting $Y_k := X_k(x^1, \dots, x^{m-1})$, we have

$$\sum_{k=1}^{D} |Y_k|^2 \geqslant \frac{1}{D^{m-1}}.$$

Choosing these points in (3.10), we obtain

$$\|A\|_{K^\circ} \geqslant \max_{x^m \in B_2^D} \sum_{k=1}^{D} X_k x^m_k = \left(\sum_{k=1}^{D} |X_k|^2 \right)^{1/2} \geqslant \frac{1}{D^{(m-1)/2}}$$

$\square$

Remark: It turns out that this lemma is surprisingly sharp. As shown in Lemma 26 below, even the *a priori* larger volume radius of K is (up to multiplicative factor depending only on m) of the same order $D^{-(m-1)/2}$. Note that for $m = 2$ we obtain even the optimal constant (these are the classical inclusion relations for balls in Schatten classes).

Let $\mathcal{H} = (\mathbf{C}^D)^{\otimes N}$ and $\Gamma(\mathcal{H}) \subset \mathcal{B}(\mathcal{H})$ be the convex hull of rank one product operators

$$\Gamma(\mathcal{H}) := \mathrm{conv}\{|x_1 \otimes \cdots \otimes x_N\rangle\langle y_1 \otimes \cdots \otimes y_N| \;:\; x_1, y_1, \ldots, x_N, y_N \in B_2^D\}.$$

The convex body $\Gamma(\mathcal{H})$ is most naturally seen as the Nth projective tensor power of the set of (not necessarily Hermitian) operators on $\mathbf{C}^D$ whose trace class norm is ≤ 1. However, it can also be identified with $(B_2^D)^{\hat{\otimes} 2N}$ when we identify $\mathcal{B}(\mathcal{K})$ with $\overline{\mathcal{K}} \otimes \mathcal{K}$. It then follows from the preceding lemma that $\Gamma(\mathcal{H})$ contains a Euclidean ball (a Hilbert–Schmidt ball in this context) of radius $D^{-(2N-1)/2}$.

The next lemma will relate $\Gamma(\mathcal{H})$ to $\Sigma(\mathcal{H})$, allowing to deduce that the latter body contains a suitably large Euclidean ball. Let d_N be the geometric distance between the sets Δ and Σ corresponding to N qubits, i.e. the smallest positive number such that $\Delta((\mathbf{C}^2)^{\otimes N}) \subset d_N \Sigma((\mathbf{C}^2)^{\otimes N})$. We then have

Lemma 23. *Let $\pi : \mathcal{B}(\mathcal{H}) \to \mathcal{B}_{sa}(\mathcal{H})$ be the projection onto Hermitian part, $\pi(A) := \frac{1}{2}(A + A^\dagger)$. Then*

$$\pi(\Gamma(\mathcal{H})) \;\subset\; d_N \,\Sigma(\mathcal{H}).$$

Proof. It is enough to show that extreme points of $\pi(\Gamma)$ are contained in $d_N\Sigma$. Any extreme point A of $\pi(\Gamma)$ can be written as

$$A = \frac{1}{2}\left(|x_1 \otimes \cdots \otimes x_N\rangle\langle y_1 \otimes \cdots \otimes y_N| + |y_1 \otimes \cdots \otimes y_N\rangle\langle x_1 \otimes \cdots \otimes x_N|\right)$$

It may appear at the first sight that the above representation shows that A is separable. However, while the two terms in the parentheses are indeed product operators, they are not Hermitian and we can only conclude that $A \in \Delta(\mathcal{H})$ (as a Hermitian operator whose trace class norm is ≤ 1).

Let $\mathcal{H}_i$ be the 2-dimensional subspace of $\mathbf{C}^D$ spanned by x_i and y_i (if the vectors are proportional, add any vector to get a 2-dimensional space) and let $\mathcal{H}' := \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$. Then A can be considered as an operator on $\mathcal{H}'$; more precisely, as an element of $\Delta(\mathcal{H}')$ (and, conversely, any operator acting on $\mathcal{H}'$ can be canonically lifted to one acting on $\mathcal{H}$). Note that since we are in the asymptotics where N is small and D is large, the dimension of the problem has been dramatically decreased. Since A belongs to $\Delta(\mathcal{H}')$, it also belongs to $d_N\Sigma(\mathcal{H}')$, and thus to $d_N\Sigma(\mathcal{H})$. $\square$

To effectively apply Lemma 23, upper bounds on d_N are needed. It has been observed in [Sza], Appendix H, that $d_N \leq 6^{N/2}$. This estimate has been subsequently slightly improved in [GB3] to $2/3 \times 6^{N/2}$, and even to $a_N \times 6^{N/2}$ with $\lim_{N\to\infty} a_N \approx 0.624$. [These bounds are in fact based on estimates for the *a priori* larger quantities, the geometric distances between $\Sigma((\mathbf{C}^2)^{\otimes N})$ (or $\mathcal{S}((\mathbf{C}^2)^{\otimes N}) - \mathrm{Id}/2^N$) and Hilbert–Schmidt balls, which are essentially reciprocals of the Hilbert–Schmidt inradii of these sets; and in this latter context they are "nearly optimal;" see Theorem 3.4 and the comments following it.] Thus $\Sigma(\mathcal{H}) \supset 3/2 \times 6^{-N/2}\pi(\Gamma(\mathcal{H}))$; combining this inclusion with Lemma 22 or, more precisely, with the observation following the definition of $\Gamma(\mathcal{H})$, we conclude that $\Sigma(\mathcal{H})$ contains the Hilbert–Schmidt ball of radius $3/2 \times 6^{-N/2} D^{-(2N-1)/2} = 3/2 \times 6^{-N/2}/d^{1-1/2N}$. This gives a lower bound for the volume radius which, together with (3.7), yields

$$\left(\frac{\mathrm{vol}(\Sigma)}{\mathrm{vol}(\Delta)}\right)^{1/d^2} \geqslant \frac{3/4 \times 6^{-N/2}}{d^{1/2-1/2N}}$$

To conclude the proof of the theorem we pass to the bodies $\mathcal{S}$ and $\mathcal{D}$ using (3.6).

Remark: The bipartite case ($N = 2$) was studied in [GB1], which contains in particular the remarkable result that $\mathcal{D}$ and $\mathcal{S}$ have then the same inradius, which equals $1/\sqrt{d(d-1)}$. However, the inradii of the symmetrized bodies, which are (in both cases) comparable with the volume radii, are (asymptotically) very different: the inradius of Δ equals $1/\sqrt{d}$, while the inradius of Σ has just been shown to be of order $1/d^{3/4}$.

3.2.4 Proof of Theorem 3.3: Large number of small subsystems

This part deals with asymptotic estimations of volumes when N, the number of subsystems, tends to infinity whereas the dimension D of each subsystem remains bounded. This case is probably the one with most physical interest. When all subsystems are 2-dimensional (qubits), Theorem 3.3 has been proved in [Sza].

For the proof of the present case it is more convenient to deal with an affine image of Σ which is *more balanced* than Σ itself or, equivalently, to consider a new scalar product which is better adapted to the analysis of Σ than the Hilbert–Schmidt product. It is a known phenomenon that high-dimensional convex bodies often enjoy hidden symmetries (or approximate symmetries) that are only revealed when one looks at them through a suitable Euclidean structure. In our situation, in the asymptotics when N is large and

D is bounded, our Theorem 3.2, obtained with the usual Euclidean structure, misses the genuine volumic behavior of the bodies $\mathcal{S}$ and Σ. The appropriate scalar product will be here the one derived from the Löwner ellipsoid of Σ. To see why, just look back at the equation (3.9). This bound is the tightest when $\mathcal{E}$ is the Löwner ellipsoid of Σ. It turns out that it is possible to describe completely this ellipsoid. First recall that $\Sigma(\mathcal{H}) = \Delta(\mathbf{C}^D)\hat{\otimes}\ldots\hat{\otimes}\Delta(\mathbf{C}^D)$. By Lemma 19, it is enough to calculate the Löwner ellipsoid of $\Delta(\mathbf{C}^D)$, and by tensoring we get the Löwner ellipsoid of $\Sigma(\mathcal{H})$.

We will determine the Löwner ellipsoid of $\Delta(\mathbf{C}^D)$ using the following elementary general lemma.

Lemma 24. *Let u be a unit vector in $\mathbf{R}^n$ and $H_0 = \{u\}^\perp$ be the orthogonal hyperplane. Let $h > 0$ be real number and $H = H_0 + hu$ be a translate of H_0. We consider a convex body $\Omega = \mathrm{conv}\{W \cup -W\}$, where W is a convex body in H. Then the following assertions are equivalent:*

1. *Ω is in Löwner position (i.e. the unit ball B_2^n is the Löwner ellipsoid of Ω).*
2. *$h = 1/\sqrt{n}$ and $B_2^n \cap H$ is the Löwner ellipsoid of W.*

Proof. Assume that Ω is in Löwner position, so $\Omega \subset B_2^n$. By John's theorem (Proposition 3.1), this means that there exists a John resolution of identity (x_i, c_i), with $x_i \in \Omega \cap S^{n-1}$ and $\sum c_i |x_i\rangle\langle x_i| = \mathrm{Id}$. Since x_i are extreme points of Ω, they must be in W or $-W$, and since Ω is symmetric we can assume they are all in W. Let P be the orthogonal projection onto H_0. It follows that $\sum c_i |Px_i\rangle\langle Px_i| = P$; note that $\|Px_i\| = \sqrt{1-h^2}$. This means that (Px_i, c_i') is a John resolution of identity in H_0, with $c_i' = (1-h^2)c_i$. By Proposition 3.1, $(1-h^2)^{-1/2}PW$ is in Löwner position, or equivalently $B_2^n \cap H$ is the Löwner ellipsoid of W. Moreover, we have the conditions $\sum c_i' = n-1$ and $\sum c_i = n$, which force $h = 1/\sqrt{n}$.

The converse follows by retracing the above argument in the opposite direction. $\square$

Lemma 25. *The Löwner ellipsoid of $\Delta(\mathbf{C}^D)$ is determined by the following scalar product defined for $A, B \in \mathcal{B}_{sa}(\mathbf{C}^D)$ by*

$$\langle A, B\rangle_{\mathrm{Löw}(\Delta(\mathbf{C}^D))} = (1 + \frac{1}{D})\mathrm{tr}(AB) - \frac{1}{D}\mathrm{tr}(A)\mathrm{tr}(B)$$

Proof. First remark that, because of its uniqueness, the Löwner ellipsoid of any body K must inherit all the symmetries of K. Since $\mathcal{D}(\mathbf{C}^D)$ is invariant under unitary conjugations (i.e., the maps $\pi_U(X) = UXU^\dagger$ with $U \in U(D)$), the ellipsoid $\text{Löw}(\mathcal{D}(\mathbf{C}^D))$ must be similarly invariant, and thus it is the circumscribed Euclidean ball. This is actually somewhat delicate; the relevant fact is that the action of the group $\{\pi_U : U \in U(D)\}$ on the hyperplane $\mathcal{T}_1$ containing $\mathcal{D}(\mathbf{C}^D)$ is irreducible (in particular, Id/D is the only fixed point and so it must be the center). In the language of convex bodies (see [Tom]) we say that $\mathcal{D}(\mathbf{C}^D)$ has enough symmetries. On the other hand, the fact that this group acts transitively on the set of extreme points of $\mathcal{D}(\mathbf{C}^D)$ (which are the pure states) implies *by itself* only that all these extreme points are contact points, i.e., belong to the boundary of the Löwner ellipsoid.

By Lemma 24, we know that the trace of the Löwner ellipsoid of $\Delta(\mathbf{C}^D)$ on the hyperplane $\mathcal{T}_1$ is a Euclidean ball (centered at Id/D), so we have for some real numbers α and β

$$\langle A, B\rangle_{\text{Löw}(\Delta(\mathbf{C}^D))} = \alpha \text{tr}(AB) + \beta \text{tr}(A)\text{tr}(B)$$

To determine α and β, observe that $\langle \rho, \rho\rangle_{\text{Löw}(\Delta(\mathbf{C}^D))} = 1$ for any pure state (hence contact point) ρ, and that (from the condition on h in Lemma 24; note that $n = D^2$), $\langle \text{Id}/D, \text{Id}/D\rangle_{\text{Löw}(\Delta(\mathbf{C}^D))} = 1/D^2$. This gives $\alpha = 1 + 1/D$ and $\beta = -1/D$. $\square$

It is possible to use the Löwner ellipsoid of $\Sigma(\mathcal{H})$ as the ellipsoid $\mathcal{E}$ in formula (3.9). Choosing $\delta = 1/\sqrt{N \log 2N}$ as earlier, we obtain the upper estimate in the formula

$$\frac{1}{d} \leqslant \left(\frac{\text{vol}(\Sigma)}{\text{vol}(\text{Löw}(\Sigma))}\right)^{1/d^2} \leqslant \frac{C\sqrt{DN \log N}}{d} \tag{3.11}$$

The lower estimate follows from the classical fact ([Bal]) that for a centrally symmetric convex body K in $\mathbf{R}^n$, we have the inclusion $\text{Löw}(K) \subset \sqrt{n}K$. Improvements on constants can be derived from a result of Barthe ([Bar]) which asserts that for an n-dimensional symmetric body K, the ratio

$$\left(\frac{\text{vol}(K)}{\text{vol}(\text{Löw}(K))}\right)^{1/n}$$

is minimal when K is the unit ball of ℓ_1^n (and thus is *at least* $(4/\pi)^{1/2}(\Gamma(n/2+1)/\Gamma(n+1))^{1/n}) = \sqrt{\frac{2e}{\pi}}(1 - O(\frac{1}{n}))\frac{1}{\sqrt{n}}$; we recall that here $n = d^2$).

It remains to calculate the volume of the Löwner ellipsoid of Σ. It follows from Lemma 19 that, if Φ denotes a linear map which sends $B_2^{D^2}$ onto

Löw($\Delta(\mathbf{C}^D)$), then $\Psi := \Phi^{\otimes N}$ maps B_{HS} onto Löw($\Sigma(\mathcal{H})$). By Lemma 25, we can define Φ by $\Phi(A) = (1+1/D)^{-1/2}A$ if A has trace 0 and $\Phi(\mathrm{Id}) = \sqrt{D}\,\mathrm{Id}$. This gives $\det(\Phi) = \sqrt{D(1+1/D)^{1-D^2}}$ and finally

$$\frac{\mathrm{vol}(\text{Löw}(\Sigma))}{\mathrm{vol}(B_{HS})} = \det(\Psi) = \det(\Phi)^{ND^{2N-2}} = d^{-\alpha_D d^2} \tag{3.12}$$

To complete the proof it remains to combine the volume estimates (3.7), (3.11), (3.12) and (3.6).

3.2.5 Proof of Theorem 3.4: Tight upper bounds on the inradii

The idea is to show that there is a projection of the set $\Sigma = \Sigma((\mathbf{C}^2)^{\otimes N})$ which is demonstrably small. Specifically, let $P : \mathcal{B}_{sa}(\mathbf{C}^2) \to \mathcal{B}_{sa}(\mathbf{C}^2)$ be the orthogonal projection onto the 3-dimensional subspace of trace zero matrices and let $\Pi := P^{\otimes N}$. Since projective tensor products commute with linear maps (in the sense that $(T_1 \otimes \ldots \otimes T_s)(K_1 \hat{\otimes} \ldots \hat{\otimes} K_s) = (T_1K_1) \hat{\otimes} \ldots \hat{\otimes} (T_sK_s)$), we have

$$\Pi\left(\Sigma((\mathbf{C}^2)^{\otimes N})\right) = P^{\otimes N}\left(\Delta(\mathbf{C}^2)^{\hat{\otimes} N}\right) = \left(P(\Delta(\mathbf{C}^2))\right)^{\hat{\otimes} N}.$$

Since $\Delta(\mathbf{C}^2)$ is a cylinder whose axis coincides with the kernel of P, the image of $\Delta(\mathbf{C}^2)$ under P is a 3-dimensional Euclidean ball of radius $1/\sqrt{2}$ (more precisely, $\mathcal{D}(\mathbf{C}^2) - Id/2$). Accordingly, the image of the corresponding set Σ under Π is the nth projective tensor power of such a ball. The relevant parameters of such sets (mean widths, volume radii) are majorized by the following statement, which is a complement of Lemma 4.

Lemma 26. *There is an absolute constant C_1 such that if D, m are positive integers ($m \geqslant 2$) and $K := (B_2^D)^{\hat{\otimes} m}$ is the projective tensor product of m copies of the D-dimensional Euclidean ball (real or complex), then*

$$\mathrm{vrad}(K) \leqslant w(K) < \frac{C_1\sqrt{m \log m}}{D^{(m-1)/2}}$$

Proof. The first inequality in Lemma 26 — comparing the volume radius of a convex body to its mean width — is just the Urysohn inequality. The proof of the second follows the same lines as — but is simpler than — the approach that yielded formula (3.9). We present the details only for the case that is relevant to Theorem 3.4, namely $D = 3$ in the real setting. The argument is very similar to the one used in [Sza] to obtain an upper bound for the volume of $\Sigma((\mathbf{C}^2)^{\otimes m})$, where the reader is referred for additional background and justifications.

We start by noting that, for any $\delta \in (0, \sqrt{2})$, the sphere S^2 contains a δ-net $\mathcal{F}$ whose cardinality is $\leqslant 16/\delta^2$. On the other hand, an elementary geometric argument shows that the convex hull of any δ-net contains a (Euclidean) ball of radius $1-\delta^2/2$. Accordingly, the convex hull of $\mathcal{F}^{\otimes m}$, the mth tensor power of $\mathcal{F}$, contains $(1-\delta^2/2)^m (B_2^3)^{\hat{\otimes} m}$. Since $\#(\mathcal{F}^{\otimes m}) \leqslant (\#\mathcal{F})^m \leqslant (4/\delta)^{2m}$, it follows from (3.4) that

$$w((1-\delta^2/2)^m (B_2^3)^{\hat{\otimes} m}) \leqslant w(\mathrm{conv}(\mathcal{F}^{\otimes m})) < \gamma_{3^m}^{-1} \sqrt{2 \log\left((4/\delta)^{2m}\right)}$$

and, consequently,

$$\mathrm{vrad}((B_2^3)^{\hat{\otimes} m}) \leqslant w((B_2^3)^{\hat{\otimes} m}) < 2\gamma_{3^m}^{-1} (1-\delta^2/2)^{-m} \sqrt{m \log\left(4/\delta\right)}.$$

We now choose $\delta = 1/\sqrt{m \log 2m}$; then, for large m, $(1-\delta^2/2)^{-m} \sim 1$, $\log(4/\delta) \sim \frac{1}{2}\log m$ and $\gamma_{3^m} \sim 3^{m/2}$. This yields the asserted upper bound on the mean width with $C_1 \sim \sqrt{2/3}$ for large d. A more careful calculation using Lemma 20 for small m shows that $C_1 = 1.67263$ works for all m. [The discussion of constants above and in the remainder of this section is specific to $D = 2$, but easily carries over to general case; for example, it is easy to show that $C_1 \sim 1$ works for large m and all D.) As in [Sza], further improvement are possible by working with explicit nets and/or by noting that $\mathcal{F}$ can be chosen to be symmetric, but we will not pursue them since it is likely that, for the problem at hand, sharper estimates can be obtained by analytic methods. $\square$

We now return to the proof of Theorem 3.4. From prior considerations, the image of Σ under the projection Π is congruent to $2^{-N/2}(B_2^3)^{\hat{\otimes} N}$ and so, by Lemma 26,

$$w(\Pi(\Sigma)) = 2^{-N/2} w((B_2^3)^{\hat{\otimes} N} < 3^{1/2} C_1 \sqrt{N \log N}\, 6^{-N/2}.$$

Since the inradius is trivially smaller than the mean width, and since the inradius of the set $\mathcal{S}$ of separable states does not exceed that of its symmetrization Σ, Theorem 3.4 follows (with $C_0 = 3^{1/2} C_1 < 3$). It is also routine to obtain an (identical or nearly identical) upper bound on the mean width of $\mathcal{S}$; however, some care is needed because the dimensions of $\mathcal{S}$ and Σ are not the same.

Since our argument is of a global nature, we are not able to produce an explicit state in the ball of radius $r := C_0 \sqrt{N \log N}\, 6^{-N/2}$ and centered at

Id/d which is not separable. However, standard tools of asymptotic geometric analysis (cf. [ST] or [Pis]) imply that even stronger properties are satisfied "generically." Denote by $\mathcal{H}_0$ the $d_0 := 3^N$-dimensional range of the projection Π. Then, for most of the unit vectors u on the unit sphere of $\mathcal{H}_0$, the state $\sigma = Id/2^N + 2ru$ is not separable, and the same holds for any state ρ such that $\Pi(\rho) = \Pi(\sigma)$ (here "most of" means that the exceptional set is of normalized measure $< 2^{-d_0/2}$). Moreover, a slightly weaker but comparable property holds *simultaneously* for all u in a "generic" (in the sense of the invariant measure on the corresponding Grassmannian) $\lceil d_0/2 \rceil$-dimensional subspace of $\mathcal{H}_0$.

As mentioned in the introduction, the above argument can be generalized to other values of D and leads to an upper bound for the inradii of the sets Σ and $\mathcal{S}$ corresponding to $(\mathbf{C}^D)^{\otimes N}$ which is, up to a logarithmic factor, $(D(D+1))^{-N/2}$. While this upper bound differs, for $D > 2$, from the lower bound for the inradius of $\mathcal{S}$ that was found in [GB3], it gives the correct order for the inradius of the set Σ. Indeed, Σ contains $\text{Löw}(\Sigma)/d$, which itself contains $(D(D+1))^{-N/2} B_{HS}$ (this argument parallels the one for qubits given in [Sza], Appendix H, where we refer the reader for details).

3.2.6 Proof of Theorem 3.5: Asymptotic weakness of PPT criterion

We will use the following proposition which is taken from [MiPa2].

Proposition 3.2. *Let K and L be convex bodies in $\mathbf{R}^n$ with the same centroid. Then*

$$\text{vol}(K)\text{vol}(L) \leqslant \text{vol}(K - L)\text{vol}(K \cap L),$$

where $K - L := \{x - y \,:\, x \in K, y \in L\}$ is the Minkowski difference.

We apply the proposition with $K = \mathcal{D}$ and $L = T\mathcal{D}$. This gives

$$\frac{\text{vol}(\mathcal{D})}{\text{vol}(\text{PPT})} \leqslant \frac{\text{vol}(\mathcal{D} - T\mathcal{D})}{\text{vol}(\mathcal{D})} \tag{3.13}$$

Note that we actually used the proposition in the space $\mathcal{T}_1 \sim \mathbf{R}^n$, seen as a vector space with Id/d as origin; the point Id/d is also the centroid of $\mathcal{D}$ (and $T\mathcal{D}$), it is even the the only fixed point under the group of symmetries of $\mathcal{D}$ (cf. the proof of Lemma 25). We rewrite (3.13) using volume radii

$$\left(\frac{\text{vol}(\mathcal{D})}{\text{vol}(\text{PPT})}\right)^{1/n} \leqslant \frac{\text{vrad}(\mathcal{D} - T\mathcal{D})}{\text{vrad}(\mathcal{D})}$$

Recall that we majorized the volume radius by the mean width using the Urysohn inequality (here mean width is also taken in $\mathcal{T}_1$). This is very convenient since, as one can check immediately from the definition, the mean width is additive with respect to the Minkowski operations: $w(\mathcal{D} - T\mathcal{D}) = w(\mathcal{D}) + w(-T\mathcal{D})$. Since $-T$ is an isometry, it preserves the uniform measure on the sphere S^{n-1} and thus $w(-T\mathcal{D}) = w(\mathcal{D})$. This gives

$$\left(\frac{\mathrm{vol}(\mathcal{D})}{\mathrm{vol}(\mathrm{PPT})}\right)^{1/n} \leqslant \frac{2w(\mathcal{D})}{\mathrm{vrad}(\mathcal{D})}$$

We now appeal to (3.8) to majorize the right hand side by 8, which proves Theorem 3.5 with $c_0 = 1/8$. Note also that one can use the explicit formula (3.3) for the volume of $\mathcal{D}$; this shows that asymptotically c_0 tends to $e^{-1/4}/4 \approx 0.195$. Moreover, numerical evidence (which presumably can be confirmed by rigorous calculation using appropriate Stirling-type formulae) suggests that $\mathrm{vrad}(\mathcal{D}) \geqslant e^{-1/4}/\sqrt{d}$ for *all* dimensions d, which would imply that the asymptotic value is in fact a bound.

Finally, observe that the proof above works actually for any (Hilbert–Schmidt) isometry in $\mathcal{T}_1$ which fixes Id/d, and not only for the partial transpose T.

3.3 Appendices

3.3.1 Preuve du théorème 3.1

Products of Bloch balls and similar bodies

G. Aubrun, S. J. Szarek, E. Werner

The purpose of this note is to show that the set of normalized separable states of an N-qubit quantum system contains a Hilbert–Schmidt ball of radius $\sqrt{3} \cdot 6^{-\frac{N}{2}}$, centered at the normalized identity. This improves slightly a result of Gurvits and Barnum [GB2, GB3], and is based on fine-tuning of their method.

Notation. For any $n \in \mathbb{N}$, we single out in the space $\mathbf{R}^n$ a unit vector which we call e_0, or $e_0^{(n)}$ to indicate the dimension. We will frequently identify $\mathbf{R}^n \otimes \mathbf{R}^p$ with $\mathbf{R}^{np}$ so that $e_0^{(np)} \simeq e_0^{(n)} \otimes e_0^{(p)}$. A concrete example when this convention is going to be used is the space $\mathcal{B}_{sa}(\mathbf{C}^d)$ of self-adjoint operators on the d-dimensional complex Hilbert space (or, equivalently, $d \times d$ Hermitian matrices), identified with $\mathbf{R}^{d^2}$ so that $e_0^{(d^2)}$ corresponds to $\mathrm{Id}/\sqrt{d}$, the identity matrix normalized in the Hilbert–Schmidt norm. The above gradation is then compatible with canonical identifications $\mathcal{B}_{sa}(\mathbf{C}^{d_1}) \otimes \mathcal{B}_{sa}(\mathbf{C}^{d_2}) \simeq \mathcal{B}_{sa}(\mathbf{C}^{d_1} \otimes \mathbf{C}^{d_2})$.

Let $\mathcal{D}_N = \mathcal{D}((\mathbb{C}^2)^{\otimes N})$ be the (convex) set of states on $\mathcal{B}((\mathbb{C}^2)^{\otimes N})$ and let $\mathcal{S}_N$ be the (convex) subset of $\mathcal{D}_N$ consisting of the separable states. Then $\mathcal{S}_N = \mathcal{D}_1^{\hat{\otimes} N}$, where the projective tensor product of convex bodies $K_1, \dots, K_N$ is defined by

$$K_1 \hat{\otimes} \dots \hat{\otimes} K_N = \mathrm{conv}\{x_1 \otimes \cdots \otimes x_N, x_i \in K_i\}$$

We write B_2^n for the unit ball in $\mathbf{R}^n$ (centered at 0) and $\breve{B}_2^n$ for the unit ball intersected with the hyperplane $e_0^\perp$. With this notation, the Bloch ball $\mathcal{D}_1$ is equal to $1/\sqrt{2}(e_0 + \breve{B}_2^4)$ and, consequently, $\mathcal{S}_N = 2^{-N/2}(e_0 + \breve{B}_2^4)^{\hat{\otimes} N}$.

Results. In the above notation, the assertion stated at the beginning of the note can be rephrased as

Theorem 3.1 . *For any $N \geqslant 1$*

$$e_0^{\otimes N} + \frac{1}{3^{\frac{N-1}{2}}} \breve{B}_2^{4^N} \subset (e_0 + \breve{B}_2^4)^{\hat{\otimes} N}.$$

Theorem 3.1 is proved by repeated application of the following

Lemma 27. *Let $0 \leqslant \beta \leqslant 1$. Then for any $n \geqslant 4$*

$$e_0 + \frac{\beta}{\sqrt{3}}\ \breve{B}_2^{4n} \subset (e_0 + \breve{B}_2^4)\hat{\otimes}(e_0 + \beta\ \breve{B}_2^n).$$

Proof. If $K \ni 0$ is a closed convex subset of the Euclidean space, the (maximal) radius of ball centered at 0 and contained in K is given by

$$\min_{|u|=1}\ \max_{x \in K}\ \langle x, u\rangle$$

One can similarly express the in-radii of convex sets of lower dimension. In particular, the maximal radius of a ball inscribed in the projective tensor product $(e_0 + \breve{B}_2^4)\hat{\otimes}(e_0 + \beta\ \breve{B}_2^n)$ and centered at $e_0 \otimes e_0$ is

$$\min_{|u|=1, u \perp e_0 \otimes e_0}\ \max_{x \in B_2^3, y \in \beta \breve{B}_2^n}\ \langle (e_0 + x) \otimes (e_0 + y), u\rangle. \tag{3.14}$$

The orthogonal complement of $e_0 \otimes e_0$ in $\mathbb{R}^4 \otimes \mathbb{R}^n$ is $(\mathbb{R}e_0 \otimes \mathbb{R}^{n-1}) \oplus (\mathbb{R}^3 \otimes \mathbb{R}e_0) \oplus (\mathbb{R}^3 \otimes \mathbb{R}^{n-1})$. Denoting $m = n-1$ and identifying the three summands with $\mathbb{R}^m$, $\mathbb{R}^3$ and $3 \times m$ matrices respectively, we may rewrite (3.14) as

$$\Phi_m(\beta) := \min_{|a|^2+|b|^2+\|A\|_{HS}^2=1}\ \max_{|x|=1, |y|=\beta}\ \langle a, x\rangle + \langle b, y\rangle + \langle Ay, x\rangle, \tag{3.15}$$

where $a, x \in \mathbb{R}^3$, $b, y \in \mathbb{R}^m$ and A is a $3 \times m$ matrix. The assertion of Lemma 27 is equivalent to $\Phi_m(\beta) \geq \beta/\sqrt{3}$ for all $m \geq 3$ and all $\beta \in [0,1]$. (The reverse inequality is trivial; choose, for example, $a = b = 0$ and $A = \mathrm{Id}/\sqrt{3}$ if $m = 3$, and similarly for $m > 3$.)

Before proceeding, we point out that when $m = 3, \beta = 1$, the inequality $\Phi_3(1) \geq 1/\sqrt{3}$ is equivalent to the case $n = 4, \beta = 1$ of Lemma 27 and, at the same time, to the case $N = 2$ of Theorem 3.1, that is, to the inradius of $\mathcal{S}_2$ being at least $\frac{1}{2\sqrt{3}}$. The in-radius of the set of separable states in the bilateral (two factors) case has been determined to be equal to the (easily calculated) in-radius of the set of all states in [GB1]. In the special case of $\mathcal{S}_2$ (two qubits) this is rather classical. One possible argument: the sufficiency of Peres' partial transpose criterion for $2 \otimes 2$ systems ([HHH1]) means that $\mathcal{S}_2 = \mathcal{D}_2 \cap T(\mathcal{D}_2)$, where T is the partial transpose (say, with respect to the first system), and so the equality of the in-radii of $\mathcal{S}_2$ and $\mathcal{D}_2$ follows from T being an ($\mathbb{R}$-linear) isometry which keeps $\mathrm{Id}/4$ (the center of the balls) fixed.

We will show first that $\Phi_3(\beta) = \frac{\beta}{\sqrt{3}}$. We have

$$\begin{aligned}\Phi_m(\beta) &= \min_{|a|^2+|b|^2+\|A\|_{HS}^2=1}\ \max_{|y|=\beta}\ \left(\langle b, y\rangle\ +\ \max_{|x|=1}\ \langle a, x\rangle + \langle Ay, x\rangle\right)\\ &= \min_{|a|^2+|b|^2+\|A\|_{HS}^2=1}\ \max_{|y|=\beta}\ \left(\langle b, y\rangle\ +\ |Ay + a|\right). \end{aligned} \tag{3.16}$$

Consequently, proving $\Phi_3(\beta) \geqslant \frac{\beta}{\sqrt{3}}$ is equivalent to establishing that, for all $a, b \in \mathbb{R}^3$ and for all 3×3 matrices A,

$$\max_{|y|=\beta} \left(\langle b, y\rangle \ + \ |Ay + a|\right) \geqslant \frac{\beta}{\sqrt{3}} \left(|a|^2 + |b|^2 + \|A\|_{HS}^2\right)^{\frac{1}{2}}.$$

In turn, setting $y^{'} = \frac{y}{\beta}$ and $a^{'} = \frac{a}{\beta}$, we see that the above is equivalent to showing that for all $a^{'}, b \in \mathbb{R}^3$ and for all 3×3 matrices A

$$\max_{|y^{'}|=1} \langle b, y^{'}\rangle \ + \ |Ay^{'} + a'| \geqslant \frac{1}{\sqrt{3}} \left(\beta^2|a^{'}|^2 + |b|^2 + \|A\|_{HS}^2\right)^{\frac{1}{2}}.$$

The left hand side of the last inequality does not depend on β, while (for fixed $a^{'}, b, A$) the right hand side is an increasing function of β. Since, as we observed, the inequality holds for $\beta = 1$, it does also hold for all $\beta \in [0, 1)$.

It remains to show that, for $m > 3$, $\Phi_m(\beta) = \Phi_3(\beta)$, or even just that $\Phi_m(\beta) \geq \Phi_3(\beta)$. The key observation is that the min-max expressions $\min_{a,b} \max_{x,y}$ for given matrix A in (3.15) or (3.16) depend only on the singular values of the matrix A. This is most easily seen from the form in the second line of (3.16), either by
• a geometric argument, by noticing is that what counts there is the shape (semi-axes) of the ellipsoid $\beta A B_2^m$, or by
• an algebraic argument, by substituting $A = UA_1V$, where $U \in O(3), V \in O(m)$, then changing variables to $a_1 = U^{\dagger}a$, $y_1 = Vy$, $b_1 = Vb$ and noticing that

$$\langle b, y\rangle \ + \ |Ay + a| = \langle b_1, y_1\rangle \ + \ |A_1y_1 + a_1|$$

Accordingly, we may assume that at most the diagonal (i.e., 11, 22, and 33) entries of the matrix A are nonzero (what we actually need is that only the first three columns are allowed to be nonzero). With this restriction, the matrix A is in effect 3×3, and the only difference between $\Phi_m(\beta)$ and $\Phi_3(\beta)$ is then that in the formula for the former the vectors y and b do not need to be supported on the first three coordinates. While it is easy to believe that, with a matrix A supported on the first three columns "all the action" must be happening on the first three coordinates of $\mathbf{R}^m$, more careful book-keeping is in order since we are dealing here with a min-max. Let us split y and b into components supported on the first 3 coordinates and on the remaining $n - 3$ coordinates, $y = y^{'} + y^{''}$ and $b = b^{'} + b^{''}$. Then

$$\Phi_m(\beta) = \min_{|a|^2+|b^{'}|^2+|b^{''}|^2+\|A\|_{HS}^2=1} \quad \max_{\substack{|x|=1 \\ |y^{'}|^2+|y^{''}|^2=\beta^2}} \langle Ay', x\rangle + \langle a, x\rangle + \langle b^{'}, y^{'}\rangle + \langle b^{''}, y^{''}\rangle$$

Setting $\tau := \frac{|y''|}{\beta}$, $\theta := |b''|$ and making the clearly optimal (for given τ) choice of y'' to be a positive multiple of b'', we can rewrite the above as

$$\Phi_m(\beta) = \min_{|a|^2+|b'|^2+\|A\|_{HS}^2=1-\theta^2} \max_{|x|=1,|y'|=\beta(1-\tau^2)^{1/2}} \langle Ax, y'\rangle + \langle a, x\rangle + \langle b', y'\rangle + \theta\tau\beta$$

We now note that, for given a, b', A, θ, τ, optimizing the sum of the first three terms under max over x, y' yields at least $\sqrt{1-\theta^2}\,\Phi_3(\beta\sqrt{1-\tau^2})$. Since $\Phi_3(t) = t/\sqrt{3}$, we get

$$\Phi_m(\beta) \geq \min_{\theta\in[0,1]} \max_{\tau\in[0,1]} \sqrt{1-\theta^2}\,\frac{\beta\sqrt{1-\tau^2}}{\sqrt{3}} + \theta\tau\beta = \beta \min_{\theta\in[0,1]} \sqrt{\frac{1-\theta^2}{3} + \theta^2}\ .$$

The last minimum is clearly achieved at $\theta = 0$ and equals $1/\sqrt{3}$. It follows that $\Phi_m(\beta) \geq \beta/\sqrt{3} = \Phi_3(\beta)$, as required. $\square$

3.3.2 Preuve du théorème 3.4'

La preuve est due à Gurvits et apparaît implicitement dans [GB3]. Elle repose sur le lemme suivant, utilisé également dans [RMNDMC].

Lemme 28 (Les projections locales ne créent pas d'intrication). *Soit $\mathcal{H}_1, \ldots, \mathcal{H}_N$ des espaces de Hilbert et, pour chacun d'entre eux, $\mathcal{H}'_i \subset \mathcal{H}_i$ un sous-espace. On note $\mathcal{H} = \bigotimes \mathcal{H}_i$ et $\mathcal{H}' = \bigotimes \mathcal{H}'_i$. Soit, pour chaque i, π_i la projection orthogonale de $\mathcal{H}_i$ sur $\mathcal{H}'_i$, de sorte que $\pi := \bigotimes \pi_i$ est la projection orthogonale de $\mathcal{H}$ sur $\mathcal{H}'$. Soit A une matrice qui est un multiple positif d'un état séparable, c'est-à-dire*

$$A \in \mathbf{R}^+ \mathcal{S}(\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N)$$

Alors, $\pi A \pi$ est un multiple positif d'un état séparable (sur $\mathcal{H}'$), c'est-à-dire

$$\pi A \pi \in \mathbf{R}^+ \mathcal{S}(\mathcal{H}'_1 \otimes \cdots \otimes \mathcal{H}'_N)$$

Démonstration. Il suffit d'écrire la définition de la séparabilité et d'utiliser l'égalité

$$\pi(\rho_1 \otimes \cdots \otimes \rho_N)\pi = (\pi_1 \rho_1 \pi_1) \otimes \cdots \otimes (\pi_N \rho_N \pi_N)$$

□

Nous pouvons maintenant déduire facilement le théorème 3.4' à partir du théorème 3.4. Pour $D \geqslant 2$, soit r_D le rayon de la plus grande boule Hilbert–Schmidt centrée en Id contenue dans le cône séparable $\mathbf{R}^+\mathcal{S}((\mathbf{C}^D)^{\otimes N})$. Appliquons le lemme 28 avec $\mathcal{H}_i = \mathbf{C}^D$ et $\mathcal{H}'_i = \mathbf{C}^2$. En utilisant le fait que $\|\pi\rho\pi - \mathrm{Id}_{(\mathbf{C}^2)^{\otimes N}}\| \leqslant \|\rho - \mathrm{Id}_{(\mathbf{C}^D)^{\otimes N}}\|$, on obtient immédiatement que $r_D \leqslant r_2$. Par ailleurs, la quantité r_D est reliée au rayon interne i_D de $\mathcal{S}((\mathbf{C}^D)^{\otimes N})$ par la relation

$$i_D = \frac{r_D}{\sqrt{D^N(D^N - r_D^2)}}$$

Ainsi, l'inégalité $r_D \leqslant r_2$ se traduit en

$$i_D \leqslant \frac{2^N i_2}{\sqrt{D^{2N} + i_2^2 (2D)^N (D^N - 2^N)}}$$

En utilisant la borne supérieure sur i_2 qui provient du théorème 3.4, on obtient

$$i_D \leqslant \frac{C_0 \sqrt{N \log N}}{6^{N/2}} \frac{2^N}{D^N}$$

C'est exactement le contenu du théorème 3.4'.

3.3.3 Majoration précise du supremum d'un processus gaussien

Lemme 29. *Si $n \geqslant 2$ et $(X_1, \ldots, X_n)$ est un vecteur gaussien tel que pour $1 \leqslant i \leqslant n$, $\mathbf{E}X_i^2 \leqslant 1$, alors*

$$\mathbf{E} \max_{1 \leqslant i \leqslant n} |X_i| \leqslant \sqrt{2 \log n}.$$

Démonstration. L'estimation $\mathbf{E} \max X_i \leqslant \sqrt{2 \log n}$ est bien connue ; voir par exemple la proposition 1.1.3. dans [Tal]. Notons qu'à la différence du résultat du lemme, cette estimation est aussi vraie pour $n = 1$. La preuve que nous présentons suit la preuve du lemme 0.6.2 dans [Fer]. Soit T un nombre à choisir ultérieurement. On écrit

$$\mathbf{E} \max_{1 \leqslant i \leqslant n} |X_i| = \int_0^\infty \mathbf{P}\left(\max_{1 \leqslant i \leqslant n} |X_n| > t \right) dt.$$

Si $0 \leqslant t \leqslant T$, on majore trivialement l'intégrande par 1, alors que si $t > T$ on utilise la borne $\mathbf{P}(\max |X_n| > t) \leqslant 2n\mathbf{P}(G > t)$, où G désigne une variable gaussienne standard. Une intégration par parties donne ensuite

$$\int_T^\infty \mathbf{P}(G > t) dt = \frac{1}{\sqrt{2\pi}} e^{-T^2/2} - T\mathbf{P}(G > T).$$

Il reste ensuite à optimiser selon la valeur de T. Ceci permet de prouver numériquement le lemme pour $n \geqslant 4$. Cependant, cela nécessite de calculer pour certaines valeurs de t la quantité $\mathbf{P}(G > t)$ qui fait intervenir une intégrale impropre, ce qu'il est possible d'éviter ici. En effet des inégalités très précises sont connues pour la fonction $\mathbf{P}(G > t)$. Il a par exemple été démontré dans [RW] que pour tout $t \geqslant 0$,

$$\mathbf{P}(G > t) \geqslant \frac{1}{\sqrt{2\pi}} e^{-t^2/2} \frac{\pi}{(\pi - 1)t + \sqrt{t^2 + 2\pi}}.$$

On vérifie alors numériquement que cette inégalité, couplée au choix

$$T = \sqrt{2 \log n - 3/2},$$

permet de conclure pour $n \geqslant 4$.

Si $n = 2$ ou $n = 3$, on utilise le lemme suivant dû à Sidak (voir par exemple [SW, SSZ]) : si $(X_i)_{1 \leqslant i \leqslant n}$ est un vecteur gaussien et si $(Y_i)_{1 \leqslant i \leqslant n}$ est un n-uplet de variables gaussiennes indépendantes telles que pour chaque i, Y_i a même loi que X_i, alors

$$\mathbf{E} \max_{1 \leqslant i \leqslant n} |X_i| \leqslant \mathbf{E} \max_{1 \leqslant i \leqslant n} |Y_i|$$

On vérifie ainsi numériquement que la conclusion du lemme est également vraie si $n = 2$ ou $n = 3$.

$\square$

Remarquons que pour $n \geqslant 4$ on a en fait prouvé le résultat suivant, qui est plus fort que la conclusion du lemme : si $n \geqslant 4$ et si $(Y_i)_{1 \leqslant i \leqslant 2n}$ sont des variables aléatoires gaussienes telles que pour tout $1 \leqslant i \leqslant 2n$ on a $\mathbf{E} Y_i^2 \leqslant 1$, alors

$$\mathbf{E} \max_{1 \leqslant i \leqslant 2n} Y_i \leqslant \sqrt{2 \log n}. \tag{3.17}$$

Cette propriété plus forte n'est pas vraie pour $n = 2$ ou $n = 3$: en effet si l'on ne suppose pas que la famille (Y_i) est un vecteur gaussien, la quantité $\mathbf{E} \max Y_i$ est maximale quand les variables aléatoires $(Y_i)_{1 \leqslant i \leqslant 2n}$ sont de variance 1 et telles que les événements $\{Y_i > \alpha_{1/2n}\}_{1 \leqslant i \leqslant 2n}$ forment une partition de l'espace probabilisé sous-jacent, où α_t l'unique nombre réel tel que $\mathbf{P}(G > t) = \alpha_t$. Sur cet exemple l'inégalité (3.17) est fausse pour $n = 2$ ou $n = 3$.

3.3.4 Preuve du lemme 20

Rappelons l'énoncé du lemme 20 :

Soient $K \subset B_2^n \subset \mathbf{R}^n$ et $K' \subset B_2^{n'} \subset \mathbf{R}^{n'}$ des corps convexes, l'un d'entre eux étant l'enveloppe convexe d'une partie de la sphère-unité correspondante. Alors

$$w_G(K \hat{\otimes} K') \leqslant w_G(K) + w_G(K').$$

Par conséquent, en termes de la largeur moyenne usuelle,

$$w(K \hat{\otimes} K') \leqslant \frac{\gamma_n}{\gamma_{nn'}} w(K) + \frac{\gamma_{n'}}{\gamma_{nn'}} w(K') \leqslant \frac{w(K)}{\sqrt{n'}} + \frac{w(K')}{\sqrt{n}},$$

Démonstration. La preuve est similaire à celle de la partie 2.3 de [DS]. L'ingrédient principal en est la version suivante du lemme de Slepian :

Lemme 30. *Soit $(X_t)_{t \in T}$ et $(Y_t)_{t \in T}$ deux vecteurs gaussiens, indexés par le même ensemble fini T et vérifiant l'hypothèse*

$$\forall t, u \in T, \ \ \mathbf{E}(X_t - X_u)^2 \leqslant \mathbf{E}(Y_t - Y_u)^2$$

Alors

$$\mathbf{E} \max_{t \in T} X_t \leqslant \mathbf{E} \max_{t \in T} Y_t$$

Supposons par exemple que $\operatorname{ext}(K) \subset S^{n-1}$ (la situation est évidemment symétrique en K et K'). On applique le lemme 30 avec $T = \operatorname{ext}(K) \times \operatorname{ext}(K')$ et les processus X et Y définis par

$$X_{(t,t')} = \langle G_{\mathbf{R}^n \otimes \mathbf{R}^{n'}}, t \otimes t' \rangle$$

$$Y_{(t,t')} = \langle G_{\mathbf{R}^n}, t \rangle + \langle G_{\mathbf{R}^{n'}}, t' \rangle$$

L'espace T n'est pas fini ; il est néanmoins compact et on applique en réalité le lemme 30 à toutes les parties finies de T, voir [Fer] pour plus de précisions. Il faut vérifier que l'hypothèse du lemme est vraie, c'est-à-dire prouver l'inégalité :

$$\forall t, u \in S^{n-1}, \ \forall t', u' \in B_2^{n'}, \ \ |t \otimes t' - u \otimes u'|^2 \leqslant |t - u|^2 + |t' - u'|^2$$

En utilisant le fait que $|t|^2 = |u|^2 = 1$, cela équivaut à

$$\langle t, u \rangle + \langle t', u' \rangle \leqslant 1 + \langle t, u \rangle \langle t', u' \rangle$$

qui est bien vérifiée pour des vecteurs de norme inférieure à 1. Ceci prouve donc la conclusion du lemme 20 sur les largeurs moyennes gaussiennes. Il reste à prouver l'inégalité $\gamma_n/\gamma_{nn'} \leqslant 1/\sqrt{n'}$, qui est une conséquence du fait que la suite $(\gamma_k/\sqrt{k})$ est croissante. Pour voir ce dernier point, définissons la fonction h sur $\mathbf{R}^+$ par

$$h(y) = \frac{\Gamma(y+1/2)}{\sqrt{y}\Gamma(y)}$$

La dérivée logarithmique de h vaut

$$(\log h)'(y) = \digamma(y+1/2) - \digamma(y) - \frac{1}{2y}$$

où $\digamma$ (« digamma ») est la dérivée logarithmique de la fonction Γ : $\digamma = (\log \Gamma)'$. Le fait que $(\log h)'$ est strictement positif sur $\mathbf{R}^+$ découle de l'inégalité suivante, prouvée dans [Luk]

$$\forall y > 0;\ y(\digamma(y+1/2) - \digamma(y)) \geqslant \frac{2y+1}{4y+1} > \frac{1}{2}$$

Ainsi la fonction h est croissante, et on conclut en remarquant que pour $k \in 2\mathbf{N}$, $h(k/2) = \gamma_k/\sqrt{k}$. $\square$

Bibliographie

[Ale] Alesker, S. ψ_2-estimate for the Euclidean norm on a convex body in isotropic position. In *Geometric aspects of functional analysis (Israel, 1992–1994)*, vol. 77 of *Oper. Theory Adv. Appl.* Birkhäuser, Basel, 1995, pp. 1–4.

[AKM] Artstein, S., Klartag, B. et Milman, V. The Santaló point of a function, and a functional form of Santaló inequality. *Mathematika* (à paraître).

[Aub1] Aubrun, G. A sharp small deviation inequality for the largest eigenvalue of a random matrix. In *Séminaire de Probabilités XXXVIII*, vol. 1857 of *Lecture Notes in Math.* Springer, Berlin, 2005, pp. 320–337.

[Aub2] Aubrun, G. Sampling convex bodies : a random matrix approach `http://www.institut.math.jussieu.fr/~aubrun/sampling.dvi`, 2003.

[Bai] Bai, Z. D. Methodologies in spectral analysis of large-dimensional random matrices, a review. *Statist. Sinica 9*, 3 (1999), 611–677. Avec des commentaires de G. J. Rodgers et Jack W. Silverstein, et une réponse de l'auteur.

[BY] Bai, Z. D. et Yin, Y. Q. Limit of the smallest eigenvalue of a large-dimensional sample covariance matrix. *Ann. Probab. 21*, 3 (1993), 1275–1294.

[Bal] Ball, K. An elementary introduction to modern convex geometry. In *Flavors of geometry*, vol. 31 of *Math. Sci. Res. Inst. Publ.* Cambridge Univ. Press, Cambridge, 1997, pp. 1–58.

[Bar] Barthe, F. On a reverse form of the Brascamp-Lieb inequality. *Invent. Math. 134*, 2 (1998), 335–361.

[BGMN] Barthe, F., Guédon, O., Mendelson, S. et Naor, A. A probabilistic approach to the geometry of the l_p^n-ball. *Ann. Probab. 33*, 2 (2005), 480–513.

[BN1] Bobkov, S. G. et Nazarov, F. L. On convex bodies and log-concave probability measures with unconditional basis. In *Geometric* *aspects of functional analysis*, vol. 1807 of *Lecture Notes in Math.* Springer, Berlin, 2003, pp. 53–69.

[BN2] Bobkov, S. G. et Nazarov, F. L. Large deviations of typical linear functionals on a convex body with unconditional basis. *Progress in Probability 56* (2003), 3–13.

[Bor] Borell, C. Convex set functions in d-space. *Period. Math. Hungar. 6*, 2 (1975), 111–136.

[Bou] Bourgain, J. Random points in isotropic convex sets. In *Convex geometric analysis (Berkeley, CA, 1996)*, vol. 34 of *Math. Sci. Res. Inst. Publ.* Cambridge Univ. Press, Cambridge, 1999, pp. 53–58.

[BLM] Bourgain, J., Lindenstrauss, J. et Milman, V. D. Minkowski sums and symmetrizations. In *Geometric aspects of functional analysis (1986/87)*, vol. 1317 of *Lecture Notes in Math.* Springer, Berlin, 1988, pp. 44–66.

[BC] Braunstein, S. L. et Caves, C. M. Statistical distance and the geometry of quantum states. *Phys. Rev. Lett. 72*, 22 (1994), 3439–3443.

[CG] Cerf, N. et Gisin, N. L'étrange pouvoir de l'intrication quantique. *La Recherche, hors-série 18* (2005), 84–89.

[DS] Davidson, K. R. et Szarek, S. J. Local operator theory, random matrices and Banach spaces. In *Handbook of the geometry of Banach spaces, Vol. I,* 317–366*, Vol. II,* 1819–1820. North-Holland, Amsterdam, 2001.

[Dud] Dudley, R. M. *Real analysis and probability.* The Wadsworth & Brooks/Cole Mathematics Series. Wadsworth & Brooks/Cole Advanced Books & Software, Pacific Grove, CA, 1989.

[Fer] Fernique, X. *Fonctions aléatoires gaussiennes, vecteurs aléatoires gaussiens*. Université de Montréal Centre de Recherches Mathématiques, Montreal, QC, 1997.

[For] Forrester, P. J. The spectrum edge of random matrix ensembles. *Nuclear Phys. B 402*, 3 (1993), 709–728.

[Gar] Gardner, R. J. The Brunn-Minkowski inequality. *Bull. Amer. Math. Soc. (N.S.) 39*, 3 (2002), 355–405 (électronique).

[Gem] Geman, S. A limit theorem for the norm of random matrices. *Ann. Probab. 8*, 2 (1980), 252–261.

[Gia] Giannopoulos, A. Notes on isotropic convex bodies. `http://eudoxos.math.uoa.gr/~apgiannop/isotropic-bodies.ps`, 2003.

[GHT] Giannopoulos, A., Hartzoulaki, M. et Tsolomitis, A. Random points in isotropic unconditional convex bodies. *Journal of the London Mathematical Society* (à paraître).

[GM] Giannopoulos, A. A. et Milman, V. D. Concentration property on probability spaces. *Adv. Math. 156*, 1 (2000), 77–106.

[GG] Gohberg, I. et Goldberg, S. *Basic operator theory.* Birkhäuser Boston, Mass., 1981.

[GGK] Gohberg, I., Goldberg, S. et Krupnik, N. *Traces and determinants of linear operators*, vol. 116 of *Operator Theory : Advances and Applications*. Birkhäuser Verlag, Basel, 2000.

[GP] Guédon, O. et Paouris, G. Concentration of mass on the schatten classes. Prépublication.

[GB1] Gurvits, L. et Barnum, H. Largest separable balls around the maximally mixed bipartite quantum state. *Phys. Rev. A 66* (2002).

[GB2] Gurvits, L. et Barnum, H. Separable balls around the maximally mixed multipartite quantum states. `quant-ph/0302102`, 2003.

[GB3] Gurvits, L. et Barnum, H. Better bound on the exponent of the radius of the multipartite separable ball. `quant-ph/0409095`, 2004.

[HT] Haagerup, U. et Thorbjørnsen, S. Random matrices with complex Gaussian entries. *Expo. Math. 21*, 4 (2003), 293–337.

[Hen] Hensley, D. Slicing convex bodies—bounds for slice area in terms of the body's covariance. *Proc. Amer. Math. Soc. 79*, 4 (1980), 619–625.

[HHH1] Horodecki, M., Horodecki, P. et Horodecki, R. Separability of mixed states : necessary and sufficient conditions. *Phys. Lett. A 223*, 1-2 (1996), 1–8.

[HHH2] Horodecki, M., Horodecki, P. et Horodecki, R. Mixed-state entanglement and quantum communication. In *Quantum Information : An Introduction to Basic Theoretical Concepts and Experiments*, Springer Tracts in Modern Physics. Springer, Berlin, 2001.

[Joh] Johnstone, I. M. On the distribution of the largest eigenvalue in principal components analysis. *Ann. Statist. 29*, 2 (2001), 295–327.

[KLS] Kannan, R., Lovász, L. et Simonovits, M. Random walks and an $O^*(n^5)$ volume algorithm for convex bodies. *Random Structures Algorithms 11*, 1 (1997), 1–50.

[KSC] Kolchin, V. F., Sevast′yanov, B. A. et Chistyakov, V. P. *Random allocations.* V. H. Winston & Sons, Washington, D.C., 1978. Traduit du russe, Traduction éditée par A. V. Balakrishnan, Scripta Series in Mathematics.

[Kwa] KWAPIEŃ, S. A remark on the median and the expectation of convex functions of Gaussian vectors. In *Probability in Banach spaces, 9 (Sandjberg, 1993)*, vol. 35 of *Progr. Probab.* Birkhäuser Boston, Boston, MA, 1994, pp. 271–272.

[Led1] LEDOUX, M. *The concentration of measure phenomenon*, vol. 89 of *Mathematical Surveys and Monographs.* American Mathematical Society, Providence, RI, 2001.

[Led2] LEDOUX, M. A remark on hypercontractivity and tail inequalities for the largest eigenvalues of random matrices. In *Séminaire de Probabilités XXXVII*, vol. 1832 of *Lecture Notes in Math.* Springer, Berlin, 2003, pp. 360–369.

[Led3] LEDOUX, M. Deviations inequalities on largest eigenvalues. `http://www.lsp.ups-tlse.fr/Ledoux/Jerusalem.pdf`, 2005.

[LQ] LI, D. ET QUEFFÉLEC, H. Introduction à l'étude des espaces de Banach. Analyse et probabilités. Société mathématique de France, 2004.

[LPRT] LITVAK, A., PAJOR, A., RUDELSON, M. ET TOMCZAK-JAEGERMANN, N. Smallest singular value of random matrices and geometry of random polytopes. *Advances in mathematics* (à paraître).

[Luk] LUKE, Y. L. Inequalities for the gamma function and its logarithmic derivative. *Math. Balkanica 2* (1972), 118–123.

[MaPa] MARČENKO, V. A. ET PASTUR, L. A. Distribution of eigenvalues in certain sets of random matrices. *Mat. Sb. (N.S.) 72 (114)* (1967), 507–536.

[Mec] MECKES, M. W. Concentration of norms and eigenvalues of random matrices. *J. Funct. Anal. 211*, 2 (2004), 508–524.

[Meh] MEHTA, M. L. *Random matrices*, second ed. Academic Press Inc., Boston, MA, 1991.

[MePa] MENDELSON, S. ET PAJOR, A. On singular values of matrices with independent rows. Prépublication.

[MPT] MENDELSON, S., PAJOR, A. ET TOMCZAK-JAEGERMANN, N. Reconstruction and subgaussian processes. Prépublication.

[MiPa1] MILMAN, V. D. ET PAJOR, A. Isotropic position and inertia ellipsoids and zonoids of the unit ball of a normed n-dimensional space. In *Geometric aspects of functional analysis (1987–88)*, vol. 1376 of *Lecture Notes in Math.* Springer, Berlin, 1989, pp. 64–104.

[MiPa2] MILMAN, V. D. ET PAJOR, A. Entropy and asymptotic geometry of non-symmetric convex bodies. *Adv. Math. 152*, 2 (2000), 314–335.

[MS] MILMAN, V. D., AND SCHECHTMAN, G. *Asymptotic theory of finite-dimensional normed spaces*, vol. 1200 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1986. With an appendix by M. Gromov.

[NC] NIELSEN, M. A. ET CHUANG, I. L. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.

[Olv] OLVER, F. W. J. *Asymptotics and special functions*. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], New York-London, 1974. Computer Science and Applied Mathematics.

[OP] ORAVECZ, F. ET PETZ, D. On the eigenvalue distribution of some symmetric random matrices. *Acta Sci. Math. (Szeged) 63*, 3-4 (1997), 383–395.

[PP] PAJOR, A. ET PASTUR, L. Communication personnelle.

[Pao] PAOURIS, G. Concentration of mass and central limit properties of isotropic convex bodies. *Proc. Amer. Math. Soc. 133*, 2 (2005), 565–575 (électronique).

[Per] PERES, A. Separability criterion for density matrices. *Phys. Rev. Lett. 77*, 8 (1996), 1413–1415.

[Pis] PISIER, G. *The volume of convex bodies and Banach space geometry*, vol. 94 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1989.

[Pré] PRÉKOPA, A. On logarithmic concave measures and functions. *Acta Sci. Math. (Szeged) 34* (1973), 335–343.

[RR] RACHEV, S. T. ET RÜSCHENDORF, L. *Mass transportation problems. Vol. I.* Probability and its Applications (New York). Springer-Verlag, New York, 1998. Theory.

[RS] ROGERS, C. A. ET SHEPHARD, G. C. Convex bodies associated with a given convex body. *J. London Math. Soc. 33* (1958), 270–281.

[Rud] RUDELSON, M. Random vectors in the isotropic position. *J. Funct. Anal. 164*, 1 (1999), 60–72.

[RMNDMC] RUNGTA, P., MUNRO, W., NEMOTO, K., DEUAR, P., MILBURN, G. ET CAVES, C. Qudit entanglement. In *Dan Walls Memorial Volume*. Springer, Berlin, 2000. `quant-ph/0001075`.

[RW] RUSKAI, M. B. ET WERNER, E. A Pair of Optimal Inequalities Related to the Error Function. `quant-ph/9711207`, 1997.

[SSZ] SCHECHTMAN, G., SCHLUMPRECHT, T. ET ZINN, J. On the Gaussian measure of the intersection. *Ann. Probab. 26* (1998), 346–357.

[Sie] SIERPIŃSKI, W. Sur la question de la mesurabilité de la base de M. Hamel. *Fund. Math. 1* (1920), 105–111.

[Sim] SIMON, B. Notes on infinite determinants of Hilbert space operators. *Advances in Math. 24*, 3 (1977), 244–273.

[Smi] SMITHIES, F. *Integral equations*. Cambridge Tracts in Mathematics and Mathematical Physics, no. 49. Cambridge University Press, New York, 1958.

[Sod] SODIN, S. On the smallest singular value of a bernoulli random matrix (following Bai and Yin). Appendice d'une prépublication de Artstein-Friedland-Milman "More geometric applications of Chernoff inequalities", 2005.

[Sos] SOSHNIKOV, A. Universality at the edge of the spectrum in Wigner random matrices. *Comm. Math. Phys. 207*, 3 (1999), 697–733.

[Sve] SVETLICHNY, G. On the Foundations of Experimental Statistical Sciences. `www.mat.puc-rio.br/~svetlich/files/statsci.pdf`, 1979.

[Sza] SZAREK, S. Volume of separable states is super-doubly-exponentially small in the number of qubits. *Phys. Rev. A* (à paraître).

[ST] SZAREK, S. ET TOMCZAK-JAEGERMANN, N. On nearly Euclidean decomposition for some classes of Banach spaces. *Compositio Math. 40*, 3 (1980), 367–385.

[SW] SZAREK, S. ET WERNER, E. A nonsymmetric correlation inequality for Gaussian measure. *J. Multivariate Anal. 68* (1999), 193–211.

[Sze] SZEGŐ, G. *Orthogonal polynomials*, third ed. American Mathematical Society, Providence, R.I., 1967. American Mathematical Society Colloquium Publications, Vol. 23.

[Tal] TALAGRAND, M. *Spin glasses : a challenge for mathematicians*, vol. 46 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, 2003. Cavity and mean field models.

[Tom] TOMCZAK-JAEGERMANN, N. *Banach-Mazur distances and finite-dimensional operator ideals*, vol. 38 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*. Longman Scientific & Technical, Harlow, 1989.

[TW1] TRACY, C. A. ET WIDOM, H. Level-spacing distributions and the Airy kernel. *Comm. Math. Phys. 159*, 1 (1994), 151–174.

[TW2] TRACY, C. A. ET WIDOM, H. On orthogonal and symplectic matrix ensembles. *Comm. Math. Phys. 177*, 3 (1996), 727–754.

[Ver] Vershynin, R. Frame expansions with erasures : an approach through the non-commutative operator theory. *Appl. Comput. Harmon. Anal. 18*, 2 (2005), 167–176.

[YBK] Yin, Y. Q., Bai, Z. D. et Krishnaiah, P. R. On the limit of the largest eigenvalue of the large-dimensional sample covariance matrix. *Probab. Theory Related Fields 78*, 4 (1988), 509–521.

[ŻHSL] Życzkowski, K., Horodecki, P., Sanpera, A. et Lewenstein, M. On the volume of the set of mixed entangled states. *Phys. Rev. A 58* (1998), 883–892.

[ŻS] Życzkowski, K. et Sommers, H.-J. Hilbert-schmidt volume of the set of mixed quantum states. *J. Phys. A : Math. Gen. 36* (2003), 10115–10130.