SAMPLING CONVEX BODIES: A RANDOM MATRIX APPROACH

GUILLAUME AUBRUN

Abstract. We prove the following result: for any $\varepsilon > 0$, only $C(\varepsilon)n$ sample points are enough to obtain $(1+\varepsilon)$-approximation of the inertia ellipsoid of an unconditional convex body in $\mathbf{R}^n$. Moreover, for any $\rho > 1$, already ρn sample points give isomorphic approximation of the inertia ellipsoid. The proofs rely on an adaptation of the moments method from the Random Matrix Theory.

Warning: this version differs from the (to be) published one (the proof of the main theorem is actually slightly simpler here).

1. Introduction and the main results

Notation kept throughout the paper: The letters C, c, C'... denote absolute positive constants, notably independent of the dimension. The value of such constants may change from line to line. Similarly, $C(\varepsilon)$ denotes a constant depending only on the parameter ε. The canonical basis of $\mathbf{R}^n$ is $(e_1, \ldots, e_n)$, and the Euclidean norm and scalar product are denoted by $|\cdot|$ and $\langle\cdot,\cdot\rangle$. The operator norm of a matrix is denoted by $\|\cdot\|$. For a real symmetric matrix A, we write $\lambda_{\max}(A)$ (respectively $\lambda_{\min}(A)$) for the largest (respectively smallest) eigenvalue of A. A *convex body* is a convex compact subset of $\mathbf{R}^n$ with non-empty interior. A convex body K is said to be *unconditional* if it is invariant under sign flips of the coordinates: for any $\eta = (\eta_1, \ldots, \eta_n) \in \{-1, 1\}^n$,

$$(x_1, \ldots, x_n) \in K \Longleftrightarrow (\eta_1 x_1, \ldots, \eta_n x_n) \in K.$$

We reserve the letters X, Y to denote an $\mathbf{R}^n$-valued random vector; $X_1, \ldots, X_N$ are i.i.d. copies of X. If $\mathbf{E}X = 0$, X is said to be *centered*. The random vector X is said to be *isotropic* if it is centered and for all $y \in \mathbf{R}^n$

$$\mathbf{E}\langle X, y\rangle^2 = |y|^2.$$

This is equivalent to the *inertia matrix* $\mathbf{E}X \otimes X$ being is the identity matrix. We will consider the special case when X is uniformly distributed on a convex body K. We will then say "inertia matrix of K", "K is isotropic[1]"... for "inertia matrix of X", "X is isotropic"... . The *inertia ellipsoid* of K is the unique ellipsoid with the same inertia matrix as K. For recent results on isotropic convex bodies, a good reference is the survey [9]. Any random vector has an affine image which is isotropic, and this image is unique up to orthogonal transformation. Thus, for affinely invariant problems we can restrict ourselves to isotropic random vectors. If we do not know the law but only N samples of the random vector X, we can only consider the *empirical inertia matrix*

$$A^N(X) := \frac{1}{N}\sum_{i=1}^{N} X_i \otimes X_i.$$

1991 *Mathematics Subject Classification.* Primary 15A52,52A20.

Key words and phrases. Isotropic, random matrix, convex body, moments method.

Research was supported in part by the European Network PHD, FP6 Marie Curie Actions, MCRN-511953 and was done in part while the author was visiting the University of Athens.

[1]This terminology slightly differs from [16, 9] where isotropic convex bodies are normalized to have volume 1.

The matrices $A^N(X)$ tend almost surely to the identity matrix when N tends to infinity; a natural question is to quantify this convergence. This problem was considered with algorithmic motivations by Kannan, Lovász and Simonovits [12] in the case when X is uniformly distributed on a convex body. It was proved in [12] that $\|A^N(X)-\mathrm{Id}\| \leqslant \varepsilon$ with probability larger than $1-\varepsilon$ provided $N \geqslant C(\varepsilon)n^2$. This was improved by Bourgain [6] to $N \geqslant C(\varepsilon)n\log^3 n$ and later by Rudelson [20] to $N \geqslant C(\varepsilon)n\log^2 n$. Rudelson proved actually the following inequality, valid for a general random vector.

Theorem (Rudelson's inequality)**.** *For any isotropic random vector X we have*

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

provided the right-hand side is smaller than 1.

If X is uniformly distributed on an isotropic convex body, then it satisfies

$$(\mathbf{E}|X|^p)^{1/p} \leqslant C\sqrt{n} \quad \text{for} \quad 2 \leqslant p \leqslant c\sqrt{n}. \tag{2}$$

This estimate was proved by Bobkov and Nazarov [4] for unconditional convex bodies and recently extended by Paouris [18] to general isotropic bodies. When plugged in Rudelson's inequality, it yields that if $N \geqslant C(\varepsilon)n\log n$, we have $\|A^N(X)-\mathrm{Id}\| \leqslant \varepsilon$ with probability larger than $1-\varepsilon$ (see [10, 18]). On the other hand, when X is isotropic we have $\mathbf{E}|X|^2 = n$ and consequently we must take N larger than $cn\log n$ to use Rudelson's inequality. Note that this value $N \sim n\log n$ is sharp for some discrete examples. The simplest is given by the isotropic random vector Y uniformly distributed on the (properly normalized) vertices of the cross-polytope

$$\{\pm\sqrt{n}e_1, \dots, \pm\sqrt{n}e_n\}.$$

The matrix $A^N(Y)$ is then diagonal and its diagonal coefficients are distributed as

$$\frac{n}{N}\left(p_1, \dots, p_n\right),$$

where p_i denote the number of balls falling in the ith urn when we put randomly, uniformly and independently N balls in n urns. This problem, known as the random allocation problem, is well-studied and it is known (see [13], chapter 2.6) than we must take $N \geqslant c(\varepsilon)n\log n$ in order to get $\max(p_i) \leqslant (1+\varepsilon)\min(p_i)$ with probability larger than $\frac{1}{2}$.

We prove that for the class of unconditional convex bodies, it is possible to go below this bound of $n\log n$ and to take N proportional to n

Theorem 1. *There are absolute constants C, c such that the following holds. Let $0 < \varepsilon \leqslant 1$. Let X be uniformly distributed on an unconditional isotropic convex body in $\mathbf{R}^n$. Then for $N \geqslant Cn/\varepsilon^2$, we have with probability larger than $1-\exp(-cn^{1/5})$*

$$\|A^N(X)-\mathrm{Id}\| \leqslant \varepsilon.$$

In other words, for every y in $\mathbf{R}^n$

$$(1-\varepsilon)|y|^2 \leqslant \frac{1}{N}\sum_{i=1}^N \langle X_i, y\rangle^2 \leqslant (1+\varepsilon)|y|^2. \tag{3}$$

We can also obtain the isomorphic analogue of theorem 1, using as few sample points as possible

Theorem 2. *Let $\rho > 1$ and $N \geqslant \rho n$. Let X be uniformly distributed on an unconditional isotropic convex body in $\mathbf{R}^n$. Then, with probability larger than $1 - 2\exp(-c(\rho)n^{1/5})$ we have for every y in $\mathbf{R}^n$*

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

Question 1. *Do both results extend to all isotropic convex bodies ?*

Remark. *With slight modifications of the proofs, one can prove the same results for all isotropic random vectors with a law being log-concave and unconditional.*

2. The random matrix approach: auxiliary results and the structure of the proof

Our proof uses standard techniques from Random Matrix Theory (RMT). A part of the classical random matrix theory deals with random vectors X with i.i.d. coordinates. Here is a reformulation of a result of Bai and Yin [2]

Theorem (Bai–Yin)**.** *Let Z be a random variable with mean 0, variance 1 and finite fourth moment. Let $X^{(n)}$ be a random vector on $\mathbf{R}^n$ whose coordinates are i.i.d. copies of Z. We consider a sequence of integers (N_n) tending to infinity in such a way that the ratio n/N_n tends to a limit $\beta \in (0,1)$. Then, almost surely,*

$$\lim_{n\to\infty} \lambda_{\max}\left(A^{N_n}(X^{(n)})\right) = (1+\sqrt{\beta})^2,$$

$$\lim_{n\to\infty} \lambda_{\min}\left(A^{N_n}(X^{(n)})\right) = (1-\sqrt{\beta})^2.$$

This theorem is restricted to random vectors with independent coordinates. Moreover, as often in RMT, this is a limit-result. Therefore it may be hard to use to get a result in a fixed dimension. In a few cases, quantified analogues (sometimes called *localized*) of limit-theorems from RMT have been proved; see [14]. For Bai–Yin theorem, this has been done by S. Sodin in the special case of random signs [21], but we still lack a quantified version for general entries. Bai and Yin proved their theorem as a consequence of the following result

$$\limsup_{n\to\infty} \left\| A^{N_n}(X^{(n)}) - (1+\beta)\mathrm{Id} \right\| \leqslant 2\sqrt{\beta} \quad \text{a.s.} \tag{4}$$

We follow an similar approach, except that we will rather estimate

$$\left\| A^{N_n}(X^{(n)}) - \mathrm{Id} \right\|. \tag{5}$$

When $\beta \ll 1$, the quantities involved in (4) and (5) are comparable. This is no longer true when β becomes large (i.e. when matrices involved become close to being square matrices). Because of $\lambda_{\max}$, it is even impossible to obtain from (5) any non-trivial information on $\lambda_{\min}$ when β is larger than $3 - 2\sqrt{2} \approx 0.172$.

In this framework, the expected norm of a self-adjoint random matrix A is usually bounded from above by $(\mathbf{E}\mathrm{tr}A^k)^{1/k}$, for even integer k (usually large, but not very large). We are led to some combinatorial problems to estimate $\mathbf{E}\mathrm{tr}A^k$. This is the so-called *moments method* initiated by Wigner. The main advantage of considering (5) rather than (4) is that the combinatorics involved are simpler. We prove the following proposition.

Proposition 1. *Let X be a random vector uniformly distributed on an unconditional convex body in $\mathbf{R}^n$, and (X_i) be i.i.d. copies of X. We write A for $A^N(X)$, the empirical inertia matrix of X with $N \geqslant n$ sample points. For $k = n^{1/5}$, we have*

$$\left(\mathbf{E}\|A - \mathrm{Id}\|^k\right)^{1/k} \leqslant C\sqrt{\frac{n}{N}}, \tag{6}$$

where C is a universal constant.

We postpone the proof of proposition 1 to section 3. Then, the lower estimate in theorem 2 is proved using the Laplace transform technique from [15] (see section 4).

Remark. *A natural question is whether the Bai–Yin theorem can be extended to random vectors uniformly distributed on convex bodies. This question needs sharper tools than the problem which is treated here. The author obtained an affirmative answer for the case of the unit ball of ℓ_p^n* [1].

We now show how proposition 1 implies the theorems

Proof of theorem 1. We write $A = A^N(X)$. Let $N \geqslant 4C^2 n/\varepsilon^2$, where C is the constant appearing in proposition 1. By proposition 1, for $k = n^{1/5}$ we have $\left(\mathbf{E}\|A - \mathrm{Id}\|^k\right)^{1/k} \leqslant \varepsilon/2$. Markov's inequality now implies that $\mathbf{P}(\|A - \mathrm{Id}\| \geqslant \varepsilon) \leqslant 2^{-k} = \exp(-cn^{1/5})$. □

Proof of theorem 2. We get as a consequence of proposition 1 a good estimate for the largest eigenvalue of A using the inequality $\|A\| \leqslant \|A - \mathrm{Id}\| + 1$ (or alternatively, using the moments method directly on A instead of $A - \mathrm{Id}$): for any $N \geqslant n$

$$\mathbf{P}(\|A\| \geqslant C) \leqslant C\exp(-cn^{1/5}).$$

The smallest eigenvalue is automatically controlled by the following general proposition, proved in section 4. □

Proposition 2. *For every $M > 0$ and $\rho > 1$ there are constants $c = c(M,\rho)$ and $\kappa = \kappa(M,\rho)$ such that, for every random vector X uniformly distributed on an isotropic convex body and any $N \geqslant \rho n$, the empirical inertia matrix $A = A^N(X)$ automatically satisfies*

$$\mathbf{P}\left(\lambda_{\min}(A) \leqslant c\right) \leqslant \mathbf{P}\left(\lambda_{\max}(A) \geqslant M\right) + \exp(-\kappa n).$$

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 this is only an isomorphic result.*

3. Proof of proposition 1: the moments method

Proof of proposition 1. We start with the following standard symmetrization lemma

Lemma 1. *Let (X_i) be i.i.d. copies of an isotropic random vector X. Let (ε_i) be i.i.d. copies of a Bernoulli random variable ($\mathbf{P}(\varepsilon = 1) = \mathbf{P}(\varepsilon = -1) = 1/2$), independent from (X_i). Then for any $k \geqslant 1$,*

$$\mathbf{E}\left\|\frac{1}{N}\sum_{i=1}^N X_i \otimes X_i - \mathrm{Id}\right\|^k \leqslant 2^k \mathbf{E}\left\|\frac{1}{N}\sum_{i=1}^N \varepsilon_i X_i \otimes X_i\right\|^k.$$

Proof of lemma 1. Let (X_i') be an independent copy of the sequence (X_i), also independent from (ε_i). We write respectively $\mathbf{E}$, $\mathbf{E}'$ and $\mathbf{E}_\varepsilon$ for expectations relative to (X_i), (X_i') and (ε_i).

$$\begin{aligned}
\mathbf{E}\left\| \frac{1}{N}\sum_{i=1}^N X_i \otimes X_i - \mathrm{Id} \right\|^k &= \mathbf{E}\left\| \frac{1}{N}\sum_{i=1}^N X_i \otimes X_i - \mathbf{E}'\frac{1}{N}\sum_{i=1}^N X_i' \otimes X_i' \right\|^k \\
&\leqslant \mathbf{E}\mathbf{E}'\left\| \frac{1}{N}\sum_{i=1}^N X_i \otimes X_i - X_i' \otimes X_i' \right\|^k \\
&= \mathbf{E}\mathbf{E}'\mathbf{E}_\varepsilon\left\| \frac{1}{N}\sum_{i=1}^N \varepsilon_i (X_i \otimes X_i - X_i' \otimes X_i') \right\|^k \\
&\leqslant 2^k\mathbf{E}\mathbf{E}_\varepsilon\left\| \frac{1}{N}\sum_{i=1}^N \varepsilon_i X_i \otimes X_i \right\|^k.
\end{aligned}$$

We used Jensen's inequality to obtain the first inequality. □

Let k be an even integer (we will choose later $k \approx n^{1/5}$). We write A for $A^N(X)$. Using lemma 1 and the moments method, we get

$$\begin{aligned}
\mathbf{E}\|A - \mathrm{Id}\|^k &\leqslant 2^k\mathbf{E}\mathrm{tr}\left(\frac{1}{N}\sum_{i=1}^N \varepsilon_i X_i \otimes X_i\right)^k \\
&= \frac{2^k}{N^k}\mathbf{E}\sum_{r_1,\dots,r_k} \varepsilon_{r_1}\dots\varepsilon_{r_k}\langle X_{r_1}, X_{r_2}\rangle \dots \langle X_{r_{k-1}}, X_{r_k}\rangle\langle X_{r_k}, X_{r_1}\rangle \\
&= \frac{2^k}{N^k}\sum_{r_1,\dots,r_k} (\mathbf{E}\varepsilon_{r_1}\dots\varepsilon_{r_k})(\mathbf{E}\langle X_{r_1}, X_{r_2}\rangle \dots \langle X_{r_{k-1}}, X_{r_k}\rangle\langle X_{r_k}, X_{r_1}\rangle).
\end{aligned}$$

The summation runs a priori on multi-indices $(r_1,\dots,r_k) \in \{1,\dots,N\}^k$. However, note that the quantity $\mathbf{E}\varepsilon_{r_1}\dots\varepsilon_{r_k}$ equals 0 or 1, and that it equals 1 if and only if every $i \in \{1,\dots,N\}$ appears an even (possibly 0) number of times among $(r_1,\dots,r_k)$. Call such a multi-index *paired*; we actually sum over paired multi-indices. We write $X_i = (x_{i1},\dots,x_{in})$ for the coordinates of X_i in the canonical basis, and expand the k scalar products as follows

$$\langle X_{r_p}, X_{r_{p+1}}\rangle = \sum_{s_p=1}^n x_{r_p s_p} x_{r_{p+1} s_p}.$$

This yields

$$\mathbf{E}\|A - \mathrm{Id}\|^k \leqslant \frac{2^k}{N^k}\sum_{\substack{r_1,\dots,r_k \text{ paired} \\ s_1,\dots,s_k}} \mathbf{E}x_{r_1 s_1}x_{r_2 s_1}x_{r_2 s_2}x_{r_3 s_2}\dots x_{r_k s_k}x_{r_1 s_k},$$

where the sum is taken over all indices $r_1,\dots,r_k$ in $\{1,\dots,N\}$ and $s_1,\dots,s_k$ in $\{1,\dots,n\}$. We now use unconditionality to show that most of these terms are actually 0. Since the random vectors $(X_1,\dots,X_N)$ are independent, each expectation appearing in the sum can be factorized as the product of N factors of the form

$$\mathbf{E}x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n} \tag{7}$$

for some integers $\alpha_1, \dots, \alpha_n$, where $X = (x_1, \dots, x_n)$. Since the vector X is unconditional, it is invariant under sign flips of coordinates, and this shows that the expectation (7) is zero if one of the α_i is odd. We are led to the following inequality (note that we changed the indexation)

$$\mathbf{E}\|A - \mathrm{Id}\|^k \leqslant \frac{2^k}{N^k} \sum_{[(r_1,s_1),\dots,(r_{2k},s_{2k})]\text{V-graph}} \mathbf{E} x_{r_1 s_1} x_{r_2 s_2} \dots x_{r_{2k-1} s_{2k-1}} x_{r_{2k} s_{2k}},$$

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

(V1) $r_{2i+1} = r_{2i}$ (and $r_1 = r_{2k}$),
(V2) $s_{2i} = s_{2i-1}$,
(V3) Each couple $(r, s) \in \{1, \dots, N\} \times \{1, \dots, n\}$ appears an even (possibly 0) number of times among $[(r_i, s_i)]$,
(V4) The number of occurences of each $r \in \{1, \dots, N\}$ among (r_i) is a multiple of 4 (possibly 0).

Condition (V4) has to be satisfied since we restricted ourself to paired multi-indices. We associate several parameters to a V-graph $G = [(r_1, s_1), \dots, (r_{2k}, s_{2k})]$, following the standard combinatorial techniques of [8, 22]. Let $r(G) = \#\{r_i\}$, $c(G) = \#\{s_i\}$ and $\ell(G) = r(G) + c(G)$; $\ell(G)$ is the number of distinct indices appearing in G. Let also $d(G) = \#\{(r_i, s_i)\}$ be the number of distinct couples of indices that appear in G. 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. We clearly have $n_2(G) + n_+(G) = 2k$.

Lemma 2. *If $G = [(r_1, s_1), \dots, (r_{2k}, s_{2k})]$ is a V-graph then*

$$\mathbf{E} x_{r_1 s_1} \dots x_{r_{2k} s_{2k}} \leqslant C^k k^{n_+(G)}.$$

Proof. First, we use the fact that the vectors (X_i) are independent to write the whole expectation as a product of N factors of the form (7). Note that the sum of all exponents α_i appearing in factors (7) is exactly $2k$, while the sum restricted to the exponents satisfying $\alpha_i \geqslant 4$ is exactly $n_+(G)$. We use the following comparison theorem by Bobkov and Nazarov. Let $B_1^n = \{x \in \mathbf{R}^n \text{ s.t. } \sum |x_j| \leqslant 1\}$ denote the unit ball of ℓ_1^n; the convex body $\alpha_n B_1^n$ is isotropic for $\alpha_n = \sqrt{(n+1)(n+2)/2}$. It has been proved in [4] that for some absolute constant C, if $X = (x_1, \dots, x_n)$ is uniformly distributed on an isotropic unconditional convex body, and if $Y = (y_1, \dots, y_n)$ is uniformly distributed on CnB_1^n, then for any increasing functions $f_i : \mathbf{R}^+ \to \mathbf{R}$

$$\mathbf{E} \prod_{i=1}^n f_i(|x_i|) \leqslant \mathbf{E} \prod_{i=1}^n f_i(|y_i|).$$

On each factor (7), we use this result with $f_i(x) = x^{\alpha_i}$ (recall that α_i is necessarily even). The resulting expectation for Y can then be estimated using sub-independence [3], a special property of ℓ_p^n-balls asserting that for any increasing functions $f_i : \mathbf{R}^+ \to \mathbf{R}$

$$\mathbf{E} \prod_{i=1}^n f_i(|y_i|) \leqslant \prod_{i=1}^n \mathbf{E} f_i(|y_i|).$$

Now, by Borell's lemma (see [5], or [17] p.135), there is an absolute constant C such that $\Psi_1(y_i) \leqslant C$, which means that $\mathbf{E}|y_i|^p \leqslant (Cp)^p$. If $\alpha_i \geqslant 4$, we use the following bound

$$\mathbf{E} y_i^{\alpha_i} \leqslant \left(\mathbf{E} y_i^{n_+(G)} \right)^{\alpha_i / n_+(G)} \leqslant (Cn_+(G))^{\alpha_i} \leqslant (2Ck)^{\alpha_i}.$$

Using this method to bound separately all the factors of the form (7), we are led to

$$\mathbf{E} x_{r_1 s_1} \dots x_{r_{2k} s_{2k}} \leqslant (\mathbf{E} y_1^2)^{n_2(G)/2} (2Ck)^{n_+(G)},$$

and the lemma is proved. □

Applying lemma 2, we obtain the inequality

$$\mathbf{E}\|A-\mathrm{Id}\|^k \leqslant \left(\frac{C}{N}\right)^k \sum_{G \text{ V-graph}} k^{n_+(G)}. \tag{8}$$

We now state some bounds on the parameters associated to a V-graph.

Lemma 3. *Let $G=[(r_1,s_1),\dots,(r_{2k},s_{2k})]$ be a V-graph. Then*

(a) $d(G)\leqslant k$.
(b) $\ell(G)\leqslant d(G)+1\leqslant k+1$.
(c) $r(G)\leqslant k/2$.
(d) $n_+(G)\leqslant 4(k-\ell(G)+1)$.

Proof. Assertion (a) is an immediate consequence of property (V3). To prove (b), read the V-graph from (r_1,s_1) to (r_{2k},s_{2k}). Each of the $d(G)$ first occurences (r_i,s_i) of some couple of indices may bring a new row index or a new column index, but not both (except for $i=1$) because of properties (V1-V2). This shows $\ell(G)\leqslant d(G)+1$, and (b) follows from (a). Assertion (c) is an immediate consequence of property (V3). For (d), note that $d(G)\leqslant \frac{1}{2}n_2(G)+\frac{1}{4}n_+(G)$ (with equality iff no couple (r,s) appears 6 times or more). The result then follows from (b) and the equality $n_2(G)+n_+(G)=2k$. □

We now need a bound on the number of V-graphs with given r and c. This can be done using standard combinatorial techniques developed in [8, 22]. We present here a different approach, suggested to us by S. Szarek, based on the facts that the combinatorics of V-graphs do not depend on the specific entries of the random matrix, and that for Gaussian random matrices very precise information is available.

Lemma 4. *Let $I\subset\{1,\dots,N\}$ and $J\subset\{1,\dots,n\}$, such that $r+c\leqslant k+1$, with $r=\#I$ and $c=\#J$. Then the number of V-graphs $G=[(r_1,s_1),\dots,(r_{2k},s_{2k})]$ such that $\{r_i\}\subset I$ and $\{s_i\}\subset J$ is bounded from above by $(Ck)^k$, for some absolute constant C.*

Proof. We can assume that $I=\{1,\dots,r\}$ and $J=\{1,\dots,c\}$. Let $G_{r,c}=(g_{ij})$ a random $r\times c$ matrix with entries being independent $N(0,1)$ random variables. It is well-known (as a consequence of Slepian's lemma, see [7] chapter 2.3, or using a net argument) that for some absolute constant C, $\mathbf{E}\|G_{r,c}\|\leqslant C(\sqrt{r}+\sqrt{c})\leqslant C'\sqrt{k}$. Moreover, the operator norm is a 1-Lipschitz function with respect to the entries of the matrix (in the Hilbert–Schmidt metric), and standard concentration property of the Gaussian measure ([7], chapter 2.2) implies that for any $t\geqslant 0$

$$\mathbf{P}(\|G_{r,c}\|\geqslant \mathbf{E}\|G_{r,c}\|+t)\leqslant \exp(-t^2/2).$$

This in turn implies that

$$\mathbf{E}\|G_{r,c}\|^{2k}=\int_0^\infty 2kt^{2k-1}\mathbf{P}(\|G_{r,c}\|\geqslant t)dt\leqslant (C\sqrt{k})^{2k}.$$

Also, since $\mathrm{tr}(G_{r,c}^tG_{r,c})^k$ is the sum of $2k$th powers of singular values of $G_{r,c}$, we have

$$\mathbf{E}\mathrm{tr}(G_{r,c}^tG_{r,c})^k\leqslant \min(r,c)\mathbf{E}\|G_{r,c}\|^{2k}\leqslant (C'k)^k.$$

On the other hand, the quantity $\mathbf{E}\mathrm{tr}(G_{r,c}^tG_{r,c})^k$ itself can also be expanded as

$$\mathbf{E}\mathrm{tr}(G_{r,c}^tG_{r,c})^k=\sum \mathbf{E}g_{r_1s_1}\dots g_{r_{2k}s_{2k}},$$

where the sum is taken over $2k$-tuples of pairs $(r_i, s_i) \subset I \times J$ satisfying conditions (V1), (V2), (V3). Notably, all V-graphs considered in the statement of the lemma enter this setting. Moreover, all terms in the sum are positive, and even larger than 1 since $\mathbf{E}g_{ij}^p \geqslant 1$ for p even integer. This shows that the number of V-graphs with indices contained in $I \times J$ is bounded from above by $\mathbf{E}\mathrm{tr}(G_{r,c}^t G_{r,c})^k$, which proves the lemma. □

Lemma 4 implies that the number of V-graphs G such that $r(G) = r$ and $c(G) = c$ is bounded by

$$\binom{N}{r}\binom{n}{c}(Ck)^k \leqslant C_1^k N^r n^c \frac{k^k}{\ell(G)^{\ell(G)}} \leqslant C_2^k N^r n^c k^{k-\ell(G)},$$

where we used the inequalities $\binom{B}{b} \leqslant (Be/b)^b$, $r^r c^c \geqslant (\ell/2)^\ell$ and $k^k/\ell^\ell \leqslant (ke)^{k-\ell}$. By lemma 3c, for any V-graph G we have

$$\begin{aligned} N^{r(G)} n^{c(G)} &\leqslant \begin{cases} N^{\ell(G)} & \text{if } \ell(G) \leqslant k/2, \\ N^{k/2} n^{\ell(G)-k/2} & \text{if } \ell(G) \geqslant k/2, \end{cases} \\ &\leqslant N^k \left(\frac{n}{N}\right)^{k/2} \frac{1}{n^{k-\ell(G)}}. \end{aligned}$$

Gathering the V-graphs with the same ℓ, we get as a consequence of inequality (8) and lemma 3d that (setting $m = l - 1$)

$$\begin{aligned} \mathbf{E}\|A - \mathrm{Id}\|^k &\leqslant \left(\frac{C}{N}\right)^k \sum_{l=2}^{k+1} k^{4(k-l+1)} k C_2^k k^{k-l} N^k \left(\frac{n}{N}\right)^{k/2} \frac{1}{n^{k-l}}, \\ &\leqslant \left(C\sqrt{\frac{n}{N}}\right)^k n \sum_{m=1}^{k} \left(\frac{k^5}{n}\right)^{k-m}. \end{aligned}$$

We now choose k to be the smallest even integer such that $k \geqslant n^{1/5}$. We then use the inequality $n\sum(k^5/n)^{k-m} \leqslant C^k$ to finish the proof (note that the l.h.s. in (6) is an increasing function of k). □

4. Proof of proposition 2: the role of log-concavity

Proof. The proof is similar to the proof of the main theorem in [15], but here the log-concavity makes things much easier. We introduce the matrix Γ defined by

$$\Gamma = \frac{1}{\sqrt{N}} \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_N \end{pmatrix}. \tag{9}$$

We have the equality $A = \Gamma^t \Gamma$; we think of Γ as an operator from ℓ_2^n to ℓ_2^N. We write $s_{\min}(\Gamma)$ for the smallest singular value of Γ, which equals $\sqrt{\lambda_{\min}(A)}$. For $\varepsilon > 0$ to be determined later, let $\mathcal{N}$ be a ε-net in S^{n-1} with cardinality smaller that $(3/\varepsilon)^n$ (existence of such a net is proved using volumetric arguments, see Lemma 4.10 in [19]). Set also $t = \varepsilon\sqrt{M}$. Let $\overline{\Omega}$ be the event "$\|\Gamma\| < \sqrt{M}$". By the standard approximation argument, the event

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

is contained in the event

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

Consequently,

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

For fixed x in the sphere S^{n-1} and j between 1 and N, let f_j be the random variable $\langle X_j, x\rangle$. It is well-known [11, 9] that when K is an isotropic convex body in $\mathbf{R}^n$, the $(n-1)$-dimensional volume of hyperplane sections is controlled: for any affine hyperplane H, we have $\mathrm{vol}_{n-1}(K \cap H) \leqslant C$ for a universal constant C. Consequently, for any $s \geqslant 0$ we have $\mathbf{P}(|f_j| \leqslant s) \leqslant Cs$. Calculations are now straightforward:

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

And consequently

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

thus for any $\rho > 1$, we can choose t (and thus ε) such that the conclusion of the proposition holds. □

Acknowledgement: I want to thank Alain Pajor, Olivier Guédon and Sasha Sodin for many fruitful discussions, and Staszek Szarek for useful remarks on a preliminary version of this paper.

References

[1] G. Aubrun. Random points in the unit ball of ℓ_p^n. http://www.institut.math.jussieu.fr/~aubrun/ellp.ps, 2005.
[2] Z. D. Bai and Y. Q. Yin. Limit of the smallest eigenvalue of a large-dimensional sample covariance matrix. *Ann. Probab.*, 21(3):1275–1294, 1993.
[3] K. Ball and I. Perissinaki. The subindependence of coordinate slabs in ℓ_p^n balls. *Israel J. Math.*, 107:289–299, 1998.
[4] S. G. Bobkov and F. L. Nazarov. Large deviations of typical linear functionals on a convex body with unconditional basis. In *Stochastic inequalities and applications*, volume 56 of *Progr. Probab.*, pages 3–13. Birkhäuser, Basel, 2003.
[5] C. Borell. The Brunn-Minkowski inequality in Gauss space. *Invent. Math.*, 30(2):207–216, 1975.
[6] J. Bourgain. Random points in isotropic convex sets. In *Convex geometric analysis (Berkeley, CA, 1996)*, volume 34 of *Math. Sci. Res. Inst. Publ.*, pages 53–58. Cambridge Univ. Press, Cambridge, 1999.
[7] K. R. Davidson and S. J. Szarek. Local operator theory, random matrices and Banach spaces. In *Handbook of the geometry of Banach spaces, Vol. I*, pages 317–366. North-Holland, Amsterdam, 2001.
[8] S. Geman. A limit theorem for the norm of random matrices. *Ann. Probab.*, 8(2):252–261, 1980.

[9] A. Giannopoulos. Notes on isotropic convex bodies (preprint). `http://eudoxos.math.uoa.gr/~apgiannop/isotropic-bodies.ps`, 2003.

[10] A. Giannopoulos, M. Hartzoulaki, and A. Tsolomitis. Random points in isotropic unconditional convex bodies. *Journal of the London Mathematical Society*, to appear.

[11] D. Hensley. Slicing convex bodies—bounds for slice area in terms of the body's covariance. *Proc. Amer. Math. Soc.*, 79(4):619–625, 1980.

[12] R. Kannan, L. Lovász, and M. Simonovits. Random walks and an $O^*(n^5)$ volume algorithm for convex bodies. *Random Structures Algorithms*, 11(1):1–50, 1997.

[13] V. F. Kolchin, B. A. Sevast′yanov, and V. P. Chistyakov. *Random allocations*. V. H. Winston & Sons, Washington, D.C., 1978. Translated from Russian, translation edited by A. V. Balakrishnan, Scripta Series in Mathematics.

[14] M. Ledoux. Deviations inequalities on largest eigenvalues. `http://www.lsp.ups-tlse.fr/Ledoux/Jerusalem.pdf`, 2005.

[15] A. Litvak, A. Pajor, M. Rudelson, and N. Tomczak-Jaegermann. Smallest singular value of random matrices and geometry of random polytopes. *Advances in mathematics*, to appear.

[16] V. D. Milman and A. Pajor. 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)*, volume 1376 of *Lecture Notes in Math.*, pages 64–104. Springer, Berlin, 1989.

[17] V. D. Milman and G. Schechtman. *Asymptotic theory of finite-dimensional normed spaces*, volume 1200 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1986. With an appendix by M. Gromov.

[18] G. Paouris. Concentration of mass on isotropic convex bodies. *C. R. Math. Acad. Sci. Paris*, 2005. To appear.

[19] G. Pisier. *The volume of convex bodies and Banach space geometry*, volume 94 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1989.

[20] M. Rudelson. Random vectors in the isotropic position. *J. Funct. Anal.*, 164(1):60–72, 1999.

[21] S. Sodin. On the smallest singular value of a Bernoulli random matrix (following Bai and Yin). Appendix to a preprint by Artstein–Friedland–Milman "More geometric applications of Chernoff inequalities".

[22] Y. Q. Yin, Z. D. Bai, and P. R. Krishnaiah. On the limit of the largest eigenvalue of the large-dimensional sample covariance matrix. *Probab. Theory Related Fields*, 78(4):509–521, 1988.

Institut de Mathématiques de Jussieu, Projet Analyse Fonctionnelle, Université de Paris 6, 175 rue du Chevaleret, 75013 PARIS, France