Smallest singular value of random matrices and geometry of random polytopes

A. E. Litvak A. Pajor M. Rudelson*
N. Tomczak-Jaegermann†

Abstract

We study the behaviour of the smallest singular value of a rectangular random matrix, i.e., matrix whose entries are independent random variables satisfying some additional conditions. We prove a deviation inequality and show that such a matrix is a "good" isomorphism on its image. Then, we obtain asymptotically sharp estimates for volumes and other geometric parameters of random polytopes (absolutely convex hulls of rows of random matrices). All our results hold with high probability, that is, with probability exponentially (in dimension) close to 1.

1 Introduction

In this paper we consider rectangular $N \times n$ random matrices, whose entries are independent and satisfy some moment conditions, and such that the whole matrix satisfies additional boundedness conditions. We are interested in singular values of such matrices and in geometric parameters of the polytopes they determine.

Assume that $N \geq n$ and denote such a matrix by $\Gamma = [\xi_{ij}]_{1 \leq i \leq N, 1 \leq j \leq n}$. Let us briefly recall some known results on singular values of Γ. Assume that the variance of the ξ_{ij} is 1, and that N is proportional to n, say $n/N = c$ (where c

*The research supported in part by an NSF grant DMS-0245380.
†This author holds the Canada Research Chair in Geometric Analysis.

is considered fixed). From a result in [MP], the empirical measure associated to the spectrum of the sample covariance matrix $\Gamma^*\Gamma/N$ has a deterministic limit distribution supported by the interval $[(1-\sqrt{c})^2, (1+\sqrt{c})^2]$. More precisely, by results from [Si] in the Gaussian case, and from [BY] in the general case (assuming the finite fourth moment of the ξ_{ij}'s), we get that the smallest eigenvalue converges a.e. to $(1-\sqrt{c})^2$. Let $s_n = s_n(\Gamma)$ be the smallest singular value of Γ. Then the above statement says, after a renormalization, that $s_n/\sqrt{N} \to 1-\sqrt{c}$ a.e., as $N \to \infty$. However, the concentration of this random variable around $1-\sqrt{c}$ is in general unknown.

In this paper, we give an (exponentially small) upper estimate for the probability that $s_n/\sqrt{N}$ is small. Denoting by $\|\cdot\|$ the operator norm of an operator acting on a Hilbert space, and considering Γ as acting onto its image, we show (in Theorem 3.1) that for any $0 < c < 1$ there is a function $\phi(c)$ such that the embedding Γ satisfies $\|\Gamma\| \, \|\Gamma^{-1}\| \le \phi(c)$, for any N and n such that $n/N \le c$, with probability larger than $1 - \exp(-c_2 N)$, for some fixed $c_2 > 0$. To the contrary to the approach discussed above, when the ratio $c = n/N$ is considered fixed (independent of n and N), in the present paper we consider n and N to be independent parameters, in particular, allowing c to depend on n. This result can be interpreted by saying that if $n/N \le c$ then, with high probability, Γ is a "good" isomorphic embedding of ℓ_2^n into ℓ_2^N. (Let us also mention that in [LPRTV] a similar result is proved for embeddings of ℓ_2^n into a large class of spaces which, for example, includes ℓ_1^N.)

Theorem 3.1 is then applied to study geometry of random polytopes generated by Γ, that is, the absolute convex hull of N rows of Γ. Such random polytopes have been extensively studied in the Gaussian case, as well as the Bernoulli case. The former case, when N is proportional to n, has many applications in the asymptotic theory of normed spaces (see e.g., [G1] and [Sz], and the survey [MT]). In the Bernoulli case, random polytopes of this form have been investigated in [GH], as well as in a combinatorial setting of the so-called 0-1 polytopes (see for instance [DFM], [BP], and the survey [Z]).

When speaking of random matrices, we identify a large class that contains the most important cases studied in the literature, such as the case when the entries are Gaussian or Bernoulli random variables.

Let us now briefly describe the organization of the paper. In Section 2, we introduce the class of matrices that we consider and we prove some basic facts about them. In Section 3, we show, in Theorem 3.1, that if n is arbitrary and $N = (1+\delta)n$ (where $\delta \geq 1/\ln n$), and if Γ belongs to a certain class M then with probability larger than $1 - \exp(-c_2 N)$, one has $s_n(\Gamma)/\sqrt{N} \geq c_1$, where $c_1, c_2 > 0$ are universal constants. In Section 4, we study some geometric parameters of the symmetric convex hull K_N of rows of Γ, such as the Euclidean inradius, the mean width and the volume.

Acknowledgement A part of this research was performed while the authors were meeting each other at several universities. Namely, the first named author visited Université Paris 6 in May 2003, the second named author visited University of Alberta in November 2002, the third named author visited University of Alberta in Novembers 2002 and 2003, and the fourth named author visited Université Marne-la-Vallée and Université Paris 6 in Spring 2003. The authors would like to thank these universities for their support and hospitality.

2 Preliminaries and some basic facts

By $|\cdot|$ and $\langle\cdot,\cdot\rangle$ we denote the canonical Euclidean norm and the canonical inner product on $\mathbb{R}^m$. By $\|\cdot\|_p$, $1 \leq p \leq \infty$, we denote the ℓ_p-norm, i.e.

$$\|a\|_p = \left(\sum_{i\geq 1} |a_i|^p\right)^{1/p} \quad \text{for} \quad p < \infty \quad \text{and} \quad \|a\|_\infty = \sup_{i\geq 1} |a_i|.$$

As usual, $\ell_p^m = (\mathbb{R}^m, \|\cdot\|_p)$, and the unit ball of ℓ_p^m is denoted by B_p^m. The unit sphere of ℓ_2^m is denoted by S^{m-1}, and the canonical basis of ℓ_2^m is denoted by $e_1, \ldots, e_m$.

Given points $x_1, \ldots, x_k$ in $\mathbb{R}^m$ we denote their convex hull by $\mathrm{conv}\,\{x_i\}_{i\leq k}$ and their absolute convex hull by $\mathrm{abs\,conv}\,\{x_i\}_{i\leq k} = \mathrm{conv}\,\{\pm x_i\}_{i\leq k}$.

Given a finite set A we denote its cardinality by $|A|$.

Given a set $L \subset \mathbb{R}^m$, a convex body $K \subset \mathbb{R}^m$, and $\varepsilon > 0$ we say that a subset $A \subset \mathbb{R}^m$ is an *ε-net* of L with respect to K if

$$A \subset L \subset \cup_{x\in A}\,(x+K).$$

It is well known that if $K = L$ is a centrally symmetric body (or if K is the boundary of a centrally symmetric body L) then for every $\varepsilon > 0$ there exists an ε-net A of K with respect to L with cardinality $|A| \leq (1+2/\varepsilon)^m$ (see e.g. [MS], [P], [T]).

Given $\sigma \subset \{1, 2, \ldots, m\}$ by P_σ we denote the coordinate projection onto $\mathbb{R}^\sigma$. Sometimes we consider P_σ as an operator $\mathbb{R}^m \to \mathbb{R}^m$ and sometimes as an operator $\mathbb{R}^m \to \mathbb{R}^\sigma$.

Given a number a we denote the largest integer not exceeding a by $[a]$ and the smallest integer larger than or equal to a by $\lceil a \rceil$.

By g, g_i, $i \geq 1$, we denote independent $N(0, 1)$ Gaussian random variables. By $\mathbb{P}(\cdot)$ we denote the probability of an event, and $\mathbb{E}$ denotes the expectation.

In this paper we are interested in rectangular $N \times n$ matrices Γ, with $N \geq n$, where the entries are real-valued random variables on some probability space $(\Omega, \mathcal{A}, \mathbb{P})$. We consider these matrices as operators acting from the Euclidean space ℓ_2^n to ℓ_2^N and we denote by $\|\Gamma\|$ the norm of Γ in $\mathrm{L}(\ell_2^n, \ell_2^N)$. If the entries of Γ are independent $N(0, 1)$ Gaussian random variables we say that Γ is *a Gaussian random matrix*. If the entries of Γ are independent ± 1 Bernoulli random variables we say that Γ is *a* ± 1 *random matrix*.

We denote by ψ the Orlicz function $\psi(x) = e^{x^2} - 1$ and by L_ψ, the Orlicz space of real-valued random variables on $(\Omega, \mathcal{A}, \mathbb{P})$, equipped with the norm

$$\|\xi\|_\psi = \inf\{t > 0 \,|\, \mathbb{E}\, \psi(\xi/t) \leq 1\}.$$

For $\mu \geq 1$, we define $\mathrm{B}(\mu)$ to be the set of real-valued *symmetric* random variables on $(\Omega, \mathcal{A}, \mathbb{P})$, satisfying the following properties:

$$1 \leq \|\xi\|_{L^2} \quad \text{and} \quad \|\xi\|_{L^3} \leq \mu. \tag{1}$$

Similarly, for $\mu \geq 1$, we define $\mathrm{B}_\psi(\mu)$ to be the set of real-valued symmetric random variables on $(\Omega, \mathcal{A}, \mathbb{P})$, satisfying:

$$1 \leq \|\xi\|_{L^2} \quad \text{and} \quad \|\xi\|_\psi \leq \mu. \tag{2}$$

A direct computation shows that $\|\xi\|_{L^3} \leq \|\xi\|_\psi$, therefore for every $\mu \geq 1$ one has

$$\mathrm{B}_\psi(\mu) \subset \mathrm{B}(\mu). \tag{3}$$

Also note that if $\xi \in \mathrm{B}_\psi(\mu)$ then

$$\mathbb{P}(\xi \geq u) \leq \exp\left(-u^2/\mu^2\right) \quad \text{for any } u \geq 0. \tag{4}$$

Indeed, ξ is symmetric and $\mathbb{E} \exp(\xi^2/\mu^2) \leq 2$, hence, by the Chebyshev inequality

$$\mathbb{P}(\xi \geq u) = (1/2)\mathbb{P}(|\xi| \geq u) \leq \frac{\mathbb{E} \exp(\xi^2/\mu^2)}{2 \exp(u^2/\mu^2)} \leq \exp(-u^2/\mu^2). \tag{5}$$

Let $\mu \geq 1$ and $a_1, a_2 > 0$. We define $\mathrm{M}(N, n, \mu, a_1, a_2)$ to be the set of all $N \times n$ matrices $\Gamma = (\xi_{ij})_{1 \leq i \leq N, 1 \leq j \leq n}$ whose entries are real-valued independent symmetric random variables on $(\Omega, \mathcal{A}, \mathbb{P})$ satisfying:

$$\xi_{ij} \in \mathrm{B}(\mu) \text{ for every } \ 1 \leq i \leq N,\ 1 \leq j \leq n \tag{6}$$

and

$$\mathbb{P}\left(\|\Gamma\| \geq a_1 \sqrt{N} \right) \leq e^{-a_2 N}. \tag{7}$$

For $\mu \geq 1$, we define $\mathrm{M}_\psi(N, n, \mu)$ to be the set of all $N \times n$ matrices $\Gamma = (\xi_{ij})_{1 \leq i \leq N, 1 \leq j \leq n}$ whose entries are real-valued independent symmetric random variables on $(\Omega, \mathcal{A}, \mathbb{P})$ satisfying:

$$\xi_{ij} \in \mathrm{B}_\psi(\mu) \text{ for every } \ 1 \leq i \leq N,\ 1 \leq j \leq n. \tag{8}$$

It is well known that, in some sense, L_ψ is the set of subgaussian random variables. We recall more precisely some facts that we will need. Let $b > 0$. A real-valued random variable ξ on $(\Omega, \mathcal{A}, \mathbb{P})$ is called *b-subgaussian* if for all $t > 0$, one has:

$$\mathbb{E}\, e^{t\xi} \leq e^{b^2 t^2/2}. \tag{9}$$

Let ξ be b-subgaussian, then it is classical to check by (9), Chebyshev inequality, and an easy optimization argument that

$$\mathbb{P}(\xi \geq u) \leq \exp\left(-\frac{u^2}{2b^2} \right) \quad \text{for any } u \geq 0. \tag{10}$$

It can be also shown by direct computations that if $\xi \in \mathrm{B}_\psi(\mu)$ then

$$\xi \ \text{ is } \ \mu\sqrt{2}\text{-subgaussian}. \tag{11}$$

Fact 2.1 *Let $\mu_i \geq 1$ and $\xi_i \in \mathrm{B}_\psi(\mu_i)$, $i = 1, \ldots, k$, be independent random variables, then for any $x_1, x_2, \ldots, x_k \in \mathbb{R}$,*

$$\sum_{i=1}^{k} \xi_i x_i \ \ \textit{is subgaussian with parameter} \ \ \sqrt{2} \left(\sum_{i=1}^{k} \mu_i^2 x_i^2 \right)^{1/2}. \tag{12}$$

Proof: If ξ_i, $i = 1, \ldots, k$, is a family of independent b_i-subgaussian random variables, then it is clear from (9) that $\sum_{1 \leq i \leq k} \xi_i$ is subgaussian with parameter $\left(\sum_{1 \leq i \leq k} b_i^2 \right)^{1/2}$. We conclude using (11). $\square$

Fact 2.2 *Let $\mu \geq 1$ and $\xi_i \in \mathrm{B}_\psi(\mu)$, $i = 1, \ldots, n$, be independent random variables. Then the random vector $x = (\xi_1, \xi_2, \ldots, \xi_n) \in \mathbb{R}^n$ satisfies*

$$\mathbb{P}(|x| \geq u\sqrt{n}) \leq \exp(n(\ln 2 - u^2/\mu^2)), \quad \textit{for any } u \geq 0. \tag{13}$$

Proof: Indeed,

$$\mathbb{P}\left(\sum_{j=1}^{n} \xi_j^2 \geq u^2 n\right) \leq \mathbb{E}\exp\left(\frac{1}{\mu^2}\left(\sum_{j=1}^{n} \xi_j^2 - u^2 n\right)\right)$$
$$\leq \exp\left(-\frac{u^2 n}{\mu^2}\right) \prod_{j=1}^{n} \mathbb{E}\exp\left(\frac{\xi_j^2}{\mu^2}\right) \leq \exp\left(-\frac{u^2 n}{\mu^2}\right) \cdot 2^n,$$

which implies the desired result. □

Applying the above fact with $u = \sqrt{3}\mu$ we obtain

Fact 2.3 *Let $n \leq N \leq 2^n$, $\mu \geq 1$ and $\Gamma \in \mathrm{M}_\psi(N, n, \mu)$. For $i \leq N$ let $x_i = \Gamma^* e_i$. Then*

$$\mathbb{P}\left(\exists i : \ |x_i| \geq \mu\sqrt{3n}\right) \leq N e^{-2n} \leq e^{-n}.$$

Fact 2.4 *For every $\mu \geq 1$, $a_2 > 0$ and all integers $N \geq n \geq 1$, one has*

$$\mathrm{M}_\psi(N, n, \mu) \subset \mathrm{M}(N, n, \mu, a_1, a_2) \tag{14}$$

with $a_1 = 6\mu\sqrt{a_2 + 4}$.

Proof: Let $\Lambda(N)$ (resp. $\Lambda(n)$) be a $(1/3)$-net of the unit sphere of ℓ_2^N (resp. ℓ_2^n) with respect to B_2^N (resp. B_2^n) and with cardinality less than 7^N (resp. 7^n). An approximation argument shows that for any operator $\Gamma \in \mathrm{L}(\ell_2^n, \ell_2^N)$ we have

$$\|\Gamma\| \leq 3 \max\{\langle y, \Gamma x\rangle \mid x \in \Lambda(n), y \in \Lambda(N)\}.$$

Let $\mu \geq 1$ and Γ be an $N \times n$ matrix with real-valued independent symmetric random variables entries $(\xi_{ij})_{1\leq i\leq N, 1\leq j\leq n}$ in $\mathrm{B}_\psi(\mu)$. It follows from (12) that for any x and y in the unit sphere of ℓ_2^n and ℓ_2^N, respectively, $\langle x, \Gamma y\rangle$ is $\mu\sqrt{2}$-subgaussian. Thus, using estimate (10), we get that for any $t > 0$ we have

$$\mathbb{P}\left(\|\Gamma\| \geq t\right) \leq 7^{n+N} e^{-t^2/36\mu^2}.$$

Therefore

$$\mathbb{P}\left(\|\Gamma\| \geq t\sqrt{N}\right) \leq 7^{n+N} e^{-Nt^2/36\mu^2} \leq e^{(-t^2/36\mu^2+4)\,N}.$$

Inclusion (3) concludes the proof of (14). $\square$

The following fact is proved by routine calculations. For the sake of completeness we provide the proof.

Fact 2.5 *Let $\mu \geq 1$, $\xi_i \in \mathrm{B}_\psi(\mu)$, $\bar{\xi}_i \in \mathrm{B}(\mu)$, $i = 1, \ldots, k$, be independent random variables. Then*

$$\mathbb{P}\left(\sum_{i=1}^{k} \xi_i^2 \leq k/4\right) \leq \exp\left(-\frac{k}{32\mu^4 \ln^2(2\mu)}\right) \tag{15}$$

and

$$\mathbb{P}\left(\sum_{i=1}^{k} (\bar{\xi}_i)^2 \leq k/4\right) \leq \exp\left(-\frac{k}{2^{11}\mu^{12}}\right). \tag{16}$$

Proof: Let ξ be a random variable such that $\mathbb{E}\xi^2 \geq 1$. Then for every $A > 0$ we have

$$1 \leq \mathbb{E}\xi^2 = \int_0^\infty \mathbb{P}\left(\xi^2 > t\right) dt = \int_0^\infty 2s\ \mathbb{P}\left(|\xi| > s\right) ds$$

$$= \int_0^A 2s\ \mathbb{P}\left(|\xi| > s\right) ds + \int_A^\infty 2s\ \mathbb{P}\left(|\xi| > s\right) ds.$$

Choose A such that the second integral does not exceed $1/2$. Then

$$1/2 \leq \int_0^A 2s\ \mathbb{P}\left(|\xi| > s\right) ds.$$

Consider the random variable h defined by $h = \min\{\xi^2, A^2\}$. Then $\|h\|_\infty \leq A^2$ and $\mathbb{E}h \geq 1/2$.

We will use the following Hoeffding's tail inequality ([Ho], see also (1.23) of [L]): let h_i, $i \leq k$, be independent random variables such that $a_i \leq h_i \leq b_i$, and let $B = \sum_{i=1}^k \mathbb{E}h_i$, $M = \sum_{i=1}^k (b_i - a_i)^2$ then

$$\mathbb{P}\left(\sum_{i=1}^{k} h_i - B \leq -t\right) \leq \exp\left(-2t^2/M\right).$$

Taking $t = B/2$ it implies

$$\mathbb{P}\left(\sum_{i=1}^{k} h_i \le B/2\right) \le \exp\left(-B^2/(2M)\right).$$

Applying this inequality to independent random variables h_i, $i \le k$, with $\mathbb{E}h_i \ge 1/2$ and $0 \le h_i \le A^2$ we obtain

$$\mathbb{P}\left(\sum_{i=1}^{k} h_i \le k/4\right) \le \exp\left(-k/(8A^4)\right). \tag{17}$$

Now we estimate the value A for the ξ_i's and $\bar{\xi}_i$'s.

Case 1. Since every $\xi_i \in \mathrm{B}_\psi(\mu)$, by (5), we get for every i

$$\int_A^\infty 2s\ \mathbb{P}\left(|\xi_i| > s\right) ds \le \int_A^\infty 4s\ e^{-s^2/\mu^2} ds = 2\mu^2 e^{-A^2/\mu^2} \le 1/2$$

for $A = \mu\sqrt{2\ln(2\mu)}$. Applying (17) with $h_i = \min\{\xi_i^2, A^2\}$ we obtain the desired result.

Case 2. Since every $\bar{\xi}_i \in \mathrm{B}(\mu)$, by the Chebyshev inequality we have

$$\mathbb{P}(|\xi| \ge u) \le \mathbb{E}|\xi|^3/u^3 \le \mu^3/u^3$$

for every $i \le k$. Therefore for every i

$$\int_A^\infty 2s\ \mathbb{P}\left(|\bar{\xi}_i| > s\right) ds \le \int_A^\infty 2\mu^3/s^2 ds = 2\mu^3/A \le 1/2$$

for $A = 4\mu^3$. Applying (17) with $h_i = \min\{\bar{\xi}_i^2, A^2\}$ we obtain the desired result. $\square$

3 Smallest singular values of matrices with independent entries

In this section, we establish deviation inequalities for the smallest singular value of random matrices from the class $\mathrm{M}(N, n, \mu, a_1, a_2)$. We show that with high probability Γ is a "good isomorphism" onto its image. Our results in this direction can be summarized in the following theorem.

Theorem 3.1 *Let $n \geq 1$ and $N = (1+\delta)n$ for some $\delta > 0$. Let Γ be an $N \times n$ random matrix from $\mathrm{M}(N, n, \mu, a_1, a_2)$, for some $\mu \geq 1$ and $a_1, a_2 > 0$. There exists $\tilde{c_1}, \tilde{c_2} > 0$ (depending on a_1, μ only) such that whenever $\delta \geq \tilde{c_1}/\ln(\tilde{c_2} n)$ then*

$$\mathbb{P}\left(s_n(\Gamma) \leq c_1\sqrt{N}\right) \leq \exp\left(-c_2 N\right),$$

where $c_1 > 0$ depends on δ and μ, a_1, and $c_2 > 0$ depends on μ, a_2.

Remark 1. Our proof below gives that c_1 can be taken of the form $c_1 = c_4 c_5^{1/\delta}$, where c_4, c_5 are positive constants depending only on μ and a_1. Then the desired probability can be made less than $\exp(-N) + \exp(-\bar{c}N/\mu^6) + \exp(-a_2 N)$, where $\bar{c} > 0$ is an absolute constant.

Remark 2. We do not know if Theorem 3.1 holds in the full generality for $0 < \delta \leq 1/\ln n$. Note, however, that in this case the sentences "a constant depends only on δ" and "a constant depends only on n" are equivalent. Therefore, if Γ is a ± 1 random matrix then the result (for $0 < \delta \leq 1/\ln n$) follows from results of Kahn, Komlós, Szemerédi ([KKS]) for square matrices, by removing an appropriate number of columns. For a Gaussian random matrix Γ the result also follows from the estimate for a square matrix, namely, from the fact that in this case the density of $s_n(\Gamma)/\sqrt{n}$ is bounded in the neighbourhood of zero (cf. [E]). Moreover, if we allow c_2 to depend on δ, then the result for the Gaussian rectangular matrix follows from the result of Gordon ([Go], cf. also Theorem 2.13 in [DS]), with $c_1 = c_1'\delta$ and $c_2 = c_2'/\delta^2$, where $c_1', c_2' > 0$ are absolute constants.

Remark 3. It is noteworthy that, as can be seen from the proof below, the case when $\delta \geq \delta_0$, where $\delta_0 > 0$ is a certain absolute constant, is much simpler than the case of a general (small) δ. Indeed, this former case follows directly from Proposition 3.4, without use of Proposition 3.2.

Remark 4. Let us note that for any $N \times n$ matrix Γ and any $a > 0$ the statement $s_n(\Gamma) \leq a$ is equivalent to the existence of $x \in \mathbb{R}^n$, $x \neq 0$, such that $|\Gamma x| \leq a|x|$. Therefore in Theorem 3.1 we shall estimate the probabilities of sets of the form $(\exists\, x \text{ s.t. } |\Gamma x| \leq a|x|)$.

The proof of the theorem is based on two key propositions. The first one will be used to estimate a single coordinate of the vector Γx (in other words, the norm $\|\Gamma x\|_\infty$) for a fixed $x \in \mathbb{R}^n$. We state it here in a more general form, as we believe it is of an independent interest.

Recall that for any subset $\sigma \subset \{1, \dots, n\}$ by P_σ we denote the coordinate projection in $\mathbb{R}^n$ associated to σ.

Proposition 3.2 *Let $(\xi_i)_{i=1}^n$ be a sequence of symmetric independent random variables with $1 \le \|\xi_i\|_{L_2} \le \|\xi_i\|_{L_3} \le \mu$ for all $i = 1, \ldots, n$. Then for any $x = (x_i) \in \mathbb{R}^n$ and any $\sigma \subset \{1, \ldots, n\}$ we have, for all $t > 0$,*

$$\mathbb{P}\Big(\big| \sum_{i=1}^n \xi_i x_i \big| < t \Big) \le \sqrt{2/\pi} \frac{t}{|P_\sigma x|} + c \Big(\frac{\|P_\sigma x\|_3}{|P_\sigma x|} \mu \Big)^3,$$

where $c > 0$ is a universal constant.

The proof of Proposition 3.2 depends on the well-known Berry-Esséen theorem (cf., e.g., [St]).

Lemma 3.3 *Let $(\zeta_i)_{i=1}^n$ be a sequence of symmetric independent random variables with finite third moments, and let $A^2 := \sum_{i=1}^n \mathbb{E}|\zeta_i|^2$. Then for every $\tau \in \mathbb{R}$ one has*

$$\Big| \mathbb{P}\Big(\sum_{i=1}^n \zeta_i < \tau A \Big) - \mathbb{P}\left(g < \tau \right) \Big| \le (c/A^3) \sum_{i=1}^n \mathbb{E}|\zeta_i|^3,$$

where g is a Gaussian random variable with $N(0,1)$ distribution and $c \ge 1$ is a universal constant.

Proof of Proposition 3.2: First we show a stronger estimate for $\sigma = \{1, \ldots, n\}$. Namely, for any $a < b$ and any $x \in \mathbb{R}^n$ we have

$$\mathbb{P}\Big(\sum_{i=1}^n \xi_i x_i \in [a, b) \Big) \le \sqrt{1/2\pi}\, \frac{b-a}{|x|} + c \Big(\frac{\|x\|_3}{|x|} \mu \Big)^3, \tag{18}$$

where $c > 0$ is a universal constant.

Indeed, let $\zeta_i = \xi_i x_i$. Then $A^2 := \sum_i \mathbb{E}\zeta_i^2 = \sum_i x_i^2 \mathbb{E}\xi_i^2 \ge |x|^2$ and $\mathbb{E} \sum_i |\zeta_i|^3 \le \mu^3 \|x\|_3^3$. By Lemma 3.3 we get

$$\begin{aligned}
\mathbb{P}\Big(a \le \sum_{i=1}^n \zeta_i < b \Big) &\le \mathbb{P}\big(a/A \le g < b/A \big) + c \Big(\frac{\|x\|_3}{A} \mu \Big)^3 \\
&\le \frac{b-a}{A\sqrt{2\pi}} + c \Big(\frac{\|x\|_3}{A} \mu \Big)^3 \\
&\le \sqrt{1/2\pi}\, \frac{b-a}{|x|} + c \Big(\frac{\|x\|_3}{|x|}\, \mu \Big)^3,
\end{aligned}$$

as required.

Now, if σ is arbitrary, denote the sequence $(\xi_i)_{i\in\sigma}$ by (ξ_i') and the sequence $(\xi_i)_{i\notin\sigma}$ by (ξ_i''), and by $\mathbb{P}'$, $\mathbb{P}''$ and $\mathbb{E}'$, $\mathbb{E}''$, the corresponding probabilities and expectations. The independence and Fubini theorem imply

$$\begin{aligned}\mathbb{P}\left(\left|\sum_{i=1}^n \xi_i x_i\right| < t\right) &= \mathbb{P}\Big(-t-\sum_{i=1}^n \xi_i'' x_i < \sum_{i=1}^n \xi_i' x_i < t-\sum_{i=1}^n \xi_i'' x_i\Big)\\ &= \mathbb{E}''\mathbb{P}'\Big(-t-\sum_{i=1}^n \xi_i'' x_i < \sum_{i=1}^n \xi_i' x_i < t-\sum_{i=1}^n \xi_i'' x_i\Big)\\ &\le \sqrt{1/2\pi}\,\frac{2t}{|P_\sigma x|}+c\Big(\frac{\|P_\sigma x\|_3}{|P_\sigma x|}\mu\Big)^3.\end{aligned}$$

The latter inequality follows from (18) and the fact that the vector appearing in the sum $\sum_i \xi_i' x_i$ is exactly $P_\sigma x$, and from the independence of $(\xi_i)_{i\in\sigma}$ and $(\xi_i)_{i\notin\sigma}$. □

Our second proposition is a general estimate for the norm $|\Gamma x|$ for a fixed vector x.

Proposition 3.4 *Let $1 \le n < N$ be positive integers. Let Γ be an $N\times n$ random matrix from $\mathrm{M}(N, n, \mu, a_1, a_2)$, for some $\mu \ge 1$ and $a_1, a_2 > 0$. Then for every $x \in \mathbb{R}^n$ we have*

$$\mathbb{P}\left(|\Gamma x| \le c'\mu^{-3}\sqrt{N}\;|x|\right) \le \exp\left(-c''N/\mu^6\right),$$

where $1 > c', c'' > 0$ are absolute constants.

The proof of this proposition will be using the following simple estimate which is a general form of the Paley-Zygmund inequality.

Lemma 3.5 *Let $p \in (1,\infty)$, $q = p/(p-1)$. Let $f \ge 0$ be a random variable with $\mathbb{E}f^{2p} < \infty$. Then for every $0 \le \lambda \le \sqrt{\mathbb{E}f^2}$ we have*

$$\mathbb{P}\left(f > \lambda\right) \ge \frac{(\mathbb{E}f^2-\lambda^2)^q}{(\mathbb{E}f^{2p})^{q/p}}.$$

Proof: We have

$$\begin{aligned}
\mathbb{E}f^2 &= \mathbb{E}f^2\ \chi_{(f>\lambda)} + \mathbb{E}f^2\ \chi_{(f\le\lambda)} \\
&\le \left(\mathbb{E}f^{2p}\right)^{1/p} \left(\mathbb{E}\ \chi_{(f>\lambda)}\right)^{1/q} + \lambda^2 \\
&= \left(\mathbb{E}f^{2p}\right)^{1/p} \left(\mathbb{P}\left(f>\lambda\right)\right)^{1/q} + \lambda^2.
\end{aligned}$$

This implies

$$\mathbb{P}\left(f>\lambda\right) \ge \frac{\left(\mathbb{E}f^2-\lambda^2\right)^q}{\left(\mathbb{E}f^{2p}\right)^{q/p}},$$

as required. □

Lemma 3.6 *Let $\mu \ge 1$ and $(\xi_i)_{i\ge1}$ be a sequence of independent symmetric random variables such that $1 \le \mathbb{E}|\xi_i|^2 \le \mathbb{E}|\xi_i|^3 \le \mu^3$ for every $i \ge 1$. Let $x = (x_i)_{i\ge1} \in \ell_2$ be such that $|x| = 1$ and let $f = |\sum_{i\ge1} x_i\xi_i|$. Then for every $0 \le \lambda \le 1$ one has*

$$\mathbb{P}\left(f>\lambda\right) \ge \left(\frac{1-\lambda^2}{2\mu^2}\right)^3.$$

Proof: By the symmetry of ξ_i's and Khinchine's inequality ([H]),

$$\mathbb{E}f^3 = \mathbb{E}_\xi\,\mathbb{E}_\varepsilon \left|\sum_{i\ge1} \varepsilon_i\xi_i x_i\right|^3 \le \sqrt{8}\ \mathbb{E}_\xi \left(\sum_{i\ge1} \xi_i^2 x_i^2\right)^{3/2},$$

where ε_i's are independent Bernoulli ±1 random variables. (In the inequality above we used the estimate for the Khinchine's constant $B_3 = \sqrt{2}\pi^{-1/6} \le \sqrt{2}$, while the standard proof gives $B_3 \le 2$.) Define a function φ on the set

$$E := \left\{ s = (s_i)_{i\ge1} \in \ell_1 \mid s_i \ge 0 \text{ for every } i \text{ and } \sum_{i\ge1} s_i = 1 \right\}$$

by

$$\varphi(s) = \mathbb{E}_\xi \left(\sum_{i\ge1} \xi_i^2 s_i\right)^{3/2},$$

for $s \in E$. Since φ is clearly convex,

$$\sup_E \varphi(s) = \sup_{i\ge1} \varphi(e_i) = \sup_{i\ge1} \mathbb{E}_\xi \left(\xi_i^2\right)^{3/2} \le \mu^3,$$

which implies

$$\mathbb{E}f^3 \le \sqrt{8}\mu^3.$$

Next, by our normalization,

$$\mathbb{E}f^2 = \mathbb{E}\sum_{i\ge 1}\xi_i^2|x_i|^2 \ge 1.$$

Applying Lemma 3.5 with $p = 3/2$ we obtain the desired result. $\square$

Proof of Proposition 3.4 Let $x = (x_i)_i \in \mathbb{R}^n$ with $|x| = 1$. Let $\Gamma = (\xi_{ji})_{j\le N, i\le n}$ where ξ_{ji} are independent random variables with $1 \le \|\xi_{ji}\|_{L_2} \le \|\xi_{ji}\|_{L_3} \le \mu$, for every $j \le N$ and every $i \le n$. Let $f_j = |\sum_{i=1}^n \xi_{ji}x_i|$. Note that $f_1, \ldots, f_N$ are independent. For any $t, \tau > 0$ we have

$$\begin{aligned}
\mathbb{P}\left(|\Gamma x|^2 \le t^2 N\right) &= \mathbb{P}\left(\sum_{j=1}^N f_j^2 \le t^2 N\right) = \mathbb{P}\left(N - \frac{1}{t^2}\sum_{j=1}^N f_j^2 \ge 0\right)\\
&\le \mathbb{E}\exp\left(\tau N - \frac{\tau}{t^2}\sum_{j=1}^N f_j^2\right) = e^{\tau N}\prod_{j=1}^N \mathbb{E}\exp\left(-\tau f_j^2/t^2\right).
\end{aligned}$$

To estimate the latter expectation first observe that by Lemma 3.6, one has, for every $0 \le \lambda \le 1$,

$$\mathbb{P}\left(f_j > \lambda\right) \ge \frac{(1-\lambda^2)^3}{8\mu^6} =: \beta$$

for every j. Therefore for every $\tau > 0$ we have

$$\begin{aligned}
\mathbb{E}\exp\left(-\tau f_j^2/t^2\right) &= \int_0^\infty \mathbb{P}\left(\exp\left(-\tau f_j^2/t^2\right) > s\right) ds\\
&= \int_0^1 \mathbb{P}\left(1/s > e^{\tau f_j^2/t^2}\right) ds\\
&\le \int_0^{e^{-\tau\lambda^2/t^2}} ds + \int_{e^{-\tau\lambda^2/t^2}}^1 (1-\beta) ds\\
&= e^{-\tau\lambda^2/t^2} + (1-\beta)\left(1 - e^{-\tau\lambda^2/t^2}\right)\\
&= 1 - \beta\left(1 - e^{-\tau\lambda^2/t^2}\right).
\end{aligned}$$

For arbitrary $\alpha > 0$ and $0 < \lambda < 1$ set $\tau = \alpha t^2/\lambda^2$. Then we get, for any $t > 0$,

$$\mathbb{P}\left(|\Gamma x|^2 \leq t^2 N\right) \leq \left(e^{\alpha t^2/\lambda^2}\left(1 - \beta(1 - e^{-\alpha})\right)\right)^N. \tag{19}$$

For example, letting $\lambda = 1/2$ we get $\beta = (3/(8\mu^2))^3$, and using $1-s < e^{-s}$ for $s > 0$, the left hand side expression in (19) is less than

$$\exp\left(\left(4\alpha t^2 - \beta(1 - e^{-\alpha})\right) N\right).$$

Thus letting $\alpha = \ln 2$ and $t = \sqrt{\beta}/4$ we get the required estimates with $c' = (27/2^{13})^{1/2}$ and $c'' = 27/2^{11}$. □

We are now ready for

Proof of Theorem 3.1: Let $\Gamma \in \mathrm{M}(N, n, \mu, a_1, a_2)$ be a random matrix and denote $\overline{\Omega} = \left\{\omega : \|\Gamma\| \leq a_1\sqrt{N}\right\}$. We have $N = (1+\delta)n$, and for the time being we assume only that $\delta > 0$. Conditions for δ necessary for the method to work will appear at the end of the proof. Fix parameters t and $b > 0$ to be determined later, depending on μ, a_1, and δ. Set $a := t/a_1$ and assume that

$$2a \leq b \leq 1/4. \tag{20}$$

Given $x = (x_i)_i \in \mathbb{R}^n$, let $\sigma = \sigma_x := \{i : |x_i| \leq a\}$, and set $z = P_\sigma x$. Now consider two subsets of $\overline{\Omega}$.

$$\Omega_t(a,b) = \overline{\Omega} \cap \Big(\exists\, x \in S^{n-1} \text{ s.t. } |\Gamma x| \leq t\sqrt{N} \text{ and } |z| \leq b\Big), \tag{21}$$

$$\Omega_t'(a,b) = \overline{\Omega} \cap \Big(\exists\, x \in S^{n-1} \text{ s.t. } |\Gamma x| \leq t\sqrt{N} \text{ and } |z| > b\Big). \tag{22}$$

We shall estimate the probabilities of these sets separately. In both cases the idea of the proof is the same. We shall estimate the probability that $|\Gamma x| \leq t\sqrt{N}$ for a single vector x and then use the ε-net argument and approximation. However, the balance between the probabilistic estimate and the cardinality of an ε-net will be different in each case. If x satisfies the conditions of (22) we have a good control of the ℓ_∞-norm of this vector, which allows us to apply the powerful estimate of Proposition 3.2. In this case the standard estimate $(3/\varepsilon)^n$ of the cardinality of an ε-net on the sphere S^{n-1}

will be sufficient. In case when x satisfies the conditions of (21), to bound the probability for a fixed x, we shall use the weaker, but more general estimate of Proposition 3.4. However, since in this case $|z| \leq b$, vector x can be approximated by another vector with small support. This observation yields a much better bound for the cardinality of an ε-net of the set described in (21).

Case I: Probability of $\Omega'_t(a,b)$. Let $\mathcal{N} \subset S^{n-1}$ be an ε-net in S^{n-1} of cardinality $|\mathcal{N}| \leq (3/\varepsilon)^n$. Setting $\varepsilon := a = t/a_1$, a standard approximation argument shows that if there exists $x \in S^{n-1}$ such that $|\Gamma x| \leq t\sqrt{N}$ and $|z| = |P_\sigma x| > b$ then there exist $v \in \mathcal{N}$ and $\bar{\sigma} = \sigma \subset \{1, \ldots, n\}$ such that

$$|\Gamma v| \leq (t + \varepsilon a_1)\sqrt{N} = 2t\sqrt{N}, \quad \|P_\sigma v\|_\infty \leq a + \varepsilon = 2a, \quad |P_\sigma v| \geq b - \varepsilon \geq b/2.$$

Denote by $\mathcal{A}$ the set of all $v \in \mathcal{N}$ for which there exists $\bar{\sigma} \subset \{1, \ldots, n\}$ such that

$$\|P_{\bar{\sigma}} v\|_\infty \leq 2a, \qquad |P_{\bar{\sigma}} v| \geq b/2.$$

Then $|\mathcal{A}| \leq |\mathcal{N}| \leq (3/\varepsilon)^n$ and

$$\mathbb{P}\left(\Omega'_t(a,b)\right) \leq \mathbb{P}\left(\exists v \in \mathcal{A} \, : \, |\Gamma v| \leq 2t\sqrt{N}\right). \tag{23}$$

Now, fix $v = (v_i)_i \in \mathcal{A}$. For every $j = 1, \ldots, N$, set

$$f_j(\lambda) = \mathbb{P}\Big(\Big|\sum_{i=1}^n \xi_{ji} v_i\Big| < \lambda\Big),$$

and let $f(\lambda) = \sup_j f_j(\lambda)$. Since $\|\cdot\|_3^3 \leq \|\cdot\|_\infty |\cdot|^2$, by Proposition 3.2 we get

$$\begin{aligned} f(\lambda) &\leq c\left(\lambda + \|P_\sigma v\|_\infty \mu^3\right)/|P_\sigma v| \\ &\leq 2c\left(\lambda + 2a\mu^3\right)/b \leq (4c/b)\max\left\{\lambda, 2a\mu^3\right\}, \end{aligned} \tag{24}$$

where $c \geq \sqrt{2/\pi}$ is an absolute constant.

Now we have

$$\begin{aligned}
\mathbb{P}\Big(|\Gamma v|^2 \le 4t^2 N\Big) &= \mathbb{P}\Big(\sum_{j=1}^N |\sum_{i=1}^n \xi_{ji} v_i|^2 \le 4t^2 N\Big) \\
&= \mathbb{P}\Big(N - \sum_{j=1}^N |\sum_{i=1}^n \xi_{ji} v_i|^2/4t^2 \ge 0\Big) \\
&\le \mathbb{E}\exp\Big(N - \sum_{j=1}^N |\sum_{i=1}^n \xi_{ji} v_i|^2/4t^2\Big) \\
&= \mathbb{E}\prod_{j=1}^N \exp\Big(1 - |\sum_{i=1}^n \xi_{ji} v_i|^2/4t^2\Big) \\
&= e^N \prod_{j=1}^N \mathbb{E}\exp\Big(-|\sum_{i=1}^n \xi_{ji} v_i|^2/4t^2\Big).
\end{aligned}$$

We estimate the expectations by passing to the integral formula. Denote $A := \sqrt{2} a\mu^3/t$. Then

$$\begin{aligned}
\mathbb{E}\exp\big(-|\sum_{i=1}^n \xi_{ji} v_i|^2/4t^2\big) &= \int_0^1 \mathbb{P}\Big(\exp\Big(-|\sum_{i=1}^n \xi_{ji} v_i|^2/4t^2\Big) > s\Big) ds \\
&= \int_0^\infty u e^{-u^2/2}\, \mathbb{P}\Big(|\sum_{i=1}^n \xi_{ji} v_i| < \sqrt{2} t u\Big) du \\
&= \int_0^\infty u e^{-u^2/2} f_j(\sqrt{2} t u) du \\
&\le (4c/b)\left(2\int_0^A u a\mu^3\, du + \int_A^\infty \sqrt{2} t u^2 e^{-u^2/2}\, du\right) \\
&\le (4c/b)\left(a\mu^3 A^2 + t\sqrt{\pi}\right) \\
&= (4c/b)\left(2a^3\mu^9/t^2 + t\sqrt{\pi}\right) \\
&= (4ct/b)\left(2\mu^9/a_1^3 + \sqrt{\pi}\right) = c_3 t/b,
\end{aligned}$$

where $c_3 := 4c\,(2\mu^9/a_1^3 + \sqrt{\pi})$. So

$$\mathbb{P}\Big(|\Gamma v|^2 \le 4t^2 N\Big) \le (c_3 e\, t/b)^N.$$

Finally, since $\varepsilon = a = t/a_1$, we get by (23),

$$\mathbb{P}\big(\Omega_t'(a,b)\big) \le |\mathcal{A}|\ (c_3 e\, t/b)^N \le \big(3a_1/t\big)^n (c_3 e\, t/b)^N \le e^{-N} \tag{25}$$

for any t satisfying

$$t \le \frac{b}{e^2 c_3} \left(\frac{b}{3e^2 c_3 a_1} \right)^{1/\delta} := c_4 c_5^{1/\delta}. \tag{26}$$

Case II: Probability of $\Omega_t(a,b)$. Given $x \in S^{n-1}$ recall that $\sigma = \{i : |x_i| \le a\}$, and set $\sigma' = \{1, \dots, n\} \setminus \sigma$. By the definition of σ, clearly, $|\sigma'| \le [1/a^2] =: m$. Let $y = P_{\sigma'} x$. If now x is a vector appearing in the definition (21) of $\Omega_t(a,b)$ then $|\Gamma y| \le (t + a_1 b)\sqrt{N}$, $|y| \ge (1-b^2)^{1/2}$ and $|\operatorname{supp}(y)| \le m$, where $\operatorname{supp}(y)$ denotes the support of y.

Of course the inequality $m \le n$ will be satisfied whenever $a \ge 1/\sqrt{n}$, or equivalently, whenever

$$t \ge a_1/\sqrt{n}. \tag{27}$$

Let $\varepsilon = b$ and let $\mathcal{N} \subset B_2^n$ be an ε-net in the set $\{y \in B_2^m : |\operatorname{supp}(y)| \le m\}$ (in the Euclidean norm). We can choose $\mathcal{N}$ with cardinality $|\mathcal{N}| \le \binom{n}{m}(3/\varepsilon)^m \le (e\,n/m)^m (3/\varepsilon)^m$. For y defined at the beginning of Case II, we choose $v \in \mathcal{N}$ such that $|v| \ge |y| - \varepsilon \ge 1 - 2b \ge 1/2$ and

$$|\Gamma v| \le (t + 2\,a_1 b)\sqrt{N} \le (5/2) a_1 b \sqrt{N} \le 5 a_1 b \sqrt{N} |v|.$$

(We used the fact that $t = a_1 a \le a_1 b/2$, by our conditions.) Thus, by Proposition 3.4, we get that if

$$b := \min\left\{1/4,\ c'/(5 a_1 \mu^3)\right\},$$

then

$$\mathbb{P}\big(\Omega_t(a,b)\big) \le (e\,n/m)^m (3/b)^m \exp\left(-c'' N/\mu^6\right) \le \exp\left(-c'' N/(2\mu^6)\right)$$

if

$$m \ln\left(\frac{3en}{bm}\right) \le \left(c'' N/(2\mu^6)\right).$$

Since $m = [1/a^2] \le n$, the last inequality is satisfied if

$$(1/a^2) \ln\left(\frac{3ena^2}{b}\right) \le \left(c'' n/(2\mu^6)\right),$$

which holds for

$$1/a^2 = (a_1/t)^2 \le \frac{c'' n}{4\mu^6 \ln\left((6e\mu^6)\,/\,(c'' b)\right)}. \tag{28}$$

Now, to satisfy inequality (26), we choose $t = c_4 c_5^{1/\delta}$ and note that (28), which implies also $t \geq a_1/\sqrt{n}$, holds for every

$$\delta \geq c_6 / \ln(c_7 n).$$

Here constants c_4, c_5, c_6 and c_7 depend only on a_1, μ. Note also that due to the form of c_5 and since $c_3 \geq \max\{1, \mu^9/a_1^3\}$ we have $t < a_1 b/2$ for every $a_1 \geq 1$.

Finally, to conclude the proof of the Theorem 3.1 observe that the set

$$\left\{ \exists\, x \in S^{n-1} \text{ s.t. } |\Gamma x| \leq t\sqrt{N} \right\}$$

is contained in the union of $\Omega_t(a,b)$, $\Omega_t'(a,b)$, and of the complement of $\overline{\Omega}$. Moreover, by the definition of the class $\mathrm{M}(N, n, \mu, a_1, a_2)$ we also have that $\mathbb{P}(\overline{\Omega}) \geq 1 - \exp(-a_2 N)$. Putting the three estimates together and letting $c_1 = t$ we get

$$\mathbb{P}\left(s_n(\Gamma) \leq c_1 \sqrt{N} \right) \leq e^{-N} + e^{-c'' N/(2\mu^6)} + e^{-a_2 N},$$

which concludes the proof. □

4 Geometry of Random Polytopes

In this section we study some classical geometric parameters of random polytopes of the form $K_N := \Gamma^* B_1^N$, where Γ is a random matrix either from $\mathrm{M}(N, n, \mu, a_1, a_2)$ or from $\mathrm{M}_\psi(N, n, \mu)$. In other words, K_N is the absolute convex hull of the rows of Γ, and as already mentioned before, this setting contains the Gaussian case as well as the case when the entries are independent Bernoulli ± 1 random variables.

We say that a random polytope has a certain property if the probability that the polytope satisfies this property is close to one. Since K_N is the absolute convex hull of N independent rows of Γ, from usual concentration phenomena, one would expect this probability to be larger than $1 - \exp(-cN)$ for some absolute constant $c > 0$. This level of concentration is not always true, though, and the concentration may be of the form $1 - \exp(-cn^\beta N^{1-\beta})$ for some $0 < \beta < 1$. However, when speaking in this context of high probability we always require that this probability is larger than $1 - \exp(-cn)$ for some absolute constant $c > 0$.

We improve the estimates from [GH] on the asymptotic behaviour of some parameters, such as the inradius, the volume, or the mean widths of K_N and its polar. Moreover, the techniques introduced in this paper allow to obtain much stronger estimates for probabilities involved.

4.1 Additional definitions and basic facts

Given a centrally symmetric convex body $K \subset \mathbb{R}^n$ we denote its volume by $|K|$, its gauge by $\|x\|_K$, its supporting functional by h_K, that is $h_K(u) = \max\{\langle u, y\rangle \mid y \in K\}$. The polar of K is

$$K^0 = \{x \in \mathbb{R}^n \mid \langle x, y\rangle \leq 1 \text{ for every } y \in K\}.$$

Note that $h_K(\cdot) = \|\cdot\|_{K^0}$. We use also the following standard notation

$$M_K = M(K) = \int_{S^{n-1}} \|x\|_K \, d\nu,$$

where ν is the normalized Lebesgue measure on S^{n-1}. We denote $M(K^0)$ by $M_K^* = M^*(K)$. It is well known that there exists a constant $c_n > 1$ such that

$$M_K = \frac{c_n}{\sqrt{n}} \mathbb{E} \| \sum_{i=1}^n e_i g_i \|_K,$$

for every $K \subset \mathbb{R}^n$. Also, $c_n \longrightarrow 1$ as $n \longrightarrow \infty$.

We recall the following inequalities, which hold for every convex body K,

$$M_K^* \geq (|K|/|B_2^n|)^{1/n} \geq 1/M_K. \tag{29}$$

The left-hand side of the inequality is Urysohn inequality (see e.g. [P]). The right-hand side is obtained by integration and Hölder inequality. We recall also that by Santaló inequality and Bourgain-Milman ([BM]) inverse Santaló inequality there exists an absolute positive constant c such that for every convex symmetric body K one has

$$c^n |B_2^n|^2 \leq |K||K^0| \leq |B_2^n|^2. \tag{30}$$

4.2 Inclusion Theorem

In this section we develop further analytic tools to show that for $\Gamma \in \mathrm{M}(N, n, \mu, a_1, a_2)$, $K_N = \Gamma^* B_1^N$ contains with high probability a large "regular" body.

We first study the inradius of random polytopes. Note that $tB_2^n \subset K_N$ if and only if $t|x| \leq \|\Gamma x\|_\infty$ for every $x \in \mathbb{R}^n$. Thus if $t\sqrt{N}|x| \leq |\Gamma x|$ for every $x \in \mathbb{R}^n$ then $tB_2^n \subset K_N$. Theorem 3.1 (see also Remark 4 after it) has the following consequence.

Corollary 4.1 *Let $n \geq 1$ and $N = (1+\delta)n$ for some $\delta > 0$. There exists $\tilde{c_1}, \tilde{c_2} > 0$ (depending on a_1, μ only) such that whenever $\delta \geq \tilde{c_1}/\ln(\tilde{c_2}n)$ then*

$$\mathbb{P}\left(K_N \supset c_1 B_2^n\right) \geq 1 - \exp\left(-c_2 N\right),$$

where $c_1 > 0$ depends only on δ, μ, a_1, and $c_2 > 0$ depends only on μ and a_2.

Remark 1. In fact, by Remark 1 after Theorem 3.1, $c_1 = c_3 c_4^{1/\delta}$, where c_3, c_4 are positive constants depending only on μ and a_1.

Remark 2. It is proved in [GH] that for all $N > cn\ln(\alpha^{-1})$, one has $\mathbb{P}(K_N \supset c' B_2^n) \geq 1 - \alpha$ where c and c' are absolute positive constants. Note that the constraint on N and n does not allow to take $\alpha \sim \exp(-c_2 N)$; and if $\alpha \sim \exp(-c_2 n)$, which is the minimum required to get a statement with high probability, then $N \gtrsim n^2$. Therefore the statement from [GH] gives a weak estimate for probability when N is proportional to n.

When N/n is large, we have more information and we can estimate the inradius with respect to a body bigger than the Euclidean unit ball.

Theorem 4.2 *Let $\Gamma \in \mathrm{M}(N, n, \mu, a_1, a_2)$ and $K_N = \Gamma^* B_1^N$. There exists an absolute constant $c_2 > 1$ such that for every $\beta \in (0,1)$ and every n, N satisfying*

$$2^n \geq N \geq n \max\left\{\exp(C_\mu/\beta), \left(c_2 \max\left\{\ln a_1, 1/(1-\beta)^2\right\}\right)^{1/(1-\beta)}\right\},$$

where $C_\mu = 12\ln(e\mu)$, one has

$$\mathbb{P}\left(K_N \supset \frac{1}{8}\left(B_\infty^n \cap R B_2^n\right)\right) \geq 1 - \exp\left(-n^\beta N^{1-\beta}/5\right) - \exp\left(-a_2 N\right)$$

with $R = \sqrt{\beta \ln(N/n)/C_\mu}$.

Remark. For a Gaussian random matrix we do not need to take the intersection with the cube. Namely, for such a matrix we have

$$\mathbb{P}\left(K_N \supset C\sqrt{\beta \ln(N/n)}\ B_2^n\right) \geq 1 - \exp\left(-cn^\beta N^{1-\beta}\right),$$

where C, c are absolute positive constants ([G2]). Moreover, the probability estimate cannot be improved. Indeed, for a Gaussian random matrix and $\beta \in (0, c'')$ we have

$$\mathbb{P}\left(K_N \supset C'\sqrt{\beta \ln(N/n)} B_2^n\right) \leq 1 - \exp\left(-c'n^\beta N^{1-\beta}\right),$$

where $C', c' > 0$ and $0 < c'' \leq 1$ are absolute constants.

To prove Theorem 4.2 we need to extend a result by Montgomery-Smith ([M]) which was proved for Bernoulli ± 1 random variables.

Lemma 4.3 *Let $\alpha \geq 1$ and $L = (1/2)(B_\infty^n \cap \alpha B_2^n)$. Let $\mu \geq 1$ and let ξ_i, $i \leq n$, be independent symmetric random variables such that $1 \leq \mathbb{E}\xi^2 \leq \mathbb{E}|\xi|^3 \leq \mu^3$. Then for every $z \in \mathbb{R}^n$, $z \neq 0$, one has*

$$\mathbb{P}\left(\sum_{i=1}^n \xi_i z_i > h_L(z)\right) > \exp\left(-C_\mu \alpha^2\right),$$

where $C_\mu = 12\ln(e\mu)$.

We postpone the proof of this lemma until the end of this section.

Lemma 4.4 *Let $\alpha \geq 1$ and $L = (1/2)(B_\infty^n \cap \alpha B_2^n)$. Let $\Gamma \in \mathrm{M}(N, n, \mu, a_1, a_2)$. Then for every $u \in \mathbb{R}^n$ and every $\sigma \subset \{1, \ldots, N\}$ one has*

$$\mathbb{P}\left(\|P_\sigma \Gamma u\|_\infty < h_L(u)\right) < \exp\left(-|\sigma| \exp(-C_\mu \alpha^2)\right),$$

where $P_\sigma \ :\ \mathbb{R}^N \to \mathbb{R}^\sigma$ and $C_\mu = 12\ln(e\mu)$.

Proof: Let $\Gamma = (\xi_{ji})_{j\leq N, i\leq n} \in \mathrm{M}(N, n, \mu, a_1, a_2)$. Then $P_\sigma\Gamma = (\xi_{ji})_{j\in\sigma, i\leq n} \in \mathrm{M}(|\sigma|, n, \mu, a_1, a_2)$. (Strictly speaking to use such notation we should require $|\sigma| \geq n$, however we do not need such a condition in this proof.) By Lemma 4.3 we have for every $u = \{u_i\}_{i=1}^n \in \mathbb{R}^n$ and every $j \in \sigma$

$$\mathbb{P}\left(\sum_{i=1}^n u_i \xi_{ji} < h_L(u)\right) \leq 1 - \exp(-C_\mu \alpha^2) < \exp\left(-\exp(-C_\mu \alpha^2)\right).$$

Thus

$$\mathbb{P}\left(\|P_\sigma \Gamma u\|_\infty < h_L(u)\right) = \mathbb{P}\left(\sup_{j\in\sigma}\left|\sum_{i=1}^n u_i\xi_{ji}\right| < h_L(u)\right)$$
$$= \prod_{j\in\sigma}\mathbb{P}\left(\left|\sum_{i=1}^n u_i\xi_{ji}\right| < h_L(u)\right) < \exp\left(-|\sigma|\exp(-C_\mu\alpha^2)\right).$$

□

Proof of Theorem 4.2: Let $\Gamma = (\xi_{ji})_{j\le N, i\le n} \in \mathrm{M}(N,n,\mu,a_1,a_2)$. Let us denote $x_j = (\xi_{ji})_{i\le n} \in \mathbb{R}^n$, $j\le N$, $K = K_N = \text{abs conv}\{x_j\}_{j\le N}$, $L = L(\alpha) = (1/2)\left(B_\infty^n \cap \alpha B_2^n\right)$. Note that

$$h_K(u) = \sup_{j\le N} |\langle u, x_j\rangle| = \|\Gamma u\|_\infty$$

for every $u\in\mathbb{R}^n$.

The proof of Theorem 4.2 is again based on a combination of a probability estimate for a fixed vector u and an ε-net argument. To make this scheme work we replace $\|\cdot\|_\infty$ with a new norm $|||\cdot||| \le \|\cdot\|_\infty$ having a smaller Lipschitz constant with respect to the Euclidean metric. This yields a larger value of δ in the approximation, and thus a smaller size of a δ-net.

Let $m = 8\lceil (N/n)^\beta\rceil$ (if the latter number is greater than $N/4$ we take $m=N$) and $k = [N/m]$. Below we assume $m<N$ (then $k\ge 4$, hence $km > 4N/5$); the proof in the case $m=N$, $k=1$ repeats the same lines with simpler calculations. Let $\sigma_1, \ldots, \sigma_k$ be a partition of $\{1,2,3,\ldots,N\}$ such that $m\le|\sigma_i|$ for every $i\le k$. Define $|||\cdot|||$ on $\mathbb{R}^N$ by

$$|||z||| = \frac{1}{k}\sum_{i=1}^k \|P_i z\|_\infty$$

for every $z\in\mathbb{R}^N$, where $P_i = P_{\sigma_i} : \mathbb{R}^N \to \mathbb{R}^{\sigma_i}$ is the coordinate projection. Clearly, $|||\cdot||| \le \|\cdot\|_\infty$.

Note that if for some $u\in\mathbb{R}^n$ we have $|||\Gamma u||| < h_L(u)/2$ then there is $I\subset\{1,\ldots,k\}$ of cardinality at least $k/2$ such that for every $i\in I$ one has $\|P_i\Gamma u\|_\infty < h_L(u)$. Therefore, by Lemma 4.4, we obtain for every $u = \{u_i\}_{i=1}^n \in\mathbb{R}^n$ and every $\alpha\ge 1$

$$
\begin{aligned}
&\mathbb{P}\left(|||\Gamma u||| < h_L(u)/2\right) \\
&\quad\le \sum_{|I|=[(k+1)/2]} \mathbb{P}\left(\|P_i\Gamma u\|_\infty < h_L(u) \ \text{ for every } \ i\in I\right) \\
&\quad\le \sum_{|I|=[(k+1)/2]} \prod_{i\in I} \mathbb{P}\left(\|P_i\Gamma u\|_\infty < h_L(u)\right) \\
&\quad\le \sum_{|I|=[(k+1)/2]} \prod_{i\in I} \exp\left(-|\sigma_i|\exp(-C_\mu\alpha^2)\right) \\
&\quad\le \binom{k}{[k/2]} \exp\left(-(km/2)\exp(-C_\mu\alpha^2)\right) \\
&\quad\le \exp\left(k\ln 2 - (km/2)\exp(-C_\mu\alpha^2)\right),
\end{aligned}
$$

where $C_\mu = 12\ln(e\mu)$. By our choice of k and m we have $(km/2)(n/N)^\beta \ge 4k$. Thus the last expression is bounded by

$$
\exp\left(-(3km/8)\exp\left(-C_\mu\alpha^2\right)\right).
$$

Take

$$
\alpha^2 = \frac{\beta\ \ln(N/n)}{C_\mu}
$$

($\alpha \ge 1$, by the condition on n and N). Since $km > 4N/5$ we obtain

$$
\mathbb{P}\left(|||\Gamma u||| < h_L(u)/2\right) \le \exp\left(-0.3\ N^{1-\beta}n^\beta\right).
$$

Let S be the boundary of L^0 and $0<\delta\le 1$ to be chosen later. By the standard volume estimates there exists a δ-net A in S with respect to L^0 of cardinality not exceeding $(3/\delta)^n$. Therefore

$$
\begin{aligned}
&\mathbb{P}\left(\exists u\in A\ :\ |||\Gamma u||| < 1/2\right) \\
&\quad\le \sum_{u\in A} \mathbb{P}\left(|||\Gamma u||| < 1/2\right) \\
&\quad\le \exp\left(n\ln(3/\delta) - 0.3\ N^{1-\beta}n^\beta\right)
\end{aligned}
$$

Let $\overline{\Omega} = \left\{\omega : \|\Gamma\| \le a_1\sqrt{N}\right\}$. Since $(1/2)B_2^n \subset L$ (for $\alpha\ge 1$) and $|||z||| \le (1/\sqrt{k})|z|$ for every $z\in\mathbb{R}^N$, we obtain that for every $u\in\mathbb{R}^n$ and every $\omega\in\overline{\Omega}$ one has

$$
|||\Gamma(u)||| \le a_1\sqrt{N/k}\ |u| \le 2a_1\sqrt{N/k}\ h_L(u).
$$

For every $u \in S$ there exists $v \in A$ such that $h_L(u-v) \le \delta$, which implies for every $\omega \in \overline{\Omega}$

$$|||\Gamma(v)||| \le |||\Gamma(u)||| + |||\Gamma(u-v)||| \le |||\Gamma(u)||| + 2a_1\sqrt{N/k}\ \delta.$$

Setting $\delta = \min\{1, \sqrt{k/N}/(8a_1)\}$ we obtain

$$\begin{aligned}
&\mathbb{P}\left(\left\{\omega \in \overline{\Omega}\ :\ \exists u \in \mathbb{R}^n\ :\ |||\Gamma u||| < h_L(u)/4\right\}\right)\\
&\quad = \ \mathbb{P}\left(\left\{\omega \in \overline{\Omega}\ :\ \exists u \in S\ :\ |||\Gamma u||| < 1/4\right\}\right)\\
&\quad \le \ \mathbb{P}\left(\left\{\omega \in \overline{\Omega}\ :\ \exists v \in A\ :\ |||\Gamma v||| < 1/2\right\}\right)\\
&\quad \le \ \exp\left(n\ln(3/\delta) - 0.3\ N^{1-\beta}n^{\beta}\right)\\
&\quad \le \ \exp\left(-N^{1-\beta}n^{\beta}/5\right)
\end{aligned}$$

for an appropriate choice of the absolute constant c_2 in

$$N/n \ge \left(c_2 \max\left\{\ln a_1, 1/(1-\beta)^2\right\}\right)^{1/(1-\beta)}.$$

The desired result follows since $h_K(u) \ge |||\Gamma u|||$ for every $u \in \mathbb{R}^n$ and since, by the assumption on Γ, we get

$$\mathbb{P}\left(\bar{\Omega}\right) \le \exp(-a_2 N).$$

This completes the proof. $\square$

Proof of Lemma 4.3: The proof mimics Montgomery-Smith's proof.

Assume first that α^2 is an integer, which we denote by m. Define the following norm on $\mathbb{R}^n$

$$\|z\| = \sup \sum_{i=1}^{m} \left(\sum_{k\in B_i} |z_k|^2\right)^{1/2}, \tag{31}$$

where the supremum is taken over all partitions $B_1, \ldots, B_m$ of $\{1, 2, \ldots, n\}$. It is known (see e.g. [M] for the proof) that

$$\|z\| \le 2h_L(z) \le \sqrt{2}\|z\|$$

for every $z \in \mathbb{R}^n$.

Given $z \in \mathbb{R}^n$, let $m' \leq m$ and let $B_1, \ldots, B_{m'}$ be a partition of $\{1, 2, \ldots, n\}$ such that

$$\|z\| = \sum_{i=1}^{m'} \left(\sum_{k \in B_i} |z_k|^2 \right)^{1/2}$$

and $\sum_{k \in B_i} |z_k|^2 \neq 0$ for every $i \leq m'$.

Then

$$\begin{aligned} P := \mathbb{P}\left(\sum_{i=1}^{n} \xi_i z_i > h_L(z) \right) &\geq \mathbb{P}\left(\sum_{i=1}^{n} \xi_i z_i > \|z\|/\sqrt{2} \right) \\ &= \mathbb{P}\left(\sum_{i=1}^{m'} \sum_{k \in B_i} \xi_k z_k > (1/\sqrt{2}) \sum_{i=1}^{m'} \left(\sum_{k \in B_i} |z_k|^2 \right)^{1/2} \right) \\ &\geq \mathbb{P}\left(\bigcap_{i \leq m'} \left(\sum_{k \in B_i} \xi_k z_k \geq (1/\sqrt{2}) (\sum_{k \in B_i} |z_k|^2)^{1/2} \right) \right). \end{aligned}$$

Since ξ_i's are independent we obtain

$$P \geq \prod_{i=1}^{m'} \mathbb{P}\left(\sum_{k \in B_i} \xi_k z_k > (1/\sqrt{2}) \left(\sum_{k \in B_i} |z_k|^2 \right)^{1/2} \right).$$

For $i \leq m'$ set

$$f_i = \left(\sum_{k \in B_i} \xi_k z_k \right) \cdot \left(\sum_{k \in B_i} |z_k|^2 \right)^{-1/2}.$$

Since ξ_i's are symmetric, by Lemma 3.6 we get

$$\begin{aligned} \mathbb{P}\left(f_i > 1/\sqrt{2} \right) &= \frac{1}{2} \, \mathbb{P}\left(|f_i| > 1/\sqrt{2} \right) \\ &\geq \frac{1}{2} \left(\frac{1 - 1/2}{2\mu^2} \right)^3 = \frac{1}{2^7 \mu^6}. \end{aligned}$$

Since $\mu \geq 1$, we obtain

$$P \geq \left(\frac{1}{2^7 \mu^6} \right)^{m'} \geq \left(\frac{1}{2^7 \mu^6} \right)^{m},$$

which implies the desired result for the case when α^2 is an integer. To complete the proof note that for every $\alpha \geq 1$, letting $m := \lceil \alpha^2 \rceil$, one has

$$B_\infty^n \cap \alpha B_2^n \subset B_\infty^n \cap \sqrt{m} B_2^n \quad \text{and} \quad m < 2\alpha^2.$$

$\square$

It is of interest to note that the radius of B_∞^n inside K_N obtained in Theorem 4.2 can be made as close to 1 as we wish. Indeed, we have the following sharper version of this theorem.

Theorem 4.5 *There exists an absolute constant $c_2 > 1$ such that for every $\beta, \delta \in (0,1)$, and $\varepsilon \in (0, 1/4)$ and every*

$$2^n \geq N \geq n \max\left\{\exp(C_{\mu,\delta}/\beta), \left((c_2/\varepsilon)\max\left\{\ln(a_1/\varepsilon), 1/(1-\beta)^2\right\}\right)^{1/(1-\beta)}\right\},$$

where $C_{\mu,\delta} = 9\ln(e\mu^2/\delta)$, one has

$$\mathbb{P}\left(K_N \supset (1-\varepsilon)(1-\delta)\left(B_\infty^n \cap RB_2^n\right)\right) \geq 1 - \exp\left(-n^\beta N^{1-\beta}/5\right) - \exp\left(-a_2 N\right),$$

with $R = \sqrt{\beta \ln(N/n)/C_{\mu,\delta}}$.

The proof of this Theorem follows the same lines as before. In particular, the only modifications needed in the actual proof of Theorem 4.2 is a more careful discussion of $|||\Gamma u|||$ and the cardinality of the corresponding sets, and a more precise approximation argument. We also need a more precise formulation of Lemma 4.3. Namely, given $\delta \in (0,1)$, Lemma 4.3 holds for $L = (1-\delta)(B_\infty^n \cap \alpha B_2^n)$ with $C_\mu = 9\ln(e\mu^2/\delta)$. To show this we consider the norm $\|\cdot\|'$ defined by the same formula as in (31), but with $m = 2\alpha^2$. Then for any $z \in \mathbb{R}^n$ we have $h_{B_\infty^n \cap \alpha B_2^n}(z) \leq \|z\|'$, and the rest of the argument is the same.

4.3 Geometric parameters of K_N

In this section we apply the main results of the previous section to obtain asymptotically sharp estimates for volumes of K_N, K_N^0 and the mean diameters $M(K_N)$, $M(K_N^0)$ of K_N and K_N^0, where $K_N = \Gamma^* B_1^N$ for $\Gamma \in \mathrm{M}_\psi(N, n, \mu)$. Recall that by Fact 2.4 for every $a_2 > 0$ one has $\mathrm{M}_\psi(N, n, \mu) \subset \mathrm{M}(N, n, \mu, a_1, a_2)$ with $a_1 = 6\mu\sqrt{a_2 + 4}$.

First we note that combining Corollary 4.1 and Theorem 4.2 we have the following result.

Theorem 4.6 *Let n, N be integers such that $n < N \le 2^n$ and let $\alpha = \alpha(N,n) = n/(N-n)$. Let $K_N = \Gamma^* B_1^N$, where $\Gamma \in \mathrm{M}(N,n,\mu,a_1,a_2)$. Then for every $0 < \beta \le 1/2$ one has*

$$\mathbb{P}\left(K_N \supset C(\alpha)\left(B_\infty^n \cap \sqrt{\beta \ln(2N/n)}B_2^n\right)\right) \ge p(N,n,\beta),$$

where

$$p(N,n,\beta) = 1 - \exp\left(-cn^\beta N^{1-\beta}\right) \quad \textit{and} \quad C(\alpha) = c_1 c_2^\alpha,$$

c_1, c_2 are positive constants depending only on a_1, μ; c is a positive constant depending only on a_2, μ.

Since $B_\infty^n \subset \sqrt{n}B_2^n$ we obtain

Corollary 4.7 *Under the assumptions of Theorem 4.6, for every $0 < \beta \le 1/2$ one has*

$$\mathbb{P}\left(K_N \supset C(\alpha)\sqrt{\frac{\beta\ln(2N/n)}{n}}B_\infty^n\right) \ge p(N,n,\beta),$$

where $C(\alpha)$ and $p(N,n,\beta)$ were introduced in Theorem 4.6.

Now we estimate the volumes of K_N and K_N^0 and obtain asymptotically sharp results. For technical reasons we separate upper and lower estimates (depending on the class M or M_ψ).

Corollary 4.7 and (30) immediately imply the following volume estimates for K_N and K_N^0 (cf. [GH]).

Theorem 4.8 *Let $n < N \le 2^n$. Let $K_N = \Gamma^* B_1^N$, where $\Gamma \in \mathrm{M}(N,n,\mu,a_1,a_2)$. There exists an absolute positive constant C such that for every $\beta \in (0,1/2)$ one has*

$$|K_N|^{1/n} \ge 2C(\alpha)\sqrt{\frac{\beta\ln(2N/n)}{n}} \quad \textit{and} \quad |K_N^0|^{1/n} \le \frac{C}{C(\alpha)\sqrt{\beta n \ln(2N/n)}},$$

with probability larger than or equal to $p(N,n,\beta)$, where $C(\alpha)$ and $p(N,n,\beta)$ were introduced in Theorem 4.6.

The following theorem is a consequence of a well known estimate ([BF], [CP], [G2]): let $z_i \in S^{n-1}$, $n \le k \le e^n$, then

$$| \text{ abs conv}\{z_i\}_{i\le k}|^{1/n} \le c\sqrt{\ln(2k/n)}/n, \tag{32}$$

where $c > 0$ is an absolute constant. This estimate, Fact 2.3, and (30) imply

Theorem 4.9 *Let $n < N \le 2^n$. Let $K_N = \Gamma^* B_1^N$, where $\Gamma \in \mathrm{M}_\psi(N, n, \mu)$. There exist absolute positive constants c and C such that one has*

$$|K_N|^{1/n} \le C\mu\sqrt{\frac{\ln(2N/n)}{n}} \quad \textit{and} \quad |K_N^0|^{1/n} \ge c/(\mu\sqrt{n\ln(2N/n)})$$

with probability larger than or equal to $1 - e^{-n}$.

Now we calculate the mean diameters $M(K_N)$ and $M(K_N^0)$ improving and extending results of [GH].

Theorem 4.10 *Let $n < N \le 2^n$. Let $K_N = \Gamma^* B_1^N$, where $\Gamma \in \mathrm{M}_\psi(N, n, \mu)$. There exists an absolute positive constant c such that*

$$M(K_N) \ge c/\sqrt{\ln(2N/n)}$$

with probability larger than or equal to $1 - e^{-n}$.

Furthermore, there exists an absolute positive constant C such that for every $\beta \in (0, 1/2)$ and every $\Gamma \in \mathrm{M}(N, n, \mu, a_1, a_2)$ one has

$$M(K_N) \le CC^{-1}(\alpha)\left(1/\sqrt{\beta\ln(2N/n)} + \sqrt{(\ln(2n))/n}\right)$$

with probability larger than or equal to $p(N, n, \beta)$, where $C(\alpha)$ and $p(N, n, \beta)$ were introduced in Theorem 4.6.

Proof: By (29) and Theorem 4.9 there exists an absolute positive constant c_1 such that

$$M(K_N) \ge (|B_2^n|/|K_N|)^{1/n} \ge c_1/(\mu\sqrt{\ln(2N/n)}),$$

with probability larger than or equal to $1 - e^{-n}$.

To prove the upper estimate we use Theorem 4.6:

$$\begin{aligned} M(K_N) &\le M\left(C(\alpha)\left(B_\infty^n \cap \sqrt{\beta \ln(2N/n)} B_2^n\right)\right) \\ &\le (1/C(\alpha))\left(M\left(B_\infty^n\right) + M\left(\sqrt{\beta \ln(2N/n)} B_2^n\right)\right), \end{aligned}$$

which implies the required result. □

Remark. Note that by Theorem 4.10, for $N \le \exp(n/\ln(2n))$ we have

$$M(K_N) \approx 1/\sqrt{\ln(2N/n)}.$$

If $N \ge \exp(n/\ln(2n))$ there is a gap between lower and upper estimates. Both estimates could be asymptotically sharp. Indeed, as it follows from remark after Theorem 4.2, the lower estimate is sharp for the case of Gaussian random matrix. The upper estimate is sharp for the case of ± 1 random matrix (see Section 4.4 below).

Theorem 4.11 *Let $n < N \le 2^n$. Let $K_N = \Gamma^* B_1^N$, where $\Gamma \in \mathrm{M}_\psi(N, n, \mu)$. There exists an absolute positive constant C such that*

$$M(K_N^0) \le C\mu\sqrt{\ln(2N)}$$

with probability larger than or equal to $1 - e^{-n}$.

Furthermore, there exists an absolute positive constant c such that for every $\beta \in (0, 1/2)$ and every $\Gamma \in \mathrm{M}(N, n, \mu, a_1, a_2)$ one has

(i) for $N \le n^2$

$$M(K_N^0) \ge c\sqrt{\ln(2 + n/a_1^2)}$$

with probability larger than or equal to

$$1 - \exp\left(-a_2 N\right) - \exp\left(-nN/(32\mu^4 \ln^2(2\mu))\right);$$

(ii) for $N > n^2$

$$M(K_N^0) \ge c_0\sqrt{\beta \ln(2N)}$$

with probability larger than or equal to $p(N, n, \beta)$, where $p(N, n, \beta)$ was introduced in Theorem 4.6, and c_0 is a constant depending only on a_1, a_2 and μ.

Proof: Let $G = \sum_{i=1}^n g_i e_i$. Recall that K_N is the absolute convex hull of N vertices $x_i = \Gamma^* e_i$. Thus we have

$$M(K_N^0) \leq \frac{c_1}{\sqrt{n}} \mathbb{E} \|G\|_{K_N^0} = \frac{c_1}{\sqrt{n}} \mathbb{E} \max_{i \leq N} \langle G, x_i \rangle ,$$

where c_1 is an absolute constant. By Fact 2.3 we obtain that with probability larger than or equal to $1 - e^{-n}$ one has $|x_i| \leq \mu \sqrt{3n}$ for every $i \leq N$. Using standard estimate for the expectation of maximum of Gaussian random variables (see e.g. [P]), we obtain that there is an absolute constant c_2 such that

$$M(K_N^0) \leq c_2 \mu \ \sqrt{\ln(2N)},$$

with probability larger than or equal to $1 - e^{-n}$.

The second estimate follows from the Bourgain-Tzafriri theorem ([BT]). However, the application of Vershynin's extension ([V]) of results from [BT] is easier and leads to slightly better probability estimates. Let $\| \cdot \|_{hs}$ denote Hilbert-Schmidt norm and denote $A = \|\Gamma^*\|_{hs}$, $B = \|\Gamma^*\|$. Vershynin's theorem implies that there exists $\sigma \subset \{1, \ldots, N\}$ of cardinality larger than $A^2/(2B^2)$ such that for all $i \in \sigma$ one has $|\Gamma^* e_i| \geq c_3 A/\sqrt{N}$, where c_3 is an absolute positive constant, and vectors $\Gamma^* e_i$, $i \in \sigma$, are almost orthogonal (up to an absolute positive constant). Recall that with probability greater than $1 - \exp(-a_2 N)$, one has $B \leq a_1 \sqrt{N}$. By Fact 2.5, $A \geq \sqrt{nN}/2$ with probability greater than $1 - \exp(-nN/(32\mu^4 \ln^2(2\mu)))$. Thus, with probability greater than $1 - \exp(-a_2 N) - \exp(-nN/(32\mu^4 \ln^2(2\mu)))$ there exists $\sigma \subset \{1, \ldots, n\}$ of cardinality larger than $n/(8a_1^2)$ such that $|\Gamma^* e_i| \geq c_3 \sqrt{n}/2$ for $i \in \sigma$ and $\{\Gamma^* e_i\}_{i \in \sigma}$ are almost orthogonal. Now,

$$M(K_N^0) \geq \frac{1}{\sqrt{n}} \mathbb{E} \|G\|_{K_N^0} = \frac{1}{\sqrt{n}} \mathbb{E} \max_{i \leq N} \langle G, \Gamma^* e_i \rangle \geq \frac{1}{\sqrt{n}} \mathbb{E} \max_{i \in \sigma} \langle G, \Gamma^* e_i \rangle .$$

Since $\{\Gamma^* e_i\}_{i \in \sigma}$ are almost orthogonal, by Sudakov inequality (see e.g. [P]), the last expectation is greater than $c_4 \sqrt{\ln(2 + n/a_1^2)}$, where c_4 is an absolute constant. This proves the second estimate.

To prove the third estimate we use again (29):

$$M(K_N^0) \geq \left(|B_2^n| / |K_N^0| \right)^{1/n} .$$

The result follows by Theorem 4.8, since $\alpha \leq 1$ and $\ln(2N/n) \geq (1/2) \ln(2N)$ in the case $N > n^2$. $\Box$

4.4 The case of ± 1 random matrix

Here we briefly discuss improvements and simplifications that can be done in the case of ± 1 random matrix.

1. If Γ is the ± 1 random matrix, then $K_N =$ abs conv $\{x_i\}_{i \le N}$, where x_i's are vertices of the cube. Thus we have $|x_i| = \sqrt{n}$ for all $i \le N$ and we do not need to use Fact 2.3. Therefore, in this case, the estimate $1 - e^{-n}$ for the probability in Theorems 4.9, 4.10, 4.11 can be substituted with 1. Moreover, since $K_N \subset B_\infty^n$, we obtain

$$M(K_N) \ge M(B_\infty^n) \ge c\sqrt{(\ln n)/n}$$

improving the result of Theorem 4.10 to the best possible one.

2. We also mention that using Sauer-Shelah lemma, one can prove that

$$M^*(K_N) \ge C_\gamma \sqrt{\ln N}$$

with probability larger than $1 - \exp(-c_1 N)$ for $N \ge 2^{\gamma n}$, where $\gamma \in (0,1)$, $C_\gamma = c_2\sqrt{\gamma}/\ln(e/\gamma)$, and c_1, c_2 are absolute constants.

3. It follows from (32) that if $L_N \subset \mathbb{R}^n$ is the absolute convex hull of $N \le e^n$ points with Euclidean norm $\sqrt{n}$ then

$$|L_N|^{1/n} \le c\sqrt{\frac{\ln(N/n)}{n}},$$

where C is an absolute positive constant. Thus Theorem 4.8 says that the volume of a random polytope K_N is of the same order as the largest possible one. A concrete example of an n-dimensional polytope L_N with N vertices, all of them of Euclidean norm $\sqrt{n}$, and satisfying

$$|L_N|^{1/n} \ge c\sqrt{\frac{\ln(N/n)}{n}}$$

for some absolute positive constant c, was constructed in [CP] and [G2]. This polytope is not a 0-1 polytope. We show here that such a 0-1 polytope does exist. Let us come back to our setting and consider vertices of the hypercube $\{-1,1\}^n$.

Let q be a power of 2 and $W = (w_{jk})_{1\le j\le q, 1\le k\le q}$ be a fixed ± 1 Hadamard $q \times q$ matrix. Let $p \ge 1$ and let S be the set of all p by q matrices

$(\varepsilon_i w_{jk})_{1\le i\le p, 1\le j\le q}$ where (ε_i) runs over the 2^p choices of signs and $k = 1, \ldots, q$. The cardinality of S is $q2^p$. Let $n := pq$ and let P be the convex hull of these $N = q2^p$ points in $\mathbb{R}^n$. Then P is a ± 1 polytope. Because of the property of the Hadamard matrix, $\mathbb{R}^n$ admits an orthogonal decomposition by q linear spaces E_i of dimension p such that P is the convex hull of q hypercubes lying respectively in E_i, $1 \le i \le q$ and with edges of length $2\sqrt{q}$. An easy computation shows that

$$|P| = (2\sqrt{q})^n \frac{(p!)^q}{n!}.$$

Therefore

$$|P|^{1/n} \ge 2\sqrt{q}\frac{p}{en} = \frac{2}{e\sqrt{q}}.$$

Since $N/n = 2^p/p \le 2^p$, one has

$$\frac{\log(N/n)}{n} \le \frac{p\log 2}{n} = \frac{\log 2}{q}.$$

Therefore

$$|P|^{1/n} \ge \frac{2}{e\sqrt{q}} \ge \frac{2}{e\sqrt{\log 2}}\sqrt{\frac{\ln(N/n)}{n}}.$$

4. Let P be ± 1 polytope in $\mathbb{R}^n$ with $N = n^2$ vertices and such that

$$(1/\lambda)B_\infty^n \subset P \subset B_\infty^n,$$

with $\lambda = O(\sqrt{n/\ln n})$. Such a polytope exists by Corollary 4.7. Following the language and the method of [BGKKLS], if C is a convex body given by a strong separation oracle, one can construct an algorithm that gives in a polynomial time and with any given accuracy the inradius $\tilde{m}$ of C with respect to P (the biggest number such that $\tilde{m}P \subset C$). From this one gets the estimates $(1/\lambda)\tilde{m} \le m \le \tilde{m}$ of the inradius m of C with respect to B_∞^n. Therefore there exists a polynomial time algorithm that gives estimates of m with accuracy $\lambda = O(\sqrt{n/\ln n})$. As proved in [BGKKLS], this is the best possible order. Unfortunately, we do not know any explicit construction of such a polytope P.

References

[BY] Z. D. Bai and Y. Q. Yin, *Limit of the smallest eigenvalue of a large dimensional sample covariance matrix*, Ann. Probab. 21 (1993), 1275–1294.

[BF] I. Bárány, Z. Füredy, *Approximation of the sphere by polytopes having few vertices,* Proc. Amer. Math. Soc. 102 (1988), no. 3, 651–659.

[BP] I. Bárány and A. Pór, *On 0-1 Polytopes with many facets,* Adv. Math. 161 (2001), 209-228.

[BM] J. Bourgain and V. D. Milman, *New volume ratio properties for symmetric bodies in* $\mathbb{R}^n$, Invent. Math. 88 (1987), no 2, 319–340.

[BT] J. Bourgain and L. Tzafriri, *Invertibility of "large" submatrices with applications to the geometry of Banach spaces and harmonic analysis*, Israel J. Math. 57 (1987), 137–224.

[BGKKLS] A. Brieden, P. Gritzmann, R. Kannan, V. Klee, L. Lovász and M. Simonovits, *Deterministic and randomized polynomial-time approximation of radii*, Mathematika 48 (2001), No.1-2, 63-105.

[CP] B. Carl and A. Pajor, *Gelfand numbers of operators with values in a Hilbert space,* Invent. Math. **94** (1988), 479–504.

[DS] K.R. Davidson and S.J. Szarek, *Local operator Theory, Random Matrices and Banach spaces,* In:"Handbook in Banach Spaces" Vol I, ed. W. B. Johnson, J. Lindenstrauss, Amsterdam: Elsevier (2001), 317–366.

[DFM] M. E. Dyer, Z. Füredi and C. McDiarmid, *Volumes spanned by random points in the hypercube,* Random structures Algorithms 3 (1992), 91-106.

[E] A. Edelman, *Eigenvalues and condition numbers of random matrices,* SIAM J. Matrix Anal. Appl., 9 (1988), 543–560.

[GH] A. Giannopoulos, M. Hartzoulaki, *Random spaces generated by vertices of the cube*, Discrete Comp. Geom., 28 (2002), 255–273.

[G1] E. D. Gluskin, *The diameter of Minkowski compactum roughly equals to n.* Funct. Anal. Appl., 15 (1981), 57–58 (English translation).

[G2] E. D. Gluskin, *Extremal properties of orthogonal parallelepipeds and their applications to the geometry of Banach spaces*, (Russian) Mat. Sb. (N.S.) 136 (178) (1988), no. 1, 85–96; translation in Math. USSR-Sb. 64 (1989), no. 1, 85–96.

[Go] Y. Gordon, *Some inequalities for Gaussian processes and applications,* Israel J. of Math., 50 (1985), 265–289.

[H] U. Haagerup, *The best constants in the Khintchine inequality*, Studia Math. 70 (1981), 231–283.

[Ho] W. Hoeffding, *Probability inequalities for sums of bounded variables*, Journal of the American Statistical Association, 58 (1963), 13–30.

[KKS] J. Kahn, J. Komlós and E. Szemerédi, *On the probability that a random* ± 1 *matrix is singular*, J. Amer. Math. Soc. 8 (1995), 223–240.

[L] M. Ledoux, *The concentration of measure phenomenon*, Mathematical Surveys and Monographs, American Math. Society, Providence, 2001.

[LPRTV] A. E. Litvak, A. Pajor, M. Rudelson, N. Tomczak-Jaegermann, R. Vershynin, *Random Euclidean embeddings in spaces of bounded volume ratio*, C. R. Acad. Sci. Paris, 339 (2004), 33–38.

[MT] P. Mankiewicz and N. Tomczak-Jaegermann, *Quotients of finite-dimensional Banach spaces; random phenomena.* In:"Handbook in Banach Spaces" Vol II, ed. W. B. Johnson, J. Lindenstrauss, Amsterdam: Elsevier (2003), 1201–1246.

[MP] V. A. Marchenko and L. A. Pastur, *Distribution of eigenvalues in certain sets of random matrices*, Mat. Sb. (N.S.), 72 (1967), 407–535 (Russian).

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

[M] S. J. Montgomery-Smith, *The distribution of Rademacher sums*, Proc. Amer. Math. Soc. 109 (1990), no. 2, 517–522.

[P] G. Pisier, *The Volume of Convex Bodies and Banach Space Geometry.* Cambridge University Press, Cambridge, 1989.

[Si] J. W. Silverstein, *The smallest eigenvalue of a large dimensional Wishart matrix*, Ann. Probab. 13 (1985), 1364–1368.

[St] D. Stroock, *Probability theory. An analytic view*, Cambridge Univ. Press 1993.

[Sz] S. J. Szarek, *The finite-dimensional basis problem with an appendix on nets of Grassman manifold*, Acta Math. 141 (1983), 153–179.

[T] N. Tomczak-Jaegermann, *Banach-Mazur distances and finite-dimensional operator ideals.* Pitman Monographs and Surveys in Pure and Applied Mathematics, 38. Longman Scientific & Technical, Harlow; co-published in the United States with John Wiley & Sons, Inc., New York, 1989.

[V] R. Vershynin, *John's decompositions: selecting a large part*, Israel J. Math. 122 (2001), 253–277.

[Z] G. M. Ziegler, *Lectures on 0/1 polytopes,* in "Polytopes-Combinatorics and Computation" (G. Kalai and G. M. Ziegler, Eds), pp. 1-44, DMV Seminars, Birkhäuser, Basel, 2000.

A. E. Litvak and N. Tomczak-Jaegermann, Dept. of Math. and Stat. Sciences, University of Alberta, Edmonton, Alberta, Canada, T6G 2G1.
e-mails: alexandr@math.ualberta.ca and ntomczak@math.ualberta.ca

A. Pajor, Equipe d'Analyse et Mathmatiques Appliques, Université de Marne-la-Vallée, 5, boulevard Descartes, Champs sur Marne, 77454 Marne-la-Vallée Cedex 2, France
email: pajor@math.univ-mlv.fr

M. Rudelson, Dept. of Math., 202 Math. Sciences Bldg., University of Missouri, Columbia, MO 65211, USA.
email: rudelson@math.missouri.edu