ISRAEL JOURNAL OF MATHEMATICS **138** (2003), 139–156

INTEGRAL KAŠIN SPLITTINGS

BY

GREG W. ANDERSON

Department of Mathematics, University of Minnesota
Minneapolis, MN 55455, USA
e-mail: gwanders@math.umn.edu

ABSTRACT

For $x \in \mathbb{R}^n$ and $p \geq 1$ put $\|x\|_p := (n^{-1} \sum |x_i|^p)^{1/p}$. An orthogonal direct sum decomposition $\mathbb{R}^{2k} = E \oplus E^\perp$ where $\dim E = k$ and $\sup_{0 \neq x \in E \cup E^\perp} \|x\|_2 / \|x\|_1 \leq C$ is called here a (k, C)-**splitting**. By a theorem of Kašin there exists $C > 0$ such that (k, C)-splittings exist for all k, and by the volume ratio method of Szarek one can take $C = 32e\pi$. All proofs of existence of (k, C)-splittings heretofore given are nonconstructive.

Here we investigate the representation of (k, C)-splittings by matrices with integral entries. For every $C > 8e^{1/2}\pi^{-1/2}$ and positive integer k we specify a positive integer $N(k, C)$ such that in the set of k by $2k$ matrices with integral entries of absolute value not exceeding $N(k, C)$ there exists a matrix with row span a summand in a (k, C)-splitting. We have $N(k, C) \leq 2^{18k}$ for k large enough depending on C. We explain in detail how to test a matrix for the property of representing a (k, C)-splitting. Taken together our results yield an explicit (if impractical) construction of (k, C)-splittings.

1. Introduction

For $p \geq 1$ and $x \in \mathbb{R}^n$ put

$$\|x\|_p := \left(\frac{1}{n} \sum_{i=1}^{n} |x_i|^p \right)^{1/p},$$

noting that

$$\|x\|_1 \leq \|x\|_2 \leq \sqrt{n}\, \|x\|_1 .$$

Received October 28, 2002

For any nonzero subspace $E \subset \mathbb{R}^n$ put

$$J_E^n := \sup_{0 \neq x \in E} \frac{\|x\|_2}{\|x\|_1}.$$

In [Kašin] it was proved that

$$K := \sup_{k=1}^{\infty} \inf_{\substack{E \subset \mathbf{R}^{2k} \\ \dim E = k}} \max(J_E^{2k}, J_{E^\perp}^{2k}) < \infty$$

where $E^\perp$ denotes the orthogonal complement of E with respect to the standard inner product in $\mathbb{R}^{2k}$. See [Pisier, Chap. 6] for a proof by the volume ratio method of [Szarek] that

$$K \leq 32e\pi = 273.2714951\ldots$$

and for many references related to Kašin's result. In this paper we prove that

$$K \leq 8e^{1/2}\pi^{-1/2} = 7.441530936\ldots$$

as a byproduct of our investigation. We shall call any orthogonal direct sum decomposition of the form

$$\mathbb{R}^{2k} = E \oplus E^\perp, \dim E = k, \max(J_E^{2k}, J_{E^\perp}^{2k}) \leq C$$

a (k, C)**-splitting**.

Suppose now that E is a k-dimensional subspace of $\mathbb{R}^{2k}$ chosen randomly with respect to the unique $O(2k)$-invariant probability measure on the Grassmannian. What actually is proved in [Pisier] is the probabilistic assertion that

$$\mathbf{P}[J_E^{2k} > 32e\pi] < 2^{-k}.$$

Since the map $E \mapsto E^\perp$ is measure-preserving, one obtains the lower bound

$$\mathbf{P}\begin{bmatrix} E \text{ is a summand in} \\ \text{a } (k, 32e\pi)\text{-splitting} \end{bmatrix} > 1 - 2 \cdot 2^{-k}$$

as an immediate corollary. This and all other proofs of existence of (k, C)-splittings heretofore given are rather vexingly nonconstructive; cf. [Pisier, Chap. 6, p. 95, Remark].

In this paper we study the problem of representing (k, C)-splittings by matrices with integral entries. Our main result (Theorem 7.2 below) is roughly as follows. For every positive integer k and number $C > 8e^{1/2}\pi^{-1/2}$, we specify a positive integer $N(k, C)$ such that in the set of k by $2k$ matrices with integral entries

of absolute value not exceeding $N(k,C)$ there exists a matrix with row span a summand in a (k,C)-splitting. Our bound $N(k,C)$ grows moderately: we have $N(k,C) \leq 2^{18k}$ for k large enough depending on C. Explicit formulas for J_E^{2k} and $J_{E^\perp}^{2k}$ in terms of the maximal minors of any k by $2k$ matrix with row span E play an important role in our method; see §2 for these formulas. Since it is possible to decide in a mechanical way whether or not a given k by $2k$ matrix defines a (k,C)-splitting, our results together yield an explicit (if quite impractical) construction of (k,C)-splittings.

Of course the construction of (k,C)-splittings presented here is far from being the most elegant one imaginable. The situation in which we find ourselves at present is analogous to that in the early stages of the theory of expanding graphs: we have only probabilistic existence proofs and no methods of construction save woefully impractical exhaustive searches. But the theory of expanding graphs has in recent times been revolutionized by explicit constructions based on deep results in number theory, algebraic geometry and representation theory. See [Lubotzky] for an account of these developments. By analogy it is conceivable that an aesthetically satisfying explicit construction of (k,C)-splittings could emerge from number theory and allied branches of mathematics. We wrote this paper in order to stimulate interest in the search for such a construction.

2. Explicit calculation of J_E^{2k} and $J_{E^\perp}^{2k}$

2.1. LINEAR AND QUADRATIC PROGRAMMING. Let V be a real vector space of finite dimension equipped with a positive definite inner product $\langle \cdot, \cdot \rangle$. Fix $b \in V$ and a real constant c. Put

$$\phi(v) := \langle v, v \rangle + \langle b, v \rangle + c$$

for all $v \in V$, thereby defining a quadratic function ϕ on V satisfying the Maximum Principle. Let $\lambda_1, \ldots, \lambda_p, \lambda_{p+1}, \ldots, \lambda_{p+q}$ be affine functionals on V and put

$$\Delta := \left(\bigcap_{i=1}^{p} \{\lambda_i \geq 0\} \right) \cap \left(\bigcap_{i=p+1}^{p+q} \{\lambda_i = 0\} \right) \subset V.$$

Assume that the closed convex set Δ is nonempty and bounded. Necessarily there exists a point $v_0 \in \Delta$ such that

$$\phi(v_0) = \sup_{v \in \Delta} \phi(v).$$

Put

$$I := \{i \in \{1, \ldots, p+q\}: \lambda_i(v_0) = 0\}.$$

We claim that:

> The family $\{\lambda_i\}_{i \in I}$ spans the space of affine functionals on V modulo constants.

Suppose rather that this is not the case. Without loss of generality we may assume that $v_0 = 0$. Moreover, after replacing V by its positive-dimensional subspace $\bigcap_{i \in I}\{\lambda_i = 0\}$, we may assume that $I = \emptyset$. Then the origin is an interior point of Δ at which ϕ attains its maximum. But this is a contradiction because ϕ satisfies the Maximum Principle. The claim is proved.

2.2. CHARACTERIZATION OF J_E^{2k} IN FINITE TERMS. Fix a positive integer k and a subspace $E \subset \mathbb{R}^{2k}$ of dimension k. For each vector

$$\epsilon = (\epsilon_1, \ldots, \epsilon_{2k}) \in \{\pm 1\}^{2k}$$

put

$$\Delta_\epsilon := \left\{x \in \mathbb{R}^{2k}: \frac{1}{2k}\sum_{i=1}^{2k} \epsilon_i x_i = 1, \min_{i=1}^{2k} \epsilon_i x_i \geq 0\right\}.$$

For each subset

$$I \subset \{1, \ldots, 2k\}$$

put

$$E_I := \{x \in E: x_i = 0 \text{ for } i \in I\}.$$

If $E \cap \Delta_\epsilon \neq \emptyset$, then we have

$$\sup_{x \in E \cap \Delta_\epsilon} \|x\|_2 = \max_{\substack{I \subset \{1, \ldots, 2k\} \\ \#I = k-1 \\ \dim E_I = 1 \\ E_I \cap \Delta_\epsilon \neq \emptyset}} \max_{x \in E_I \cap \Delta_\epsilon} \|x\|_2$$

by straightforward application of the optimization principle enunciated in the preceding paragraph. It follows that

$$J_E^{2k} = \max_{\substack{I \subset \{1, \ldots, 2k\} \\ \#I = k-1 \\ \dim E_I = 1}} \max_{0 \neq x \in E_I} \frac{\|x\|_2}{\|x\|_1}$$

because the union of the sets Δ_ϵ is the unit sphere $\{\|x\|_1 = 1\} \subset \mathbb{R}^{2k}$.

2.3. NOTATION FOR DETERMINANTS OF SQUARE SUBMATRICES. Let A be an m by n matrix. Let

$$I = \{i_1 < \cdots < i_\nu\} \subset \{1, \ldots, m\}, \quad J = \{j_1 < \cdots < j_\nu\} \subset \{1, \ldots, n\}$$

be sets of the same cardinality ν. We write

$$A_{IJ} := \det_{\alpha,\beta=1}^{\nu} A_{i_\alpha, j_\beta}.$$

This notation is going to be used on several occasions in the sequel.

LEMMA 2.4: *Let A be a k by $2k$ matrix with real entries and of full rank. Let $E \subset \mathbb{R}^{2k}$ be the k-dimensional subspace spanned by the rows of A. Let $I \subset \{1, \ldots, 2k\}$ be a subset of cardinality $k-1$.*

(i) *The following three conditions are equivalent:*

- *E_I is one-dimensional.*
- *The columns of A with indices in I are linearly independent.*
- *$A_{\{1,\ldots,k\}, I\cup\{i\}} \neq 0$ for some $i \in \{1, \ldots, 2k\} \setminus I$.*

(ii) *Under the equivalent conditions above we have*

$$\max_{0\neq x\in E_I} \frac{\|x\|_2}{\|x\|_1} = \frac{\sqrt{\frac{1}{2k}\sum_{i\in\{1,\ldots,2k\}\setminus I} |A_{\{1,\ldots,k\}, I\cup\{i\}}|^2}}{\frac{1}{2k}\sum_{i\in\{1,\ldots,2k\}\setminus I} |A_{\{1,\ldots,k\}, I\cup\{i\}}|}.$$

Proof: (i) Since A is of full rank, the equivalence of the three conditions is clear.

(ii) After permuting the columns of A suitably, we may assume without loss of generality that $I = \{1, \ldots, k-1\}$ and that the leftmost k by k block of A is nonsingular. After left-multiplying A by a suitably chosen invertible k by k matrix, we may further assume that the leftmost k by k block of A is the k by k identity matrix. Then the subspace E_I is spanned by the last row of A and we have

$$A_{ki} = \begin{cases} 0 & \text{for } i = 1, \ldots, k-1, \\ A_{\{1,\ldots,k\},\{1,\ldots,k-1\}\cup\{i\}} & \text{for } i = k, \ldots, 2k, \end{cases}$$

whence the result. ∎

LEMMA 2.5: *Let A, E and I be as in the preceding lemma. Let $E_I^\perp = (E^\perp)_I$.*

(i) *The following three conditions are equivalent:*

- *$E_I^\perp$ is one-dimensional.*
- *Some k among the columns of A with indices in $\{1, \ldots, 2k\} \setminus I$ are linearly independent.*
- *$A_{\{1,\ldots,k\},\{1,\ldots,2k\}\setminus(I\cup\{i\})} \neq 0$ for some $i \in \{1, \ldots, 2k\} \setminus I$.*

(ii) *Under the equivalent conditions above we have*

$$\max_{0\neq x\in E_I^\perp} \frac{\|x\|_2}{\|x\|_1} = \frac{\sqrt{\frac{1}{2k}\sum_{i\in\{1,\dots,2k\}\setminus I} |A_{\{1,\dots,k\},\{1,\dots,2k\}\setminus(I\cup\{i\})}|^2}}{\frac{1}{2k}\sum_{i\in\{1,\dots,2k\}\setminus I} |A_{\{1,\dots,k\},\{1,\dots,2k\}\setminus(I\cup\{i\})}|}.$$

Proof: (i) Let $e_1,\dots,e_{2k}$ be the standard basis of $\mathbb{R}^{2k}$. View the e_i as row vectors. Since A is of full rank, each of the given three conditions is equivalent to the linear independence of the family of vectors $\{\text{rows of } A\}\cup\{e_i\}_{i\in I}$.

(ii) After permuting the columns of A suitably we may assume without loss of generality that $I=\{1,\dots,k-1\}$ and that the rightmost k by k block of A is nonsingular. After left-multiplying A by a suitable k by k invertible matrix we may assume that the rightmost k by k block of A is the k by k identity matrix. Now decompose A into side by side k by k blocks, writing $A=[X,1]$, and put $B=[1,-X^T]$. Then $E^\perp$ is the row span of B, $E_I^\perp$ is spanned by the last row of B and we have

$$B_{ki} = \begin{cases} 0 & \text{for } i=1,\dots,k-1, \\ \pm A_{\{1,\dots,k\},\{k,\dots,2k\}\setminus\{i\}} & \text{for } i=k,\dots,2k, \end{cases}$$

whence the result. ∎

2.6. DETERMINANTAL FORMULAS FOR J_E AND $J_{E^\perp}$. Let A be a k by $2k$ matrix with real entries and of full rank. Let $E\subset\mathbb{R}^{2k}$ be the k-dimensional subspace of $\mathbb{R}^{2k}$ spanned by the rows of A. In order to abbreviate notation, for each subset $I\subset\{1,\dots,2k\}$ put $I^*:=\{1,\dots,2k\}\setminus I$ and if $\#I=k$ put $A_I:=A_{\{1,\dots,k\},I}$, where the latter notation is as defined in §2.3. By Lemma 2.4 and the last formula of §2.2 we have

$$J_E^{2k} = \sqrt{\frac{2k}{k+1}} \max_{\substack{I\subset\{1,\dots,2k\}\\ \#I=k+1\\ \{i\in I:\ A_{I^*\cup\{i\}}\neq 0\}\neq\emptyset}} \frac{\sqrt{\frac{1}{\#I}\sum_{i\in I}|A_{I^*\cup\{i\}}|^2}}{\frac{1}{\#I}\sum_{i\in I}|A_{I^*\cup\{i\}}|}.$$

By Lemma 2.5 and the last formula of §2.2 we have

$$J_{E^\perp}^{2k} = \sqrt{\frac{2k}{k+1}} \max_{\substack{I\subset\{1,\dots,2k\}\\ \#I=k+1\\ \{i\in I:\ A_{I\setminus\{i\}}\neq 0\}\neq\emptyset}} \frac{\sqrt{\frac{1}{\#I}\sum_{i\in I}|A_{I\setminus\{i\}}|^2}}{\frac{1}{\#I}\sum_{i\in I}|A_{I\setminus\{i\}}|}.$$

Thus it can be decided in a mechanical (if terribly laborious) way if $E\subset\mathbb{R}^{2k}$ is a summand in a (k,C)-splitting.

2.7. REMARK. In the rest of the paper we study the right sides of the formulas above for various random matrices A with i.i.d. entries.

3. Existence of $(k, 8e^{1/2}\pi^{-1/2})$-splittings

3.1. VOLUME RATIOS. Let λ_n be Lebesgue measure on $\mathbb{R}^n$. We have

$$\int_{\mathbb{R}^n} e^{-\|x\|_p^p} d\lambda_n(x) = \int_0^\infty \lambda_n\{\|x\|_p < u^{1/p}\} e^{-u} du$$

and hence

$$\lambda_n\{\|x\|_p \le 1\} = \frac{(2\int_0^\infty e^{-t^p/n} dt)^n}{\int_0^\infty u^{n/p} e^{-u} du} = \frac{2^n n^{n/p} \Gamma(1+1/p)^n}{\Gamma(1+n/p)}.$$

Recall Stirling's formula:

$$\Gamma(t) = \sqrt{2\pi} t^{t-1/2} e^{-t} e^{\theta(t)/12t} \quad (t > 0, 0 < \theta(t) < 1).$$

Combining the formulas above we obtain an estimate

$$\left(\frac{\lambda_n\{\|x\|_p \le 1\}}{\lambda_n\{\|x\|_2 \le 1\}}\right)^{1/n} \le \frac{\Gamma(1+1/p) p^{1/p} e^{1/p}}{\Gamma(1+1/2) 2^{1/2} e^{1/2}} \cdot \left(\frac{p^{1/2}}{2^{1/2}} e^{1/6n}\right)^{1/n}$$

such that left and right sides tend to a common limit as $n \to \infty$. In particular, we have a sharp inequality

$$\left(\frac{\lambda_n\{\|x\|_1 \le 1\}}{\lambda_n\{\|x\|_2 \le 1\}}\right)^{1/n} < 2^{1/2} e^{1/2} \pi^{-1/2};$$

cf. [Pisier, Chap. 6, p. 89].

PROPOSITION 3.2: *Let* $\mathbf{X}$ *be any* $\mathbb{R}^n$*-valued random variable with rotationally invariant distribution. We have*

$$\mathbf{P}[\|\mathbf{X}\|_2 > \beta^{-1} \cdot 2^{1/2} e^{1/2} \pi^{-1/2} \cdot \|\mathbf{X}\|_1] \le \beta^n$$

for all $0 < \beta < 1$. *(Estimates of this sort are characteristic of the volume ratio method of* [Szarek].*)*

Proof: Let σ_{n-1} be the unique rotationally invariant probability measure on the sphere $\{\|x\|_2 = 1\} \subset \mathbb{R}^n$. In general, for any Banach norm $\|\cdot\|$ on $\mathbb{R}^n$, we have

$$\int_{\|x\|_2=1} \|x\|^{-n} d\sigma_{n-1}(x) = \frac{\lambda_n\{\|x\| \le 1\}}{\lambda_n\{\|x\|_2 \le 1\}};$$

cf. [Pisier, Chap. 6, p. 91]. In particular, we have

$$\int_{\|x\|_2=1} \|x\|_1^{-n} d\sigma_{n-1}(x) < (2e/\pi)^{n/2},$$

and hence by Markov's inequality

$$\sigma_{n-1}\{\|x\|_1^{-1} > \beta^{-1} \cdot 2^{1/2}e^{1/2}\pi^{-1/2}\} \leq \beta^n$$

for all $0 < \beta < 1$. From the latter the claimed inequality follows by, say, conditioning on $\|\mathbf{X}\|_2$. ∎

PROPOSITION 3.3: *For every positive integer k there exists a $(k, 8e^{1/2}\pi^{-1/2})$-splitting. (This is a version of the main result of* [Kašin] *with an explicit constant.)*

Proof: Let A be a k by $2k$ matrix with i.i.d. Gaussian entries of mean 0 and positive variance. For each subset $I \subset \{1, \ldots, 2k\}$, to abbreviate notation, put $I^* := \{1, \ldots, 2k\} \setminus I$ and if $\#I = k$ put $A_I := A_{\{1,\ldots,k\},I}$; see §2.3 for the latter notation. Since the set of k by k real matrices with vanishing determinant is of Lebesgue measure zero within the space of all such matrices, we have

$$\mathbf{P}[A_I \neq 0 \text{ for all subsets } I \subset \{1, \ldots, 2k\} \text{ of cardinality } k] = 1,$$

and in particular A is certain to be of full rank. We have

$$\mathbf{P}\left[\sqrt{\frac{1}{\#I}\sum_{i\in I}|A_{I^*\cup\{i\}}|^2} > 4 \cdot 2^{1/2}e^{1/2}\pi^{-1/2} \cdot \frac{1}{\#I}\sum_{i\in I}|A_{I^*\cup\{i\}}|\right] \leq 4^{-\#I}$$

and

$$\mathbf{P}\left[\sqrt{\frac{1}{\#I}\sum_{i\in I}|A_{I\setminus\{i\}}|^2} > 4 \cdot 2^{1/2}e^{1/2}\pi^{-1/2} \cdot \frac{1}{\#I}\sum_{i\in I}|A_{I\setminus\{i\}}|\right] \leq 4^{-\#I}$$

for all I with $\#I = k+1$ by Proposition 3.2. Let $E \subset \mathbb{R}^{2k}$ be the row span of A. Then the subspace E is certainly of dimension k and we have

$$\mathbf{P}[\max(J_E^{2k}, J_{E^\perp}^{2k}) > 8e^{1/2}\pi^{-1/2}] \leq 2 \cdot \binom{2k}{k+1} \cdot 4^{-(k+1)} < \frac{1}{\sqrt{\pi k}}$$

by the estimates immediately above, the explicit formulas of §2.6 for J_E^{2k} and $J_{E^\perp}^{2k}$, and Stirling's formula. Therefore E has a positive probability of being a summand in a $(k, 8e^{1/2}\pi^{-1/2})$-splitting. ∎

3.4. REMARKS. (i) The subspace E figuring in the proof above is equidistributed with respect to the unique $O(2k)$-invariant probability measure on

the Grassmannian. So our proof of Proposition 3.3 does not differ radically from the proof of [Pisier, Chap. 6, Cor. 6.4].

(ii) Since the method of the proof of Proposition 3.3 works for matrices with i.i.d. Gaussian entries of mean 0, it ought to work for matrices with i.i.d. entries sufficiently close to being Gaussian. The rest of the paper is devoted to working out this simple idea.

4. ϵ-Gaussian random variables

4.1. DEFINITIONS. Fix $\epsilon > 0$ and let Y be a real-valued random variable. We say that Y is **strictly ϵ-Gaussian** if on the same probability space as Y there exists a Gaussian random variable X such that

$$\mathbf{E}(X^2) = \mathbf{E}(Y^2), \quad \mathbf{E}(X) = \mathbf{E}(Y), \quad \mathbf{E}((X-Y)^2) \leq \epsilon^2 \operatorname{Var}(X).$$

In this situation we call X an **ϵ-parametrix** for Y. We say that a random variable is **ϵ-Gaussian** if it has the same distribution as some strictly ϵ-Gaussian random variable.

PROPOSITION 4.2: *Every finite linear combination of independent ϵ-Gaussian random variables is again ϵ-Gaussian.*

Proof: The verification is routine. We omit the details. ∎

PROPOSITION 4.3: *Fix a positive integer ℓ and a constant $\epsilon \geq \ell^{-1/4}$. Let Y be a random variable giving the excess of heads over tails in ℓ tosses of a fair coin. Then Y is ϵ-Gaussian.*

Proof: Let $\{W_t\}_{t\geq 0}$ be a Wiener process. For background on the Wiener process see [Billingsley] or [Durrett]. Each random variable W_t is Gaussian of mean 0 and variance t, and moreover increments are independent. Let

$$0 = \tau_0 \leq \tau_1 \leq \tau_2 \leq \cdots$$

be the sequence of stopping times defined inductively by the rule that τ_n is the first time after τ_{n-1} that W_t takes a value in the set of integers congruent to n modulo 2. Then the increments

$$\tau_1 - \tau_0, \tau_2 - \tau_1, \ldots$$

are i.i.d. and so are the increments

$$W_{\tau_1} - W_{\tau_0}, W_{\tau_2} - W_{\tau_1}, \ldots.$$

Moreover, one finds that

$$\mathbf{E}(\tau_1) = 1, \quad \mathbf{E}(\tau_1^2) = \frac{5}{3}, \quad \mathbf{P}(W_{\tau_1} = \pm 1) = \frac{1}{2},$$

and

$$\mathbf{E}((W_n - W_{\tau_n})^2) = \mathbf{E}(|\tau_n - n|) \leq \sqrt{\mathrm{Var}(\tau_n)} = \sqrt{2n/3}$$

by standard martingale calculations. For example, the calculation of the second moment of the stopping time τ_1 appears in the textbook literature as [Durrett, Sec. 7.5, (5.9) Thm., p. 401]. The process W_{τ_n} is (so to speak) the image of coin-flipping in Brownian motion under the Skorokhod embedding. Clearly we may assume without loss of generality that $Y = W_{\tau_\ell}$. Put $X := W_\ell$. The facts recalled above concerning Brownian motion taken for granted, it is clear that Y is strictly ϵ-Gaussian with ϵ-parametrix X. ∎

5. Expected values of certain statistics of normally distributed random matrices

PROPOSITION 5.1: *Let A be an n by n matrix with i.i.d. Gaussian entries of mean 0 and variance 1. Put*

$$R_{\nu,n} := \Big(\sum_{\substack{I \subset \{1,\ldots,n\} \\ \#I = \nu}} |A_{\{1,\ldots,\nu\},I}|^2 \Big)^{1/2}$$

for $\nu = 1, \ldots, n$. (See §2.3 for the notation.) We have

$$\mathbf{E}(R_{\nu,n}^s) = 2^{\nu s/2} \prod_{i=1}^{\nu} \frac{\Gamma(\frac{s+n-i+1}{2})}{\Gamma(\frac{n-i+1}{2})}.$$

More precisely, for $\Re(s) > -(n - \nu + 1)$, the integral on the left converges absolutely to the value specified on the right.

Proof: We evaluate the integral by following [Weil, Chap. X]. Let G be the n by n real general linear group. Let $T \subset G$ be the subgroup consisting of upper triangular matrices with positive diagonal entries. Let $K \subset G$ be an n by n orthogonal group. The map $(k,t) \mapsto kt$ identifies the topological space underlying $K \times T$ with that of G. Let dx denote Lebesgue measure on the real line. The formula

$$\int_G \phi(g) d\mu(g) = \int_G \phi(g) \det(g)^{-n} \prod_{i=1}^{n} \prod_{j=1}^{n} dg_{ij}$$

defines a Haar measure μ on G. Note that μ is invariant under both left and right translation. For a uniquely determined Haar measure σ on K we also have

$$\int_G \phi(g)d\mu(g) = \int_T \left(\int_K \phi(kt)d\sigma(k) \right) \cdot \prod_{i=1}^{n} t_{ii}^{-i} \cdot \prod_{1 \le i \le j \le n} dt_{ij},$$

cf. [Weil, Chap. X, §3, Lemma 7, p. 199]; this is checked by verifying that the outside integral on the right over T is invariant under right translation. For $g \in G$ and $\nu = 1, \ldots, n$ put

$$r_{\nu,n}(g) := \left(\sum_{\substack{I \subset \{1,\ldots,n\} \\ \#I = \nu}} |g_{I,\{1,\ldots,\nu\}}|^2 \right)^{1/2}.$$

The function $r_{\nu,n}$ on G thus defined is left K-invariant and has further the property that

$$r_{\nu,n}(t) = \prod_{i=1}^{\nu} t_{ii}$$

for all $t \in T$. We have

$$\begin{aligned}
\mathbf{E}(R_{\nu,n}^s) &= \frac{\int_G r_{\nu,n}(g)^s \exp(-\frac{1}{2}\sum_{i=1}^n \sum_{j=1}^n g_{ij}^2)(\det g)^n d\mu(g)}{\int_G \exp(-\frac{1}{2}\sum_{i=1}^n \sum_{j=1}^n g_{ij}^2)(\det g)^n d\mu(g)} \\
&= \frac{\int_T (\prod_{i=1}^{\nu} t_{ii})^s \exp(-\frac{1}{2}\sum_{1 \le i \le j \le n} t_{ij}^2) \cdot \prod_{i=1}^n t_{ii}^{n-i} \cdot \prod_{1 \le i \le j \le n} dt_{ij}}{\int_T \exp(-\frac{1}{2}\sum_{1 \le i \le j \le n} t_{ij}^2) \cdot \prod_{i=1}^n t_{ii}^{n-i} \cdot \prod_{1 \le i \le j \le n} dt_{ij}} \\
&= \frac{\prod_{i=1}^{\nu} \int_0^\infty x^{s+n-i} e^{-x^2/2} dx}{\prod_{i=1}^{\nu} \int_0^\infty x^{n-i} e^{-x^2/2} dx} = 2^{\nu s/2} \prod_{i=1}^{\nu} \frac{\Gamma(\frac{s+n-i+1}{2})}{\Gamma(\frac{n-i+1}{2})}.
\end{aligned}$$

The method of calculation makes it clear that the integral converges absolutely for $\Re(s) > -(n - \nu + 1)$. ∎

5.2. REMARK. In the sequel we are not going to need Proposition 5.1 at full strength. Rather, we are only going to need the moment estimates

$$\mathbf{E}(R_{1,n}^{-1}) = 2^{-\frac{1}{2}} \frac{\Gamma(\frac{n-1}{2})}{\Gamma(\frac{n}{2})} \le 2n^{-\frac{1}{2}}$$

and

$$\mathbf{E}(R_{n-1,n}^{-1}) = 2^{-\frac{n-1}{2}} \frac{\Gamma(\frac{1}{2})}{\Gamma(\frac{n}{2})} \le 2^{-\frac{1}{2}} e^{\frac{n}{2}} n^{-\frac{n-1}{2}}$$

for $n > 1$ obtained from the proposition via Stirling's formula.

6. Estimates

LEMMA 6.1: *Fix vectors $x, y \in \mathbb{R}^n$ and constants $\beta, \theta, \lambda > 0$. If*

$$\|x\|_2 \geq \frac{(2+\theta)\lambda\sqrt{n}}{\theta}, \quad \|x-y\|_2 \leq \lambda, \quad \|y\|_2 > (1+\theta)\beta\,\|y\|_1\,,$$

then

$$\|x\|_2 > \beta\,\|x\|_1\,.$$

Proof: Recall that

$$\|x\|_p = \left(\frac{1}{n}\sum_{i=1}^{n}|x_i|^p\right)^{1/p}, \quad \|x\|_1 \leq \|x\|_2 \leq \sqrt{n}\,\|x\|_1\,.$$

Our first two hypotheses yield chains of inequalities

$$\left(1+\frac{\theta}{2+\theta}\right)\|x\|_2 \geq \|x\|_2 + \lambda \geq \|x\|_2 + \|x-y\|_2 \geq \|y\|_2\,,$$

$$\|y\|_1 \geq \|x\|_1 - \|x-y\|_1 \geq \|x\|_1 - \lambda \geq \left(1-\frac{\theta}{2+\theta}\right)\|x\|_1\,.$$

These in combination with our last hypothesis imply that

$$\|x\|_2 > \left(1+\frac{\theta}{2+\theta}\right)^{-1}(1+\theta)\beta\left(1-\frac{\theta}{2+\theta}\right)\|x\|_1 = \beta\,\|x\|_1\,,$$

as claimed. ∎

PROPOSITION 6.2: *Let $\mathbf{X}$ and $\mathbf{Y}$ be $\mathbb{R}^n$-valued random variables defined on a common probability space. Fix constants $\beta, \theta > 0$. We have*

$$\begin{aligned}&\mathbf{P}[\|\mathbf{Y}\|_2 > (1+\theta)\beta\,\|\mathbf{Y}\|_1]\\ \leq&\mathbf{P}[\|\mathbf{X}\|_2 > \beta\,\|\mathbf{X}\|_1] + M_\theta n^{1/3}\mathbf{E}(\|\mathbf{X}\|_2^{-1})^{2/3}\mathbf{E}(\|\mathbf{X}-\mathbf{Y}\|_2^2)^{1/3}\end{aligned}$$

where

$$M_\theta := (2^{1/3}+2^{-2/3})\cdot\left(\frac{2+\theta}{\theta}\right)^{2/3}.$$

Proof: Fix a constant $\lambda > 0$ arbitrarily. By the preceding lemma we have a relation

$$\begin{aligned}&[\|\mathbf{Y}\|_2 > (1+\theta)\beta\,\|\mathbf{Y}\|_1]\\ \subset&[\|\mathbf{X}\|_2 > \beta\,\|\mathbf{X}\|_1] \cup [\|\mathbf{X}\|_2 < \frac{(2+\theta)\lambda\sqrt{n}}{\theta}] \cup [\|\mathbf{X}-\mathbf{Y}\|_2 > \lambda]\end{aligned}$$

among events. In turn we get an estimate

$$\begin{aligned}\mathbf{P}[\|\mathbf{Y}\|_2 > (1+\theta)\beta\,\|\mathbf{Y}\|_1] \leq&\mathbf{P}[\|\mathbf{X}\|_2 > \beta\,\|\mathbf{X}\|_1]\\ &+ \mathbf{E}(\|\mathbf{X}\|_2^{-1})\cdot\frac{(2+\theta)\lambda\sqrt{n}}{\theta} + \mathbf{E}(\|\mathbf{X}-\mathbf{Y}\|_2^2)\cdot\lambda^{-2}\end{aligned}$$

by applying Markov's inequality twice. Finally, we obtain the desired inequality by freshman calculus. ∎

6.3. REMARK. The exact value of constant M_θ is going to be of no concern to us. The important thing is simply that M_θ is independent of both β and n.

PROPOSITION 6.4: *Let $\mathbf{Y}$ be an $\mathbb{R}^n$-valued random variable with entries that are i.i.d. ϵ-Gaussian of mean 0. Assume that $n > 1$. Fix a constant $\theta > 0$. Then we have*

$$\mathbf{P}[\|\mathbf{Y}\|_2 > (1+\theta)\cdot 4\cdot 2^{1/2}e^{1/2}\pi^{-1/2}\cdot\|\mathbf{Y}\|_1] \leq 4^{-n} + 2M_\theta n^{1/3}\epsilon^{2/3}$$

where M_θ is the constant figuring in Proposition 6.2.

Proof: Let Y be a strictly ϵ-Gaussian random variable of mean 0 and variance 1 with ϵ-parametrix X. We may assume without loss of generality that the random vector $\mathbf{Y} = (Y_1, \ldots, Y_n)$ arises from an i.i.d. family $\{(X_i, Y_i)\}_{i=1}^n$ of copies of the random vector (X, Y). Put $\mathbf{X} := (X_1, \ldots, X_n)$. By Propositions 3.2 and 6.2 we have

$$\begin{aligned}&\mathbf{P}[\|\mathbf{Y}\|_2 > (1+\theta)\cdot 4\cdot 2^{1/2}e^{1/2}\pi^{-1/2}\cdot\|\mathbf{Y}\|_1]\\ \leq& 4^{-n} + M_\theta n^{1/3}\mathbf{E}(\|\mathbf{X}\|_2^{-1})^{2/3}\mathbf{E}(\|\mathbf{X}-\mathbf{Y}\|_2^2)^{1/3}.\end{aligned}$$

By Proposition 5.1 and the remark following we have

$$\mathbf{E}(\|\mathbf{X}\|_2^{-1}) = \sqrt{n}\mathbf{E}((\mathbf{X}\cdot\mathbf{X})^{-1/2}) = \sqrt{n}\mathbf{E}(R_{1,n}^{-1}) \leq 2.$$

Clearly we have

$$\mathbf{E}(\|\mathbf{X}-\mathbf{Y}\|_2^2) = n^{-1}\mathbf{E}((\mathbf{X}-\mathbf{Y})\cdot(\mathbf{X}-\mathbf{Y})) \leq \epsilon^2.$$

The three inequalities above together imply the desired estimate. ∎

LEMMA 6.5: *Let Y be a strictly ϵ-Gaussian random variable of mean 0 and variance 1 with ϵ-parametrix X. Let $\{(X_{ij}, Y_{ij})\}_{i,j=1}^n$ be an i.i.d. family of copies of the random vector (X, Y). Then we have*

$$\mathbf{E}\Big(\Big(\det_{i,j=1}^n X_{ij} - \det_{i,j=1}^n Y_{ij}\Big)^2\Big) \leq \epsilon^2 n^{2+n}.$$

Proof: Put

$$Z_{ij}^{(k)} := \begin{cases} Y_{ij} & \text{if } j < k \\ X_{ij} - Y_{ij} & \text{if } j = k \\ X_{ij} & \text{if } j > k \end{cases}$$

for $i, j, k = 1, \ldots, n$. Since the entries of $Z^{(k)}$ are independent we have

$$\mathbf{E}\Big(\Big(\det_{i,j=1}^{n} Z_{ij}^{(k)}\Big)^2\Big) \leq \prod_{j=1}^{n} \mathbf{E}\Big(\sum_{i=1}^{n} (Z_{ij}^{(k)})^2\Big) \leq \epsilon^2 n^n.$$

But we also have

$$\det_{i,j=1}^{n} X_{ij} - \det_{i,j=1}^{n} Y_{ij} = \sum_{k=1}^{n} \det_{i,j=1}^{n} Z_{ij}^{(k)},$$

and hence

$$\mathbf{E}\Big(\Big(\det_{i,j=1}^{n} X_{ij} - \det_{i,j=1}^{n} Y_{ij}\Big)^2\Big)^{1/2} \leq n \cdot \epsilon n^{n/2}. \qquad \blacksquare$$

PROPOSITION 6.6: *Fix a constant $\theta > 0$ and an integer $n > 1$. Let B be an $n-1$ by n matrix with i.i.d. ϵ-Gaussian entries of mean 0 and put*

$$\mathbf{Y} := (B_{\{1,\ldots,n-1\},\{1,\ldots,n\}\setminus\{1\}}, \ldots, B_{\{1,\ldots,n-1\},\{1,\ldots,n\}\setminus\{n\}})$$

thereby defining an $\mathbb{R}^n$-valued random variable. (See §2.3 for the notation.) We have

$$\mathbf{P}[\|\mathbf{Y}\|_2 > (1+\theta) \cdot 4 \cdot 2^{1/2} e^{1/2} \pi^{-1/2} \cdot \|\mathbf{Y}\|_1] \leq 4^{-n} + 2^n M_\theta n^{1/3} \epsilon^{2/3}$$

where M_θ is the constant figuring in Proposition 6.2.

Proof: Let Y be a strictly ϵ-Gaussian random variable of mean zero and variance 1 with ϵ-parametrix X. Let $\{\{(X_{ij}, Y_{ij})\}_{i=1}^{n-1}\}_{j=1}^{n}$ be an i.i.d. family of copies of the random vector (X, Y). We may assume without loss of generality Y_{ij} is the entry of B in row i and column j. Let A be the $n-1$ by n matrix with entry X_{ij} in row i and column j and put

$$\mathbf{X} := (A_{\{1,\ldots,n-1\},\{1,\ldots,n\}\setminus\{1\}}, \ldots, A_{\{1,\ldots,n-1\},\{1,\ldots,n\}\setminus\{n\}}).$$

By Propositions 3.2 and 6.2 we have

$$\begin{aligned}&\mathbf{P}[\|\mathbf{Y}\|_2 > (1+\theta) \cdot 4 \cdot 2^{1/2} e^{1/2} \pi^{-1/2} \cdot \|\mathbf{Y}\|_1] \\ \leq &4^{-n} + M_\theta n^{1/3} \mathbf{E}(\|\mathbf{X}\|_2^{-1})^{2/3} \mathbf{E}(\|\mathbf{X} - \mathbf{Y}\|_2^2)^{1/3}.\end{aligned}$$

By Proposition 5.1 and the remark following we have

$$\mathbf{E}(\|\mathbf{X}\|_2^{-1}) = \sqrt{n}\mathbf{E}(R_{n-1,n}^{-1}) \leq 2^{-1/2} e^{n/2} n^{1-n/2}.$$

Further, by Lemma 6.5 we have

$$\begin{aligned}\mathbf{E}(\|\mathbf{X} - \mathbf{Y}\|_2^2) =& n^{-1} \mathbf{E}((\mathbf{X} - \mathbf{Y}) \cdot (\mathbf{X} - \mathbf{Y})) \\ \leq& \epsilon^2 (n-1)^{2+(n-1)} \leq \epsilon^2 n^{1+n}.\end{aligned}$$

Finally, freshman calculus yields the bound

$$\sup_{x\geq 2}(2^{-1/2}e^{x/2}x^{1-x/2})^{2/3}(x^{1+x})^{1/3}/2^x \leq 1.$$

The four inequalities above together imply the desired estimate. ∎

PROPOSITION 6.7: *Fix positive integers k and ℓ such that*

$$\ell \geq 4 + \log_2 k.$$

Let Y be a random variable giving the excess of heads over tails in ℓ tosses of a fair coin. Let B be a k by $2k$ matrix the entries of which are i.i.d. copies of Y. Then we have

$$\mathbf{P}[B \text{ is of full rank}] > 1 - 2^{-(k+1)} \geq 3/4.$$

Proof: Let $\overline{Y}$ be a random variable equidistributed in the field $\mathbb{Z}/3\mathbb{Z}$ of 3 elements. Let $\overline{B}$ be a k by $2k$ matrix with entries that are i.i.d. copies of $\overline{Y}$. Now if a k by $2k$ matrix b with entries in $\mathbb{Z}/3\mathbb{Z}$ fails to be of full rank, then there exists some nonzero row vector v of length k with entries in $\mathbb{Z}/3\mathbb{Z}$ such that $vb = 0$. Accordingly, we have

$$\mathbf{P}[\overline{B} \text{ fails to be of full rank}] \leq \frac{3^k - 1}{3 - 1} \cdot \frac{3^{(k-1)(2k)}}{3^{2k^2}} < 3^{-k}/2.$$

One finds that

$$\mathbf{P}[Y \equiv 0 \bmod 3] = \left(1 + 2\left(-\frac{1}{2}\right)^{\ell}\right) \cdot \frac{1}{3},$$

$$\mathbf{P}[Y \equiv 1 \bmod 3] = \mathbf{P}[Y \equiv -1 \bmod 3] = \left(1 - \left(-\frac{1}{2}\right)^{\ell}\right) \cdot \frac{1}{3}$$

by a straightforward Markov chain calculation and hence

$$\mathbf{P}[Y \equiv i \bmod 3] < e^{2^{1-\ell}} \cdot \mathbf{P}[\overline{Y} \equiv i \bmod 3]$$

for $i = -1, 0, 1$. Finally, we have

$$\begin{aligned}&\mathbf{P}[B \text{ fails to be of full rank}]\\ \leq\, &e^{2k^2 \cdot 2^{1-\ell}}\mathbf{P}[\overline{B} \text{ fails to be of full rank}] < e^{k/4}3^{-k}/2 < 2^{-k-1},\end{aligned}$$

since

$$e^{1/4} = 1.284025417\ldots < 3/2. \qquad \blacksquare$$

7. The main result

7.1. FORMULATION. Fix a positive integer k. Fix $\theta > 0$ and put

$$C := (1+\theta)8e^{1/2}\pi^{-1/2}, \quad M_\theta := (2^{1/3}+2^{-2/3}) \cdot \left(\frac{2+\theta}{\theta}\right)^{2/3}.$$

The constant M_θ is the one figuring in Proposition 6.2 above. Consider now the set $L(k,C)$ of positive integers ℓ with the following properties:

- $\ell \geq 4 + \log_2 k$.
- $2 \cdot \binom{2k}{k+1} \cdot 4^{-(k+1)} \cdot (1 + 2^{3(k+1)} M_\theta (k+1)^{1/3} \ell^{-1/6}) \leq \frac{3}{4}$.

In view of the inequality

$$2 \cdot \binom{2k}{k+1} \cdot 4^{-(k+1)} \leq \frac{1}{\sqrt{\pi k}} < \frac{2}{3},$$

noted at the end of the proof of Proposition 3.3, it is clear that the set $L(k,C)$ is nonempty. Put

$$N(k,C) := \min L(k,C).$$

It is easy to see that $2^{18k} \in L(k,C)$ for $k \gg 0$ and hence that

$$\limsup_{k\to\infty} N(k,C) \leq 2^{18k},$$

i.e., $N(k,C) \leq 2^{18k}$ for k large enough depending on C.

THEOREM 7.2: *In the set of k by $2k$ matrices with integral entries of absolute value not exceeding $N(k,C)$ there exists some matrix with row span a summand in a (k,C)-splitting.*

Proof: To simplify writing now put

$$\ell := N(k,C).$$

Let Y be a random variable giving the excess of heads over tails in ℓ tosses of a fair coin. By Proposition 4.3 the random variable Y is ϵ-Gaussian with

$$\epsilon = \ell^{-1/4}.$$

Let B be a k by $2k$ matrix the entries of which are i.i.d. copies of Y. For each subset $I \subset \{1,\ldots,2k\}$ of cardinality k, put

$$B_I := B_{\{1,\ldots,k\},I}.$$

(See §2.3 for the notation.) For each subset $I \subset \{1, \ldots, 2k\}$ put

$$I^* := \{1, \ldots, 2k\} \setminus I.$$

For each subset $I = \{i_1 < \ldots < i_{k+1}\} \subset \{1, \ldots, 2k\}$ of cardinality $k+1$ we define $\mathbb{R}^{k+1}$-valued random variables

$$\mathbf{Y}_I := (B_{I^* \cup \{i_\nu\}})_{\nu=1}^{k+1}, \quad \hat{\mathbf{Y}}_I := (B_{I \setminus \{i_\nu\}})_{\nu=1}^{k+1}$$

and we denote by $\mathcal{F}_I$ the (finite) σ-field of events generated by the entries of the matrix B in columns indexed by elements of the set I^*. We have a conditional bound

$$\begin{aligned}
&\mathbf{P}[\|\mathbf{Y}_I\|_2 > 4 \cdot (1+\theta) 2^{1/2} e^{1/2} \pi^{-1/2} \cdot \|\mathbf{Y}_I\|_1 \, \|\mathcal{F}_I] \\
\leq &4^{-(k+1)} + 2M_\theta (k+1)^{1/3} \ell^{-1/6} \\
\leq &4^{-(k+1)} (1 + 2^{3(k+1)} M_\theta (k+1)^{1/3} \ell^{-1/6})
\end{aligned}$$

almost surely by Propositions 4.2 and 6.4. We also have

$$\begin{aligned}
&\mathbf{P}[||\hat{\mathbf{Y}}_I||_2 > 4 \cdot (1+\theta) 2^{1/2} e^{1/2} \pi^{-1/2} \cdot ||\hat{\mathbf{Y}}_I||_1] \\
\leq &4^{-(k+1)} + 2^{k+1} M_\theta (k+1)^{1/3} \ell^{-1/6} \\
= &4^{-(k+1)} (1 + 2^{3(k+1)} M_\theta (k+1)^{1/3} \ell^{-1/6})
\end{aligned}$$

by Proposition 6.6. Let $E \subset \mathbb{R}^{2k}$ be the row span of B. We have

$$\mathbf{P}[\dim E = k] = \mathbf{P}[B \text{ is of full rank}] > 3/4$$

by the first of the conditions for membership in the set $L(k, C)$ and Proposition 6.7. Finally, we have

$$\mathbf{P}([\dim E = k] \cap [\max(J_E^{2k}, J_{E^\perp}^{2k}) \leq C]) > 0$$

by the explicit formulas of §2.6 for J_E^{2k} and $J_{E^\perp}^{2k}$, the estimates immediately above, and the second of the conditions for membership in the set $L(k, C)$. ∎

7.3. ACKNOWLEDGEMENTS. I thank John Baxter for several helpful conversations about Brownian motion. These conversations formed the basis of the proof of Proposition 4.3.

References

[Billingsley] P. Billingsley, *Probability and Measure*, third edition, Wiley, New York, 1995.

[Durrett] R. Durrett, *Probability: Theory and Examples*, second edition, Duxbury Press, Wadsworth Publishing Company, Belmont, California, 1996.

[Kašin] B. Kašin, *Sections of some finite dimensional sets and classes of smooth functions*, Izvestiya Akademii Nauk SSSR **41** (1977), 334–351 (Russian); English translation: Mathematics of the USSR-Izvestiya **11** (1977), 317–333.

[Lubotzky] A. Lubotzky, *Discrete groups, expanding graphs and invariant measures*, Progress in Mathematics **125**, Birkhaüser, Boston, 1994.

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

[Szarek] S. Szarek, *On Kašin's almost Euclidean orthogonal decomposition of* ℓ_1^n, Bulletin de l'Académie Polonaise des Sciences **26** (1978), 691–694.

[Weil] A. Weil, *Basic Number Theory*, third edition, Springer-Verlag, New York, 1974.