Djalil Chafaï
Olivier Guédon
Guillaume Lecué
Alain Pajor

INTERACTIONS BETWEEN COMPRESSED SENSING RANDOM MATRICES AND HIGH DIMENSIONAL GEOMETRY

Djalil Chafaï
Laboratoire d'Analyse et de Mathématiques Appliquées, UMR CNRS 8050, 5 boulevard Descartes, Champs-sur-Marne, F-77454 Marne-la-Vallée, Cedex 2, France.
E-mail : djalil.chafai(at)univ-mlv.fr
Url : http://perso-math.univ-mlv.fr/users/chafai.djalil/

Olivier Guédon
Laboratoire d'Analyse et de Mathématiques Appliquées, UMR CNRS 8050, 5 boulevard Descartes, Champs-sur-Marne, F-77454 Marne-la-Vallée, Cedex 2, France.
E-mail : olivier.guedon(at)univ-mlv.fr
Url : http://perso-math.univ-mlv.fr/users/guedon.olivier/

Guillaume Lecué
Laboratoire d'Analyse et de Mathématiques Appliquées, UMR CNRS 8050, 5 boulevard Descartes, Champs-sur-Marne, F-77454 Marne-la-Vallée, Cedex 2, France.
E-mail : guillaume.lecue(at)univ-mlv.fr
Url : http://perso-math.univ-mlv.fr/users/lecue.guillaume/

Alain Pajor
Laboratoire d'Analyse et de Mathématiques Appliquées, UMR CNRS 8050, 5 boulevard Descartes, Champs-sur-Marne, F-77454 Marne-la-Vallée, Cedex 2, France.
E-mail : Alain.Pajor(at)univ-mlv.fr
Url : http://perso-math.univ-mlv.fr/users/pajor.alain/

16–20 November 2009
Compiled June 21, 2012

INTERACTIONS BETWEEN COMPRESSED SENSING RANDOM MATRICES AND HIGH DIMENSIONAL GEOMETRY

Djalil Chafaï, Olivier Guédon, Guillaume Lecué, Alain Pajor

Abstract. — This book is based on a series of lectures given at Université Paris-Est Marne-la-Vallée in fall 2009, by Djalil Chafaï, Olivier Guédon, Guillaume Lecué, Shahar Mendelson, and Alain Pajor.

CONTENTS

INTRODUCTION

Compressed sensing, also referred to in the literature as compressive sensing or compressive sampling, is a framework that enables one to recover approximate or exact reconstruction of sparse signals from incomplete measurements. The existence of efficient algorithms for this reconstruction, such as the ℓ_1-minimization algorithm, and the potential for applications in signal processing and imaging, led to a rapid and extensive development of the theory after the seminal articles by D. Donoho [**Don06**], E. Candes, J. Romberg and T. Tao [**CRT06**] and E. Candes and T. Tao [**CT06**].

The principles underlying the discoveries of these phenomena in high dimensions are related to more general problems and their solutions in Approximation Theory. One significant example of such a relation is the study of Gelfand and Kolmogorov widths of classical Banach spaces. There is already a huge literature on both the theoretical and numerical aspects of compressed sensing. Our aim is not to survey the state of the art in this rapidly developing field, but to highlight and study its interactions with other fields of mathematics, in particular with asymptotic geometric analysis, random matrices and empirical processes.

To introduce the subject, let T be a subset of $\mathbb{R}^N$ and let A be an $n \times N$ real matrix with rows $Y_1, \ldots, Y_n \in \mathbb{R}^N$. Consider the general problem of reconstructing a vector $x \in T$ from the *data* $Ax \in \mathbb{R}^n$: that is, from the known *measurements*

$$\langle Y_1, x\rangle, \ldots, \langle Y_n, x\rangle$$

of an unknown x. Classical linear algebra suggests that the number n of measurements should be at least as large as the dimension N in order to ensure reconstruction. Compressed sensing provides a way of reconstructing the original signal x from its compression Ax that uses only a small number of linear measurements: that is with $n \ll N$. Clearly one needs some a priori hypothesis on the subset T of signals that we want to reconstruct, and of course the matrix A should be suitably chosen in order to allow the reconstruction of every vector of T.

The first point concerns the subset T and is a matter of *complexity*. Many tools within this framework were developed in Approximation Theory and in the Geometry of Banach Spaces. One of our goals is to present these tools.

The second point concerns the design of the measurement matrix A. To date the only good matrices are random *sampling* matrices and the key is to sample $Y_1, \dots, Y_n \in \mathbb{R}^N$ in a suitable way. For this reason probability theory plays a central role in our exposition. These random sampling matrices will usually be of Gaussian or Bernoulli (± 1) type or be random sub-matrices of the discrete Fourier $N \times N$ matrix (partial Fourier matrices). There is a huge technical difference between the study of unstructured compressive matrices (with i.i.d entries) and structured matrices such as partial Fourier matrices. Another goal of this work is to describe the main tools from probability theory that are needed within this framework. These tools range from classical probabilistic inequalities and concentration of measure to the study of empirical processes and random matrix theory.

The purpose of Chapter 1 is to present some basic tools and preliminary background. We will look briefly at elementary properties of Orlicz spaces in relation to tail inequalities for random variables. An important connection between high dimensional geometry and the study of empirical processes comes from the behavior of the sum of independent centered random variables with sub-exponential tails. An important step in the study of empirical processes is Discretization: in which we replace an infinite space by an approximating net. It is essential to estimate the size of the discrete net and such estimates depend upon the study of covering numbers. Several upper estimates for covering numbers, such as Sudakov's inequality, are presented in the last part of Chapter 1.

Chapter 2 is devoted to compressed sensing. The purpose is to provide some of the key mathematical insights underlying this new sampling method. We present first the exact reconstruction problem informally introduced above. The a priori hypothesis on the subset of signals T that we investigate is *sparsity.* A vector in $\mathbb{R}^N$ is said to be m-sparse ($m \leqslant N$) if it has at most m non-zero coordinates. An important feature of this subset is its peculiar structure: its intersection with the Euclidean unit sphere is a union of unit spheres supported on m-dimensional coordinate subspaces. This set is highly compact when the degree of compactness is measured in terms of covering numbers. As long as $m \ll N$ the sparse vectors form a *very small* subset of the sphere.

A fundamental feature of compressive sensing is that practical reconstruction can be performed by using efficient algorithms such as the ℓ_1-minimization method which consists, for given data $y = Ax$, to solve the "linear program":

$$\min_{t \in \mathbb{R}^N} \sum_{i=1}^N |t_i| \quad \text{subject to} \quad At = y.$$

At this step, the problem becomes that of finding matrices for which the algorithm reconstructs any m-sparse vector with m relatively large. A study of the cone of constraints that ensures that every m-sparse vector can be reconstructed by the ℓ_1-minimization method leads to a necessary and sufficient condition known as the *null space property* of order m:

$$\forall h \in \ker A,\ h \neq 0,\ \forall I \subset [N],\ |I| \leq m,\ \sum_{i \in I} |h_i| < \sum_{i \in I^c} |h_i|.$$

This property has a nice geometric interpretation in terms of the structure of faces of polytopes called *neighborliness*. Indeed, if P is the polytope obtained by taking the symmetric convex hull of the columns of A, the *null space property* of order m for A is equivalent to the *neighborliness* property of order m for P: that the matrix A which maps the vertices of the cross-polytope

$$B_1^N = \Big\{ t \in \mathbb{R}^N \,:\, \sum_{i=1}^N |t_i| \le 1 \Big\}$$

onto the vertices of P preserves the structure of k-dimensional faces up to the dimension $k = m$. This remarkable connection between compressed sensing and high dimensional geometry is due to D. Donoho [**Don05**].

Unfortunately, the null space property is not easy to verify nor is the neighborliness. An ingenious sufficient condition is the so-called *Restricted Isometry Property* (RIP) of order m that requires that all sub-matrices of size $n \times m$ of the matrix A are uniformly well-conditioned. More precisely, we say that A satisfies the RIP of order $p \leqslant N$ with parameter $\delta = \delta_p$ if the inequalities

$$1 - \delta_p \leqslant |Ax|_2^2 \leqslant 1 + \delta_p$$

hold for all p-sparse unit vectors $x \in \mathbb{R}^N$. An important feature of this concept is that if A satisfies the RIP of order $2m$ with a parameter δ small enough, then every m-sparse vector can be reconstructed by the ℓ_1-minimization method. Even if this RIP condition is difficult to check on a given matrix, it actually holds true with high probability for certain models of random matrices and can be easily checked for some of them.

Here probabilistic methods come into play. Among good unstructured sampling matrices we shall study the case of Gaussian and Bernoulli random matrices. The case of partial Fourier matrices, which is more delicate, will be studied in Chapter 5. Checking the RIP for the first two models may be treated with a simple scheme: the ε-net argument presented in Chapter 2.

Another way to tackle the problem of reconstruction by ℓ_1-minimization is to analyse the Euclidean diameter of the intersection of the cross-polytope B_1^N with the kernel of A. This study leads to the notion of Gelfand widths, particularly for the cross-polytope B_1^N. Its Gelfand widths are defined by the numbers

$$d^n(B_1^N, \ell_2^N) = \inf_{\operatorname{codim} S \leqslant n} \operatorname{rad}(S \cap B_1^N), \quad n = 1, \dots, N$$

where $\operatorname{rad}(S \cap B_1^N) = \max\{ |x| \,:\, x \in S \cap B_1^N \}$ denotes the half Euclidean diameter of the section of B_1^N and the infimum is over all subspaces S of $\mathbb{R}^N$ of dimension less than or equal to n.

A great deal of work was done in this direction in the seventies. These Approximation Theory and Asymptotic Geometric Analysis standpoints shed light on a new aspect of the problem and are based on a celebrated result of B. Kashin [**Kas77**] stating that

$$d^n(B_1^N, \ell_2^N) \leqslant \frac{C}{\sqrt{n}} \log^{O(1)}(N/n)$$

for some numerical constant C. The relevance of this result to compressed sensing is highlighted by the following fact.

Let $1 \le m \le n$, if
$$\mathrm{rad}\,(\ker A \cap B_1^N) < 1/2\sqrt{m}$$
then every m-sparse vector can be reconstructed by ℓ_1-minimization.

From this perspective, the goal is to estimate the diameter $\mathrm{rad}\,(\ker A \cap B_1^N)$ from above. We discussed this in detail for several models of random matrices. The connection with the RIP is clarified by the following result.

Assume that A satisfies the RIP of order p with parameter δ. Then
$$\mathrm{rad}\,(\ker A \cap B_1^N) \le \frac{C}{\sqrt{p}} \frac{1}{1-\delta}$$
where C is a numerical constant and so $\mathrm{rad}\,(\ker A \cap B_1^N) < 1/2\sqrt{m}$ *is satisfied with $m = O(p)$.*

The ℓ_1-minimization method extends to the study of approximate reconstruction of vectors which are not too far from being sparse. Let $x \in \mathbb{R}^N$ and let $x^\sharp$ be a minimizer of
$$\min_{t \in \mathbb{R}^N} \sum_{i=1}^N |t_i| \quad \text{subject to} \quad At = Ax.$$
Again the notion of width is very useful. We prove the following:

Assume that $\mathrm{rad}\,(\ker A \cap B_1^N) < 1/4\sqrt{m}$. *Then for any $I \subset [N]$ such that $|I| \leqslant m$ and any $x \in \mathbb{R}^N$, we have*
$$|x - x^\sharp|_2 \le \frac{1}{\sqrt{m}} \sum_{i \notin I} |x_i|.$$

This applies in particular to unit vectors of the space $\ell_{p,\infty}^N$, $0 < p < 1$ for which $\min_{|I| \leqslant m} \sum_{i \notin I} |x_i| = O(m^{1-1/p})$.

In the last section of Chapter 2 we introduce a measure of complexity $\ell_*(T)$ of a subset $T \subset \mathbb{R}^N$ defined by
$$\ell_*(T) = \mathbb{E} \sup_{t \in T} \sum_{i=1}^N g_i t_i,$$
where $g_1, ..., g_N$ are independent $N(0,1)$ Gaussian random variables. This kind of parameter plays an important role in the theory of empirical processes and in the Geometry of Banach spaces ([**Mil86, PTJ86, Tal87**]). It allows to control the size of $\mathrm{rad}\,(\ker A \cap T)$ which as we have seen is a crucial issue in approximate reconstruction.

This line of investigation goes deeper in Chapter 3 where we first present classical results from the Theory of Gaussian processes. To make the link with compressed sensing, observe that if A is a $n \times N$ matrix with row vectors $Y_1, \ldots, Y_n$, then the RIP of order p with parameter δ_p can be rewritten in terms of an empirical process property since
$$\delta_p = \sup_{x \in S_2(\Sigma_p)} \left| \frac{1}{n} \sum_{i=1}^n \langle Y_i, x \rangle^2 - 1 \right|$$

where $S_2(\Sigma_p)$ is the set of norm one p-sparse vectors of $\mathbb{R}^N$. While Chapter 2 makes use of a simple ε-net argument to study such processes, we present in Chapter 3 the chaining and generic chaining techniques based on measures of metric complexity such as the γ_2 functional. The γ_2 functional is equivalent to the parameter $\ell_*(T)$ in consequence of the majorizing measure theorem of M. Talagrand [**Tal87**]. This technique enables to provide a criterion that implies the RIP for unstructured models of random matrices, which include the Bernoulli and Gaussian models.

It is worth noticing that the ε-net argument, the chaining argument and the generic chaining argument all share two ideas: the classical trade-off between complexity and concentration on the one hand and an approximation principle on the other. For instance, consider a Gaussian matrix $A = n^{-1/2}(g_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant N}$ where the g_{ij}'s are i.i.d. standard Gaussian variables. Let T be a subset of the unit sphere S^{N-1} of $\mathbb{R}^N$. A classical problem is to understand how A acts on T. In particular, does A preserve the Euclidean norm on T? In the Compressed Sensing setup, the "input" dimension N is much larger than the number of measurements n, because A is used as a compression matrix. So clearly A cannot preserve the Euclidean norm on the whole sphere S^{N-1}. Hence, it is natural to identify the subsets T of S^{N-1} for which A acts on T in a norm preserving way. Let's start with a single point $x \in T$. Then for any $\varepsilon \in (0,1)$, with probability greater than $1 - 2\exp(-c_0 n\varepsilon^2)$, one has

$$1 - \varepsilon \leqslant |Ax|_2^2 \leqslant 1 + \varepsilon.$$

This result is the one expected since $\mathbb{E}|Ax|_2^2 = |x|_2^2$ (we say that the standard Gaussian measure is isotropic) and the Gaussian measure on $\mathbb{R}^N$ has strong concentration properties. Thus proving that A acts in a norm preserving way on a single vector is only a matter of isotropicity and concentration. Now we want to see how many points in T may share this property simultaneously. This is where the trade-off between complexity and concentration is at stake. A simple union bound argument tells us that if $\Lambda \subset T$ has a cardinality less than $\exp(c_0 n\varepsilon^2/2)$, then, with probability greater than $1 - 2\exp(-c_0 n\varepsilon^2/2)$, one has

$$\forall x \in \Lambda \qquad 1 - \varepsilon \leqslant |Ax|_2^2 \leqslant 1 + \varepsilon.$$

This means that A preserves the norm of all the vectors of Λ at the same time, as long as $|\Lambda| \leqslant \exp(c_0 n\varepsilon^2/2)$. If the entries in A had different concentration properties, we would have ended up with a different cardinality for $|\Lambda|$. As a consequence, it is possible to control the norm of the images by A of $\exp(c_0 n\varepsilon^2/2)$ points in T simultaneously. The first way of choosing Λ that may come to mind is to use an ε-net of T with respect to ℓ_2^N and then to ask if the norm preserving property of A on Λ extends to T? Indeed, if $m \leq C(\varepsilon) n \log^{-1}(N/n)$, there exists an ε-net Λ of size $\exp(c_0 n\varepsilon^2/2)$ in $S_2(\Sigma_m)$ for the Euclidean metric. And, by what is now called the ε-net argument, we can describe all the points in $S_2(\Sigma_m)$ using only the points in Λ:

$$\Lambda \subset S_2(\Sigma_m) \subset (1-\varepsilon)^{-1}\mathrm{conv}(\Lambda).$$

This allows to extend the norm preserving property of A on Λ to the entire set $S_2(\Sigma_m)$ and was the scheme used in Chapter 2.

But this scheme does not apply to several important sets T in S^{N-1}. That is why we present the chaining and generic chaining methods in Chapter 3. Unlike the ε-net argument which demanded only to know how A acts on a single ε-net of T, these two methods require to study the action of A on a sequence (T_s) of subsets of T with exponentially increasing cardinality. In the case of the chaining argument, T_s can be chosen as an ε_s-net of T where ε_s is chosen so that $|T_s| = 2^s$ and for the generic chaining argument, the choice of (T_s) is recursive: for large values of s, the set T_s is a maximal separated set in T of cardinality 2^{2^s} and for small values of s, the construction of T_s depends on the sequence $(T_r)_{r\geqslant s+1}$. For these methods, the approximation argument follows from the fact that $d_{\ell_2^N}(t, T_s)$ tends to zero when s tends to infinity for any $t \in T$ and the trade-off between complexity and concentration is used at every stage s of the approximation of T by T_s. The metric complexity parameter coming from the chaining method is called the Dudley entropy integral

$$\int_0^\infty \sqrt{\log N(T, d, \varepsilon)}\, d\varepsilon$$

while the one given by the generic chaining mechanism is the γ_2 functional

$$\gamma_2(T, \ell_2^N) = \inf_{(T_s)_s} \sup_{t\in T} \sum_{s=0}^{\infty} 2^{s/2} d_{\ell_2^N}(t, T_s)$$

where the infimum is taken over all sequences (T_s) of subsets of T such that $|T_0| \leqslant 1$ and $|T_s| \leqslant 2^{2^s}$ for every $s \geqslant 1$. In Chapter 3, we prove that A acts in a norm preserving way on T with probability exponentially in n close to 1 as long as

$$\gamma_2(T, \ell_2^N) = O(\sqrt{n}).$$

In the case $T = S_2(\Sigma_m)$ treated in Compressed Sensing, this condition implies that $m = O\big(n \log^{-1}\big(N/n\big)\big)$ which is the same as the condition obtained using the ε-net argument in Chapter 2. So, as far as norm preserving properties of random operators are concerned, the results of Chapter 3 generalize those of Chapter 2. Nevertheless, the norm preserving property of A on a set T implies an exact reconstruction property of A of all m-sparse vectors by the ℓ_1-minimization method only when $T = S_2(\Sigma_m)$. In this case, the norm preserving property is the RIP of order m.

On the other hand, the RIP constitutes a control on the largest and smallest singular values of all sub-matrices of a certain size. Understanding the singular values of matrices is precisely the subject of Chapter 4. An $m \times n$ matrix A with $m \leqslant n$ maps the unit sphere to an ellipsoid, and the half lengths of the principle axes of this ellipsoid are precisely the singular values $s_1(A) \geqslant \cdots \geqslant s_m(A)$ of A. In particular,

$$s_1(A) = \max_{|x|_2=1} |Ax|_2 = \|A\|_{2\to 2} \quad \text{and} \quad s_n(A) = \min_{|x|_2=1} |Ax|_2.$$

Geometrically, A is seen as a correspondence–dilation between two orthonormal bases. In matrix form $UAV^* = \mathrm{diag}(s_1(A), \dots, s_m(A))$ for a pair of unitary matrices U and V of respective sizes $m \times m$ and $n \times n$. This *singular value decomposition* – SVD for short – has tremendous importance in numerical analysis. One can read off from the singular values the rank and the norm of the inverse of the matrix: the singular values are the eigenvalues of the Hermitian matrix $\sqrt{AA^*}$: and the largest and smallest singular values appear in the definition of the condition number s_1/s_m which allows to control the behavior of linear systems under perturbations of small norm.

The first part of Chapter 4 is a compendium of results on the singular values of deterministic matrices, including the most useful perturbation inequalities. The Gram–Schmidt algorithm applied to the rows and the columns of A allows to construct a bidiagonal matrix which is unitarily equivalent to A. This structural fact is at the heart of most numerical algorithms for the actual computation of singular values.

The second part of Chapter 4 deals with random matrices with i.i.d. entries and their singular values. The aim is to offer a cultural tour in this vast and growing subject. The tour begins with Gaussian random matrices with i.i.d. entries forming the Ginibre Ensemble. The probability density of this Ensemble is proportional to $G \mapsto \exp(-\mathrm{Tr}(GG^*))$. The matrix $W = GG^*$ follows a Wishart law, a sort of multivariate χ^2. The unitary bidiagonalization allows to compute the density of the singular values of these Gaussian random matrices, which turns out to be proportional to a function of the form

$$s \mapsto \prod_k s_k^\alpha e^{-s_k^2} \prod_{i \neq j} |s_i^2 - s_j^2|^\beta.$$

The change of variable $s_k \mapsto s_k^2$ reveals Laguerre weights in front of the Vandermonde determinant, the starting point of a story involving orthogonal polynomials. As for most random matrix ensembles, the determinant measures a logarithmic repulsion between eigenvalues. Here it comes from the Jacobian of the SVD. Such Gaussian models can be analysed with explicit but cumbersome computations. Many large dimensional aspects of random matrices depend only on the first two moments of the entries, and this makes the Gaussian case universal. The most well known universal asymptotic result is indubitably the Marchenko-Pastur theorem. More precisely if M is an $m \times n$ random matrix with i.i.d. entries of variance $n^{-1/2}$, the empirical counting probability measure of the singular values of M

$$\frac{1}{m} \sum_{k=1}^m \delta_{s_k(M)}$$

tends weakly, when $n, m \to \infty$ with $m/n \to \rho \in (0,1]$, to the Marchenko-Pastur law

$$\frac{1}{\rho \pi x} \sqrt{((x+1)^2 - \rho)(\rho - (x-1)^2)}\, \mathbf{1}_{[1-\sqrt{\rho}, 1+\sqrt{\rho}]}(x) dx.$$

We provide a proof of the Marchenko-Pastur theorem by using the methods of moments. When the entries of M have zero mean and finite fourth moment, Bai-Yin theorem furnishes the convergence at the edge of the support, in the sense that

$$s_m(M) \to 1 - \sqrt{\rho} \quad \text{and} \quad s_1(M) \to 1 + \sqrt{\rho}.$$

Chapter 4 gives only the basic aspects of the study of the singular values of random matrices; an immense and fascinating subject still under active development.

As it was pointed out in Chapter 2, studying the radius of the section of the cross-polytope with the kernel of a matrix is a central problem in approximate reconstruction. This approach is pursued in Chapter 5 for the model of partial discrete

Fourier matrices or Walsh matrices. The discrete Fourier matrix and the Walsh matrix are particular cases of orthogonal matrices with nicely bounded entries. More generally, we consider matrices whose rows are a system of pairwise orthogonal vectors $\phi_1, \ldots, \phi_N$ such that for any $i = 1, \ldots, N$, $|\phi_i|_2 = K$ and $|\phi_i|_\infty \leq 1/\sqrt{N}$. Several other models fall into this setting. Let Y be the random vector defined by $Y = \phi_i$ with probability $1/N$ and let $Y_1, \ldots, Y_n$ be independent copies of Y. One of the main results of Chapter 5 states that if

$$m \leq C_1 \ K^2 \frac{n}{\log N (\log n)^3}$$

then with probability greater than

$$1 - C_2 \exp\left(-C_3 K^2 n/m\right)$$

the matrix $\Phi = (Y_1, \ldots, Y_n)^\top$ satisfies

$$\mathrm{rad}\,(\ker \Phi \cap B_1^N) < \frac{1}{2\sqrt{m}}.$$

In Compressed Sensing, n is chosen relatively small with respect to N and the result is that up to logarithmic factors, if m is of the order of n, the matrix Φ has the following property that every m-sparse vector can be exactly reconstructed by the ℓ_1-minimization algorithm. The numbers C_1, C_2 and C_3 are numerical constants and replacing C_1 by a smaller constant allows approximate reconstruction by the ℓ_1-minimization algorithm. The randomness introduced here is called the *empirical method* and it is worth noticing that it can be replaced by the method of selectors: defining Φ with its row vectors $\{\phi_i, i \in I\}$ where $I = \{i, \delta_i = 1\}$ and $\delta_1, \ldots, \delta_N$ are independent identically distributed selectors taking values 1 with probability $\delta = n/N$ and 0 with probability $1 - \delta$. In this case the cardinality of I is approximately n with high probability.

Within the framework of the selection of characters, the situation is different. A useful observation is that it follows from the orthogonality of the system $\{\phi_1, \ldots, \phi_N\}$, that $\ker \Phi = \mathrm{span}\,\{\phi_j\}_{j \in J}$ where $\{Y_i\}_{i=1}^n = \{\phi_i\}_{i \notin J}$. Therefore the previous statement on $\mathrm{rad}\,(\ker \Phi \cap B_1^N)$ is equivalent to selecting $|J| \geq N - n$ vectors in $\{\phi_1, \ldots, \phi_N\}$ such that the ℓ_1^N norm and the ℓ_2^N norm are comparable on the linear span of these vectors. Indeed, the conclusion $\mathrm{rad}\,(\ker \Phi \cap B_1^N) < \frac{1}{2\sqrt{m}}$ is equivalent to the following inequality

$$\forall (\alpha_j)_{j \in J}, \ \left| \sum_{j \in J} \alpha_j \phi_j \right|_2 \leq \frac{1}{2\sqrt{m}} \left| \sum_{j \in J} \alpha_j \phi_j \right|_1 .$$

At issue is how large can be the cardinality of J so that the comparison between the ℓ_1^N norm and the ℓ_2^N norm on the subspace spanned by $\{\phi_j\}_{j \in J}$ is better than the trivial Hölder inequality. Choosing n of the order of $N/2$ gives already a remarkable result: there exists a subset J of cardinality greater than $N/2$ such that

$$\forall (\alpha_j)_{j \in J}, \ \frac{1}{\sqrt{N}} \left| \sum_{j \in J} \alpha_j \phi_j \right|_1 \leq \left| \sum_{j \in J} \alpha_j \phi_j \right|_2 \leq C_4 \, \frac{(\log N)^2}{\sqrt{N}} \left| \sum_{j \in J} \alpha_j \phi_j \right|_1 .$$

This is a Kashin type result. Nevertheless, it is important to remark that in the statement of the Dvoretzky [**FLM77**] or Kashin [**Kas77**] theorems concerning Euclidean sections of the cross-polytope, the subspace is such that the ℓ_2^N norm and the ℓ_1^N norm are equivalent (without the factor $\log N$): the cost is that the subspace has no particular structure. In the setting of Harmonic Analysis, the issue is to find a subspace with very strong properties. It should be a coordinate subspace with respect to the basis given by $\{\phi_1, \dots, \phi_N\}$. J. Bourgain noticed that a factor $\sqrt{\log N}$ is necessary in the last inequality above. Letting μ be the discrete probability measure on $\mathbb{R}^N$ with weight $1/N$ on each vectors of the canonical basis, the above inequalities tell that for all scalars $(\alpha_j)_{j\in J}$,

$$\left\|\sum_{j\in J}\alpha_j\phi_j\right\|_{L_1(\mu)} \leq \left\|\sum_{j\in J}\alpha_j\phi_j\right\|_{L_2(\mu)} \leq C_4\,(\log N)^2\left\|\sum_{j\in J}\alpha_j\phi_j\right\|_{L_1(\mu)}.$$

This explains the deep connection between Compressed Sensing and the problem of selecting a large part of a system of characters such that on its linear span, the $L_2(\mu)$ and the $L_1(\mu)$ norms are as close as possible. This problem of Harmonic Analysis goes back to the construction of $\Lambda(p)$ sets which are not $\Lambda(q)$ for $q > p$, where powerful methods based on random selectors were developed by J. Bourgain [**Bou89**]. M. Talagrand proved in [**Tal98**] that there exists a small numerical constant δ_0 and a subset J of cardinality greater than $\delta_0 N$ such that for all scalars $(\alpha_j)_{j\in J}$,

$$\left\|\sum_{j\in J}\alpha_j\phi_j\right\|_{L_1(\mu)} \leq \left\|\sum_{j\in J}\alpha_j\phi_j\right\|_{L_2(\mu)} \leq C_5\,\sqrt{\log N\log\log N}\left\|\sum_{j\in J}\alpha_j\phi_j\right\|_{L_1(\mu)}.$$

It is the purpose of Chapter 5 to emphasize the connections between Compressed Sensing and these problems of Harmonic Analysis. Tools from the theory of empirical processes lie at the heart of the techniques of proof. We will present the classical results from the theory of empirical processes and show how techniques from the Geometry of Banach Spaces are relevant in this setting. We will also present a strategy for extending the result of M. Talagrand [**Tal98**] to a Kashin type setting.

This book is based on a series of post-doctoral level lectures given at Université Paris-Est Marne-la-Vallée in fall 2009, by Djalil Chafaï, Olivier Guédon, Guillaume Lecué, Shahar Mendelson, and Alain Pajor. This collective pedagogical work aimed to bridge several actively developed domains of research. Each chapter of this book ends with a “Notes and comments” section gathering historical remarks and bibliographical references. We hope that the interactions at the heart of this book will be helpful to the non-specialist reader and may serve as an opening to further research.

We are grateful to all the 2009 fall school participants for their feedback. We are also indebted to all friends and colleagues, who made an important proofreading effort. In particular, the final form of this book benefited from the comments of Radek Adamczak, Florent Benaych-Georges, Simon Foucart, Rafal Latala, Mathieu Meyer, Holger Rauhut, and anonymous referees. We are indebted to the editorial board of the SMF publication Panoramas et Synthèses who has done a great job. We would like to thank in particular Franck Barthe, our editorial contact for this project. This collective work benefited from the excellent support of the Laboratoire d'Analyse et de Mathématiques Appliquées (LAMA) of Université Paris-Est Marne-la-Vallée.

CHAPTER 1

EMPIRICAL METHODS AND HIGH DIMENSIONAL GEOMETRY

This chapter is devoted to the presentation of classical tools that will be used within this book. We present some elementary properties of Orlicz spaces and develop the particular case of ψ_α random variables. Several characterizations are given in terms of tail estimates, Laplace transform and moments behavior. One of the important connections between high dimensional geometry and empirical processes comes from the behavior of the sum of independent ψ_α random variables. An important part of these preliminaries concentrates on this subject. We illustrate these connections with the presentation of the Johnson-Lindenstrauss lemma. The last part is devoted to the study of covering numbers. We focus our attention on some elementary properties and methods to obtain upper bounds for covering numbers.

1.1. Orlicz spaces

An Orlicz space is a function space which extends naturally the classical L_p spaces when $1 \leq p \leq +\infty$. A function $\psi : [0, \infty) \to [0, \infty]$ is said to be an Orlicz function if it is convex increasing with closed support (that is the convex set $\{x, \psi(x) < \infty\}$ is closed) such that $\psi(0) = 0$ and $\psi(x) \to \infty$ when $x \to \infty$.

Definition 1.1.1. — *Let ψ be an Orlicz function. For any real random variable X on a measurable space (Ω, σ, μ), we define its L_ψ norm by*

$$\|X\|_\psi = \inf \big\{ c > 0 : \mathbb{E}\psi\big(|X|/c\big) \leqslant \psi(1) \big\}.$$

The space $L_\psi(\Omega, \sigma, \mu) = \{X : \|X\|_\psi < \infty\}$ is called the Orlicz space associated to ψ.

Sometimes in the literature, Orlicz norms are defined differently, with 1 instead of $\psi(1)$. It is well known that L_ψ is a Banach space. Classical examples of Orlicz functions are for $p \geqslant 1$ and $\alpha \geqslant 1$:

$$\forall x \geq 0, \quad \phi_p(x) = x^p/p \quad \text{and} \quad \psi_\alpha(x) = \exp(x^\alpha) - 1.$$

The Orlicz space associated to ϕ_p is the classical L_p space. It is also clear by the monotone convergence theorem that the infimum in the definition of the L_ψ norm of a random variable X, if finite, is attained at $\|X\|_\psi$.

Let ψ be a nonnegative convex function on $[0,\infty)$. Its *convex conjugate* ψ^* (also called the *Legendre transform*) is defined on $[0,\infty)$ by:

$$\forall y \geq 0, \quad \psi^*(y) = \sup_{x>0}(xy - \psi(x)).$$

The convex conjugate of an Orlicz function is also an Orlicz function.

Proposition 1.1.2. — *Let ψ be an Orlicz function and ψ^* be its convex conjugate. For every real random variables $X \in L_\psi$ and $Y \in L_{\psi^*}$, one has*

$$\mathbb{E}|XY| \leqslant (\psi(1) + \psi^*(1)) \|X\|_\psi \|Y\|_{\psi^*} .$$

Proof. — By homogeneity, we can assume $\|X\|_\psi = \|Y\|_{\psi^*} = 1$. By definition of the convex conjugate, we have

$$|XY| \leqslant \psi(|X|) + \psi^*(|Y|) .$$

Taking the expectation, since $\mathbb{E}\psi(|X|) \leq \psi(1)$ and $\mathbb{E}\psi^*(|Y|) \leqslant \psi^*(1)$, we get that $\mathbb{E}|XY| \leq \psi(1) + \psi^*(1)$. □

If $p^{-1} + q^{-1} = 1$ then $\phi_p^* = \phi_q$ and it gives Young's inequality. In this case, Proposition 1.1.2 corresponds to Hölder inequality.

Any information about the ψ_α norm of a random variable is very useful to describe its tail behavior. This will be explained in Theorem 1.1.5. For instance, we say that X is a *sub-Gaussian* random variable when $\|X\|_{\psi_2} < \infty$ and that X is a *sub-exponential* random variable when $\|X\|_{\psi_1} < \infty$. In general, we say that X is ψ_α when $\|X\|_{\psi_\alpha} < \infty$. It is important to notice (see Corollary 1.1.6 and Proposition 1.1.7) that for any $\alpha_2 \geqslant \alpha_1 \geq 1$

$$L_\infty \subset L_{\psi_{\alpha_2}} \subset L_{\psi_{\alpha_1}} \subset \bigcap_{p\geq 1} L_p.$$

One of the main goal of these preliminaries is to understand the behavior of the maximum of a family of L_ψ-random variables and of the sum and product of ψ_α random variables. We start with a general maximal inequality.

Proposition 1.1.3. — *Let ψ be an Orlicz function. Then, for any positive integer n and any real valued random variables $X_1, \dots, X_n$,*

$$\mathbb{E} \max_{1\leq i\leq n} |X_i| \leq \psi^{-1}(n\psi(1)) \max_{1\leq i\leq n} \|X_i\|_\psi,$$

where ψ^{-1} is the inverse function of ψ. Moreover if ψ satisfies

$$\exists\, c > 0,\ \forall x,\, y \geq 1/2,\ \psi(x)\psi(y) \leqslant \psi(c\,x\,y) \tag{1.1}$$

then

$$\left\| \max_{1\leqslant i\leqslant n} |X_i| \right\|_\psi \leqslant c\ \max\left\{1/2, \psi^{-1}(2n)\right\} \max_{1\leqslant i\leqslant n} \|X_i\|_\psi ,$$

where c is the same as in (1.1).

Remark 1.1.4. —
(i) *Since for any* $x, y \geq 1/2$, $(e^x - 1)(e^y - 1) \leq e^{x+y} \leq e^{4xy} \leq (e^{8xy} - 1)$, *we get that for any* $\alpha \geq 1$, ψ_α *satisfies (1.1) with* $c = 8^{1/\alpha}$. *Moreover, one has* $\psi_\alpha^{-1}(n\psi_\alpha(1)) \leq (1 + \log(n))^{1/\alpha}$ *and* $\psi_\alpha^{-1}(2n) = (\log(1 + 2n))^{1/\alpha}$.
(ii) *Assumption(1.1) may be weakened to* $\limsup_{x,y\to\infty} \psi(x)\psi(y)/\psi(cxy) < \infty$.
(iii) *By monotonicity of* ψ, *for* $n \geq \psi(1/2)/2$, $\max\left\{1/2, \psi^{-1}(2n)\right\} = \psi^{-1}(2n)$.

Proof. — By homogeneity, we can assume that for any $i = 1, \ldots, n$, $\|X_i\|_\psi \leq 1$.

The first inequality is a simple consequence of Jensen's inequality. Indeed,

$$\psi(\mathbb{E} \max_{1\leq i\leq n} |X_i|) \leq \mathbb{E}\psi(\max_{1\leq i\leq n} |X_i|) \leq \sum_{i=1}^{n} \mathbb{E}\psi(|X_i|) \leq n\psi(1).$$

To prove the second assertion, we define $y = \max\{1/2, \psi^{-1}(2n)\}$. For any integer $i = 1, \ldots, n$, let $x_i = |X_i|/cy$. We observe that if $x_i \geq 1/2$ then we have by (1.1)

$$\psi\left(|X_i|/cy\right) \leq \frac{\psi(|X_i|)}{\psi(y)}.$$

Also note that by monotonicity of ψ,

$$\psi(\max_{1\leq i\leq n} x_i) \leq \psi(1/2) + \sum_{i=1}^{n} \psi(x_i) \mathbb{1}_{\{x_i \geq 1/2\}}.$$

Therefore, we have

$$\begin{aligned}\mathbb{E}\psi\left(\max_{1\leqslant i\leqslant n} |X_i|/cy\right) &\leqslant \psi(1/2) + \sum_{i=1}^{n} \mathbb{E}\psi\left(|X_i|)/cy\right) \mathbb{1}_{\{(|X_i|)/cy) \geq 1/2\}} \\ &\leq \psi(1/2) + \frac{1}{\psi(y)} \sum_{i=1}^{n} \mathbb{E}\psi(|X_i|) \leq \psi(1/2) + \frac{n\psi(1)}{\psi(y)}.\end{aligned}$$

From the convexity of ψ and the fact that $\psi(0) = 0$, we have $\psi(1/2) \leq \psi(1)/2$. The proof is finished since by definition of y, $\psi(y) \geq 2n$. □

For every $\alpha \geq 1$, there are very precise connections between the ψ_α norm of a random variable, the behavior of its L_p norms, its tail estimates and its Laplace transform. We sum up these connections.

Theorem 1.1.5. — *Let* X *be a real valued random variable and* $\alpha \geqslant 1$. *The following assertions are equivalent:*
(1) There exists $K_1 > 0$ *such that* $\|X\|_{\psi_\alpha} \leqslant K_1$.
(2) There exists $K_2 > 0$ *such that for every* $p \geq \alpha$,

$$\left(\mathbb{E}|X|^p\right)^{1/p} \leqslant K_2\, p^{1/\alpha}.$$

(3) There exist $K_3, K_3' > 0$ *such that for every* $t \geq K_3'$,

$$\mathbb{P}\left(|X| \geqslant t\right) \leqslant \exp\left(-t^\alpha/K_3^\alpha\right).$$

Moreover, we have

$$K_2 \leq 2eK_1, K_3 \leq eK_2, K_3' \leq e^2 K_2 \text{ and } K_1 \leq 2\max(K_3, K_3').$$

In the case $\alpha > 1$, let β be such that $1/\alpha + 1/\beta = 1$. The preceding assertions are also equivalent to the following:
(4) There exist $K_4, K_4' > 0$ such that for every $\lambda \geq 1/K_4'$,

$$\mathbb{E}\exp\big(\lambda|X|\big) \leqslant \exp\left(\lambda K_4\right)^{\beta}.$$

Moreover, $K_4 \leq K_1$, $K_4' \leq K_1$, $K_3 \leq 2K_4$ and $K_3' \leq 2K_4^{\beta}/(K_4')^{\beta-1}$.

Proof. — We start by proving that (1) implies (2). By the definition of the L_{ψ_α} norm, we have

$$\mathbb{E}\exp\left(\frac{|X|}{K_1}\right)^{\alpha} \leq e.$$

Moreover, for every positive integer q and every $x \geq 0$, $\exp x \geq x^q/q!$. Hence

$$\mathbb{E}|X|^{\alpha q} \leq e\, q! K_1^{\alpha q} \leq e q^q K_1^{\alpha q}.$$

For any $p \geq \alpha$, let q be the positive integer such that $q\alpha \leq p < (q+1)\alpha$ then

$$\begin{aligned}(\mathbb{E}|X|^p)^{1/p} \leq \Big(\mathbb{E}|X|^{(q+1)\alpha}\Big)^{1/(q+1)\alpha} &\leq e^{1/(q+1)\alpha} K_1 (q+1)^{1/\alpha} \\ &\leq e^{1/p} K_1 \left(\frac{2p}{\alpha}\right)^{1/\alpha} \leq 2eK_1 p^{1/\alpha}\end{aligned}$$

which means that (2) holds with $K_2 = 2eK_1$.

We now prove that (2) implies (3). We apply Markov inequality and the estimate of (2) to deduce that for every $t > 0$,

$$\mathbb{P}(|X| \geq t) \leq \inf_{p>0} \frac{\mathbb{E}|X|^p}{t^p} \leq \inf_{p\geq\alpha} \left(\frac{K_2}{t}\right)^p p^{p/\alpha} = \inf_{p\geq\alpha} \exp\left(p\log\left(\frac{K_2 p^{1/\alpha}}{t}\right)\right).$$

Choosing $p = (t/eK_2)^\alpha \geq \alpha$, we get that for $t \geq e\, K_2 \alpha^{1/\alpha}$, we indeed have $p \geq \alpha$ and conclude that

$$\mathbb{P}(|X| \geq t) \leq \exp\left(-t^\alpha/(K_2 e)^\alpha\right).$$

Since $\alpha \geq 1$, $\alpha^{1/\alpha} \leq e$ and (3) holds with $K_3' = e^2 K_2$ and $K_3 = eK_2$.

To prove that (3) implies (1), assume (3) and let $c = 2\max(K_3, K_3')$. By integration by parts, we get

$$\begin{aligned}\mathbb{E}\exp\left(\frac{|X|}{c}\right)^{\alpha} - 1 &= \int_0^{+\infty} \alpha u^{\alpha-1} e^{u^\alpha} \mathbb{P}(|X| \geq uc) du \\ &\leq \int_0^{K_3'/c} \alpha u^{\alpha-1} e^{u^\alpha} du + \int_{K_3'/c}^{+\infty} \alpha u^{\alpha-1} \exp\left(u^\alpha\left(1 - \frac{c^\alpha}{K_3^\alpha}\right)\right) du \\ &= \exp\left(\frac{K_3'}{c}\right)^{\alpha} - 1 + \frac{1}{\frac{c^\alpha}{K_3^\alpha} - 1} \exp\left(-\left(\frac{c^\alpha}{K_3^\alpha} - 1\right)\left(\frac{K_3'}{c}\right)^{\alpha}\right) \\ &\leq 2\cosh(K_3'/c)^\alpha - 1 \leq 2\cosh(1/2) - 1 \leq e - 1\end{aligned}$$

by definition of c and the fact that $\alpha \geq 1$. This proves (1) with $K_1 = 2\max(K_3, K_3')$.

We now assume that $\alpha > 1$ and prove that (4) implies (3). We apply Markov inequality and the estimate of (4) to get that for every $t > 0$,

$$\begin{aligned}\mathbb{P}(|X| > t) &\leqslant \inf_{\lambda>0} \exp(-\lambda t)\mathbb{E}\exp\big(\lambda|X|\big)\\ &\leqslant \inf_{\lambda\geq 1/K_4'} \exp\big((\lambda K_4)^\beta - \lambda t\big).\end{aligned}$$

Choosing $\lambda t = 2(\lambda K_4)^\beta$ we get that if $t \geq 2K_4^\beta/(K_4')^{\beta-1}$, then $\lambda \geq 1/K_4'$. We conclude that

$$\mathbb{P}(|X| > t) \leq \exp\left(-t^\alpha/(2K_4)^\alpha\right).$$

This proves (3) with $K_3 = 2K_4$ and $K_3' = 2K_4^\beta/(K_4')^{\beta-1}$.

It remains to prove that (1) implies (4). We already observed that the convex conjugate of the function $\phi_\alpha(t) = t^\alpha/\alpha$ is ϕ_β which implies that for $x, y \geqslant 0$,

$$xy \leq \frac{x^\alpha}{\alpha} + \frac{y^\beta}{\beta}.$$

Hence for $\lambda > 0$, by convexity of the exponential

$$\exp(\lambda|X|) \leq \frac{1}{\alpha}\exp\left(\frac{|X|}{K_1}\right)^\alpha + \frac{1}{\beta}\exp\left(\lambda K_1\right)^\beta.$$

Taking the expectation, we get by definition of the L_{ψ_α} norm that

$$\mathbb{E}\exp(\lambda|X|) \leq \frac{e}{\alpha} + \frac{1}{\beta}\exp\left(\lambda K_1\right)^\beta.$$

We conclude that if $\lambda \geq 1/K_1$ then

$$\mathbb{E}\exp(\lambda|X|) \leq \exp\left(\lambda K_1\right)^\beta$$

which proves (4) with $K_4 = K_1$ and $K_4' = K_1$. □

A simple corollary of Theorem 1.1.5 is the following connection between the L_p norms of a random variable and its ψ_α norm.

Corollary 1.1.6. — *For every $\alpha \geq 1$ and every real random variable X,*

$$\frac{1}{2e^2}\|X\|_{\psi_\alpha} \leqslant \sup_{p\geqslant\alpha} \frac{(\mathbb{E}|X|^p)^{1/p}}{p^{1/\alpha}} \leqslant 2e\|X\|_{\psi_\alpha}.$$

Moreover, one has $L_\infty \subset L_{\psi_\alpha}$ and $\|X\|_{\psi_\alpha} \leq \|X\|_{L_\infty}$.

Proof. — This follows from the implications (1) ⇒ (2) ⇒ (3) ⇒ (1) in Theorem 1.1.5 and the computations of K_2, K_3, K_3' and K_1. The moreover part is a direct application of the definition of the ψ_α norm. □

We conclude with a kind of Hölder inequality for ψ_α random variables.

Proposition 1.1.7. — *Let p and q be in $[1, +\infty]$ such that $1/p + 1/q = 1$. For any real random variables $X \in L_{\psi_p}$ and $Y \in L_{\psi_q}$, we have*

$$\|XY\|_{\psi_1} \leq \|X\|_{\psi_p}\|Y\|_{\psi_q}. \tag{1.2}$$

Moreover, if $1 \leq \alpha \leq \beta$, one has $\|X\|_{\psi_1} \leq \|X\|_{\psi_\alpha} \leq \|X\|_{\psi_\beta}$.

Proof. — By homogeneity, we assume that $\|X\|_{\psi_p} = \|Y\|_{\psi_q} = 1$. Since p and q are conjugate, we know by Young inequality that for every $x, y \in \mathbb{R}$, $|xy| \leq \frac{|x|^p}{p} + \frac{|x|^q}{q}$. By convexity of the exponential, we deduce that

$$\mathbb{E}\exp(|XY|) \leq \frac{1}{p}\mathbb{E}\exp|X|^p + \frac{1}{q}\mathbb{E}\exp|X|^q \leq e$$

which proves that $\|XY\|_{\psi_1} \leq 1$.

For the "moreover part", by definition of the ψ_q-norm, the random variable $Y = 1$ satisifes $\|Y\|_{\psi_q} = 1$. Hence applying (1.2) with $p = \alpha$ and q being the conjugate of p, we get that for every $\alpha \geq 1$, $\|X\|_{\psi_1} \leq \|X\|_{\psi_\alpha}$. We also observe that for any $\beta \geq \alpha$, if $\delta \geq 1$ is such that $\beta = \alpha\delta$ then we have

$$\|X\|_{\psi_\alpha}^\alpha = \||X|^\alpha\|_{\psi_1} \leq \||X|^\alpha\|_{\psi_\delta} = \|X\|_{\psi_{\alpha\delta}}^\alpha$$

which proves that $\|X\|_{\psi_\alpha} \leq \|X\|_{\psi_\beta}$. □

1.2. Linear combination of Psi-alpha random variables

In this part, we focus on the case of independent centered ψ_α random variables when $\alpha \geq 1$. We present several results concerning the linear combination of such random variables. The cases $\alpha = 2$ and $\alpha \neq 2$ are analyzed by different means. We start by looking at the case $\alpha = 2$. Even if we prove a sharp estimate for their linear combination, we also consider the simple and well known example of linear combination of independent Rademacher variables, which shows the limitation of the classification through the ψ_α-norms of certain random variables. However in the case $\alpha \neq 2$, different regimes appear in the tail estimates of such sum. This will be of importance in the next chapters.

The sub-Gaussian case.— We start by taking a look at sums of ψ_2 random variables. The following proposition can be seen as a generalization of the classical Hoeffding inequality [**Hoe63**] since $L_\infty \subset L_{\psi_2}$.

Theorem 1.2.1. — *Let $X_1, \ldots, X_n$ be independent real valued random variables such that for any $i = 1, \ldots, n$, $\mathbb{E}X_i = 0$. Then*

$$\left\|\sum_{i=1}^n X_i\right\|_{\psi_2} \leqslant c\left(\sum_{i=1}^n \|X_i\|_{\psi_2}^2\right)^{1/2}$$

where $c \leq 16$.

Before proving the theorem, we start with the following lemma concerning the Laplace transform of a ψ_2 random variable which is centered. The fact that $\mathbb{E}X = 0$ is crucial to improve assertion(4) of Theorem 1.1.5.

Lemma 1.2.2. — *Let X be a ψ_2 centered random variable. Then, for any $\lambda > 0$, the Laplace transform of X satisfies*

$$\mathbb{E}\exp(\lambda X) \leqslant \exp\left(e\lambda^2 \|X\|_{\psi_2}^2\right).$$

Proof. — By homogeneity, we can assume that $\|X\|_{\psi_2} = 1$. By the definition of the L_{ψ_2} norm, we know that

$$\mathbb{E}\exp\left(X^2\right) \le e \quad \text{and} \quad \text{for any integer } k, \mathbb{E}X^{2k} \le ek!$$

Let Y be an independent copy of X. By convexity of the exponential and Jensen's inequality, since $\mathbb{E}Y = 0$ we have

$$\mathbb{E}\exp(\lambda X) \le \mathbb{E}_X\mathbb{E}_Y \exp\lambda(X - Y).$$

Moreover, since the random variable $X - Y$ is symmetric, one has

$$\mathbb{E}_X\mathbb{E}_Y \exp\lambda(X-Y) = 1 + \frac{\lambda^2}{2}\mathbb{E}_X\mathbb{E}_Y(X-Y)^2 + \sum_{k=2}^{+\infty}\frac{\lambda^{2k}}{(2k)!}\mathbb{E}_X\mathbb{E}_Y(X-Y)^{2k}.$$

Obviously, $\mathbb{E}_X\mathbb{E}_Y(X-Y)^2 = 2\mathbb{E}X^2 \le 2e$ and $\mathbb{E}_X\mathbb{E}_Y(X-Y)^{2k} \le 4^k\mathbb{E}X^{2k} \le e4^kk!$. Since the sequence $v_k = (2k)!/3^k(k!)^2$ is nondecreasing, we know that for $k \ge 2$ $v_k \ge v_2 = 6/3^2$ so that

$$\forall k \ge 2,\ \frac{1}{(2k)!}\mathbb{E}_X\mathbb{E}_Y(X-Y)^{2k} \le \frac{e4^kk!}{(2k)!} \le \frac{e3^2}{6}\left(\frac{4}{3}\right)^k\frac{1}{k!} \le \left(\frac{4\sqrt{e}}{\sqrt{6}}\right)^k\frac{1}{k!} \le \frac{e^k}{k!}.$$

It follows that for every $\lambda > 0$, $\mathbb{E}\exp(\lambda X) \le 1 + e\lambda^2 + \sum_{k=2}^{+\infty}\frac{(e\lambda^2)^k}{k!} = \exp(e\lambda^2)$. □

Proof of Theorem 1.2.1. — It is enough to get an upper bound of the Laplace transform of the random variable $\left|\sum_{i=1}^n X_i\right|$. Let $Z = \sum_{i=1}^n X_i$. By independence of the X_i's, we get from Lemma 1.2.2 that for every $\lambda > 0$,

$$\mathbb{E}\exp(\lambda Z) = \prod_{i=1}^n \mathbb{E}\exp(\lambda X_i) \leqslant \exp\left(e\lambda^2\sum_{i=1}^n \|X_i\|_{\psi_2}^2\right).$$

For the same reason, $\mathbb{E}\exp(-\lambda Z) \leqslant \exp\left(e\lambda^2\sum_{i=1}^n \|X_i\|_{\psi_2}^2\right)$. Thus,

$$\mathbb{E}\exp(\lambda|Z|) \leqslant 2\exp\left(3\lambda^2\sum_{i=1}^n \|X_i\|_{\psi_2}^2\right).$$

We conclude that for any $\lambda \ge 1/\left(\sum_{i=1}^n \|X_i\|_{\psi_2}^2\right)^{1/2}$,

$$\mathbb{E}\exp(\lambda|Z|) \leqslant \exp\left(4\lambda^2\sum_{i=1}^n \|X_i\|_{\psi_2}^2\right)$$

and using the implication $((4) \Rightarrow (1))$ in Theorem 1.1.5 with $\alpha = \beta = 2$ (with the estimates of the constants), we get that $\|Z\|_{\psi_2} \le c(\sum_{i=1}^n \|X_i\|_{\psi_2}^2)^{1/2}$ with $c \le 16$. □

Now, we take a particular look at Rademacher processes. Indeed, Rademacher variables are the simplest example of non-trivial bounded (hence ψ_2) random variables. We denote by $\varepsilon_1, \dots, \varepsilon_n$ independent random variables taking values ± 1 with probability $1/2$. By definition of L_{ψ_2}, for any $(a_1, \dots, a_n) \in \mathbb{R}^n$, the random variable

$a_i\varepsilon_i$ is centered and has ψ_2 norm equal to $|a_i|$. We apply Theorem 1.2.1 to deduce that

$$\left\|\sum_{i=1}^n a_i\varepsilon_i\right\|_{\psi_2} \le c|a|_2 = c\left(\mathbb{E}\left|\sum_{i=1}^n a_i\varepsilon_i\right|^2\right)^{1/2}.$$

Therefore we get from Theorem 1.1.5 that for any $p \ge 2$,

$$\left(\mathbb{E}\left|\sum_{i=1}^n a_i\varepsilon_i\right|^2\right)^{1/2} \le \left(\mathbb{E}\left|\sum_{i=1}^n a_i\varepsilon_i\right|^p\right)^{1/p} \le 2c\sqrt{p}\left(\mathbb{E}\left|\sum_{i=1}^n a_i\varepsilon_i\right|^2\right)^{1/2}. \tag{1.3}$$

This is Khinchine's inequality. It is not difficult to extend it to the case $0 < q \le 2$ by using Hölder inequality: for any random variable Z, if $0 < q \le 2$ and $\lambda = q/(4-q)$ then

$$\left(\mathbb{E}|Z|^2\right)^{1/2} \le \left(\mathbb{E}|Z|^q\right)^{\lambda/q}\left(\mathbb{E}|Z|^4\right)^{(1-\lambda)/4}.$$

Let $Z = \sum_{i=1}^n a_i\varepsilon_i$, we apply (1.3) to the case $p = 4$ to deduce that for any $0 < q \le 2$,

$$\left(\mathbb{E}\left|\sum_{i=1}^n a_i\varepsilon_i\right|^q\right)^{1/q} \le \left(\mathbb{E}\left|\sum_{i=1}^n a_i\varepsilon_i\right|^2\right)^{1/2} \le (4c)^{2(2-q)/q}\left(\mathbb{E}\left|\sum_{i=1}^n a_i\varepsilon_i\right|^q\right)^{1/q}.$$

Since for any $x \ge 0$, $e^{x^2} - 1 \ge x^2$, we also observe that

$$(e-1)\left\|\sum_{i=1}^n a_i\varepsilon_i\right\|_{\psi_2} \ge \left(\mathbb{E}\left|\sum_{i=1}^n a_i\varepsilon_i\right|^2\right)^{1/2}.$$

However the precise knowledge of the ψ_2 norm of the random variable $\sum_{i=1}^n a_i\varepsilon_i$ is not enough to understand correctly the behavior of its L_p norms and consequently of its tail estimate. Indeed, a more precise statement holds.

Theorem 1.2.3. — *Let $p \geqslant 2$, let $a_1, \ldots, a_n$ be real numbers and let $\varepsilon_1, \ldots, \varepsilon_n$ be independent Rademacher variables. We have*

$$\left(\mathbb{E}\left|\sum_{i=1}^n a_i\varepsilon_i\right|^p\right)^{1/p} \le \sum_{i\leqslant p} a_i^* + 2c\sqrt{p}\left(\sum_{i>p} a_i^{*2}\right)^{1/2},$$

where $(a_1^*, \ldots, a_n^*)$ is the non-increasing rearrangement of $(|a_1|, \ldots, |a_n|)$. Moreover, this estimate is sharp, up to a multiplicative factor.

Remark 1.2.4. — *We do not present the proof of the lower bound even if it is the difficult part of Theorem 1.2.3. It is beyond the scope of this chapter.*

Proof. — Since Rademacher random variables are bounded by 1, we have

$$\left(\mathbb{E}\left|\sum_{i=1}^n a_i\varepsilon_i\right|^p\right)^{1/p} \le \sum_{i=1}^n |a_i|. \tag{1.4}$$

By independence and by symmetry of Rademacher variables we have

$$\left(\mathbb{E}\left|\sum_{i=1}^{n} a_i \varepsilon_i\right|^p\right)^{1/p} = \left(\mathbb{E}\left|\sum_{i=1}^{n} a_i^* \varepsilon_i\right|^p\right)^{1/p}.$$

Splitting the sum into two parts, we get that

$$\left(\mathbb{E}\left|\sum_{i=1}^{n} a_i^* \varepsilon_i\right|^p\right)^{1/p} \leq \left(\mathbb{E}\left|\sum_{i=1}^{p} a_i^* \varepsilon_i\right|^p\right)^{1/p} + \left(\mathbb{E}\left|\sum_{i>p} a_i^* \varepsilon_i\right|^p\right)^{1/p}.$$

We conclude by applying (1.4) to the first term and (1.3) to the second one. □

Rademacher processes as studied in Theorem 1.2.3 provide good examples of one of the main drawbacks of a classification of random variables based on ψ_α-norms. Indeed, being a ψ_α random variable allows only one type of tail estimate: if $Z \in L_{\psi_\alpha}$ then the tail decay of Z behaves like $\exp(-Kt^\alpha)$ for t large enough. But this result is sometimes too weak for a precise study of the L_p norm of Z.

Bernstein's type inequalities, the case $\alpha = 1$. — We start with Bennett's inequalities for an empirical mean of bounded random variables, see also the Azuma-Hoeffding inequality in Chapter 4, Lemma 4.7.2.

Theorem 1.2.5. — *Let $X_1, \ldots, X_n$ be n independent random variables and M be a positive number such that for any $i = 1, \ldots, n$, $\mathbb{E}X_i = 0$ and $|X_i| \leqslant M$ almost surely. Set $\sigma^2 = n^{-1}\sum_{i=1}^n \mathbb{E}X_i^2$. For any $t > 0$, we have*

$$\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^{n} X_i \geqslant t\right) \leqslant \exp\left(-\frac{n\sigma^2}{M^2} h\left(\frac{Mt}{\sigma^2}\right)\right),$$

where $h(u) = (1+u)\log(1+u) - u$ for all $u > 0$.

Proof. — Let $t > 0$. By Markov inequality and independence, we have

$$\begin{aligned}\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^{n} X_i \geqslant t\right) &\leqslant \inf_{\lambda>0} \exp(-\lambda t)\mathbb{E}\exp\left(\frac{\lambda}{n}\sum_{i=1}^{n} X_i\right) \\ &= \inf_{\lambda>0} \exp(-\lambda t)\prod_{i=1}^{n}\mathbb{E}\exp\left(\frac{\lambda X_i}{n}\right). \qquad (1.5)\end{aligned}$$

Since for any $i = 1, \ldots, n$, $\mathbb{E}X_i = 0$ and $|X_i| \leq M$,

$$\begin{aligned}\mathbb{E}\exp\left(\frac{\lambda X_i}{n}\right) &= 1 + \sum_{k\geqslant 2}\frac{\lambda^k \mathbb{E}X_i^k}{n^k k!} \leq 1 + \mathbb{E}X_i^2 \sum_{k\geqslant 2}\frac{\lambda^k M^{k-2}}{n^k k!} \\ &= 1 + \frac{\mathbb{E}X_i^2}{M^2}\left(\exp\left(\frac{\lambda M}{n}\right) - \left(\frac{\lambda M}{n}\right) - 1\right).\end{aligned}$$

Using the fact that $1+u \leqslant \exp(u)$ for all $u \in \mathbb{R}$, we get

$$\prod_{i=1}^{n} \mathbb{E}\exp\left(\frac{\lambda X_i}{n}\right) \leq \exp\left(\frac{\sum_{i=1}^{n}\mathbb{E}X_i^2}{M^2}\left(\exp\left(\frac{\lambda M}{n}\right) - \left(\frac{\lambda M}{n}\right) - 1\right)\right).$$

By definition of σ and (1.5), we conclude that for any $t > 0$,

$$\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^{n} X_i \geqslant t\right) \leq \inf_{\lambda>0} \exp\left(\frac{n\sigma^2}{M^2}\left(\exp\left(\frac{\lambda M}{n}\right) - \left(\frac{\lambda M}{n}\right) - 1\right) - \lambda t\right).$$

The claim follows by choosing λ such that $(1 + tM/\sigma^2) = \exp(\lambda M/n)$. □

Using a Taylor expansion, we see that for every $u > 0$ we have $h(u) \geqslant u^2/(2+2u/3)$. This proves that if $u \geq 1$, $h(u) \geq 3u/8$ and if $u \leq 1$, $h(u) \geq 3u^2/8$. Therefore Bernstein's inequality for bounded random variables is an immediate corollary of Theorem 1.2.5.

Theorem 1.2.6. — *Let $X_1, \dots, X_n$ be n independent random variables such that for all $i = 1, \dots, n$, $\mathbb{E}X_i = 0$ and $|X_i| \leqslant M$ almost surely. Then, for every $t > 0$,*

$$\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^{n} X_i \geqslant t\right) \leqslant \exp\left(-\frac{3n}{8}\min\left(\frac{t^2}{\sigma^2}, \frac{t}{M}\right)\right),$$

where $\sigma^2 = \frac{1}{n}\sum_{i=1}^{n}\mathbb{E}X_i^2$.

From Bernstein's inequality, we can deduce that the tail behavior of a sum of centered, bounded random variables has two regimes. There is a sub-exponential regime with respect to M for large values of t ($t \geqslant \sigma^2/M$) and a sub-Gaussian behavior with respect to σ^2 for small values of t ($t \leqslant \sigma^2/M$). Moreover, this inequality is always stronger than the tail estimate that we could deduce from Theorem 1.2.1 (which is only sub-Gaussian with respect to M^2).

Now, we turn to the important case of sum of sub-exponential centered random variables.

Theorem 1.2.7. — *Let $X_1, \dots, X_n$ be n independent centered ψ_1 random variables. Then, for every $t > 0$,*

$$\mathbb{P}\left(\left|\frac{1}{n}\sum_{i=1}^{n} X_i\right| \geqslant t\right) \leqslant 2\exp\left(-c\,n\min\left(\frac{t^2}{\sigma_1^2}, \frac{t}{M_1}\right)\right),$$

where $M_1 = \max_{1\leqslant i\leqslant n}\|X_i\|_{\psi_1}$, $\sigma_1^2 = \frac{1}{n}\sum_{i=1}^{n}\|X_i\|_{\psi_1}^2$ *and* $c \leqslant 1/2(2e-1)$.

Proof. — Since for every $x \geq 0$ and any positive natural integer k, $e^x - 1 \geq x^k/k!$, we get by definition of the ψ_1 norm that for any integer $k \geq 1$ and any $i = 1, \dots, n$,

$$\mathbb{E}|X_i|^k \leqslant (e-1)k!\,\|X_i\|_{\psi_1}^k.$$

Moreover $\mathbb{E}X_i = 0$ for $i = 1, \dots, n$ and using Taylor expansion of the exponential, we deduce that for every $\lambda > 0$ such that $\lambda \|X_i\|_{\psi_1} \le \lambda M_1 < n$,

$$\mathbb{E}\exp\left(\frac{\lambda}{n}X_i\right) \leqslant 1 + \sum_{k\geqslant 2} \frac{\lambda^k \mathbb{E}|X_i|^k}{n^k k!} \leqslant 1 + \frac{(e-1)\lambda^2 \|X_i\|_{\psi_1}^2}{n^2\left(1 - \frac{\lambda}{n}\|X_i\|_{\psi_1}\right)} \le 1 + \frac{(e-1)\lambda^2 \|X_i\|_{\psi_1}^2}{n^2\left(1 - \frac{\lambda M_1}{n}\right)}.$$

Let $Z = n^{-1}\sum_{i=1}^n X_i$. Since for any real number x, $1+x \le e^x$, we get by independence of the X_i's that for every $\lambda > 0$ such that $\lambda M_1 < n$

$$\mathbb{E}\exp(\lambda Z) \le \exp\left(\frac{(e-1)\lambda^2}{n^2\left(1-\frac{\lambda M_1}{n}\right)}\sum_{i=1}^n \|X_i\|_{\psi_1}^2\right) = \exp\left(\frac{(e-1)\lambda^2\sigma_1^2}{n - \lambda M_1}\right).$$

We conclude by Markov inequality that for every $t > 0$,

$$\mathbb{P}(Z \ge t) \le \inf_{0<\lambda<n/M_1} \exp\left(-\lambda\, t + \frac{(e-1)\lambda^2\sigma_1^2}{n-\lambda M_1}\right).$$

We consider two cases. If $t \le \sigma_1^2/M_1$, we choose $\lambda = nt/2e\sigma_1^2 \le n/2eM_1$. A simple computation gives that

$$\mathbb{P}(Z \ge t) \le \exp\left(-\frac{1}{2(2e-1)}\,\frac{n\,t^2}{\sigma_1^2}\right).$$

If $t > \sigma_1^2/M_1$, we choose $\lambda = n/2eM_1$. We get

$$\mathbb{P}(Z \ge t) \le \exp\left(-\frac{1}{2(2e-1)}\,\frac{n\,t}{M_1}\right).$$

We can apply the same argument for $-Z$ and this concludes the proof. □

The ψ_α case: $\alpha > 1$. — In this part we will focus on the case $\alpha \neq 2$ and $\alpha > 1$. Our goal is to explain the behavior of the tail estimate of a sum of independent ψ_α centered random variables. As in Bernstein inequalities, there are two different regimes depending on the level of deviation t.

Theorem 1.2.8. — *Let $\alpha > 1$ and β be such that $\alpha^{-1} + \beta^{-1} = 1$. Let $X_1, \dots, X_n$ be independent mean zero ψ_α real-valued random variables, set*

$$A_1 = \left(\sum_{i=1}^n \|X_i\|_{\psi_1}^2\right)^{1/2}, \quad B_\alpha = \left(\sum_{i=1}^n \|X_i\|_{\psi_\alpha}^\beta\right)^{1/\beta} \quad \text{and} \quad A_\alpha = \left(\sum_{i=1}^n \|X_i\|_{\psi_\alpha}^2\right)^{1/2}.$$

Then, for every $t > 0$,

$$\mathbb{P}\left(\left|\sum_{i=1}^n X_i\right| \geqslant t\right) \le \begin{cases} 2\exp\left(-C\min\left(\frac{t^2}{A_1^2}, \frac{t^\alpha}{B_\alpha^\alpha}\right)\right) & \text{if } \alpha < 2, \\ 2\exp\left(-C\max\left(\frac{t^2}{A_\alpha^2}, \frac{t^\alpha}{B_\alpha^\alpha}\right)\right) & \text{if } \alpha > 2 \end{cases}$$

where C is an absolute constant.

Remark 1.2.9. — *This result can be stated with the same normalization as in Bernstein's inequalities. Let*

$$\sigma_1^2 = \frac{1}{n}\sum_{i=1}^n \|X_i\|_{\psi_1}^2, \quad \sigma_\alpha^2 = \frac{1}{n}\sum_{i=1}^n \|X_i\|_{\psi_\alpha}^2, \quad M_\alpha^\beta = \frac{1}{n}\sum_{i=1}^n \|X_i\|_{\psi_\alpha}^\beta,$$

then we have

$$\mathbb{P}\left(\left|\frac{1}{n}\sum_{i=1}^n X_i\right| \geqslant t\right) \leq \begin{cases} 2\exp\left(-Cn\min\left(\frac{t^2}{\sigma_1^2}, \frac{t^\alpha}{M_\alpha^\alpha}\right)\right) & \text{if } \alpha < 2, \\ 2\exp\left(-Cn\max\left(\frac{t^2}{\sigma_\alpha^2}, \frac{t^\alpha}{M_\alpha^\alpha}\right)\right) & \text{if } \alpha > 2. \end{cases}$$

Before proving Theorem 1.2.8, we start by exhibiting a sub-Gaussian behavior of the Laplace transform of any ψ_1 centered random variable.

Lemma 1.2.10. — *Let X be a ψ_1 mean-zero random variable. If λ satisfies $0 \leq \lambda \leqslant \left(2\|X\|_{\psi_1}\right)^{-1}$, we have*

$$\mathbb{E}\exp(\lambda X) \leqslant \exp\left(4(e-1)\lambda^2\|X\|_{\psi_1}^2\right).$$

Proof. — Let X' be an independent copy of X and denote $Y = X - X'$. Since X is centered, by Jensen's inequality,

$$\mathbb{E}\exp\lambda X = \mathbb{E}\exp(\lambda(X - \mathbb{E}X')) \leqslant \mathbb{E}\exp\lambda(X - X') = \mathbb{E}\exp\lambda Y.$$

The random variable Y is symmetric thus, for every λ, $\mathbb{E}\exp\lambda Y = \mathbb{E}\cosh\lambda Y$ and using the Taylor expansion,

$$\mathbb{E}\exp\lambda Y = 1 + \sum_{k\geq 1}\frac{\lambda^{2k}}{(2k)!}\mathbb{E}Y^{2k} = 1 + \lambda^2\sum_{k\geq 1}\frac{\lambda^{2(k-1)}}{(2k)!}\mathbb{E}Y^{2k}.$$

By definition of Y, for every $k \geq 1$, $\mathbb{E}Y^{2k} \leq 2^{2k}\mathbb{E}X^{2k}$. Hence, for $0 \leqslant \lambda \leqslant \left(2\|X\|_{\psi_1}\right)^{-1}$, we get

$$\mathbb{E}\exp\lambda Y \leq 1 + 4\lambda^2\|X\|_{\psi_1}^2\sum_{k\geq 1}\frac{\mathbb{E}X^{2k}}{(2k)!\|X\|_{\psi_1}^{2k}} \leq 1 + 4\lambda^2\|X\|_{\psi_1}^2\left(\mathbb{E}\exp\left(\frac{|X|}{\|X\|_{\psi_1}}\right) - 1\right).$$

By definition of the ψ_1 norm, we conclude that

$$\mathbb{E}\exp\lambda X \leq 1 + 4(e-1)\lambda^2\|X\|_{\psi_1}^2 \leq \exp\left(4(e-1)\lambda^2\|X\|_{\psi_1}^2\right).$$

□

Proof of Theorem 1.2.8. — We start with the case $1 < \alpha < 2$.
For $i = 1, \ldots, n$, X_i is ψ_α with $\alpha > 1$. Thus, it is a ψ_1 random variable (see Proposition 1.1.7) and from Lemma 1.2.10, we get

$$\forall\ 0 \leq \lambda \leq 1/(2\|X_i\|_{\psi_1}),\ \mathbb{E}\exp\lambda X_i \leq \exp\left(4(e-1)\lambda^2\|X_i\|_{\psi_1}^2\right).$$

It follows from Theorem 1.1.5 that

$$\forall\,\lambda \geq 1/\|X_i\|_{\psi_\alpha},\ \mathbb{E}\exp\lambda X_i \leq \exp\left(\lambda\,\|X_i\|_{\psi_\alpha}\right)^\beta.$$

Since $1 < \alpha < 2$ one has $\beta > 2$ and it is easy to conclude that for $c = 4(e-1)$ we have

$$\forall\,\lambda > 0,\ \mathbb{E}\exp\lambda X_i \leq \exp\left(c\left(\lambda^2\|X_i\|_{\psi_1}^2 + \lambda^\beta\|X_i\|_{\psi_\alpha}^\beta\right)\right). \tag{1.6}$$

Indeed when $\|X_i\|_{\psi_\alpha} > 2\|X_i\|_{\psi_1}$, we just have to glue the two estimates. When we have $\|X_i\|_{\psi_\alpha} \leq 2\|X_i\|_{\psi_1}$, we get by Hölder inequality, for every $\lambda \in \left(1/2\,\|X_i\|_{\psi_1}, 1/\|X_i\|_{\psi_\alpha}\right)$,

$$\mathbb{E}\exp\lambda X_i \leq \left(\mathbb{E}\exp\left(\frac{X_i}{\|X_i\|_{\psi_\alpha}}\right)\right)^{\lambda\|X_i\|_{\psi_\alpha}} \leq \exp\left(\lambda\|X_i\|_{\psi_\alpha}\right) \leq \exp\left(\lambda^2 4\|X_i\|_{\psi_1}^2\right).$$

Let now $Z = \sum_{i=1}^n X_i$. We deduce from (1.6) that for every $\lambda > 0$,

$$\mathbb{E}\exp\lambda Z \leq \exp\left(c\left(A_1^2\lambda^2 + B_\alpha^\beta\lambda^\beta\right)\right).$$

From Markov inequality, we have

$$\mathbb{P}(Z \geq t) \leq \inf_{\lambda>0} e^{-\lambda t}\mathbb{E}\exp\lambda Z \leq \inf_{\lambda>0}\exp\left(c\left(A_1^2\lambda^2 + B_\alpha^\beta\lambda^\beta\right) - \lambda t\right). \tag{1.7}$$

If $(t/A_1)^2 \geq (t/B_\alpha)^\alpha$, we have $t^{2-\alpha} \geq A_1^2/B_\alpha^\alpha$ and we choose $\lambda = \frac{t^{\alpha-1}}{4cB_\alpha^\alpha}$. Therefore,

$$\lambda t = \frac{t^\alpha}{4cB_\alpha^\alpha}, \quad B_\alpha^\beta\lambda^\beta = \frac{t^\alpha}{(4c)^\beta B_\alpha^\alpha} \leq \frac{t^\alpha}{(4c)^2 B_\alpha^\alpha}, \quad \text{and}$$
$$A_1^2\lambda^2 = \frac{t^\alpha}{(4c)^2 B_\alpha^\alpha}\frac{t^{\alpha-2}A_1^2}{B_\alpha^\alpha} \leq \frac{t^\alpha}{(4c)^2 B_\alpha^\alpha}.$$

We conclude from (1.7) that

$$\mathbb{P}(Z \geq t) \leq \exp\left(-\frac{1}{8c}\frac{t^\alpha}{B_\alpha^\alpha}\right).$$

If $(t/A_1)^2 \leq (t/B_\alpha)^\alpha$, we have $t^{2-\alpha} \leq A_1^2/B_\alpha^\alpha$ and since $(2-\alpha)\beta/\alpha = (\beta-2)$ we also have $t^{\beta-2} \leq A_1^{2(\beta-1)}/B_\alpha^\beta$. We choose $\lambda = \frac{t}{4cA_1^2}$. Therefore,

$$\lambda t = \frac{t^2}{4cA_1^2}, \quad A_1^2\lambda^2 = \frac{t^2}{(4c)^2 A_1^2} \quad \text{and} \quad B_\alpha^\beta\lambda^\beta = \frac{t^2}{(4c)^\beta A_1^2}\frac{t^{\beta-2}B_\alpha^\beta}{A_1^{2(\beta-1)}} \leq \frac{t^2}{(4c)^2 A_1^2}.$$

We conclude from (1.7) that

$$\mathbb{P}(Z \geq t) \leq \exp\left(-\frac{1}{8c}\frac{t^2}{A_1^2}\right).$$

The proof is complete with $C = 1/8c = 1/32(e-1)$.

In the case $\alpha > 2$, we have $1 < \beta < 2$ and the estimate (1.6) for the Laplace transform of the X_i's has to be replaced by

$$\forall\,\lambda > 0,\ \mathbb{E}\exp\lambda X_i \leq \exp\left(c\lambda^2\|X_i\|_{\psi_\alpha}^2\right) \text{ and } \mathbb{E}\exp\lambda X_i \leq \exp\left(c\lambda^\beta\|X_i\|_{\psi_\alpha}^\beta\right) \tag{1.8}$$

where $c = 4(e-1)$. We study two separate cases.
If $\lambda \|X_i\|_{\psi_1} \le 1/2$ then $(\lambda \|X_i\|_{\psi_1})^2 \le (\lambda \|X_i\|_{\psi_1})^\beta \le (\lambda \|X_i\|_{\psi_\alpha})^\beta$ and from Lemma 1.2.10, we get that if $0 \le \lambda \le 1/(2\|X_i\|_{\psi_1})$,

$$\mathbb{E}\exp \lambda X_i \le \exp\left(c\lambda^2 \|X_i\|_{\psi_1}^2\right) \le \exp\left(c\lambda^\beta \|X_i\|_{\psi_\alpha}^\beta\right).$$

In the second case, we start with Young's inequality: for every $\lambda \ge 0$,

$$\lambda X_i \le \frac{1}{\beta}\lambda^\beta \|X_i\|_{\psi_\alpha}^\beta + \frac{1}{\alpha}\frac{|X_i|^\alpha}{\|X_i\|_{\psi_\alpha}^\alpha}$$

which implies by convexity of the exponential and integration that for every $\lambda \ge 0$,

$$\mathbb{E}\exp \lambda X_i \le \frac{1}{\beta}\exp\left(\lambda^\beta \|X_i\|_{\psi_\alpha}^\beta\right) + \frac{1}{\alpha}e.$$

Therefore, if $\lambda \ge 1/2\|X_i\|_{\psi_\alpha}$, then $e \le \exp\left(2^\beta\lambda^\beta\|X_i\|_{\psi_\alpha}^\beta\right) \le \exp\left(2^2\lambda^2\|X_i\|_{\psi_\alpha}^2\right)$ since $\beta < 2$ and we get that if $\lambda \ge 1/(2\|X_i\|_{\psi_\alpha})$

$$\mathbb{E}\exp \lambda X_i \le \exp\left(2^\beta\lambda^\beta\|X_i\|_{\psi_\alpha}^\beta\right) \le \exp\left(2^2\lambda^2\|X_i\|_{\psi_\alpha}^2\right).$$

Since $\|X_i\|_{\psi_1} \le \|X_i\|_{\psi_\alpha}$ and $2^\beta \le 4$, we glue both estimates and get (1.8). We conclude as before that for $Z = \sum_{i=1}^n X_i$, for every $\lambda > 0$,

$$\mathbb{E}\exp \lambda Z \le \exp\left(c \min\left(A_\alpha^2\lambda^2, B_\alpha^\beta\lambda^\beta\right)\right).$$

The end of the proof is identical to the preceding case. □

1.3. A geometric application: the Johnson-Lindenstrauss lemma

The Johnson-Lindenstrauss lemma [**JL84**] states that a finite number of points in a high-dimensional space can be embedded into a space of much lower dimension (which depends of the cardinality of the set) in such a way that distances between the points are nearly preserved. The mapping which is used for this embedding is a linear map and can even be chosen to be an orthogonal projection. We present here an approach with random Gaussian matrices.

Let $G_1, \dots, G_k$ be independent Gaussian vectors in $\mathbb{R}^n$ distributed according to the normal law $\mathcal{N}(0, \mathrm{I}d)$. Let $\Gamma : \mathbb{R}^n \to \mathbb{R}^k$ be the random operator defined for every $x \in \mathbb{R}^n$ by

$$\Gamma x = \begin{pmatrix} \langle G_1, x\rangle \\ \vdots \\ \langle G_k, x\rangle \end{pmatrix} \in \mathbb{R}^k. \tag{1.9}$$

We will prove that with high probability, this random matrix satisfies the desired property in the Johnson-Lindenstrauss lemma.

***Lemma 1.3.1* (Johnson-Lindenstrauss lemma).** — *There exists a numerical constant C such that, given $0 < \varepsilon < 1$, a set T of N distinct points in $\mathbb{R}^n$ and an* *integer $k > k_0 = C\log(N)/\varepsilon^2$, there exists a linear operator $A : \mathbb{R}^n \to \mathbb{R}^k$ such that for every $x, y \in T$,*

$$\sqrt{1-\varepsilon}\ |x-y|_2 \le |A(x-y)|_2 \le \sqrt{1+\varepsilon}\ |x-y|_2.$$

Proof. — Let Γ be as in (1.9). For $z \in \mathbb{R}^n$ and $i = 1, \dots, k$, we have $\mathbb{E}\langle G_i, z\rangle^2 = |z|_2^2$. Therefore, for every $x, y \in T$,

$$\left|\frac{\Gamma(x-y)}{\sqrt{k}}\right|_2^2 - |x-y|_2^2 = \frac{1}{k}\sum_{i=1}^k \langle G_i, x-y\rangle^2 - \mathbb{E}\langle G_i, x-y\rangle^2.$$

Define $X_i = \langle G_i, x-y\rangle^2 - \mathbb{E}\langle G_i, x-y\rangle^2$ for every $i = 1, \dots, k$. It is a centered random variable. Since $e^u \ge 1 + u$, we know that $\mathbb{E}\langle G_i, x-y\rangle^2 \le (e-1)\left\|\langle G_i, x-y\rangle^2\right\|_{\psi_1}$. Hence by definition of the ψ_2 norm,

$$\|X_i\|_{\psi_1} \le 2(e-1)\left\|\langle G_i, x-y\rangle^2\right\|_{\psi_1} = 2(e-1)\,\|\langle G_i, x-y\rangle\|_{\psi_2}^2. \tag{1.10}$$

By definition of the Gaussian law, $\langle G_i, x-y\rangle$ is distributed like $|x-y|_2\, g$ where g is a standard real Gaussian variable. With our definition of the ψ_2 norm, $\|g\|_{\psi_2}^2 = 2e^2/(e^2-1)$. We call c_0^2 this number and set $c_1^2 = 2(e-1)c_0^2$. We conclude that $\|\langle G_i, x-y\rangle\|_{\psi_2}^2 = c_0^2\,|x-y|_2^2$ and $\|X_i\|_{\psi_1} \le c_1^2\,|x-y|_2^2$. We apply Theorem 1.2.7 together with $M_1 = \sigma_1 \le c_1^2\,|x-y|_2^2$ and get for $t = \varepsilon|x-y|_2^2$ and $0 < \varepsilon < 1$,

$$\mathbb{P}\left(\left|\frac{1}{k}\sum_{i=1}^k \langle G_i, x-y\rangle^2 - \mathbb{E}\langle G_i, x-y\rangle^2\right| > \varepsilon|x-y|_2^2\right) \le 2\exp(-c'\,k\,\varepsilon^2)$$

since $t \le |x-y|_2^2 \le c_1^2\,|x-y|_2^2 \le \sigma_1^2/M_1$. The constant c' is defined by $c' = c/c_1^4$ where c comes from Theorem 1.2.7. Since the cardinality of the set $\{(x,y) : x \in T, y \in T\}$ is less than N^2, we get by the union bound that

$$\mathbb{P}\left(\exists\, x, y \in T : \left|\left|\frac{\Gamma(x-y)}{\sqrt{k}}\right|_2^2 - |x-y|_2^2\right| > \varepsilon|x-y|_2^2\right) \le 2\,N^2\exp(-c'\,k\,\varepsilon^2)$$

and if $k > k_0 = \log(N^2)/c'\varepsilon^2$ then the probability of this event is strictly less than one. This means that there exists some realization of the matrix $\Gamma/\sqrt{k}$ that defines A and that satisfies the contrary i.e.

$$\forall\, x, y \in T,\ \sqrt{1-\varepsilon}\ |x-y|_2 \le |A(x-y)|_2 \le \sqrt{1+\varepsilon}\ |x-y|_2.$$

□

Remark 1.3.2. — *The value of C is less than 1800.*
In fact, the proof uses only the ψ_2 behavior of $\langle G_i, x\rangle$. The Gaussian vectors can be replaced by any copies of an isotropic vector Y with independent entries and bounded ψ_2 norms, like e.g. a random vector with independent Rademacher coordinates. Indeed, by Theorem 1.2.1, $\|\langle Y, x-y\rangle\|_{\psi_2} \le c|x-y|_2$ can be used in place of (1.10). *Then the rest of the proof is identical.*

1.4. Complexity and covering numbers

The study of covering and packing numbers is a wide subject. We present only a few useful estimates.

In approximation theory as well as in compressed sensing and statistics, it is important to measure the complexity of a set. An important tool is the entropy numbers which measure the compactness of a set. Given U and V two closed sets of $\mathbb{R}^n$, we define the covering number $N(U,V)$ to be the minimum number of translates of V needed to cover U. The formal definition is

$$N(U,V) = \inf \left\{ N : \exists x_1, \dots, x_N \in \mathbb{R}^n, U \subset \bigcup_{i=1}^{N} (x_i + V) \right\}.$$

If moreover V is a symmetric closed convex set (we always mean symmetric with respect to the origin), the packing number $M(U,V)$ is the maximal number of points in U that are 1-separated for the norm induced by V. Formally, for every closed sets $U, V \subset \mathbb{R}^n$,

$$M(U,V) = \sup \left\{ N : \exists x_1, \dots, x_N \in U, \forall i \neq j, x_i - x_j \notin V \right\}.$$

If V is a symmetric closed convex set, the semi-norm associated to V is defined for $x \in \mathbb{R}^n$ by

$$\|x\|_V = \inf\{t > 0, x \in tV\}.$$

Hence $x_i - x_j \notin V$ is equivalent to $\|x_i - x_j\|_V > 1$. For any $\varepsilon > 0$, we also use the notation

$$N(U, \varepsilon, \|\cdot\|_V) = N(U, \varepsilon V).$$

Moreover, a family $x_1, \dots, x_N$ is called an *ε-net* if it is such that $U \subset \bigcup_{i=1}^{N} (x_i + \varepsilon V)$.

Finally, if the polar of V is defined by

$$V^o = \{y \in \mathbb{R}^n : \forall x \in V, \langle x, y \rangle \leq 1\}$$

then the dual space of the normed vector space $(\mathbb{R}^n, \|\cdot\|_V)$ is isometric to $(\mathbb{R}^n, \|\cdot\|_{V^o})$.

In the case where V is a symmetric closed convex set, the notions of packing and covering numbers are closely related.

Proposition 1.4.1. — *If $U, V \subset \mathbb{R}^n$ are closed and $0 \in V$ then $N(U,V) \leq M(U,V)$. If moreover, U is convex and V convex symmetric then $M(U,V) \leq N(U, V/2)$.*

Proof. — Let $N = M(U,V)$ and $x_1, \dots, x_N$ be in U such that for every $i \neq j$, $x_i - x_j \notin V$. Let $u \in U \setminus \{x_1, \dots, x_N\}$. Then $\{x_1, \dots, x_N, u\}$ is not 1-separated in V, which means that there exists $i \in \{1, \dots, N\}$ such that $u - x_i \in V$. Consequently, since $0 \in V$, $U \subset \bigcup_{i=1}^{N} (x_i + V)$ and $N(U,V) \leq M(U,V)$.

Let $x_1, \dots, x_M$ be a family of vectors of U that are 1-separated. Let $z_1, \dots, z_N$ be a family of vectors such that $U \subset \bigcup_{i=1}^{N} (z_i + V/2)$. Since for $i = 1, \dots, M$, $x_i \in U$, we define a mapping $j : \{1, \dots, M\} \to \{1, \dots, N\}$ where $j(i)$ is such that $x_i \in z_{j(i)} + V/2$. If $j(i_1) = j(i_2)$ then $x_{i_1} - x_{i_2} \in V/2 - V/2$. By convexity and symmetry of V, $V/2 - V/2 = V$. Hence $x_{i_1} - x_{i_2} \in V$. But the family $x_1, \dots, x_M$ is 1-separated in

V and necessarily $i_1 = i_2$. Therefore, j is injective and this implies that $M(U, V) \leq N(U, V/2)$. □

Moreover, it is not difficult to check that for any U, V, W closed convex bodies, one has $N(U, W) \leq N(U, V)N(V, W)$. The following simple volumetric estimate is an important tool.

Lemma 1.4.2. — *Let V be a symmetric compact convex set in $\mathbb{R}^n$. Then, for every $\varepsilon > 0$,*

$$N(V, \varepsilon V) \leq \left(1 + \frac{2}{\varepsilon}\right)^n.$$

Proof. — By Proposition 1.4.1, $N(V, \varepsilon V) \leq M(V, \varepsilon V)$. Let $M = M(V, \varepsilon V)$ be the maximal number of points $x_1, \ldots, x_M$ in V such that for every $i \neq j$, $x_i - x_j \notin \varepsilon V$. Since V is a symmetric compact convex set, the sets $x_i + \varepsilon V/2$ are pairwise disjoints and

$$\bigcup_{i=1}^{M} (x_i + \varepsilon V/2) \subset V + \varepsilon V/2 = \left(1 + \frac{\varepsilon}{2}\right) V.$$

Taking the volume, we get

$$M \left(\frac{\varepsilon}{2}\right)^n \leq \left(1 + \frac{\varepsilon}{2}\right)^n$$

which gives the desired estimate. □

We present some classical tools to estimate the covering numbers of the unit ball of ℓ_1^n by parallelepipeds and some classical estimates relating covering numbers of T by a multiple of the Euclidean ball with a parameter of complexity associated to T.

The empirical method. — We introduce this method through a concrete example. Let d be a positive integer and Φ be an $d \times d$ matrix. We assume that the entries of Φ satisfy for all $i, j \in \{1, \ldots, d\}$,

$$|\Phi_{ij}| \leqslant \frac{K}{\sqrt{d}} \tag{1.11}$$

where $K > 0$ is an absolute constant.

We denote by $\Phi_1, \ldots, \Phi_d$ the row vectors of Φ and we define for all $p \in \{1, \ldots, d\}$ the semi-norm $\|\cdot\|_{\infty,p}$, for $x \in \mathbb{R}^d$, by

$$\|x\|_{\infty,p} = \max_{1 \leqslant j \leqslant p} |\langle \Phi_j, x \rangle|.$$

Let $B_{\infty,p} = \{x \in \mathbb{R}^d : \|x\|_{\infty,p} \leqslant 1\}$ denote its unit ball. If $E = \operatorname{span}\{\Phi_1, \ldots, \Phi_p\}$ and P_E is the orthogonal projection on E, then $B_{\infty,p} = P_E B_{\infty,p} + E^{\perp}$, moreover, $P_E B_{\infty,p}$ is a parallelepiped in E. In the next theorem, we obtain an upper bound of the logarithm of the covering numbers of the unit ball of ℓ_1^d, denoted by B_1^d, by a multiple of $B_{\infty,p}$. Observe first that from hypothesis (1.11) on the entries of the matrix Φ, we get that for any $x \in B_1^d$ and any $j = 1, \ldots, p$, $|\langle \Phi_j, x \rangle| \leq |\Phi_j|_\infty |x|_1 \leq K/\sqrt{d}$. Therefore

$$B_1^d \subset \frac{K}{\sqrt{d}} B_{\infty,p} \tag{1.12}$$

and for $\varepsilon \geq K/\sqrt{d}$, $N(B_1^d, \varepsilon B_{\infty,p}) = 1$.

Theorem 1.4.3. — *With the preceding notations, we have for* $0 < t < 1$,

$$\log N\left(B_1^d, \frac{tK}{\sqrt{d}} B_{\infty,p}\right) \leqslant \min\left\{c_0 \frac{\log(p)\log(2d+1)}{t^2},\ p\log\left(1+\frac{2}{t}\right)\right\}$$

where c_0 *is an absolute constant.*

The first estimate is proven using an empirical method, while the second one is based on a volumetric estimate.

Proof. — Let x be in B_1^d. Define a random variable Z by

$$\mathbb{P}\big(Z = \mathrm{Sign}(x_i)e_i\big) = |x_i| \text{ for all } i = 1, \dots, d \text{ and } \mathbb{P}(Z = 0) = 1 - |x|_1$$

where $(e_1, \dots, e_d)$ is the canonical basis of $\mathbb{R}^d$. Observe that $\mathbb{E}Z = x$.

We use a well known symmetrization argument, see Chapter 5 for a more complete description. Let m be some integer to be chosen later and $Z_1, \dots, Z_m, Z'_1, \dots, Z'_m$ be i.i.d. copies of Z. We have by Jensen's inequality

$$\mathbb{E}\left\|x - \frac{1}{m}\sum_{i=1}^m Z_i\right\|_{\infty,p} = \left\|\frac{1}{m}\sum_{i=1}^m \mathbb{E}' Z'_i - Z_i\right\|_{\infty,p} \leq \mathbb{E}\mathbb{E}'\left\|\frac{1}{m}\sum_{i=1}^m Z'_i - Z_i\right\|_{\infty,p}.$$

The random variable $(Z'_i - Z_i)$ is symmetric hence and has the same law as $\varepsilon_i(Z'_i - Z_i)$ where $\varepsilon_1, \dots, \varepsilon_m$ are i.i.d. Rademacher random variables. Therefore, by the triangle inequality

$$\mathbb{E}\mathbb{E}'\left\|\frac{1}{m}\sum_{i=1}^m Z'_i - Z_i\right\|_{\infty,p} = \frac{1}{m}\mathbb{E}\mathbb{E}'\mathbb{E}_\varepsilon\left\|\sum_{i=1}^m \varepsilon_i(Z'_i - Z_i)\right\|_{\infty,p} \leq \frac{2}{m}\mathbb{E}\mathbb{E}_\varepsilon\left\|\sum_{i=1}^m \varepsilon_i Z_i\right\|_{\infty,p}.$$

and

$$\begin{aligned}\mathbb{E}\left\|x - \frac{1}{m}\sum_{i=1}^m Z_i\right\|_{\infty,p} &\leq \frac{2}{m}\mathbb{E}\mathbb{E}_\varepsilon\left\|\sum_{i=1}^m \varepsilon_i Z_i\right\|_{\infty,p} \\ &= \frac{2}{m}\mathbb{E}\mathbb{E}_\varepsilon \max_{1\leq j\leq p}\left|\sum_{i=1}^m \varepsilon_i\langle Z_i, \Phi_j\rangle\right|. \qquad (1.13)\end{aligned}$$

By definition of Z and (1.11), we know that $|\langle Z_i, \Phi_j\rangle| \leq K/\sqrt{d}$. Let a_{ij} be any sequence of real numbers such that $|a_{ij}| \leq K/\sqrt{d}$. For any j, let $X_j = \sum_{i=1}^m a_{ij}\varepsilon_i$. From Theorem 1.2.1, we deduce that

$$\forall j = 1, \dots, p,\ \|X_j\|_{\psi_2} \leq c\left(\sum_{i=1}^m a_{ij}^2\right)^{1/2} \leq c\frac{K\sqrt{m}}{\sqrt{d}}.$$

Therefore, by Proposition 1.1.3 and remark 1.1.4, we get

$$\mathbb{E}\max_{1\leq j\leq p}|X_j| \leq c\sqrt{(1+\log p)}\ \frac{K\sqrt{m}}{\sqrt{d}}.$$

From (1.13) and the preceding argument, we conclude that

$$\mathbb{E}\left\|x - \frac{1}{m}\sum_{i=1}^{m} Z_i\right\|_{\infty,p} \leq \frac{2\,c\,K\sqrt{(1+\log p)}}{\sqrt{md}}$$

Let m satisfy

$$\frac{4c^2(1+\log p)}{t^2} \leq m \leq \frac{4c^2(1+\log p)}{t^2} + 1$$

For this choice of m we have

$$\mathbb{E}\left\|x - \frac{1}{m}\sum_{i=1}^{m} Z_i\right\|_{\infty,p} \leqslant \frac{tK}{\sqrt{d}}.$$

In particular, there exists $\omega \in \Omega$ such that

$$\left\|x - \frac{1}{m}\sum_{i=1}^{m} Z_i(\omega)\right\|_{\infty,p} \leqslant \frac{tK}{\sqrt{d}}.$$

So the set

$$\left\{\frac{1}{m}\sum_{i=1}^{m} z_i : z_1, \ldots, z_m \in \{\pm e_1, \ldots, \pm e_d\} \cup \{0\}\right\}$$

is a $tK/\sqrt{d}$-net of B_1^d with respect to $\|\cdot\|_{\infty,p}$. Since its cardinality is less than $(2d+1)^m$, we get the first estimate:

$$\log N\left(B_1^d, \frac{tK}{\sqrt{d}}B_{\infty,p}\right) \leqslant \frac{c_0(1+\log p)\log(2d+1)}{t^2}$$

where c_0 is an absolute constant.

To prove the second estimate, we recall that by (1.12) $B_1^d \subset K/\sqrt{d}B_{\infty,p}$. Hence

$$N\left(B_1^d, \frac{tK}{\sqrt{d}}B_{\infty,p}\right) \leq N\left(\frac{K}{\sqrt{d}}B_{\infty,p}, \frac{tK}{\sqrt{d}}B_{\infty,p}\right) = N\left(B_{\infty,p}, tB_{\infty,p}\right).$$

Moreover, we have already observed that $B_{\infty,p} = P_E B_{\infty,p} + E^{\perp}$ which means that

$$N\left(B_{\infty,p}, tB_{\infty,p}\right) = N(V, tV)$$

where $V = P_E B_{\infty,p}$. Since $\dim E \leq p$, we may apply Lemma1.4.2 to conclude that

$$N\left(B_1^d, \frac{tK}{\sqrt{d}}B_{\infty,p}\right) \leq \left(1 + \frac{2}{t}\right)^p.$$

□

Sudakov's inequality and dual Sudakov's inequality. — Among the classical tools to compute covering numbers of a closed set by Euclidean balls, or in the dual situation, covering numbers of a Euclidean ball by translates of a symmetric closed convex set, are the Sudakov and dual Sudakov inequalities. They relate these covering numbers with an important parameter which measures the size of a subset T of $\mathbb{R}^n$, $\ell_*(T)$. Define

$$\ell_*(T) = \mathbb{E} \sup_{t \in T} \langle G, t \rangle$$

where G is a Gaussian vector in $\mathbb{R}^n$ distributed according to the normal law $\mathcal{N}(0, \mathrm{I}d)$. We refer to Chapter 2 and 3 for deeper results involving this parameter. Remark that $\ell_*(T) = \ell_*(\operatorname{conv} T)$ where $\operatorname{conv} T$ denotes the convex hull of T.

Theorem 1.4.4. — *Let T be a closed subset of $\mathbb{R}^N$ and V be a symmetric closed convex set in $\mathbb{R}^N$. Then, the following inequalities hold:*

$$\sup_{\varepsilon > 0} \varepsilon \sqrt{\log N(T, \varepsilon B_2^N)} \leqslant c\, \ell_*(T) \tag{1.14}$$

and

$$\sup_{\varepsilon > 0} \varepsilon \sqrt{\log N(B_2^N, \varepsilon V)} \leqslant c\, \ell_*(V^o). \tag{1.15}$$

The proof of the Sudakov inequality (1.14) is based on comparison properties between Gaussian processes. We recall the Slepian-Fernique comparison lemma without proving it.

Lemma 1.4.5. — *Let $X_1, \ldots, X_M, Y_1, \ldots, Y_M$ be Gaussian random variables such that for $i, j = 1, \ldots, M$*

$$\mathbb{E}|Y_i - Y_j|^2 \leq \mathbb{E}|X_i - X_j|^2$$

then

$$\mathbb{E} \max_{1 \leq k \leq M} Y_k \leq \mathbb{E} \max_{1 \leq k \leq M} X_k.$$

Proof of Theorem 1.4.4. — We start by proving (1.14). Let $x_1, \ldots, x_M$ be M points of T that are ε-separated with respect to the Euclidean norm $|\cdot|_2$. Define for $i = 1, \ldots, M$, the Gaussian variables $X_i = \langle x_i, G \rangle$ where G is a standard Gaussian vector in $\mathbb{R}^N$. We have

$$\mathbb{E}|X_i - X_j|^2 = |x_i - x_j|_2^2 \geq \varepsilon^2 \quad \text{for all } i \neq j.$$

Let $g_1, \ldots, g_M$ be standard independent Gaussian random variables and for $i = 1, \ldots, M$, define $Y_i = \frac{\varepsilon}{\sqrt{2}} g_i$. We have for all $i \neq j$

$$\mathbb{E}|Y_i - Y_j|^2 = \varepsilon^2$$

and by Lemma1.4.5

$$\frac{\varepsilon}{\sqrt{2}} \mathbb{E} \max_{1 \leq k \leq M} g_k \leq \mathbb{E} \max_{1 \leq k \leq M} \langle x_k, G \rangle \leq 2\ell(T).$$

Moreover there exists a constant $c > 0$ such that for every positive integer M

$$\mathbb{E} \max_{1 \leq k \leq M} g_k \geq \sqrt{\log M} / c \tag{1.16}$$

which proves $\varepsilon\sqrt{\log M} \leq c\sqrt{2}\ell(T)$. By Proposition 1.4.1, the proof of inequality (1.14) is complete. The lower bound (1.16) is a classical fact. First, we observe that $\mathbb{E}\max(g_1, g_2)$ is computable, it is equal to $1/\sqrt{\pi}$. Hence we can assume that M is large enough (say greater than 10^4). In this case, we observe that

$$2\,\mathbb{E}\max_{1\leq k\leq M} g_k \geq \mathbb{E}\max_{1\leq k\leq M}|g_k| - \mathbb{E}|g_1|.$$

Indeed,

$$\mathbb{E}\max_{1\leq k\leq M} g_k = \mathbb{E}\max_{1\leq k\leq M}(g_k - g_1) = \mathbb{E}\max_{1\leq k\leq M}\max((g_k - g_1), 0)$$

and by symmetry of the g_i's,

$$\begin{aligned}\mathbb{E}\max_{1\leq k\leq M}|g_k - g_1| &\leq \mathbb{E}\max_{1\leq k\leq M}\max((g_k - g_1), 0) + \mathbb{E}\max_{1\leq k\leq M}\max((g_1 - g_k), 0)\\ &= 2\,\mathbb{E}\max_{1\leq k\leq M}(g_k - g_1) = 2\mathbb{E}\max_{1\leq k\leq M} g_k.\end{aligned}$$

But, by independence of the g_i's

$$\begin{aligned}\mathbb{E}\max_{1\leq k\leq M}|g_k| &= \int_0^{+\infty}\mathbb{P}\left(\max_{1\leq k\leq M}|g_k| > t\right)dt = \int_0^{+\infty}\left(1 - \mathbb{P}\left(\max_{1\leq k\leq M}|g_k| \leq t\right)\right)dt\\ &= \int_0^{+\infty}\left(1 - \left(1 - \sqrt{\frac{2}{\pi}}\int_t^{+\infty} e^{-u^2/2}du\right)^M\right)dt\end{aligned}$$

and it is easy to see that for every $t > 0$,

$$\int_t^{+\infty} e^{-u^2/2}du \geq e^{-(t+1)^2/2}.$$

Let $t_0 + 1 = \sqrt{2\log M}$ then

$$\begin{aligned}\mathbb{E}\max_{1\leq k\leq M}|g_k| &\geq \int_0^{t_0}\left(1 - \left(1 - \sqrt{\frac{2}{\pi}}\int_t^{+\infty} e^{-u^2/2}du\right)^M\right)dt\\ &\geq t_0\left(1 - \left(1 - \frac{\sqrt{2}}{M\sqrt{\pi}}\right)^M\right) \geq t_0(1 - e^{-\sqrt{2/\pi}})\end{aligned}$$

which concludes the proof of (1.16).

To prove the dual Sudakov inequality (1.15), the argument is very similar to the volumetric argument introduced in Lemma 1.4.2, replacing the Lebesgue measure by the Gaussian measure. Let $r > 0$ to be chosen later. By definition, $N(B_2^N, \varepsilon V) = N(rB_2^N, r\varepsilon V)$. Let $x_1, \ldots, x_M$ be in rB_2^N that are $r\varepsilon$ separated for the norm induced by the symmetric convex set V. By Proposition 1.4.1, it is enough to prove that

$$\varepsilon\sqrt{\log M} \leq c\,\ell_*(V^o).$$

The balls $x_i + (r\varepsilon/2)V$ are disjoints and taking the Gaussian measure of the union of these sets, we get

$$\gamma_N\left(\bigcup_{i=1}^{M}(x_i + r\varepsilon/2\,V)\right) = \sum_{i=1}^{M}\int_{\|z-x_i\|_V\le r\varepsilon/2} e^{-|z|_2^2/2}\frac{dz}{(2\pi)^{N/2}} \le 1.$$

However, by the change of variable $z - x_i = u_i$, we have

$$\int_{\|z-x_i\|_V\le r\varepsilon/2} e^{-|z|_2^2/2}\frac{dz}{(2\pi)^{N/2}} = e^{-|x_i|_2^2/2}\int_{\|u_i\|_V\le r\varepsilon/2} e^{-|u_i|_2^2/2}e^{-\langle u_i,x_i\rangle}\frac{du_i}{(2\pi)^{N/2}}$$

and from Jensen's inequality and the symmetry of V,

$$\frac{1}{\gamma_N\left(\frac{r\varepsilon}{2}V\right)}\int_{\|z-x_i\|_V\le r\varepsilon/2} e^{-|z|_2^2/2}\frac{dz}{(2\pi)^{N/2}} \ge e^{-|x_i|_2^2/2}.$$

Since $x_i \in rB_2^N$, we proved

$$M\,e^{-r^2/2}\,\gamma_N\left(\frac{r\varepsilon}{2}V\right) \le 1.$$

To conclude, we choose r such that $r\varepsilon/2 = 2\ell_*(V^o)$. By Markov inequality, $\gamma_N\left(\frac{r\varepsilon}{2}V\right) \ge 1/2$ and $M \le 2e^{r^2/2}$ which means that for some constant c,

$$\varepsilon\sqrt{\log M} \le c\,\ell_*(V^o).$$

□

The metric entropy of the Schatten balls. — As a first application of Sudakov and dual Sudakov, we compute the metric entropy of Schatten balls with respect to Schatten norms. We denote by $B_p^{m,n}$ the unit ball of the Banach spaces of matrices in $\mathcal{M}_{m,n}$ endowed with the Schatten norm $\|\cdot\|_{S_p}$ defined for any $A \in \mathcal{M}_{m,n}$ by

$$\|A\|_{S_p} = \Big(\mathrm{Tr}\big((A^*A)^{p/2}\big)\Big)^{1/p}.$$

It is also the ℓ_p-norm of the singular values of A. We refer to Chapter 4 for more information about the singular values of a matrix.

Proposition 1.4.6. — *For $m \ge n \geqslant 1$, $p, q \in [1, +\infty]$ and $\varepsilon > 0$, one has*

$$\varepsilon\sqrt{\log N(B_p^{m,n}, \varepsilon B_2^{m,n})} \leqslant c_1\sqrt{m}\;n^{(1-1/p)} \tag{1.17}$$

and

$$\varepsilon\sqrt{\log N(B_2^{m,n}, \varepsilon B_q^{m,n})} \leqslant c_2\sqrt{m}\;n^{1/q} \tag{1.18}$$

where c_1 and c_2 are numerical constants. Moreover, for $n \ge m \ge 1$ the same result holds by exchanging m and n.

Proof. — We start by proving a rough upper bound of the operator norm of a Gaussian random matrix $\Gamma \in \mathcal{M}_{m,n}$ i.e. a matrix with independent standard Gaussian entries:

$$\mathbb{E}\,\|\Gamma\|_{S_\infty} \le c(\sqrt{n} + \sqrt{m}) \tag{1.19}$$

for some numerical constant c. Let $X_{u,v}$ be the Gaussian process defined for $u \in B_2^m, v \in B_2^n$ by

$$X_{u,v} = \langle \Gamma v, u \rangle$$

so

$$\mathbb{E} \|\Gamma\|_{S_\infty} = \mathbb{E} \sup_{u \in B_2^m, v \in B_2^n} X_{u,v}.$$

From Lemma 1.4.2, there exists $(1/4)$-nets $\Lambda \subset B_2^m$ and $\Lambda' \subset B_2^n$ of B_2^m and B_2^n for their own metric such that $|\Lambda| \leqslant 9^m$ and $|\Lambda'| \leqslant 9^n$. Let $(u,v) \in B_2^m \times B_2^n$ and $(u',v') \in \Lambda \times \Lambda'$ such that $|u-u'|_2 < 1/4$ and $|v-v'|_2 < 1/4$. Then we have

$$|X_{u,v} - X_{u',v'}| = |\langle \Gamma v, u-u' \rangle + \langle \Gamma(v-v'), u' \rangle| \le \|\Gamma\|_{S_\infty} |u-u'|_2 + \|\Gamma\|_{S_\infty} |v-v'|_2.$$

We deduce that $\|\Gamma\|_{S_\infty} \leqslant \sup_{u' \in \Lambda, v' \in \Lambda'} |X_{u',v'}| + (1/2) \|\Gamma\|_{S_\infty}$ and therefore

$$\|\Gamma\|_{S_\infty} \leqslant 2 \sup_{u' \in \Lambda, v' \in \Lambda'} |X_{u',v'}|.$$

Now $X_{u',v'}$ is a Gaussian centered random variable with variance $|u'|_2^2 \, |v'|_2^2 \leqslant 1$. By Lemma 1.1.3,

$$\mathbb{E} \sup_{u' \in \Lambda, v' \in \Lambda'} |X_{u',v'}| \leqslant c\sqrt{\log |\Lambda||\Lambda'|} \le c\sqrt{\log 9}\,(\sqrt{m} + \sqrt{n})$$

and (1.19) follows.

Now, we first prove (1.17) when $m \ge n \ge 1$. Using Sudakov inequality (1.14), we have for all $\varepsilon > 0$,

$$\varepsilon \sqrt{\log N(B_p^{m,n}, \varepsilon B_2^{m,n})} \leqslant c\ell_*(B_p^{m,n}).$$

Since

$$\ell_*(B_p^{m,n}) = \mathbb{E} \sup_{A \in B_p^{m,n}} \langle \Gamma, A \rangle$$

where $\langle \Gamma, A \rangle = \mathrm{Tr}(\Gamma\, A^*)$. If p' satisfies $1/p + 1/p' = 1$, we have by trace duality

$$\langle \Gamma, A \rangle \le \|\Gamma\|_{S_{p'}} \|A\|_{S_p} \leqslant n^{1/p'} \|\Gamma\|_{S_\infty} \|A\|_{S_p}.$$

Taking the supremum over $A \in B_p^{m,n}$, the expectation and using (1.19), we get

$$\ell_*(B_p^{m,n}) \le n^{1/p'} \mathbb{E} \|\Gamma\|_{S_\infty} \le c\sqrt{m}\; n^{1/p'}$$

which ends the proof of (1.17)

To prove (1.18) in the case $m \ge n \ge 1$, we use the dual Sudakov inequality (1.15) and (1.19) to get that for $q \in [1, +\infty]$:

$$\varepsilon \sqrt{\log N(B_2^{m,n}, \varepsilon B_q^{m,n})} \leqslant c\,\mathbb{E} \|\Gamma\|_{S_q} \leqslant c\, n^{1/q} \mathbb{E} \|\Gamma\|_{S_\infty} \leqslant c' n^{1/q} \sqrt{m}.$$

The proof of the case $n \ge m$ is similar.

□

Concentration of norms of Gaussian vectors. — We finish this chapter by another important property of Gaussian processes, a concentration of measure inequality which will be used in the next chapter. It is stated without proof. The reader is referred to [**Led01**] to learn more about this and to [**Pis89**] for other consequences in geometry of Banach spaces.

Theorem 1.4.7. — *Let $G \in \mathbb{R}^n$ be a Gaussian vector distributed according to the normal law $\mathcal{N}(0, \mathrm{Id})$. Let $T \subset \mathbb{R}^n$ and let*

$$\sigma(T) = \sup_{t \in T} \{ \left(\mathbb{E} \langle G, t \rangle |^2 \right)^{1/2} \}.$$

We have

$$\forall u > 0 \qquad \mathbb{P}\left(\left| \sup_{t \in T} \langle G, t \rangle - \mathbb{E} \sup_{t \in T} \langle G, t \rangle \right| > u \right) \leq 2 \exp\left(-u^2 / 2\sigma^2(T) \right) \tag{1.20}$$

where c is a numerical constant.

1.5. Notes and comments

In this chapter, we focused on some very particular concentration inequalities. Of course, there exist different and powerful other type of concentration inequalities. Several books and surveys are devoted to this subject and we refer for example to [**LT91, vdVW96, Led01, BBL04, Mas07**] for the interested reader. The classical references for Orlicz spaces are [**KR61, LT77, LT79, RR91, RR02**].

Tail and moment estimates for Rademacher averages are well understood. Theorem 1.2.3 is due to Montgomery-Smith [**MS90**] and several extensions to the vector valued case are known [**DMS93, MS95**]. The case of sum of independent random variables with logarithmically concave tails has been studied by Gluskin and Kwapien [**GK95**]. For the proof of Theorem 1.2.8, we could have followed a classical probabilistic trick which reduces the proof of the result to the case of Weibull random variables. These variables are defined such that their tails are equals to e^{-t^α}. Hence, they are logarithmically concave and the conclusion follows from a result of Gluskin and Kwapien in [**GK95**]. We have presented here an approach which follows the line of [**Tal94**]. The results are only written for random variables with densities $c_\alpha e^{-t^\alpha}$, but the proofs work in the general context of ψ_α random variables.

Originally, Lemma 1.3.1 was proved in [**JL84**] and the operator is chosen at random in the set of orthogonal projections onto a random k-dimensional subspace of ℓ_2, uniformly according to the Haar measure on the Grassman manifold $\mathcal{G}_{n,k}$.

The classical references for the study of entropy numbers are [**Pie72, Pie80, Pis89, CS90**]. The method of proof of Theorem 1.4.3 has been introduced by Maurey, in particular for studying entropy numbers of operators from ℓ_1^d into a Banach space of type p. This was published in [**Pis81**]. The method was extended and developed by Carl in [**Car85**]. Sudakov inequality 1.14 is due to Sudakov [**Sud71**] while the dual Sudakov inequality 1.15 is due to Pajor and Tomczak-Jaegermann [**PTJ86**]. The proof that we presented follows the lines of Ledoux-Talagrand [**LT91**]. We have chosen to speak only about Slepian-Fernique inequality which is Lemma 1.4.5. The result of Slepian [**Sle62**] is more general and tells about distribution inequality. In the context of Lemma 1.4.5, however, a multiplicative factor 2 appears when applying Slepian's lemma. Fernique [**Fer74**] proved that the constant 2 can be replaced by 1 and Gordon [**Gor85, Gor87**] extended these results to min-max of some Gaussian processes. About the covering numbers of the Schatten balls, Proposition 1.4.6 is due to Pajor [**Paj99**]. Theorem 1.4.7 is due to Cirel′son, Ibragimov, Sudakov [**CIS76**] (see the book [**Pis89**] and [**Pis86**] for variations on the same theme).

CHAPTER 2

COMPRESSED SENSING AND GELFAND WIDTHS

2.1. A short introduction to compressed sensing

Compressed Sensing is a quite new framework that enables to get exact and approximate reconstruction of sparse or almost sparse signals from incomplete measurements. The ideas and principles are strongly related to other problems coming from different fields such as approximation theory, in particular to the study of Gelfand and Kolmogorov widths of classical Banach spaces (diameter of sections). Since the seventies an important work was done in this direction, in Approximation Theory and in Asymptotic Geometric Analysis (called Geometry of Banach spaces at that time).

It is not in our aim to give a comprehensive and exhaustive presentation of compressed sensing, there are many good references for that, but mainly to emphasize some interactions with other fields of mathematics, in particular with asymptotic geometric analysis, random matrices and empirical processes. The possibility of reconstructing any vector from a given subset is highly related to some *complexity* of this subset and in the field of Geometry of Banach spaces, many tools were developed to analyze various concepts of complexity.

In this introduction to compressive sensing, for simplicity, we will consider only the real case, real vectors and real matrices. Let $1 \leq n \leq N$ be integers. We are given a rectangular $n \times N$ real matrix A. One should think of $N \gg n$. We have in mind to compress some vectors from $\mathbb{R}^N$ for large N into vectors in $\mathbb{R}^n$. Let $X_1, \ldots, X_N \in \mathbb{R}^n$ be the columns of A and let $Y_1, \cdots, Y_n \in \mathbb{R}^N$ its rows. We write

$$A = \begin{pmatrix} X_1 \cdots\cdots\cdots X_N \end{pmatrix} = \begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_n \end{pmatrix}.$$

We are also given a subset $T \subset \mathbb{R}^N$ of vectors. Let $x \in T$ be an *unknown* vector. The data one is given are n linear measurements of x (again, think of $N \gg n$)

$$\langle Y_1, x\rangle, \cdots, \langle Y_n, x\rangle$$

or equivalently

$$y = Ax.$$

We wish to *recover* x or more precisely to *reconstruct* x, exactly or approximately, within a given accuracy and in an efficient way (fast algorithm).

2.2. The exact reconstruction problem

Let us first discuss the exact reconstruction question. Let $x \in T$ be unknown and recall that the given data is $y = Ax$. When $N \gg n$, the problem is *ill-posed* because the system $At = y$, $t \in \mathbb{R}^N$ is highly under-determined. Thus if we want to recover x we need some information on its *nature*. Moreover if we want to recover any x from T, one should have some a priori information on the set T, on its *complexity* whatever it means at this stage. We shall consider here various parameters of complexity in these notes. The a priori hypothesis that we investigate now is *sparsity*.

Sparsity. — We first introduce some notation. We equip $\mathbb{R}^n$ and $\mathbb{R}^N$ with the canonical scalar product $\langle \cdot, \cdot \rangle$ and Euclidean norm $|\cdot|_2$. We use the notation $|\cdot|$ to denote the cardinality of a set. By B_2^N we denote the unit Euclidean ball of $\mathbb{R}^N$ and by S^{N-1} its unit sphere.

Definition 2.2.1. — *Let $0 \le m \le N$ be integers. For $x = (x_1, \dots, x_N) \in \mathbb{R}^N$, denote by* $\operatorname{supp} x = \{k : 1 \le k \le N, x_k \neq 0\}$ *the support of x, that is the set of indices of non-zero coordinates of x. A vector x is said to be m-sparse if $|\operatorname{supp} x| \le m$. The set of m-sparse vectors of $\mathbb{R}^N$ is denoted by $\Sigma_m = \Sigma_m(\mathbb{R}^N)$ and its unit sphere by*

$$S_2(\Sigma_m) = \{x \in \mathbb{R}^N : |x|_2 = 1 \text{ and } |\operatorname{supp} x| \le m\} = \Sigma_m(\mathbb{R}^N) \cap S^{N-1}.$$

Similarly let

$$B_2(\Sigma_m) = \{x \in \mathbb{R}^N : |x|_2 \le 1 \text{ and } |\operatorname{supp} x| \le m\} = \Sigma_m(\mathbb{R}^N) \cap B_2^N.$$

Note that Σ_m is not a linear subspace and that $B_2(\Sigma_m)$ is not convex (except when $m = N$).

Problem 2.2.2. — **The exact reconstruction problem.** *We wish to reconstruct exactly any m-sparse vector $x \in \Sigma_m$ from the given data $y = Ax$. Thus we are looking for a* decoder Δ *such that*

$$\forall x \in \Sigma_m, \qquad \Delta(A, Ax) = x.$$

Claim 2.2.3. — *Linear algebra tells us that such a decoder Δ exists iff*

$$\ker A \cap \Sigma_{2m} = \{0\}.$$

Example 2.2.4. — *Let $m \ge 1$, $N \ge 2m$ and $0 < a_1 < \cdots < a_N = 1$. Let $n = 2m$ and build the Vandermonde matrix $A = (a_j^{i-1}), 1 \le i \le n, 1 \le j \le N$. Clearly all the $2m \times 2m$ minors of A are non singular Vandermonde matrices. Unfortunately it is known that such matrices are ill-conditioned. Therefore reconstructing $x \in \Sigma_m$ from $y = Ax$ is numerically unstable.*

Metric entropy. — As already said, there are many different approaches to seize and measure complexity of a metric space. The most simple is probably to estimate a degree of compactness via the so-called covering and packing numbers.

Since all the metric spaces that we will consider here are subsets of normed spaces, we restrict to this setting. We denote by $\mathrm{conv}(\Lambda)$ the convex hull of a subset Λ of a linear space.

Definition 2.2.5. — *Let B and C be subsets of a vector space and let $\varepsilon > 0$. An ε-net of B by translates of εC is a subset Λ of B such that for every $x \in B$, there exits $y \in \Lambda$ and $z \in C$ such that $x = y + \varepsilon z$. In other words, one has*

$$B \subset \Lambda + \varepsilon C = \bigcup_{y \in \Lambda} (y + \varepsilon C),$$

where $\Lambda + \varepsilon C := \{a + \varepsilon c : a \in \Lambda, c \in C\}$ is the Minkowski sum of the sets Λ and εC. The covering number of B by εC is the smallest cardinality of such an ε-net and is denoted by $N(B, \varepsilon C)$. The function $\varepsilon \to \log N(B, \varepsilon C)$ is called the metric entropy of B by C.

Remark 2.2.6. — *If (B, d) is a metric space, an ε-net of (B, d) is a covering of B by balls of radius ε for the metric d. The covering number is the smallest cardinality of an ε-net and is denoted by $N(B, d, \varepsilon)$. In our setting, the metric d will be defined by a norm with unit ball say C. Then $x + \varepsilon C$ is the ball of radius ε centered at x.*

Let us start with an easy but important fact. A subset $C \subset \mathbb{R}^N$, is said to be symmetric or centrally symmetric, if it is symmetric with respect to the origin, that is if $C = -C$. Let $C \subset \mathbb{R}^N$ be a *symmetric convex body*, that is a symmetric convex compact subset of $\mathbb{R}^N$ with non-empty interior. Equivalently, C is unit ball of a norm on $\mathbb{R}^N$. Consider a subset $\Lambda \subset C$ of maximal cardinality such that the points of Λ are εC-apart in the sense that:

$$\forall x \neq y, x, y \in \Lambda, \text{ one has } x - y \notin \varepsilon C$$

(recall that $C = -C$). It is clear that Λ is an ε-net of C by εC. Moreover the balls

$$(x + (\varepsilon/2)C)_{x \in \Lambda}$$

of radius $(\varepsilon/2)$ centered at the points of Λ are pairwise disjoint and their union is a subset of $(1 + (\varepsilon/2))\,C$ (this is where convexity is involved). Taking volume of this union, we get that $N(C, \varepsilon C) \leq (1 + (2/\varepsilon))^N$. This proves part ii) of the following proposition.

Proposition 2.2.7. — *Let $\varepsilon \in (0, 1)$. Let $C \subset \mathbb{R}^N$ be a symmetric convex body.*

i) *Let $\Lambda \subset C$ be an ε-net of C by translates of εC, then $\Lambda \subset C \subset (1 - \varepsilon)^{-1}\,\mathrm{conv}\,(\Lambda)$.*

ii) *There exists an ε-net Λ of C by translates of εC such that $|\Lambda| \leq (1 + 2/\varepsilon)^N$.*

Proof. — We prove i) by successive approximation. Since Λ is an ε-net of C by translates of εC, every $z \in C$ can be written as $z = x_0 + \varepsilon z_1$, where $x_0 \in \Lambda$ and $z_1 \in C$. Iterating, it follows that $z = x_0 + \varepsilon x_1 + \varepsilon^2 x_2 + \ldots$, with $x_i \in \Lambda$, which implies by convexity that $C \subset (1 - \varepsilon)^{-1}\mathrm{conv}\,(\Lambda)$. □

This gives the next result:

Claim 2.2.8. — *Covering the unit Euclidean sphere by Euclidean balls of radius ε. One has*

$$\forall \varepsilon \in (0,1), \qquad N(S^{N-1}, \varepsilon B_2^N) \leq \left(\frac{3}{\varepsilon}\right)^N.$$

Now, since $S_2(\Sigma_m)$ is the union of spheres of dimension m,

$$N(S_2(\Sigma_m), \varepsilon B_2^N) \leq \binom{N}{m} N(S^{m-1}, \varepsilon B_2^m).$$

Using the well known inequality $\binom{N}{m} \leq (eN/m)^m$, we get:

Claim 2.2.9. — *Covering the set of sparse unit vectors by Euclidean balls of radius ε. Let $1 \leq m \leq N$ and $\varepsilon \in (0,1)$, then*

$$N(S_2(\Sigma_m), \varepsilon B_2^N) \leq \left(\frac{3eN}{m\varepsilon}\right)^m.$$

The ℓ_1-minimization method. — Coming back to the exact reconstruction problem, if we want to solve in t the system

$$At = y$$

where $y = Ax$ is given and x is m-sparse, it is tempting to test all possible supports of the unknown vector x. This is the so-called ℓ_0-method. But there are $\binom{N}{m}$ possible supports, too many to answer the request of a fast algorithm. A more clever approach was proposed, namely the convex relaxation of the ℓ_0-method. Let x be the unknown vector. The given data is $y = Ax$. For $t = (t_i) \in \mathbb{R}^N$ denote by

$$|t|_1 = \sum_{i=1}^{N} |t_i|$$

its ℓ_1 norm. The ℓ_1-minimization method (also called *basis pursuit*) is the following program:

$$(P) \qquad \min_{t \in \mathbb{R}^N} |t|_1 \quad \text{subject to} \quad At = y.$$

This program may be recast as a linear programming by

$$\min \sum_{i=1}^{N} s_i, \ \text{subject to } s \geq 0, -s \leq t \leq s, At = y.$$

Definition 2.2.10. — **Exact reconstruction by ℓ_1-minimization.** *We say that a $n \times N$ matrix A has the exact reconstruction property of order m by ℓ_1-minimization if, for every $x \in \Sigma_m$, the problem*

$$(P) \ \min_{t \in \mathbb{R}^N} |t|_1 \quad \textit{subject to} \quad At = Ax \ \textit{has a unique solution equal to } x. \qquad (2.1)$$

Note that the above property is not specific to the matrix A but rather a property of its null space. In order to emphasize this point, let us introduce some notation.

For any subset $I \subset [N]$ where $[N] = \{1, \ldots, N\}$, let I^c be its complement. For any $x \in \mathbb{R}^N$, let us write x_I for the vector in $\mathbb{R}^N$ with the same coordinates as x for indices in I and 0 for indices in I^c. We are ready for a criterion on the null space.

Proposition 2.2.11. — **The null space property.** *Let A be $n \times N$ matrix. The following properties are equivalent*

i) *For any $x \in \Sigma_m$, the problem*

$$(P) \qquad \min_{t \in \mathbb{R}^N} |t|_1 \quad \textit{subject to} \quad At = Ax$$

has a unique solution equal to x (that is A has the exact reconstruction property of order m by ℓ_1-minimization)

ii)

$$\forall h \in \ker A, h \neq 0, \forall I \subset [N], |I| \leq m, \text{ one has } |h_I|_1 < |h_{I^c}|_1. \tag{2.2}$$

Proof. — On one side, let $h \in \ker A, h \neq 0$ and $I \subset [N], |I| \leq m$. Put $x = -h_I$. Then $x \in \Sigma_m$ and (2.1) implies that $|x + h|_1 > |x|_1$, that is $|h_{I^c}|_1 > |h_I|_1$.

For the reverse implication, suppose that ii) holds. Let $x \in \Sigma_m$ and $I = \text{supp}(x)$. Then $|I| \leq m$ and for any $h \in \ker A$ such that $h \neq 0$,

$$|x + h|_1 = |x_I + h_I|_1 + |h_{I^c}|_1 > |x_I + h_I|_1 + |h_I|_1 \geq |x|_1,$$

which shows that x is the unique minimizer of the problem (P). □

Definition 2.2.12. — *Let $1 \leq m \leq N$. We say that an $n \times N$ matrix A satisfies the null space property of order m if it satisfies (2.2).*

This property has a nice geometric interpretation. To introduce it, we need some more notation. Recall that $\text{conv}(\,\cdot\,)$ denotes the convex hull. Let $(e_i)_{1 \leq i \leq N}$ be the canonical basis of $\mathbb{R}^N$. Let ℓ_1^N be the N-dimensional space $\mathbb{R}^N$ equipped with the ℓ_1 norm and B_1^N be its unit ball. Denote also

$$S_1(\Sigma_m) = \{x \in \Sigma_m \,:\, |x|_1 = 1\} \quad \text{and} \quad B_1(\Sigma_m) = \{x \in \Sigma_m \,:\, |x|_1 \leq 1\} = \Sigma_m \cap B_1^N.$$

We have $B_1^N = \text{conv}(\pm e_1, \ldots, \pm e_N)$. A $(m-1)$-dimensional face of B_1^N is of the form $\text{conv}(\{\varepsilon_i e_i \,:\, i \in I\})$ with $I \subset [N], |I| = m$ and $(\varepsilon_i) \in \{-1, 1\}^I$. From the geometric point of view, $S_1(\Sigma_m)$ is the union of the $(m-1)$-dimensional faces of B_1^N.

Let A be an $n \times N$ matrix and $X_1, \ldots, X_N \in \mathbb{R}^n$ be its columns then

$$A(B_1^N) = \text{conv}(\pm X_1, \ldots, \pm X_N).$$

Proposition 2.2.11 can be reformulated in the following geometric language:

Proposition 2.2.13. — **The geometry of faces of $A(B_1^N)$.** *Let $1 \leq m \leq n \leq N$. Let A be an $n \times N$ matrix with columns $X_1, \ldots, X_N \in \mathbb{R}^n$. Then A satisfies the null space property (2.2) if and only if one has*

$$\begin{gathered} \forall I \subset [N],\ 1 \leq |I| \leq m, \forall (\varepsilon_i) \in \{-1, 1\}^I, \\ \text{conv}(\{\varepsilon_i X_i \,:\, i \in I\}) \cap \text{conv}(\{\theta_j X_j \,:\, j \notin I, \theta_j = \pm 1\}) = \emptyset. \end{gathered} \tag{2.3}$$

Proof. — Let $I \subset [N]$, $1 \le |I| \le m$ and $(\varepsilon_i) \in \{-1,1\}^I$. Observe that $y \in \mathrm{conv}(\{\theta_j X_j : j \notin I, \theta_j = \pm 1\})$ iff there exists $(\lambda_j)_{j\in I^c} \in [-1,1]^{I^c}$ such that

$$\sum_{j\in I^c} |\lambda_j| \leqslant 1 \text{ and } y = \sum_{j\in I^c} \lambda_j X_j.$$

Therefore

$$\mathrm{conv}(\{\varepsilon_i X_i \,:\, i \in I\}) \cap \mathrm{conv}(\{\theta_j X_j \,:\, j \notin I, \theta_j = \pm 1\}) \neq \emptyset$$

iff there exist $(\lambda_i)_{i\in I} \in [0,1]^I$ and $(\lambda_j)_{j\in I^c} \in [-1,1]^{I^c}$ such that

$$\sum_{i\in I} \lambda_i = 1 \geqslant \sum_{j\in I^c} |\lambda_j|$$

and

$$h = \sum_{i\in I} \lambda_i \varepsilon_i e_i - \sum_{j\in I^c} \lambda_j e_j \in \ker A.$$

We have $h_i = \lambda_i \varepsilon_i$ for $i \in I$ and $h_j = -\lambda_j$ for $j \notin I$, thus $|h_I|_1 \geqslant |h_{I^c}|_1$. This shows that if (2.3) fails, the null space property (2.2) is not satisfied.

Conversely, assume that (2.2) fails. Thus there exist $I \subset [N]$, $1 \le |I| \le m$ and $h \in \ker A$, $h \neq 0$, such that $|h_I|_1 \geqslant |h_{I^c}|_1$ and since $h \neq 0$, we may assume by homogeneity that $|h_I|_1 = 1$. For every $i \in I$, let $\lambda_i = \varepsilon_i h_i$ where ε_i is the sign of h_i if $h_i \neq 0$ and $\varepsilon_i = 1$ otherwise and set $y = \sum_{i\in I} h_i X_i$. Since $h \in \ker A$, we also have $y = -\sum_{j\in I^c} h_j X_j$. Clearly, $y \in \mathrm{conv}(\{\varepsilon_i X_i \,:\, i \in I\}) \cap \mathrm{conv}(\{\theta_j X_j \,:\, j \notin I, \theta_j = \pm 1\})$ and therefore (2.3) is not satisfied. This concludes the proof. □

Proposition 2.2.14. — *Let $1 \le m \le n \le N$. Let A be an $n \times N$ matrix with columns $X_1, \dots, X_N \in \mathbb{R}^n$. Then A satisfies the null space property (2.2) if and only if one has*

$$\forall I \subset [N],\ 1 \le |I| \le m, \forall (\varepsilon_i) \in \{-1,1\}^I,$$
$$\mathrm{Aff}(\{\varepsilon_i X_i \,:\, i \in I\}) \cap \mathrm{conv}(\{\theta_j X_j \,:\, j \notin I, \theta_j = \pm 1\}) = \emptyset \tag{2.4}$$

where $\mathrm{Aff}(\{\varepsilon_i X_i \,:\, i \in I\})$ *denotes the affine hull of* $\{\varepsilon_i X_i \,:\, i \in I\}$.

Proof. — In view of Proposition 2.2.13, we are left to prove that (2.3) implies (2.4). Assume that (2.4) fails, let $I \subset [N]$, $1 \le |I| \le m$ and $(\varepsilon_i) \in \{-1,1\}^I$. If

$$y \in \mathrm{Aff}(\{\varepsilon_i X_i \,:\, i \in I\}) \cap \mathrm{conv}(\{\theta_j X_j \,:\, j \notin I, \theta_j = \pm 1\}),$$

there exist $(\lambda_i)_{i\in I} \in \mathbb{R}^I$ and $(\lambda_j)_{j\in I^c} \in [-1,1]^{I^c}$ such that $\sum_{i\in I} \lambda_i = 1 \geqslant \sum_{j\in I^c} |\lambda_j|$ and $y = \sum_{i\in I} \lambda_i \varepsilon_i X_i = \sum_{j\in I^c} \lambda_j X_j$. Let

$$I^+ = \{i \in I : \lambda_i > 0\} \quad \text{and} \quad I^- = \{i \in I : \lambda_i \leqslant 0\}.$$

Clearly,

$$y \in \mathrm{conv}(\{\varepsilon_i' X_i \,:\, i \in I\}) \cap \mathrm{conv}(\{\theta_j X_j \,:\, j \notin I, \theta_j = \pm 1\})$$

where $\varepsilon_i' = \varepsilon_i$ for $i \in I^+$ and $\varepsilon_i' = -\varepsilon_i$ for $i \in I^-$. This shows that (2.3) fails. □

Observe that a face of $A(B_1^N) = \mathrm{conv}(\pm X_1, \dots, \pm X_N)$ is a subset of the form $\mathrm{conv}(\{\varepsilon_i X_i : i \in I\})$ for some $I \subset [N]$ and some $(\varepsilon_i) \in \{-1, 1\}^I$, that satisfies

$$\mathrm{Aff}(\{\varepsilon_i X_i : i \in I\}) \cap \mathrm{conv}(\{\theta_j X_j : j \notin I, \theta_j = \pm 1\}) = \emptyset.$$

Note that the dimension of this face may be strictly less than $|I| - 1$ and that in general not every subset $\mathrm{conv}(\{\varepsilon_i X_i : i \in I\})$ is a face of $A(B_1^N)$. The next definition introduces very special polytopes.

Definition 2.2.15. — *Let $1 \le m \le n$. A centrally symmetric polytope $P \subset \mathbb{R}^n$ is said to be centrally symmetric m-neighborly if every set of m of its vertices, containing no antipodal pair, is the set of all vertices of some face of P.*

Note that every centrally symmetric polytope is centrally symmetric 1-neighborly. Neighborliness property becomes non-trivial when $m \geqslant 2$.

Proposition 2.2.16. — *Let $1 \le m \le n \le N$. Let A be an $n \times N$ matrix with columns $X_1, \dots, X_N \in \mathbb{R}^n$. The matrix A has the null space property of order m iff its columns $\pm X_1, \dots, \pm X_N$ are the $2N$ vertices of $A(B_1^N)$ and moreover $A(B_1^N)$ is centrally symmetric m-neighborly.*

Proof. — Proposition 2.2.14 and (2.4) show that if A has the null space property of order m then its columns $\pm X_1, \dots, \pm X_N$ are the $2N$ vertices of $A(B_1^N)$ and $A(B_1^N)$ is centrally symmetric m-neighborly.

Assume conversely that $\pm X_1, \dots, \pm X_N$ are the $2N$ vertices of $A(B_1^N)$ and that $A(B_1^N)$ is centrally symmetric m-neighborly. Let $m > 1$, $I \subset [N], |I| = m$ and $(\varepsilon_i) \in \{-1, 1\}^I$. Then for any $k \in I$, $\varepsilon_k X_k \notin \mathrm{Aff}(\{\varepsilon_i X_i : i \in I \setminus \{k\}\})$, because if not, $\varepsilon_k X_k \in \mathrm{conv}(\{\varepsilon'_i X_i : i \in I \setminus \{k\}\})$ for some $(\varepsilon'_i) \in \{-1, 1\}^I$, which contradicts the hypothesis that $\varepsilon_k X_k$ is a vertex of $\mathrm{conv}(\{\varepsilon'_i X_i : i \in I \setminus \{k\}\} \cup \{\varepsilon_k X_k\})$. We conclude that $\mathrm{conv}(\{\varepsilon_i X_i : i \in I)$ is a face of dimension $m - 1$ so that it is a simplex. This is also valid when $m = 1$ since $\pm X_1, \dots, \pm X_N$ are all vertices. Therefore the faces of $\mathrm{conv}(\{\varepsilon_i X_i : i \in I\})$ are the simplices $\mathrm{conv}(\{\varepsilon_i X_i : i \in J\})$ for $J \subset I$. Since a face of a face is a face, (2.4) is satisfied and Proposition 2.2.14 allows to conclude the proof. □

Let $A : \mathbb{R}^N \to \mathbb{R}^n$. Consider the quotient map

$$Q : \ell_1^N \longrightarrow \ell_1^N / \ker A.$$

If A has rank n, then $\ell_1^N / \ker A$ is n-dimensional. Denote by $\|\cdot\|$ the quotient norm on $\ell_1^N / \ker A$ defined by

$$\|Qx\| = \min_{h \in \ker A} |x + h|_1.$$

Property (2.1) implies that Q is norm preserving on Σ_m. Since $\Sigma_{\lfloor m/2 \rfloor} - \Sigma_{\lfloor m/2 \rfloor} \subset \Sigma_m$, Q is an isometry on $\Sigma_{\lfloor m/2 \rfloor}$ equipped with the ℓ_1 metric. In other words,

$$\forall x, y \in \Sigma_{\lfloor m/2 \rfloor} \quad \|Qx - Qy\| = |x - y|_1.$$

As it is classical in approximation theory, we can take benefit of such an isometric embedding to bound the entropic complexity by comparing the metric entropy of the source space $(\Sigma_{\lfloor m/2\rfloor}, \ell_1^N)$ with the target space, which lives in a much lower dimension.

The following lemma is a well-known fact on packing.

Lemma 2.2.17. — *There exists a family Λ of subsets of $[N]$ each of cardinality $m \leqslant N/2$ such that for every $I, J \in \Lambda, I \neq J, |I \cap J| \leq \lfloor m/2 \rfloor$ and $|\Lambda| \geq \left\lfloor \frac{N}{8em} \right\rfloor^{\lfloor m/2\rfloor}$.*

Proof. — We use successive enumeration of the subsets of cardinality m and exclusion of wrong items. Without loss of generality, assume that $m/2$ is an integer. Pick any subset I_1 of $\{1, ..., N\}$ of cardinality m and throw away all subsets J of $\{1, ..., N\}$ of size m such that the Hamming distance $|I_1 \Delta J| \leq m$, where Δ stands for the symmetric difference. There are at most

$$\sum_{k=m/2}^{m} \binom{m}{k}\binom{N-m}{m-k}$$

such subsets and since $m \leq N/2$ we have

$$\sum_{k=m/2}^{m} \binom{m}{k}\binom{N-m}{m-k} \leq 2^m \max_{m/2 \leq k \leq m} \binom{N-m}{m-k} \leq 2^m \binom{N}{m/2}.$$

Now, select a new subset I_2 of size m from the remaining subsets. Repeating this argument, we obtain a family $\Lambda = \{I_1, I_2, \ldots, I_p\}$, $p = |\Lambda|$, of subsets of cardinality m which are m-separated in the Hamming metric and such that

$$|\Lambda| \geq \left\lfloor \binom{N}{m} \Big/ 2^m \binom{N}{m/2} \right\rfloor .$$

Since for $m \leq N/2$ we have $\left(\frac{N}{m}\right)^m \leq \binom{N}{m} \leq \left(\frac{eN}{m}\right)^m$, we get that

$$|\Lambda| \geq \left\lfloor \frac{(N/m)^m}{2^m (Ne/(m/2))^{(m/2)}} \right\rfloor \geq \left\lfloor \left(\frac{N}{8em}\right)^{m/2} \right\rfloor \geq \left\lfloor \frac{N}{8em} \right\rfloor^{\lfloor m/2 \rfloor}$$

which concludes the proof. □

Let Λ be the family constructed in the previous lemma. For every $I \in \Lambda$, define $x(I) = \frac{1}{m}\sum_{i \in I} e_i$. Then $x(I) \in S_1(\Sigma_m)$ and for every $I, J \in \Lambda, I \neq J$, one has

$$|x(I) - x(J)|_1 = 2\left(1 - \frac{|I \cap J|}{m}\right) \geqslant 2\left(1 - \frac{\lfloor m/2 \rfloor}{m}\right) \geq 1.$$

If the matrix A has the exact reconstruction property of order $2m$, then

$$\forall I, J \in \Lambda\ I \neq J, \quad \|Q(x(I)) - Q(x(J))\| = \|Q(x(I) - x(J))\| = |x(I) - x(J)|_1 \geq 1.$$

On one side $|\Lambda| \geq \left\lfloor C\frac{N}{\lfloor m/2 \rfloor} \right\rfloor^{\lfloor m/2 \rfloor}$, but on the other side, the cardinality of the set $(Q(x(I)))_{I \in \Lambda}$ cannot be too big. Indeed, it is a subset of the unit ball $Q(B_1^N)$ of the quotient space and we already saw that the maximum cardinality of a set of points of a unit ball which are 1-apart is less than 3^n. It follows that

$$\lfloor N/32em \rfloor^{\lfloor m/2 \rfloor} \leq 3^n$$

and the next proposition is thus proved.

Proposition 2.2.18. — *Let $m \geqslant 1$. If the matrix A has the exact reconstruction property of order $2m$ by ℓ_1-minimization, then*

$$m \log(cN/m) \leq Cn.$$

where $C, c > 0$ are universal constants.

Whatever the matrix A is, this proposition gives an upper bound on the size m of sparsity such that any vectors from Σ_m can be exactly reconstructed by the ℓ_1-minimization method.

2.3. The restricted isometry property

So far, we do not know of any "simple" condition in order to check whether a matrix A satisfies the exact reconstruction property (2.1). Let us start with the following definition which plays an important role in compressed sensing.

Definition 2.3.1. — *Let A be an $n \times N$ matrix. For any $0 \leq p \leq N$, the restricted isometry constant of order p of A is the smallest number $\delta_p = \delta_p(A)$ such that*

$$(1 - \delta_p)|x|_2^2 \leq |Ax|_2^2 \leq (1 + \delta_p)|x|_2^2$$

for all p-sparse vectors $x \in \mathbb{R}^N$. Let $\delta \in (0, 1)$. We say that the matrix A satisfies the Restricted Isometry Property of order p with parameter δ, shortly $\mathrm{RIP}_p(\delta)$, if $0 \leqslant \delta_p(A) < \delta$.

The relevance of the Restricted Isometry parameter is revealed in the following result:

Theorem 2.3.2. — *Let $1 \leqslant m \leqslant N/2$. Let A be an $n \times N$ matrix. If*

$$\delta_{2m}(A) < \sqrt{2} - 1,$$

then A satisfies the exact reconstruction property of order m by ℓ_1-minimization.

For simplicity, we shall discuss an other parameter involving a more general concept. The aim is to relax the constraint $\delta_{2m}(A) < \sqrt{2} - 1$ in Theorem 2.3.2 and still get an exact reconstruction property of a certain order by ℓ_1-minimization.

Definition 2.3.3. — *Let $0 \leq p \leq n$ be integers and let A be an $n \times N$ matrix. Define $\alpha_p = \alpha_p(A)$ and $\beta_p = \beta_p(A)$ as the best constants such that*

$$\forall x \in \Sigma_p, \quad \alpha_p|x|_2 \leq |Ax|_2 \leq \beta_p|x|_2.$$

Thus $\beta_p = \max\{|Ax|_2 : x \in \Sigma_p \ |x|_2 = 1\}$ *and* $\alpha_p = \min\{|Ax|_2 : x \in \Sigma_p \ |x|_2 = 1\}$. *Now we define the parameter $\gamma_p = \gamma_p(A)$ by*

$$\gamma_p(A) := \frac{\beta_p(A)}{\alpha_p(A)}.$$

In other words, let $I \subset [N]$ with $|I| = p$. Denote by A^I the $n \times p$ matrix with columns $(X_i)_{i\in I}$ obtained by extracting from A the columns X_i with index $i \in I$. Then α_p is the smallest singular value of A^I among all the block matrices A^I with $|I| = p$, and β_p is the largest. In other words, denoting by $B^\top$ the transposed matrix of a matrix B and $\lambda_{min}((A^I)^\top A^I)$, respectively $\lambda_{max}((A^I)^\top A^I)$, the smallest and largest eigenvalues of $(A^I)^\top A^I$, one has

$$\alpha_p^2 = \alpha_p^2(A) = \min_{I\subset[N],|I|=p} \lambda_{min}((A^I)^\top A^I)$$

whereas

$$\beta_p^2 = \beta_p^2(A) = \max_{I\subset[N],|I|=p} \lambda_{max}((A^I)^\top A^I).$$

Of course, if A satisfies $\mathrm{RIP}_p(\delta)$, one has $\gamma_p(A)^2 \le \frac{1+\delta}{1-\delta}$. The concept of RIP is not homogenous, in the sense that A may satisfy $\mathrm{RIP}_p(\delta)$ but not a multiple of A. One can "rescale" the matrix to satisfy a Restricted Isometry Property. This does not ensure that the new matrix, say A' will satisfy $\delta_{2m}(A') < \sqrt{2} - 1$ and will not allow to conclude to an exact reconstruction from Theorem 2.3.2 (compare with Corollary 2.4.3 in the next section). Also note that the Restricted Isometry Property for A can be written

$$\forall x \in S_2(\Sigma_p) \quad \big||Ax|_2^2 - 1\big| \le \delta$$

expressing a form of concentration property of $|Ax|_2$. Such a property may not be satisfied despite the fact that A does satisfy the exact reconstruction property of order p by ℓ_1-minimization (see Example 2.6.6).

2.4. The geometry of the null space

Let $1 \leqslant m \leqslant p \leqslant N$. Let $h \in \mathbb{R}^N$ and let $\varphi = \varphi_h : [N] \to [N]$ be a one-to-one mapping associated to a non-increasing rearrangement of $(|h_i|)$; in others words $|h_{\varphi(1)}| \ge |h_{\varphi(2)}| \ge \cdots \ge |h_{\varphi(N)}|$. Denote by $I_1 = \varphi_h(\{1, \dots, m\})$ a subset of indices of the largest m coordinates of $(|h_i|)$, then by $I_2 = \varphi_h(\{m + 1, \dots, m + p\})$ a subset of indices of the next p largest coordinates of $(|h_i|)$ and for $k \ge 2$, iterate with $I_{k+1} = \varphi_h(\{m+(k-1)p+1, \dots, m+kp\})$, as long as $m+kp \le N$, in order to partition $[N]$ in subsets of cardinality p, except for the first one I_1, which has cardinality m and the last one, which may have cardinality not greater than p. For $J \subset [N]$ and $h \in \mathbb{R}^N$, let $h_J \in \mathbb{R}^N$ be the vector with the same coordinates as h for indices in J and 0 elsewhere.

Claim 2.4.1. — *Let $h \in \mathbb{R}^N$. Suppose that $1 \leqslant m \leqslant p \leqslant N$ and $N \ge m + p$. With the previous notation, we have*

$$\forall k \ge 2, \quad |h_{I_{k+1}}|_2 \le \frac{1}{\sqrt{p}}\, |h_{I_k}|_1$$

and

$$\sum_{k\ge3} |h_{I_k}|_2 \le \frac{1}{\sqrt{p}}\, |h_{I_1^c}|_1.$$

Proof. — Let $k \geq 2$. We have

$$|h_{I_{k+1}}|_2 \leq \sqrt{|I_{k+1}|}\ \max\{|h_i| : i \in I_{k+1}\}$$

and

$$\max\{|h_i| : i \in I_{k+1}\} \leq \min\{|h_i| : i \in I_k\} \leq |h_{I_k}|_1/|I_k|.$$

We deduce that

$$\forall k \geq 2 \quad |h_{I_{k+1}}|_2 \leq \frac{\sqrt{|I_{k+1}|}}{|I_k|}\ |h_{I_k}|_1.$$

Adding up these inequalities for all $k \geq 2$, for which $\sqrt{|I_{k+1}|}/|I_k| \leqslant 1/\sqrt{p}$, we conclude. □

We are ready for the main result of this section

Theorem 2.4.2. — *Let $1 \leqslant m \leqslant p \leqslant N$ and $N \geq m+p$. Let A be an $n \times N$ matrix. Then*

$$\forall h \in \ker A, h \neq 0, \quad \forall I \subset [N], |I| \leq m, \quad |h_I|_1 < \sqrt{\frac{m}{p}}\ \gamma_{2p}(A)\ |h_{I^c}|_1 \tag{2.5}$$

and $\forall h \in \ker A,\ \forall I \subset [N], |I| \leq m,$

$$|h|_2 \leq \sqrt{\frac{1+\gamma_{2p}^2(A)}{p}}\ |h_{I^c}|_1 \leq \sqrt{\frac{1+\gamma_{2p}^2(A)}{p}}\ |h|_1. \tag{2.6}$$

In particular,

$$\mathrm{rad}\,(\ker A \cap B_1^N) \leq \sqrt{\frac{1+\gamma_{2p}^2(A)}{p}}$$

where $\mathrm{rad}\,(B) = \sup_{x\in B} |x|_2$ *is the radius of* B.

Proof. — Let $h \in \ker A$, $h \neq 0$ and organize the coordinates of h as in the introduction of Section 2.4. By definition of α_{2p} (see 2.3.3), one has

$$|h_{I_1} + h_{I_2}|_2 \leq \frac{1}{\alpha_{2p}}|A(h_{I_1} + h_{I_2})|_2.$$

Since $h \in \ker A$ we obtain

$$|h_{I_1} + h_{I_2}|_2 \leq \frac{1}{\alpha_{2p}}|A(h_{I_1} + h_{I_2} - h)|_2 = \frac{1}{\alpha_{2p}}|A(-\sum_{k\geq 3} h_{I_k})|_2.$$

Then from the definition of β_p and γ_p (2.3.3), using Claim 2.4.1, we get

$$|h_{I_1}|_2 < |h_{I_1} + h_{I_2}|_2 \leq \frac{\beta_p}{\alpha_{2p}} \sum_{k\geq 3} |h_{I_k}|_2 \leq \frac{\gamma_{2p}(A)}{\sqrt{p}}|h_{I_1^c}|_1. \tag{2.7}$$

This first inequality is strict because in case of equality, $h_{I_2} = 0$, which implies $h_{I_1^c} = 0$ and thus from above, $h_{I_1} = 0$, that is $h = 0$. To conclude the proof of (2.5), note that for any subset $I \subset [N], |I| \leq m$, $|h_{I_1^c}|_1 \leq |h_{I^c}|_1$ and $|h_I|_1 \leq |h_{I_1}|_1$.

To prove (2.6), we start from

$$|h|_2^2 = |h - h_{I_1} - h_{I_2}|_2^2 + |h_{I_1} + h_{I_2}|_2^2$$

Using Claim 2.4.1, the first term satisfies

$$|h - h_{I_1} - h_{I_2}|_2 \le \sum_{k\ge 3} |h_{I_k}|_2 \le \frac{1}{\sqrt{p}}\, |h_{I_1^c}|_1.$$

From(2.7), $|h_{I_1} + h_{I_2}|_2 \le \frac{\gamma_{2p}(A)}{\sqrt{p}}\ |h_{I_1^c}|_1$ and putting things together, we derive that

$$|h|_2 \le \sqrt{\frac{1+\gamma_{2p}^2(A)}{p}}\ |h_{I_1^c}|_1 \le \sqrt{\frac{1+\gamma_{2p}^2(A)}{p}}\ |h|_1.$$

□

From relation (2.5) and the null space property (Proposition 2.2.11) we derive the following corollary.

Corollary 2.4.3. — *Let $1 \leqslant p \leqslant N/2$. Let A be an $n \times N$ matrix. If $\gamma_{2p}(A) \le \sqrt{p}$, then A satisfies the exact reconstruction property of order m by ℓ_1-minimization with*

$$m = \left\lfloor p/\gamma_{2p}^2(A)\right\rfloor.$$

Our main goal now is to find p such that γ_{2p} is bounded by some numerical constant. This means that we need a uniform control of the smallest and largest singular values of all block matrices of A with $2p$ columns. By Corollary 2.4.3 this is a sufficient condition for the exact reconstruction of m-sparse vectors by ℓ_1-minimization with $m \sim p$. When $|Ax|_2$ satisfies good concentration properties, the restricted isometry property is more adapted. In this situation, $\gamma_{2p} \sim 1$. When the isometry constant δ_{2p} is sufficiently small, A satisfies the exact reconstruction of m-sparse vectors with $m = p$ (see Theorem 2.3.2).

Similarly, an estimate of $\mathrm{rad}\,(\ker A \cap B_1^N)$ gives an estimate of the size of sparsity of vectors which can be reconstructed by ℓ_1-minimization.

Proposition 2.4.4. — *Let A be an $n \times N$ matrix. If $1 \le m$ and*

$$\mathrm{rad}\,(\ker A \cap B_1^N) < \frac{1}{2\sqrt{m}}$$

then the matrix A satisfies the exact reconstruction property of order m by ℓ_1-minimization.

Proof. — Let $h \in \ker A$ and $I \subset [N], |I| \le m$. By our assumption, we have that

$$\forall h \in \ker A, h \neq 0 \quad |h|_2 < |h|_1/2\sqrt{m}.$$

Thus $|h_I|_1 \le \sqrt{m}\ |h_I|_2 \le \sqrt{m}\ |h|_2 < |h|_1/2$ and $|h_I|_1 < |h_{I^c}|_1$. We conclude using the null space property (Proposition 2.2.11). □

To conclude the section, note that (2.6) implies that whenever an $n \times N$ matrix A satisfies a restricted isometry property of order $m \ge 1$, then $\mathrm{rad}\,(\ker A \cap B_1^N) = \frac{O(1)}{\sqrt{m}}$.

2.5. Gelfand widths

The study of the previous section leads to the notion of Gelfand widths.

Definition 2.5.1. — *Let T be a bounded subset of a normed space E. Let $k \geq 0$ be an integer. The k-th Gelfand width of T is defined as*

$$d^k(T, E) := \inf_S \sup_{x \in S \cap T} \|x\|_E,$$

where $\|\cdot\|_E$ denotes the norm of E and the infimum is taken over all linear subspaces S of E of codimension less than or equal to k.

A different notation is used in Banach space and Operator Theory. Let $u : X \longrightarrow Y$ be an operator between two normed spaces X and Y. The k-th Gelfand number is defined by

$$c_k(u) = \inf\{\| \, u_{|S} \, \| : S \subset X, \operatorname{codim} S < k\}$$

where $u_{|S}$ denotes the restriction of the operator u to the subspace S. This reads equivalently as

$$c_k(u) = \inf_S \sup_{x \in S \cap B_X} \|u(x)\|_Y,$$

where B_X denotes the unit ball of X and the infimum is taken over all subspaces S of X with codimension strictly less than k. These different notations are related by

$$c_{k+1}(u) = d^k(u(B_X), Y).$$

If F is a linear space ($\mathbb{R}^N$ for instance) equipped with two norms defining two normed spaces X and Y and if $id : X \to Y$ is the identity mapping of F considered from the normed spaces X to Y, then

$$d^k(B_X, Y) = c_{k+1}(id : X \to Y).$$

As a particular but important instance, we have

$$d^k(B_1^N, \ell_2^N) = c_{k+1}(id : \ell_1^N \to \ell_2^N) = \inf_{\operatorname{codim} S \leqslant k} \operatorname{rad}(S \cap B_1^N).$$

The study of these numbers has attracted a lot of attention during the seventies and the eighties. An important result is the following.

Theorem 2.5.2. — *There exist $c, C > 0$ such that for any integers $1 \leq k \leq N$,*

$$c \min\left\{1, \sqrt{\frac{\log(N/k) + 1}{k}}\right\} \leq c_k(id : \ell_1^N \to \ell_2^N) \leq C \min\left\{1, \sqrt{\frac{\log(N/k) + 1}{k}}\right\}.$$

Moreover, if $\mathbb{P}$ is the rotation invariant probability measure on the Grassmann manifold of subspaces S of $\mathbb{R}^N$ with $\operatorname{codim}(S) = k - 1$, then

$$\mathbb{P}\left(\operatorname{rad}(S \cap B_1^N) \leq C \min\left\{1, \sqrt{\frac{\log(N/k) + 1}{k}}\right\}\right) \geq 1 - \exp(-ck).$$

Coming back to compressed sensing, let $1 \leqslant m \leqslant n$ and let us assume that

$$d^n(B_1^N, \ell_2^N) < \frac{1}{2\sqrt{m}}.$$

In other words, we assume that there is a subspace $S \subset \mathbb{R}^N$ of codimension less than or equal to n such that $\mathrm{rad}\,(S \cap B_1^N) < \frac{1}{2\sqrt{m}}$. Choose any $n \times N$ matrix A such that $\ker A = S$, then

$$\mathrm{rad}\,(\ker A \cap B_1^N) < \frac{1}{2\sqrt{m}}.$$

Proposition 2.4.4 shows that A satisfies the exact reconstruction property of order m by ℓ_1-minimization.

It follows from Theorem 2.5.2 that there exists a matrix A satisfying the exact reconstruction property of order

$$\lfloor c_1 n / \log(c_2 N/n) \rfloor$$

where c_1, c_2 are universal constants. From Proposition 2.2.18 it is the optimal order.

Performance of sensing algorithm and Gelfand widths. — The optimal performance of sensing algorithm is closely connected to Gelfand widths. Consider the problem of reconstruction of a vector $x \in T \subset \mathbb{R}^N$ from the data $y = Ax \in \mathbb{R}^n$, where A is an $n \times N$ matrix, called the *encoder* and T is some given subset of $\mathbb{R}^N$. Let $\Delta : \mathbb{R}^n \to \mathbb{R}^N$ be a *decoder* which to every $x \in T$ returns $\Delta(A, Ax) = \Delta(Ax)$, an approximation to x (see Problem 2.2.2). Let E be the space $\mathbb{R}^N$ equipped with a norm $\|\cdot\|_E$. To evaluate the optimal performance of a pair (A, Δ) with respect to this norm, the following quantity was considered

$$E^n(T, E) = \inf_{(A,\Delta)} \sup_{x \in T} \|x - \Delta(Ax)\|$$

where (A, Δ) describes all possible pairs of encoder-decoder with A linear. As shown by the following well known lemma, it is equivalent to the Gelfand width $d^n(T, E)$.

Lemma 2.5.3. — *Let $T \subset \mathbb{R}^N$ be a symmetric subset such that $T + T \subset 2aT$ for some $a > 0$. Let E be the space $\mathbb{R}^N$ equipped with a norm $\|\,.\,\|_E$. Then*

$$\forall 1 \le n \le N, \quad d^n(T, E) \leqslant E^n(T, E) \leqslant 2a\, d^n(T, E).$$

Proof. — Let (A, Δ) be a pair of encoder-decoder. To prove the left-hand side inequality, observe that

$$d^n(T, E) = \inf_B \sup_{x \in \ker B \cap T} \|x\|_E$$

where the infimum is taken over all $n \times N$ matrices B. Since $\ker A \cap T$ is symmetric, for any $x \in \ker A$, one has

$$2\|x\|_E \leqslant \|x - \Delta(0)\|_E + \|-x - \Delta(0)\|_E \leqslant 2 \sup_{z \in \ker A \cap T} \|z - \Delta(Az)\|_E.$$

Therefore

$$d^n(T, E) \leqslant \sup_{x \in \ker A \cap T} \|x\|_E \leqslant \sup_{z \in T} \|z - \Delta(Az)\|_E.$$

This shows that $d^n(T, E) \leqslant E^n(T, E)$.

To prove the right-hand side inequality, let A be an $n \times N$ matrix. It is enough to define Δ on $A(T)$. Let $x \in T$ and let $y = Ax$ be the data. Denote by $S(y)$ the affine subspace $\{x' \in \mathbb{R}^N : Ax' = y\}$. We choose some $x' \in T \cap S(y)$ and define $\Delta(y) = x'$. Since T is symmetric and $T + T \subset 2aT$, one has $x - x' \in \ker A \cap (2aT)$ and

$$\|x - x'\|_E \leqslant 2a \sup_{z \in \ker A \cap T} \|z\|_E.$$

Therefore

$$E^n(T, E) \leqslant \|x - \Delta(Ax)\| = \|x - x'\|_E \leqslant 2a \sup_{z \in \ker A \cap T} \|z\|_E.$$

Taking the infimum over A, we deduce that $E^n(T, E) \leqslant 2ad^n(T, E)$.

□

This equivalence between $d^n(T, E)$ and $E^n(T, E)$ can be used to estimate Gelfand widths by means of methods from compressed sensing. This approach gives a simple way to prove the upper bound of Theorem 2.5.2. The condition $T + T \subset 2aT$ is of course satisfied when T is convex (with $a = 1$). See Claim 2.7.13 for non-convex examples.

2.6. Gaussian random matrices satisfy a RIP

So far, we did not give yet any example of matrices satisfying the exact reconstruction property of order m with large m. It is known that with high probability Gaussian matrices do satisfy this property.

The subgaussian Ensemble. — We consider here a probability $\mathbb{P}$ on the space $M(n, N)$ of real $n \times N$ matrices satisfying the following concentration inequality: there exists an absolute constant c_0 such that for every $x \in \mathbb{R}^N$ we have

$$\mathbb{P}\left(\left||Ax|_2^2 - |x|_2^2\right| \geq t|x|_2^2\right) \leq 2e^{-c_0 t^2 n} \qquad \text{for all } 0 < t \leq 1. \tag{2.8}$$

Definition 2.6.1. — *For a real random variable Z we define the ψ_2-norm by*

$$\|Z\|_{\psi_2} = \inf\left\{s > 0 \,:\, \mathbb{E}\exp\left(|Z|/s\right)^2 \leqslant e\right\}.$$

We say that a random vector $Y \in \mathbb{R}^N$ is isotropic if it is centered and satisfies

$$\forall y \in \mathbb{R}^N, \quad \mathbb{E}|\langle Y, y\rangle|^2 = |y|_2^2.$$

A random vector $Y \in \mathbb{R}^N$ satisfies a ψ_2-estimate with constant α (shortly Y is ψ_2 with constant α) if

$$\forall y \in \mathbb{R}^N, \quad \|\langle Y, y\rangle\|_{\psi_2} \leqslant \alpha|y|_2.$$

It is well-known that a real random variable Z is ψ_2 (with some constant) if and only if it satisfies a subgaussian tail estimate. In particular if Z is a real random variable with $\|Z\|_{\psi_2} \leq \alpha$, then for every $t \geq 0$,

$$\mathbb{P}(|Z| \geq t) \leq e^{-(t/\alpha)^2 + 1}.$$

This ψ_2 property can also be characterized by the growth of moments. Well known examples are Gaussian random variables and bounded centered random variables (see Chapter 1 for details).

Let $Y_1, \ldots, Y_n \in \mathbb{R}^N$ be independent isotropic random vectors which are ψ_2 with the same constant α. Let A be the matrix with $Y_1, \ldots, Y_n \in \mathbb{R}^N$ as rows. We consider the probability $\mathbb{P}$ on the space of matrices $M(n,N)$ induced by the mapping $(Y_1, \ldots, Y_n) \to A$.

Let us recall Bernstein's inequality (see Chapter 1). For $y \in S^{N-1}$ consider the average of n independent copies of the random variable $\langle Y_1, y\rangle^2$. Then for every $t > 0$,

$$\mathbb{P}\left(\left| \frac{1}{n} \sum_{i=1}^{n} \langle Y_i, y\rangle^2 - 1 \right| > t \right) \leqslant 2\exp\left(-cn \min\left\{ \frac{t^2}{\alpha^4}, \frac{t}{\alpha^2} \right\} \right),$$

where c is an absolute constant. Note that since $\mathbb{E}\langle Y_1, y\rangle^2 = 1$, one has $\alpha \geqslant 1$ and $\left|\frac{Ay}{\sqrt{n}}\right|_2^2 = \frac{1}{n}\sum_{i=1}^n \langle Y_i, y\rangle^2$. This shows the next claim:

Claim 2.6.2. — *Let $Y_1, \ldots, Y_n \in \mathbb{R}^N$ be independent isotropic random vectors that are ψ_2 with constant α. Let $\mathbb{P}$ be the probability induced on $M(n,N)$. Then for every $x \in \mathbb{R}^N$ we have*

$$\mathbb{P}\left(\left| \left| \frac{A}{\sqrt{n}} x \right|_2^2 - |x|_2^2 \right| \geq t|x|_2^2 \right) \leq 2e^{-\frac{c}{\alpha^4} t^2 n} \qquad \text{for all } 0 < t \leq 1$$

where $c > 0$ is an absolute constant.

Among the most important examples of model of random matrices satisfying (2.8) are matrices with independent subgaussian rows, normalized in the right way.

Example 2.6.3. — *Some classical examples:*

- *$Y_1, \ldots, Y_n \in \mathbb{R}^N$ are independent copies of the Gaussian vector $Y = (g_1, \ldots, g_N)$ where the g_i's are independent $\mathcal{N}(0,1)$ Gaussian variables*
- *$Y_1, \ldots, Y_n \in \mathbb{R}^N$ are independent copies of $Y = (\varepsilon_1, \ldots, \varepsilon_N)$ where the ε_i's are independent, symmetric ± 1 (Bernoulli) random variables*
- *$Y_1, \ldots, Y_n \in \mathbb{R}^N$ are independent copies of a random vector uniformly distributed on the Euclidean sphere of radius $\sqrt{N}$.*

In all these cases $Y_1, \ldots, Y_n \in \mathbb{R}^N$ are independent isotropic with a ψ_2 constant α, for a suitable $\alpha \geqslant 1$. For the last case see e.g. [**LT91**]. For more details on Orlicz norm and probabilistic inequalities used here see Chapter 1.

Sub-Gaussian matrices are almost norm preserving on Σ_m. — An important feature of Σ_m and its subsets $S_2(\Sigma_m)$ and $B_2(\Sigma_m)$ is their peculiar structure: the last two are the unions of the unit spheres, and unit balls, respectively, supported on m-dimensional coordinate subspaces of $\mathbb{R}^N$.

We begin with the following lemma which allows to step up from a net to the whole unit sphere.

Lemma 2.6.4. — *Let $q \geq 1$ be an integer and B be a symmetric $q \times q$ matrix. Let $\Lambda \subset S^{q-1}$ be a θ-net of S^{q-1} by θB_2^q for some $\theta \in (0, 1/2)$. Then*

$$\|B\| = \sup_{x \in S^{q-1}} |\langle Bx, x\rangle| \leqslant (1-2\theta)^{-1} \sup_{y\in\Lambda} |\langle By, y\rangle|.$$

Proof. — For any $x, y \in \mathbb{R}^q$, $\langle Bx, x\rangle = \langle By, y\rangle + \langle Bx, x-y\rangle + \langle B(x-y), y\rangle$. Theferore $|\langle Bx, x\rangle| \leqslant |\langle By, y\rangle| + 2|x-y|\|B\|$. Since the matrix B is symmetric, its norm may be computed using its associated quadratic form, that is $\|B\| = \sup_{x\in S^{q-1}} |\langle Bx, x\rangle|$. Thus, if $|x-y| \leqslant \theta$, then $\|B\| \leqslant \sup_{y\in\Lambda} |\langle By, y\rangle| + 2\theta\|B\|$ and the conclusion follows. □

We are able now to give a simple proof that subgaussian matrices satisfy the exact reconstruction property of order m by ℓ_1-minimization with large m.

Theorem 2.6.5. — *Let $\mathbb{P}$ be a probability on $M(n, N)$ satisfying (2.8). Then there exist positive constants c_1, c_2 and c_3 depending only on c_0 from (2.8), for which the following holds: with probability at least $1 - 2\exp(-c_3 n)$, A satisfies the exact reconstruction property of order m by ℓ_1-minimization with*

$$m = \left\lfloor \frac{c_1 n}{\log (c_2 N/n)} \right\rfloor.$$

Moreover, A satisfies RIP$_m(\delta)$ for any $\delta \in (0,1)$ with $m \sim c\delta^2 n/\log(CN/\delta^2 n)$ where c and C depend only on c_0.

Proof. — Let y_i, $i = 1, 2, \ldots, n$, be the rows of A. Let $1 \leq p \leq N/2$. For every subset I of $[N]$ of cardinality $2p$, let Λ_I be a $(1/3)$-net of the unit sphere of $\mathbb{R}^I$ by $(1/3)B_2^I$ satisfying $|\Lambda_I| \leq 9^{2p}$ (see Claim 2.2.8).

For each subset I of $[N]$ of cardinality $2p$, consider on $\mathbb{R}^I$, the quadratic form

$$q_I(y) := \frac{1}{n}\sum_{i=1}^n \langle y_i, y\rangle^2 - |y|^2\,,\ y \in \mathbb{R}^I.$$

There exist symmetric $q \times q$ matrices B_I with $q = 2p$, such that $q_I(y) = \langle B_I y, y\rangle$.

Applying Lemma 2.6.4 with $\theta = 1/3$, to each symmetric matrix B_I and then taking the supremum over I, we get that

$$\sup_{y\in S_2(\Sigma_{2p})} \Big|\frac{1}{n}\sum_{i=1}^n (\langle y_i, y\rangle^2 - 1)\Big| \leqslant 3 \sup_{y\in\Lambda} \Big|\frac{1}{n}\sum_{i=1}^n (\langle y_i, y\rangle^2 - 1)\Big|,$$

where $\Lambda \subset \mathbb{R}^N$ is the union of the Λ_I for $|I| = 2p$.

Note that there is nothing random in that relation. This is why we changed the notation of the rows from (Y_i) to (y_i). Thus checking how well the matrix A defined by the rows (y_i) is acting on Σ_{2p} is reduced to checking that on the finite set Λ. Now recall that $|\Lambda| \leq \binom{N}{2p} 9^{2p} \leq \exp\left(2p\log\left(\frac{9eN}{2p}\right)\right)$.

Given a probability $\mathbb{P}$ on $M(n, N)$ satisfying (2.8), and using a union bound estimate, we get that

$$\sup_{y\in S_2(\Sigma_{2p})} \Big|\frac{1}{n}\sum_{i=1}^n (\langle y_i, y\rangle^2 - 1)\Big| \leqslant 3\varepsilon$$

holds with probability at least

$$1 - 2|\Lambda|e^{-c_0\varepsilon^2 n} \geq 1 - 2\exp\left(2p\log\left(\frac{9eN}{2p}\right)\right)e^{-c_0\varepsilon^2 n} \geq 1 - 2e^{-c_0\varepsilon^2 n/2}$$

whenever

$$2p\log\left(\frac{9eN}{2p}\right) \leq c_0\varepsilon^2 n/2.$$

Assuming this inequality, we get that

$$\delta_{2p}(A) \leq 3\varepsilon$$

with probability larger than $1 - 2\exp(-c_0\varepsilon^2 n/2)$.

The moreover part of the statement is obtained by solving in p the relation $2p\log(9eN/2p) \leq c_0\varepsilon^2 n/2$ with $3\varepsilon = \delta$. The first part of the statement follows from Theorem 2.3.2 or Corollary 2.4.3 by a convenient choice of ε. □

The strategy used in the preceding proof was the following:

- *discretization*: discretization of the set Σ_{2p} by a net argument
- *concentration*: $|Ax|_2^2$ concentrates around its mean for each individual x of the net
- *union bound*: concentration should be good enough to balance the cardinality of the net and to conclude to uniform concentration on the net of $|Ax|_2^2$ around its mean
- *from the net to the whole set*, that is checking RIP, is obtained by Lemma 2.6.4.

We conclude this section by an example of an $n \times N$ matrix A which is a good compressed sensing matrix such that none of the $n \times N$ matrices with the same kernel as A satisfy a restricted isometry property of any order ≥ 1 with good parameter. As we already noticed, if A has parameter γ_p, one can find $t_0 > 0$ and rescale the matrix so that $\delta_p(t_0 A) = \gamma_p^2 - 1/\gamma_p^2 + 1 \in [0, 1)$. In this example, γ_p is large, $\delta_p(t_0 A) \sim 1$ and one cannot deduce any result about exact reconstruction from Theorem 2.3.2.

Example 2.6.6. — *Let $1 \leq n \leq N$. Let $\delta \in (0, 1)$. There exists an $n \times N$ matrix A such that for any $p \leq cn/\log(CN/n)$, one has $\gamma_{2p}(A)^2 \leq c'(1-\delta)^{-1}$. Thus, for any $m \leq c"(1-\delta)n/\log(CN/n)$, the matrix A satisfies the exact reconstruction property of m-sparse vectors by ℓ_1-minimization. Nevertheless, for any $n \times n$ matrix U, the restricted isometry constant of order 1 of UA satisfies, $\delta_1(UA) \geq \delta$ (think of $\delta \geq 1/2$). Here, $C, c, c', c" > 0$ are universal constants.*

The proof is left as an exercise.

2.7. RIP for other "simple" subsets: almost sparse vectors

As already mentioned, various "random projection" operators act as "almost norm preserving" on "thin" subsets of the sphere. We analyze a simple structure of the metric entropy of a set $T \subset \mathbb{R}^N$ in order that, with high probability, (a multiple of) a Gaussian or subgaussian matrix acts almost like an isometry on T. This will apply to a more general case than sparse vectors.

Theorem 2.7.1. — *Consider a probability on the space of $n \times N$ matrices satisfying (2.8). Let $T \subset S^{N-1}$ and $0 < \varepsilon < 1/15$. Assume the following:*

i) *There exists an ε-net $\Lambda \subset S^{N-1}$ of T satisfying $|\Lambda| \leq \exp(c_0 \varepsilon^2 n/2)$*

ii) *There exists a subset Λ' of εB_2^N such that $(T - T) \cap \varepsilon B_2^N \subset 2 \operatorname{conv} \Lambda'$ and $|\Lambda'| \leq \exp(c_0 n/2)$.*

Then with probability at least $1 - 4\exp(-c_0\varepsilon^2 n/2)$, one has that for all $x \in T$,

$$1 - 15\varepsilon \leq |Ax|_2^2 \leq 1 + 15\varepsilon. \tag{2.9}$$

Proof. — The idea is to show that A acts on Λ in an almost norm preserving way. This is the case because the degree of concentration of each variable $|Ax|_2^2$ around its mean defeats the cardinality of Λ. Then one shows that $A(\operatorname{conv}\Lambda')$ is contained in a small ball - thanks to a similar argument.

Consider the set Ω of matrices A such that

$$\big|\, |Ax_0|_2 - 1 \,\big| \leq \big| |Ax_0|_2^2 - 1 \big| \leq \varepsilon \qquad \text{for all} \;\; x_0 \in \Lambda, \tag{2.10}$$

and

$$|Az|_2 \leq 2\varepsilon \qquad \text{for all} \;\; z \in \Lambda'. \tag{2.11}$$

From our assumption (2.8), i) and ii), one has

$$\mathbb{P}(\Omega) \geq 1 - 2\exp(-c_0\varepsilon^2 n/2) - 2\exp(-c_0 n/2) \geq 1 - 4\exp(-c_0\varepsilon^2 n/2).$$

Let $x \in T$ and consider $x_0 \in \Lambda$ such that $|x - x_0|_2 \leq \varepsilon$. Then for every $A \in \Omega$

$$|Ax_0|_2 - |A(x - x_0)|_2 \leq |Ax|_2 \leq |Ax_0|_2 + |A(x - x_0)|_2 \,.$$

Since $x - x_0 \in (T - T) \cap \varepsilon B_2^N$, property ii) and (2.11) give that

$$|A(x - x_0)|_2 \leq 2 \sup_{z \in \operatorname{conv}\Lambda'} |Az|_2 = 2 \sup_{z \in \Lambda'} |Az|_2 \leq 4\varepsilon. \tag{2.12}$$

Combining this with (2.10) implies that $1 - 5\varepsilon \leq |Ax|_2 \leq 1 + 5\varepsilon$. The proof is completed by squaring. □

Approximate reconstruction of almost sparse vectors. — After analyzing the restricted isometry property for thin sets of the type of Σ_m, we look again at the ℓ_1-minimization method in order to get approximate reconstruction of vectors which are not far from the set of sparse vectors. As well as for the exact reconstruction, approximate reconstruction depends on a null space property.

Proposition 2.7.2. — *Let A be an $n \times N$ matrix and $\lambda \in (0, 1)$. Assume that*

$$\forall h \in \ker A,\; \forall I \subset [N], |I| \leq m, |h_I|_1 \leqslant \lambda |h_{I^c}|_1. \tag{2.13}$$

Let $x \in \mathbb{R}^N$ and let $x^\sharp$ be a minimizer of

$$(P) \qquad \min_{t \in \mathbb{R}^N} |t|_1 \quad \textit{subject to} \quad At = Ax.$$

Then for any $I \subset [N], |I| \leqslant m$,

$$|x - x^\sharp|_1 \leq 2\,\frac{1 + \lambda}{1 - \lambda}\, |x - x_I|_1.$$

Proof. — Let $x^\sharp$ be a minimizer of (P) and set $h = x^\sharp - x \in \ker A$. Let $m \geqslant 1$ and $I \subset [N]$ such that $|I| \leqslant m$. Observe that

$$|x|_1 \geq |x+h|_1 = |x_I + h_I|_1 + |x_{I^c} + h_{I^c}|_1 \geq |x_I|_1 - |h_I|_1 + |h_{I^c}|_1 - |x_{I^c}|_1$$

and thus

$$|h_{I^c}|_1 \leq |h_I|_1 + 2|x_{I^c}|_1.$$

On the other hand, from the null space assumption, we get

$$|h_{I^c}|_1 \leq |h_I|_1 + 2|x_{I^c}|_1 \leq \lambda |h_{I^c}|_1 + 2|x_{I^c}|_1.$$

Therefore

$$|h_{I^c}|_1 \leq \frac{2}{1-\lambda}\, |x_{I^c}|_1.$$

Since the null space assumption reads equivalently $|h|_1 \leqslant (1+\lambda)\, |h_{I^c}|_1$, we can conclude the proof. □

Note that the minimum of $|x - x_I|_1$ over all subsets I such that $|I| \leq m$, is obtained when I is the support of the m largest coordinates of x. The vector x_I is henceforth the best m-sparse approximation of x (in the ℓ_1 norm). Thus if x is m-sparse we go back to the exact reconstruction scheme.

Property (2.13), which is a strong form of the null space property, may be studied by means of parameters such as the Gelfand widths, like in the next proposition.

Proposition 2.7.3. — *Let A be an $n \times N$ matrix and $1 \leq m \leq n$. Let $x \in \mathbb{R}^N$ and let $x^\sharp$ be a minimizer of*

$$(P) \qquad \min_{t \in \mathbb{R}^N} |t|_1 \quad \textit{subject to} \quad At = Ax.$$

Let $\rho = \operatorname{rad}(B_1^N \cap \ker A) = \sup_{x \in B_1^N \cap \ker A} |x|_2$. Assume that $\rho \leqslant 1/4\sqrt{m}$. Then for every $I \subset [N], |I| \leqslant m$,

$$|x - x^\sharp|_1 \leq 4\, |x - x_I|_1$$

and

$$|x - x^\sharp|_2 \leq \frac{1}{\sqrt{m}}\, |x - x_I|_1.$$

Proof. — Let $h = x - x^\sharp \in \ker A$. We have

$$|h_I|_1 \leq \sqrt{m}\, |h_I|_2 \leqslant \sqrt{m}\, |h|_2 \leqslant \sqrt{m}\rho |h|_1.$$

Therefore

$$|h_I|_1 \leq \frac{\rho\sqrt{m}}{1-\rho\sqrt{m}}\, |h_{I^c}|_1$$

whenever $\rho\sqrt{m} < 1$. We deduce that Property (2.13) is satisfied with $\lambda = \frac{\rho\sqrt{m}}{1-\rho\sqrt{m}}$. The inequality $|x - x^\sharp|_1 \leq 4\, |x - x_I|_1$ follows directly from Proposition 2.7.2 and the assumption $\rho \leqslant 1/4\sqrt{m}$. The relation $|h|_2 \leqslant \rho |h|_1 \leq 4\rho |x - x_I|_1$ concludes the proof of the last inequality. □

Let $1 \leq m \leq p \leq n$ and $N \geqslant m + p$. The last proposition can be reformulated in terms of the constant of the restricted isometry property or in terms of the parameter γ_p, since from (2.6),

$$\rho \leq \sqrt{\frac{1 + \gamma_{2p}^2(A)}{p}},$$

but we shall not go any further ahead.

Remark 2.7.4. — *To sum up, Theorem 2.4.2 shows that if an $n \times N$ matrix A satisfies a restricted isometry property of order $m \geq 1$, then*

$$\mathrm{rad}\,(\ker A \cap B_1^N) = \frac{O(1)}{\sqrt{m}}. \tag{2.14}$$

On the other hand, Propositions 2.4.4 and 2.7.3 show that if an $n \times N$ matrix A satisfies (2.14), then A satisfies the exact reconstruction property of order $O(m)$ by ℓ_1-minimization as well as an approximate reconstruction property.

Based on this remark, we could focus on estimates of the diameters, but the example of Gaussian matrices shows that it may be easier to prove a restricted isometry property than computing widths. We conclude this section by an application of Proposition 2.7.3.

Corollary 2.7.5. — *Let $0 < p < 1$ and consider*

$$T = B_{p,\infty}^N = \left\{ x = (x_1, \ldots, x_N) \in \mathbb{R}^N \,:\, |\{i \,:\, |x_i| \geq s\}| \leq s^{-p} \text{ for all } \ s > 0 \right\}$$

the "unit ball" of $\ell_{p,\infty}^N$. Let A be an $n \times N$ matrix and $1 \leq m \leq n$. Let $x \in T$ and let $x^\sharp$ be a minimizer of

$$(P) \qquad \min_{t \in \mathbb{R}^N} |t|_1 \quad \text{subject to} \quad At = Ax.$$

Let $\rho = \mathrm{rad}\,(B_1^N \cap \ker A) = \sup_{x \in B_1^N \cap \ker A} |x|_2$ and assume that $\rho \leqslant 1/4\sqrt{m}$, then

$$|x - x^\sharp|_2 \leqslant ((1/p) - 1)^{-1} m^{1/2 - 1/p}.$$

Proof. — Observe that for any $x \in B_{p,\infty}^N$, one has $x_i^* \leq 1/i^{1/p}$, for every $i \geq 1$, where $(x_i^*)_{i=1}^N$ is a non-increasing rearrangement of $(|x_i|)_{i=1}^N$. Let $I \subset [N]$, such that $|I| = m$ and let x_I be one of the best m-sparse approximation of x. Note that

$$\sum_{i > m} i^{-1/p} \leq (1/p - 1)^{-1} m^{1 - 1/p}.$$

From Proposition 2.7.3, we get that if $\rho \leqslant 1/4\sqrt{m}$ and if $x^\sharp$ is a minimizer of (P), then

$$|x - x^\sharp|_2 \leq \frac{1}{\sqrt{m}} |x - x_I|_1 \leqslant ((1/p) - 1)^{-1} m^{1/2 - 1/p}.$$

□

Reducing the computation of Gelfand widths by truncation. — We begin with a simple principle.

Definition 2.7.6. — *We say that a subset $T \subset \mathbb{R}^N$ is star-shaped around 0 or shortly, star-shaped, if $\lambda T \subset T$ for every $0 \leq \lambda \leq 1$. Let $\rho > 0$ and let $T \subset \mathbb{R}^N$ be star-shaped, we denote*

$$T_\rho = T \cap \rho S^{N-1}.$$

Recall that $\mathrm{rad}\,(S) = \sup_{x \in S} |x|_2$.

Lemma 2.7.7. — *Let $\rho > 0$ and let $T \subset \mathbb{R}^N$ be star-shaped. Then for any linear subspace $E \subset \mathbb{R}^N$ such that $E \cap T_\rho = \emptyset$, we have* $\mathrm{rad}\,(E \cap T) < \rho$.

Proof. — If $\mathrm{rad}\,(E \cap T) \geqslant \rho$, there would be $x \in E \cap T$ of norm greater or equal to ρ. Since T is star-shaped, so is $E \cap T$ and thus $\rho x / |x|_2 \in E \cap T_\rho$; a contradiction. □

This easy lemma will be a useful tool in the next sections and in Chapter 5. The subspace E will be the kernel of our matrix A, ρ a parameter that we try to estimate as small as possible such that $\ker A \cap T_\rho = \emptyset$, that is such that $Ax \neq 0$ for all $x \in T$ with $|x|_2 = \rho$. This will be in particular the case when A or a multiple of A acts on T_ρ in an almost norm-preserving way.

With Theorem 2.7.1 in mind, we apply this plan to subsets T like Σ_m.

Corollary 2.7.8. — *Let $\mathbb{P}$ be a probability on $M(n, N)$ satisfying (2.8). Consider a star-shaped subset $T \subset \mathbb{R}^N$ and $\rho > 0$. Assume that $\frac{1}{\rho} T_\rho \subset S^{N-1}$ satisfies the hypothesis of Theorem 2.7.1 for some $0 < \varepsilon < 1/15$. Then* $\mathrm{rad}\,(\ker A \cap T) < \rho$, *with probability at least $1 - 2\exp(-cn)$ where $c > 0$ is an absolute constant.*

Application to subsets related to ℓ_p unit balls. — To illustrate this method, we consider some examples of sets T:

- the unit ball of ℓ_1^N
- the "unit ball" $B_p^N = \{x \in \mathbb{R}^N : \sum_1^N |x_i|^p \leq 1\}$ of ℓ_p^N, $0 < p < 1$
- the "unit ball" $B_{p,\infty}^N = \big\{x \in \mathbb{R}^N : |\{i : |x_i| \geq s\}| \leq s^{-p} \text{ for all } s > 0\big\}$ of $\ell_{p,\infty}^N$ (weak ℓ_p^N), for $0 < p < 1$.

Note that for $0 < p < 1$, the "unit balls" B_p^N or $B_{p,\infty}^N$ are not really balls since they are not convex. Note also that $B_p^N \subset B_{p,\infty}^N$, so that for estimating Gelfand widths, we can restrict to the balls $B_{p,\infty}^N$.

We need two lemmas. The first uses the following classical fact:

Claim 2.7.9. — *Let $(a_i), (b_i)$ two sequences of positive numbers such that (a_i) is non-increasing. Then the sum $\sum a_i b_{\pi(i)}$ is maximized over all permutations π of the index set, if $b_{\pi(1)} \geq b_{\pi(2)} \geq \ldots$.*

Lemma 2.7.10. — *Let $0 < p < 1$, $1 \leqslant m \leqslant N$ and $r = (1/p - 1)m^{1/p-1/2}$. Then, for every $x \in \mathbb{R}^N$,*

$$\sup_{z \in rB_{p,\infty}^N \cap B_2^N} \langle x, z\rangle \leqslant 2 \left(\sum_{i=1}^m {x_i^*}^2 \right)^{1/2},$$

where $(x_i^*)_{i=1}^N$ is a non-increasing rearrangement of $(|x_i|)_{i=1}^N$. Equivalently,

$$rB_{p,\infty}^N \cap B_2^N \subset 2\,\mathrm{conv}\,(S_2(\Sigma_m)). \tag{2.15}$$

Moreover one has

$$\sqrt{m}B_1^N \cap B_2^N \subset 2\,\mathrm{conv}\,(S_2(\Sigma_m)). \tag{2.16}$$

Proof. — We treat only the case of $B_{p,\infty}^N$, $0 < p < 1$. The case of B_1^N is similar. Note first that if $z \in B_{p,\infty}^N$, then for any $i \geq 1$, $z_i^* \leq 1/i^{1/p}$, where $(z_i^*)_{i=1}^N$ is a non-increasing rearrangement of $(|z_i|)_{i=1}^N$. Using Claim 2.7.9 we get that for any $r > 0, m \geq 1$ and $z \in rB_{p,\infty}^N \cap B_2^N$,

$$\begin{aligned}
\langle x, z\rangle &\leqslant \left(\sum_{i=1}^m {x_i^*}^2 \right)^{1/2} + \sum_{i>m} \frac{r x_i^*}{i^{1/p}} \\
&\leqslant \left(\sum_{i=1}^m {x_i^*}^2 \right)^{1/2} \left(1 + \frac{r}{\sqrt{m}} \sum_{i>m} \frac{1}{i^{1/p}} \right) \\
&\leqslant \left(\sum_{i=1}^m {x_i^*}^2 \right)^{1/2} \left(1 + \left(\frac{1}{p} - 1 \right)^{-1} \frac{r}{m^{1/p-1/2}} \right).
\end{aligned}$$

By the definition of r, this completes the proof. □

The second lemma shows that $m^{1/p-1/2}B_{p,\infty}^N \cap S^{N-1}$ is well approximated by vectors on the sphere with short support.

Lemma 2.7.11. — *Let $0 < p < 2$ and $\delta > 0$, and set $\varepsilon = 2(2/p - 1)^{-1/2}\delta^{1/p-1/2}$. Let $1 \leq m \leq N$. Then $S_2(\Sigma_{\lceil m/\delta \rceil})$ is an ε-net of $m^{1/p-1/2}B_{p,\infty}^N \cap S^{N-1}$ with respect to the Euclidean metric.*

Proof. — Let $x \in m^{1/p-1/2}B_{p,\infty}^N \cap S^{N-1}$ and assume without loss of generality that $x_1 \geq x_2 \geq \ldots \geq x_N \geq 0$. Define z' by $z'_i = x_i$ for $1 \leq i \leq \lceil m/\delta \rceil$ and $z'_i = 0$ otherwise. Then

$$|x - z'|_2^2 = \sum_{i > m/\delta} |x_i|^2 \leq m^{2/p-1} \sum_{i > m/\delta} 1/i^{2/p} < (2/p - 1)^{-1}\,\delta^{2/p-1}.$$

Thus $1 \geq |z'|_2 \geq 1 - (2/p - 1)^{-1/2}\,\delta^{1/p-1/2}$. Put $z = z'/|z'|_2$. Then $z \in S_2(\Sigma_{\lceil m/\delta \rceil})$ and

$$|z - z'|_2 = 1 - |z'|_2 \leq (2/p - 1)^{-1/2}\,\delta^{1/p-1/2}.$$

By the triangle inequality $|x - z|_2 < \varepsilon$. This completes the proof. □

The preceding lemmas will be used to show that the hypothesis of Theorem 2.7.1 are satisfied for an appropriate choice of T and ρ. Before that, property ii) of Theorem 2.7.1, brings us to the following definition.

Definition 2.7.12. — *We say that a subset T of $\mathbb{R}^N$ is quasi-convex with constant $a \geq 1$, if T is star-shaped and $T + T \subset 2aT$.*

Let us note the following easy fact.

Claim 2.7.13. — *Let $0 < p < 1$, then $B_{p,\infty}^N$ and B_p^N are quasi-convex with constant $2^{(1/p)-1}$.*

We come up now with the main claim:

Claim 2.7.14. — *Let $0 < p < 1$ and $T = B_{p,\infty}^N$. Then $(1/\rho)T_\rho$ satisfies properties i) and ii) of Theorem 2.7.1 with*

$$\rho = C_p \left(\frac{n}{\log(cN/n)} \right)^{1/p-1/2}$$

where C_p depends only on p and $c > 0$ is an absolute constant.

If $T = B_1^N$, then $(1/\rho)T_\rho$ satisfies properties i) and ii) of Theorem 2.7.1 with

$$\rho = \left(\frac{c_1 n}{\log(c_2 N/n)} \right)^{1/2}$$

where c_1, c_2 are positive absolute constants.

Proof. — We consider only the case of $T = B_{p,\infty}^N$, $0 < p < 1$. The case of B_1^N is similar. Since the mechanism has already been developed in details, we will only indicate the different steps. Fix $\varepsilon_0 = 1/20$. To get i) we use Lemma 2.7.11 with $\varepsilon = \varepsilon_0/2$ and δ obtained from the equation $\varepsilon_0/2 = 2(2/p-1)^{-1/2}\delta^{1/p-1/2}$. Let $1 \leq m \leq N$. We get that $S_2(\Sigma_{\lceil m/\delta \rceil})$ is an $(\varepsilon_0/2)$-net of $m^{1/p-1/2}B_{p,\infty}^N \cap S^{N-1}$ with respect to the Euclidean metric. Set $m' = \lceil m/\delta \rceil$. By Claim 2.2.9, we have

$$N(S_2(\Sigma_{m'}), \frac{\varepsilon_0}{2} B_2^N) \leq \left(\frac{3eN}{m'(\varepsilon_0/2)} \right)^{m'} = \left(\frac{6eN}{m'\varepsilon_0} \right)^{m'}.$$

Thus, by the triangle inequality, we have

$$N(m^{1/p-1/2}B_{p,\infty}^N \cap S^{N-1}, \varepsilon_0 B_2^N) \leq \left(\frac{6eN}{m'\varepsilon_0} \right)^{m'}$$

so that

$$N(m^{1/p-1/2}B_{p,\infty}^N \cap S^{N-1}, \varepsilon_0 B_2^N) \leq \exp(c_0 n/2)$$

whenever

$$\left(\frac{6eN}{m'\varepsilon_0} \right)^{m'} \leq \exp(c_0 n/2).$$

Thus under this condition on m' (therefore on m), $m^{1/p-1/2}B_{p,\infty}^N \cap S^{N-1}$ satisfies i).

In order to tackle ii), recall that $B_{p,\infty}$ is quasi-convex with constant $2^{1/p-1}$ (Claim 2.7.13). By symmetry, we have

$$B_{p,\infty}^N - B_{p,\infty}^N \subset 2^{1/p} B_{p,\infty}^N.$$

Let $r = (1/p-1)m^{1/p-1/2}$. From Lemma 2.7.10, one has

$$rB_{p,\infty}^N \cap B_2^N \subset 2\,\mathrm{conv}\, S_2(\Sigma_m).$$

As we saw previously,

$$N(S_2(\Sigma_m), \frac{1}{2}\, B_2^N) \leq \left(\frac{3eN}{m(1/2)}\right)^m = \left(\frac{6eN}{m}\right)^m$$

and by Proposition 2.2.7 there exists a subset $\Lambda' \subset S^{N-1}$ with $|\Lambda'| \leq N(S_2(\Sigma_m), \frac{1}{2}\, B_2^N)$ such that $S_2(\Sigma_m) \subset 2\,\mathrm{conv}\,\Lambda'$. We arrive at

$$\begin{aligned}\varepsilon_0 2^{-1/p}\left(rB_{p,\infty}^N - rB_{p,\infty}^N\right) \cap \varepsilon_0 B_2^N &\subset \varepsilon_0\left(rB_{p,\infty}^N \cap B_2^N\right)\\ &\subset 4\varepsilon_0\,\mathrm{conv}\,\Lambda' \subset 2\,\mathrm{conv}\,(\varepsilon_0\Lambda' \cup -\varepsilon_0\Lambda').\end{aligned}$$

Therefore $\varepsilon_0 2^{-1/p} r B_{p,\infty}^N \cap S^{N-1}$ satisfies ii) whenever $(6eN/m)^m \leq \exp(c_0 n/2)$.

Finally $\varepsilon_0 2^{-1/p} r B_{p,\infty}^N \cap S^{N-1}$ satisfies i) and ii) whenever the two conditions on m are verified, that is when $cm\log(CN/m) \leq c_0 n/2$ where $c, C > 0$ are absolute constants. We compute m and r and set $\rho = \varepsilon_0 2^{-1/p} r$ to conclude. □

Now we can apply Corollary 2.7.8, to conclude

Theorem 2.7.15. — *Let $\mathbb{P}$ be a probability satisfying (2.8) on the space of $n \times N$ matrices and let $0 < p < 1$. There exist c_p depending only on p, c' depending on c_0 and an absolute constant c such that the set Ω of $n \times N$ matrices A satisfying*

$$\mathrm{rad}\left(\ker A \cap B_p^N\right) \leqslant \mathrm{rad}\left(\ker A \cap B_{p,\infty}^N\right) \leqslant c_p\left(\frac{\log(cN/n)}{n}\right)^{1/p-1/2}$$

has probability at least $1 - \exp(-c'n)$.

In particular, if $A \in \Omega$ and if $x', x \in B_{p,\infty}^n$ are such that $Ax' = Ax$ then

$$|x' - x|_2 \leqslant c_p'\left(\frac{\log(cN/n)}{n}\right)^{1/p-1/2}.$$

An analogous result holds for the ball B_1^N.

Remark 2.7.16. — *The estimate of Theorem 2.7.15 is optimal. In other words, for all $1 \leqslant n \leqslant N$,*

$$d^n(B_p^N, \ell_2^N) \sim_p \min\left(1, \frac{\log(N/n)+1}{n}\right)^{1/p-1/2}.$$

See the notes and comments at the end of this chapter.

2.8. An other complexity measure

In this last section, we introduce a new parameter $\ell_*(T)$ which is a gaussian *complexity measure* of a set $T \subset \mathbb{R}^N$. We define

$$\ell_*(T) = \mathbb{E} \sup_{t \in T} \left(\sum_{i=1}^{N} g_i t_i \right), \tag{2.17}$$

where $t = (t_i)_{i=1}^N \in T$ and $g_1, ..., g_N$ are independent $\mathcal{N}(0,1)$ Gaussian random variables. This parameter plays an important role in empirical processes (see Chapter 1) and in Geometry of Banach spaces.

Theorem 2.8.1. — *There exist absolute constants $c, c' > 0$ for which the following holds. Let $1 \le n \le N$. Let A be a Gaussian matrix with i.i.d. entries that are centered and variance one Gaussian random variables. Let $T \subset \mathbb{R}^N$ be a star-shaped set. Then, with probability at least $1 - \exp(-c'n)$,*

$$\mathrm{rad}\,(\ker A \cap T) \le c\,\ell_*(T)/\sqrt{n}.$$

Proof. — The plan of the proof consists first in proving a restricted isometry property for $\widetilde{T} = \frac{1}{\rho} T \cap S^{N-1}$ for some $\rho > 0$, then to argue as in Lemma 2.7.7. In a first part we consider an arbitrary subset $\widetilde{T} \subset S^{N-1}$. It will be specified in the last step.

Let $\delta \in (0,1)$. The restricted isometry property is proved using a discretization by a net argument and an approximation argument.

For any $\theta > 0$, let $\Lambda(\theta) \subset \widetilde{T}$ be a θ-net of $\widetilde{T}$ for the Euclidean metric. Let $\pi_\theta : \widetilde{T} \to \Lambda(\theta)$ be a mapping such that for every $t \in \widetilde{T}$, $|t - \pi_\theta(t)|_2 \leqslant \theta$. Let Y be a Gaussian random vector with the identity as covariance matrix. Note that because $\widetilde{T} \subset S^{N-1}$, one has $\mathbb{E}|\langle Y, t\rangle|^2 = 1$ for any $t \in \widetilde{T}$. By the triangle inequality, we have

$$\sup_{t \in \widetilde{T}} \left| \frac{|At|_2^2}{n} - \mathbb{E}|\langle Y, t\rangle|^2 \right| \leqslant \sup_{s \in \Lambda(\theta)} \left| \frac{|As|_2^2}{n} - \mathbb{E}|\langle Y, s\rangle|^2 \right| + \sup_{t \in \widetilde{T}} \left| \frac{|At|_2^2}{n} - \frac{|A\pi_\theta(t)|_2^2}{n} \right|.$$

– First step. *Entropy estimate via Sudakov minoration.* Let $s \in \Lambda(\theta)$. Let (Y_i) be the rows of A. Since $\langle Y, s\rangle$ is a standard Gaussian random variable, $|\langle Y, s\rangle|^2$ is a χ^2 random variable. By the definition of section 1.1 of Chapter 1, $|\langle Y, s\rangle|^2$ is ψ_1 with respect to some absolute constant. Thus Bernstein inequality from Theorem 1.2.7 of Chapter 1 applies and gives for any $0 < \delta < 1$,

$$\left| \frac{|As|_2^2}{n} - \mathbb{E}|\langle Y, s\rangle|^2 \right| = \left| \frac{1}{n} \sum_{1}^{n} (\langle Y_i, s\rangle^2 - \mathbb{E}|\langle Y, s\rangle|^2) \right| \leqslant \delta/2$$

with probability larger than $1 - 2\exp(-cn\delta^2)$, where $c > 0$ is a numerical constant. A union bound principle ensures that

$$\sup_{s \in \Lambda(\theta)} \left| \frac{|As|_2^2}{n} - \mathbb{E}|\langle Y, s\rangle|^2 \right| \leqslant \delta/2$$

holds with probability larger than $1 - 2\exp(-cn\delta^2 + \log|\Lambda(\theta)|)$.

From Sudakov inequality (1.14) (Theorem 1.4.4 of Chapter 1), there exists $c' > 0$ such that, if

$$\theta = c' \frac{\ell_*(\widetilde{T})}{\delta\sqrt{n}}$$

then $\log|\Lambda(\theta)| \leqslant cn\delta^2/2$. Therefore, for that choice of θ, the inequality

$$\sup_{s\in\Lambda(\theta)} \left| \frac{|As|_2^2}{n} - 1 \right| \leqslant \delta/2$$

holds with probability larger than $1 - 2\exp(-cn\delta^2/2)$.

– Second step. *The approximation term.* To begin with, observe that for any $s, t \in \widetilde{T}$, $\big||As|_2^2 - |At|_2^2\big| \leqslant |A(s-t)|_2\, |A(s+t)|_2 \leqslant |A(s-t)|_2\, (|As|_2 + |At|_2)$. Thus

$$\sup_{t\in\widetilde{T}} \big||At|_2^2 - |A\pi_\theta(t)|_2^2\big| \leqslant 2 \sup_{t\in\widetilde{T}(\theta)} |At|_2 \sup_{t\in\widetilde{T}} |At|_2$$

where $\widetilde{T}(\theta) = \{s - t\,;\, s, t \in \widetilde{T}, |s-t|_2 \leqslant \theta\}$. In order to estimate these two norms of the matrix A, we consider a $(1/2)$-net of S^{n-1}. According to Proposition 2.2.7, there exists such a net $\mathcal{N}$ with cardinality not larger than 5^n and such that $B_2^n \subset 2\,\mathrm{conv}(\mathcal{N})$. Therefore

$$\sup_{t\in\widetilde{T}} |At|_2 = \sup_{t\in\widetilde{T}} \sup_{|u|_2\leqslant 1} \langle At, u\rangle \leqslant 2 \sup_{u\in\mathcal{N}} \sup_{t\in\widetilde{T}} \langle t, A^\top u\rangle.$$

Since A is a standard Gaussian matrix with i.i.d. entries, centered and with variance one, for every $u \in \mathcal{N}$, $A^\top u$ is a standard Gaussian vector and

$$\mathbb{E} \sup_{t\in\widetilde{T}} \langle t, A^\top u\rangle = \ell_*(\widetilde{T}).$$

It follows from Theorem 1.4.7 of Chapter 1 that for any fixed $u \in \mathcal{N}$,

$$\forall z > 0 \qquad \mathbb{P}\left(\left| \sup_{t\in\widetilde{T}} \langle t, A^\top u\rangle - \mathbb{E} \sup_{t\in\widetilde{T}} \langle t, A^\top u\rangle \right| > z \right) \leq 2\exp\left(-c'' z^2/\sigma^2(\widetilde{T})\right)$$

for some numerical constant c'', where $\sigma(\widetilde{T}) = \sup_{t\in\widetilde{T}}\{\big(\mathbb{E}|\langle t, A^\top u\rangle|^2\big)^{1/2}\}$.

Combining a union bound inequality and the estimate on the cardinality of the net, we get

$$\forall z > 0 \quad \mathbb{P}\left(\sup_{u\in\mathcal{N}} \sup_{t\in\widetilde{T}} \langle A^\top u, t\rangle \geq \ell_*(\widetilde{T}) + z\sigma(\widetilde{T})\sqrt{n} \right) \leq 2\exp\left(-c'' n(\,z^2 - \log 5\,)\right).$$

We deduce that

$$\sup_{t\in\widetilde{T}} |At|_2 \leqslant 2\left(\ell_*(\widetilde{T}) + z\sigma(\widetilde{T})\sqrt{n}\right)$$

with probability larger than $1 - 2\exp\left(-c'' n(\,z^2 - \log 5\,)\right)$. Observe that because $\widetilde{T} \subset S^{N-1}$, one has $\sigma(\widetilde{T}) = 1$.

This reasoning applies as well to $\widetilde{T}(\theta)$, but notice that now $\sigma(\widetilde{T}(\theta)) \leqslant \theta$ and because of the symmetry of the Gaussian random variables, $\ell_*(\widetilde{T}(\theta)) \leqslant 2\ell_*(\widetilde{T})$. Therefore,

$$\sup_{t\in\widetilde{T}} \big||At|_2^2 - |A\pi_\theta(t)|_2^2\big| \leq 8\left(\ell_*(\widetilde{T}) + z\sqrt{n}\right)\left(2\ell_*(\widetilde{T}) + z\theta\sqrt{n}\right)$$

with probability larger than $1 - 4\exp\left(-c''n(\,z^2 - \log 5\,)\right)$.

– Third step. *The restricted isometry property.* Set $z = \sqrt{2\log 5}$, say, and recall that $\delta < 1$. Plugging the value of θ from step one, we get that with probability larger than $1 - 2\exp(-c\,n\delta^2/2) - 4\exp(-c''nz^2/2)$,

$$\sup_{t\in\widetilde{T}} \left| |At|_2^2 - |A\pi_\theta(t)|_2^2 \right| \leqslant 8\left(\ell_*(\widetilde{T}) + z\sqrt{n}\right)\left(2\ell_*(\widetilde{T}) + zc'\frac{\ell_*(\widetilde{T})}{\delta}\right)$$

and

$$\sup_{t\in\widetilde{T}} \left| \frac{|At|_2^2}{n} - 1 \right| \leqslant \frac{\delta}{2} + c'''\left(\frac{\ell_*(\widetilde{T})}{\sqrt{n}} + z\right)\frac{\ell_*(\widetilde{T})}{\delta\sqrt{n}}$$

for some new constant c'''. It is now clear that one can choose c'''' such that, whenever

$$\ell_*(\widetilde{T}) \leqslant c''''\delta^2\sqrt{n}$$

then

$$\sup_{t\in\widetilde{T}} \left| \frac{|At|_2^2}{n} - 1 \right| \leqslant \delta$$

with probability larger than $1 - 2\exp(-c\,n\delta^2/2) - 4\exp(-c''nz^2/2)$.

– Last step. *Estimating the width.* Let $\rho > 0$ be a parameter. We apply the previous estimate with $\delta = 1/2$ to the subset $\widetilde{T} = \frac{1}{\rho}T \cap S^{N-1}$ of the unit sphere. Because $\delta = 1/2$, $At \neq 0$ whenever $\left|\frac{|At|_2^2}{n} - 1\right| \leqslant \delta$. Therefore, with the above probability,

$$\ker A \cap \left(\frac{1}{\rho}T \cap S^{N-1}\right) = \emptyset$$

whenever ρ satisfies the inequality

$$\ell_*\left(\frac{1}{\rho}T \cap S^{N-1}\right) < c''''\delta^2\sqrt{n}.$$

Since $\ell_*\left(\frac{1}{\rho}T \cap S^{N-1}\right) \leqslant \frac{\ell_*(T)}{\rho}$, the previous inequality is satisfied whenever

$$\frac{\ell_*(T)}{\rho} < c''''\delta^2\sqrt{n}.$$

The conclusion follows from Lemma 2.7.7.

□

Remark 2.8.2. — *The proof of Theorem 2.8.1 generalizes to the case of a matrix with independent sub-Gaussian rows. Only the second step has to be modified by using the majorizing measure theorem which precisely allows to compare deviation inequalities of supremum of sub-Gaussian processes to their equivalent in the Gaussian case. We will not give here the proof of this result, see Theorem 3.2.1 in Chapter 3, where an other approach is developed.*

We show now how Theorem 2.8.1 applies to some sets T.

Corollary 2.8.3. — *There exist absolute constants $c, c' > 0$ such that the following holds. Let $1 \leqslant n \leqslant N$ and let A be as in Theorem 2.8.1. Let $\lambda > 0$. Let $T \subset S^{N-1}$ and assume that $T \subset 2\operatorname{conv}\Lambda$ for some $\Lambda \subset B_2^N$ with $|\Lambda| \leq \exp(\lambda^2 n)$. Then with probability at least $1 - \exp(-c'n)$,*

$$\operatorname{rad}(\ker A \cap T) \leq c\lambda.$$

Proof. — The main point in the proof is that if $T \subset 2\operatorname{conv}\Lambda$, $\Lambda \subset B_2^N$ and if we have a reasonable control of $|\Lambda|$, then $\ell_*(T)$ can be bounded from above. The rest is a direct application of Theorem 2.8.1. Let $c, c' > 0$ be constants from Theorem 2.8.1. It is well-known (see Chapter 3) that there exists an absolute constant $c'' > 0$ such that for every $\Lambda \subset B_2^N$,

$$\ell_*(\operatorname{conv}\Lambda) = \ell_*(\Lambda) \leqslant c'' \sqrt{\log(|\Lambda|)}\,,$$

and since $T \subset 2\operatorname{conv}\Lambda$,

$$\ell_*(T) \leq 2\ell_*(\operatorname{conv}\Lambda) \leqslant 2c'' \left(\lambda^2 n\right)^{1/2}.$$

The conclusion follows from Theorem 2.8.1. □

2.9. Notes and comments

For further information on the origin and the genesis of compressed sensing and on the ℓ_1-minimization method, the reader may consult the articles by D. Donoho [**Don06**], E. Candes, J. Romberg and T. Tao [**CRT06**] and E. Candes and T. Tao [**CT06**]. For further and more advanced studies on compressed sensing, see the book [**FR11**].

Proposition 2.2.16 is due to D. Donoho [**Don05**]. Proposition 2.2.18 and its proof is a particular case of a more general result from [**FPRU11**]. See also [**LN06**] where the analogous problem for neighborliness is studied.

The definition 2.3.1 of the Restricted Isometry Property was introduced in [**CT05**] and plays an important role in compressed sensing. The relevance of the Restricted Isometry parameter for the reconstruction property was for instance revealed in [**CT06**], [**CT05**], where it was shown that if

$$\delta_m(A) + \delta_{2m}(A) + \delta_{3m}(A) < 1$$

then the encoding matrix A has the exact reconstruction property of order m. This result was improved in [**Can08**] to $\delta_{2m}(A) < \sqrt{2} - 1$ as stated in Theorem 2.3.2. This constant $\sqrt{2} - 1$ was recently improved in [**FL09**]. In the same paper these authors introduced the parameter γ_p from Definition 2.3.3.

The proofs of results of Section 2.4 are following lines from [**CT05**], [**CDD09**], [**FL09**], [**FPRU11**] and [**KT07**]. Relation (2.5) was proved in [**FL09**] with a better numerical constant. Theorem 2.5.2 from [**GG84**] gives the optimal behavior of the Gelfand widths of the cross-polytope. This completes a celebrated result of B. Kashin [**Kas77**] which was proved using Kolmogorov widths (dual to the Gelfand widths) and with a non-optimal power of the logarithm (power 3/2 instead of 1/2 later improved in [**GG84**]). The upper bound of Kolmogorov widths was obtained via random matrices with i.i.d. Bernoulli entries, whereas [**Glu83**] and [**GG84**] used properties of random Gaussian matrices.

The simple proof of Theorem 2.6.5 stating that subgaussian matrices satisfy the exact reconstruction property of order m by ℓ_1-minimization with large m is taken from [**BDDW08**] and [**MPTJ08**]. The strategy of this proof is very classical in Approximation Theory, see [**Kas77**] and in Banach space theory where it has played an important role in quantitative version of Dvoretsky's theorem on almost spherical sections, see [**FLM77**] and [**MS86**].

Section 2.7 follows the lines of [**MPTJ08**]. Proposition 2.7.3 from [**KT07**] is stated in terms of Gelfand width rather than in terms of constants of isometry as in [**Can08**] and [**CDD09**]. The principle of reducing the computation of Gelfand widths by truncation as stated in Subsection 2.7 goes back to [**Glu83**]. The optimality of the estimates of Theorem 2.7.15 as stated in Remark 2.7.16 is a result of [**FPRU11**]. The parameter $\ell_*(T)$ defined in Section 2.8 plays an important role in Geometry of Banach spaces (see [**Pis89**]). Theorem 2.8.1 is from [**PTJ86**].

The restricted isometry property for the model of partial discrete Fourier matrices will be studied in Chapter 5. There exists many other interesting models of random sensing matrices (see [**FR11**]). Random matrices with i.i.d. entries satisfying uniformly a sub-exponential tail inequality or with i.i.d. columns with log-concave density, the so-called log-concave Ensemble, have been studied in [**ALPTJ10**] and in [**ALPTJ11**] where it was shown that they also satisfy a RIP with $m \sim n/\log^2(2N/n)$.

CHAPTER 3

INTRODUCTION TO CHAINING METHODS

The restricted isometry property has been introduced in Chapter 2 in order to provide a simple way of showing that some matrices satisfy an exact reconstruction property. Indeed, if A is a $n \times N$ matrix such that for every $2m$-sparse vector $x \in \mathbb{R}^N$,

$$(1 - \delta_{2m})|x|_2^2 \leqslant |Ax|_2^2 \leqslant (1 + \delta_{2m})|x|_2^2$$

where $\delta_{2m} < \sqrt{2} - 1$ then A satisfies the exact reconstruction property of order m by ℓ_1-minimization (cf. Chapter 2). In particular, if A is a random matrix with row vectors $n^{-1/2}Y_1, \ldots, n^{-1/2}Y_n$, this property can be translated in terms of an empirical processes property since

$$\delta_{2m} = \sup_{x \in S_2(\Sigma_{2m})} \Big| \frac{1}{n} \sum_{i=1}^{n} \langle Y_i, x \rangle^2 - 1 \Big|. \tag{3.1}$$

If we show an upper bound on the supremum (3.1) smaller than $\sqrt{2} - 1$, this will prove that A has the exact reconstruction property of order m by ℓ_1-minimization. In Chapter 2, it was shown that matrices from the subgaussian Ensemble satisfy the restricted isometry property (with high probability) thanks to a technique called the epsilon-net argument. In this chapter, we present a technique called the *chaining method* in order to obtain upper bounds on the supremum of stochastic processes. Upper bounds on the supremum (3.1) may follow from such chaining methods.

3.1. The chaining method

The chaining mechanism is a technique used to obtain upper bounds on the supremum $\sup_{t \in T} X_t$ of a stochastic process $(X_t)_{t \in T}$ indexed by a set T. These upper bounds are usually expressed in terms of some metric complexity measure of T.

One key idea behind the chaining method is the trade-off between the deviation or concentration estimates of the increments of the process $(X_t)_{t \in T}$ and the complexity of T which is endowed with a metric structure connected with $(X_t)_{t \in T}$.

As an introduction, we show an upper bound on the supremum $\sup_{t \in T} X_t$ in terms of an entropy integral known as the *Dudley entropy integral*. This entropy integral is based on some metric quantities of T that were introduced in Chapter 1 and that we recall now.

Definition 3.1.1. — *Let (T, d) be a semi-metric space, that is for every x, y and z in T, $d(x, y) = d(y, x)$ and $d(x, y) \leqslant d(x, z) + d(z, y)$. For $\varepsilon > 0$, the ε-covering number $N(T, d, \varepsilon)$ of (T, d) is the minimal number of open balls for the semi-metric d of radius ε needed to cover T. The metric entropy is the logarithm of the ε-covering number, as a function of ε.*

We develop the chaining argument under a subgaussian assumption on the increments of the process $(X_t)_{t\in T}$ saying that for every $s, t \in T$ and $u > 0$,

$$\mathbb{P}\Big[|X_s - X_t| > ud(s,t)\Big] \leqslant 2\exp(-u^2/2), \tag{3.2}$$

where d is a semi-metric on T. To avoid some technical complications that are less important from our point of view, we only consider processes indexed by finite sets T. To handle more general sets one may study the random variable $\sup_{T'\subset T : T' \text{ finite}} \sup_{t\in T'} X_t$ or the supremum $\sup_{T'\subset T : T' \text{ finite}} \mathbb{E}\sup_{t,s\in T'} |X_t - X_s|$ which are equal to $\sup_{t\in T} X_t$ and $\mathbb{E}\sup_{t,s\in T} |X_t - X_s|$ respectively under suitable separability conditions on T.

Theorem 3.1.2. — *There exist absolute constants c_0, c_1, c_2 and c_3 for which the following holds. Let (T, d) be a semi-metric space and assume that $(X_t)_{t\in T}$ is a stochastic process satisfying (3.2). Then, for every $v \geqslant c_0$, with probability greater than $1 - c_1 \exp(-c_2 v^2)$, one has*

$$\sup_{s,t\in T} |X_t - X_s| \leqslant c_3 v \int_0^\infty \sqrt{\log N(T, d, \varepsilon)}\ d\varepsilon.$$

In particular,

$$\mathbb{E} \sup_{s,t\in T} |X_t - X_s| \leqslant c_3 \int_0^\infty \sqrt{\log N(T, d, \varepsilon)}\ d\varepsilon.$$

Proof. — Put $\eta_{-1} = \operatorname{rad}(T, d)$ and for every integer $i \geqslant 0$ set

$$\eta_i = \inf\big\{\eta > 0 : N(T, d, \eta) \leqslant 2^{2^i}\big\}.$$

Let $(T_i)_{i\geqslant 0}$ be a sequence of subsets of T defined as follows. Take T_0 as a subset of T containing only one element. Then, for every $i \geqslant 0$, by definition of η_i (note that the infimum is not necessarily achieved), it is possible to take T_{i+1} as a subset of T of cardinality smaller than $2^{2^{i+1}}$ such that

$$T \subset \bigcup_{x\in T_{i+1}} \Big(x + \eta_i B_d\Big),$$

where B_d is the unit ball associated with the semi-metric d. For every $t \in T$ and integer i, put $\pi_i(t)$ a nearest point to t in T_i (that is $\pi_i(t)$ is some point in T_i such that $d(t, \pi_i(t)) = \min_{s\in T_i} d(t, s)$). In particular, $d(t, \pi_i(t)) \leqslant \eta_{i-1}$.

Since T is finite, then for every $t \in T$, one has

$$X_t - X_{\pi_0(t)} = \sum_{i=0}^{\infty} \Big(X_{\pi_{i+1}(t)} - X_{\pi_i(t)} \Big). \tag{3.3}$$

Let $i \in \mathbb{N}$ and $t \in T$. By the subgaussian assumption (3.2), for every $u > 0$, with probability greater than $1 - 2\exp(-u^2)$,

$$|X_{\pi_{i+1}(t)} - X_{\pi_i(t)}| \leqslant ud(\pi_{i+1}(t), \pi_i(t)) \leqslant u(\eta_{i-1} + \eta_i) \leqslant 2u\eta_{i-1}. \tag{3.4}$$

To get this result uniformly over every link $(\pi_{i+1}(t), \pi_i(t))$ for $t \in T$ at level i, we use an union bound (note that there are at most $|T_{i+1}||T_i| \leqslant 2^{2^{i+2}}$ such links): with probability greater than $1 - 2|T_{i+1}||T_i|\exp(-u^2) \geqslant 1 - 2\exp\big(2^{i+2}\log 2 - u^2\big)\big)$, for every $t \in T$, one has

$$|X_{\pi_{i+1}(t)} - X_{\pi_i(t)}| \leqslant 2u\eta_{i-1}.$$

To balance the "complexity" of the set of "links" with our deviation estimate, we take $u = v2^{i/2}$, where $v \geqslant \sqrt{8\log 2}$. Thus, for the level i, we obtain with probability greater than $1 - 2\exp\big(- v^2 2^{i-1}\big)$, for all $t \in T$,

$$|X_{\pi_{i+1}(t)} - X_{\pi_i(t)}| \leqslant 2v2^{i/2}\eta_{i-1},$$

for every v larger than an absolute constant.

Using (3.3) and summing over $i \in \mathbb{N}$, we have with probability greater than $1 - 2\sum_{i=0}^{\infty} \exp\big(- v^2 2^{i-1}\big) \geqslant 1 - c_1\exp(-c_2 v^2)$, for every $t \in T$,

$$|X_t - X_{\pi_0(t)}| \leqslant 2v \sum_{i=0}^{\infty} 2^{i/2}\eta_{i-1} = 2^{3/2} v \sum_{i=-1}^{\infty} 2^{i/2}\eta_i. \tag{3.5}$$

Observe that if $i \in \mathbb{N}$ and $\eta < \eta_i$ then $N(T, d, \eta) > 2^{2^i}$. Therefore, one has

$$\sqrt{\log(1 + 2^{2^i})}(\eta_i - \eta_{i+1}) \leqslant \int_{\eta_{i+1}}^{\eta_i} \sqrt{\log N(T, d, \eta)}d\eta,$$

and since $\log(1 + 2^{2^i}) \geqslant 2^i \log 2$, summing over all $i \geqslant -1$, we get

$$\sqrt{\log 2} \sum_{i=-1}^{\infty} 2^{i/2}(\eta_i - \eta_{i+1}) \leqslant \int_0^{\eta_{-1}} \sqrt{\log N(T, d, \eta)}d\eta$$

and

$$\sum_{i=-1}^{\infty} 2^{i/2}(\eta_i - \eta_{i+1}) = \sum_{i=-1}^{\infty} 2^{i/2}\eta_i - \sum_{i=0}^{\infty} 2^{(i-1)/2}\eta_i \geqslant \Big(1 - \frac{1}{\sqrt{2}}\Big) \sum_{i=-1}^{\infty} 2^{i/2}\eta_i.$$

This proves that

$$\sum_{i=-1}^{\infty} 2^{i/2}\eta_i \leqslant c_3 \int_0^{\infty} \sqrt{\log N(T, d, \eta)}d\eta. \tag{3.6}$$

We conclude that, for every $v \geqslant \sqrt{8\log 2}$, with probability greater than $1 - c_1\exp(-c_2 v^2)$, we have

$$\sup_{t \in T} |X_t - X_{\pi_0(t)}| \leqslant c_4 v \int_0^{\infty} \sqrt{\log N(T, d, \eta)}d\eta.$$

By integrating the tail estimate, we obtain

$$\mathbb{E}\sup_{t\in T}|X_t - X_{\pi_0(t)}| = \int_0^\infty \mathbb{P}\Big[\sup_{t\in T}|X_t - X_{\pi_0(t)}| > u\Big]du$$
$$\leqslant c_5 \int_0^\infty \sqrt{\log N(T,d,\varepsilon)}d\varepsilon.$$

Finally, since $|T_0| = 1$, it follows that, for every $t, s \in T$,

$$|X_t - X_s| \leqslant |X_t - X_{\pi_0(t)}| + |X_s - X_{\pi_0(s)}|$$

and the theorem is shown. □

In the case of a stochastic process with subgaussian increments (cf. condition (3.2)), the entropy integral

$$\int_0^\infty \sqrt{\log N(T,d,\varepsilon)}d\varepsilon$$

is called the *Dudley entropy integral*. Note that the subgaussian assumption (3.2) is equivalent to a ψ_2 control on the increments: $\|X_s - X_t\|_{\psi_2} \leqslant d(s,t), \forall s,t \in T$. It follows from the maximal inequality 1.1.3 and the chaining argument used in the previous proof that the following equivalent formulation of Theorem 3.1.2 holds:

$$\Big\|\sup_{s,t\in T}|X_s - X_t|\Big\|_{\psi_2} \leqslant c\int_0^\infty \sqrt{\log N(T,d,\epsilon)}d\epsilon.$$

A careful look at the previous proof reveals one potential source of looseness. At each level of the chaining mechanism, we used a uniform bound (depending only on the level) to control each link. Instead, one can use "individual" bounds for every link rather than the worst at every level. This idea is the basis of what is now called the *generic chaining*. The natural metric complexity measure coming from this method is the γ_2-functional which is now introduced.

Definition 3.1.3. — *Let (T,d) be a semi-metric space. A sequence $(T_s)_{s\geqslant 0}$ of subsets of T is said to be admissible if $|T_0| = 1$ and $1 \leqslant |T_s| \leqslant 2^{2^s}$ for every $s \geqslant 1$. The γ_2-functional of (T,d) is*

$$\gamma_2(T,d) = \inf_{(T_s)}\sup_{t\in T}\Big(\sum_{s=0}^\infty 2^{s/2}d(t,T_s)\Big)$$

where the infimum is taken over all admissible sequences $(T_s)_{s\in\mathbb{N}}$ and $d(t,T_s) = \min_{y\in T_s} d(t,y)$ for every $t \in T$ and $s \in \mathbb{N}$.

We note that the γ_2-functional is upper bounded by the Dudley entropy integral:

$$\gamma_2(T,d) \leqslant c_0\int_0^\infty \sqrt{\log N(T,d,\varepsilon)}d\varepsilon, \tag{3.7}$$

where c_0 is an absolute positive constant. Indeed, we construct an admissible sequence $(T_s)_{s\in\mathbb{N}}$ in the following way: let T_0 be a subset of T containing one element and for every $s \in \mathbb{N}$, let T_{s+1} be a subset of T of cardinality smaller than $2^{2^{s+1}}$ such that for every $t \in T$ there exists $x \in T_{s+1}$ satisfying $d(t,x) \leqslant \eta_s$, where η_s is defined by

$$\eta_s = \inf\big(\eta > 0 : N(T,d,\eta) \leqslant 2^{2^s}\big).$$

Inequality (3.7) follows from (3.6) and

$$\sup_{t\in T}\Big(\sum_{s=0}^{\infty} 2^{s/2} d(t,T_s)\Big) \leqslant \sum_{s=0}^{\infty} 2^{s/2}\sup_{t\in T} d(t,T_s) \leqslant \sum_{s=0}^{\infty} 2^{s/2}\eta_{s-1},$$

where $\eta_{-1} = \mathrm{rad}(T,d)$.

Now, we apply the generic chaining mechanism to show an upper bound on the supremum of processes whose increments satisfy the subgaussian assumption (3.2).

Theorem 3.1.4. — *There exist absolute constants c_0, c_1, c_2 and c_3 such that the following holds. Let (T,d) be a semi-metric space. Let $(X_t)_{t\in T}$ be a stochastic process satisfying the subgaussian condition (3.2). For every $v \geqslant c_0$, with probability greater than $1 - c_1\exp(-c_2 v^2)$,*

$$\sup_{s,t\in T} |X_t - X_s| \leqslant c_3 v \gamma_2(T,d)$$

and

$$\mathbb{E}\sup_{s,t\in T} |X_t - X_s| \leqslant c_3 \gamma_2(T,d).$$

Proof. — Let $(T_s)_{s\in\mathbb{N}}$ be an admissible sequence. For every $t \in T$ and $s \in \mathbb{N}$ denote by $\pi_s(t)$ a point in T_s such that $d(t,T_s) = d(t,\pi_s(t))$. Since T is finite, we can write for every $t \in T$,

$$|X_t - X_{\pi_0(t)}| \leqslant \sum_{s=0}^{\infty} |X_{\pi_{s+1}(t)} - X_{\pi_s(t)}|. \tag{3.8}$$

Let $s \in \mathbb{N}$. For every $t \in T$ and $v > 0$, with probability greater than $1 - 2\exp(-2^{s-1}v^2)$, one has

$$|X_{\pi_{s+1}(t)} - X_{\pi_s(t)}| \leqslant v 2^{s/2} d(\pi_{s+1}(t), \pi_s(t)).$$

We extend the last inequality to every link of the chains at level s by using an union bound (in the same way as in the proof of Theorem 3.1.2): for every $v \geqslant c_1$, with probability greater than $1 - 2\exp(-c_2 2^s v^2)$, for every $t \in T$, one has

$$|X_{\pi_{s+1}(t)} - X_{\pi_s(t)}| \leqslant v 2^{s/2} d(\pi_{s+1}(t), \pi_s(t)).$$

An union bound on every level $s \in \mathbb{N}$ yields: for every $v \geqslant c_1$, with probability greater than $1 - 2\sum_{s=0}^{\infty}\exp(-c_2 2^s v^2)$, for every $t \in T$,

$$|X_t - X_{\pi_0(t)}| \leqslant v\sum_{s=0}^{\infty} 2^{s/2} d(\pi_s(t), \pi_{s+1}(t)) \leqslant c_3 v \sum_{s=0}^{\infty} 2^{s/2} d(t,T_s).$$

The claim follows since the sum in the last probability estimate is comparable to its first term. □

Note that, by using the maximal inequality 1.1.3 and the previous generic chaining argument, we get the following equivalent formulation of Theorem 3.1.4: under the same assumption as in Theorem 3.1.4, we have

$$\left\| \sup_{s,t\in T} |X_s - X_t| \right\|_{\psi_2} \leqslant c\gamma_2(T,d).$$

For Gaussian processes, the upper bound in expectation obtained in Theorem 3.1.4 is sharp up to some absolute constants. This deep result, called the *Majorizing measure theorem*, makes an equivalence between two different quantities measuring the complexity of a set $T \subset \mathbb{R}^N$:

1. a metric complexity measure given by the γ_2 functional

   $$\gamma_2(T,\ell_2^N) = \inf_{(T_s)} \sup_{t\in T} \sum_{s=0}^{\infty} 2^{s/2} d_{\ell_2^N}(t,T_s),$$

   where the infimum is taken over all admissible sequences $(T_s)_{s\in\mathbb{N}}$ of T;
2. a probabilistic complexity measure given by the expectation of the supremum of the canonical Gaussian process indexed by T:

   $$\ell_*(T) = \mathbb{E} \sup_{t\in T} \sum_{i=1}^{N} g_i t_i,$$

   where $g_1,\dots,g_N$ are N i.i.d. standard Gaussian variables.

Theorem 3.1.5 **(Majorizing measure Theorem)**. — *There exist two absolute positive constants c_0 and c_1 such that for every countable subset T of $\mathbb{R}^N$, we have*

$$c_0\gamma_2(T,\ell_2^N) \leqslant \ell_*(T) \leqslant c_1\gamma_2(T,\ell_2^N).$$

3.2. An example of a more sophisticated chaining argument

In this section, we show upper bounds on the supremum

$$\sup_{f\in F} \left| \frac{1}{n}\sum_{i=1}^{n} f^2(X_i) - \mathbb{E}f^2(X) \right|, \tag{3.9}$$

where $X_1,\dots,X_n$ are n i.i.d. random variables with values in a measurable space $\mathcal{X}$ and F is a class of real-valued functions defined on $\mathcal{X}$. Once again and for the sake of simplicity, we consider only finite classes F. Results can be extended beyond the finite case under suitable separability conditions on F.

In Chapter 2, such a bound was used to show the restricted isometry property in Theorem 2.7.1. In this example, the class F is a class of linear functions indexed by a set of sparse vectors and was not, in particular, uniformly bounded.

In general, when $\|F\|_\infty = \sup_{f\in F} \|f\|_{L_\infty(\mu)} < \infty$, a bound on (3.9) follows from a symmetrization argument combined with the contraction principle. In the present study, we do not want to use a uniform bound on F but only that F has a finite diameter in $L_{\psi_2(\mu)}$ where μ is the probability distribution of the X_i's. This means that the norm (cf. Definition 1.1.1)

$$\|f\|_{\psi_2(\mu)} = \|f(X)\|_{\psi_2} = \inf\Big(c > 0 : \mathbb{E}\exp\big(|f(X)|^2/c^2\big) \leqslant e\Big)$$

is uniformly bounded on F where X is distributed according to μ. We denote this bound by α and thus we assume that

$$\alpha = \operatorname{rad}(F, \psi_2(\mu)) = \sup_{f \in F} \|f\|_{\psi_2(\mu)} < \infty. \tag{3.10}$$

In terms of random variables, Assumption (3.10) means that for all $f \in F$, $f(X)$ has a subgaussian behaviour and its ψ_2 norm is uniformly bounded over F.

Under (3.10), we can apply the classical generic chaining mechanism and obtain a bound on (3.9). Indeed, denote by $(X_f)_{f\in F}$ the empirical process defined by $X_f = n^{-1}\sum_{i=1}^n f^2(X_i) - \mathbb{E}f^2(X)$ for every $f \in F$. Assume that for every f and g in F, $\mathbb{E}f^2(X) = \mathbb{E}g^2(X)$. Then, the increments of the process $(X_f)_{f\in F}$ are

$$X_f - X_g = \frac{1}{n}\sum_{i=1}^n \big(f^2(X_i) - g^2(X_i)\big)$$

and we have (cf. Chapter 1)

$$\big\|f^2 - g^2\big\|_{\psi_1(\mu)} \leqslant \|f+g\|_{\psi_2(\mu)} \|f-g\|_{\psi_2(\mu)} \leqslant 2\alpha \|f-g\|_{\psi_2(\mu)}. \tag{3.11}$$

In particular, the increment $X_f - X_g$ is a sum of i.i.d. mean-zero ψ_1 random variables. Hence, the concentration properties of the increments of $(X_f)_{f\in F}$ follow from Theorem 1.2.7. Provided that for some $f_0 \in F$, we have $X_{f_0} = 0$ (for instance if F contains a constant function f_0) or $(X_f)_{f\in F}$ is a symmetric process then running the classical generic chaining mechanism with this increment condition yields the following: for every $u \geqslant c_0$, with probability greater than $1 - c_1\exp(-c_2 u)$, one has

$$\sup_{f\in F}\left|\frac{1}{n}\sum_{i=1}^n f^2(X_i) - \mathbb{E}f^2(X)\right| \leqslant c_3 u\alpha\left(\frac{\gamma_2(F,\psi_2(\mu))}{\sqrt{n}} + \frac{\gamma_1(F,\psi_2(\mu))}{n}\right) \tag{3.12}$$

for some absolute positive constants c_0, c_1, c_2 and c_3 and with

$$\gamma_1(F, \psi_2(\mu)) = \inf_{(F_s)}\sup_{f\in F}\Big(\sum_{s=0}^{\infty} 2^s d_{\psi_2(\mu)}(f, F_s)\Big)$$

where the infimum is taken over all admissible sequences $(F_s)_{s\in\mathbb{N}}$ and $d_{\psi_2(\mu)}(f, F_s) = \min_{g\in F_s}\|f-g\|_{\psi_2(\mu)}$ for every $f \in F$ and $s \in \mathbb{N}$. Result (3.12) can be derived from theorem 1.2.7 of [**Tal05**].

In some cases, computing $\gamma_1(F, d)$ for some metric d may be difficult and only weak estimates can be shown. Getting upper bounds on (3.9) which does not require the computation of $\gamma_1(F, \psi_2(\mu))$ may be of importance. In particular, upper bounds depending only on $\gamma_2(F, \psi_2(\mu))$ can be useful when the metrics $L_{\psi_2}(\mu)$ and $L_2(\mu)$ are equivalent on F because of the Majorizing measure theorem (cf. Theorem 3.1.5). In the next result, we show an upper bound on the supremum (3.9) depending only on the $\psi_2(\mu)$ diameter of F and on the complexity measure $\gamma_2(F, \psi_2(\mu))$.

Theorem 3.2.1. — *There exists absolute constants c_0, c_1, c_2 and c_3 such that the following holds. Let F be a finite class of real-valued functions in $\mathcal{S}(L_2(\mu))$, the unit sphere of $L_2(\mu)$, and denote by α the diameter* $\mathrm{rad}(F, \psi_2(\mu))$. *Then, with probability at least* $1 - c_1 \exp\Big(-(c_2/\alpha^2) \min\Big(n\alpha^2, \gamma_2(F, \psi_2(\mu))^2\Big)\Big)$,

$$\sup_{f\in F} \left| \frac{1}{n}\sum_{i=1}^n f^2(X_i) - \mathbb{E} f^2(X) \right| \leqslant c_3 \max\left(\alpha \frac{\gamma_2(F,\psi_2(\mu))}{\sqrt{n}}, \frac{\gamma_2(F,\psi_2(\mu))^2}{n} \right).$$

Moreover, if F is a symmetric subset of $\mathcal{S}(L_2(\mu))$ then,

$$\mathbb{E}\sup_{f\in F} \left| \frac{1}{n}\sum_{i=1}^n f^2(X_i) - \mathbb{E} f^2(X) \right| \leqslant c_3 \max\left(\alpha \frac{\gamma_2(F,\psi_2(\mu))}{\sqrt{n}}, \frac{\gamma_2(F,\psi_2(\mu))^2}{n} \right).$$

To show Theorem 3.2.1, we introduce the following notation. For every $f \in L_2(\mu)$, we set

$$Z(f) = \frac{1}{n}\sum_{i=1}^n f^2(X_i) - \mathbb{E} f^2(X) \text{ and } W(f) = \Big(\frac{1}{n}\sum_{i=1}^n f^2(X_i)\Big)^{1/2}. \tag{3.13}$$

For the sake of shortness, in what follows, L_2, ψ_2 and ψ_1 stand for $L_2(\mu)$, $\psi_1(\mu)$ and $\psi_2(\mu)$, for which we omit to write the probability measure μ.

To obtain upper bounds on the supremum (3.9) we study the deviation behaviour of the increments of the underlying process. Namely, we need deviation results for $Z(f) - Z(g)$ for $f, g \in F$. Since the "end of the chains" will be analysed by different means, the deviation behaviour of the increments $W(f-g)$ will be of importance as well.

Lemma 3.2.2. — *There exists an absolute constant C_1 such that the following holds. Let $F \subset \mathcal{S}(L_2(\mu))$ and $\alpha = \mathrm{rad}(F, \psi_2)$. For every $f, g \in F$, we have:*

1. *for every $u \geqslant 2$,*
$$\mathbb{P}\Big[W(f-g) \geqslant u \left\|f-g\right\|_{\psi_2}\Big] \leqslant 2\exp\big(-C_1 n u^2\big)$$
2. *for every $u > 0$,*
$$\mathbb{P}\Big[|Z(f) - Z(g)| \geqslant u\alpha \left\|f-g\right\|_{\psi_2}\Big] \leqslant 2\exp\big(-C_1 n \min(u, u^2)\big)$$
and
$$\mathbb{P}\Big[|Z(f)| \geqslant u\alpha^2\Big] \leqslant 2\exp\big(-C_1 n \min(u, u^2)\big).$$

Proof. — Let $f, g \in F$. Since $f, g \in L_{\psi_2}$, we have $\left\|(f-g)^2\right\|_{\psi_1} = \left\|f-g\right\|_{\psi_2}^2$ and by Theorem 1.2.7, for every $t \geqslant 1$,

$$\mathbb{P}\Big[\frac{1}{n}\sum_{i=1}^n (f-g)^2(X_i) - \left\|f-g\right\|_{L_2}^2 \geqslant t\left\|f-g\right\|_{\psi_2}^2\Big] \leqslant 2\exp(-c_1 n t). \tag{3.14}$$

Using $\|f-g\|_{L_2} \leqslant \sqrt{e-1}\,\|f-g\|_{\psi_2}$ together with Equation (3.14), it is easy to get for every $u \geqslant 2$,

$$\begin{aligned}
&\mathbb{P}\Big[W(f-g) \geqslant u\,\|f-g\|_{\psi_2}\Big] \\
&\leqslant \mathbb{P}\Big[\frac{1}{n}\sum_{i=1}^{n}(f-g)^2(X_i) - \|f-g\|_{L_2}^2 \geqslant (u^2-(e-1))\,\|f-g\|_{\psi_2}^2\Big] \\
&\leqslant 2\exp\big(-c_2 n u^2\big).
\end{aligned}$$

For the second statement, since $\mathbb{E}f^2 = \mathbb{E}g^2$, the increments are

$$Z(f) - Z(g) = \frac{1}{n}\sum_{i=1}^{n}\big(f^2(X_i) - g^2(X_i)\big).$$

Thanks to (3.11), $Z(f)-Z(g)$ is a sum of mean-zero ψ_1 random variables and the result follows from Theorem 1.2.7. The last statement is a consequence of Theorem 1.2.7, since $\|f^2\|_{\psi_1} = \|f\|_{\psi_2}^2 \leqslant \alpha^2$ for all f in F. □

Once obtained the deviation properties of the increments of the underlying process(es) (that is $(Z(f))_{f\in F}$ and $(W(f))_{f\in F}$), we use the generic chaining mechanism to obtain a uniform bound on (3.9). Since we work in a special framework (sum of squares of ψ_2 random variables), we will perform a particular chaining argument which allows us to avoid the $\gamma_1(F,\psi_2)$ term coming from the classical generic chaining (cf. (3.12)).

If $\gamma_2(F,\psi_2) = \infty$, then the upper bound of Theorem 3.2.1 is trivial, otherwise consider an *almost optimal admissible sequence* $(F_s)_{s\in\mathbb{N}}$ of F with respect to $\psi_2(\mu)$, that is an admissible sequence $(F_s)_{s\in\mathbb{N}}$ such that

$$\gamma_2(F,\psi_2) \geqslant \frac{1}{2}\sup_{f\in F}\Big(\sum_{s=0}^{\infty} 2^{s/2} d_{\psi_2}(f,F_s)\Big).$$

For every $f \in F$ and integer s, put $\pi_s(f)$ a nearest point to f in F_s with respect to the $\psi_2(\mu)$ distance.

The idea of the proof is for every $f \in F$ to analyze the links $\pi_{s+1}(f) - \pi_s(f)$ for $s \in \mathbb{N}$ of the chain $(\pi_s(f))_{s\in\mathbb{N}}$ in three different regions - values of the level s in $[0,s_1]$, $[s_1+1, s_0-1]$ or $[s_0,\infty)$ for some well chosen s_1 ans s_0 - depending on the deviation properties of the increments of the underlying process(es) at the s stage:

1. The end of the chain: we study the link $f - \pi_{s_0}(f)$. In this part of the chain, we work with the process $\big(W(f-\pi_{s_0}(f))\big)_{f\in F}$ which is subgaussian (cf. Lemma 3.2.2). Thanks to this remark, we avoid the sub-exponential behaviour of the process $(Z(f))_{f\in F}$ and thus the term $\gamma_1(F,\psi_2(\mu))$ appearing in (3.12);
2. The middle of the chain: for these stages, we work with the process $(Z(\pi_{s_0}(f)) - Z(\pi_{s_1}(f)))_{f\in F}$ which has subgaussian increments in this range;
3. The beginning of the chain: we study the process $(Z(\pi_{s_1}(f))_{f\in F}$. For this part of the chain, the complexity of F_{s_1} is so small that a trivial comparison of the process with the ψ_2-diameter of F will be enough.

***Proposition 3.2.3* (End of the chain).** — *There exist absolute constant c_0, c_1, c_2 and c_3 for which the following holds. Let $F \subset \mathcal{S}(L_2(\mu))$ be finite and $\alpha = \mathrm{rad}(F, \psi_2)$. For every $v \geqslant c_0$, with probability greater than $1 - c_1 \exp(-c_2 n v^2)$, one has*

$$\sup_{f \in F} W(f - \pi_{s_0}(f)) \leqslant c_3 v \frac{\gamma_2(F, \psi_2)}{\sqrt{n}},$$

where $s_0 = \min\big(s \geqslant 0 : 2^s \geqslant n\big)$.

Proof. — Let f be in F. Since F is finite, we can write

$$f - \pi_{s_0}(f) = \sum_{s=s_0}^{\infty} \pi_{s+1}(f) - \pi_s(f),$$

and, since W is the empirical $L_2(P_n)$ norm (where P_n is the empirical distribution $n^{-1}\sum_{i=1}^n \delta_{X_i}$), it is sub-additive and so

$$W(f - \pi_{s_0}(f)) \leqslant \sum_{s=s_0}^{\infty} W(\pi_{s+1}(f) - \pi_s(f)).$$

Now, fix a level $s \geqslant s_0$. Using a union bound on the set of links $\{(\pi_{s+1}(f), \pi_s(f)) : f \in F\}$ (note that there are at most $|F_{s+1}||F_s|$ such links) and the subgaussian property of W (i.e. Lemma 3.2.2), we get, for every $u \geqslant 2$, with probability greater than $1 - 2|F_{s+1}||F_s| \exp(-C_1 n u^2)$, for every $f \in F$,

$$W(\pi_{s+1}(f) - \pi_s(f)) \leqslant u \left\| \pi_{s+1}(f) - \pi_s(f) \right\|_{\psi_2}.$$

Then, note that for every $s \in \mathbb{N}, |F_{s+1}||F_s| \leqslant 2^{2^s} 2^{2^{s+1}} = 2^{2^{s+2}}$ so that a union bound over all the levels $s \geqslant s_0$ yields for every u such that nu^2 is larger than some absolute constant, with probability greater than $1 - 2\sum_{s=s_0}^{\infty} |F_{s+1}||F_s| \exp(-C_1 n 2^s u^2) \geqslant 1 - c_1 \exp(-c_0 n 2^{s_0} u^2)$, for every $f \in F$,

$$\begin{aligned} W(f - \pi_{s_0}(f)) &\leqslant \sum_{s=s_0}^{\infty} W(\pi_{s+1}(f) - \pi_s(f)) \leqslant \sum_{s=s_0}^{\infty} u 2^{s/2} \left\| \pi_{s+1}(f) - \pi_s(f) \right\|_{\psi_2} \\ &\leqslant 2u \sum_{s=s_0}^{\infty} 2^{s/2} d_{\psi_2}(f, F_s). \end{aligned}$$

We conclude with $v^2 = 2^{s_0} u^2$ for v large enough and noting that $2^{s_0} \sim n$ by definition of s_0 and with the quasi-optimality of the admissible sequence $(F_s)_{s \geqslant 0}$. □

***Proposition 3.2.4* (Middle of the chain).** — *There exist absolute constants c_0, c_1, c_2 and c_3 for which the following holds. Let $s_1 \in \mathbb{N}$ be such that $s_1 \leqslant s_0$ (where $s_0 = \min\big(s \geqslant 0 : 2^s \geqslant n\big)$ has been defined in Proposition 3.2.3). Let $F \subset \mathcal{S}(L_2(\mu))$ and $\alpha = \mathrm{rad}(F, \psi_2)$. For every $u \geqslant c_0$, with probability greater than $1 - c_1 \exp(-c_2 2^{s_1} u)$,*

$$\sup_{f \in F} \left| Z(\pi_{s_0}(f)) - Z(\pi_{s_1}(f)) \right| \leqslant c_3 u \alpha \frac{\gamma_2(F, \psi_2)}{\sqrt{n}}.$$

Proof. — For every $f \in F$, we write

$$Z(\pi_{s_0}(f)) - Z(\pi_{s_1}(f)) = \sum_{s=s_1}^{s_0-1} Z(\pi_{s+1}(f)) - Z(\pi_s(f)).$$

Let $s_1 \leqslant s \leqslant s_0 - 1$ and $u > 0$. Thanks to the second deviation result of Lemma 3.2.2, with probability greater than $1 - 2\exp\big(-C_1 n \min\big((u2^{s/2}/\sqrt{n}), (u^2 2^s/n)\big)\big)$,

$$|Z(\pi_{s+1}(f)) - Z(\pi_s(f))| \leqslant \frac{u2^{s/2}}{\sqrt{n}} \alpha \left\|\pi_{s+1}(f) - \pi_s(f)\right\|_{\psi_2}. \tag{3.15}$$

Now, $s \leqslant s_0 - 1$, thus $2^s/n \leqslant 1$ and so $\min\big(u2^{s/2}/\sqrt{n}, u^2 2^s/n\big) \geqslant \min(u, u^2)(2^s/n)$. In particular, (3.15) holds with probability greater than

$$1 - 2\exp\big(-C_1 2^s \min(u, u^2)\big)\big).$$

Now, a union bound on the set of links for every level $s = s_1, \dots, s_0 - 1$ yields, for any $u > 0$, with probability greater than $1 - 2\sum_{s=s_1}^{s_0-1} |F_{s+1}||F_s| \exp\big(-C_1 2^s \min(u, u^2)\big)$, for every $f \in F$,

$$\big|Z(\pi_{s_0}(f)) - Z(\pi_{s_1}(f))\big| \leqslant \sum_{s=s_1}^{s_0-1} \frac{u2^{s/2}}{\sqrt{n}} \alpha \left\|\pi_{s+1}(f) - \pi_s(f)\right\|_{\psi_2}.$$

The result follows since $|F_{s+1}||F_s| \leqslant 2^{2^{s+2}}$ for every integer s and so for u large enough,

$$2\sum_{s=s_1}^{s_0-1} |F_{s+1}||F_s| \exp\big(-C_1 2^s \min(u, u^2)\big) \leqslant c_1 \exp(-c_2 2^{s_1} u).$$

□

***Proposition 3.2.5* (Beginning of the chain).** — *There exist $c_0, c_1 > 0$ such that the following holds. Let $w > 0$ and s_1 be such that $2^{s_1} < (C_1/2) n \min(w, w^2)$ (where C_1 is the constant appearing in Lemma 3.2.2). Let $F \subset \mathcal{S}(L_2(\mu))$ and $\alpha = \mathrm{rad}(F, \psi_2)$. For every $t \geqslant w$, with probability greater than $1 - c_0 \exp(-c_1 n \min(t, t^2))$, one has*

$$\sup_{f \in F} \big|Z(\pi_{s_1}(f))\big| \leqslant \alpha^2 t.$$

Proof. — It follows from the third deviation result of Lemma 3.2.2 and a union bound over F_{s_1}, that with probability greater than $1 - 2|F_{s_1}| \exp\big(-C_1 n \min(t, t^2)\big)$, one has for every $f \in F$,

$$|Z(\pi_{s_1}(f))| \leqslant \alpha^2 t.$$

Since $|F_{s_1}| \leqslant 2^{2^{s_1}} < \exp\big((C_1/2) n \min(t, t^2)\big)$, the result follows. □

Proof of Theorem 3.2.1. — Denote by $(F_s)_{s \in \mathbb{N}}$ an almost optimal admissible sequence of F with respect to the ψ_2-norm and, for every $s \in \mathbb{N}$ and $f \in F$, denote by $\pi_s(f)$ one of the closest point of f in F_s with respect to the $\psi_2(\mu)$ distance. Let $s_0 \in \mathbb{N}$ be such that $s_0 = \min\big(s \geqslant 0 : 2^s \geqslant n\big)$. We have, for every $f \in F$,

$$\begin{aligned}
|Z(f)| &= \Big|\frac{1}{n}\sum_{i=1}^n f^2(X_i) - \mathbb{E}f^2(X)\Big| = \Big|\frac{1}{n}\sum_{i=1}^n (f - \pi_{s_0}(f) + \pi_{s_0}(f))^2(X_i) - \mathbb{E}f^2(X)\Big| \\
&= \Big|P_n(f - \pi_{s_0}(f))^2 + 2P_n\big((f - \pi_{s_0}(f))\pi_{s_0}(f)\big) + P_n\pi_{s_0}(f)^2 - \mathbb{E}\pi_{s_0}(f)^2\Big| \\
&\leqslant W(f - \pi_{s_0}(f))^2 + 2W(f - \pi_{s_0}(f))W(\pi_{s_0}(f)) + |Z(\pi_{s_0}(f))| \\
&\leqslant W(f - \pi_{s_0}(f))^2 + 2W(f - \pi_{s_0}(f))\big(Z(\pi_{s_0}(f)) + 1\big)^{1/2} + |Z(\pi_{s_0}(f))| \\
&\leqslant 3W(f - \pi_{s_0}(f))^2 + 2W(f - \pi_{s_0}(f)) + 3|Z(\pi_{s_0}(f))|, \qquad (3.16)
\end{aligned}$$

where we used $\|\pi_{s_0}(f)\|_{L_2} = 1 = \|f\|_{L_2}$ and the notation P_n stands for the empirical probability distribution $n^{-1}\sum_{i=1}^n \delta_{X_i}$.

Thanks to Proposition 3.2.3 for v a constant large enough, with probability greater than $1 - c_0\exp(-c_1 n)$, for every $f \in F$,

$$W(f - \pi_{s_0}(f))^2 \leqslant c_2\frac{\gamma_2(F,\psi_2)^2}{n}. \qquad (3.17)$$

Let $w > 0$ to be chosen later and define $s_1 \in \mathbb{N}$ by

$$s_1 = \max\Big(s \geqslant 0 : 2^s \leqslant \min\big(2^{s_0}, (C_1/2)n\min(w, w^2)\big)\Big), \qquad (3.18)$$

where C_1 is the constant defined in Lemma 3.2.2. We apply Proposition 3.2.4 for u a constant large enough and Proposition 3.2.5 to get, with probability greater than $1 - c_3\exp(-c_4 2^{s_1})$ that for every $f \in F$,

$$\begin{aligned}
|Z(\pi_{s_0}(f))| &\leqslant |Z(\pi_{s_0}(f)) - Z(\pi_{s_1}(f))| + |Z(\pi_{s_1}(f))| \\
&\leqslant c_5\alpha\frac{\gamma_2(F,\psi_2)}{\sqrt{n}} + \alpha^2 w. \qquad (3.19)
\end{aligned}$$

We combine Equations (3.16), (3.17) and (3.19) to get, with probability greater than $1 - c_6\exp(-c_7 2^{s_1})$ that for every $f \in F$,

$$|Z(f)| \leqslant c_8\frac{\gamma_2(F,\psi_2)^2}{n} + c_9\frac{\gamma_2(F,\psi_2)}{\sqrt{n}} + c_{10}\alpha\frac{\gamma_2(F,\psi_2)}{\sqrt{n}} + 3\alpha^2 w.$$

The first statement of Theorem 3.2.1 follows for

$$w = \max\Big(\frac{\gamma_2(F,\psi_2)}{\alpha\sqrt{n}}, \frac{\gamma_2(F,\psi_2)^2}{\alpha^2 n}\Big). \qquad (3.20)$$

For the last statement, we use Proposition 3.2.3 to get

$$\mathbb{E}\sup_{f\in F} W(f - \pi_{s_0}(f))^2 = \int_0^\infty \mathbb{P}\big[\sup_{f\in F} W(f - \pi_{s_0}(f))^2 \geqslant t\big]dt \leqslant c_{11}\frac{\gamma_2(F,\psi_2)^2}{n} \qquad (3.21)$$

and

$$\mathbb{E}\sup_{f\in F} W(f - \pi_{s_0}(f)) \leqslant c_{12}\frac{\gamma_2(F,\psi_2)}{\sqrt{n}}. \qquad (3.22)$$

It follows from Propositions 3.2.4 and 3.2.5 for s_1 and w defined in (3.18) and (3.20) that

$$\begin{aligned}\mathbb{E}\sup_{f\in F}|Z(\pi_{s_0}(f))| &\leqslant \mathbb{E}\sup_{f\in F}|Z(\pi_{s_0}(f))-Z(\pi_{s_1}(f))|+\mathbb{E}\sup_{f\in F}|Z(\pi_{s_1}(f))|\\ &\leqslant \int_0^\infty \mathbb{P}\Big[\sup_{f\in F}|Z(\pi_{s_0}(f))-Z(\pi_{s_1}(f))|\geqslant t\Big]dt+\int_0^\infty \mathbb{P}\Big[\sup_{f\in F}|Z(\pi_{s_1}(f))|\geqslant t\Big]dt\\ &\leqslant c\max\Big(\alpha\frac{\gamma_2(F,\psi_2)}{\sqrt{n}},\frac{\gamma_2(F,\psi_2)^2}{n}\Big). \qquad (3.23)\end{aligned}$$

The claim follows by combining Equations (3.21), (3.22) and (3.23) in Equation (3.16). □

3.3. Application to Compressed Sensing

In this section, we apply Theorem 3.2.1 to prove that a $n\times N$ random matrix with i.i.d. isotropic row vectors which are ψ_2 with constant α satisfies $\mathrm{RIP}_{2m}(\delta)$ with overwhelming probability under suitable assumptions on n, N, m, α and δ. Let A be such a matrix and denote by $n^{-1/2}Y_1,\dots,n^{-1/2}Y_n$ its rows vectors such that $Y_1,\dots,Y_n$ are distributed according to a probability measure μ.

For a functions class F in $\mathcal{S}(L_2(\mu))$, it follows from Theorem 3.2.1 that with probability greater than $1-c_1\exp\Big(-(c_2/\alpha^2)\min\Big(n\alpha^2,\gamma_2(F,\psi_2)^2\Big)\Big)$,

$$\sup_{f\in F}\left|\frac{1}{n}\sum_{i=1}^n f^2(Y_i)-\mathbb{E}f^2(Y)\right|\leqslant c_3\max\left(\alpha\frac{\gamma_2(F,\psi_2)}{\sqrt{n}},\frac{\gamma_2(F,\psi_2)^2}{n}\right).$$

where $\alpha=\mathrm{rad}(F,\psi_2(\mu))$. In particular, for a class F of linear functions indexed by a subset T of $\mathcal{S}^{N-1}$, the $\psi_2(\mu)$ norm and the $L_2(\mu)$ norm are equivalent on F and so with probability greater than $1-c_1\exp\big(-c_2\min\big(n,\gamma_2(T,\ell_2^N)^2\big)\big)$,

$$\sup_{x\in T}\left|\frac{1}{n}\sum_{i=1}^n\langle Y_i,x\rangle^2-1\right|\leqslant c_3\alpha^2\max\left(\frac{\gamma_2(T,\ell_2^N)}{\sqrt{n}},\frac{\gamma_2(T,\ell_2^N)^2}{n}\right). \qquad (3.24)$$

A bound on the restricted isometry constant δ_{2m} follows from (3.24). Indeed let $T=S_2(\Sigma_{2m})$ then with probability greater than

$$1-c_1\exp\big(-c_2\min\big(n,\gamma_2(S_2(\Sigma_{2m}),\ell_2^N)^2\big)\big),$$

$$\delta_{2m}\leqslant c_3\alpha^2\max\left(\frac{\gamma_2(S_2(\Sigma_{2m}),\ell_2^N)}{\sqrt{n}},\frac{\gamma_2(S_2(\Sigma_{2m}),\ell_2^N)^2}{n}\right).$$

Now, it remains to bound $\gamma_2(S_2(\Sigma_{2m}),\ell_2^N)$. Such a bound may follow from the Majorizing measure theorem (cf. Theorem 3.1.5):

$$\gamma_2(S_2(\Sigma_{2m}),\ell_2^N)\sim\ell_*(S_2(\Sigma_{2m})).$$

Since $S_2(\Sigma_{2m})$ can be written as a union of spheres with short support, it is easy to obtain

$$\ell_*(S_2(\Sigma_{2m})) = \mathbb{E}\Big(\sum_{i=1}^{2m}(g_i^*)^2\Big)^{1/2} \tag{3.25}$$

where $g_1,\dots,g_N$ are N i.i.d. standard Gaussian variables and $(g_i^*)_{i=1}^N$ is a non-decreasing rearrangement of $(|g_i|)_{i=1}^N$. A bound on (3.25) follows from the following technical result.

Lemma 3.3.1. — *There exist absolute positive constants c_0, c_1 and c_2 such that the following holds. Let $(g_i)_{i=1}^N$ be a family of N i.i.d. standard Gaussian variables. Denote by $(g_i^*)_{i=1}^N$ a non-increasing rearrangement of $(|g_i|)_{i=1}^N$. For any $k=1,\dots,N/c_0$, we have*

$$\sqrt{c_1\log\Big(\frac{N}{k}\Big)} \leqslant \mathbb{E}\Big(\frac{1}{k}\sum_{i=1}^{k}(g_i^*)^2\Big)^{1/2} \leqslant 2\sqrt{\log\Big(\frac{c_2N}{k}\Big)}.$$

Proof. — Let g be a standard real-valued Gaussian variable and define $c_1>0$ such that $\mathbb{E}\exp(g^2/4)=c_1$. By convexity, it follows that

$$\exp\Big(\mathbb{E}\Big(\frac{1}{k}\sum_{i=1}^{k}\frac{(g_i^*)^2}{4}\Big)\Big) \leqslant \frac{1}{k}\sum_{i=1}^{k}\mathbb{E}\exp\big((g_i^*)^2/4\big) \leqslant \frac{1}{k}\sum_{i=1}^{N}\mathbb{E}\exp(g_i^2/4) \leqslant \frac{c_1N}{k}.$$

Finally,

$$\mathbb{E}\Big(\frac{1}{k}\sum_{i=1}^{k}(g_i^*)^2\Big)^{1/2} \leqslant \Big(\mathbb{E}\frac{1}{k}\sum_{i=1}^{k}(g_i^*)^2\Big)^{1/2} \leqslant 2\sqrt{\log\big(c_1N/k\big)}.$$

For the lower bound, we note that for $x>0$,

$$\sqrt{\frac{2}{\pi}}\int_x^\infty \exp(-s^2/2)ds \geqslant \sqrt{\frac{2}{\pi}}\int_x^{2x}\exp(-s^2/2)ds \geqslant \sqrt{\frac{2}{\pi}}x\exp(-2x^2).$$

In particular, for any $c_0>0$ and $1\leqslant k\leqslant N$,

$$\mathbb{P}\Big[|g|\geqslant\sqrt{c_0\log\big(N/k\big)}\Big] \geqslant \sqrt{\frac{2c_0}{\pi}\log\Big(\frac{N}{k}\Big)}\Big(\frac{k}{N}\Big)^{2c_0}. \tag{3.26}$$

It follows from Markov inequality that

$$\begin{aligned}\mathbb{E}\Big(\frac{1}{k}\sum_{i=1}^{k}(g_i^*)^2\Big)^{1/2} &\geqslant \mathbb{E}g_k^* \geqslant \sqrt{c_0\log\big(N/k\big)}\,\mathbb{P}\Big[g_k^*\geqslant\sqrt{c_0\log\big(N/k\big)}\Big]\\ &= \sqrt{c_0\log\big(N/k\big)}\,\mathbb{P}\Big[\sum_{i=1}^{N}I\Big(|g_i|\geqslant\sqrt{c_0\log\big(N/k\big)}\Big)\geqslant k\Big]\\ &= \sqrt{c_0\log\big(N/k\big)}\,\mathbb{P}\Big[\sum_{i=1}^{N}\delta_i\geqslant k\Big]\end{aligned}$$

where $I(\cdot)$ denotes the indicator function and $\delta_i = I\Big(|g_i|\geqslant\sqrt{c_0\log\big(N/k\big)}\Big)$ for $i=1,\dots,N$. Since $(\delta_i)_{i=1}^N$ is a family of i.i.d. Bernoulli variables with mean $\delta =$

$\mathbb{P}\Big[|g| \geqslant \sqrt{c_0 \log\big(N/k\big)}\Big]$, it follows from Bernstein inequality (cf. Theorem 1.2.6) that, as long as $k \leqslant \delta N/2$ and $N\delta \geqslant 10 \log 4$,

$$\mathbb{P}\Big[\sum_{i=1}^{N} \delta_i \geqslant k\Big] \geqslant \mathbb{P}\Big[\frac{1}{N}\sum_{i=1}^{N} \delta_i - \delta \geqslant \frac{-\delta}{2}\Big] \geqslant 1/2.$$

Thanks to (3.26), it is easy to check that for $c_0 = 1/4$, we have $k \leqslant \delta N/2$ as long as $k \leqslant N/\exp(4\pi)$. □

It is now possible to prove the result announced at the beginning of the section.

Theorem 3.3.2. — *There exist absolute positive constants c_0, c_1, c_2 and c_3 such that the following holds. Let A be a $n \times N$ random matrix with rows vectors $n^{-1/2}Y_1, \dots, n^{-1/2}Y_n$. Assume that $Y_1, \dots, Y_n$ are i.i.d. isotropic vectors of $\mathbb{R}^N$, which are ψ_2 with constant α. Let m be an integer and $\delta \in (0,1)$ such that*

$$m \log\big(c_0 N/m\big) = c_1 n\delta^2/\alpha^4.$$

Then, with probability greater than $1 - c_2 \exp(-c_3 n\delta^2/\alpha^4)$, the restricted isometry constant δ_{2m} of order $2m$ of A satisfies

$$\delta_{2m} = \sup_{x \in S_2(\Sigma_{2m})} \Big|\frac{1}{n}\sum_{i=1}^{n} \langle Y_i, x\rangle^2 - 1\Big| \leqslant \delta.$$

3.4. Notes and comments

Dudley entropy bound (cf. Theorem 3.1.2) can be found in [**Dud67**]. Other Dudley type entropy bounds for processes $(X_t)_{t\in T}$ with Orlicz norm of the increments satisfying, for every $s, t \in T$,

$$\|X_t - X_s\|_\psi \leqslant d(s,t) \tag{3.27}$$

may be obtained (see [**Pis80**] and [**Kôn80**]). Under the increment condition (3.27) and (1.1) and for ψ^{-1} denoting the inverse function of the Orlicz function ψ, the Dudley entropy integral

$$\int_0^\infty \psi^{-1}\big(N(T,d,\epsilon)\big) d\epsilon,$$

is an upper bound for $\big\|\sup_{s,t\in T}|X_s - X_t|\big\|_\psi$ and in particular of $\mathbb{E}\sup_{t,s\in T}|X_t - X_s|$ (up to an absolute constant factor).

For the partition scheme method used in the generic chaining mechanism of Theorem 3.1.4, we refer to [**Tal05**] and [**Tal01**]. The generic chaining mechanism was first introduced using majorizing measures. This tool was introduced in [**Fer74, Fer75**] and is implicit in earlier work by Preston based on an important result of Garcia, Rodemich and Rumsey. In [**Tal87**], Talagrand proves that majorizing measures are the key quantities to analyze the supremum of Gaussian processes. In particular, the majorizing measure theorem (cf. Theorem 3.1.5) is shown in [**Tal87**]. More about majorizing measures and majorizing measure theorems for other processes than Gaussian processes can be found in [**Tal96a**] and [**Tal95**]. Connections between the majorizing measures and partition schemes have been shown in [**Tal05**] and [**Tal01**].

The upper bounds on the process

$$\sup_{f \in F} \Big| \frac{1}{n} \sum_{i=1}^{n} f^2(X_i) - \mathbb{E} f^2(X) \Big| \tag{3.28}$$

developed in Section 3.2 follow the line of [**MPTJ07**]. Other bounds on (3.28) can be found in the next chapter (cf. Theorem 5.3.14).

CHAPTER 4

SINGULAR VALUES AND WISHART MATRICES

The singular values of a matrix are very natural geometrical quantities which play an important role in pure and applied mathematics. The first part of this chapter is a compendium on the properties of the singular values. The second part concerns random matrices, and constitutes a quick tour in this vast subject. It starts with properties of Gaussian random matrices, gives a proof of the universal Marchenko–Pastur theorem regarding the counting probability measure of the singular values, and ends with the Bai–Yin theorem statement on the extremal singular values.

For every square matrix $A \in \mathcal{M}_{n,n}(\mathbb{C})$, we denote by $\lambda_1(A), \ldots, \lambda_n(A)$ the eigenvalues of A which are the roots in $\mathbb{C}$ of the characteristic polynomial $\det(A - zI) \in \mathbb{C}[z]$ where I denotes the identity matrix. Unless otherwise stated we label the eigenvalues of A so that $|\lambda_1(A)| \geqslant \cdots \geqslant |\lambda_n(A)|$. In all this chapter, $\mathbb{K}$ stands for $\mathbb{R}$ or $\mathbb{C}$, and we say that $U \in \mathcal{M}_{n,n}(\mathbb{K})$ is $\mathbb{K}$–unitary when $UU^* = I$, where the star super-script denotes the conjugate-transpose operation.

4.1. The notion of singular values

This section gathers a selection of classical results from linear algebra. We begin with the Singular Value Decomposition (SVD), a fundamental tool in matrix analysis. It expresses a diagonalization up to unitary transformations of the space.

Theorem 4.1.1 **(Singular Value Decomposition)**. — *For every $A \in \mathcal{M}_{m,n}(\mathbb{K})$, there exists a couple of $\mathbb{K}$–unitary matrices U $(m \times m)$ and V $(n \times n)$ and a sequence of real numbers $s_1 \geqslant \cdots \geqslant s_{m \wedge n} \geqslant 0$ such that $A = UDV^*$ where*

$$D = U^* AV = \operatorname{diag}(s_1, \ldots, s_{m \wedge n}) \in \mathcal{M}_{m,n}(\mathbb{K}).$$

This sequence of real numbers does not depend on the particular choice of U, V.

Proof. — Let $v \in \mathbb{K}^n$ be such that $|v|_2 = 1$ and $|Av|_2 = \max_{|x|_2=1} |Ax|_2 = \|A\|_{2\to 2} = s$. If $s = 0$ then $A = 0$ and the result is trivial. If $s > 0$ then let us define $u = Av/s$. One can find a $\mathbb{K}$-unitary $m \times m$ matrix U with first column vector equal to u, and a $\mathbb{K}$-unitary $n \times n$ matrix V with first column vector equal to v. It follows that

$$U^*AV = \begin{pmatrix} s & w^* \\ 0 & B \end{pmatrix} = A_1$$

for some $w \in \mathcal{M}_{n-1,1}(\mathbb{K})$ and $B \in \mathcal{M}_{m-1,n-1}(\mathbb{K})$. If t is the first row of A_1 then $|A_1 t^*|_2^2 \geqslant (s^2 + |w|_2^2)^2$ and therefore $\|A_1\|_{2\to 2}^2 \geqslant s^2 + |w|_2^2 \geqslant \|A\|_{2\to 2}^2$. On the other hand, since A and A_1 are unitary equivalent, we have $\|A_1\|_{2\to 2} = \|A\|_{2\to 2}$. Therefore $w = 0$, and the desired decomposition follows by an induction on $m \wedge n$.

If one sees the diagonal matrix $D = \mathrm{diag}(s_1(A)^2, \ldots, s_{m\wedge n}(A)^2)$ as an element of $\mathcal{M}_{m,m}(\mathbb{K})$ or $\mathcal{M}_{n,n}(\mathbb{K})$ by appending as much zeros as needed, we have

$$U^*AA^*U = D \quad \text{and} \quad V^*A^*AV = D.$$

The positive semidefinite Hermitian matrices $AA^* \in \mathcal{M}_{m,m}(\mathbb{K})$ and $A^*A \in \mathcal{M}_{n,n}(\mathbb{K})$ share the same sequence of eigenvalues, up to the multiplicity of the eigenvalue 0, and for every $k \in \{1, \ldots, m \wedge n\}$,

$$s_k(A) = \lambda_k(\sqrt{AA^*}) = \sqrt{\lambda_k(AA^*)} = \sqrt{\lambda_k(A^*A)} = \lambda_k(\sqrt{A^*A}) = s_k(A^*).$$

This shows the uniqueness of $s_1, \ldots, s_{m\wedge n}$. The columns of U and V are the eigenvectors of the positive semidefinite Hermitian matrices AA^* and A^*A. □

Singular values. — The numbers $s_k(A) = s_k$ for $k \in \{1, \ldots, m \wedge n\}$ in Theorem 4.1.1 are called the *singular values* of A. It is often convenient to use the convention $s_k(A) = 0$ if $k > m \wedge n$. For any $A \in \mathcal{M}_{m,n}(\mathbb{K})$, the matrices A, $\bar{A}$, $A^\top$, A^*, UA, AV share the same sequences of singular values, for any $\mathbb{K}$–unitary matrices U, V.

Normal matrices. — Recall that a square matrix $A \in \mathcal{M}_{n,n}(\mathbb{K})$ is *normal* when $AA^* = A^*A$. This is equivalent to say that there exists a $\mathbb{K}$–unitary matrix U such that U^*AU is diagonal, and the diagonal elements are indeed the eigenvalues of A. In this chapter, the word "normal" is used solely in this way and never as a synonym for "Gaussian". Every Hermitian or unitary matrix is normal, while a non identically zero nilpotent matrix is never normal. If $A \in \mathcal{M}_{n,n}(\mathbb{K})$ is normal then $s_k(A) = |\lambda_k(A)|$ and $s_k(A^r) = s_k(A)^r$ for every $k \in \{1, \ldots, n\}$ and for any $r \geqslant 1$. Moreover if A has unitary diagonalization U^*AU then its SVD is U^*AV with $V = PU$ and $P = \mathrm{diag}(\varphi_1, \ldots, \varphi_n)$ where $\varphi_k = \lambda_k/|\lambda_k|$ (here $0/0 = 1$) is the phase of λ_k for every $k \in \{1, \ldots, n\}$.

Polar decomposition. — If $A \in \mathcal{M}_{n,n}(\mathbb{K})$ has SVD $D = U^*AV$, then the Hermitian matrix $H = VDV^*$ and the unitary matrix $W = UV^*$ form the *polar decomposition* $A = WH$ of A. Conversely, one may deduce the SVD of a square matrix A from its polar decomposition $A = WH$ by using a unitary diagonalization of H.

Hermitization. — The eigenvalues of the $(m+n) \times (m+n)$ Hermitian matrix

$$H_A = \begin{pmatrix} 0 & A^* \\ A & 0 \end{pmatrix} \tag{4.1}$$

are $\pm s_1(A), \ldots, \pm s_{m\wedge n}(A), 0, \ldots, 0$ where $0, \ldots, 0$ stands for a sequence of 0's of length $m + n - 2(m \wedge n) = (m \vee n) - (m \wedge n)$. This turns out to be useful because the mapping $A \mapsto H_A$ is linear in A, in contrast with the mapping $A \mapsto \sqrt{AA^*}$. One may deduce the singular values of A from the eigenvalues of H, and $H^2 = A^*A \oplus AA^*$. If $m = n$ and $A_{i,j} \in \{0,1\}$ for all i,j, then A is the adjacency matrix of an oriented graph, and H is the adjacency matrix of a companion nonoriented bipartite graph.

Left and right eigenvectors. — If $u_1 \perp \cdots \perp u_m \in \mathbb{K}^m$ and $v_1 \perp \cdots \perp v_n \in \mathbb{K}^n$ are the columns of U, V then for every $k \in \{1, \ldots, m \wedge n\}$,

$$Av_k = s_k(A)u_k \quad \text{and} \quad A^*u_k = s_k(A)v_k \tag{4.2}$$

while $Av_k = 0$ and $A^*u_k = 0$ for $k > m \wedge n$. The SVD gives an intuitive geometrical interpretation of A and A^* as a dual correspondence/dilation between two orthonormal bases known as the left and right eigenvectors of A and A^*. Additionally, A has exactly $r = \mathrm{rank}(A)$ nonzero singular values $s_1(A), \ldots, s_r(A)$ and

$$A = \sum_{k=1}^{r} s_k(A)u_k v_k^* \quad \text{and} \quad \begin{cases} \mathrm{kernel}(A) & = \mathrm{span}\{v_{r+1}, \ldots, v_n\}, \\ \mathrm{range}(A) & = \mathrm{span}\{u_1, \ldots, u_r\}. \end{cases}$$

We have also $s_k(A) = |Av_k|_2 = |A^*u_k|_2$ for every $k \in \{1, \ldots, m \wedge n\}$.

Condition number. — The condition number of an invertible $A \in \mathcal{M}_{n,n}(\mathbb{K})$ is

$$\kappa(A) = \|A\|_{2\to2} \left\|A^{-1}\right\|_{2\to2} = \frac{s_1(A)}{s_n(A)}.$$

The condition number quantifies the numerical sensitivity of linear systems involving A. For instance, if $x \in \mathbb{K}^n$ is the solution of the linear equation $Ax = b$ then $x = A^{-1}b$. If b is known up to precision $\delta \in \mathbb{K}^n$ then x is known up to precision $A^{-1}\delta$. Therefore, the ratio of relative errors for the determination of x is given by

$$R(b,\delta) = \frac{\left|A^{-1}\delta\right|_2 / \left|A^{-1}b\right|_2}{|\delta|_2/|b|_2} = \frac{\left|A^{-1}\delta\right|_2}{|\delta|_2} \frac{|b|_2}{\left|A^{-1}b\right|_2}.$$

Consequently, we obtain

$$\max_{b\neq0,\delta\neq0} R(b,\delta) = \left\|A^{-1}\right\|_{2\to2} \|A\|_{2\to2} = \kappa(A).$$

Geometrically, $\kappa(A)$ measures the "spherical defect" of the ellipsoid in Figure 1.

Computation of the SVD. — To compute the SVD of $A \in \mathcal{M}_{m,n}(\mathbb{K})$ one can diagonalize AA^* or diagonalize the Hermitian matrix H defined in (4.1). Unfortunately, this approach can lead to a loss of precision numerically. In practice, and up to machine precision, the SVD is better computed by using for instance a variant of the QR algorithm after *unitary bidiagonalization*.

Let us explain how works the unitary bidiagonalization of a matrix $A \in \mathcal{M}_{m,n}(\mathbb{K})$ with $m \leqslant n$. If r_1 is the first row of A, the Gram–Schmidt (or Householder) algorithm provides a $n \times n$ $\mathbb{K}$–unitary matrix V_1 which maps r_1^* to a multiple of e_1. Since V_1 is unitary the matrix AV_1^* has first row equal to $|r_1|_2 e_1$. Now one can construct similarly a $m \times m$ $\mathbb{K}$–unitary matrix U_1 with first row and column equal to e_1 which maps the first column of AV_1^* to an element of $\mathrm{span}(e_1, e_2)$. This gives to $U_1AV_1^*$ a nice structure and suggests a recursion on the dimension m. Indeed by induction one may construct bloc diagonal $m \times m$ $\mathbb{K}$–unitary matrices $U_1, \ldots, U_{m-2}$ and bloc diagonal $n \times n$ $\mathbb{K}$–unitary matrices $V_1, \ldots, V_{m-1}$ such that if $U = U_{m-2} \cdots U_1$ and $V = V_1^* \cdots V_{m-1}^*$ then the matrix

$$B = UAV \tag{4.3}$$

is real $m \times n$ lower triangular bidiagonal i.e. $B_{i,j} = 0$ for every i and every $j \notin \{i, i+1\}$. If A is Hermitian then taking $U = V$ provides a Hermitian tridiagonal matrix $B = UAU^*$ having the same spectrum as A.

4.2. Basic properties

It is very well known that the eigenvalues of a Hermitian matrix can be expressed in terms of the entries via minimax variational formulas. The following result is the counterpart for the singular values. It can be deduced from its Hermitian cousin.

Theorem 4.2.1 **(Courant–Fischer minimax variational formulas)**
For every $A \in \mathcal{M}_{m,n}(\mathbb{K})$ and every $k \in \{1, \ldots, m \wedge n\}$,

$$s_k(A) = \max_{V \in \mathcal{G}_{n,k}} \min_{\substack{x \in V \\ |x|_2 = 1}} |Ax|_2 = \min_{V \in \mathcal{G}_{n,n-k+1}} \max_{\substack{x \in V \\ |x|_2 = 1}} |Ax|_2$$

where $\mathcal{G}_{n,k}$ is the set of all subspaces of $\mathbb{K}^n$ of dimension k. In particular, we have

$$s_1(A) = \max_{\substack{x \in \mathbb{K}^n \\ |x|_2 = 1}} |Ax|_2 \quad \text{and} \quad s_{m \wedge n}(A) = \max_{V \in \mathcal{G}_{n,m \wedge n}} \min_{\substack{x \in V \\ |x|_2 = 1}} |Ax|_2.$$

We have also the following alternative formulas, for every $k \in \{1, \ldots, m \wedge n\}$,

$$s_k(A) = \max_{\substack{V \in \mathcal{G}_{n,k} \\ W \in \mathcal{G}_{m,k}}} \min_{\substack{(x,y) \in V \times W \\ |x|_2 = |y|_2 = 1}} \langle Ax, y \rangle.$$

Remark 4.2.2 **(Smallest singular value)**. — *The smallest singular value is always a minimum. Indeed, if $m \geqslant n$ then $\mathcal{G}_{n,m \wedge n} = \mathcal{G}_{n,n} = \{\mathbb{K}^n\}$ and thus*

$$s_{m \wedge n}(A) = \min_{\substack{x \in \mathbb{K}^n \\ |x|_2 = 1}} |Ax|_2,$$

while if $m \leqslant n$ then using the latter for $A^\top$ we get

$$s_{m \wedge n}(A) = s_{m \wedge n}(A^\top) = \min_{\substack{x \in \mathbb{K}^m \\ |x|_2 = 1}} \left|A^\top x\right|_2.$$

As an exercise, one can check that if $A \in \mathcal{M}_{m,n}(\mathbb{R})$ then the variational formulas for $\mathbb{K} = \mathbb{C}$, if one sees A as an element of $\mathcal{M}_{m,n}(\mathbb{C})$, coincide actually with the formulas for $\mathbb{K} = \mathbb{R}$. Geometrically, the matrix A maps the Euclidean unit ball to an ellipsoid, and the singular values of A are exactly the half lengths of the $m \wedge n$ largest principal axes of this ellipsoid, see Figure 1. The remaining axes have zero length. In particular, for $A \in \mathcal{M}_{n,n}(\mathbb{K})$, the variational formulas for the extremal singular values $s_1(A)$ and $s_n(A)$ correspond to the half length of the longest and shortest axes.

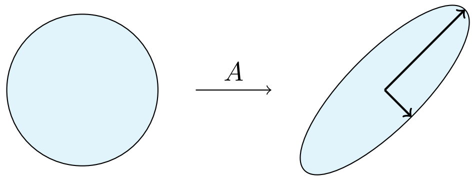

FIGURE 1. Largest and smallest singular values of $A \in \mathcal{M}_{2,2}(\mathbb{R})$.

From the Courant–Fischer variational formulas, the largest singular value is the *operator norm* of A for the Euclidean norm $|\cdot|_2$, namely

$$s_1(A) = \|A\|_{2\to 2}\,.$$

The map $A \mapsto s_1(A)$ is Lipschitz and convex. In the same spirit, if U, V are the couple of $\mathbb{K}$–unitary matrices from an SVD of A, then for any $k \in \{1, \dots, \operatorname{rank}(A)\}$,

$$s_k(A) = \min_{\substack{B\in\mathcal{M}_{m,n}(\mathbb{K})\\ \operatorname{rank}(B)=k-1}} \|A - B\|_{2\to 2} = \|A - A_k\|_{2\to 2} \quad \text{where} \quad A_k = \sum_{i=1}^{k-1} s_i(A) u_i v_i^*$$

with u_i, v_i as in (4.2). Let $A \in \mathcal{M}_{n,n}(\mathbb{K})$ be a square matrix. If A is invertible then the singular values of A^{-1} are the inverses of the singular values of A, in other words

$$\forall k \in \{1, \dots, n\}, \quad s_k(A^{-1}) = s_{n-k+1}(A)^{-1}.$$

Moreover, a square matrix $A \in \mathcal{M}_{n,n}(\mathbb{K})$ is invertible iff $s_n(A) > 0$, and in this case

$$s_n(A) = s_1(A^{-1})^{-1} = \left\|A^{-1}\right\|_{2\to 2}^{-1}.$$

Contrary to the map $A \mapsto s_1(A)$, the map $A \mapsto s_n(A)$ is Lipschitz but is not convex when $n \geqslant 2$. Regarding the Lipschitz nature of the singular values, the Courant–Fischer variational formulas provide the following more general result.

***Theorem 4.2.3* (Interlacing by perturbations).** — *If $A, B \in \mathcal{M}_{m,n}(\mathbb{K})$ then for every $i, j \in \{1, \dots, m \wedge n\}$ with $i + j \leqslant 1 + (m \wedge n)$,*

$$s_{i+j-1}(A) \leqslant s_i(B) + s_j(A - B).$$

In particular, taking $j = r + 1$ and $1 \leqslant i \leqslant (m \wedge n) - r$ gives, for every $1 \leqslant k \leqslant m \wedge n$,

$$s_{k+r}(A) \leqslant s_k(B) \leqslant s_{k-r}(A)$$

where $r = \operatorname{rank}(A - B)$ and with $s_i(A) = \infty$ if $i < 1$ and $s_i(A) = 0$ if $i > m \wedge n$.

Theorem 4.2.3 implies (take $j = 1$) that the map $A \mapsto s(A) = (s_1(A), \dots, s_{m\wedge n}(A))$ is actually 1-Lipschitz from $(\mathcal{M}_{m,n}(\mathbb{K}), \|\cdot\|_{2\to 2})$ to $([0,\infty)^{m\wedge n}, |\cdot|_\infty)$ since

$$\max_{1\leqslant k\leqslant m\wedge n} |s_k(A) - s_k(B)| \leqslant \|A - B\|_{2\to 2}\,.$$

From the Courant–Fischer variational formulas we obtain also the following result.

***Theorem 4.2.4* (Interlacing by deletion).** — *Under the convention that $s_i(C) = 0$ for any $C \in \mathcal{M}_{p,q}(\mathbb{K})$ and any $i > p \wedge q$. Let $A \in \mathcal{M}_{m,n}(\mathbb{K})$ and let B be obtained from A by deleting k rows and/or columns. Then for every $i \in \{1, \ldots, m \wedge n\}$,*

$$s_i(A) \geqslant s_i(B) \geqslant s_{i+k}(A)$$

Form Theorem 4.2.4, if $B \in \mathcal{M}_{m-k,n}(\mathbb{K})$ is obtained from $A \in \mathcal{M}_{m,n}(\mathbb{K})$ $(m \leqslant n)$ by deleting $k \in \{1, \ldots, m-1\}$ rows then $[s_{m-k}(B), s_1(B)] \subset [s_m(A), s_1(A)]$. Row deletions produce a compression of the singular values interval. Another way to express this phenomenon consists in saying that if we add a row to B then the largest singular value increases while the smallest singular value is diminished.

Trace norm. — The *trace norm* $\|\cdot\|_{\mathrm{HS}}$ on $\mathcal{M}_{m,n}(\mathbb{K})$ is defined by

$$\|A\|_{\mathrm{HS}}^2 = \mathrm{Tr}(AA^*) = \mathrm{Tr}(A^*A) = \sum_{i=1}^{m}\sum_{j=1}^{n} |A_{i,j}|^2 = s_1(A)^2 + \cdots + s_{m\wedge n}(A)^2.$$

This norm is also known as the Frobenius norm, the Schur norm, or the Hilbert–Schmidt norm (which explains our notation). For every $A \in \mathcal{M}_{m,n}(\mathbb{K})$ we have

$$\|A\|_{2\to 2} \leqslant \|A\|_{\mathrm{HS}} \leqslant \sqrt{\mathrm{rank}(A)}\ \|A\|_{2\to 2}$$

where equalities are achieved respectively when $\mathrm{rank}(A) = 1$ and when $A = \lambda I \in \mathcal{M}_{m,n}(\mathbb{K})$ with $\lambda \in \mathbb{K}$ (here I stands for the $m \times n$ matrix $I_{i,j} = \delta_{i,j}$ for any i, j). The advantage of $\|\cdot\|_{\mathrm{HS}}$ over $\|\cdot\|_{2\to 2}$ lies in its convenient expression in terms of the matrix entries. Actually, the trace norm is Hilbertian for the Hermitian form

$$(A, B) \mapsto \langle A, B\rangle = \mathrm{Tr}(AB^*).$$

We have seen that a matrix $A \in \mathcal{M}_{m,n}(\mathbb{K})$ has exactly $r = \mathrm{rank}(A)$ non zero singular values. If $k \in \{0, 1, \ldots, r\}$ and if A_k is obtained from the SVD of A by forcing $s_i = 0$ for all $i > k$ then we have the Eckart and Young observation:

$$\min_{\substack{B\in\mathcal{M}_{m,n}(\mathbb{K})\\ \mathrm{rank}(B)=k}} \|A - B\|_{\mathrm{HS}}^2 = \|A - A_k\|_{\mathrm{HS}}^2 = s_{k+1}(A)^2 + \cdots + s_r(A)^2. \tag{4.4}$$

The following result shows that $A \mapsto s(A)$ is 1-Lipschitz for $\|\cdot\|_{\mathrm{HS}}$ and $|\cdot|_2$.

***Theorem 4.2.5* (Hoffman–Wielandt inequality).** — *If $A, B \in \mathcal{M}_{m,n}(\mathbb{K})$ then*

$$\sum_{k=1}^{m\wedge n} (s_k(A) - s_k(B))^2 \leqslant \|A - B\|_{\mathrm{HS}}^2 .$$

Proof. — Let us consider the case where A and B are $d \times d$ Hermitian. We have

$$C = UAU^* = \mathrm{diag}(\lambda_1(A), \ldots, \lambda_d(A)) \text{ and } D = VBV^* = \mathrm{diag}(\lambda_1(B), \ldots, \lambda_d(B))$$

for some $d \times d$ unitary matrices U and V. By unitary invariance, we have

$$\|A - B\|_{\mathrm{HS}}^2 = \|U^*CU - V^*DV\|_{\mathrm{HS}}^2 = \|CUV^* - UV^*D\|_{\mathrm{HS}}^2 = \|CW - WD\|_{\mathrm{HS}}^2$$

where $W = UV^*$. This gives, denoting $P = (|W_{i,j}|^2)_{1\leqslant i,j\leqslant d}$,

$$\|A-B\|_{\mathrm{HS}}^2 = \sum_{i,j=1}^d ((CW)_{i,j} - (WD)_{i,j})^2 = \sum_{i,j=1}^d P_{i,j}(\lambda_i(A) - \lambda_j(B))^2.$$

The expression above is linear in P. Moreover, since W is unitary, the matrix P has all its entries in $[0,1]$ and each of its rows and columns sums up to 1 (we say that P is *doubly stochastic*). If $\mathcal{P}_d$ is the set of all $d \times d$ doubly stochastic matrices then

$$\|A-B\|_{\mathrm{HS}}^2 \geqslant \inf_{Q\in\mathcal{P}_d} \Phi(Q) \quad \text{where} \quad \Phi(Q) = \sum_{i,j=1}^d Q_{i,j}(\lambda_i(A) - \lambda_j(B))^2.$$

But Φ is linear and $\mathcal{P}_d$ is convex and compact, and thus the infimum above is achieved for some extremal point Q of $\mathcal{P}_d$. Now the Birkhoff–von Neumann theorem states that the extremal points of $\mathcal{P}_d$ are exactly the permutation matrices. Recall that $P \in \mathcal{P}_d$ is a permutation matrix when for a permutation π belonging to the symmetric group $\mathcal{S}_d$ of $\{1,\dots,d\}$, we have $P_{i,j} = \delta_{\pi(i),j}$ for every $i,j \in \{1,\dots,d\}$. This gives

$$\|A-B\|_{\mathrm{HS}}^2 \geqslant \min_{\pi\in\mathcal{S}_d} \sum_{i=1}^d (\lambda_i(A) - \lambda_{\pi(i)}(B))^2.$$

Finally, the desired inequality for arbitrary matrices $A, B \in \mathcal{M}_{m,n}(\mathbb{K})$ follows from the Hermitian case above used for their Hermitization H_A and H_B (see (4.1)). □

Remark 4.2.6 **(Fréchet–Wasserstein distance)**. — *The Fréchet–Wasserstein W_2 coupling distance between two probability measures η_1, η_2 on $\mathbb{R}$ with finite second moment is defined by $W_2(\eta_1,\eta_2) = \inf \sqrt{\mathbb{E}(|X_1 - X_2|^2)}$ where the infimum runs over the set of couples of random variables (X_1, X_2) on $\mathbb{R}\times\mathbb{R}$ with $X_1 \sim \eta_1$ and $X_2 \sim \eta_2$. Let us consider the finite discrete case where $\eta_1 = \frac{1}{m}\sum_{i=1}^m \delta_{a_i}$ and $\eta_2 = \frac{1}{m}\sum_{i=1}^m \delta_{b_i}$ where $(a_i)_{1\leqslant i\leqslant m}$ and $(b_i)_{1\leqslant i\leqslant m}$ are non-increasing sequences in $[0,\infty)$. If (X_1,X_2) is a couple of random variables in $[0,\infty)^2$ with $X_1 \sim \eta_1$ and $X_2 \sim \eta_2$, then, denoting $C_{i,j} = \mathbb{P}(X_1 = a_i, X_2 = b_j)$ for every $i,j \in \{1,\dots,m\}$,*

$$\mathbb{E}(|X_1 - X_2|^2) = \sum_{1\leqslant i,j\leqslant m} C_{i,j}(a_i - b_j)^2.$$

The marginal constraints on the couple (X_1,X_2) are actually equivalent to state that the matrix $(mC_{i,j})_{1\leqslant i,j\leqslant m}$ is doubly stochastic. Consequently, as in the proof of Theorem 4.2.5, by using the Birkhoff–von Neumann theorem, we get

$$W_2(\eta_1,\eta_2)^2 = \inf_{mC\in\mathcal{P}_d} \sum_{1\leqslant i,j\leqslant m} C_{i,j}(a_i - b_j)^2 = \frac{1}{m}\min_{\pi\in\mathcal{S}_d}\sum_{i=1}^m (a_i - b_{\pi(i)})^2 = \frac{1}{m}\sum_{i=1}^m (a_i - b_i)^2.$$

Unitary invariant norms. — For every $k \in \{1,\dots,m\wedge n\}$ and any real number $p \geqslant 1$, the map $A \in \mathcal{M}_{m,n}(\mathbb{K}) \mapsto (s_1(A)^p + \cdots + s_k(A)^p)^{1/p}$ is a left and right unitary invariant norm on $\mathcal{M}_{m,n}(\mathbb{K})$. We recover the operator norm $\|A\|_{2\to2}$ for $k = 1$ and the trace norm $\|A\|_{\mathrm{HS}}$ for $(k,p) = (m\wedge n, 2)$. The special case $(k,p) = (m\wedge n, 1)$

gives the Ky Fan norms, while the special case $k = m \wedge n$ gives the Schatten norms, a concept already considered in the first chapter.

4.3. Relationships between eigenvalues and singular values

We know that if $A \in \mathcal{M}_{n,n}(\mathbb{K})$ is normal (i.e. $AA^* = A^*A$) then $s_k(A) = |\lambda_k(A)|$ for every $k \in \{1,\dots,n\}$. Beyond normal matrices, for every $A \in \mathcal{M}_{n,n}(\mathbb{K})$ with row vectors $R_1,\dots,R_n$, we have, by viewing $|\det(A)|$ as the volume of a parallelepiped,

$$|\det(A)| = \prod_{k=1}^{n} |\lambda_k(A)| = \prod_{k=1}^{n} s_k(A) = \prod_{k=1}^{n} \mathrm{dist}(R_k, \mathrm{span}\{R_1,\dots,R_{k-1}\}) \qquad (4.5)$$

(basis $\times$ height etc.). The following result, due to Weyl, is less global and more subtle.

Theorem 4.3.1 **(Weyl inequalities)**. — *If $A \in \mathcal{M}_{n,n}(\mathbb{K})$, then*

$$\forall k \in \{1,\dots,n\}, \quad \prod_{i=1}^{k} |\lambda_i(A)| \leqslant \prod_{i=1}^{k} s_i(A) \quad \text{and} \quad \prod_{i=k}^{n} s_i(A) \leqslant \prod_{i=k}^{n} |\lambda_i(A)|. \qquad (4.6)$$

Equalities are achieved in (4.6) for $k = n$ and $k = 1$ respectively thanks to (4.5).

Proof. — Let us prove first that if $A \in \mathcal{M}_{m,n}(\mathbb{C})$ then for every unitary matrices $V \in \mathcal{M}_{m,m}(\mathbb{C})$ and $W \in \mathcal{M}_{n,n}(\mathbb{C})$ and for every $k \leqslant m \wedge n$, denoting $V_k = V_{1:m,1:k}$ and $W_k = W_{1:n,1:k}$ the matrices formed by the first k columns of V and W respectively,

$$|\det(V_k^* A W_k)| \leqslant s_1(A) \cdots s_k(A). \qquad (4.7)$$

Indeed, since $(V^*AW)_{1:k,1:k} = V_k^* A W_k$, we get from Theorem 4.2.4 and unitary invariance that $s_i(V_k^* A W_k) \leqslant s_i(V^*AW) = s_i(A)$ for every $i \in \{1,\dots,k\}$, and therefore

$$|\det(V_k^* A W_k)| = s_1(V_k^* A W_k) \cdots s_k(V_k^* A W_k) \leqslant s_1(A) \cdots s_k(A),$$

which gives (4.7). We turn now to the proof of (4.6). The right hand side inequalities follow actually from the left hand side inequalities, for instance by taking the inverse if A is invertible, and using the density of invertible matrices and the continuity of the eigenvalues and the singular values if not (both are continuous since they are the roots of a polynomial with polynomial coefficients in the matrix entries). Let us prove the left hand side inequalities in (4.6). By the Schur unitary decomposition, there exists a $\mathbb{C}$-unitary matrix $U \in \mathcal{M}_{n,n}(\mathbb{C})$ such that the matrix $T = U^*AU$ is upper triangular with diagonal $\lambda_1(A),\dots,\lambda_n(A)$. For every $k \in \{1,\dots,n\}$, we have

$$T_{1:k,1:k} = (U^*AU)_{1:k,1:k} = U_k^* A U_k.$$

Thus $U_k^* A U_k$ is upper triangular with diagonal $\lambda_1(A),\dots,\lambda_k(A)$. From (4.7) we get

$$|\lambda_1(A) \cdots \lambda_k(A)| = |\det(T_{1:k,1:k})| = |\det(U_k^* A U_k)| \leqslant s_1(A) \cdots s_k(A).$$

$\square$

In matrix analysis and convex analysis, it is customary to say that Weyl's inequalities express a *logarithmic majorization* between the sequences $|\lambda_n(A)|,\dots,|\lambda_1(A)|$ and $s_n(A),\dots,s_1(A)$. Such a logarithmic majorization has a number of consequences. In particular, it implies that for every real valued function φ such that $t\mapsto\varphi(e^t)$ is increasing and convex on $[s_n(A),s_1(A)]$, we have

$$\forall k\in\{1,\dots,n\},\quad \sum_{i=1}^k\varphi(|\lambda_i(A)|)\leqslant\sum_{i=1}^k\varphi(s_i(A)). \tag{4.8}$$

In particular, we obtain from (4.8) that

$$\sum_{k=1}^n|\lambda_k(A)|^2\leqslant\sum_{k=1}^n s_k(A)^2=\mathrm{Tr}(AA^*)=\sum_{i,j=1}^n|A_{i,j}|^2=\|A\|_{\mathrm{HS}}^2. \tag{4.9}$$

Let us mention the following result, a sort of a converse to Weyl inequalities (4.6).

***Theorem 4.3.2* (Horn inverse problem).** — *If $\lambda\in\mathbb{C}^n$ and $s\in[0,\infty)^n$ satisfy $|\lambda_1|\geqslant\cdots\geqslant|\lambda_n|$ and $s_1\geqslant\cdots\geqslant s_n$ and the Weyl relationships* (4.6) *then there exists $A\in\mathcal{M}_{n,n}(\mathbb{C})$ such that $\lambda_i(A)=\lambda_i$ and $s_i(A)=s_i$ for every $i\in\{1,\dots,n\}$.*

From (4.6) we get $s_n(A)\leqslant|\lambda_n(A)|\leqslant|\lambda_1(A)|\leqslant s_1(A)$ for any $A\in\mathcal{M}_{n,n}(\mathbb{K})$. In particular, we have the following spectral radius / operator norm comparison:

$$\rho(A)=|\lambda_1(A)|\leqslant s_1(A)=\|A\|_{2\to2}.$$

In this spirit, the following result allows to estimate the spectral radius $\rho(A)$ with the operator norm of the powers of A. The proof relies on the fact that thanks to the finite dimension, all norms are equivalent, and in particular equivalent to a sub-multiplicative norm. The result remains valid on Banach algebras, for which the norm is sub-multiplicative by definition (the proof is less elementary than for matrices).

***Theorem 4.3.3* (Gelfand spectral radius formula).** — *For any norm $\|\cdot\|$ on the finite dimensional vector space $\mathcal{M}_{n,n}(\mathbb{C})$ and for every matrix $A\in\mathcal{M}_{n,n}(\mathbb{C})$,*

$$\rho(A)=|\lambda_1(A)|=\lim_{k\to\infty}\left\|A^k\right\|^{1/k}.$$

Proof. — Recall that the $\ell^n_\infty(\mathbb{C})$ operator norm defined for every $A\in\mathcal{M}_{n,n}(\mathbb{C})$ by

$$\|A\|_\infty=\max_{\substack{x\in\mathbb{C}^n\\ \|x\|_\infty=1}}\|Ax\|_\infty=\max_{1\leqslant i\leqslant n}\sum_{j=1}^n|A_{i,j}|$$

is sub-multiplicative, as every operator norm, i.e. $\|AB\|_\infty\leqslant\|A\|_\infty\|B\|_\infty$ for every $A,B\in\mathcal{M}_{n,n}(\mathbb{C})$. From now on, we fix $A\in\mathcal{M}_{n,n}(\mathbb{C})$. Let $\ell_1,\dots,\ell_r$ be the distinct eigenvalues of A, with multiplicities $n_1,\dots,n_r$. We have $n_1+\cdots+n_r=n$. The Jordan decomposition states that there exists an invertible matrix $P\in\mathcal{M}_{n,n}(\mathbb{C})$ such that

$$J=PAP^{-1}=J_1\oplus\cdots\oplus J_r$$

is bloc diagonal, upper triangular, and bidiagonal, with for all $m\in\{1,\dots,r\}$, $J_m=\ell_mI+N\in\mathcal{M}_{n_m,n_m}(\mathbb{C})$ where I is the $m\times m$ identity matrix and where N is the

$m \times m$ nilpotent matrix given by $N_{i,j} = \delta_{i+1,j}$ for every $i, j \in \{1, \ldots, n_m\}$. Let us prove now the following couple of statements:

(i) $\rho(A) < 1$ if and only if $\lim_{k\to\infty} A^k = 0$,
(ii) if $\rho(A) > 1$ then $\lim_{k\to\infty} \|A^k\| = \infty$.

Proof of (i). If $\lim_{k\to\infty} A^k = 0$ then for any eigenvalue λ of A with eigenvector x,

$$\lim_{k\to\infty} \lambda^k x = \lim_{k\to\infty} A^k x = 0.$$

Since $x \neq 0$, we get $\lim_{k\to\infty} \lambda^k = 0$, giving $\rho(A) < 1$. Conversely, if $\rho(A) < 1$ then the eigenvalues of A have module < 1, and computing J^k gives then $\lim_{k\to\infty} A^k = 0$.

Proof of (ii). If $\rho(A) > 1$ then A has an eigenvalue λ with $|\lambda| > 1$, and thus $\lim_{k\to\infty} |(J^k)_{i,i}| = \lim_{k\to\infty} |\lambda|^k = \infty$ for some $i \in \{1, \ldots, n\}$. This gives

$$\lim_{k\to\infty} \|J^k\|_\infty = \infty.$$

Now since $J^k = PA^kP^{-1}$ and since $\|\cdot\|_\infty$ is sub-multiplicative, we get

$$\lim_{k\to\infty} \|A^k\|_\infty = \infty.$$

Finally, since all norms are equivalent we obtain

$$\lim_{k\to\infty} \|A^k\| = \infty.$$

Proof of main result. For any $\varepsilon > 0$, if $A_\varepsilon = (\rho(A) + \varepsilon)^{-1}A$ and since $\rho(A_\varepsilon) < 1$, we get by (i) that $\lim_{k\to\infty} A_\varepsilon^k = 0$. In particular, $\|A_\varepsilon^k\| \leqslant 1$ for k large enough. In other words, $\|A^k\| \leqslant (\varepsilon + \rho(A))^k$ for k large enough. Next, if $A_{-\varepsilon} = (\rho(A) - \varepsilon)^{-1}A$, then $\rho(A_{-\varepsilon}) > 1$, and (ii) gives $\lim_{k\to\infty} \|A^k\| = \infty$, and thus $\|A^k\| \geqslant (\rho(A) - \varepsilon)^k$ for k large enough. Since $\varepsilon > 0$ is arbitrary, we get $\lim_{k\to\infty} \sqrt[k]{\|A^k\|} = \rho(A)$. □

The eigenvalues of non normal matrices are far more sensitive to perturbations than the singular values, and this is captured by the notion of *pseudo-spectrum*:

$$\text{pseudospec}_\varepsilon(A) = \bigcup_{\|B-A\|_{2\to2}\leqslant\varepsilon} \{\lambda_1(B), \ldots, \lambda_n(B)\}.$$

If A is normal then $\text{pseudospec}_\varepsilon(A)$ is an ε-neighborhood of the spectrum of A.

4.4. Relation with rows distances

The following couple of results relate the singular values of matrices to distances between rows (or columns). For square random matrices, they provide a convenient control on the operator norm and trace norm of the inverse respectively. Such bounds are particularly helpful for random matrices.

***Theorem 4.4.1* (Rows and operator norm).** — *If $A \in \mathcal{M}_{m,n}(\mathbb{K})$ with $m \leqslant n$ has row vectors $R_1, \ldots, R_m$, then, denoting $R_{-i} = \text{span}\{R_j : j \neq i\}$, we have*

$$m^{-1/2} \min_{1\leqslant i\leqslant m} \text{dist}_2(R_i, R_{-i}) \leqslant s_{m\wedge n}(A) \leqslant \min_{1\leqslant i\leqslant m} \text{dist}_2(R_i, R_{-i}).$$

Proof. — Note that $R_1, \dots, R_m$ are the columns of $B = A^\top \in \mathcal{M}_{n,m}(\mathbb{K})$ and that A and B have the same singular values. For every $x \in \mathbb{K}^m$ and every $i \in \{1, \dots, m\}$, the triangle inequality and the identity $Bx = x_1R_1 + \cdots + x_mR_m$ give

$$|Bx|_2 \geqslant \mathrm{dist}_2(Bx, R_{-i}) = \min_{y \in R_{-i}} |Bx - y|_2 = \min_{y \in R_{-i}} |x_iR_i - y|_2 = |x_i|\mathrm{dist}_2(R_i, R_{-i}).$$

If $|x|_2 = 1$ then necessarily $|x_i| \geqslant m^{-1/2}$ for some $i \in \{1, \dots, m\}$, and therefore

$$s_{n\wedge m}(B) = \min_{|x|_2=1} |Bx|_2 \geqslant m^{-1/2} \min_{1\leqslant i\leqslant m} \mathrm{dist}_2(R_i, R_{-i}).$$

Conversely, for any $i \in \{1, \dots, m\}$, there exists a vector $y \in \mathbb{K}^m$ with $y_i = 1$ such that

$$\mathrm{dist}_2(R_i, R_{-i}) = |y_1R_1 + \cdots + y_mR_m|_2 = |By|_2 \geqslant |y|_2 \min_{|x|_2=1} |Bx|_2 \geqslant s_{n\wedge m}(B)$$

where we used the fact that $|y|_2^2 = |y_1|^2 + \cdots + |y_n|^2 \geqslant |y_i|^2 = 1$. □

***Theorem 4.4.2* (Rows and trace norm).** — *If $A \in \mathcal{M}_{m,n}(\mathbb{K})$ with $m \leqslant n$ has rows $R_1, \dots, R_m$ and if* $\mathrm{rank}(A) = m$ *then, denoting* $R_{-i} = \mathrm{span}\{R_j : j \neq i\}$,

$$\sum_{i=1}^m s_i^{-2}(A) = \sum_{i=1}^m \mathrm{dist}_2(R_i, R_{-i})^{-2}.$$

Proof. — The orthogonal projection of R_i^* on R_{-i} is $B^*(BB^*)^{-1}BR_i^*$ where B is the $(m-1) \times n$ matrix obtained from A by removing the row R_i. In particular, we have

$$|R_i|_2^2 - \mathrm{dist}_2(R_i, R_{-i})^2 = \left|B^*(BB^*)^{-1}BR_i^*\right|_2^2 = (BR_i^*)^*(BB^*)^{-1}BR_i^*$$

by the Pythagoras theorem. On the other hand, the Schur bloc inversion formula states that if M is a $m \times m$ matrix then for every partition $\{1, \dots, m\} = I \cup I^c$,

$$(M^{-1})_{I,I} = (M_{I,I} - M_{I,I^c}(M_{I^c,I^c})^{-1}M_{I^c,I})^{-1}.$$

Now we take $M = AA^*$ and $I = \{i\}$, and we note that $(AA^*)_{i,j} = R_iR_j^*$, which gives

$$((AA^*)^{-1})_{i,i} = (R_iR_i^* - (BR_i^*)^*(BB^*)^{-1}BR_i^*)^{-1} = \mathrm{dist}_2(R_i, R_{-i})^{-2}.$$

The desired formula follows by taking the sum over $i \in \{1, \dots, m\}$. □

4.5. Gaussian random matrices

This section gathers some facts concerning random matrices with i.i.d. Gaussian entries. The standard Gaussian law on $\mathbb{K}$ is $\mathcal{N}(0,1)$ if $\mathbb{K} = \mathbb{R}$ and $\mathcal{N}(0, \frac{1}{2}I_2)$ if $\mathbb{K} = \mathbb{C} = \mathbb{R}^2$. If Z is a standard Gaussian random variable on $\mathbb{K}$ then

$$\mathrm{Var}(Z) = \mathbb{E}(|Z - \mathbb{E}Z|^2) = \mathbb{E}(|Z|^2) = 1.$$

Let $(G_{i,j})_{i,j\geqslant 1}$ be i.i.d. standard Gaussian random variables on $\mathbb{K}$. For any $m, n \geqslant 1$,

$$G = (G_{i,j})_{1\leqslant i\leqslant m,\, 1\leqslant j\leqslant n}$$

is a random $m \times n$ matrix with density in $\mathcal{M}_{m,n}(\mathbb{K}) \equiv \mathbb{K}^{nm}$ proportional to

$$G \mapsto \exp\left(-\frac{\beta}{2}\sum_{i=1}^{m}\sum_{j=1}^{n}|G_{i,j}|^2\right) = \exp\left(-\frac{\beta}{2}\mathrm{Tr}(GG^*)\right) = \exp\left(-\frac{\beta}{2}\|G\|_{\mathrm{HS}}^2\right)$$

where

$$\beta = \begin{cases} 1 & \text{if } \mathbb{K} = \mathbb{R}, \\ 2 & \text{if } \mathbb{K} = \mathbb{C}. \end{cases}$$

The law of G is unitary invariant in the sense that $UGV \overset{d}{=} G$ for every deterministic $\mathbb{K}$–unitary matrices U $(m \times m)$ and V $(n \times n)$. We say that the random $m \times n$ matrix G belongs to the Ginibre Ensemble, real if $\beta = 1$ and complex if $\beta = 2$.

Remark 4.5.1 **(Complex Ginibre and GUE)**. — *If $m = n$ and $\beta = 2$ then $H_1 = \frac{1}{2}(G + G^*)$ and $H_2 = \frac{1}{2\sqrt{-1}}(G - G^*)$ are independent and in the Gaussian Unitary Ensemble (GUE). Conversely, if H_1 and H_2 are independent $m \times m$ random matrices in the GUE then $H_1 + \sqrt{-1}\,H_2$ has the law of G with $m = n$ and $\beta = 2$.*

Theorem 4.5.2 **(Wishart)**. — *Let $\mathcal{S}_m^+$ be the cone of $m \times m$ Hermitian positive definite matrices. If $m \leqslant n$ then the law of the random Hermitian matrix $W = GG^*$ is a Wishart distribution with Lebesgue density proportional to*

$$W \mapsto \det(W)^{\beta(n-m+1)/2-1}\exp\left(-\frac{\beta}{2}\mathrm{Tr}(W)\right)\mathbf{1}_{\mathcal{S}_m^+}(W).$$

Idea of the proof. — The Gram–Schmidt algorithm for the rows of G furnishes a $n \times m$ matrix V such that $T = GV$ is $m \times m$ lower triangular with a real positive diagonal. Note that V can be completed into a $n \times n$ $\mathbb{K}$–unitary matrix. We have

$$W = GVV^*G^* = TT^*, \quad \det(W) = \det(T)^2 = \prod_{k=1}^{m} T_{k,k}^2, \quad \text{and} \quad \mathrm{Tr}(W) = \sum_{i,j=1}^{m}|T_{i,j}|^2.$$

The desired result follows from the formulas for the Jacobian of the change of variables $G \mapsto (T, V)$ and $T \mapsto TT^*$ and the integration of the independent variable V. □

From the statistical point of view, the Wishart distribution can be understood as a sort of multivariate χ^2 distribution. Note that the determinant $\det(W^{\beta(n-m+1)/2-1})$ disappears when $n = m + (2-\beta)/\beta$ (i.e. $m = n$ if $\beta = 2$ or $n = m + 1$ if $\beta = 1$). From the physical point of view, the “potential” – which is minus the logarithm of the density – is purely spectral and is given up to an additive constant by

$$W \mapsto \sum_{i=1}^{m}\mathcal{E}(\lambda_i(W)) \quad \text{where} \quad \mathcal{E}(\lambda) = \frac{\beta}{2}\lambda - \frac{\beta(n-m+1)-2}{2}\log(\lambda).$$

Theorem 4.5.3 **(Bidiagonalization)**. — *If $m \leqslant n$ then there exists two random $\mathbb{K}$–unitary matrices U $(m \times m)$ and V $(n \times n)$ such that $B = \sqrt{\beta}UGV \in \mathcal{M}_{m,n}(\mathbb{K})$*

is lower triangular and bidiagonal with independent real entries of law

$$\begin{pmatrix} \chi_{\beta n} & 0 & 0 & 0 & & \cdots & & & 0 \\ \chi_{\beta(m-1)} & \chi_{\beta(n-1)} & 0 & 0 & & \cdots & & & 0 \\ 0 & \chi_{\beta(m-2)} & \chi_{\beta(n-2)} & 0 & & \cdots & & & 0 \\ 0 & 0 & \ddots & \ddots & & \cdots & & & 0 \\ \vdots & \vdots & & & & \cdots & & & 0 \\ 0 & 0 & 0 & \cdots\ 0 & \chi_\beta & \chi_{\beta(n-(m-1))} & 0 & \cdots & 0 \end{pmatrix}.$$

Recall that if $X_1, \ldots, X_\ell$ are independent and identically distributed with law $\mathcal{N}(0,1)$ then $\|X\|_2^2 = X_1^2 + \cdots + X_\ell^2 \sim \chi_\ell^2$ and $\|X\|_2 = \sqrt{X_1^2 + \cdots + X_\ell^2} \sim \chi_\ell$. The densities of χ_ℓ^2 and χ_ℓ are proportional to $t \mapsto t^{\ell/2-1}e^{-t/2}$ and $t \mapsto t^{\ell-1}e^{-t^2/2}$.

Idea of the proof. — The desired result follows from (4.3) and basic properties of Gaussian laws (Cochran's theorem on the orthogonal Gaussian projections). □

Here is an application of Theorem 4.5.3 : since B and G have same singular values, one may use B for their simulation, reducing the dimension from nm to $2m-1$.

Theorem 4.5.4 **(Laguerre Ensembles).** — *If $m \leqslant n$ then the random vector*

$$(s_1^2(G), \ldots, s_m^2(G)) = (\lambda_1(GG^*), \ldots, \lambda_m(GG^*))$$

admits a density on $\{\lambda \in [0,\infty)^m : \lambda_1 \geqslant \cdots \geqslant \lambda_n\}$ proportional to

$$\lambda \mapsto \exp\left(-\frac{\beta}{2}\sum_{i=1}^m \lambda_i\right) \prod_{i=1}^m \lambda_i^{\beta(n-m+1)/2-1} \prod_{1\leqslant i<j\leqslant m} (\lambda_i - \lambda_j)^\beta.$$

The correlation is captured by the Vandermonde determinant and expresses an electrostatic logarithmic repulsive potential, given up to an additive constant by

$$\lambda \mapsto \frac{\beta}{2}\left(\sum_{i=1}^m \lambda_i - (\beta(n-m+1)-2)\sum_{1\leqslant i<j\leqslant m} \log(\lambda_i - \lambda_j)\right).$$

On the other hand, we recognize in the expression of the density the Laguerre weight $t \mapsto t^\alpha e^{-t}$. We say that GG^* belongs to the β–Laguerre ensemble or Laguerre Orthogonal Ensemble (LOE) for $\beta = 1$ and Laguerre Unitary Ensemble (LUE) for $\beta = 2$.

Proof. — Let us consider the $m \times m$ tridiagonal real symmetric matrix

$$T = \begin{pmatrix} a_m & b_{m-1} & & & \\ b_{m-1} & a_{m-1} & b_{m-2} & & \\ & \ddots & \ddots & \ddots & \\ & & b_2 & a_2 & b_1 \\ & & & b_1 & a_1 \end{pmatrix}.$$

We denote by $\lambda_1, \ldots, \lambda_m \in \mathbb{R}$ its eigenvalues. Let $v_1, \ldots, v_m$ be an orthonormal system of eigenvectors. If V is the $m \times m$ orthogonal matrix with columns $v_1, \ldots, v_m$

then $T = V\mathrm{diag}(\lambda_1, \ldots, \lambda_m)V^\top$. For every $k \in \{1, \ldots, m\}$, the equation $Tv_k = \lambda_k v_k$ writes, for every $i \in \{1, \ldots, m\}$, with the convention $b_0 = b_m = v_{k,0} = v_{k,m+1} = 0$,

$$b_{m-i+1}v_{k,i-1} + a_{m-i+1}v_{k,i} + b_{m-i}v_{k,i+1} = \lambda_k v_{k,i}.$$

It follows from these recursive equations that the matrix V is entirely determined by its first row $r = (r_1, \ldots, r_m) = (v_{1,1}, \ldots, v_{m,1})$ and $\lambda_1, \ldots, \lambda_m$. From now on, we assume that $\lambda_i \neq \lambda_j$ for every $i \neq j$ and that $r_1 > 0, \ldots, r_m > 0$, which makes V unique. Our first goal is to compute the Jacobian of the change of variable

$$(a, b) \mapsto (\lambda, r).$$

Note that $r_1^2 + \cdots + r_m^2 = 1$. For every $\lambda \notin \{\lambda_1, \ldots, \lambda_m\}$ we have

$$((T - \lambda I)^{-1})_{1,1} = \sum_{i=1}^m \frac{r_i^2}{\lambda_i - \lambda}.$$

On the other hand, for every $m \times m$ matrix A with $\det(A) \neq 0$, we have

$$(A^{-1})_{1,1} = \frac{\det(A_{m-1})}{\det(A)}$$

where A_k stands for the $k \times k$ right bottom sub-matrix $A_k = (A_{i,j})_{m-k+1 \leqslant i,j \leqslant m}$. If $\lambda_{k,1}, \ldots, \lambda_{k,k}$ are the eigenvalues of T_k, then we obtain, with $A = T - \lambda I$,

$$\frac{\prod_{i=1}^{m-1}(\lambda_{m-1,i} - \lambda)}{\prod_{i=1}^m(\lambda_i - \lambda)} = \sum_{i=1}^m \frac{r_i^2}{\lambda_i - \lambda}.$$

Recall that $\lambda_1, \ldots, \lambda_m$ are all distinct. By denoting $P_k(\lambda) = \prod_{i=1}^k(\lambda - \lambda_{k,i})$ the characteristic polynomial of T_k, we get, for every $i \in \{1, \ldots, m\}$,

$$\frac{P_{m-1}(\lambda_i)}{P_m'(\lambda_i)} = r_i^2.$$

Since $P_m'(\lambda_i) = \prod_{1 \leqslant j \neq i \leqslant m}(\lambda_i - \lambda_j)$ we obtain

$$\prod_{i=1}^m r_i^2 = \frac{\prod_{i=1}^m |P_{m-1}(\lambda_i)|}{\prod_{1 \leqslant i < j \leqslant m}(\lambda_i - \lambda_j)^2}.$$

Let us rewrite the numerator of the right hand side. By expanding the first row in the determinant $\det(\lambda I - T) = P_m(\lambda)$, we get, with $P_{-1} = 0$ and $P_0 = 1$,

$$P_m(\lambda) = (\lambda - a_m)P_{m-1}(\lambda) - b_{m-1}^2 P_{m-2}(\lambda).$$

Additionally, we obtain

$$\prod_{i=1}^{m-1} |P_m(\lambda_{m-1,i})| = b_{m-1}^{2(m-1)} \prod_{i=1}^{m-1} |P_{m-2}(\lambda_{m-1,i})|.$$

Now the observation

$$\prod_{i=1}^{m-1} |P_{m-2}(\lambda_{m-1,i})| = \prod_{i=1}^{m-1}\prod_{j=1}^{m-2} |\lambda_{m-2,j} - \lambda_{m-1,i}| = \prod_{j=1}^{m-2} |P_{m-1}(\lambda_{m-2,j})|$$

leads by induction to the identity

$$\prod_{i=1}^{m-1} |P_m(\lambda_{m-1,i})| = \prod_{i=1}^{m-1} b_i^{2i}.$$

Finally, we have shown that

$$\prod_{1\leqslant i<j\leqslant m} (\lambda_i - \lambda_j)^2 = \frac{\prod_{i=1}^{m-1} b_i^{2i}}{\prod_{i=1}^{m} r_i^2}. \tag{4.10}$$

To compute the Jacobian of the change of variable $(a, b) \mapsto (\lambda, r)$, we start from

$$((I - \lambda T)^{-1})_{1,1} = \sum_{i=1}^{m} \frac{r_i^2}{1 - \lambda\lambda_i}$$

with $|\lambda| < 1/\max(\lambda_1, \dots, \lambda_m)$ (this gives $\|\lambda T\|_{2\to 2} < 1$). By expanding both sides in power series of λ and identifying the coefficients, we get the system of equations

$$(T^k)_{1,1} = \sum_{i=1}^{m} r_i^2 \lambda_i^k \quad \text{where} \quad k \in \{0, 1, \dots, 2m-1\}.$$

Since $(T^k)_{1,1} = \langle T^k e_1, e_1\rangle$ and since T is tridiagonal, we see that this system of equations is triangular with respect to the variables $a_m, b_{m-1}, a_{m-1}, b_{m-2}, \dots$. The first equation is $1 = r_1^2 + \cdots + r_m^2$ and gives $-r_m dr_m = r_1 dr_1 + \cdots + r_{m-1} dr_{m-1}$. This identity and the remaining triangular equations give, after some tedious calculus,

$$dadb = \pm \frac{1}{r_m} \frac{\prod_{i=1}^{m-1} b_i}{\prod_{i=1}^{m} r_i} \left(\frac{\prod_{i=1}^{m} r_i^2}{\prod_{i=1}^{m-1} b_i^{2i}} \right)^2 \prod_{1\leqslant i<j\leqslant m} (\lambda_i - \lambda_j)^4 \, d\lambda dr.$$

which gives, using (4.10),

$$dadb = \pm \frac{1}{r_m} \frac{\prod_{i=1}^{m-1} b_i}{\prod_{i=1}^{m} r_i} \, d\lambda dr. \tag{4.11}$$

Let us consider now the $m \times n$ lower triangular bidiagonal real matrix ($m \leqslant n$)

$$B = \begin{pmatrix} x_n & & & \\ y_{m-1} & x_{n-1} & & \\ & \ddots & \ddots & \\ & & y_1 & x_{n-(m-1)} \end{pmatrix}$$

The matrix $T = BB^\top$ is $m \times m$ symmetric tridiagonal and for $i \in \{1, \dots, m-1\}$,

$$a_m = x_n^2, \quad a_i = y_i^2 + x_{n-(m-i)}^2, \quad b_i = y_i x_{n-(m-i)+1}. \tag{4.12}$$

Let us assume that B has real non negative entries. We get, after some calculus,

$$dxdy = \left(2^m x_{n-(m-1)} \prod_{i=0}^{m-2} x_{n-i}^2 \right)^{-1} dadb. \tag{4.13}$$

From Theorem 4.5.3 we have, with a normalizing constant $c_{m,n,\beta}$,

$$dB = c_{m,n,\beta} \prod_{i=0}^{m-1} x_{n-i}^{\beta(n-i)-1} \prod_{i=1}^{m-1} y_i^{\beta i-1} \exp\left(-\frac{\beta}{2}\sum_{i=0}^{m-1} x_{n-i}^2 - \frac{\beta}{2}\sum_{i=1}^{m-1} y_i^2\right) dxdy.$$

Let us consider T as a function of λ and r. We first note that

$$\sum_{i=0}^{m-1} x_{n-i}^2 + \sum_{i=1}^{m-1} y_i^2 = \mathrm{Tr}(BB^\top) = \mathrm{Tr}(T) = \sum_{i=1}^{m} \lambda_i.$$

Since the law of B is unitary (orthogonal!) invariant, we get that λ and r are independent and with probability one the components of λ are all distinct. Let φ be the density of r (can be made explicit). Using (4.11-4.12-4.13), we obtain

$$dB = c_{m,n,\beta} \frac{\prod_{i=0}^{m-1} x_{n-i}^{\beta(n-i)-2} \prod_{i=1}^{m-1} y_i^{\beta i}}{r_m \prod_{i=1}^{m} r_i} \exp\left(-\frac{\beta}{2}\sum_{i=1}^{m}\lambda_i\right)\varphi(r)\, d\lambda dr.$$

But using (4.10-4.12) we have

$$\prod_{1\leqslant i<j\leqslant m} |\lambda_i - \lambda_j| = \frac{\prod_{i=1}^{m-1} b_i^i}{\prod_{i=1}^{m} r_i} = \frac{\prod_{i=1}^{m-1} y_i^i x_{n-(m-i)+1}^i}{\prod_{i=1}^{m} r_i} = \frac{\prod_{i=0}^{m-1} x_{n-i}^{m-i-1} \prod_{i=1}^{m-1} y_i^i}{\prod_{i=1}^{m} r_i}$$

and therefore

$$dB = c_{m,n,\beta} \frac{\left(\prod_{i=0}^{m-1} x_{n-i}^2\right)^{\frac{1}{2}\beta(n-m+1)-1}}{r_m \prod_{i=1}^{m} r_i} \prod_{1\leqslant i<j\leqslant m} |\lambda_i - \lambda_j|^\beta \exp\left(-\frac{\beta}{2}\sum_{i=1}^{m}\lambda_i\right)\varphi(r)\, d\lambda dr.$$

Now it remains to use the identity $\prod_{i=0}^{m-1} x_{n-i}^2 = \det(B)^2 = \det(T) = \prod_{i=1}^{m} \lambda_i$ to get only (λ, r) variables, and to eliminate the r variable by separation and integration. □

***Remark 4.5.5* (Universality of Gaussian models).** — *Gaussian models of random matrices have the advantage to allow explicit computations. However, in some applications such as in compressed sensing, Gaussian models can be less relevant than discrete models such as Bernoulli/Rademacher models. It turns out that most large dimensional properties are the same, such as in the Marchenko–Pastur theorem.*

4.6. The Marchenko–Pastur theorem

The Marchenko–Pastur theorem concerns the asymptotics of the counting probability measure of the singular values of large random rectangular matrices, with i.i.d. entries, when the aspect ratio (number of rows over number of columns) of the matrix converges to a finite positive real number.

***Theorem 4.6.1* (Marchenko–Pastur).** — *Let $(M_{i,j})_{i,j\geqslant 1}$ be an infinite table of i.i.d. random variables on $\mathbb{K}$ with unit variance and arbitrary mean. Let*

$$\nu_{m,n} = \frac{1}{m}\sum_{k=1}^{m} \delta_{s_k(\frac{1}{\sqrt{n}}M)} = \frac{1}{m}\sum_{k=1}^{m} \delta_{\lambda_k(\sqrt{\frac{1}{n}MM^*})}$$

be the counting probability measure of the singular values of the $m \times n$ random matrix

$$\frac{1}{\sqrt{n}}M = \left(\frac{1}{\sqrt{n}}M_{i,j}\right)_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}.$$

Suppose that $m = m_n$ depends on n in such a way that

$$\lim_{n\to\infty}\frac{m_n}{n} = \rho \in (0,\infty).$$

Then with probability one, for any bounded continuous function $f : [0,\infty) \to \mathbb{R}$,

$$\int f\,d\nu_{m,n} \underset{n\to+\infty}{\longrightarrow} \int f\,d\nu_\rho$$

where ν_ρ is the Marchenko–Pastur law with shape parameter ρ given by

$$\left(1-\frac{1}{\rho}\right)_+ \delta_0 + \frac{1}{\rho\pi x}\sqrt{(b-x^2)(x^2-a)}\,\mathbf{1}_{[\sqrt{a},\sqrt{b}]}(x)dx. \tag{4.14}$$

where $a = (1-\sqrt{\rho})^2$ and $b = (1+\sqrt{\rho})^2$ (atom at point 0 if and only if $\rho > 1$).

Theorem 4.6.1 is a sort of strong law of large numbers: it states the almost sure convergence of the sequence $(\nu_{m,n})_{n\geqslant 1}$ to a deterministic probability measure ν_ρ.

Weak convergence. — Recall that for probability measures, the weak convergence with respect to bounded continuous functions is equivalent to the pointwise convergence of cumulative distribution functions at every continuity point of the limit. This convergence, known as the narrow convergence, corresponds also to the convergence in law of random variables. Consequently, the Marchenko–Pastur Theorem 4.6.1 states that if m depends on n with $\lim_{n\to\infty} m/n = \rho \in (0,\infty)$ then with probability one, for every $x \in \mathbb{R}$ ($x \neq 0$ if $\rho > 1$) denoting $I = (-\infty, x]$,

$$\lim_{n\to\infty}\nu_{m,n}(I) = \nu_\rho(I).$$

Atom at 0. — The atom at 0 in ν_ρ when $\rho > 1$ can be understood by the fact that $s_k(M) = 0$ for any $k > m \wedge n$. If $m \geqslant n$ then $\nu_\rho(\{0\}) \geqslant (m-n)/m$.

Quarter circle law. — When $\rho = 1$ then M is asymptotically square, $a = 0$, $b = 4$, and ν_1 is the so-called *quarter circle law*

$$\frac{1}{\pi}\sqrt{4-x^2}\,\mathbf{1}_{[0,2]}(x)dx.$$

Actually, the normalization factor makes it an ellipse instead of a circle.

Alternate formulation. — Recall that $s_k^2(\frac{1}{\sqrt{n}}M) = \lambda_k(\frac{1}{n}MM^*)$ for every $k \in \{1,\dots,m\}$. The image of $\nu_{m,n}$ by the map $x \mapsto x^2$ is the probability measure

$$\mu_{m,n} = \frac{1}{m}\sum_{k=1}^{m} \delta_{\lambda_k(\frac{1}{n}MM^*)}.$$

Similarly, the image μ_ρ of ν_ρ by the map $x \mapsto x^2$ is given by

$$\left(1-\frac{1}{\rho}\right)_+ \delta_0 + \frac{1}{\rho 2\pi x}\sqrt{(b-x)(x-a)}\,\mathbf{1}_{[a,b]}(x)dx \tag{4.15}$$

where $a = (1-\sqrt{\rho})^2$ and $b = (1+\sqrt{\rho})^2$ as in Theorem 4.6.1. As an immediate consequence, the Marchenko–Pastur theorem 4.6.1 can be usefully rephrased as follows:

Theorem 4.6.2 **(Marchenko–Pastur)**. — *Let $(M_{i,j})_{i,j\geqslant 1}$ be an infinite table of i.i.d. random variables on $\mathbb{K}$ with unit variance and arbitrary mean. Let*

$$\mu_{m,n} = \frac{1}{m}\sum_{k=1}^{m} \delta_{\lambda_k(\frac{1}{n}MM^*)}$$

be the counting probability measure of the eigenvalues of the $m \times m$ random matrix $\frac{1}{n}MM^*$ where $M = (M_{i,j})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$. Suppose that $m = m_n$ depends on n with

$$\lim_{n\to\infty} \frac{m_n}{n} = \rho \in (0,\infty)$$

then with probability one, for any bounded continuous function $f : [0,\infty) \to \mathbb{R}$,

$$\int f\,d\mu_{m,n} \underset{n\to+\infty}{\longrightarrow} \int f\,d\mu_\rho$$

where μ_ρ is the Marchenko–Pastur law defined by (4.15).

Remark 4.6.3 **(First moment and tightness)**. — *By the strong law of large numbers, we have, with probability one,*

$$\begin{aligned}\int x\,d\mu_{m,n}(x) &= \frac{1}{m}\sum_{k=1}^{m} s_k^2(\frac{1}{\sqrt{n}}M)\\ &= \frac{1}{m}\mathrm{Tr}\left(\frac{1}{n}MM^*\right)\\ &= \frac{1}{nm}\sum_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}} |M_{i,j}|^2 \underset{n,m\to+\infty}{\longrightarrow} 1.\end{aligned}$$

This shows the almost sure convergence of the first moment in the Marchenko–Pastur theorem. Moreover, by Markov's inequality, for any $r > 0$, we have

$$\mu_{m,n}([0,r]^c) \leqslant \frac{1}{r}\int x\,d\mu_{m,n}(x).$$

This shows that almost surely the sequence $(\mu_{m_n,n})_{n\geqslant 1}$ is tight.

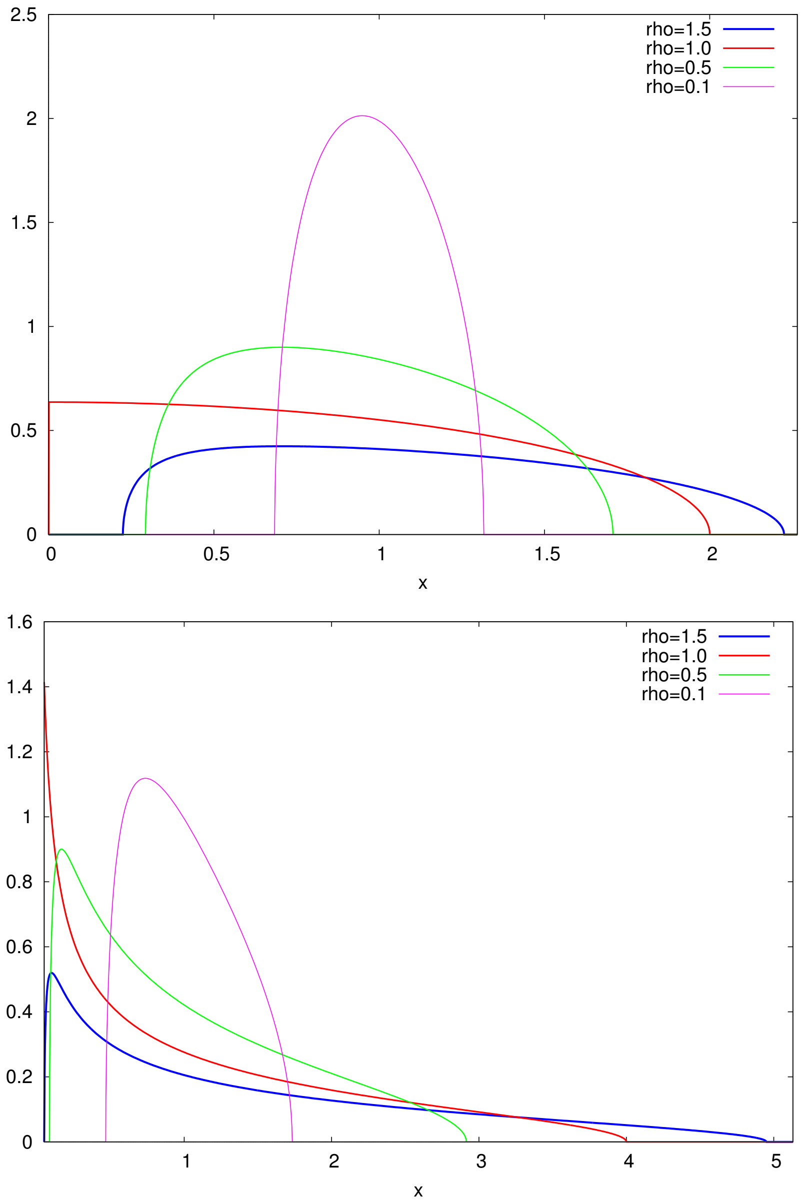

FIGURE 2. Absolutely continuous parts of the Marchenko–Pastur laws ν_ρ (4.14) and μ_ρ (4.15) for different values of the shape parameter ρ. These graphics were produced with the wxMaxima free software package.

***Remark 4.6.4* (Covariance matrices).** — *Suppose that M has centered entries. The column vectors $C_1,\dots,C_n$ of M are independent and identically distributed random vectors of $\mathbb{R}^m$ with mean 0 and covariance I_m, and $\frac{1}{n}MM^*$ is the empirical covariance matrix of this sequence of vectors seen as a sample of $\mathcal{N}(0,I_m)$. We have*

$$\frac{1}{n}MM^* = \frac{1}{n}\sum_{k=1}^n C_k {C_k}^*.$$

Also, if m is fixed then by the strong law of large numbers, with probability one, $\lim_{n\to\infty}\frac{1}{n}MM^* = \mathbb{E}(C_1{C_1}^*) = I_m$. This is outside the regime of the Marchenko–Pastur theorem, for which m depends on n in such a way that $\lim_{n\to\infty} m/n \in (0,\infty)$.

4.7. Proof of the Marchenko–Pastur theorem

This section is devoted to a proof of Theorem 4.6.1. We will actually provide a proof of the equivalent version formulated in Theorem 4.6.2, by using the method of moments. Let us define the truncated matrix $\widetilde{M} = (\widetilde{M}_{i,j})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$ where

$$\widetilde{M}_{i,j} = M_{i,j}\mathbf{1}_{\{|M_{i,j}|\leqslant C\}}$$

with $C>0$. Let us denote the empirical spectral distribution of M and $\widetilde{M}$ by

$$\eta_1 = \mu_{m,n} = \frac{1}{m}\sum_{i=1}^m \delta_{s_i^2(\frac{1}{\sqrt{n}}M)} \quad\text{and}\quad \eta_2 = \frac{1}{m}\sum_{i=1}^m \delta_{s_i^2(\frac{1}{\sqrt{n}}\widetilde{M})}.$$

From Remark 4.2.6 and the Hoffman–Wielandt inequality of Theorem 4.2.5, we get

$$\begin{aligned} W_2^2(\eta_1,\eta_2) &= \frac{1}{m}\sum_{k=1}^{m\wedge n}\left(s_k\left(\frac{1}{\sqrt{n}}M\right) - s_k\left(\frac{1}{\sqrt{n}}\widetilde{M}\right)\right)^2 \\ &\leqslant \frac{1}{m}\left\|\frac{1}{\sqrt{n}}M - \frac{1}{\sqrt{n}}\widetilde{M}\right\|_{\mathrm{HS}}^2 \\ &= \frac{1}{nm}\sum_{i=1}^m\sum_{j=1}^n |M_{i,j}|^2\mathbf{1}_{\{|M_{i,j}|>C\}}. \end{aligned}$$

By the strong law of large numbers, we get, with probability one,

$$\varlimsup_{m,n\to\infty} W_2^2(\eta_1,\eta_2) \leqslant \mathbb{E}(|M_{1,1}|^2\mathbf{1}_{\{|M_{1,1}|>C\}}).$$

Since $M_{1,1}$ has finite second moment, the right hand side can be made arbitrary small by taking C sufficiently large. Now it is well known that the convergence for the W_2 distance implies the weak convergence with respect to continuous and bounded functions. Therefore, one may assume that the entries of M have bounded support (note that by scaling, one may take entries of arbitrary variance, for instance 1).

The next step consists in a reduction to the centered case. Let us define the $m\times n$ centered matrix $\overline{M} = M - \mathbb{E}(M)$, and this time the probability measures η_1,η_2 by

$$\eta_1 = \frac{1}{m}\sum_{i=1}^m \delta_{s_i^2(\frac{1}{\sqrt{n}}M)} \quad\text{and}\quad \eta_2 = \frac{1}{m}\sum_{i=1}^m \delta_{s_i^2(\frac{1}{\sqrt{n}}\overline{M})}.$$

Let $F_1, F_2 : \mathbb{R} \to [0,1]$ be their cumulative distribution functions defined by

$$F_1(x) = \frac{|\{1 \leqslant i \leqslant m : s_i(M) \leqslant \sqrt{nx}\}|}{m} \quad \text{and} \quad F_2(x) = \frac{\left|\{1 \leqslant i \leqslant m : s_i(\overline{M}) \leqslant \sqrt{nx}\}\right|}{m}.$$

Since $\operatorname{rank}(M - \overline{M}) = \operatorname{rank}(\mathbb{E}(M)) \leqslant 1$, we get by Theorem 4.2.3 that

$$\sup_{x\in\mathbb{R}} |F_1(x) - F_2(x)| \leqslant \frac{\operatorname{rank}(M - \overline{M})}{m} \leqslant \frac{1}{m}.$$

We recognize on the left hand side the Kolmogorov–Smirnov distance between η_1 and η_2. Recall that the convergence for this distance implies the weak convergence. Consequently, one may further assume that M has mean 0. Recall that if μ is a random probability measure then $\mathbb{E}\mu$ is the non random probability measure defined by $(\mathbb{E}\mu)(A) = \mathbb{E}(\mu(A))$ for every measurable set A. Lemma 4.7.1 below reduces the problem to the weak convergence of $\mathbb{E}\mu_{m,n}$ to μ_ρ (via the first Borel-Cantelli lemma and the countable test functions $f = \mathbf{1}_{(-\infty,x]}$ with x rational). Next, Lemmas 4.7.3 and 4.7.4 below reduce in turn the problem to the convergence of the moments of $\mathbb{E}\mu_{m,n}$ to the ones of μ_ρ computed in Lemma 4.7.5 below.

Summarizing, it remains to show that if M has i.i.d. entries of mean 0, variance 1, and support $[-C, C]$, and if $\lim_{n\to\infty} m/n = \rho \in (0,\infty)$, then, for every $r \geqslant 1$,

$$\lim_{n\to\infty} \mathbb{E} \int x^r \, d\mu_{m,n} = \sum_{k=0}^{r-1} \frac{\rho^k}{k+1} \binom{r}{k} \binom{r-1}{k}. \tag{4.16}$$

The result is immediate for the first moment ($r = 1$) since

$$\begin{aligned}\mathbb{E} \int x \, d\mu_{m,n} &= \frac{1}{mn} \mathbb{E} \sum_{k=1}^{m} \lambda_k(MM^*) \\ &= \frac{1}{nm} \mathbb{E}\operatorname{Tr}(MM^*) \\ &= \frac{1}{nm} \sum_{\substack{1\leqslant i\leqslant m\\1\leqslant j\leqslant n}} \mathbb{E}(|M_{i,j}|^2) = 1.\end{aligned}$$

This shows actually that $\mathbb{E}\mu_{m,n}$ and μ_ρ have even the same first moment for all values of m and n. The convergence of the second moment ($r = 2$) is far more subtle:

$$\begin{aligned}\mathbb{E} \int x^2 \, d\mu_{m,n} &= \frac{1}{mn^2} \mathbb{E} \sum_{k=1}^{m} \lambda_k^2(MM^*) \\ &= \frac{1}{mn^2} \mathbb{E}\operatorname{Tr}(MM^*MM^*) \\ &= \frac{1}{mn^2} \sum_{\substack{1\leqslant i,k\leqslant m\\1\leqslant j,l\leqslant n}} \mathbb{E}(M_{i,j}\overline{M}_{k,j}M_{k,l}\overline{M}_{i,l}).\end{aligned}$$

If an element of $\{(ij), (kj), (kl), (il)\}$ appears one time and exactly one in the product $M_{i,j}\overline{M}_{k,j}M_{k,l}\overline{M}_{i,l}$ then by the assumptions of independence and mean 0 we get $\mathbb{E}(M_{i,j}\overline{M}_{k,j}M_{k,l}\overline{M}_{i,l}) = 0$. The case when the four elements are the same appears with mn possibilities and is thus asymptotically negligible. It remains only to consider the cases where two different elements appear twice. The case $(ij) = (kj)$ and $(kl) = (il)$ gives $i = k$ and contributes $\mathbb{E}(|M_{i,j}|^2|M_{i,l}|^2) = 1$ with $m(n^2 - n)$ possibilities (here $j \neq l$ since the case $j = l$ was already considered). The case $(ij) = (kl)$ and $(kj) = (il)$ gives $i = k$ (and $j = l$) and was thus already considered. The case $(ij) = (il)$ and $(kj) = (kl)$ gives $j = l$ and contributes $\mathbb{E}(|M_{i,j}|^2|M_{k,j}|^2) = 1$ with $n(m^2 - m)$ possibilities (here $i \neq k$ since the case $i = k$ was already considered). We used here the assumptions of independence, mean 0, and variance 1. At the end, the second moment of $\mathbb{E}\mu_{m,n}$ tends to $\lim_{n\to\infty}(m(n^2 - n) + n(m^2 - m))/(mn^2) = 1 + \rho$ which is the second moment of μ_ρ. We have actually in hand a method reducing the proof of (4.16) to combinatorial arguments. Namely, for all $r \geqslant 1$, we write

$$\int x^r \, d\mu_{m,n}(x) = \frac{1}{mn^r}\sum_{k=1}^{m}\lambda_k(MM^*)^r = \frac{1}{mn^r}\mathrm{Tr}((MM^*)^r)$$

which gives

$$\mathbb{E}\int x^r \, d\mu_{m,n}(x) = \frac{1}{mn^r}\sum_{\substack{1\leqslant i_1,\dots,i_r\leqslant m\\ 1\leqslant j_1,\dots,j_r\leqslant n}} \mathbb{E}(M_{i_1,j_1}\overline{M}_{i_2,j_1}M_{i_2,j_2}\overline{M}_{i_3,j_2}\cdots M_{i_r,j_r}\overline{M}_{i_1,j_r}).$$

Draw $i_1,\dots,i_r$ on a horizontal line representing $\mathbb{N}$ and $j_1,\dots,j_r$ on another parallel horizontal line below the previous one representing another copy of $\mathbb{N}$. Draw r down edges from i_s to j_s and r up edges from j_s to i_{s+1}, with the convention $i_{r+1} = i_1$, for all $s = 1,\dots,r$. This produces an oriented "MP" graph with possibly multiple edges between two nodes (certain vertices or edges of this graph may have a degree larger that one due to the possible coincidence of certain values of i_s or of j_s). We have

$$\mathbb{E}\int x^r \, d\mu_{m,n}(x) = \frac{1}{n^r m}\sum_G \mathbb{E}M_G$$

where $\sum_G$ runs over the set of MP graphs and where M_G is the product of $M_{a,b}$ or $\overline{M}_{a,b}$ over the edges ab of G. We say that two MP graphs are equivalent when they are identical up to permutation of $\{1,\dots,m\}$ and $\{1,\dots,n\}$. Each equivalent class contains a unique canonical graph such that $i_1 = j_1 = 1$ and $i_s \leqslant \max\{i_1,\dots,i_{s-1}\}+1$ and $j_s \leqslant \max\{j_1,\dots,j_{s-1}\} + 1$ for all s. A canonical graph possesses $\alpha + 1$ distinct i-vertices and β distinct j-vertices with $0 \leqslant \alpha \leqslant r - 1$ and $1 \leqslant \beta \leqslant r$. We say that such a canonical graph is $T(\alpha,\beta)$, and we distinguish three types :

- $T_1(\alpha,\beta)$: $T(\alpha,\beta)$ graphs for which each down edge coincides with one and only one up edge. We have necessarily $\alpha + \beta = r$ and we abridge $T_1(\alpha,\beta)$ into $T_1(\alpha)$
- $T_2(\alpha,\beta)$: $T(\alpha,\beta)$ graphs with at least one edge of multiplicity exactly 1
- $T_3(\alpha,\beta)$: $T(\alpha,\beta)$ graphs which are not $T_1(\alpha,\beta)$ nor $T_2(\alpha,\beta)$

We admit the following combinatorial facts :

(C1) the cardinal of the equivalent class of each $T(\alpha,\beta)$ canonical graph is

$$m(m-1)\cdots(m-\alpha)n(n-1)\cdots(n-\beta+1).$$

(C2) each $T_3(\alpha,\beta)$ canonical graph has at most r distinct vertices (i.e. $\alpha + \beta < r$).

(C3) the number of $T_1(\alpha,\beta)$ canonical graphs is

$$\frac{1}{\alpha+1}\binom{r}{\alpha}\binom{r-1}{\alpha}.$$

The quantity $\mathbb{E}(M_G)$ depends only on the equivalent class of G. We denote by $\mathbb{E}(M_{T(\alpha,\beta)})$ the common value to all $T(\alpha,\beta)$ canonical graphs. We get, using (C1),

$$\frac{1}{n^r m}\sum_G M_G = \frac{1}{n^r m}\sum_{T(\alpha,\beta)} m(m-1)\cdots(m-\alpha)n(n-1)\cdots(n-\beta+1)\mathbb{E}(M_{T(\alpha,\beta)})$$

where the sum runs over the set of all canonical graphs. The contribution of T_2 graphs is zero thanks to the assumption of independence and mean 0. The contribution of T_3 graphs is asymptotically negligible since there are few of them. Namely, by the bounded support assumption we have $|M_{T_3(\alpha,\beta)}| \leqslant C^{2r}$, moreover the number of $T_3(\alpha,\beta)$ canonical graphs is bounded by a constant c_r, and then, from (C2), we get

$$\frac{1}{n^r m}\sum_{T_3(\alpha,\beta)} m(m-1)\cdots(m-\alpha)n(n-1)\cdots(n-\beta+1)\mathbb{E}(M_{T(\alpha,\beta)})$$
$$\leqslant \frac{c_r}{n^r m}C^{2r}m^{\alpha+1}n^{\beta} = O(n^{-1}).$$

Therefore we know now that only T_1 graphs contributes asymptotically. Let us consider a $T_1(\alpha,\beta)=T_1(\alpha)$ canonical graph ($\beta = r-\alpha$). Since $M_{T(\alpha,\beta)} = M_{T(\alpha)}$ is a product of squared modules of distinct entries of M, which are independent, of mean 0, and variance 1, we have $\mathbb{E}(M_{T(\alpha)}) = 1$. Consequently, using (C3) we obtain

$$\frac{1}{n^r m}\sum_{T_1(\alpha)} m(m-1)\cdots(m-\alpha)n(n-1)\cdots(n-r+\alpha+1)\mathbb{E}(M_{T(\alpha,r-\alpha)})$$
$$= \sum_{\alpha=0}^{r-1}\frac{1}{1+\alpha}\binom{r}{\alpha}\binom{r-1}{\alpha}\frac{1}{n^r m}m(m-1)\cdots(m-\alpha)n(n-1)\cdots(n-r+\alpha+1)$$
$$= \sum_{\alpha=0}^{r-1}\frac{1}{1+\alpha}\binom{r}{\alpha}\binom{r-1}{\alpha}\prod_{i=1}^{\alpha}\left(\frac{m}{n}-\frac{i}{n}\right)\prod_{i=1}^{r-\alpha}\left(1-\frac{i-1}{n}\right).$$

Therefore, denoting $\rho_n = m/n$, we have

$$\mathbb{E}\int x^r\,d\mu_n(x) = \sum_{\alpha=0}^{r-1}\frac{\rho_n^{\alpha}}{\alpha+1}\binom{r}{\alpha}\binom{r-1}{\alpha} + O(n^{-1}).$$

This achieves the proof of (4.16), and thus of the Marchenko–Pastur Theorem 4.6.2.

Concentration for empirical spectral distributions. — This section is devoted to the proof of Lemma 4.7.1 below. This lemma provides a concentration inequality which complements the results of the first chapter. The variation of $f:\mathbb{R}\to\mathbb{R}$ is

$$V(f) = \sup_{(x_k)_{k\in\mathbb{Z}}}\sum_{k\in\mathbb{Z}}|f(x_{k+1})-f(x_k)| \in [0,+\infty],$$

where the supremum runs over all non decreasing sequences $(x_k)_{k\in\mathbb{Z}}$. If f is differentiable with $f' \in \mathrm{L}^1(\mathbb{R})$ then $V(f) = \|f'\|_1$. If $f = \mathbf{1}_{(-\infty,s]}$ for $s \in \mathbb{R}$ then $V(f) = 1$.

***Lemma 4.7.1* (Concentration).** — *Let M be a $m\times n$ complex random matrix with independent rows and $\mu_M = \frac{1}{m}\sum_{k=1}^m \delta_{\lambda_k(MM^*)}$. Then for every bounded measurable function $f:\mathbb{R}\to\mathbb{R}$ and every $r \geqslant 0$,*

$$\mathbb{P}\left(\left|\int f\,d\mu_M - \mathbb{E}\int f\,d\mu_M\right| \geqslant r\right) \leqslant 2\exp\left(-\frac{mr^2}{2V(f)^2}\right).$$

Proof. — Let A and B be two $m \times n$ complex matrices and let $G_A : \mathbb{R} \to [0,1]$ and $G_B : \mathbb{R} \to [0,1]$ be the cumulative distributions functions of the probability measures

$$\mu_A = \frac{1}{m}\sum_{k=1}^m \delta_{s_k^2(A)} \quad \text{and} \quad \mu_B = \frac{1}{m}\sum_{k=1}^m \delta_{s_k^2(B)},$$

defined for every $t \in \mathbb{R}$ by

$$G_A(t) = \frac{\left|\{1 \leqslant k \leqslant m : s_k(A) \leqslant \sqrt{t}\}\right|}{m} \quad \text{and} \quad G_B(t) = \frac{\left|\{1 \leqslant k \leqslant m : s_k(B) \leqslant \sqrt{t}\}\right|}{m}.$$

By Theorem 4.2.3 we get

$$\sup_{t\in\mathbb{R}} |G_A(t) - G_B(t)| \leqslant \frac{\mathrm{rank}(A-B)}{m}.$$

Now if $f : \mathbb{R} \to \mathbb{R}$ is differentiable with $f' \in \mathrm{L}^1(\mathbb{R})$ then by integration by parts,

$$\left|\int f\,d\mu_A - \int f\,d\mu_B\right| = \left|\int_{\mathbb{R}} f'(t)(G_A(t) - G_B(t))\,dt\right| \leqslant \frac{\mathrm{rank}(A-B)}{m}\int_{\mathbb{R}} |f'(t)|\,dt.$$

Since the left hand side depends on at most $2m$ points, we get, by approximation, for every measurable function $f : \mathbb{R} \to \mathbb{R}$,

$$\left|\int f\,d\mu_A - \int f\,d\mu_B\right| \leqslant \frac{\mathrm{rank}(A-B)}{m} V(f).$$

From now on, $f : \mathbb{R} \to \mathbb{R}$ is a fixed measurable function with $V(f) \leqslant 1$. For every row vectors $x_1, \ldots, x_m$ in $\mathbb{C}^n$, we denote by $A(x_1, \ldots, x_m)$ the $m \times n$ matrix with row vectors $x_1, \ldots, x_m$ and we define $F : (\mathbb{C}^n)^m \to \mathbb{R}$ by

$$F(x_1, \ldots, x_m) = \int f\,d\mu_{A(x_1,\ldots,x_m)}.$$

For any $i \in \{1, \ldots, m\}$ and any row vectors $x_1, \ldots, x_m, x_i'$ of $\mathbb{C}^n$, we have

$$\mathrm{rank}(A(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_m) - A(x_1, \ldots, x_{i-1}, x_i', x_{i+1}, \ldots, x_m)) \leqslant 1$$

and thus

$$|F(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_m) - F(x_1, \ldots, x_{i-1}, x_i', x_{i+1}, \ldots, x_m)| \leqslant \frac{V(f)}{m}.$$

Let us define $X = F(R_1, \ldots, R_m)$ where $R_1, \ldots, R_m$ are the rows of M. Let $(R_1', \ldots, R_n')$ be an independent copy of $(R_1, \ldots, R_n)$. If $\mathcal{F}_k$ is the σ-field generated by $R_1, \ldots, R_k$ then for every $1 \leqslant k \leqslant n$ we have, with $\mathcal{F}_0 = \{\varnothing, \Omega\}$,

$$\mathbb{E}(X \,|\, \mathcal{F}_{k-1}) = \mathbb{E}(F(R_1, \ldots, R_k, \ldots, R_n) \,|\, \mathcal{F}_{k-1}) = \mathbb{E}(F(R_1, \ldots, R_k', \ldots, R_n) \,|\, \mathcal{F}_k).$$

Now the desired result follows from the Azuma–Hoeffding Lemma 4.7.2 since

$$\begin{aligned} d_k &= \mathbb{E}(X \mid \mathcal{F}_k) - \mathbb{E}(X \mid \mathcal{F}_{k-1}) \\ &= \mathbb{E}(F(R_1,\dots,R_k,\dots,R_n) - F(R_1,\dots,R'_k,\dots,R_n) \mid \mathcal{F}_k) \end{aligned}$$

gives $\mathrm{osc}(d_k) \leqslant 2\|d_k\|_\infty \leqslant 2V(f)/m$ for every $1 \leqslant k \leqslant n$. □

The following lemma on concentration of measure is close in spirit to Theorem 1.2.1. The condition on the oscillation (support diameter) rather than on the variance (second moment) is typical of Hoeffding type statements.

***Lemma 4.7.2* (Azuma–Hoeffding).** — *If* $X \in \mathrm{L}^1(\Omega, \mathcal{F}, \mathbb{P})$ *then for every* $r \geqslant 0$

$$\mathbb{P}(|X - \mathbb{E}(X)| \geqslant r) \leqslant 2\exp\left(-\frac{2r^2}{\mathrm{osc}(d_1)^2 + \cdots + \mathrm{osc}(d_n)^2}\right)$$

where $\mathrm{osc}(d_k) = \sup(d_k) - \inf(d_k)$ *and where* $d_k = \mathbb{E}(X \mid \mathcal{F}_k) - \mathbb{E}(X \mid \mathcal{F}_{k-1})$ *for an arbitrary filtration* $\{\varnothing, \Omega\} = \mathcal{F}_0 \subset \mathcal{F}_1 \subset \cdots \subset \mathcal{F}_n = \mathcal{F}$.

Proof. — By convexity, for all $t \geqslant 0$ and $a \leqslant x \leqslant b$,

$$e^{tx} \leqslant \frac{x-a}{b-a}e^{tb} + \frac{b-x}{b-a}e^{ta}.$$

Let U be a random variable with $\mathbb{E}(U) = 0$ and $a \leqslant U \leqslant b$. Denoting $p = -a/(b-a)$ and $\varphi(s) = -ps + \log(1 - p + pe^s)$ for any $s \geqslant 0$, we get

$$\mathbb{E}(e^{tU}) \leqslant \frac{b}{b-a}e^{ta} - \frac{a}{b-a}e^{tb} = e^{\varphi(t(b-a))}.$$

Now $\varphi(0) = \varphi'(0) = 0$ and $\varphi'' \leqslant 1/4$, so $\varphi(s) \leqslant s^2/8$, and therefore

$$\mathbb{E}(e^{tU}) \leqslant e^{\frac{t^2}{8}(b-a)^2}.$$

Used with $U = d_k = \mathbb{E}(X \mid \mathcal{F}_k) - \mathbb{E}(X \mid \mathcal{F}_{k-1})$ conditional on $\mathcal{F}_{k-1}$, this gives

$$\mathbb{E}(e^{td_k} \mid \mathcal{F}_{k-1}) \leqslant e^{\frac{t^2}{8}\mathrm{osc}(d_k)^2}.$$

By writing the Doob martingale telescopic sum $X - \mathbb{E}(X) = d_n + \cdots + d_1$, we get

$$\mathbb{E}(e^{t(X-\mathbb{E}(X))}) = \mathbb{E}(e^{t(d_{n-1}+\cdots+d_1)}\mathbb{E}(e^{td_n} \mid \mathcal{F}_{n-1})) \leqslant \cdots \leqslant e^{\frac{t^2}{8}(\mathrm{osc}(d_1)^2+\cdots+\mathrm{osc}(d_n)^2)}.$$

Now the desired result follows from Markov's inequality and an optimization of t. □

Moments and weak convergence. — This section is devoted to the proof of Lemmas 4.7.4 and 4.7.5 below. Let $\mathcal{P}$ be the set of probability measures μ on $\mathbb{R}$ such that $\mathbb{R}[X] \subset \mathrm{L}^1(\mu)$. For every $\mu \in \mathcal{P}$ and $n \geqslant 0$, the n-th moment of μ is defined by $\int x^n\,d\mu(x)$. The knowledge of the sequence of moments of μ is equivalent to the knowledge of $\int P\,d\mu$ for every $P \in \mathbb{R}[X]$. We say that $\mu_1, \mu_2 \in \mathcal{P}$ are equivalent when

$$\int P\,d\mu_1 = \int P\,d\mu_2$$

for all $P \in \mathbb{R}[X]$, in other words μ_1 and μ_2 have the same moments. We say that $\mu \in \mathcal{P}$ is *characterized by its moments* when its equivalent class is a singleton. Lemma 4.7.3 below provides a simpler sufficient condition, which is strong enough to imply that every compactly supported probability measure, such as the Marchenko–Pastur law μ_ρ, is characterized by its moments. Note that by the Weierstrass theorem on the density of polynomials, we already know that every compactly supported probability measure is characterized by its moments among the class of compactly supported probability measures.

***Lemma 4.7.3* (Moments and analyticity).** — *Let $\mu \in \mathcal{P}$, $\varphi(t) = \int e^{itx}\,d\mu(x)$ and $\kappa_n = \int x^n\,d\mu(x)$. The following three statements are equivalent :*

(i) *φ is analytic in a neighborhood of the origin*
(ii) *φ is analytic on $\mathbb{R}$*
(iii) $\overline{\lim}_n \left(\frac{1}{(2n)!}\kappa_{2n}\right)^{\frac{1}{2n}} < \infty$.

If these statement hold true then μ is characterized by its moments. This is the case for instance if μ is compactly supported.

Proof. — For all n we have $\int |x|^n\,d\mu < \infty$ and thus φ is n times differentiable on $\mathbb{R}$. Moreover, $\varphi^{(n)}$ is continuous on $\mathbb{R}$ and for all $t \in \mathbb{R}$,

$$\varphi^{(n)}(t) = \int_{\mathbb{R}} (ix)^n e^{itx}\,d\mu(x).$$

In particular, $\varphi^{(n)}(0) = i^n\kappa_n$, and the Taylor series of φ at the origin is determined by $(\kappa_n)_{n\geqslant 1}$. The convergence radius r of the power series $\sum_n a_n z^n$ associated to a sequence of complex numbers $(a_n)_{n\geqslant 0}$ is given by Hadamard's formula $r^{-1} = \overline{\lim}_n |a_n|^{\frac{1}{n}}$. Taking $a_n = i^n\kappa_n/n!$ gives that (i) and (iii) are equivalent. Next, we have

$$\left| e^{isx}\left(e^{itx} - 1 - \frac{itx}{1!} - \cdots - \frac{(itx)^{n-1}}{(n-1)!}\right)\right| \leqslant \frac{|tx|^n}{n!}$$

for all $n \in \mathbb{N}$, $s, t \in \mathbb{R}$. In particular, it follows that for all $n \in \mathbb{N}$ and all $s, t \in \mathbb{R}$,

$$\left|\varphi(s+t) - \varphi(s) - \frac{t}{1!}\varphi'(s) - \cdots - \frac{t^{2n-1}}{(2n-1)!}\varphi^{(2n-1)}(s)\right| \leqslant \kappa_{2n}\frac{t^{2n}}{(2n)!},$$

and thus (iii) implies (ii). Since (ii) implies property (i) we get that (i)-(ii)-(iii) are equivalent. If these properties hold then by the preceding arguments, there exists $r > 0$ such that the series expansion of φ at any $x \in \mathbb{R}$ has radius $> r$, and thus, φ is characterized by its sequence of derivatives at point 0. If μ is compactly supported then $\sup_n |\kappa_n|^{\frac{1}{n}} < \infty$ and thus (iii) holds. □

***Lemma 4.7.4* (Moments convergence).** — *Let $\mu \in \mathcal{P}$ be characterized by its moments. If $(\mu_n)_{n\geqslant 1}$ is a sequence in $\mathcal{P}$ such that for every polynomial $P \in \mathbb{R}[X]$,*

$$\lim_{n\to\infty} \int P\,d\mu_n = \int P\,d\mu$$

then for every bounded continuous function $f : \mathbb{R} \to \mathbb{R}$,

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

Proof. — By assumption, for any $P \in \mathbb{R}[X]$, we have $C_P = \sup_{n\geqslant 1}\int P\,d\mu_n < \infty$, and therefore, by Markov's inequality, for any real $R > 0$,

$$\mu_n([-R,R]^c) \leqslant \frac{C_{X^2}}{R^2}.$$

This shows that $(\mu_n)_{n\geqslant 1}$ is tight. Thanks to Prohorov's theorem, it suffices then to show that if a subsequence $(\mu_{n_k})_{k\geqslant 1}$ converges with respect to bounded continuous functions toward a probability measure ν as $k\to\infty$ then $\nu = \mu$. Let us fix $P \in \mathbb{R}[X]$ and a real number $R > 0$. Let $\varphi_R : \mathbb{R} \to [0,1]$ be continuous and such that

$$\mathbf{1}_{[-R,R]} \leqslant \varphi_R \leqslant \mathbf{1}_{[-R-1,R+1]}.$$

We have the decomposition

$$\int P\,d\mu_{n_k} = \int \varphi_R P\,d\mu_{n_k} + \int (1-\varphi_R)P\,d\mu_{n_k}.$$

Since $(\mu_{n_k})_{k\geqslant 1}$ converges weakly to ν we have

$$\lim_{k\to\infty}\int \varphi_R P\,d\mu_{n_k} = \int \varphi_R P\,d\nu.$$

Moreover, by the Cauchy-Schwarz and Markov inequalities we have

$$\left|\int (1-\varphi_R)P\,d\mu_{n_k}\right|^2 \leqslant \mu_{n_k}([-R,R]^c)\int P^2\,d\mu_{n_k} \leqslant \frac{C_{X^2}C_{P^2}}{R^2}.$$

On the other hand, we know that $\lim_{k\to\infty}\int P\,d\mu_{n_k} = \int P\,d\mu$ and thus

$$\lim_{R\to\infty}\int \varphi_R P\,d\nu = \int P\,d\mu.$$

Using this for P^2 provides via monotone convergence that $P \in \mathrm{L}^2(\nu) \subset \mathrm{L}^1(\nu)$ and by dominated convergence that $\int P\,d\nu = \int P\,d\mu$. Since P is arbitrary and μ is characterized by its moments, we obtain $\mu = \nu$. ☐

***Lemma 4.7.5* (Moments of the M.–P. law μ_ρ).** — *The sequence of moments of the Marchenko–Pastur distribution μ_ρ defined by* (4.15) *is given for all $r \geqslant 1$ by*

$$\int x^r\,d\mu_\rho(x) = \sum_{k=0}^{r-1}\frac{\rho^k}{k+1}\binom{r}{k}\binom{r-1}{k}.$$

In particular, μ_ρ has mean 1 *and variance ρ.*

Proof. — Since $a+b = 2(1+\rho)$ and $ab = (1-\rho)^2$ we have

$$\sqrt{(b-x)(x-a)} = \sqrt{\frac{(a+b)^2}{4} - ab - \left(x - \frac{a+b}{2}\right)^2} = \sqrt{4\rho - (x-(1+\rho))^2}$$

The change of variable $y = (x-(1+\rho))/\sqrt{\rho}$ gives

$$\int x^r\,d\mu_\rho(x) = \frac{1}{2\pi}\int_{-2}^{2}(\sqrt{\rho}y + 1 + \rho)^{r-1}\sqrt{4-y^2}\,dy.$$

The even moments of the semicircle law are the Catalan numbers :

$$\frac{1}{2\pi}\int_{-2}^{2} y^{2k+1}\sqrt{4-y^2}\,dy = 0 \quad\text{and}\quad \frac{1}{2\pi}\int_{-2}^{2} y^{2k}\sqrt{4-y^2}\,dy = \frac{1}{1+k}\binom{2k}{k}.$$

By using binomial expansions and the Vandermonde convolution identity,

$$\begin{aligned}
\int x^r\,d\mu_\rho(x) &= \sum_{k=0}^{\lfloor (r-1)/2\rfloor} \rho^k(1+\rho)^{r-1-2k}\binom{r-1}{2k}\binom{2k}{k}\frac{1}{1+k}\\
&= \sum_{k=0}^{\lfloor (r-1)/2\rfloor} \rho^k(1+\rho)^{r-1-2k}\frac{(r-1)!}{(r-1-2k)!k!(k+1)!}\\
&= \sum_{k=0}^{\lfloor (r-1)/2\rfloor}\sum_{s=0}^{r-1-2k} \rho^{k+s}\frac{(r-1)!}{k!(k+1)!(r-1-2k-s)!s!}\\
&= \sum_{t=0}^{r-1}\rho^t \sum_{k=0}^{\min(t,r-1-t)} \frac{(r-1)!}{k!(k+1)!(r-1-t-k)!(t-k)!}\\
&= \frac{1}{r}\sum_{t=0}^{r-1}\rho^t\binom{r}{t}\sum_{k=0}^{\min(t,r-1-t)}\binom{t}{k}\binom{r-t}{k+1}\\
&= \frac{1}{r}\sum_{t=0}^{r-1}\rho^t\binom{r}{t}\binom{r}{t+1}\\
&= \sum_{t=0}^{r-1}\frac{\rho^t}{t+1}\binom{r}{t}\binom{r-1}{t}.
\end{aligned}$$

□

Other proof of the Marchenko–Pastur theorem. — An alternate proof of the Marchenko–Pastur theorem 4.6.1 is based on the Cauchy–Stieltjes transform. Recall that the Cauchy–Stieltjes transform of a probability measure μ on $\mathbb{R}$ is

$$z \in \mathbb{C}_+ = \{z\in\mathbb{C} : \mathrm{Im}(z) > 0\} \mapsto S_\mu(z) = \int \frac{1}{x-z}\,d\mu(x).$$

For instance, the Cauchy–Stieltjes transform of the Marchenko–Pastur law μ_ρ is

$$S_{\mu_\rho}(z) = \frac{1-\rho-z+\sqrt{(z-1-\rho)^2-4\rho}}{2\rho z}.$$

The knowledge of S_μ fully characterizes μ, and the pointwise convergence along a sequence of probability measures implies the weak convergence of the sequence. For any $m\times m$ Hermitian matrix H with spectral distribution $\mu_H = \frac{1}{m}\sum_{k=1}^m \delta_{\lambda_k(H)}$, the Cauchy–Stieltjes transform S_{μ_H} is the normalized trace of the resolvent of H since

$$S_{\mu_H}(z) = \frac{1}{m}\mathrm{Tr}((H-zI)^{-1}).$$

This makes the Cauchy–Stieltjes transform an analogue of the Fourier transform, well suited for spectral distributions of matrices. Note that $|S_\mu(z)| \leqslant 1/\mathfrak{Im}(z)$. To prove the Marchenko–Pastur theorem one takes $H = \frac{1}{n}MM^*$ and one first shows that $S_{\mu_H}(z) - \mathbb{E}S_{\mu_H}(z)$ tends to 0 with probability one as $m, n \to \infty$. This can be done in the upper half plane using the concentration Lemma 4.7.1 with $f(t) = 1/(t-z)$. Beware that $\mathbb{E}S_{\mu_A} \neq S_{\mathbb{E}\mu_A}$. Next the Schur bloc inversion allows to deduce a recursive equation for $\mathbb{E}S_{\mu_H}$ leading to the fixed point equation $S = 1/(1 - z - \rho - \rho z S)$ at the limit $m, n \to \infty$. This quadratic equation in S admits two solutions including the Cauchy–Stieltjes transform S_{μ_ρ} of the Marchenko–Pastur law μ_ρ.

The behavior of μ_H when H is random can be captured by looking at $\mathbb{E}\int f\,d\mu_H$ with a test function f running over a sufficiently large family $\mathcal{F}$. The method of moments corresponds to the family $\mathcal{F} = \{x \mapsto x^r : r \in \mathbb{N}\}$ whereas the Cauchy–Stieltjes transform method corresponds to the family $\mathcal{F} = \{z \mapsto 1/(x-z) : z \in \mathbb{C}_+\}$. Each of these allows to prove Theorem 4.6.2, with advantages and drawbacks.

4.8. The Bai–Yin theorem

The convergence stated by the Marchenko–Pastur theorem 4.6.1 is too weak to provide the convergence of the smallest and largest singular values. More precisely, one can only deduce from Theorem 4.6.1 that with probability one,

$$\varlimsup_{n\to\infty} s_{n\wedge m}\left(\frac{1}{\sqrt{n}}M\right) \leqslant \sqrt{a} = 1 - \sqrt{\rho} \quad \text{and} \quad \varliminf_{n\to\infty} s_1\left(\frac{1}{\sqrt{n}}M\right) \geqslant \sqrt{b} = 1 + \sqrt{\rho}.$$

Of course if $\rho = 1$ then $a = 0$ and we obtain $\lim_{n\to\infty} s_{n\wedge m}\left(\frac{1}{\sqrt{n}}M\right) = 0$. The Bai and Yin theorem below provides a complete answer for any value of ρ when the entries have mean zero and finite fourth moment.

***Theorem 4.8.1* (Bai–Yin).** — *Let $(M_{i,j})_{i,j\geqslant 1}$ be an infinite table of i.i.d. random variables on $\mathbb{K}$ with mean 0, variance 1 and finite fourth moment : $\mathbb{E}(|M_{1,1}|^4) < \infty$. As in the Marchenko–Pastur theorem 4.6.1, let M be the $m \times n$ random matrix*

$$M = (M_{i,j})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}.$$

Suppose that $m = m_n$ depends on n in such a way that

$$\lim_{n\to\infty} \frac{m_n}{n} = \rho \in (0, \infty).$$

Then with probability one

$$\lim_{n\to\infty} s_{m\wedge n}\left(\frac{1}{\sqrt{n}}M\right) = \sqrt{a} \quad \textit{and} \quad \lim_{n\to\infty} s_1\left(\frac{1}{\sqrt{n}}M\right) = \sqrt{b}.$$

Regarding the assumptions, it can be shown that if M is not centered or does not have finite fourth moment then $\varlimsup_{n\to\infty} s_1(M/\sqrt{n})$ is infinite.

When $m < n$ the Bai–Yin theorem can be roughly rephrased as follows

$$\sqrt{n} - \sqrt{m} + \sqrt{n}o_{n\to\infty}(1) \leqslant s_{m\wedge n}(M) \leqslant s_1(M) \leqslant \sqrt{n} + \sqrt{m} + \sqrt{n}o_{n\to\infty}(1).$$

The proof of the Bai–Yin theorem is tedious and is outside the scope of this book. In the Gaussian case, the result may be deduced from Theorem 4.5.3. It is worthwhile to mention that in the Gaussian case, we have the following result due to Gordon:

$$\sqrt{n}-\sqrt{m} \leqslant \mathbb{E}(s_{m\wedge n}(M)) \leqslant \mathbb{E}(s_1(M)) \leqslant \sqrt{n}+\sqrt{m}.$$

***Remark 4.8.2* (Jargon).** — *The Marchenko–Pastur theorem 4.6.1 concerns the global behavior of the spectrum using the counting probability measure: we say* bulk of the spectrum*. The Bai–Yin Theorem 4.8.1 concerns the boundary of the spectrum: we say* edge of the spectrum*. When $\rho = 1$ then the left limit $\sqrt{a} = 0$ acts like a hard wall forcing single sided fluctuations, and we speak about a* hard edge*. In contrast, we have a* soft edge *at $\sqrt{b}$ for any ρ and at $\sqrt{a}$ for $\rho \neq 1$ in the sense that the spectrum can fluctuate around the limit at both sides. The asymptotic fluctuation at the edge depends on the nature of the edge: soft edges give rise to Tracy–Widom laws, while hard edges give rise to (deformed) exponential laws (depending on $\mathbb{K}$).*

4.9. Notes and comments

A proof of the Courant–Fischer variational formulas for the singular values (Theorem 4.2.1) can be found for instance in [**HJ94**, theorem 3.1.2] and in [**GVL96**, theorem 8.6.1]. A proof of the interlacing inequalities (Theorem 4.2.3) can be found in [**HJ94**, theorem 3.3.16] which also provides the multiplicative analogue statement. A proof of the interlacing inequalities (Theorem 4.2.4) can be found in [**GVL96**, theorem 8.6.3] or in [**HJ94**, theorem 3.1.4]. The formula (4.4) is due to Eckart and Young [**EY39**]. Theorem 4.3.1 is due to Weyl [**Wey49**]. The derivation of (4.8) using majorization techniques is also due to Weyl, see for instance [**HJ94**, theorem 3.3.13]. The proof of the Horn inverse theorem (Theorem 4.3.2) can be found in the short paper [**Hor54**]. It is worthwhile to mention the book [**CG05**] on inverse eigenvalue problems. Theorem 4.2.5 is due to Hoffman and Wielandt [**HW53**]. Theorem 4.3.3 is due to Gelfand [**Gel41**]. Beyond Gelfand's result, it was shown by Yamamoto that $\lim_{k\to\infty} s_i(A^k)^{1/k} = |\lambda_k(A)|$ for every $A \in \mathcal{M}_{n,n}(\mathbb{K})$ and every $i \in \{1,\ldots,n\}$, see [**HJ94**, theorem 3.3.1] for a proof. There are plenty of nice theorems on the singular values and on the eigenvalues of deterministic matrices. We refer to [**HJ90, HJ94, Bha97, Zha02, BS10**]. For the numerical aspects such as the algorithms for the computation of the SVD, we refer to [**GVL96**]. Theorems 4.4.1 and 4.4.2 connecting the rows distances of a matrix with the norm of its inverse are due to Rudelson and Vershynin [**RV08a**] (operator norm) and Tao and Vu [**TV10**] (trace norm). The pseudo-spectra are studied by Trefethen and Embree in [**TE05**].

The SVD is typically used for dimension reduction and for regularization. For instance, the SVD allows to construct the so-called Moore–Penrose pseudoinverse [**Moo20, Pen56**] of a matrix by replacing the non null singular values by their inverse while leaving in place the null singular values. Generalized inverses of integral operators were introduced earlier by Fredholm in [**Fre03**]. Such generalized inverse of matrices provide for instance least squares solutions to degenerate systems of linear equations. A diagonal shift in the SVD is used in the so-called Tikhonov regularization [**Tik43, Tar05**] or ridge regression for solving over determined systems of linear equations. The SVD is at the heart of the so-called principal component analysis (PCA) technique in applied statistics for multivariate data analysis [**Jol02**]. The partial least squares (PLS) regression technique is also connected to PCA/SVD. In the last decade, the PCA was used together with the so-called kernel methods in learning theory. Generalizations of the SVD are used for the regularization of ill posed inverse problems [**BB98**].

The study of the singular values of random matrices takes its roots in the works of Wishart [**Wis28**] on the empirical covariance matrices of Gaussian samples, and in the works of von Neumann and Goldstine in numerical analysis [**vNG47**]. The singular values of Gaussian random matrices were extensively studied and we refer to [**Jam60, Mui82, Ede89, DS01, ER05, HT03, For10**]. A proof of Theorems 4.5.2 and 4.5.3 can be found in [**For10**, propositions 3.2.7 and introduction of section 3.10]. Theorem 4.5.3 is due to Silverstein [**Sil85**], see also the more recent and general work of Dumitriu and Edelman [**DE02**]. The analogous result for Gaussian Hermitian matrices (GUE) consists in a unitary tridiagonalization and goes back to Trotter [**Tro84**]. The proof of Theorem 4.5.4 is taken from Forrester [**For10**, proposition 3.10.1]. For simplicity, we have skipped the link with Laguerre orthogonal polynomials, which may be used to represent the determinant in the singular values distribution, and which play a key role in the asymptotic analysis of the spectral edge.

The Marchenko–Pastur theorem (Theorem 4.6.1 or Theorem 4.6.2) goes back to Marchenko and Pastur [**MP67**]. The modern universal version with minimal moments assumptions was obtained after a sequence of works including [**Gir75**] and can be found in [**PS11, BS10**]. Most of the proof given in this chapter is taken from [**BS10**, Chapter 3]. The argument using the Fréchet–Wasserstein distance is taken from [**BC12**]. We have learned Lemma 4.7.1 from Bordenave in 2009, who discovered later that it can also be found in [**GL09**]. The Azuma–Hoeffding inequality of lemma 4.7.2 is taken from McDiarmid [**McD89**]. Beyond lemma 4.7.3, it is well known that $\mu \in \mathcal{P}$ is characterized by its moments $(\kappa_n)_{n\geqslant 1}$ if and only if the characteristic function of μ is quasi-analytic i.e. characterized by its sequence of derivatives at the origin, and the celebrated Carleman criterion states that this is the case if $\sum_n \kappa_{2n}^{-1/(2n)} = \infty$, see [**Fel71**] (the odd moments do not appear here: they are controlled by the even moments for instance via Hölder's inequality). An extension of the Marchenko–Pastur theorem to random matrices with independent row vectors or column vectors is given in [**MP06**] and [**PP09**]. In the Gaussian case, and following Pastur [**Pas99**], the Marchenko–Pastur theorem can be proved using Gaussian integration by parts together with the method of moments or the Cauchy–Stieltjes transform. Still in the Gaussian case, there exists additionally an approach due to Haagerup and Thorbjørnsen [**HT03**], based on Laguerre orthogonal polynomials, and further developed in [**Led04**] from a Markovian viewpoint.

The Bai–Yin theorem (Theorem 4.8.1) was obtained after a series of works by Bai and Yin [**BY93**], see also [**BS10**]. The non-asymptotic analysis of the singular values of random matrices is the subject of a recent survey by Vershynin [**Ver12**].

CHAPTER 5

EMPIRICAL METHODS AND SELECTION OF CHARACTERS

The purpose of this chapter is to present the connections between two different topics. The first one concerns the recent subject about reconstruction of signals with small supports from a small amount of linear measurements, called also compressed sensing and was presented in Chapter 2. A big amount of work was recently made to develop some strategy to construct an encoder (to compress a signal) and an associate decoder (to reconstruct exactly or approximately the original signal). Several deterministic methods are known but recently, some random methods allowed the reconstruction of signal with much larger size of support. A lot of ideas are common with a subject of harmonic analysis, going back to the construction of $\Lambda(p)$ sets which are not $\Lambda(q)$ for $q > p$. This is the second topic that we would like to address, the problem of selection of characters. The most powerful method was to use a random selection via the method of selectors. We will discuss about the problem of selecting a large part of a bounded orthonormal system such that on the vector span of this family, the L_2 and the L_1 norms are as close as possible. Solving this type of problems leads to questions about the Euclidean radius of the intersection of the kernel of a matrix with the unit ball of a normed space. That is exactly the subject of study of Gelfand width and Kashin splitting theorem. In all this theory, empirical processes are essential tools. Numerous results of this theory are at the heart of the proofs and we will present some of them.

Notations. — We briefly indicate some notations that will be used in this section. For any $p \geq 1$ and $t = (t_1, \dots, t_N) \in \mathbb{R}^N$, we define its ℓ_p-norm by

$$|t|_p = \left(\sum_{i=1}^{N} |t_i|^p \right)^{1/p}$$

and its L_p-norm by

$$\|t\|_p = \left(\frac{1}{N} \sum_{i=1}^{N} |t_i|^p \right)^{1/p}.$$

For $p \in (0,1)$, the definition is still valid but it is not a norm. For $p = \infty$, $|t|_\infty = \|t\|_\infty = \max\{|t_i| : i = 1, \ldots, N\}$. We denote by B_p^N the unit ball of the ℓ_p-norm in $\mathbb{R}^N$. The radius of a set $T \subset \mathbb{R}^N$ is

$$\operatorname{rad} T = \sup_{t \in T} |t|_2.$$

More generally, if μ is a probability measure on a measurable space Ω, for any $p > 0$ and any measurable function f, we denote its L_p-norm and its L_∞-norm by

$$\|f\|_p = \left(\int |f|^p d\mu \right)^{1/p} \quad \text{and} \quad \|f\|_\infty = \sup |f|.$$

The $\sup |f|$ should be everywhere understand as the essential supremum of the function $|f|$. The unit ball of $L_p(\mu)$ is denoted by B_p and the unit sphere by S_p. If $T \subset L_2(\mu)$ then its radius with respect to $L_2(\mu)$ is defined by

$$\operatorname{Rad} T = \sup_{t \in T} \|t\|_2.$$

Observe that if μ is the counting probability measure on $\mathbb{R}^N$, $B_p = N^{1/p} B_p^N$ and for a subset $T \subset L_2(\mu)$, $\sqrt{N} \operatorname{Rad} T = \operatorname{rad} T$.

The letters c, C are used for numerical constants which do not depend on any parameter (dimension, size of sparsity, ...). Since the dependence on these parameters is important in this study, we will always indicate it as precisely as we can. Sometimes, the value of these numerical constants can change from line to line.

5.1. Selection of characters and the reconstruction property.

Exact and approximate reconstruction.— We start by recalling briefly from Chapter 2 the ℓ_1-minimization method to reconstruct any unknown sparse signal from a small number of linear measurements. Let $u \in \mathbb{R}^N$ (or $\mathbb{C}^N$) be an unknown signal. We receive Φu where Φ is an $n \times N$ matrix with row vectors $Y_1, \ldots, Y_n \in \mathbb{R}^N$ (or $\mathbb{C}^N$) which means that

$$\Phi = \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} \qquad \text{and} \qquad \Phi u = (\langle Y_i, u \rangle)_{1 \le i \le n}$$

and we assume that $n \le N - 1$. This linear system to reconstruct u is ill-posed. However, the main information is that u has a small support in the canonical basis chosen at the beginning, that is $|\operatorname{supp} u| \le m$. We also say that u is m-sparse and we denote by Σ_m the set of m-sparse vectors. Our aim is to find conditions on Φ, m, n and N such that the following property is satisfied: for every $u \in \Sigma_m$, the solution of the problem

$$\min_{t \in \mathbb{R}^N} \{|t|_1 : \Phi u = \Phi t\} \tag{5.1}$$

is unique and equal to u. From Proposition 2.2.11, we know that this property is equivalent to

$$\forall h \in \ker \Phi, h \neq 0, \forall I \subset [N], |I| \leq m, \sum_{i \in I} |h_i| < \sum_{i \notin I} |h_i|.$$

It is also called the null space property. Let $\mathcal{C}_m$ be the cone

$$\mathcal{C}_m = \{h \in \mathbb{R}^N, \exists I \subset [N] \text{ with } |I| \leq m, |h_{I^c}|_1 \leq |h_I|_1\}.$$

The null space property is equivalent to $\ker \Phi \cap \mathcal{C}_m = \{0\}$. Taking the intersection with the Euclidean sphere S^{N-1}, we can say that

"for every signal $u \in \Sigma_m$, the solution of (5.1) is unique and equal to u"
if and only if
$$\ker \Phi \cap \mathcal{C}_m \cap S^{N-1} = \emptyset.$$

Observe that if $t \in \mathcal{C}_m \cap S^{N-1}$ then

$$|t|_1 = \sum_{i=1}^{N} |t_i| = \sum_{i \in I} |t_i| + \sum_{i \notin I} |t_i| \leq 2 \sum_{i \in I} |t_i| \leq 2\sqrt{m}$$

since $|I| \leq m$ and $|t|_2 = 1$. This implies that

$$\mathcal{C}_m \cap S^{N-1} \subset 2\sqrt{m} B_1^N \cap S^{N-1}$$

from which we conclude that if

$$\ker \Phi \cap 2\sqrt{m} B_1^N \cap S^{N-1} = \emptyset$$

then "for every $u \in \Sigma_m$, the solution of (5.1) is unique and equal to u". We can now restate Proposition 2.4.4 as follows.

Proposition 5.1.1. — *Denote by* $\operatorname{rad} T$ *the radius of a set* T *with respect to the Euclidean distance:* $\operatorname{rad} T = \sup_{t \in T} |t|_2$. *If*

$$\operatorname{rad}(\ker \Phi \cap B_1^N) < \rho \text{ with } \rho \leq \frac{1}{2\sqrt{m}} \tag{5.2}$$

then "for every $u \in \Sigma_m$*, the solution of the basis pursuit algorithm* (5.1) *is unique and equal to* u*".*

It has also been noticed in Chapter 2 Proposition 2.7.3 that it is very stable and allows approximate reconstruction of vectors close to sparse signals. Indeed by Proposition 2.7.3, if $u^\sharp$ is a solution of the minimization problem (5.1)

$$\min_{t \in \mathbb{R}^N} \{|t|_1 : \Phi u = \Phi t\}$$

and if for some integer m such that $1 \leq m \leq N$, we have

$$\operatorname{rad}(\ker \Phi \cap B_1^N) \leq \rho < \frac{1}{2\sqrt{m}}$$

then for any set $I \subset \{1, \ldots, N\}$ of cardinality less than m

$$|u^\sharp - u|_2 \leq \rho\, |u^\sharp - u|_1 \leq \frac{2\rho}{1 - 2\rho\sqrt{m}}\, |u_{I^c}|_1.$$

In particular: if $\mathrm{rad}\,(\ker\Phi\cap B_1^N)\le 1/4\sqrt{m}$ then for any subset I of cardinality less than m,

$$|u^\sharp-u|_2\le\frac{|u^\sharp-u|_1}{4\sqrt{m}}\le\frac{|u_{I^c}|_1}{\sqrt{m}}.$$

Moreover if $u\in B_{p,\infty}^N$ i.e. if for all $s>0$, $|\{i,|u_i|\ge s\}|\le s^{-p}$ then

$$|u^\sharp-u|_2\le\frac{|u^\sharp-u|_1}{4\sqrt{m}}\le\frac{1}{(1-1/p)\,m^{\frac{1}{p}-\frac{1}{2}}}.$$

A problem coming from Harmonic Analysis. — Let μ be a probability measure and let $(\psi_1,\dots,\psi_N)$ be an orthonormal system of $L_2(\mu)$, bounded in $L_\infty(\mu)$ i.e. such that for every $i\le N$, $\|\psi_i\|_\infty\le 1$. Typically, we consider a system of characters in $L_2(\mu)$. It is clear that for any subset $I\subset[N]$

$$\forall\,(a_i)_{i\in I}\,,\ \left\|\sum_{i\in I}a_i\psi_i\right\|_1\le\left\|\sum_{i\in I}a_i\psi_i\right\|_2\le\sqrt{|I|}\left\|\sum_{i\in I}a_i\psi_i\right\|_1.$$

Dvoretzky theorem, as proved by Milman and improved by Gordon, asserts that for any $\varepsilon\in(0,1)$, there exists a subspace $E\subset\mathrm{span}\{\psi_1,\dots,\psi_N\}$ of dimension $\dim E=n=c\,\varepsilon^2N$ on which the L_1 and L_2 norms are comparable:

$$\forall\,(a_i)_{i=1}^N\,,\ \text{if } x=\sum_{i=1}^N a_i\psi_i\in E,\ \text{then}\,(1-\varepsilon)\,r\,\|x\|_1\le\|x\|_2\le(1+\varepsilon)\,r\,\|x\|_1$$

where r depends on the dimension N and can be bounded from above and below by some numerical constants (independent of the dimension N). Observe that E is a general subspace and the fact that $x\in E$ does not say anything about the number of non zero coordinates. Moreover the constant c which appears in the dependence of $\dim E$ is very small hence this formulation of Dvoretzy's theorem does not provide a subspace of say half dimension such that the L_1 norm and the L_2 norm are comparable up to constant factors. This question was solved by Kashin. He proved in fact a very strong result which is called now a *Kashin decomposition*: there exists a subspace E of dimension $[N/2]$ such that $\forall\,(a_i)_{i=1}^N$,

$$\text{if } x=\sum_{i=1}^N a_i\psi_i\in E \text{ then } \|x\|_1\le\|x\|_2\le C\,\|x\|_1\,,$$

$$\text{and if } y=\sum_{i=1}^N a_i\psi_i\in E^\perp \text{ then } \|y\|_1\le\|y\|_2\le C\,\|y\|_1$$

where C is a numerical constant. Again the subspaces E and $E^\perp$ have not any particular structure, like being coordinate subspaces.

In the setting of Harmonic Analysis, the questions are more related with coordinate subspaces because the requirement is to find a subset $I\subset\{1,\dots,N\}$ such that the L_1 and L_2 norms are well comparable on $\mathrm{span}\,\{\psi_i\}_{i\in I}$. Reproving a result of Bourgain, Talagrand showed that there exists a small constant δ_0 such that for any bounded orthonormal system $\{\psi_1, \dots, \psi_N\}$, there exists a subset I of cardinality greater than $\delta_0 N$ such that

$$\forall (a_i)_{i \in I}, \quad \left\| \sum_{i \in I} a_i \psi_i \right\|_2 \leq C \sqrt{\log N \, (\log \log N)} \left\| \sum_{i \in I} a_i \psi_i \right\|_1 . \tag{5.3}$$

This is a Dvoretzky type theorem. We will present in Section 5.5 an extension of this result to a Kashin type setting.

An important observation relates this study with Proposition 5.1.1. Let Ψ be the operator defined on $\operatorname{span}\{\psi_1, \dots, \psi_N\} \subset L_2(\mu)$ by $\Psi(f) = (\langle f, \psi_i \rangle)_{i \notin I}$. Because of the orthogonality condition between the ψ_i's, the linear span of $\{\psi_i, i \in I\}$ is nothing else than the kernel of Ψ and inequality (5.3) is equivalent to

$$\operatorname{Rad}(\ker \Psi \cap B_1) \leq C \sqrt{\log N \, (\log \log N)}$$

where Rad is the Euclidean radius with respect to the norm on $L_2(\mu)$ and B_1 is the unit ball of $L_1(\mu)$. The question is reduced to finding the relations among the size of I, the dimension N and ρ_1 such that $\operatorname{Rad}(\ker \Psi \cap B_1) \leq \rho_1$. This is analogous to condition (5.2) in Proposition 5.1.1. Just notice that in this situation, we have a change of normalization because we work in the probability space $L_2(\mu)$ instead of ℓ_2^N.

The strategy. — We will focus on the condition about the radius of the section of the unit ball of ℓ_1^N (or B_1) with the kernel of some matrices. As noticed in Chapter 2, the RIP condition implies a control of this radius. Moreover, condition (5.2) was deeply studied in the so called Local Theory of Banach Spaces during the seventies and the eighties and is connected with the study of Gelfand widths. These notions were presented in Chapter 2 and we recall that the strategy consists in studying the width of a truncated set $T_\rho = T \cap \rho S^{N-1}$. Indeed by Proposition 2.7.7, Φ satisfies condition (5.2) if ρ is such that $\ker \Phi \cap T_\rho = \emptyset$. This observation is summarized in the following proposition.

Proposition 5.1.2. — *Let T be a star body with respect to the origin (i.e. T is a compact subset T of $\mathbb{R}^N$ such that for any $x \in T$, the segment $[0, x]$ is contained in T). Let Φ be an $n \times N$ matrix with row vectors $Y_1, \dots, Y_n$. Then*

$$\textit{if} \quad \inf_{y \in T \cap \rho S^{N-1}} \sum_{i=1}^{n} \langle Y_i, y \rangle^2 > 0, \quad \textit{one has} \quad \operatorname{rad}(\ker \Phi \cap T) < \rho.$$

Proof. — If $z \in T \cap \rho S^{N-1}$ then $|\Phi z|_2^2 > 0$ so $z \notin \ker \Phi$. Since T is star shaped, if $y \in T$ and $|y|_2 \geq \rho$ then $z = \rho y / |y|_2 \in T \cap \rho S^{N-1}$ so z and y do not belong to $\ker \Phi$. □

Remark 5.1.3. — *By a simple compactness argument, the converse of this statement holds true. We can also replace the Euclidean norm $|\Phi z|_2$ by any other norm $\|\Phi z\|$ since the hypothesis is just made to ensure that $\ker \Phi \cap T \cap \rho S^{N-1} = \emptyset$.*

The vectors $Y_1, \ldots, Y_n$ will be chosen at random and we will find the good conditions such that, in average, the key inequality of Proposition 5.1.2 holds true. An important case is when the Y_i's are independent copies of a standard random Gaussian vector in $\mathbb{R}^N$. It is a way to prove Theorem 2.5.2 with Φ being this standard random Gaussian matrix. However, in the context of Compressed Sensing or Harmonic Analysis, we are looking for more structured matrices, like Fourier or Walsh matrices.

5.2. A way to construct a random data compression matrix

The setting is the following. We start with a square $N \times N$ orthogonal matrix and we would like to select n rows of this matrix such that the $n \times N$ matrix Φ that we obtain is a good encoder for every m-sparse vectors. In view of Proposition 5.1.1, we want to find conditions on n, N and m insuring that

$$\operatorname{rad}\left(\ker \Phi \cap B_1^N\right) < \frac{1}{2\sqrt{m}}.$$

The main examples are the discrete Fourier matrix with

$$\phi_{k\ell} = \frac{1}{\sqrt{N}}\,\omega^{k\ell} \quad 1 \le k, \ell \le N \quad \text{where } \omega = \exp\left(-2i\pi/N\right),$$

and the Walsh matrix defined by induction: $W_1 = 1$ and for any $p \ge 2$,

$$W_p = \frac{1}{\sqrt{2}} \begin{pmatrix} W_{p-1} & W_{p-1} \\ -W_{p-1} & W_{p-1} \end{pmatrix}.$$

The matrix W_p is an orthogonal matrix of size $N = 2^p$ with entries $\frac{\pm 1}{\sqrt{N}}$. In each case, the column vectors form an orthonormal basis of ℓ_2^N, with ℓ_∞^N-norm bounded by $1/\sqrt{N}$. We will consider more generally a system of vectors $\phi_1, \ldots, \phi_N$ such that

$$(H) \quad \begin{cases} (\phi_1, \ldots, \phi_N) \text{ is an orthogonal system of } \ell_2^N, \\ \forall i \le N, |\phi_i|_\infty \le 1/\sqrt{N} \text{ and } |\phi_i|_2 = K \text{ where } K \text{ is a fixed number.} \end{cases}$$

The empirical method. — The first definition of randomness is empirical. Let Y be the random vector defined by $Y = \phi_i$ with probability $1/N$, $1 \le i \le N$, and let $Y_1, \ldots, Y_n$ be independent copies of Y. We define the random matrix Φ by

$$\Phi = \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix}.$$

We have the following properties:

$$\mathbb{E}\langle Y, y\rangle^2 = \frac{1}{N}\sum_{i=1}^{N} \langle \phi_i, y\rangle^2 = \frac{K^2}{N}|y|_2^2 \quad \textit{and} \quad \mathbb{E}|\Phi y|_2^2 = \frac{K^2\, n}{N}|y|_2^2. \tag{5.4}$$

In view of Proposition 5.1.2, we would like to find ρ such that

$$\mathbb{E} \inf_{y \in T \cap \rho S^{N-1}} \sum_{i=1}^{n} \langle Y_i, y\rangle^2 > 0.$$

However it is difficult to study the infimum of an empirical process. We shall prefer to study

$$\mathbb{E} \sup_{y \in T \cap \rho S^{N-1}} \left| \sum_{i=1}^{n} \langle Y_i, y\rangle^2 - \frac{K^2\, n\rho^2}{N} \right|$$

that is the supremum of the deviation of the empirical process to its mean (because of (5.4)). We will focus on the following problem.

Problem 5.2.1. — *Find the conditions on ρ such that*

$$\mathbb{E} \sup_{y \in T \cap \rho S^{N-1}} \left| \sum_{i=1}^{n} \langle Y_i, y\rangle^2 - \frac{K^2\, n\rho^2}{N} \right| \le \frac{2}{3} \frac{K^2\, n\rho^2}{N}.$$

Indeed if this inequality is satisfied, there exists a choice of vectors $(Y_i)_{1 \le i \le n}$ such that

$$\forall y \in T \cap \rho S^{N-1}, \left| \sum_{i=1}^{n} \langle Y_i, y\rangle^2 - \frac{K^2\, n\rho^2}{N} \right| \le \frac{2}{3} \frac{K^2\, n\rho^2}{N},$$

from which we deduce that

$$\forall y \in T \cap \rho S^{N-1}, \sum_{i=1}^{n} \langle Y_i, y\rangle^2 \ge \frac{1}{3} \frac{K^2\, n\rho^2}{N} > 0.$$

Therefore, by Proposition 5.1.2, we conclude that $\operatorname{rad}(\ker \Phi \cap T) < \rho$. Doing this with $T = B_1^N$, we will conclude by Proposition 5.1.1 that if

$$m \le \frac{1}{4\rho^2}$$

then the matrix Φ is a good encoder, that is for every $u \in \Sigma_m$, the solution of the basis pursuit algorithm (5.1) is unique and equal to u.

Remark 5.2.2. — *The number $2/3$ can be replaced by any real $r \in (0, 1)$.*

The method of selectors. — The second definition of randomness uses the notion of selectors. Let $\delta \in (0, 1)$ and let δ_i be i.i.d. random variables taking the values 1 with probability δ and 0 with probability $1 - \delta$.

We start from an orthogonal matrix with rows $\phi_1, \dots, \phi_N$ and we select randomly some rows to construct a matrix Φ with row vectors ϕ_i if $\delta_i = 1$. The random variables $\delta_1, \dots, \delta_N$ are called selectors and the number of rows of Φ, equal to $|\{i : \delta_i = 1\}|$, will be highly concentrated around δN. Problem 5.2.1 can be stated in the following way:

Problem 5.2.3. — *Find the conditions on* ρ *such that*

$$\mathbb{E} \sup_{y \in T \cap \rho S^{N-1}} \left| \sum_{i=1}^{N} \delta_i \langle \phi_i, y \rangle^2 - \delta K^2 \rho^2 \right| \leq \frac{2}{3} \delta K^2 \rho^2.$$

The same argument as before shows that if this inequality holds for $T = B_1^N$, there exists a choice of selectors such that $\operatorname{rad}(\ker \Phi \cap B_1^N) < \rho$ and we can conclude as before that the matrix Φ is a good encoder.

These two definitions of randomness are not very different. The empirical method refers to sampling with replacement while the method of selectors refers to sampling without replacement.

Before stating the main results, we need some tools from the theory of empirical processes to solve Problems 5.2.1 and 5.2.3. Another question is to prove that the random matrix Φ is a good decoder with high probability. We will also present some concentration inequalities of the supremum of empirical processes around their mean, that will enable us to get better deviation inequality than the Markov bound.

5.3. Empirical processes

Classical tools. — A lot is known about the supremum of empirical processes and the connection with Rademacher averages. We refer to chapter 4 of [**LT91**] for a detailed description. We recall the important comparison theorem for Rademacher average.

Theorem 5.3.1. — *Let* $F : \mathbb{R}^+ \to \mathbb{R}^+$ *be an increasing convex function, let* $h_i : \mathbb{R} \to \mathbb{R}$ *be functions such that* $|h_i(s) - h_i(t)| \leq |s - t|$ *and* $h_i(0) = 0$, $1 \leq i \leq n$. *Then for any separable bounded set* $T \subset \mathbb{R}^n$,

$$\mathbb{E} F \left(\frac{1}{2} \sup_{t \in T} \left| \sum_{i=1}^{n} \varepsilon_i h_i(t_i) \right| \right) \leq \mathbb{E} F \left(\sup_{t \in T} \left| \sum_{i=1}^{n} \varepsilon_i t_i \right| \right).$$

The proof of this theorem is however beyond the scope of this chapter. We concentrate now on the study of the average of the supremum of some empirical processes. Consider n independent random vectors $Y_1, \ldots, Y_n$ taking values in a measurable space Ω and $\mathcal{F}$ be a class of measurable functions on Ω. Define

$$Z = \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} \big(f(Y_i) - \mathbb{E} f(Y_i) \big) \right|.$$

The situation will be different from Chapter 1 because the control on the ψ_α norm of $f(Y_i)$ is not relevant in our situation. In this case, a classical strategy consists to "symmetrize" the variable and to introduce Rademacher averages.

Theorem 5.3.2. — *Consider* n *independent random vectors* $Y_1, \ldots, Y_n$ *taking values in a measurable space* Ω, $\mathcal{F}$ *be a class of measurable functions and* $\varepsilon_1, \ldots, \varepsilon_n$ *be independent Rademacher random variables, independent of the* Y_i*'s. Denote by* $\mathbb{E}_\varepsilon$ *the* *expectation with respect to these Rademacher random variables. Then the following inequalities hold:*

$$\mathbb{E}\sup_{f\in\mathcal{F}}\left|\sum_{i=1}^{n}(f(Y_i)-\mathbb{E}f(Y_i))\right|\leq 2\mathbb{E}\mathbb{E}_\varepsilon\sup_{f\in\mathcal{F}}\left|\sum_{i=1}^{n}\varepsilon_i f(Y_i)\right|, \tag{5.5}$$

$$\mathbb{E}\sup_{f\in\mathcal{F}}\sum_{i=1}^{n}|f(Y_i)|\leq\sup_{f\in\mathcal{F}}\sum_{i=1}^{n}\mathbb{E}|f(Y_i)|+4\mathbb{E}\mathbb{E}_\varepsilon\sup_{f\in\mathcal{F}}\left|\sum_{i=1}^{n}\varepsilon_i f(Y_i)\right|. \tag{5.6}$$

Moreover

$$\mathbb{E}\mathbb{E}_\varepsilon\sup_{f\in\mathcal{F}}\left|\sum_{i=1}^{n}\varepsilon_i(f(Y_i)-\mathbb{E}f(Y_i))\right|\leq 2\mathbb{E}\sup_{f\in\mathcal{F}}\left|\sum_{i=1}^{n}(f(Y_i)-\mathbb{E}f(Y_i))\right|. \tag{5.7}$$

Proof. — Let $Y_1',\dots,Y_n'$ be independent copies of $Y_1,\dots,Y_n$. We replace $\mathbb{E}f(Y_i)$ by $\mathbb{E}'f(Y_i')$ where $\mathbb{E}'$ denotes the expectation with respect to the random vectors $Y_1',\dots,Y_n'$ then by Jensen inequality,

$$\mathbb{E}\sup_{f\in\mathcal{F}}\left|\sum_{i=1}^{n}(f(Y_i)-\mathbb{E}f(Y_i))\right|\leq\mathbb{E}\mathbb{E}'\sup_{f\in\mathcal{F}}\left|\sum_{i=1}^{n}(f(Y_i)-f(Y_i'))\right|.$$

The random variables $(f(Y_i)-f(Y_i'))_{1\leq i\leq n}$ are independent and now symmetric, hence $(f(Y_i)-f(Y_i'))_{1\leq i\leq n}$ has the same law as $(\varepsilon_i(f(Y_i)-f(Y_i')))_{1\leq i\leq n}$ where $\varepsilon_1,\dots,\varepsilon_n$ are independent Rademacher random variables. We deduce that

$$\mathbb{E}\sup_{f\in\mathcal{F}}\left|\sum_{i=1}^{n}(f(Y_i)-\mathbb{E}f(Y_i))\right|\leq\mathbb{E}\mathbb{E}'\mathbb{E}_\varepsilon\sup_{f\in\mathcal{F}}\left|\sum_{i=1}^{n}\varepsilon_i(f(Y_i)-f(Y_i'))\right|.$$

We conclude the proof of (5.5) by using the triangle inequality.
Inequality (5.6) is a consequence of (5.5) when applying it to $|f|$ instead of f, using the triangle inequality and Theorem 5.3.1 (in the case $F(x)=x$ and $h_i(x)=|x|$) to deduce that

$$\mathbb{E}_\varepsilon\sup_{f\in\mathcal{F}}\left|\sum_{i=1}^{n}\varepsilon_i|f(Y_i)|\right|\leq 2\mathbb{E}_\varepsilon\sup_{f\in\mathcal{F}}\left|\sum_{i=1}^{n}\varepsilon_i f(Y_i)\right|.$$

For the proof of (5.7), we can assume without loss of generality that $\mathbb{E}f(Y_i)=0$. We compute the expectation conditionally with respect to the Rademacher random variables. Let $I=I(\varepsilon)=\{i,\varepsilon_i=1\}$ then

$$\begin{aligned}\mathbb{E}\mathbb{E}_\varepsilon\sup_{f\in\mathcal{F}}\left|\sum_{i=1}^{n}\varepsilon_i f(Y_i)\right| &\leq\mathbb{E}_\varepsilon\mathbb{E}\sup_{f\in\mathcal{F}}\left|\sum_{i\in I}f(Y_i)-\sum_{i\notin I}f(Y_i)\right|\\ &\leq\mathbb{E}_\varepsilon\mathbb{E}\sup_{f\in\mathcal{F}}\left|\sum_{i\in I}f(Y_i)\right|+\mathbb{E}_\varepsilon\mathbb{E}\sup_{f\in\mathcal{F}}\left|\sum_{i\notin I}f(Y_i)\right|.\end{aligned}$$

However, since for every $i \le n$, $\mathbb{E}f(Y_i) = 0$ we deduce from Jensen inequality that for any $I \subset \{1, \dots, n\}$

$$\mathbb{E} \sup_{f \in \mathcal{F}} \left| \sum_{i \in I} f(Y_i) \right| = \mathbb{E} \sup_{f \in \mathcal{F}} \left| \sum_{i \in I} f(Y_i) + \sum_{i \notin I} \mathbb{E} f(Y_i) \right| \le \mathbb{E} \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} f(Y_i) \right|$$

which ends the proof of (5.7). □

Another simple fact is the following comparison between the supremum of Rademacher processes and the supremum of the same Gaussian processes.

Proposition 5.3.3. — *Let $\varepsilon_1, \dots, \varepsilon_n$ be independent Rademacher random variables and $g_1, \dots, g_n$ be independent Gaussian $\mathcal{N}(0,1)$ random variables Then for any set $T \subset \mathbb{R}^n$*

$$\mathbb{E} \sup_{t \in T} \left| \sum_{i=1}^{n} \varepsilon_i t_i \right| \le \sqrt{\frac{2}{\pi}} \mathbb{E} \sup_{t \in T} \left| \sum_{i=1}^{n} g_i t_i \right|.$$

Proof. — Indeed, $(g_1, \dots, g_n)$ has the same law as $(\varepsilon_1 |g_1|, \dots, \varepsilon_n |g_n|)$ and by Jensen inequality,

$$\mathbb{E}_\varepsilon \mathbb{E}_g \sup_{t \in T} \left| \sum_{i=1}^{n} \varepsilon_i |g_i| t_i \right| \ge \mathbb{E}_\varepsilon \sup_{t \in T} \left| \mathbb{E}_g \sum_{i=1}^{n} \varepsilon_i |g_i| t_i \right| = \sqrt{\frac{\pi}{2}} \mathbb{E} \sup_{t \in T} \left| \sum_{i=1}^{n} \varepsilon_i t_i \right|.$$

□

To conclude, we state without proof an important result about the concentration of the supremum of empirical processes around its mean. This is why we will focus on the estimation of the expectation of the supremum of such empirical process.

Theorem 5.3.4. — *Consider n independent random vectors $Y_1, \dots, Y_n$ and $\mathcal{G}$ a class of measurable functions. Let*

$$Z = \sup_{g \in \mathcal{G}} \left| \sum_{i=1}^{n} g(Y_i) \right|, \; M = \sup_{g \in \mathcal{G}} \|g\|_\infty, \; V = \mathbb{E} \sup_{g \in \mathcal{G}} \sum_{i=1}^{n} g(Y_i)^2.$$

Then for any $t > 0$, we have

$$\mathbb{P}\left(|Z - \mathbb{E}Z| > t\right) \le C \exp\left(-c \, \frac{t}{M} \, \log\left(1 + \frac{tM}{V}\right)\right).$$

Sometimes, we need a more simple quantity than V in this concentration inequality.

Proposition 5.3.5. — *Consider n independent random vectors $Y_1, \dots, Y_n$ and $\mathcal{F}$ a class of measurable functions. Let*

$$Z = \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} f(Y_i) - \mathbb{E} f(Y_i) \right|, \; u = \sup_{f \in \mathcal{F}} \|f\|_\infty, \; \textit{and}$$

$$v = \sup_{f \in \mathcal{F}} \sum_{i=1}^{n} \mathrm{Var} f(Y_i) + 32 \, u \, \mathbb{E} \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} f(Y_i) - \mathbb{E} f(Y_i) \right|.$$

Then for any $t > 0$, we have

$$\mathbb{P}\left(|Z - \mathbb{E}Z| > t\right) \leq C \exp\left(-c\,\frac{t}{u}\,\log\left(1 + \frac{tu}{v}\right)\right).$$

Proof. — It is a typical use of the symmetrization principle. Let $\mathcal{G}$ be the set of functions defined by $g(Y) = f(Y) - \mathbb{E}f(Y)$ where $f \in \mathcal{F}$. Using Theorem 5.3.4, the conclusion will follow when estimating

$$M = \sup_{g\in\mathcal{G}} \|g\|_\infty \text{ and } V = \mathbb{E}\sup_{g\in\mathcal{G}} \sum_{i=1}^n g(Y_i)^2.$$

It is clear that $M \leq 2u$ and by the triangle inequality we get

$$\mathbb{E}\sup_{g\in\mathcal{G}} \sum_{i=1}^n g(Y_i)^2 \;\leq\; \mathbb{E}\sup_{g\in\mathcal{G}} \left|\sum_{i=1}^n g(Y_i)^2 - \mathbb{E}g(Y_i)^2\right| + \sup_{g\in\mathcal{G}} \sum_{i=1}^n \mathbb{E}g(Y_i)^2.$$

Using inequality (5.5), we deduce that

$$\mathbb{E}\sup_{g\in\mathcal{G}} \left|\sum_{i=1}^n g(Y_i)^2 - \mathbb{E}g(Y_i)^2\right| \leq 2\,\mathbb{E}\mathbb{E}_\varepsilon \sup_{g\in\mathcal{G}} \left|\sum_{i=1}^n \varepsilon_i g(Y_i)^2\right| = 2\,\mathbb{E}\mathbb{E}_\varepsilon \sup_{t\in T} \left|\sum_{i=1}^n \varepsilon_i t_i^2\right|$$

where T is the random set $\{t = (t_1, \ldots, t_n) = (g(Y_1), \ldots, g(Y_n)) : g \in \mathcal{G}\}$. Since $T \subset [-2u, 2u]^n$, the function $h(x) = x^2$ is $4u$-Lipschitz on T. By Theorem 5.3.1, we get

$$\mathbb{E}_\varepsilon \sup_{t\in T} \left|\sum_{i=1}^n \varepsilon_i t_i^2\right| \leq 8\,u\,\mathbb{E}_\varepsilon \sup_{t\in T} \left|\sum_{i=1}^n \varepsilon_i t_i\right|.$$

Since for $1 \leq i \leq n$, $\mathbb{E}g(Y_i) = 0$, we deduce from (5.7) that

$$\mathbb{E}\mathbb{E}_\varepsilon \sup_{g\in\mathcal{G}} \left|\sum_{i=1}^n \varepsilon_i g(Y_i)^2\right| \leq 16\,u\,\mathbb{E}\sup_{g\in\mathcal{G}} \left|\sum_{i=1}^n g(Y_i)\right|.$$

This allows to conclude that

$$V \leq 32\,u\,\mathbb{E}\sup_{f\in\mathcal{F}} \left|\sum_{i=1}^n f(Y_i) - \mathbb{E}f(Y_i)\right| + \sup_{f\in\mathcal{F}} \sum_{i=1}^n \mathrm{Var} f(Y_i).$$

This ends the proof of the proposition. □

The expectation of the supremum of some empirical processes. — We go back to Problem 5.2.1 with a definition of randomness given by the empirical method. The situation is similar if we had worked with the method of selectors. For a star body $T \subset \mathbb{R}^N$, we define the class $\mathcal{F}$ of functions in the following way:

$$\mathcal{F} = \left\{f_y : \mathbb{R}^N \to \mathbb{R},\ \text{defiined by } f_y(Y) = \langle Y, y\rangle \;:\; y \in T \cap \rho S^{N-1}\right\}.$$

Therefore

$$Z = \sup_{f\in\mathcal{F}} \left|\sum_{i=1}^n (f^2(Y_i) - \mathbb{E}f^2(Y_i))\right| = \sup_{y\in T\cap\rho S^{N-1}} \left|\sum_{i=1}^n \langle Y_i, y\rangle^2 - \frac{n\rho^2}{N}\right|.$$

Applying the symmetrization procedure to Z (cf (5.5)) and comparing Rademacher and Gaussian processes, we conclude that

$$\mathbb{E} \sup_{y \in T \cap \rho S^{N-1}} \left| \sum_{i=1}^{n} \langle Y_i, y \rangle^2 - \frac{n\rho^2}{N} \right| \leq 2\mathbb{E}\mathbb{E}_\varepsilon \sup_{y \in T \cap \rho S^{N-1}} \left| \sum_{i=1}^{n} \varepsilon_i \langle Y_i, y \rangle^2 \right|$$
$$\leq \sqrt{2\pi}\mathbb{E}\mathbb{E}_g \sup_{y \in T \cap \rho S^{N-1}} \left| \sum_{i=1}^{n} g_i \langle Y_i, y \rangle^2 \right|.$$

We will first get a bound for the Rademacher average (or the Gaussian one) and then we will take the expectation with respect to the Y_i's. Before working with these difficult processes, we present a result of Rudelson where the supremum is taken on the unit sphere S^{N-1}.

Theorem 5.3.6. — *For any fixed vectors $x_1, \ldots, x_n$ in $\mathbb{R}^N$,*

$$\mathbb{E}_\varepsilon \sup_{y \in S^{N-1}} \left| \sum_{i=1}^{n} \varepsilon_i \langle x_i, y \rangle^2 \right| \leq C \sqrt{\log n} \max_{1 \leq i \leq n} |x_i|_2 \sup_{y \in S^{N-1}} \left(\sum_{i=1}^{n} \langle x_i, y \rangle^2 \right)^{1/2}.$$

Proof. — Let $S : \mathbb{R}^N \to \mathbb{R}^N$ be a self-adjoint operator and $(\lambda_i)_{1 \leq i \leq N}$ be its eigenvalues written in decreasing order. By definition of the S_q^N norms for $q \geq 1$,

$$\|S\|_{2 \to 2} = \|S\|_{S_\infty^N} = \max_{1 \leq i \leq n} |\lambda_i| \quad \text{and} \quad \|S\|_{S_q^N} = \left(\sum_{i=1}^{N} |\lambda_i|^q \right)^{1/q}.$$

Assume that the operator S has rank less than n then for $i \geq n+1$, $\lambda_i = 0$ and we deduce by Hölder inequality that

$$\|S\|_{S_\infty^N} \leq \|S\|_{S_q^N} \leq n^{1/q} \|S\|_{S_\infty^N} \leq e\|S\|_{S_\infty^N} \quad \text{for} \quad q \geq \log n.$$

By the non-commutative Khinchine inequality of Lust-Piquard and Pisier, we know that for any operator $T_1, \ldots, T_n$,

$$\mathbb{E}_\varepsilon \left\| \sum_{i=1}^{n} \varepsilon_i T_i \right\|_{S_q^N} \leq C \sqrt{q} \max \left\{ \left\| \left(\sum_{i=1}^{n} T_i^* T_i \right)^{1/2} \right\|_{S_q^N}, \left\| \left(\sum_{i=1}^{n} T_i T_i^* \right)^{1/2} \right\|_{S_q^N} \right\}.$$

For the proof of the Proposition, we define for every $i = 1, \ldots, n$ the self-adjoint rank 1 operators

$$T_i = x_i \otimes x_i : \left\{ \begin{array}{ccc} \mathbb{R}^N & \to & \mathbb{R}^N \\ y & \mapsto & \langle x_i, y \rangle x_i \end{array} \right.$$

in such a way that

$$\sup_{y \in S^{N-1}} \left| \sum_{i=1}^{n} \varepsilon_i \langle x_i, y \rangle^2 \right| = \sup_{y \in S^{N-1}} \left| \langle \sum_{i=1}^{n} \varepsilon_i T_i y, y \rangle \right| = \left\| \sum_{i=1}^{n} \varepsilon_i T_i \right\|_{2 \to 2}.$$

Therefore, $T_i^*T_i = T_iT_i^* = |x_i|_2^2 T_i$ and $S = \left(\sum_{i=1}^n T_i^*T_i\right)^{1/2}$ has rank less than n, hence for $q = \log n$,

$$\left\| \left(\sum_{i=1}^n T_i^* T_i \right)^{1/2} \right\|_{S_q^N} \leq e \left\| \left(\sum_{i=1}^n |x_i|_2^2 T_i \right)^{1/2} \right\|_{S_\infty^N} \leq e \max_{1\leq i\leq n} |x_i|_2 \left\| \sum_{i=1}^n T_i \right\|_{S_\infty^N}^{1/2}.$$

Combining these estimates with the non-commutative Khinchine inequality, we conclude that for $q = \log n$

$$\begin{aligned}\mathbb{E}_\varepsilon \left\| \sum_{i=1}^n \varepsilon_i T_i \right\|_{S_\infty^N} &\leq C\sqrt{\log n} \left\| \left(\sum_{i=1}^n T_i^* T_i \right)^{1/2} \right\|_{S_{\log n}^N} \\ &\leq C\, e\sqrt{\log n} \max_{1\leq i\leq n} |x_i|_2 \sup_{y\in S^{N-1}} \left(\sum_{i=1}^n \langle x_i, y\rangle^2 \right)^{1/2}.\end{aligned}$$

□

Remark 5.3.7. — *Since the non-commutative Khinchine inequality holds true for independent Gaussian standard random variables, this result is also valid for Gaussian random variables.*

The proof that we presented here is based on an expression related to some operator norms and our original question can not be expressed with these tools. The original proof of Rudelson used the majorizing measure theory. The forthcoming Theorem 5.3.12 is an improvement of this result and it is necessary to give some definitions from the theory of Banach spaces.

Definition 5.3.8. — *A Banach space B is of type 2 if there exists a constant $c > 0$ such that for every n and every $x_1, \ldots, x_n \in B$,*

$$\left(\mathbb{E}_\varepsilon \left\| \sum_{i=1}^n \varepsilon_i x_i \right\|^2 \right)^{1/2} \leq c \left(\sum_{i=1}^n \|x_i\|^2 \right)^{1/2}.$$

The smallest constant $c > 0$ satisfying this statement is called the type 2 constant of B and is denoted by $T_2(B)$.

Classical examples of infinite dimensional Banach spaces of type 2 are Hilbert spaces and L_q space for $2 \leq q < +\infty$. Be aware that Theorem 1.2.1 in Chapter 1 does not mean that L_{ψ_2} has type 2. In fact, it is not the case.

Definition 5.3.9. — *A Banach space B has modulus of convexity of power type 2 with constant λ if*

$$\forall x, y \in B, \quad \left\| \frac{x+y}{2} \right\|^2 + \lambda^{-2} \left\| \frac{x-y}{2} \right\|^2 \leq \frac{1}{2} \left(\|x\|^2 + \|y\|^2 \right).$$

The modulus of convexity of a Banach space B is defined for $\varepsilon \in (0, 2]$ by

$$\delta_B(\varepsilon) = \inf \left\{ 1 - \left\| \frac{x+y}{2} \right\| : \quad \|x\| = \|y\| = 1 \text{ and } \|x-y\| \le \varepsilon \right\}.$$

It is obvious that if B has modulus of convexity of power type 2 with constant λ then $\delta_B(\varepsilon) \ge \varepsilon^2/2\lambda^2$ and it is well known that the reverse holds true (with a constant different from 2). Moreover, for $1 < p \le 2$, Clarkson inequality tells that for any $f, g \in L_p$,

$$\left\| \frac{f+g}{2} \right\|_p^2 + \frac{p(p-1)}{8} \left\| \frac{f-g}{2} \right\|_p^2 \le \frac{1}{2}(\|f\|_p^2 + \|g\|_p^2).$$

This proves that for any $p \in (1, 2]$, L_p has modulus of convexity of power type 2 with $\lambda = c\sqrt{p-1}$.

Definition 5.3.10. — *A Banach space B has modulus of smoothness of power type 2 with constant μ if*

$$\forall x, y \in B, \quad \left\| \frac{x+y}{2} \right\|^2 + \mu^2 \left\| \frac{x-y}{2} \right\|^2 \ge \frac{1}{2} \left(\|x\|^2 + \|y\|^2 \right).$$

The modulus of smoothness of a Banach space B is defined for every $\tau > 0$ by

$$\rho_B(\tau) = \sup \left\{ \frac{\|x + \tau y\| + \|x - \tau y\|}{2} - 1 : \quad \|x\| = \|y\| = 1 \right\}.$$

It is clear that if B has modulus of smoothness of power type 2 with constant μ then for every $\tau \in (0, 1), \rho_B(\tau) \le 2\tau^2\mu^2$ and it is well known that the reverse holds true (with a constant different from 2).
More generally, a Banach space B is said to be uniformly convex if for every $\varepsilon > 0$, $\delta_B(\varepsilon) > 0$ and uniformly smooth if $\lim_{\tau \to 0} \rho_B(\tau)/\tau = 0$. We have the following simple relation between these notions.

Proposition 5.3.11. — *For every Banach space B, $B^\star$ being its dual, we have*
(*i*) *For every $\tau > 0$, $\rho_{B^\star}(\tau) = \sup\{\tau\varepsilon/2 - \delta_B(\varepsilon), 0 < \varepsilon \le 2\}$.*
(*ii*) *B is uniformly convex if and only if $B^\star$ is uniformly smooth.*
(*iii*) *For any Banach space B, if B has modulus of convexity of power type 2 with constant λ then $B^\star$ has modulus of smoothness of power type 2 with constant $c\lambda$ and $T_2(B^\star) \le c\lambda$.*

Proof. — The proof of (*i*) is straightforward, using the definition of duality. We have for $\tau > 0$,

$$\begin{aligned} 2\rho_{B^\star}(\tau) &= \sup\{\|x^\star + \tau y^\star\| + \|x^\star - \tau y^\star\| - 2 : \ \|x^\star\| = \|y^\star\| = 1\} \\ &= \sup\{x^\star(x) + \tau y^\star(x) + x^\star(y) - \tau y^\star(y) - 2 : \ \|x^\star\| = \|y^\star\| = \|x\| = \|y\| = 1\} \\ &= \sup\{x^\star(x+y) + \tau y^\star(x-y) - 2 : \ \|x^\star\| = \|y^\star\| = \|x\| = \|y\| = 1\} \\ &= \sup\{\|x+y\| + \tau\|x-y\| - 2 : \ \|x\| = \|y\| = 1\} \\ &= \sup\{\|x+y\| + \tau\varepsilon - 2 : \ \|x\| = \|y\| = 1, \|x-y\| \le \varepsilon, \varepsilon \in (0, 2]\} \\ &= \sup\{\tau\varepsilon - 2\delta_B(\varepsilon) : \ \varepsilon \in (0, 2]\}. \end{aligned}$$

The proof of (*ii*) follows directly from (*i*). We will just prove (*iii*). If B has modulus of convexity of power type 2 with constant λ then $\delta_B(\varepsilon) \geq \varepsilon^2/2\lambda^2$. By (*i*) we deduce that $\rho_{B^\star}(\tau) \geq \tau^2\lambda^2/4$. It implies that for any $x^\star$, $y^\star \in B^\star$,

$$\left\|\frac{x^\star + y^\star}{2}\right\|_\star^2 + (c\lambda)^2\left\|\frac{x^\star - y^\star}{2}\right\|_\star^2 \geq \frac{1}{2}\left(\|x^\star\|_\star^2 + \|y^\star\|_\star^2\right)$$

where $c > 0$. We deduce that for $u^\star$, $v^\star \in B^\star$,

$$\mathbb{E}_\varepsilon\|\varepsilon u^\star + v^\star\|_\star^2 = \frac{1}{2}\left(\|u^\star + v^\star\|_\star^2 + \|-u^\star + v^\star\|_\star^2\right) \leq \|v^\star\|_\star^2 + (c\lambda)^2\|u^\star\|_\star^2.$$

We conclude by induction that for any integer n and any vectors $x_1^\star, \dots, x_n^\star \in B^\star$,

$$\mathbb{E}_\varepsilon\left\|\sum_{i=1}^n \varepsilon_i x_i^\star\right\|_\star^2 \leq (c\lambda)^2\left(\sum_{i=1}^n \|x_i^\star\|_\star^2\right)$$

which proves that $T_2(B^\star) \leq c\lambda$. □

It is now possible to state without proof one main estimate of the average of the supremum of empirical processes.

Theorem 5.3.12. — *If B is a Banach space with modulus of convexity of power type 2 with constant λ then for any integer n and $x_1^*, \dots x_n^* \in B^\star$,*

$$\mathbb{E}_g \sup_{\|x\|\leq 1}\left|\sum_{i=1}^n g_i\langle x_i^*, x\rangle^2\right| \leq C\,\lambda^5\,\sqrt{\log n}\,\max_{1\leq i\leq n}\|x_i^*\|_\star \sup_{\|x\|\leq 1}\left(\sum_{i=1}^n \langle x_i^*, x\rangle^2\right)^{1/2}$$

where $g_1, \dots, g_n$ are independent $\mathcal{N}(0,1)$ Gaussian random variables and C is a numerical constant.

The proof of Theorem 5.3.12 is slightly complicated. It involves a specific construction of majorizing measures and deep results about the duality of covering numbers (it is where the notion of type is used). We will not present it.

Corollary 5.3.13. — *Let B be a Banach space with modulus of convexity of power type 2 with constant λ. Let $Y_1, \dots, Y_n$ taking values in $B^\star$ be independent random vectors and denote*

$$K(n,Y) = 2\sqrt{\frac{2}{\pi}}C\lambda^5\sqrt{\log n}\left(\mathbb{E}\max_{1\leq i\leq n}\|Y_i\|_\star^2\right)^{1/2} \quad \text{and} \quad \sigma^2 = \sup_{\|y\|\leq 1}\sum_{i=1}^n \mathbb{E}\langle Y_i, y\rangle^2$$

where C is the numerical constant of Theorem 5.3.12. Then we have

$$\mathbb{E}\sup_{\|y\|\leq 1}\left|\sum_{i=1}^n \langle Y_i, y\rangle^2 - \mathbb{E}\langle Y_i, y\rangle^2\right| \leq K(n,Y)^2 + K(n,Y)\,\sigma.$$

Proof. — Let

$$V_2 = \mathbb{E}\sup_{\|y\|\leq 1}\left|\sum_{i=1}^n \left(\langle Y_i, y\rangle^2 - \mathbb{E}\langle Y_i, y\rangle^2\right)\right|.$$

We start with a symmetrization argument. By (5.5) and Proposition 5.3.3 we have

$$V_2 \leq 2\, \mathbb{E}\mathbb{E}_\varepsilon \sup_{\|y\|\leq 1} \left| \sum_{i=1}^n \varepsilon_i \langle Y_i, y\rangle^2 \right| \leq 2\sqrt{\frac{2}{\pi}}\, \mathbb{E}\mathbb{E}_g \sup_{\|y\|\leq 1} \left| \sum_{i=1}^n g_i \langle Y_i, y\rangle^2 \right|.$$

In view of Theorem 5.3.12, observe that the crucial quantity in the estimate is $\sup_{\|x\|\leq 1} \left(\sum_{i=1}^n \langle Y_i, x\rangle^2\right)^{1/2}$. Indeed, by the triangle inequality,

$$\mathbb{E} \sup_{\|x\|\leq 1} \sum_{i=1}^n \langle Y_i, x\rangle^2 \leq \mathbb{E} \sup_{\|y\|\leq 1} \left| \sum_{i=1}^n \left(\langle Y_i, y\rangle^2 - \mathbb{E}\langle Y_i, y\rangle^2\right) \right| + \sup_{\|y\|\leq 1} \sum_{i=1}^n \mathbb{E}\langle Y_i, y\rangle^2 = V_2 + \sigma^2.$$

Therefore, applying Theorem 5.3.12 and Cauchy Schwarz inequality, we get

$$\begin{aligned} V_2 &\leq 2\sqrt{\frac{2}{\pi}}\, C\lambda^5 \sqrt{\log n}\, \mathbb{E}\left(\max_{1\leq i\leq n} \|Y_i\|_\star \sup_{\|x\|\leq 1} \left(\sum_{i=1}^n \langle Y_i, x\rangle^2 \right)^{1/2} \right) \\ &\leq 2\sqrt{\frac{2}{\pi}}\, C\lambda^5 \sqrt{\log n} \left(\mathbb{E} \max_{1\leq i\leq n} \|Y_i\|_\star^2 \right)^{1/2} \left(\mathbb{E} \sup_{\|x\|\leq 1} \sum_{i=1}^n \langle Y_i, x\rangle^2 \right)^{1/2} \\ &\leq K(n, Y) \left(V_2 + \sigma^2\right)^{1/2}. \end{aligned}$$

We get

$$V_2^2 - K(n,Y)^2 V_2 - K(n,Y)^2\sigma^2 \leq 0$$

from which it is easy to conclude that

$$V_2 \leq K(n,Y)\ (K(n,Y) + \sigma).$$

□

Using simpler ideas than for the proof of Theorem 5.3.12, we can present a general result where the assumption that B has a good modulus of convexity is not needed.

Theorem 5.3.14. — *Let B be a Banach space and $Y_1, \dots, Y_n$ be independent random vectors taking values in $B^\star$. Let $\mathcal{F}$ be a set of functionals on $B^\star$ with $0 \in \mathcal{F}$. Denote by $d_{\infty,n}$ the random pseudo-metric on $\mathcal{F}$ defined for every $f, \overline{f}$ in $\mathcal{F}$ by*

$$d_{\infty,n}(f, \overline{f}) = \max_{1\leq i\leq n} \left| f(Y_i) - \overline{f}(Y_i) \right|.$$

We have

$$\mathbb{E} \sup_{f\in\mathcal{F}} \left| \sum_{i=1}^n \left(f(Y_i)^2 - \mathbb{E} f(Y_i)^2 \right) \right| \leq \max(\sigma_{\mathcal{F}} U_n, U_n^2)$$

where for a numerical constant C,

$$U_n = C\left(\mathbb{E}\gamma_2^2(\mathcal{F}, d_{\infty,n})\right)^{1/2} \quad \textit{and} \quad \sigma_{\mathcal{F}} = \left(\sup_{f\in\mathcal{F}} \sum_{i=1}^n \mathbb{E} f(Y_i)^2 \right)^{1/2}.$$

We refer to Chapter 3 for the definition of $\gamma_2(\mathcal{F}, d_{\infty,n})$ (see Definition 3.1.3) and to the same Chapter to learn how to bound the γ_2 functional. A simple example will be given in the proof of Theorem 5.4.1.

Proof. — As in the proof of Corollary 5.3.13, we need first to get a bound of

$$\mathbb{E}_g \sup_{f\in\mathcal{F}} \left| \sum_{i=1}^n g_i f(Y_i)^2 \right|.$$

Let $(X_f)_{f\in\mathcal{F}}$ be the Gaussian process defined conditionally with respect to the Y_i's, $X_f = \sum_{i=1}^n g_i f(Y_i)^2$ and indexed by $f \in \mathcal{F}$. The pseudo-metric d associated to this process is given for $f, \overline{f} \in \mathcal{F}$ by

$$\begin{aligned} d(f,\overline{f})^2 = \mathbb{E}_g|X_f - X_{\overline{f}}|^2 &= \sum_{i=1}^n \left(f(Y_i)^2 - \overline{f}(Y_i)^2\right)^2 \\ &= \sum_{i=1}^n \left(f(Y_i) - \overline{f}(Y_i)\right)^2 \left(f(Y_i) + \overline{f}(Y_i)\right)^2 \\ &\leq 2\sum_{i=1}^n \left(f(Y_i) - \overline{f}(Y_i)\right)^2 \left(f(Y_i)^2 + \overline{f}(Y_i)^2\right) \\ &\leq 4 \sup_{f\in\mathcal{F}} \left(\sum_{i=1}^n f(Y_i)^2\right) \max_{1\leq i\leq n} (f(Y_i) - \overline{f}(Y_i))^2. \end{aligned}$$

Thus we have

$$d(f,\overline{f}) \leq 2 \sup_{f\in\mathcal{F}} \left(\sum_{i=1}^n f(Y_i)^2\right)^{1/2} d_{\infty,n}(f,\overline{f}).$$

By definition of the γ_2 functionals, it follows that for every vectors $Y_1,\ldots,Y_n \in B^\star$,

$$\mathbb{E}_g \sup_{f\in\mathcal{F}} \left| \sum_{i=1}^n g_i f(Y_i)^2 \right| \leq C \sup_{f\in\mathcal{F}} \left(\sum_{i=1}^n f(Y_i)^2\right)^{1/2} \gamma_2(\mathcal{F}, d_{\infty,n})$$

where C is a universal constant. We repeat the proof of Corollary 5.3.13. Let

$$V_2 = \mathbb{E} \sup_{f\in\mathcal{F}} \left| \sum_{i=1}^n \left(f(Y_i)^2 - \mathbb{E}f(Y_i)^2\right) \right|.$$

By a symmetrization argument and Cauchy-Schwarz inequality,

$$\begin{aligned} V_2 &\leq 2\sqrt{\frac{2}{\pi}} \mathbb{E}\mathbb{E}_g \sup_{f\in\mathcal{F}} \left| \sum_{i=1}^n g_i f(Y_i)^2 \right| \leq C \left(\mathbb{E}\gamma_2(\mathcal{F}, d_{\infty,n})^2\right)^{1/2} \left(\mathbb{E} \sup_{f\in\mathcal{F}} \sum_{i=1}^n f(Y_i)^2\right)^{1/2} \\ &\leq C \left(\mathbb{E}\gamma_2(\mathcal{F}, d_{\infty,n})^2\right)^{1/2} \left(V_2 + \sigma_{\mathcal{F}}^2\right)^{1/2}, \end{aligned}$$

where the last inequality follows from the triangle inequality:

$$\mathbb{E} \sup_{f\in\mathcal{F}} \sum_{i=1}^n f(Y_i)^2 \leq V_2 + \sigma_{\mathcal{F}}^2.$$

This shows that V_2 satisfies an inequality of degree 2. It is easy to conclude that

$$V_2 \leq \max(\sigma_{\mathcal{F}} U_n, U_n^2), \text{ where } U_n = C \left(\mathbb{E}\gamma_2(\mathcal{F}, d_{\infty,n})^2\right)^{1/2}.$$

□

5.4. Reconstruction property

We are now able to state one main theorem concerning the reconstruction property of a random matrix obtained by taking empirical copies of the rows of a fixed orthogonal matrix (or by selecting randomly its rows).

Theorem 5.4.1. — *Let $\phi_1, \dots, \phi_N$ be an orthogonal system in ℓ_2^N such that for some real number K*

$$\forall i \leq N, \ |\phi_i|_2 = K \ \text{and} \ |\phi_i|_\infty \leq \frac{1}{\sqrt{N}}.$$

Let Y be the random vector defined by $Y = \phi_i$ with probability $1/N$ and $Y_1, \dots, Y_n$ be independent copies of Y. If

$$m \leq C_1 K^2 \frac{n}{\log N (\log n)^3}$$

then with probability greater than

$$1 - C_2 \exp(-C_3 K^2 n/m)$$

the matrix $\Phi = \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix}$ *is a good reconstruction matrix for sparse signals of size m, that is for every $u \in \Sigma_m$, the basis pursuit algorithm* (5.1), $\min_{t \in \mathbb{R}^N} \{|t|_1 : \Phi u = \Phi t\}$, *has a unique solution equal to u.*

Remark 5.4.2. — (*i*) *By definition of m, the probability of this event is always greater than $1 - C_2 \exp\left(-C_3 \log N (\log n)^3\right)$.*
(*ii*) *The same result holds when using the method of selectors.*
(*iii*) *As we already mentioned, this theorem covers the case of a lot of classical systems like the Fourier system and the Walsh system.*
(*iv*) *The result is also valid if the orthogonal system $\phi_1, \dots, \phi_N$ satisfies the weaker condition that for all $i \leq N$, $K_1 \leq |\phi_i|_2 \leq K_2$. In this new statement, K is replaced by K_2^2/K_1.*

Proof. — Observe that $\mathbb{E}\langle Y, y\rangle^2 = K^2 |y|_2^2/N$. We define the class of functions $\mathcal{F}$ in the following way:

$$\mathcal{F} = \left\{ f_y : \mathbb{R}^N \to \mathbb{R}, \text{ defiined by } f_y(Y) = \langle Y, y\rangle \ : \ y \in B_1^N \cap \rho S^{N-1} \right\}.$$

Therefore

$$Z = \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^n (f(Y_i)^2 - \mathbb{E} f(Y_i)^2) \right| = \sup_{y \in B_1^N \cap \rho S^{N-1}} \left| \sum_{i=1}^n \langle Y_i, y\rangle^2 - \frac{K^2 n \rho^2}{N} \right|.$$

With the notation of Theorem 5.3.14, we have

$$\sigma_{\mathcal{F}}^2 = \sup_{y \in B_1^N \cap \rho S^{N-1}} \sum_{i=1}^n \mathbb{E}\langle Y_i, y\rangle^2 = \frac{K^2 n \rho^2}{N}. \tag{5.8}$$

Moreover, since $B_1^N \cap \rho S^{N-1} \subset B_1^N$,

$$\gamma_2(B_1^N \cap \rho S^{N-1}, d_{\infty,n}) \le \gamma_2(B_1^N, d_{\infty,n}).$$

It is well known that the γ_2 functional is bounded by the Dudley integral (see (3.7) in Chapter 3):

$$\gamma_2(B_1^N, d_{\infty,n}) \le C \int_0^{+\infty} \sqrt{\log N(B_1^N, \varepsilon, d_{\infty,n})}\, d\varepsilon.$$

Moreover, for $1 \le i \le n$, $|Y_i|_\infty \le 1/\sqrt{N}$ and

$$\sup_{y,\overline{y}\in B_1^N} d_{\infty,n}(y,\overline{y}) = \sup_{y,\overline{y}\in B_1^N} \max_{1\le i\le n} |\langle Y_i, y-\overline{y}\rangle| \le 2 \max_{1\le i\le n} |Y_i|_\infty \le \frac{2}{\sqrt{N}}.$$

Hence, the integral is only computed from 0 to $2/\sqrt{N}$ and by the change of variable $t = \varepsilon\sqrt{N}$, we deduce that

$$\int_0^{+\infty} \sqrt{\log N(B_1^N, \varepsilon, d_{\infty,n})} d\varepsilon = \frac{1}{\sqrt{N}} \int_0^2 \sqrt{\log N\left(B_1^N, \frac{t}{\sqrt{N}}, d_{\infty,n}\right)}\, dt.$$

From Theorem 1.4.3, since for every $i \le n$, $|Y_i|_\infty \le 1/\sqrt{N}$, we have

$$\sqrt{\log N\left(B_1^N, \frac{t}{\sqrt{N}}, d_{\infty,n}\right)} \le \begin{cases} \dfrac{C}{t}\sqrt{\log n}\sqrt{\log N}, \\ C\sqrt{n\log\left(1+\dfrac{3}{t}\right)} \end{cases}.$$

We split the integral into two parts. We have

$$\begin{aligned}\int_0^{1/\sqrt{n}} \sqrt{n\log\left(1+\frac{3}{t}\right)} dt &= \int_0^1 \sqrt{\log\left(1+\frac{3\sqrt{n}}{u}\right)}\, du \\ &\le \int_0^1 \sqrt{\log n + \log\left(\frac{3}{u}\right)}\, du \le C\sqrt{\log n}\end{aligned}$$

and since

$$\int_{1/\sqrt{n}}^2 \frac{1}{t} dt \le C \log n,$$

we conclude that

$$\gamma_2(B_1^N \cap \rho S^{N-1}, d_{\infty,n}) \le \gamma_2(B_1^N, d_{\infty,n}) \le C\sqrt{\frac{(\log n)^3 \log N}{N}}. \tag{5.9}$$

Combining this estimate and (5.8) with Theorem 5.3.14, we get that for some $C \ge 1$,

$$\mathbb{E}Z \le C \max\left(\frac{(\log n)^3 \log N}{N},\ \rho K\sqrt{\frac{n}{N}}\sqrt{\frac{(\log n)^3 \log N}{N}}\right).$$

We choose ρ such that

$$(\log n)^3 \log N \le \rho K\sqrt{n(\log n)^3 \log N} \le \frac{1}{3C} K^2 \rho^2 n$$

which means that ρ satisfies

$$K\,\rho \geq 3\,C\,\sqrt{\frac{(\log n)^3 \log N}{n}}. \tag{5.10}$$

For this choice of ρ, we conclude that

$$\mathbb{E}Z = \mathbb{E} \sup_{y \in B_1^N \cap \rho S^{N-1}} \left| \sum_{i=1}^{n} \langle Y_i, y\rangle^2 - \frac{K^2 n \rho^2}{N} \right| \leq \frac{1}{3}\frac{K^2 n\rho^2}{N}.$$

We use Proposition 5.3.5 to get a deviation inequality for the random variable Z. With the notations of Proposition 5.3.5, we have

$$u = \sup_{y \in B_1^N \cap \rho S^{N-1}} \max_{1\leq i \leq N} \langle \phi_i, y\rangle^2 \leq \max_{1 \leq i \leq N} |\phi_i|_\infty^2 \leq \frac{1}{N}$$

and

$$\begin{aligned} v &= \sup_{y \in B_1^N \cap \rho S^{N-1}} \sum_{i=1}^{n} \mathbb{E}\left(\langle Y_i, y\rangle^2 - \mathbb{E}\langle Y_i, y\rangle^2\right)^2 \ + \ 32\,u\,\mathbb{E}Z \\ &\leq \sup_{y \in B_1^N \cap \rho S^{N-1}} \sum_{i=1}^{n} \mathbb{E}\langle Y_i, y\rangle^4 \ + \frac{CK^2 n\rho^2}{N^2} \leq \frac{CK^2 n \rho^2}{N^2} \end{aligned}$$

since for every $y \in B_1^N$, $\mathbb{E}\langle Y, y\rangle^4 \leq \mathbb{E}\langle Y, y\rangle^2/N$. We conclude using Proposition 5.3.5 and taking $t = \frac{1}{3}\frac{K^2 n\rho^2}{N}$, that

$$\mathbb{P}\left(Z \geq \frac{2}{3}\frac{K^2 n \rho^2}{N}\right) \leq C\exp(-c\,K^2\,n\,\rho^2).$$

With probability greater than $1 - C\exp(-c\,K^2\,n\,\rho^2)$, we get

$$\sup_{y \in B_1^N \cap \rho S^{N-1}} \left| \sum_{i=1}^{n} \langle Y_i, y\rangle^2 - \frac{K^2 n\rho^2}{N} \right| \leq \frac{2}{3}\frac{K^2 n \rho^2}{N}$$

from which it is easy to deduce by Proposition 5.1.2 that

$$\operatorname{rad}\left(\ker \Phi \cap B_1^N\right) < \rho.$$

We choose $m = 1/4\rho^2$ and conclude by Proposition 5.1.1 that with probability greater than $1 - C\exp(-cK^2 n/m)$, the matrix Φ is a good reconstruction matrix for sparse signals of size m, that is for every $u \in \Sigma_m$, the basis pursuit algorithm (5.1) has a unique solution equal to u. The condition on m in Theorem 5.4.1 comes from (5.10). □

Remark 5.4.3. — *By Proposition 2.7.3, it is clear that the matrix Φ shares also the property of approximate reconstruction. It is enough to set $m = 1/16\rho^2$. Therefore, if u is any unknown signal and x a solution of*

$$\min_{t \in \mathbb{R}^N} \{|t|_1, \Phi u = \Phi t\},$$

then for any subset I of cardinality less than m,

$$|x-u|_2 \le \frac{|x-u|_1}{4\sqrt{m}} \le \frac{|u_{I^c}|_1}{\sqrt{m}}.$$

5.5. Random selection of characters within a coordinate subspace

In this part, we consider the problem presented in section 5.1. We briefly recall the notations. Let (Ω,μ) be a probability space and $(\psi_1,\ldots,\psi_N)$ be an orthogonal system of $L_2(\mu)$ bounded in L_∞ i.e. such that for every $i \le N$, $\|\psi_i\|_\infty \le 1$ and $\|\psi_i\|_2 = K$ for a fixed number K. A typical example is a system of characters in $L_2(\mu)$ like the Fourier or the Walsh system. For a measurable function f and for $p>0$, we denote its L_p norm and its L_∞ norm by

$$\|f\|_p = \left(\int |f|^p d\mu\right)^{1/p} \quad \text{and} \quad \|f\|_\infty = \sup|f|.$$

As before, $\sup|f|$ means the essential supremum of $|f|$. In $\mathbb{R}^N$ or $\mathbb{C}^N$, we may define μ as the counting probability measure so that the L_p-norm of a vector $x=(x_1,\ldots,x_N)$ is defined by

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

In this case, ℓ_∞^N and L_∞^N coincide and we observe that if $(\psi_1,\ldots,\psi_N)$ is a bounded orthogonal system in L_2^N then $(\psi_1/\sqrt{N},\ldots,\psi_N/\sqrt{N})$ is an orthogonal system of ℓ_2^N such that for every $i \le N$, $|\psi_i/\sqrt{N}|_\infty \le 1/\sqrt{N}$. Therefore the setting is exactly the same as in the previous part up to a normalization factor of $\sqrt{N}$.

Of course the notation of the radius of a set T is now adapted to the $L_2(\mu)$ Euclidean structure. The radius of a set T is defined by

$$\operatorname{Rad} T = \sup_{t\in T}\|t\|_2.$$

For any $q>0$, we denote by B_q the unit ball of $L_q(\mu)$ and by S_q its unit sphere. Our problem is to find a very large subset I of $\{1,\ldots,N\}$ such that

$$\forall (a_i)_{i\in I}, \quad \left\|\sum_{i\in I} a_i\psi_i\right\|_2 \le \rho \left\|\sum_{i\in I} a_i\psi_i\right\|_1$$

with the smallest possible ρ. As we already said, Talagrand showed that there exists a small constant δ_0 such that for any bounded orthonormal system $\{\psi_1,\ldots,\psi_N\}$, there exists a subset I of cardinality greater than $\delta_0 N$ such that $\rho \le C\sqrt{\log N\,(\log\log N)}$. The proof involves the construction of specific majorizing measures. Moreover, it was known from Bourgain that the $\sqrt{\log N}$ is necessary in the estimate. We will now explain why the strategy that we developed in the previous part is adapted to this type of question. We will extend the result of Talagrand to a Kashin type setting, that is for example to find I of cardinality greater than $N/2$.

We start with a simple Proposition concerning some properties of a matrix that we will later define randomly as in Theorem 5.4.1.

Proposition 5.5.1. — *Let μ be a probability measure and let $(\psi_1, \dots, \psi_N)$ be an orthogonal system of $L_2(\mu)$ such that for every $i \le N$, $\|\psi_i\|_2 = K$ for a fixed number K. Let $Y_1, \dots, Y_n$ be a family of vectors taking values in the set of vectors $\{\psi_1, \dots, \psi_N\}$. Let Ψ be the matrix* $\Psi = \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix}$. *Then*
(i) $\ker \Psi = \mathrm{span}\,\{\{\psi_1, \dots, \psi_N\} \setminus \{Y_i\}_{i=1}^n\} = \mathrm{span}\,\{\psi_i\}_{i \in I}$ *where* $I \subset \{1, \dots, N\}$ *has cardinality greater than* $N - n$.
(ii) $(\ker \Psi)^\perp = \mathrm{span}\,\{\psi_i\}_{i \notin I}$.
(iii) For a star body T, if

$$\sup_{y \in T \cap \rho S_2} \left| \sum_{i=1}^n \langle Y_i, y \rangle^2 - \frac{nK^2\rho^2}{N} \right| \le \frac{1}{3} \frac{nK^2\rho^2}{N} \tag{5.11}$$

then $\mathrm{Rad}\,(\ker \Psi \cap T) < \rho$.
(iv) If $n < 3N/4$ and if (5.11) *is satisfied then we also have*

$$\mathrm{Rad}\,((\ker \Psi)^\perp \cap T) < \rho.$$

Proof. — Since $\{\psi_1, \dots, \psi_N\}$ is an orthogonal system, parts (i) and (ii) are obvious. For the proof of (iii), we first remark that if (5.11) holds, we get from the lower bound that for all $y \in T \cap \rho S_2$,

$$\sum_{i=1}^n \langle Y_i, y \rangle^2 \ge \frac{2}{3} \frac{nK^2\rho^2}{N}$$

and we deduce as in Proposition 5.1.2 that $\mathrm{Rad}\,(\ker \Psi \cap T) < \rho$.
For the proof of (iv), we deduce from the upper bound of (5.11) that for all $y \in T \cap \rho S_2$,

$$\begin{aligned} \sum_{i \in I} \langle \psi_i, y \rangle^2 &= \sum_{i=1}^N \langle \psi_i, y \rangle^2 - \sum_{i=1}^n \langle Y_i, y \rangle^2 = K^2 \|y\|_2^2 - \sum_{i=1}^n \langle Y_i, y \rangle^2 \\ &\ge K^2\rho^2 - \frac{4}{3} \frac{nK^2\rho^2}{N} = K^2\rho^2 \left(1 - \frac{4n}{3N}\right) > 0 \text{ since } n < 3N/4. \end{aligned}$$

This inequality means that for the matrix $\tilde{\Psi}$ defined by with raws $\{\psi_i, i \in I\}$, for every $y \in T \cap \rho S_2$, we have

$$\inf_{y \in T \cap \rho S_2} \|\tilde{\Psi} y\|_2^2 > 0.$$

We conclude as in Proposition 5.1.2 that $\mathrm{Rad}\,(\ker \tilde{\Psi} \cap T) < \rho$ and it is obvious that $\ker \tilde{\Psi} = (\ker \Psi)^\perp$. □

The case of L_2^N. — We now present a result concerning the problem of selection of characters in L_2^N. It is not the most general one but we would like to emphasize the similarity between its proof and the proof of Theorem 5.4.1.

Theorem 5.5.2. — *Let $(\psi_1, \dots, \psi_N)$ be an orthogonal system of L_2^N bounded in L_∞^N i.e. such that for every $i \le N$, $\|\psi_i\|_\infty \le 1$ and $\|\psi_i\|_2 = K$ for a fixed number K. For any $2 \le n \le N-1$, there exists a subset $I \subset [N]$ of cardinality greater than $N-n$ such that for all $(a_i)_{i\in I}$,*

$$\left\|\sum_{i\in I} a_i\psi_i\right\|_2 \le \frac{C}{K}\sqrt{\frac{N}{n}}\sqrt{\log N}(\log n)^{3/2}\left\|\sum_{i\in I} a_i\psi_i\right\|_1.$$

Proof. — Let Y be the random vector defined by $Y = \psi_i$ with probability $1/N$ and let $Y_1, \dots, Y_n$ be independent copies of Y. Observe that $\mathbb{E}\langle Y, y\rangle^2 = K^2\|y\|_2^2/N$ and define

$$Z = \sup_{y\in B_1\cap\rho S_2}\left|\sum_{i=1}^n \langle Y_i, y\rangle^2 - \frac{nK^2\rho^2}{N}\right|.$$

Following the proof of Theorem 5.4.1 (the normalization is different from a factor $\sqrt{N}$), we obtain that if ρ satisfies

$$K\rho \ge C\sqrt{\frac{N(\log n)^3\log N}{n}},$$

then

$$\mathbb{P}\left(Z \ge \frac{1}{3}\frac{nK^2\rho^2}{N}\right) \le C\exp\left(-c\,\frac{n\,K^2\rho^2}{N}\right).$$

Therefore there exists a choice of $Y_1, \dots, Y_n$ (in fact it is with probability greater than $1 - C\exp(-c\,\frac{n\,K^2\rho^2}{N}))$ such that

$$\sup_{y\in B_1\cap\rho S_2}\left|\sum_{i=1}^n \langle Y_i, y\rangle^2 - \frac{nK^2\rho^2}{N}\right| \le \frac{1}{3}\frac{nK^2\rho^2}{N}$$

and if I is defined by $\{\psi_i\}_{i\in I} = \{\psi_1, \dots, \psi_N\} \setminus \{Y_1, \dots, Y_n\}$ then by Proposition 5.5.1 (*iii*) and (*i*), we conclude that $\mathrm{Rad}\,(\mathrm{span}\,\{\psi_i\}_{i\in I} \cap B_1) \le \rho$ and $|I| \ge N - n$. This means that for every $(a_i)_{i\in I}$,

$$\left\|\sum_{i\in I} a_i\psi_i\right\|_2 \le \rho\left\|\sum_{i\in I} a_i\psi_i\right\|_1.$$

□

Remark 5.5.3. — *Theorem 5.4.1 follows easily from Theorem 5.5.2. Indeed, if we write the inequality with the classical ℓ_1^N and ℓ_2^N norms, we get that*

$$\left|\sum_{i\in I} a_i\psi_i\right|_2 \le \frac{C}{K}\sqrt{\frac{\log N}{n}}(\log n)^{3/2}\left|\sum_{i\in I} a_i\psi_i\right|_1$$

which means that $\operatorname{rad}(\ker\Psi \cap B_1^N) \le \frac{C}{K}\sqrt{\frac{\log N}{n}}(\log n)^{3/2}$*. To conclude, use Proposition 5.1.1.*

The general case of $L_2(\mu)$. — We can now state a general result about the selection of characters. It is an extension of (5.3) to the existence of a subset of arbitrary size, with a slightly worse dependence in $\log\log N$.

Theorem 5.5.4. — *Let μ be a probability measure and let $(\psi_1, \ldots, \psi_N)$ be an orthonormal system of $L_2(\mu)$ bounded in $L_\infty(\mu)$ i.e. such that for every $i \le N$, $\|\psi_i\|_\infty \le 1$.*
For any $n \le N-1$, there exists a subset $I \subset [N]$ of cardinality greater than $N-n$ such that for all $(a_i)_{i\in I}$,

$$\left\|\sum_{i\in I} a_i\psi_i\right\|_2 \le C\,\gamma\,(\log\gamma)^{5/2}\left\|\sum_{i\in I} a_i\psi_i\right\|_1$$

where $\gamma = \sqrt{\frac{N}{n}}\sqrt{\log n}$.

Remark 5.5.5. — *(i) If n is proportional to N then $\gamma\,(\log\gamma)^{5/2}$ is of the order of $\sqrt{\log N}\,(\log\log N)^{5/2}$. However, if n is chosen to be a power of N then $\gamma\,(\log\gamma)^{5/2}$ is of the order $\sqrt{\frac{N}{n}}\sqrt{\log n}(\log N)^{5/2}$ which is a worse dependence than in Theorem 5.5.2.*
(ii) Exactly as in Theorem 5.4.1 we could assume that $(\psi_1, \ldots, \psi_N)$ is an orthogonal system of L_2 such that for every $i \le N$, $\|\psi_i\|_2 = K$ and $\|\psi_i\|_\infty \le 1$ for a fixed real number K.

The second main result is an extension of (5.3) to a Kashin type decomposition. Since the method of proof is probabilistic, we are able to find a subset of cardinality close to $N/2$ such that on both I and $\{1, \ldots, N\} \setminus I$, the L_1 and L_2 norms are well comparable.

Theorem 5.5.6. — *With the assumptions of Theorem 5.5.4, if N is an even natural integer, there exists a subset $I \subset [N]$ with $\frac{N}{2} - c\sqrt{N} \le |I| \le \frac{N}{2} + c\sqrt{N}$ such that for all $(a_i)_{i=1}^N$*

$$\left\|\sum_{i\in I} a_i\psi_i\right\|_2 \le C\,\sqrt{\log N}\,(\log\log N)^{5/2}\left\|\sum_{i\in I} a_i\psi_i\right\|_1$$

and

$$\left\|\sum_{i\notin I} a_i\psi_i\right\|_2 \le C\,\sqrt{\log N}\,(\log\log N)^{5/2}\left\|\sum_{i\notin I} a_i\psi_i\right\|_1.$$

For the proof of both theorems, in order to use Theorem 5.3.12 and its Corollary 5.3.13, we replace the unit ball B_1 by a ball which has a good modulus of convexity that is for example B_p for $1 < p \le 2$. We start recalling a classical trick which is often used to compare L_r norms of a measurable function (for example in the theory of thin sets in Harmonic Analysis).

Lemma 5.5.7. — *Let f be a measurable function on a probability space (Ω, μ). For $1 < p < 2$,*

$$\text{if } \ \|f\|_2 \le A\|f\|_p \ \text{ then } \ \|f\|_2 \le A^{\frac{p}{2-p}}\|f\|_1.$$

Proof. — This is just an application of Hölder inequality. Let $\theta \in (0,1)$ such that $1/p = (1-\theta) + \theta/2$ that is $\theta = 2(1-1/p)$. By Hölder,

$$\|f\|_p \le \|f\|_1^{1-\theta}\|f\|_2^{\theta}.$$

Therefore if $\|f\|_2 \le A\|f\|_p$ we deduce that $\|f\|_2 \le A^{\frac{1}{1-\theta}}\|f\|_1$. □

Proposition 5.5.8. — *Under the assumptions of Theorem 5.5.4, the following holds.*

1) For any $p \in (1,2)$ and any $2 \le n \le N-1$ there exists a subset $I \subset \{1,\dots,N\}$ with $|I| \ge N-n$ such that for every $(a_i) \in \mathbb{C}^N$,

$$\Big\|\sum_{i\in I} a_i\psi_i\Big\|_2 \le \frac{C}{(p-1)^{5/2}}\sqrt{N/n}\,\sqrt{\log n}\,\Big\|\sum_{i\in I} a_i\psi_i\Big\|_p.$$

2) Moreover, if N is an even natural integer, there exists a subset $I \subset \{1,\dots,N\}$ with $N/2 - c\sqrt{N} \le |I| \le N/2 + c\sqrt{N}$ such that for every $a = (a_i) \in \mathbb{C}^N$,

$$\Big\|\sum_{i\in I} a_i\psi_i\Big\|_2 \le \frac{C}{(p-1)^{5/2}}\sqrt{N/n}\,\sqrt{\log n}\,\Big\|\sum_{i\in I} a_i\psi_i\Big\|_p$$

and

$$\Big\|\sum_{i\notin I} a_i\varphi_i\Big\|_2 \le \frac{C}{(p-1)^{5/2}}\sqrt{N/n}\,\sqrt{\log n}\,\Big\|\sum_{i\notin I} a_i\psi_i\Big\|_p.$$

Proof of Theorem 5.5.4 and Theorem 5.5.6. — We combine the first part of Proposition 5.5.8 with Lemma 5.5.7. Indeed, let $\gamma = \sqrt{N/n}\,\sqrt{\log n}$ and choose $p = 1 + 1/\log\gamma$. Using Proposition 5.5.8, there is a subset I of cardinality greater than $N-n$ for which

$$\forall (a_i)_{i\in I}, \quad \Big\|\sum_{i\in I} a_i\psi_i\Big\|_2 \le C_p\,\gamma\,\Big\|\sum_{i\in I} a_i\psi_i\Big\|_p$$

where $C_p = C/(p-1)^{5/2}$. By the choice of p and Lemma 5.5.7,

$$\Big\|\sum_{i\in I} a_i\psi_i\Big\|_2 \le \gamma\, C_p^{p/(2-p)}\gamma^{2(p-1)/(2-p)}\Big\|\sum_{i\in I} a_i\psi_i\Big\|_1 \le C\,\gamma\,(\log\gamma)^{5/2}\Big\|\sum_{i\in I} a_i\psi_i\Big\|_1.$$

The same argument works for the Theorem 5.5.6 using the second part of Proposition 5.5.8. □

It remains to prove Proposition 5.5.8.

Proof. — Let Y be the random vector defined by $Y = \psi_i$ with probability $1/N$ and let $Y_1, \ldots, Y_n$ be independent copies of Y. Observe that for any $y \in L_2(\mu)$, $\mathbb{E}\langle Y, y\rangle^2 = \|y\|_2^2/N$. Let $E = \operatorname{span}\{\psi_1, \ldots, \psi_N\}$ and for $\rho > 0$ let E_p be the vector space E endowed with the norm defined by

$$\|y\| = \left(\frac{\|y\|_p^2 + \rho^{-2}\|y\|_2^2}{2}\right)^{1/2}.$$

We restrict our study to the vector space E and it is clear that

$$(B_p \cap \rho B_2) \subset B_{E_p} \subset \sqrt{2}(B_p \cap \rho B_2) \tag{5.12}$$

where B_{E_p} is the unit ball of E_p. Moreover, by Clarkson inequality, for any $f, g \in L_p$,

$$\left\|\frac{f+g}{2}\right\|_p^2 + \frac{p(p-1)}{8}\left\|\frac{f-g}{2}\right\|_p^2 \leq \frac{1}{2}(\|f\|_p^2 + \|g\|_p^2).$$

It is easy to deduce that E_p has modulus of convexity of power type 2 with constant λ such that $\lambda^{-2} = p(p-1)/8$.

Define the random variable

$$Z = \sup_{y \in B_p \cap \rho S_2}\left|\sum_{i=1}^n \langle Y_i, y\rangle^2 - \frac{n\rho^2}{N}\right|.$$

We deduce from (5.12) that

$$\mathbb{E}Z \leq \mathbb{E}\sup_{y \in B_{E_p}}\left|\sum_{i=1}^n \langle Y_i, y\rangle^2 - \mathbb{E}\langle Y_i, y\rangle^2\right|.$$

From (5.12), we have

$$\sigma^2 = \sup_{y \in B_{E_p}} n\|y\|_2^2/N \leq 2n\rho^2/N$$

and for every $i \leq N$, $\|\psi_i\|_{E_p^\star} \leq \sqrt{2}\|\psi_i\|_\infty \leq \sqrt{2}$. By Corollary 5.3.13, we get

$$\mathbb{E}\sup_{y \in B_{E_p}}\left|\sum_{i=1}^n \langle Y_i, y\rangle^2 - \mathbb{E}\langle Y_i, y\rangle^2\right| \leq C\max\left(\lambda^{10}\log n, \rho\lambda^5\sqrt{\frac{n\log n}{N}}\right).$$

We conclude that

$$\text{if} \quad \rho \geq C\lambda^5\sqrt{\frac{N\log n}{n}}, \quad \text{then} \quad \mathbb{E}Z \leq \frac{1}{3}\frac{n\rho^2}{N}$$

and using Proposition 5.1.2 we get

$$\operatorname{Rad}(\ker\Psi \cap B_p) < \rho$$

where $\Psi = \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix}$. We choose $\rho = C\lambda^5\sqrt{\frac{N\,\log n}{n}}$ and deduce from Proposition 5.5.1 (iii) and (i) that for I defined by $\{\psi_i\}_{i\in I} = \{\psi_1,\dots,\psi_N\} \setminus \{Y_1,\dots,Y_n\}$, we have

$$\forall (a_i)_{i\in I}, \qquad \left\|\sum_{i\in I} a_i\psi_i\right\|_2 \le \rho \left\|\sum_{i\in I} a_i\psi_i\right\|_p .$$

This ends the proof of the first part.

For the second part, we add the following observation. By a combinatorial argument, it is not difficult to prove that if $n = [\delta N]$ with $\delta = \log 2 < 3/4$, then with probability greater than $3/4$,

$$N/2 - c\sqrt{N} \le |I| = N - |\{Y_1,\dots,Y_n\}| \le N/2 + c\sqrt{N},$$

for some absolute constant $c > 0$. Hence $n < 3N/4$ and we can also use part (iv) of Proposition 5.5.1 which proves that

$$\mathrm{Rad}\,(\ker\Psi \cap B_p) \le \rho \quad \text{and} \quad \mathrm{Rad}\,((\ker\Psi)^\perp \cap B_p) \le \rho.$$

Since $\ker\Psi = \mathrm{span}\,\{\psi_i\}_{i\in I}$ and $(\ker\Psi)^\perp = \mathrm{span}\,\{\psi_i\}_{i\notin I}$, this ends the proof of the Proposition. □

5.6. Notes and comments

For the study of the supremum of an empirical process and the connection with Rademacher averages, we already referred to chapter 4 of [**LT91**]. Theorem 5.3.1 is due to Talagrand and can be found in theorem 4.12 in [**LT91**]. Theorem 5.3.2 is often called a "symmetrization principle". This strategy was already used by Kahane in [**Kah68**] for studying random series on Banach spaces. It was pushed forward by Giné and Zinn in [**GZ84**] for studying limit theorem for empirical processes. The concentration inequality, Theorem 5.3.4, is due to Talagrand [**Tal96b**]. Several improvements and simplifications are known, in particular in the case of independent identically distributed random variables. We refer to [**Rio02, Bou03, Kle02, KR05**] for more precise results. Proposition 5.3.5 is taken from [**Mas00**].

Theorem 5.3.6 is due to Rudelson [**Rud99**]. The proof that we presented was suggested by Pisier to Rudelson. It used a refined version of non-commutative Khinchine inequality that can be found in [**LP86, LPP91, Pis98**]. Explicit constants for the non-commutative Khinchine inequality are derived in [**Buc01**]. There is presently a more modern way of proving Theorem 5.3.6, using non-commutative Bernstein inequalities [**Tro12**]. However, all the known proofs are based on an expression related to operator norms and we have seen that in other situations, we need an estimate of the supremum of some empirical processes which can not be expressed in terms of operator norms. The original proof of Rudelson [**Rud96**] uses the majorizing measure theory. Some improvements of this result are proved in [**GR07**] and in [**GMPTJ08**]. The proof of Theorem 5.3.12 can be found in [**GMPTJ08**] and it is based on the same type of construction of majorizing measures as in [**GR07**] and on deep results about the duality of covering numbers [**BPSTJ89**]. The notions of type and cotype of a Banach space are important in this study and we refer the interested reader to [**Mau03**]. The notions of modulus of convexity and smoothness of a Banach space are classical and we refer the interested reader to [**LT79, Pis75**].

Theorem 5.3.14 comes from [**GMPTJ07**]. It was used to study the problem of selection of characters like Theorem 5.5.2. As we have seen, the proof is very similar to the proof of Theorem 5.4.1 and this result is due to Rudelson and Vershynin [**RV08b**]. They improved a result due to Candès and Tao [**CT05**] and their strategy was to study the RIP condition instead of the size of the radius of sections of B_1^N. Moreover, the probabilistic estimate is slightly better than in [**RV08b**] and was shown to us by Holger Rauhut [**Rau10**]. We refer to [**Rau10, FR10**] for a deeper presentation of the problem of compressed sensing and for some other points of view. We refer also to [**KT07**] where connections between the Compressed Sensing problem and the problem of estimating the Kolmogorov widhts are discussed and to [**CDD09, KT07**] for the study of approximate reconstruction.

For the classical study of local theory of Banach spaces, see [**MS86**] and [**Pis89**]. Euclidean sections or projections of a convex body are studied in detail in [**FLM77**] and the Kashin decomposition can be found in [**Kas77**]. About the question of selection of characters, see the paper of Bourgain [**Bou89**] where it is proved for $p > 2$ the existence of $\Lambda(p)$ sets which are not $\Lambda(r)$ for $r > p$. This problem was related to the theory of majorizing measure in [**Tal95**]. The existence of a subset of a bounded orthonormal system satisfying inequality (5.3) is proved by Talagrand in [**Tal98**]. Theorems 5.5.4 and 5.5.6 are taken from [**GMPTJ08**] where it is also shown that the factor $\sqrt{\log N}$ is necessary in the estimate.

NOTATIONS

- The sets of numbers are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
- For all $x \in \mathbb{R}^N$ and $p > 0$,

$$|x|_p = (|x_1|^p + \cdots + |x_N|^p)^{1/p} \quad \text{and} \quad |x|_\infty = \max_{1 \leqslant i \leqslant N} |x_i|$$

- $B_p^N = \{x \in \mathbb{R}^N : |x|_p \leq 1\}$
- Scalar product $\langle x, y \rangle$ and $x \perp y$ means $\langle x, y \rangle = 0$
- $A^* = \bar{A}^\top$ is the conjugate transpose of the matrix A
- $s_1(A) \geqslant \cdots \geqslant s_n(A)$ are the singular values of the $n \times N$ matrix A where $n \leqslant N$
- $\|A\|_{2\to 2}$ is the operator norm of A ($\ell^2 \to \ell^2$)
- $\|A\|_{\mathrm{HS}}$ is the Hilbert-Schmidt norm of A
- $e_1, \ldots, e_n$ is the canonical basis of $\mathbb{R}^n$
- $\stackrel{d}{=}$ stands for the equality in distribution
- $\stackrel{d}{\to}$ stands for the convergence in distribution
- $\stackrel{w}{\to}$ stands for weak convergence of measures
- $\mathcal{M}_{m,n}(K)$ are the $m \times n$ matrices with entries in K, and $\mathcal{M}_n(K) = \mathcal{M}_{n,n}(K)$
- I is the identity matrix
- $x \wedge y = \min(x, y)$ and $x \vee y = \max(x, y)$
- $[N] = \{1, \ldots, N\}$
- E^c is the complement of a subset E
- $|S|$ cardinal of the set S
- $\mathrm{dist}_2(x, E) = \inf_{y \in E} |x - y|_2$
- $\mathrm{supp}\, x$ is the subset of non-zero coordinates of x
- The vector x is said to be m-sparse if $|\mathrm{supp}\, x| \leq m$.
- $\Sigma_m = \Sigma_m(\mathbb{R}^N)$ is the subset of m-sparse vectors of $\mathbb{R}^N$
- $S_p(\Sigma_m) = \{x \in \mathbb{R}^N : |x|_p = 1, |\mathrm{supp}\, x| \leq m\}$
- $B_p(\Sigma_m) = \{x \in \mathbb{R}^N : |x|_p \leq 1, |\mathrm{supp}\, x| \leq m\}$
- $B_{p,\infty}^N = \left\{x \in \mathbb{R}^N : |\{i : |x_i| \geq s\}| \leq s^{-p} \text{ for all } \ s > 0\right\}$
- $\mathrm{conv}(E)$ is the convex hull of E
- $\mathrm{Aff}(E)$ is the affine hull of E

- $\mathrm{rad}(F, \|\cdot\|) = \sup\{\|x\| : x \in F\}$
- For a random variable Z and any $\alpha \geqslant 1$, $\|Z\|_{\psi_\alpha} = \inf\{s > 0 \,:\, \mathbb{E}\exp\left(|Z|/s\right)^\alpha \leqslant e\}$
- $\ell_*(T) = \mathbb{E}\sup_{t\in T}\sum_{i=1}^N g_i t_i$

BIBLIOGRAPHY

[ALPTJ10] R. Adamczak, A. E. Litvak, A. Pajor & N. Tomczak-Jaegermann – "Quantitative estimates of the convergence of the empirical covariance matrix in log-concave ensembles", *J. Amer. Math. Soc.* **23** (2010), no. 2, p. 535–561.

[ALPTJ11] R. Adamczak, A. E. Litvak, A. Pajor & N. Tomczak-Jaegermann – "Restricted isometry property of matrices with independent columns and neighborly polytopes by random sampling", *Constructive Approximation* **34** (2011), no. 1, p. 61–88.

[BB98] M. Bertero & P. Boccacci – *Introduction to inverse problems in imaging*, Institute of Physics Publishing, Bristol, 1998.

[BBL04] S. Boucheron, O. Bousquet & G. Lugosi – "Concentration inequalities", in *Advanced Lectures in Machine Learning*, Lecture Notes in Comput. Sci., vol. 3176, Springer, Berlin, 2004, p. 208–240.

[BC12] C. Bordenave & D. Chafaï – "Around the circular law", *Probability Surveys* **9** (2012), p. 1–89.

[BDDW08] R. Baraniuk, M. Davenport, R. DeVore & M. Wakin – "A simple proof of the restricted isometry property for random matrices", *Constr. Approx.* **28** (2008), no. 3, p. 253–263.

[Bha97] R. Bhatia – *Matrix analysis*, Graduate Texts in Mathematics, vol. 169, Springer-Verlag, New York, 1997.

[Bou89] J. Bourgain – "Bounded orthogonal systems and the $\Lambda(p)$-set problem", *Acta Math.* **162** (1989), no. 3-4, p. 227–245.

[Bou03] O. Bousquet – "Concentration inequalities for sub-additive functions using the entropy method", in *Stochastic inequalities and applications*, Progr. Probab., vol. 56, Birkhäuser, Basel, 2003, p. 213–247.

[BPSTJ89] J. Bourgain, A. Pajor, S. J. Szarek & N. Tomczak-Jaegermann – "On the duality problem for entropy numbers of operators", in *Geometric aspects of functional analysis (1987–88)*, Lecture Notes in Math., vol. 1376, Springer, Berlin, 1989, p. 50–63.

[BS10] Z. Bai & J. W. Silverstein – *Spectral analysis of large dimensional random matrices*, second ed., Springer Series in Statistics, Springer, New York, 2010.

[Buc01] A. Buchholz – "Operator Khintchine inequality in non-commutative probability", *Math. Ann.* **319** (2001), no. 1, p. 1–16.

[BY93] Z. D. Bai & Y. Q. Yin – "Limit of the smallest eigenvalue of a large-dimensional sample covariance matrix", *Ann. Probab.* **21** (1993), no. 3, p. 1275–1294.

[Can08] E. J. Candès – "The restricted isometry property and its implications for compressed sensing", *C. R. Math. Acad. Sci. Paris* **346** (2008), no. 9-10, p. 589–592.

[Car85] B. Carl – "Inequalities of Bernstein-Jackson-type and the degree of compactness of operators in Banach spaces", *Ann. Inst. Fourier (Grenoble)* **35** (1985), no. 3, p. 79–118.

[CDD09] A. Cohen, W. Dahmen & R. DeVore – "Compressed sensing and best k-term approximation", *J. Amer. Math. Soc.* **22** (2009), no. 1, p. 211–231.

[CG05] M. T. Chu & G. H. Golub – *Inverse eigenvalue problems: theory, algorithms, and applications*, Numerical Mathematics and Scientific Computation, Oxford University Press, New York, 2005.

[CIS76] B. S. Cirel′son, I. A. Ibragimov & V. N. Sudakov – "Norms of Gaussian sample functions", in *Proceedings of the Third Japan-USSR Symposium on Probability Theory (Tashkent, 1975)* (Berlin), Springer, 1976, p. 20–41. Lecture Notes in Math., Vol. 550.

[CRT06] E. J. Candès, J. K. Romberg & T. Tao – "Stable signal recovery from incomplete and inaccurate measurements", *Comm. Pure Appl. Math.* **59** (2006), no. 8, p. 1207–1223.

[CS90] B. Carl & I. Stephani – *Entropy, compactness and the approximation of operators*, Cambridge Tracts in Mathematics, vol. 98, Cambridge University Press, Cambridge, 1990.

[CT05] E. J. Candes & T. Tao – "Decoding by linear programming", *IEEE Trans. Inform. Theory* **51** (2005), no. 12, p. 4203–4215.

[CT06] ———, "Near-optimal signal recovery from random projections: universal encoding strategies?", *IEEE Trans. Inform. Theory* **52** (2006), no. 12, p. 5406–5425.

[DE02] I. Dumitriu & A. Edelman – "Matrix models for beta ensembles", *J. Math. Phys.* **43** (2002), no. 11, p. 5830–5847.

[DMS93] S. J. Dilworth & S. J. Montgomery-Smith – "The distribution of vector-valued Rademacher series", *Ann. Probab.* **21** (1993), no. 4, p. 2046–2052.

[Don05] D. L. Donoho – "Neighborly polytopes and sparse solutions of underdetermined linear equations", Department of Statistics, Stanford University, 2005.

[Don06] ———, "Compressed sensing", *IEEE Trans. Inform. Theory* **52** (2006), no. 4, p. 1289–1306.

[DS01] K. R. Davidson & S. J. Szarek – "Local operator theory, random matrices and Banach spaces", in *Handbook of the geometry of Banach spaces, Vol. I*, North-Holland, Amsterdam, 2001, p. 317–366.

[Dud67] R. M. Dudley – "The sizes of compact subsets of Hilbert space and continuity of Gaussian processes", *J. Functional Analysis* **1** (1967), p. 290–330.

[Ede89] A. Edelman – "Eigenvalues and condition numbers of random matrices", Ph.D. Thesis, MIT, 1989.

[ER05] A. Edelman & N. R. Rao – "Random matrix theory", *Acta Numer.* **14** (2005), p. 233–297.

[EY39] C. Eckart & G. Young – "A principal axis transformation for non-hermitian matrices", *Bull. Amer. Math. Soc.* **45** (1939), no. 2, p. 118–121.

[Fel71] W. Feller – *An introduction to probability theory and its applications. Vol. II.*, Second edition, John Wiley & Sons Inc., New York, 1971.

[Fer74] X. Fernique – "Des résultats nouveaux sur les processus gaussiens", *C. R. Acad. Sci. Paris Sér. A* **278** (1974), p. 363–365.

[Fer75] X. Fernique – "Regularité des trajectoires des fonctions aléatoires gaussiennes", in *École d'Été de Probabilités de Saint-Flour, IV-1974*, Springer, Berlin, 1975, p. 1–96. Lecture Notes in Math., Vol. 480.

[FL09] S. Foucart & M.-J. Li – "Sparsest solutions of underdetermined linear systems via ℓ_q-minimization for $0 < q \leq 1$", *Applied and Computational Harmonic Analysis* **26** (2009), no. 3, p. 395–407.

[FLM77] T. Figiel, J. Lindenstrauss & V. D. Milman – "The dimension of almost spherical sections of convex bodies", *Acta Math.* **139** (1977), no. 1-2, p. 53–94.

[For10] P. J. Forrester – *Log-gases and random matrices*, London Mathematical Society Monographs Series, vol. 34, Princeton University Press, Princeton, NJ, 2010.

[FPRU11] S. Foucart, A. Pajor, H. Rauhut & T. Ullrich – "The gelfand widths of ℓ_p-balls for $0 < p \leq 1$", *Journal of Complexity* **26** (2011), no. 6, p. 629–640.

[FR10] M. Fornasier & H. Rauhut – "Compressive Sensing - An Introduction", in *Handbook of Mathematical Methods in Imaging* (O. Scherzer, ed.), Springer, 2010.

[FR11] S. Foucart & O. Rauhut – *A mathematical introduction to compressive sensing*, Appl. Numer. Harmon. Anal., Birkhaäuser, Boston, New York, 2011, In preparation.

[Fre03] I. Fredholm – "Sur une classe d'équations fonctionnelles", *Acta Math.* **27** (1903), no. 1, p. 365–390.

[Gel41] I. Gelfand – "Normierte Ringe", *Rec. Math. [Mat. Sbornik] N. S.* **9 (51)** (1941), p. 3–24.

[GG84] A. Y. Garnaev & E. D. Gluskin – "The widths of a Euclidean ball", *Dokl. Akad. Nauk SSSR* **277** (1984), no. 5, p. 1048–1052.

[Gir75] V. L. Girko – *Sluchainye matritsy*, Izdat. Ob. ed. "Visca Skola" pri Kiev. Gosudarstv. Univ., Kiev, 1975.

[GK95] E. D. Gluskin & S. Kwapień – "Tail and moment estimates for sums of independent random variables with logarithmically concave tails", *Studia Math.* **114** (1995), no. 3, p. 303–309.

[GL09] A. Guntuboyina & H. Leeb – "Concentration of the spectral measure of large Wishart matrices with dependent entries", *Electron. Commun. Probab.* **14** (2009), p. 334–342.

[Glu83] E. D. Gluskin – "Norms of random matrices and diameters of finite-dimensional sets", *Mat. Sb. (N.S.)* **120(162)** (1983), no. 2, p. 180–189, 286.

[GMPTJ07] O. Guédon, S. Mendelson, A. Pajor & N. Tomczak-Jaegermann – "Subspaces and orthogonal decompositions generated by bounded orthogonal systems", *Positivity* **11** (2007), no. 2, p. 269–283.

[GMPTJ08] ______, "Majorizing measures and proportional subsets of bounded orthonormal systems", *Rev. Mat. Iberoam.* **24** (2008), no. 3, p. 1075–1095.

[Gor85] Y. Gordon – "Some inequalities for Gaussian processes and applications", *Israel J. Math.* **50** (1985), no. 4, p. 265–289.

[Gor87] ______, "Elliptically contoured distributions", *Probab. Theory Related Fields* **76** (1987), no. 4, p. 429–438.

[GR07] O. Guédon & M. Rudelson – "L_p-moments of random vectors via majorizing measures", *Adv. Math.* **208** (2007), no. 2, p. 798–823.

[GVL96] G. H. Golub & C. F. Van Loan – *Matrix computations*, third ed., Johns Hopkins Studies in the Mathematical Sciences, Johns Hopkins University Press, Baltimore, MD, 1996.

[GZ84] E. Giné & J. Zinn – "Some limit theorems for empirical processes", *Ann. Probab.* **12** (1984), no. 4, p. 929–998, With discussion.

[HJ90] R. A. Horn & C. R. Johnson – *Matrix analysis*, Cambridge University Press, Cambridge, 1990, Corrected reprint of the 1985 original.

[HJ94] ______, *Topics in matrix analysis*, Cambridge University Press, Cambridge, 1994, Corrected reprint of the 1991 original.

[Hoe63] W. Hoeffding – "Probability inequalities for sums of bounded random variables", *J. Amer. Statist. Assoc.* **58** (1963), p. 13–30.

[Hor54] A. Horn – "On the eigenvalues of a matrix with prescribed singular values", *Proc. Amer. Math. Soc.* **5** (1954), p. 4–7.

[HT03] U. Haagerup & S. Thorbjørnsen – "Random matrices with complex Gaussian entries", *Expo. Math.* **21** (2003), no. 4, p. 293–337.

[HW53] A. J. Hoffman & H. W. Wielandt – "The variation of the spectrum of a normal matrix", *Duke Math. J.* **20** (1953), p. 37–39.

[Jam60] A. T. James – "The distribution of the latent roots of the covariance matrix", *Ann. Math. Statist.* **31** (1960), p. 151–158.

[JL84] W. B. Johnson & J. Lindenstrauss – "Extensions of Lipschitz mappings into a Hilbert space", in *Conference in modern analysis and probability (New Haven, Conn., 1982)*, Contemp. Math., vol. 26, Amer. Math. Soc., Providence, RI, 1984, p. 189–206.

[Jol02] I. T. Jolliffe – *Principal component analysis*, second ed., Springer Series in Statistics, Springer-Verlag, New York, 2002.

[Kah68] J.-P. Kahane – *Some random series of functions*, D. C. Heath and Co. Raytheon Education Co., Lexington, Mass., 1968.

[Kas77] B. S. Kashin – "The widths of certain finite-dimensional sets and classes of smooth functions", *Izv. Akad. Nauk SSSR Ser. Mat.* **41** (1977), no. 2, p. 334–351, 478.

[Kle02] T. Klein – "Une inégalité de concentration à gauche pour les processus empiriques", *C. R. Math. Acad. Sci. Paris* **334** (2002), no. 6, p. 501–504.

[Kôn80] N. Kôno – "Sample path properties of stochastic processes", *J. Math. Kyoto Univ.* **20** (1980), no. 2, p. 295–313.

[KR61] M. A. Krasnosel′skiĭ & J. B. Rutickiĭ – *Convex functions and Orlicz spaces*, Translated from the first Russian edition by Leo F. Boron, P. Noordhoff Ltd., Groningen, 1961.

[KR05] T. Klein & E. Rio – "Concentration around the mean for maxima of empirical processes", *Ann. Probab.* **33** (2005), no. 3, p. 1060–1077.

[KT07] B. S. Kashin & V. N. Temlyakov – "A remark on the problem of compressed sensing", *Mat. Zametki* **82** (2007), no. 6, p. 829–837.

[Led01] M. Ledoux – *The concentration of measure phenomenon*, Mathematical Surveys and Monographs, vol. 89, American Mathematical Society, Providence, RI, 2001.

[Led04] M. Ledoux – "Differential operators and spectral distributions of invariant ensembles from the classical orthogonal polynomials. The continuous case", *Electron. J. Probab.* **9** (2004), p. no. 7, 177–208 (electronic).

[LN06] N. Linial & I. Novik – "How neighborly can a centrally symmetric polytope be?", *Discrete Comput. Geom.* **36** (2006), no. 2, p. 273–281.

[LP86] F. Lust-Piquard – "Inégalités de Khintchine dans C_p $(1 < p < \infty)$", *C. R. Acad. Sci. Paris Sér. I Math.* **303** (1986), no. 7, p. 289–292.

[LPP91] F. Lust-Piquard & G. Pisier – "Noncommutative Khintchine and Paley inequalities", *Ark. Mat.* **29** (1991), no. 2, p. 241–260.

[LT77] J. Lindenstrauss & L. Tzafriri – *Classical Banach spaces. I*, Springer-Verlag, Berlin, 1977, Sequence spaces, Ergebnisse der Mathematik und ihrer Grenzgebiete, Vol. 92.

[LT79] ———, *Classical Banach spaces. II*, Ergebnisse der Mathematik und ihrer Grenzgebiete [Results in Mathematics and Related Areas], vol. 97, Springer-Verlag, Berlin, 1979, Function spaces.

[LT91] M. Ledoux & M. Talagrand – *Probability in Banach spaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 23, Springer-Verlag, Berlin, 1991, Isoperimetry and processes.

[Mas00] P. Massart – "About the constants in Talagrand's concentration inequalities for empirical processes", *Ann. Probab.* **28** (2000), no. 2, p. 863–884.

[Mas07] ———, *Concentration inequalities and model selection*, Lecture Notes in Mathematics, vol. 1896, Springer, Berlin, 2007, Lectures from the 33rd Summer School on Probability Theory held in Saint-Flour, July 6–23, 2003, With a foreword by Jean Picard.

[Mau03] B. Maurey – "Type, cotype and K-convexity", in *Handbook of the geometry of Banach spaces, Vol. 2*, North-Holland, Amsterdam, 2003, p. 1299–1332.

[McD89] C. McDiarmid – "On the method of bounded differences", in *Surveys in combinatorics, 1989 (Norwich, 1989)*, London Math. Soc. Lecture Note Ser., vol. 141, Cambridge Univ. Press, Cambridge, 1989, p. 148–188.

[Mil86] V. D. Milman – "Random subspaces of proportional dimension of finite-dimensional normed spaces; approach through the isoperimetric inequality", in

Séminaire d'Analyse Fonctionelle 1984/1985, Publ. Math. Univ. Paris VII, vol. 26, Univ. Paris VII, Paris, 1986, p. 19–29.

[Moo20] E. H. Moore – "On the reciprocal of the general algebraic matrix", *Bulletin of the American Mathematical Society* **26** (1920), p. 394–395.

[MP67] V. A. Marchenko & L. A. Pastur – "Distribution of eigenvalues in certain sets of random matrices", *Mat. Sb. (N.S.)* **72 (114)** (1967), p. 507–536.

[MP06] S. Mendelson & A. Pajor – "On singular values of matrices with independent rows", *Bernoulli* **12** (2006), no. 5, p. 761–773.

[MPTJ07] S. Mendelson, A. Pajor & N. Tomczak-Jaegermann – "Reconstruction and subgaussian operators in asymptotic geometric analysis", *Geom. Funct. Anal.* **17** (2007), no. 4, p. 1248–1282.

[MPTJ08] ———, "Uniform uncertainty principle for Bernoulli and subgaussian ensembles", *Constr. Approx.* **28** (2008), no. 3, p. 277–289.

[MS86] V. D. Milman & G. Schechtman – *Asymptotic theory of finite-dimensional normed spaces*, Lecture Notes in Mathematics, vol. 1200, Springer-Verlag, Berlin, 1986, With an appendix by M. Gromov.

[MS90] S. J. Montgomery-Smith – "The distribution of Rademacher sums", *Proc. Amer. Math. Soc.* **109** (1990), no. 2, p. 517–522.

[MS95] ———, "The distribution of non-commutative Rademacher series", *Math. Ann.* **302** (1995), no. 3, p. 395–416.

[Mui82] R. J. Muirhead – *Aspects of multivariate statistical theory*, John Wiley & Sons Inc., New York, 1982, Wiley Series in Probability and Mathematical Statistics.

[Paj99] A. Pajor – "Metric entropy of the Grassmann manifold", in *Convex geometric analysis (Berkeley, CA, 1996)*, Math. Sci. Res. Inst. Publ., vol. 34, Cambridge Univ. Press, Cambridge, 1999, p. 181–188.

[Pas99] L. Pastur – "A simple approach to global regime of random matrix theory", in *Mathematical results in statistical mechanics (Marseilles, 1998)*, World Sci. Publ., River Edge, NJ, 1999, p. 429–454.

[Pen56] R. Penrose – "On best approximation solutions of linear matrix equations", *Proc. Cambridge Philos. Soc.* **52** (1956), p. 17–19.

[Pie72] A. Pietsch – *Theorie der Operatorenideale (Zusammenfassung)*, Friedrich-Schiller-Universität, Jena, 1972, Wissenschaftliche Beiträge der Friedrich-Schiller-Universität Jena.

[Pie80] ———, *Operator ideals*, North-Holland Mathematical Library, vol. 20, North-Holland Publishing Co., Amsterdam, 1980, Translated from German by the author.

[Pis75] G. Pisier – "Martingales with values in uniformly convex spaces", *Israel J. Math.* **20** (1975), no. 3-4, p. 326–350.

[Pis80] G. Pisier – "Conditions d'entropie assurant la continuité de certains processus et applications à l'analyse harmonique", in *Seminar on Functional Analysis, 1979–1980 (French)*, École Polytech., Palaiseau, 1980, p. Exp. No. 13–14, 43.

[Pis81] ______, "Remarques sur un résultat non publié de B. Maurey", in *Seminar on Functional Analysis, 1980–1981*, École Polytech., Palaiseau, 1981, p. Exp. No. V, 13.

[Pis86] G. Pisier – "Probabilistic methods in the geometry of Banach spaces", in *Probability and analysis (Varenna, 1985)*, Lecture Notes in Math., vol. 1206, Springer, Berlin, 1986, p. 167–241.

[Pis89] ______, *The volume of convex bodies and Banach space geometry*, Cambridge Tracts in Mathematics, vol. 94, Cambridge University Press, Cambridge, 1989.

[Pis98] ______, "Non-commutative vector valued L_p-spaces and completely p-summing maps", *Astérisque* (1998), no. 247, p. vi+131.

[PP09] A. Pajor & L. Pastur – "On the limiting empirical measure of eigenvalues of the sum of rank one matrices with log-concave distribution", *Studia Math.* **195** (2009), no. 1, p. 11–29.

[PS11] L. Pastur & M. Shcherbina – *Eigenvalue Distribution of Large Random Matrices*, American Mathematical Society, 2011.

[PTJ86] A. Pajor & N. Tomczak-Jaegermann – "Subspaces of small codimension of finite-dimensional Banach spaces", *Proc. Amer. Math. Soc.* **97** (1986), no. 4, p. 637–642.

[Rau10] H. Rauhut – "Compressive sensing and structured random matrices", in *Theoretical Foundations and Numerical Methods for Sparse Recovery* (R. S. C. A. Math., ed.), deGruyter, 2010.

[Rio02] E. Rio – "Une inégalité de Bennett pour les maxima de processus empiriques", *Ann. Inst. H. Poincaré Probab. Statist.* **38** (2002), no. 6, p. 1053–1057, En l'honneur de J. Bretagnolle, D. Dacunha-Castelle, I. Ibragimov.

[RR91] M. M. Rao & Z. D. Ren – *Theory of Orlicz spaces*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 146, Marcel Dekker Inc., New York, 1991.

[RR02] ______, *Applications of Orlicz spaces*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 250, Marcel Dekker Inc., New York, 2002.

[Rud96] M. Rudelson – "Random vectors in the isotropic position", preprint link, 1996.

[Rud99] ______, "Random vectors in the isotropic position", *J. Funct. Anal.* **164** (1999), no. 1, p. 60–72.

[RV08a] M. Rudelson & R. Vershynin – "The Littlewood-Offord problem and invertibility of random matrices", *Adv. Math.* **218** (2008), no. 2, p. 600–633.

[RV08b] ______, "On sparse reconstruction from Fourier and Gaussian measurements", *Comm. Pure Appl. Math.* **61** (2008), no. 8, p. 1025–1045.

[Sil85] J. W. Silverstein – "The smallest eigenvalue of a large-dimensional Wishart matrix", *Ann. Probab.* **13** (1985), no. 4, p. 1364–1368.

[Sle62] D. Slepian – "The one-sided barrier problem for Gaussian noise", *Bell System Tech. J.* **41** (1962), p. 463–501.

[Sud71] V. N. Sudakov – "Gaussian random processes, and measures of solid angles in Hilbert space", *Dokl. Akad. Nauk SSSR* **197** (1971), p. 43–45.

[Tal87] M. Talagrand – "Regularity of Gaussian processes", *Acta Math.* **159** (1987), no. 1-2, p. 99–149.

[Tal94] ______, "The supremum of some canonical processes", *Amer. J. Math.* **116** (1994), no. 2, p. 283–325.

[Tal95] ______, "Sections of smooth convex bodies via majorizing measures", *Acta Math.* **175** (1995), no. 2, p. 273–300.

[Tal96a] ______, "Majorizing measures: the generic chaining", *Ann. Probab.* **24** (1996), no. 3, p. 1049–1103.

[Tal96b] ______, "New concentration inequalities in product spaces", *Invent. Math.* **126** (1996), no. 3, p. 505–563.

[Tal98] ______, "Selecting a proportion of characters", *Israel J. Math.* **108** (1998), p. 173–191.

[Tal01] ______, "Majorizing measures without measures", *Ann. Probab.* **29** (2001), no. 1, p. 411–417.

[Tal05] ______, *The generic chaining*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005, Upper and lower bounds of stochastic processes.

[Tar05] A. Tarantola – *Inverse problem theory and methods for model parameter estimation*, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2005.

[TE05] L. N. Trefethen & M. Embree – *Spectra and pseudospectra*, Princeton University Press, Princeton, NJ, 2005, The behavior of nonnormal matrices and operators.

[Tik43] A. N. Tikhonov – "On the stability of inverse problems", *C. R. (Doklady) Acad. Sci. URSS (N.S.)* **39** (1943), p. 176–179.

[Tro84] H. F. Trotter – "Eigenvalue distributions of large Hermitian matrices; Wigner's semicircle law and a theorem of Kac, Murdock, and Szegő", *Adv. in Math.* **54** (1984), no. 1, p. 67–82.

[Tro12] J. Tropp – "User-friendly tail bounds for sums of random matrices", *Found. Comput. Math* (2012).

[TV10] T. Tao & V. Vu – "Random matrices: Universality of ESDs and the circular law", *Annals of Probability* **38** (2010), no. 5, p. 2023–2065.

[vdVW96] A. W. van der Vaart & J. A. Wellner – *Weak convergence and empirical processes*, Springer Series in Statistics, Springer-Verlag, New York, 1996, With applications to statistics.

[Ver12] R. Vershynin – "Compressed sensing, theory and applications – introduction to the non-asymptotic analysis of random matrices", ch. 5, p. 210–268, Cambridge University Press, 2012.

[vNG47] J. von Neumann & H. H. Goldstine – "Numerical inverting of matrices of high order", *Bull. Amer. Math. Soc.* **53** (1947), p. 1021–1099.

[Wey49] H. Weyl – "Inequalities between the two kinds of eigenvalues of a linear transformation", *Proc. Nat. Acad. Sci. U. S. A.* **35** (1949), p. 408–411.

[Wis28] J. Wishart – "The generalized product moment distribution in samples from a normal multivariate population", *Biometrika* **20** (1928), no. A, p. 32–52.

[Zha02] X. Zhan – *Matrix inequalities*, Lecture Notes in Mathematics, vol. 1790, Springer-Verlag, Berlin, 2002.

INDEX