ON THE REDUCTION OF A RANDOM BASIS

ALI AKHAVI, JEAN-FRANÇOIS MARCKERT, AND ALAIN ROUAULT

ABSTRACT. For $p \leq n$, let $b_1^{(n)}, \dots, b_p^{(n)}$ be independent random vectors in $\mathbb{R}^n$ with the same distribution invariant by rotation and without mass at the origin. Almost surely these vectors form a basis for the Euclidean lattice they generate. The topic of this paper is the property of reduction of this random basis in the sense of Lenstra-Lenstra-Lovász (LLL). If $\widehat{b}_1^{(n)}, \dots, \widehat{b}_p^{(n)}$ is the basis obtained from $b_1^{(n)}, \dots, b_p^{(n)}$ by Gram-Schmidt orthogonalization, the quality of the reduction depends upon the sequence of ratios of squared lengths of consecutive vectors $r_j^{(n)} = \|\widehat{b}_{n-j+1}^{(n)}\|^2 / \|\widehat{b}_{n-j}^{(n)}\|^2$, $j = 1, \dots, p$. We show that as $n \to \infty$ the process $(r_j^{(n)} - 1, j \geq 1)$ tends in distribution in some sense to an explicit process $(\mathcal{R}_j - 1, j \geq 1)$; some properties of the latter are provided.

1. Introduction.

Let $\mathbf{b}_p^{(n)} := (b_1^{(n)}, b_2^{(n)}, \dots, b_p^{(n)})$ be a linearly independent system of $p \leq n$ vectors of $\mathbb{R}^n$. The set of all their integer linear combinations is a *lattice*, i.e. an additive discrete subgroup of $\mathbb{R}^n$. The system $\mathbf{b}_p^{(n)}$ is then a *basis* of the lattice. The lattice basis reduction problem deals with finding a basis of a given lattice, whose vectors are "short" and "almost orthogonal". The problem is old and there are numerous notions of reduction (for a general survey, see for example [**?**, **?**, **?**]). Solving even approximately the lattice basis reduction problem has numerous theoretical and practical applications in integer optimization [**?**], computational number theory [**?**] and cryptography [**?**]. In 1982, Lenstra, Lenstra and Lovász [**?**] introduced for the first time an efficient (polynomial with respect to the length of the input) approximation reduction algorithm. It depends on a real approximation parameter $s \in]0, \sqrt{3}/2[$ and is called LLL(s). The output basis of the LLL algorithm is called a LLL(s) reduced or s-reduced basis. The next definition (characterizing a s-reduced

Date: July 7, 2009.

2000 *Mathematics Subject Classification.* Primary 15 A 52, 15 A 03, 60 B 12; Secondary 60 F 99, 06 B 99, 68 W 40.

Key words and phrases. Random matrices, Random basis, orthogonality index, determinant, lattice reduction.

basis) and the LLL-algorithm itself make a broad use of the classical Gram-Schmidt orthogonalization. With the linearly independent system $\mathbf{b}_p^{(n)}$, it associates the orthogonal system $\widehat{\mathbf{b}}_p^{(n)} := (\widehat{b}_1^{(n)}, \cdots, \widehat{b}_p^{(n)})$ defined by the recursion

$$\widehat{b}_1^{(n)} = b_1^{(n)} \ , \ \widehat{b}_j^{(n)} = b_j^{(n)} - \sum_{i=1}^{j-1} \frac{\langle b_j^{(n)}, \widehat{b}_i^{(n)} \rangle}{\|\widehat{b}_i^{(n)}\|^2} \, \widehat{b}_i^{(n)} \quad \text{for } j = 2, \cdots, p. \tag{1.1}$$

Let us stress that the vectors need not to be unit.

Definition 1.1. *Let $s \in \left(0, \dfrac{\sqrt{3}}{2}\right)$. A system $\mathbf{b}_p^{(n)}$ of p linearly independent vectors of $\mathbb{R}^n$ is a LLL(s)-reduced basis of the generated lattice if for all $1 \leq i \leq p-1$,*

$$\frac{\|\widehat{b}_{i+1}^{(n)}\|^2}{\|\widehat{b}_i^{(n)}\|^2} > s^2. \tag{1.2}$$

It is a local property of two–dimensional bases. For fixed i, this inequality concerns the basis composed of the projections of $b_i^{(n)}$ and $b_{i+1}^{(n)}$ on the orthogonal complement of the linear subspace $\mathrm{Span}\{b_1^{(n)}, b_2^{(n)}, \dots, b_{i-1}^{(n)}\}$. In [**?**] it is shown that when all these two–dimensional bases are s-reduced then the Euclidean properties of the whole basis are nice enough. For instance, the length of the first vector of n LLL-reduced basis is not larger than $(1/s)^{p-1}$ times the length of a shortest vector in the lattice generated by $\mathbf{b}_p^{(n)}$. Two important quantities are involved in the reduction of a basis.

Definition 1.2. *Let $\mathbf{b}_p^{(n)}$ be a linearly independent system of vectors of $\mathbb{R}^n$. The* reduction level *of $\mathbf{b}_p^{(n)}$ is the quantity*

$$\mathcal{M}_n^g := \min_{i \in \{1, \dots, n-(g+1)\}} \frac{\|\widehat{b}_{i+1}^{(n)}\|^2}{\|\widehat{b}_i^{(n)}\|^2}, \tag{1.3}$$

where $g = n - p$ is the codimension. The index of worst local reduction *of $\mathbf{b}_p^{(n)}$ is the quantity*

$$\mathcal{I}_n^g := \min \left\{ j \in \{g, \cdots, n-2\} : \ \frac{\|\widehat{b}_{n-j}^{(n)}\|^2}{\|\widehat{b}_{n-j-1}^{(n)}\|^2} = \mathcal{M}_n^g \right\}.$$

The variable $\mathcal{M}_n^g$ is the supremum of the set of those s^2 for which the basis is s-reduced. The second variable $\mathcal{I}_n^g$ is the place where the satisfied local condition is the weakest. This indicates where the limitation of the reduction comes from locally.

When $\mathbf{b}_p^{(n)}$ is chosen at random, the reduction level $\mathcal{M}_n^g$ and the index of worst local reduction $\mathcal{I}_n^g$ are two random variables, well defined whenever $\mathbf{b}_p^{(n)}$ is a linearly independent system. This paper is essentially devoted to the study of these random variables when the dimension n of the ambient space grows, for general codimensions of the random basis. It can be noticed that although we work with the whole system $\mathbf{b}_n^{(n)}$, the system $\widehat{\mathbf{b}}_p^{(n)}$ depends only on the p first vectors of $\mathbf{b}_n^{(n)}$; the same conclusion holds for $\mathcal{M}_n^g$ and $\mathcal{I}_n^g$.

In various previous works ([**?**], [**?**]), the vectors $b_1^{(n)}, \cdots, b_n^{(n)}$ are picked randomly from $\mathbb{R}^n$, independently, and uniformly in the Euclidean ball of radius M. The motivations are the following : the main reduction algorithms (in particular the LLL algorithm) act in the same way on a basis and on its transformed by a similarity. In the applications in computer science, the vectors have large integer coordinates. Roughly speaking, when M is large, the random choice of an integer vector in the ball of radius M is not so far from the random choice of a real vector in the unit ball $\mathbb{B}^n := \{x \in \mathbb{R}^n : \|x\| \leq 1\}$. Choosing real valued vectors greatly simplifies the computations, and allows one to derive exact results, as done in the present paper, when the computation are for the moment untractable in the case of integers valued vectors.

We extend slightly this model to the following class of distributions which is particularly simple and leads to interesting asymptotic results.

Definition 1.3. *A* spherical model *is a sequence $(\nu_n)_n$ where for each $n \geq 1$, ν_n is a rotationally invariant distribution on $\mathbb{R}^n$ satisfying $\nu_n(\{0\}) = 0$.*

It is well known (see for instance [**?**] Th.1.5.6 p.38 and [**?**] Prop.3.2), that under such a ν_n,
• the radial part $\|x\|$ and the angular part $\theta(x) := x/\|x\|$ are independent
• $\theta(x)$ is uniformly distributed on $\mathbb{S}^{n-1} := \{x \in \mathbb{R}^n : \|x\| = 1\}$.

The most natural examples of ν_n (quoted in the book of Knuth ([**?**, Section 3.4.1])) are:

a) the uniform distribution on the sphere $\mathbb{S}^{n-1}$; the corresponding distribution $\nu_n^{\otimes n}$ of the system is denoted $\mathbb{U}_n^S$,
b) the uniform distribution in the unit ball $\mathbb{B}^n$; the corresponding distribution $\nu_n^{\otimes n}$ is denoted $\mathbb{U}_n^B$ – called the "random ball model",
c) the n-variate standard normal (the coordinates are i.i.d. $\mathcal{N}(0,1)$); the corresponding distribution $\nu_n^{\otimes n}$ is denoted $\mathbb{G}_n$.

When $b_1^{(n)}, \cdots, b_n^{(n)}$ are n vectors picked randomly from $\mathbb{R}^n$, independently, and with some rotationaly invariant distribution ν_n, for any $p \leq n$ the system $\mathbf{b}_p^{(n)}$ is almost surely linearly independent. We call it a (p-dimensional) *random basis*.

We will also assume that roughly speaking, under (ν_n) the lengths of the vectors are concentrated around their mean (see Assumption 2.1). Under this assumption, we prove in particular that for s fixed, a full random basis is s-reduced with a positive probability when n is large, or more precisely that $\mathcal{M}_n^0$ converges in distribution to a random variable with interesting properties. Moreover the index $\mathcal{I}_n^g$ also converges in distribution, for any finite g. On the contrary, in the regime $g \to \infty$, the probability of reduction tends to 1, i.e. $\mathcal{M}_n^g$ converges in distribution to the Dirac measure at 1. The starting point of our study is the known fact (which will be recalled) that under a spherical model, the random variables $\|\widehat{b}_k^{(n)}\|^2$, $k = 1, \ldots, n$ are independent and beta distributed with varying parameters. This paper may be considered as an extension of some results obtained in [**?**] and [**?**] by one of us with a rather involved use of the Laplace method. The novelty of our approach here consists in a representation of these beta variables by means of independent gamma variables. This allows to work in a large probability space, (independent of n) and to consider strong convergences.

Besides, another interesting statistic of a basis is the so-called orthogonality defect, which plays a role in its reduction.

Definition 1.4 (Schnorr ([**?**])). *The orthogonality defect of a basis* $\mathbf{b}_p^{(n)}$ *is the quantity*

$$\rho_{p,n} := \prod_{k=1}^{p} \frac{\|b_k^{(n)}\|}{\|\widehat{b}_k^{(n)}\|} \quad (p \leq n)\,.$$

It is strongly related to the determinant of the lattice. If $B = [b_1^{(n)}, \ldots, b_p^{(n)}]$ is the $n \times p$ matrix with p column vectors $b_1^{(n)}, \ldots, b_p^{(n)}$ of $\mathbb{R}^n$ and B' denotes its transpose, then the determinant of the lattice generated by $\mathbf{b}_p^{(n)}$ is $\left(\det B'B\right)^{1/2}$. Since

$$\det B'B = \prod_{i=1}^{p} \|\widehat{b}_i^{(n)}\|^2$$

we have

$$\frac{1}{\rho_{p,n}^2} = \frac{\det B'B}{\|b_1^{(n)}\|^2 \cdots \|b_p^{(n)}\|^2} \tag{1.4}$$

and this quantity is usually called the Hadamard ratio, referring to the well known Hadamard inequality (1893):

$$\det B'B \leq \|b_1^{(n)}\|^2 \cdots \|b_p^{(n)}\|^2 \tag{1.5}$$

(meaning equivalently that $\rho_{p,n} \geq 1$) with equality if and only if $b_1^{(n)}, \dots, b_p^{(n)}$ are orthogonal ([**?**]). It means that the volume (or p-content) of the parallelotope built from $b_1^{(n)}, \dots, b_p^{(n)}$ is maximal when the vectors are orthogonal. Abbott and Mulders [**?**], Dixon [**?**] are concerned with the tightness of the bound $\rho_{n,n}^2 \geq 1$ when $\mathbf{b}_n^{(n)}$ is sampled from $\mathbb{U}_n^S$. In a recent paper, one of us ([**?**]) proved asymptotic results for some random determinants. We present here direct consequences for the orthogonality defect, considered as a random process indexed by t when $p = \lfloor nt \rfloor$ and $t \in [0,1]$.

The paper is organized as follows. Section 2 is devoted to the statement of the main results on reduction of random basis. In Section 3 we first recall known results on the connection between random bases and beta distributions and put them in the framework of spherical models. Then, we define two random processes on $(0,\infty)^{\mathbb{N}}$. The first one, (for fixed n), is the sequence $r_j^{(n)} = \|b_{n-j+1}^{(n)}\|^2/\|b_{n-j}^{(n)}\|^2, j \leq n-1$, extended by an infinite array of 1. The second one, $(\mathcal{R}_j, j \geq 1)$ (the foreseen limiting process) is the sequence of ratios of consecutive elements of an infinite array of independent gamma variables with varying parameters.

In Section 4, we give the probabilistic background for the properties of random variables involved in the limiting process. In particular, we prove that $(\mathcal{R}_j - 1)_j$ lives almost surely in ℓ^q, for $q > 2$. We give also a description of the distribution of $\inf_j \mathcal{R}_j$, which has its own interest.

Section 5 is devoted to the convergence in distribution of the sequence $(r_j^{(n)} - 1, j \geq 1)$ of ℓ^q valued random processes to $(\mathcal{R}_j - 1, j \geq 1)$. The key tool is a representation of the main random variables involved in the reduction of the random basis by versions living in a fixed probability space. In Section 6 are quoted connections between the different forms of reduction. In Section 7 we study possible extensions and in Section 8 we give the asymptotic behavior of the orthogonality defect. A large part of the results of this paper were announced in [**?**].

2. Main results

The following assumption on the sequence $(\nu_n)_n$ means roughly that the length of the vectors are concentrated around their mean.

Assumption 2.1. *There exists a deterministic sequence $(a_n)_n$ and constants $d_1 > 0, d_2 > 0, \alpha > 0$, $\rho_0 \in (0,1)$ such that, for every $n \geq 1$ and $\rho \in (0, \rho_0)$*

$$\nu_n \left(\left| \frac{\|x\|^2}{a_n} - 1 \right| \geq \rho \right) \leq d_1 e^{-n d_2 \rho^\alpha} . \tag{2.1}$$

Theorem 2.2. *Let $b_1^{(n)}, b_2^{(n)}, \dots, b_{n-g}^{(n)}$ be a random basis under a spherical model (ν_n) satisfying Assumption 2.1.*

(1) *If g is constant and $s \in (0,1)$ is fixed, the probability that the basis is s–reduced converges to a constant in $(0,1)$ (depending on s and g). More precisely, there exists a random variable $\mathcal{M}^g$ supported by $[0,1]$ having a density, such that $(\mathcal{M}_n^g)$ converges to $\mathcal{M}^g$ in distribution as n tends to infinity. Moreover, the index of worst local reduction $(\mathcal{I}_n^g)$ converges in distribution as n tends to infinity.*
(2) *For $s \in (0,1)$ fixed, if $g = g(n)$ tends to infinity, the probability that the basis is s–reduced tends to 1 as n tends to infinity, or in other words $(\mathcal{M}_n^g)$ converges in distribution to 1.*

Although "convergence in distribution" and "convergence in probability" are equivalent when the limit is a constant and all the variables are defined on the same probability space, we stress that the latter convergence in (2) is in distribution since our variables $\mathcal{M}_n^g$ live on a probability space depending on n.

This theorem will be proved in Section 5.

Proposition 2.3. *The three examples of (ν_n) given in the introduction satisfy Assumption 2.1.*

This proposition will be proved in Section 3.2.

Notice that in [?] Lemma 3 p.376, under $\mathbb{U}_n^B$, it was proved that $\mathbb{P}(\mathcal{M}_n^{cn-1} \leq s) \to 0$, as soon as $s < \frac{1}{2}(1-c)^{\frac{1-c}{c}}(1+c)^{\frac{1}{c}}$, (and that this convergence is exponentially fast). The author conjectured that it could be extended to $s < 1$. Theorem 2.2(2) answers positively this conjecture.

In [?], Donaldson considered a different random model where the basis $b_1^{(n)}, \cdots, b_{n-g}^{(n)}$ is picked uniformly from the set $\{\|b_1^{(n)}\|^2 + \cdots + \|b_{n-g}^{(n)}\|^2 = 1\}$ (Euclidean sphere in $\mathbb{R}^{n\times(n-g)}$), so that the vectors are not independent. He proved that as $n, g \to \infty$ with $n-g$ fixed, the basis is asymptotically reduced in the sense of Minkowski, i.e. each $b_i^{(n)}$ is a shortest vector among all vectors of the lattice that complete $b_1^{(n)}, \cdots, b_{i-1}^{(n)}$ to form a bigger subset of a lattice basis. It is a stronger form of reduction, but a particular case of codimension. The following result, which is a Corollary of Theorem 2.2, states the behavior of random basis under the Donaldson model as regards the s-reduction in a large range of codimensions.

Corollary 2.4. *Assertions (1) and (2) of Theorem 2.2 hold true in the Donaldson model.*

This corollary will be proved in Section 3.2.

3. Spherical models and beta distributions

3.1. **Preliminaries.** We summarize some properties of the Gamma and Beta distributions used throughout the paper. They can be found in [?] pp. 93-94.

For $a > 0$, the gamma distribution γ_a (with parameter a) is

$$\gamma_a(dx) = \frac{e^{-x}x^{a-1}}{\Gamma(a)} \ \mathbb{1}_{[0,\infty)}(x)\ dx\,,$$

its mean is a and its variance is a.
For $a > 0$ and $b > 0$ the beta distribution $\beta_{a,b}$ (with parameters (a, b)) is

$$\beta_{a,b}(dx) = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} x^{a-1}(1-x)^{b-1} \ \mathbb{1}_{(0,1)}(x)\ dx.$$

In the following, $\gamma(a)$ denotes a variable with distribution γ_a, and $\beta(a, b)$ denotes a variable with distribution $\beta_{a,b}$. The first relation[1] is

$$\big(\gamma(a), \gamma(b)\big) \ \overset{(d)}{=} \ \big(\beta(a,b)\gamma(a+b), (1-\beta(a,b))\gamma(a+b)\big)\,, \tag{3.1}$$

where on the left hand side the random variables $\gamma(a)$ and $\gamma(b)$ are independent and on the right hand side the random variables $\beta(a, b)$ and $\gamma(a + b)$ are independent. It entails

$$\gamma(a) + \gamma(b) \overset{(d)}{=} \gamma(a+b)\,, \tag{3.2}$$

$$\frac{\gamma(a)}{\gamma(a)+\gamma(b)} \ \overset{(d)}{=} \ \beta(a,b)\,, \tag{3.3}$$

and

$$\frac{\gamma(a)}{\gamma(b)} \ \overset{(d)}{=} \ \frac{\beta(a,b)}{1-\beta(a,b)}\,, \tag{3.4}$$

which gives

$$\mathbb{P}\big(\gamma(a)/\gamma(b) \in dx\big) = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} \frac{x^{a-1}}{(1+x)^{a+b}} \ \mathbb{1}_{[0,\infty[}(x)\ dx\,. \tag{3.5}$$

This distribution is sometimes called the beta-prime distribution of parameter (a, b). Notice that if $2a$ and $2b$ are integers, then $b\gamma(a)/a\gamma(b)$ has the Fisher $F_{2a,2b}$ distribution. The second relation is

$$\beta(a,b)\beta(c,a-c) \ \overset{(d)}{=} \ \beta(c,a+b-c)\,, \tag{3.6}$$

where on the left hand side the random variables are independent. As an immediate consequence of the additivity (3.2) and the law of large numbers, we have

$$\frac{\gamma(a)}{a} \xrightarrow[a\to\infty]{(d)} 1\,, \tag{3.7}$$

[1] In the whole paper, $\overset{(d)}{=}$ stands for equality in distribution, and $\xrightarrow[n]{(d)}$ stands for convergence in distribution

with an almost sure convergence if all the variables $\gamma(a)$ are defined on the same space. This can be proved using the following classical lemma.

Lemma 3.1. *The Laplace transform of γ_a is*

$$\mathbb{E}e^{\theta\gamma(a)} = (1-\theta)^{-a} \qquad (\theta < 1)\,, \tag{3.8}$$

and we have the Chernov bounds:

$$\begin{aligned} \mathbb{P}\big(\gamma(a) \geq ax\big) &\leq e^{-aH(x)} \qquad (x \geq 1) \\ \mathbb{P}\big(\gamma(a) \leq ax\big) &\leq e^{-aH(x)} \qquad (x \leq 1)\,, \end{aligned} \tag{3.9}$$

where H is the Cramér transform

$$H(x) = \sup_{\theta<1}\Big\{\theta x - \log\mathbb{E}(e^{\theta\gamma(1)})\Big\} = x - 1 - \log x,\ \ (x \geq 0)\,. \tag{3.10}$$

3.2. **Identification of distributions.** We first recall some facts concerning the spherical models, facts that have been proved several times and that are more or less part of the folklore.

For any $j = 1, \dots, n$, let

$$Y_j^{(n)} := \|\widehat{b}_j^{(n)}\|^2 / \|b_j^{(n)}\|^2.$$

Theorem 3.2 (Anderson [?], Theorem 9.3.3). *Under $\mathbb{U}_n^S$, the variables $\|\widehat{b}_j^{(n)}\|^2$, $j = 1, \cdots, n$ are independent and for $1 \leq j \leq n$*

$$\|\widehat{b}_j^{(n)}\|^2 \overset{(d)}{=} \beta\left(\frac{n-j+1}{2}, \frac{j-1}{2}\right). \tag{3.11}$$

An easy extension to spherical distributions is the following.

Theorem 3.3. *Under a spherical model, the variables $\|\widehat{b}_j^{(n)}\|^2$, $j = 1, \cdots, n$ are independent. For every $j = 2, \dots, n$,*

$$Y_j^{(n)} \overset{(d)}{=} \beta\left(\frac{n-j+1}{2}, \frac{j-1}{2}\right). \tag{3.12}$$

Moreover, all the random variables $Y_j^{(n)}, j \geq 1$, $\|b_j^{(n)}\|^2, j \geq 1$ are independent.

Corollary 3.4 (Daudé-Vallée [?]). *Under $\mathbb{U}_n^B$, the variables $\|\widehat{b}_j^{(n)}\|^2$, $j = 1, \cdots, n$ are independent and for $1 \leq j \leq n$*

$$\|\widehat{b}_j^{(n)}\|^2 \overset{(d)}{=} \beta\left(\frac{n-j+1}{2}, \frac{j+1}{2}\right). \tag{3.13}$$

Although Daudé and Vallée gave a direct analytic proof, their result may be viewed as a consequence of Theorem 3.3 and identity (3.6), since under the random ball model $\|b_i^{(n)}\|^2 \overset{(d)}{=} \beta(n/2, 1)$. For the convenience of the reader, we give below a probabilistic proof of Theorem 3.3.

Proof of Theorem 3.3: Let us skip the superscript (n) in this proof. We have $b_i = \|b_i\|\theta_i$ and from (1.1), we see that $\widehat{b}_i = \|b_i\|\widehat{\theta}_i$, where the $\widehat{\theta}_i$'s are obtained by the Gram-Schmidt algorithm applied to the θ_i's. As recalled in the introduction, $(\theta_1, \dots \theta_n)$ is $(\mathbb{U}_n^S)^{\otimes n}$ distributed. From Theorem 3.2, the variables $\|\widehat{\theta}_i\|^2$, $i = 2, \dots, n$ are independent with the convenient beta distributions.

From the radial-angular independence, $(\|b_1\|^2, \cdots, \|b_n\|^2)$ is independent of $(\|\widehat{\theta}_2\|^2, \dots, \|\widehat{\theta}_n\|^2) = (Y_2, \dots, Y_n)$. The independence of the variables $\|\widehat{b}_j\|^2$ is then a consequence of all the other independences. □

Let us check now that our natural distributions satisfy Assumption 2.1.

Proof of Proposition 2.3. • If ν_n is the uniform distribution on $\mathbb{S}^{n-1}$, then $\|x\|^2 = 1$, and $a_n = 1$.

• If ν_n is the uniform distribution in the ball, the distribution of the radial part is

$$\nu_n(\{x : \|x\| \leq r\}) = r^n, \quad 0 \leq r \leq 1\,, \tag{3.14}$$

so that, taking $a_n = 1$,

$$\nu_n(|\|x\|^2/a_n - 1| \geq \rho) = (1-\rho)^{n/2} \leq e^{-n\rho/2}\,,$$

and Assumption 2.1 is satisfied with $\alpha = 1$.

• ν_n is the n-variate standard normal (the coordinates are i.i.d. $\mathcal{N}(0,1)$). Then $\|x\|^2/2$ is $\gamma_{n/2}$-distributed. For $a_n = n$,

$$\nu_n\left(\left|\frac{\|x\|^2}{n} - 1\right| \geq \rho\right) = \mathbb{P}\left(\gamma(n/2) \geq (1+\rho)\frac{n}{2}\right) + \mathbb{P}\left(\gamma(n/2) \leq (1-\rho)\frac{n}{2}\right).$$

Using (3.9), we get

$$\mathbb{P}(\gamma(n/2) \geq (1+\rho)\frac{n}{2}) \leq e^{-\frac{n}{2}H(1+\rho)} = e^{-\frac{n}{2}(\rho - \log(1+\rho))}$$

and similarly,

$$\mathbb{P}(\gamma(n/2) \leq (1-\rho)\frac{n}{2}) \leq e^{\frac{n}{2}(\rho + \log(1-\rho))}\,.$$

Hence Assumption 2.1 is satisfied with $\alpha = 2$. □

Proof of Corollary 2.4. Let us come back to the notation $n - g = p$ for simplicity. A realization of the Donaldson model can be obtained by taking np independent $\mathcal{N}(0,1)$ random variables $G_{i,j}$, $i = 1, \dots, n$, $j = 1, \dots, p$ and setting

$$V_n^2 = \sum_{i \leq n} \sum_{m \leq p} G_{i,m}^2 \quad , \quad b_j^{(n)} = \left(\frac{G_{1,j}}{V_n}, \dots, \frac{G_{n,j}}{V_n}\right)^T \quad , \quad j = 1, \dots p\,.$$

It is then clear that the vectors $\widehat{b}_j^{(n)}$ given by the Gram-Schmidt algorithm are proportional to those obtained by the same algorithm when the inputs are the vectors of the Gaussian model $\mathbb{G}_n$. The factor of proportionality is just V_n^{-1}. The ratios of consecutive vectors are then unchanged, and since they are the only ingredients in $\mathcal{M}_n^g$, the conclusions of Theorem 2.2 are preserved for this model. □

3.3. **First consequences for random bases.** Here is some information on the asymptotic behavior of the random variables $Y_j^{(n)}$ and $\widehat{b}_j^{(n)}$:

Proposition 3.5. *Under a spherical model,*

(1) *for each $j \geq 1$,*

$$\frac{n}{2}\, Y_{n-j}^{(n)} \quad \xrightarrow[n]{(d)} \quad \gamma_{\frac{j+1}{2}}\,, \tag{3.15}$$

$$Y_j^{(n)} \quad \xrightarrow[n]{(d)} \quad 1\,; \tag{3.16}$$

(2) *if there exists a deterministic sequence a_n such that*

$$\|b_1^{(n)}\|^2/a_n \xrightarrow[n]{(d)} 1\,, \tag{3.17}$$

then,

$$\frac{n}{2a_n}\, \|\widehat{b}_{n-j}^{(n)}\|^2 \quad \xrightarrow[n]{(d)} \quad \gamma_{\frac{j+1}{2}}\,, \quad \textit{for } j \geq 0 \tag{3.18}$$

$$\frac{1}{a_n}\, \|\widehat{b}_j^{(n)}\|^2 \quad \xrightarrow[n]{(d)} \quad 1,, \quad \textit{for } j \geq 1\,. \tag{3.19}$$

Remark 3.6. *Under the same assumptions, we have also:*
If $h(n) \to \infty$ and $h(n)/n \to 0$, then

$$\frac{n}{h(n)a_n}\, \|\widehat{b}_{n-h(n)}^{(n)}\|^2 \xrightarrow[n]{(d)} 1\,. \tag{3.20}$$

If $0 < \alpha < 1$ and $k(n)/n \to 0$, then

$$\frac{1}{a_n}\, \|\widehat{b}_{\alpha n+k(n)}^{(n)}\|^2 \xrightarrow[n]{(d)} 1-\alpha\,. \tag{3.21}$$

The above limits ((3.18), (3.19), (3.20), (3.21)), stated under $\mathbb{U}_n^B$, can be found in [**?**, Theorem 8] in a slightly different form and proved in an involved analytic way. We give now a new direct proof, valid for spherical models. This prefigures the main arguments used to prove the convergences in Section 5.2.

Proof of Proposition 3.5. From Theorem 3.3 we have the decomposition,

$$\|\widehat{b}_{n-j}^{(n)}\|^2 \overset{(d)}{=} Y_{n-j}^{(n)}\, \|b_1^{(n)}\|^2\,, \tag{3.22}$$

with $Y_{n-j}^{(n)} \overset{(d)}{=} \beta\left(\frac{j+1}{2}, \frac{n-j-1}{2}\right)$. From (3.3)

$$Y_{n-j}^{(n)} \overset{(d)}{=} \frac{\gamma\left(\frac{j+1}{2}\right)}{\gamma\left(\frac{j+1}{2}\right) + \gamma\left(\frac{n-j-1}{2}\right)}$$

and from (3.7), for fixed j,

$$\frac{1}{n}\gamma\left(\frac{n-j-1}{2}\right) \xrightarrow[n]{(d)} \frac{1}{2}\,,$$

which yields (3.15). With the help of Assumption (3.17), we get also (3.18).

To prove (3.16), notice that by symmetry

$$\beta(a, b) \overset{(d)}{=} 1 - \beta(b, a)$$

so that $1 - Y_j^{(n)} \overset{(d)}{=} Y_{n-j+2}^{(n)}$, and that $Y_{n-j+2}^{(n)} \xrightarrow[n]{(d)} 0$ by (3.15).

To end, (3.19) is a consequence of (3.16) and (3.17). □

3.4. **The processes of ratios** $(r_j^{(n)}, j \geq 1)$ **and** $(\mathcal{R}_j, j \geq 1)$**.** Recall the definition of $\mathcal{M}_n^g$ given in (1.3). From the independence of the $\|\widehat{b}_j^{(n)}\|^2$ and (3.15), we have, for j fixed :

$$\frac{\|\widehat{b}_{n-j+1}^{(n)}\|^2}{\|\widehat{b}_{n-j}^{(n)}\|^2} \xrightarrow[n]{(d)} \frac{\gamma\left(\frac{j+1}{2}\right)}{\gamma\left(\frac{j}{2}\right)}\,, \tag{3.23}$$

where $\gamma\left(\frac{j+1}{2}\right)$ and $\gamma\left(\frac{j}{2}\right)$ are independent. Now, if we let $j \to \infty$, (3.7) tells us that $\gamma\left(\frac{j+1}{2}\right)/\gamma\left(\frac{j}{2}\right) \xrightarrow[n]{(d)} 1$. This makes plausible that the minimum in (1.3) is reached in the end of the sequence of ratios. This motivate a time inversion

$$\mathcal{M}_n^g = \min_{g+1 \leq j \leq n-1} r_j^{(n)}\ , \ \text{where}\ \ r_j^{(n)} := \frac{\|\widehat{b}_{n-j+1}^{(n)}\|^2}{\|\widehat{b}_{n-j}^{(n)}\|^2}\,. \tag{3.24}$$

The variable $\mathcal{M}_n^g$ is a function of the $(n-g-1)$-tuple $(r_{g+1}^{(n)}, \dots, r_{n-1}^{(n)})$, and then the convergence of each coordinate is not sufficient to yield a convergence of $\mathcal{M}_n^g$. We have to take into account that the variables $(r_j^{(n)}, j \leq n-1)$ are dependent and that their number is growing. Since $r_{n-i}^{(n)} \xrightarrow[n]{(d)} 1$ for any fixed i by (3.19), it is convenient to embed the $(n-1)$-tuple $(r_1^{(n)}, \cdots r_{n-1}^{(n)})$ into $\mathbb{R}_+^{\mathbb{N}}$, the set of infinite sequences of positive real numbers, setting

$$r_j^{(n)} := 1\ ,\ j \geq n\,. \tag{3.25}$$

In view of the convergence (3.23), we are lead to define a discrete time process $(\mathcal{R}_j, j \geq 1)$ in the following way. Let $(\eta_i, i \geq 1)$ be a sequence of independent random variables such that $\eta_i \stackrel{(d)}{=} \gamma_{i/2}$ and set

$$\mathcal{R}_j := \eta_j/\eta_{j+1}\ ,\ j \geq 1\,. \tag{3.26}$$

For $g \in \mathbb{N}$, set

$$\mathcal{M}^g := \inf\left\{\mathcal{R}_j, j \geq g+1\right\}.$$

Some properties of $\mathcal{M}^g$ are stated in Section 4, and the convergence of $(r_j^{(n)}, j \geq 1)$ to $(\mathcal{R}_j, j \geq 1)$ is stated in Section 5.

4. Results on $(\mathcal{R}_j, j \geq 1)$ based on the Beta-Gamma algebra

We give some important properties of $(\mathcal{R}_j, j \geq 1)$ and of $\mathcal{M}^g$. The proofs are at the end of the section. For $q \geq 1$, let ℓ_q be the set of sequences of real numbers $\mathsf{x} = (\mathsf{x}_i)_{i\geq 1}$ such that $\|\mathsf{x}\|_q := \left(\sum_{i\geq 1} |\mathsf{x}_i|^q\right)^{1/q}$ is finite, equipped with the norm $\|.\|_q$. The following proposition will allow later to consider convergence of random elements with values in ℓ_q.

Proposition 4.1. *For any $q > 2$, almost surely the process $(\mathcal{R}_k - 1, k \geq 1)$ is in ℓ_q, i.e. satisfies $\sum_k |\mathcal{R}_k - 1|^q < \infty$.*

The variables $\mathcal{M}^g$ have remarkable properties.

Proposition 4.2. (1) *For each $g \geq 0$, the distribution of $\mathcal{M}^g$ has a density, and its support is $[0,1]$.*

(2) *For each $g \geq 0$,*

$$\lim_{x\downarrow 0} x^{-\frac{g+1}{2}}\,\mathbb{P}(\mathcal{M}^g \leq x) = \frac{\Gamma\left(\frac{2g+3}{2}\right)}{\Gamma\left(\frac{g+3}{2}\right)\Gamma\left(\frac{g+2}{2}\right)}. \tag{4.1}$$

(3) *There exists $\tau > 0$ such that for each $g \geq 0$,*

$$\limsup_{x\downarrow 0}\ e^{\frac{\tau}{x^2}}\,\mathbb{P}(\mathcal{M}^g \geq 1-x) \leq 1\,. \tag{4.2}$$

(4) *For each $g \geq 0$, there is a.s. a unique random index $\mathcal{I}^g$ such that $\mathcal{R}_{\mathcal{I}^g} = \mathcal{M}^g$.*

The proofs of Propositions 4.1 and 4.2 raise on the following proposition devoted to the fluctuations and large deviations of $\mathcal{R}_k$ around 1.

Proposition 4.3. (1) *The following convergence in distribution holds*

$$\sqrt{k}\,(\mathcal{R}_k - 1) \xrightarrow[k]{(d)} \mathcal{N}(0,4)\,. \tag{4.3}$$

(2) *Let $f_{\mathcal{R}_k}$ be the density of $\mathcal{R}_k$ and*

$$\Phi_k(x) = (4x)^{\frac{k}{2}-1}(1+x)^{-k-\frac{1}{2}}\,.$$

For $A < 2\pi^{-1/2} < B$ we can find an integer K such that

$$A\sqrt{k}\ \Phi_k(x) \le f_{\mathcal{R}_k}(x) \le B\sqrt{k}\ \Phi_k(x) \tag{4.4}$$

for every $x \in (0,\infty)$ and every $k \ge K$.

(3) *There exists a constant C such that for every $k \ge 1$ and $\rho \in [0,1]$*

$$\mathbb{P}(\mathcal{R}_k < 1-\rho) \ \le\ C\left(1 - \frac{\rho^2}{(2-\rho)^2}\right)^{k/2} \tag{4.5}$$

$$\mathbb{P}(\mathcal{R}_k > 1+\rho) \ \le\ C\left(1 - \frac{\rho^2}{(2+\rho)^2}\right)^{k/2}\,. \tag{4.6}$$

(4) *Assertion (3) holds true when $\mathcal{R}_k$ is replaced by $\mathcal{R}'_k := \dfrac{\eta'_k}{\eta_k}$ where η'_k is independent of η_k and $\gamma_{k/2}$ distributed.*

Coming back to the preliminaries, we see that $\mathcal{R}_k$ has the distribution given by (3.5) with $a = k/2$ and $b = (k+1)/2$. Its mean is $k/(k-1)$. Noticing that $\mathcal{R}_k$ and $\mathcal{R}'_k$ are Fisher-distributed, Assertions (3) and (4) above are related to Section 4 of [**?**], but our bounds are not asymptotic: they hold for every ρ and k.

The proof is postponed to the end of this section.

Proof of Proposition 4.1. Thanks to the Borel-Cantelli lemma, it suffices to find a sequence $(v_k)_{k\ge1} \in \ell_q$, such that

$$\sum_k \mathbb{P}(|\mathcal{R}_k - 1| \ge v_k) < \infty\,. \tag{4.7}$$

Taking $\rho = v_k = k^{-1/\mu}$ in the bounds (4.6) and (4.5), we see that (4.7) is satisfied as soon as $\mu > 2$. To ensure $(v_k, k \ge 1) \in \ell_q$, it remains to choose $\mu \in (2, q)$. $\square$

Proof of Proposition 4.2 (1). We give a proof only for $g = 1$, since the argument is the same for any $g > 0$. We know that almost surely $\mathcal{R}_j > 0$ for every j and $\lim_k \mathcal{R}_k = 1$ (Proposition 4.1). The support of $\mathcal{M}^0$ is then a subset of $[0,1]$. For the same reason, the sequence $(\mathcal{R}_k)$ does not accumulate at 0, so that the distribution of $\mathcal{M}^0$ has no atom at 0.

Using (4.3), we have

$$\mathbb{P}(\mathcal{R}_{2j} < 1) = \mathbb{P}\left(\sqrt{2j}\,(\mathcal{R}_{2j} - 1) < 0\right) \xrightarrow[j\to\infty]{} 1/2\,,$$

so that $\sum_j \mathbb{P}(\mathcal{R}_{2j} < 1) = \infty$. From the definition (3.26) of the variables $\mathcal{R}_k$, the events $\{\mathcal{R}_{2j} < 1\}$ are independent, so we may apply the reverse Borel Cantelli lemma and claim that, a.s. there exists an infinite sequence of j such that $\mathcal{R}_{2j} < 1$, which yields that $\mathcal{M}^0$ has no atom at 1. (In fact, the existence of a unique $j > g$ satisfying $\mathcal{R}_j < 1$ is enough to prove the fact that $\mathcal{M}^g$ has no atom at 1).

It remains to check that the support of $\mathcal{M}^0$ is exactly $[0,1]$ (see (A) below) and that $\mathcal{M}^0$ has a density (see (B) below).
(A) Let us prove that $\mathbb{P}(\inf_j \mathcal{R}_j \in [a,b]) > 0$, for every $[a,b] \subset [0,1]$. It is enough to find a sequence of (independent) events $B_j := \{\eta_j \in (\alpha_j, \beta_j)\}, j \geq 0$ such that

$$\bigcap_{j=1}^{\infty} B_j \subset \left\{\inf_j \mathcal{R}_j \in [a,b]\right\} \quad \text{and} \quad \prod_{j=1}^{\infty} \mathbb{P}(B_j) > 0. \tag{4.8}$$

Let $j_a = \inf\{j : j \in \{1,2,\dots\}, j > 2(1+a)/(1-a)\}$, $A := j_a(1+a)/4$ and $c_1 < c_2$ in (a,b). Choose

$$\alpha_1 = Ac_1\,,\ \beta_1 = Ac_2\,,\quad \alpha_2 = A\,,\ \beta_2 = \frac{Ac_1}{a}\,,\quad \alpha_j = A\,,\ \beta_j = \frac{A}{a}\,,\qquad (3 \leq j \leq j_a)$$

and

$$\alpha_j = \frac{j(1+a)}{4}\,,\ \beta_j = \frac{(j-1)(1+a)}{4a}\,,\qquad (j \geq j_a + 1)\,.$$

We check easily that $B_1 \cap B_2 \subset \{\mathcal{R}_1 \in (a, c_2)\}$, and $B_j \cap B_{j+1} \subset \{\mathcal{R}_j \in (a,\infty)\}$ for $j \geq 2$. This proves the first claim of (4.8).

It remains to prove that the infinite product is convergent. Since each of its terms is clearly not 0, writting , $\prod_{j=1}^{\infty} \mathbb{P}(B_j) = \exp(\sum_{j\geq 1} \log(1 - \mathbb{P}(B_j^c)))$, and observing that $\mathbb{P}(B_j^c))$ goes to 0 with k (see below), in order to prove that $\prod_{j=1}^{\infty} \mathbb{P}(B_j) > 0$ it suffices to check that

$$\sum_{k > j_a} \mathbb{P}(B_k^c) < \infty\,. \tag{4.9}$$

For $j > j_a$, the interval (α_j, β_j) straddles the mean $j/2$ of η_j :

$$\alpha_j = \frac{j(1+a)}{4} < \frac{j}{2} < \frac{j(1+3a)}{8a} \leq \beta_j\,,$$

so that the large deviations inequalities (3.9) hold:

$$\mathbb{P}(\eta_j < \alpha_j) \leq \exp\left(-\frac{j}{2} H\left(\frac{1+a}{2}\right)\right)\ ,\ \mathbb{P}(\eta_j > \beta_j) \leq \exp\left(-\frac{j}{2} H\left(\frac{1+3a}{4a}\right)\right)\,.$$

This yields a positive constant M such that for $j > j_a$

$$\mathbb{P}(B_j^c) = \mathbb{P}(\eta_j < \alpha_j) + \mathbb{P}(\eta_j > \beta_j) \leq 2e^{-jM}$$

and the series is convergent, which proves (4.9) and $\mathbb{P}(\inf_j \mathcal{R}_j \in [a,b]) > 0$.

(B) According to Radon-Nikodym's theorem, it suffices to find a positive integrable function f on $(0,1)$, such that for any $[a,b] \subset (0,1)$,

$$\mathbb{P}(\mathcal{M}^0 \in [a,b]) \leq \int_{[a,b]} f(x)dx$$

By the union bound, we have for every $b' \in (b,1)$:

$$\mathbb{P}(\mathcal{M}^0 \in [a,b]) = \mathbb{P}(\inf_{k\geq 1} \mathcal{R}_k \in [a,b]) \leq \mathbb{P}\Big(\bigcup_k \{\mathcal{R}_k \in [a,b']\}\Big) \leq \sum_{k=1}^{\infty} \mathbb{P}\big(\mathcal{R}_k \in [a,b']\big)\,.$$

For $B > 2/\sqrt{\pi}$, thanks to formula (4.4), there exists $K \geq 1$ such that

$$\begin{aligned}
\sum_{k=K}^{\infty} \mathbb{P}\big(\mathcal{R}_k \in [a,b]\big) &\leq B\int_a^{b'} \left(\sum_{k=K}^{\infty} \sqrt{k}\ \Phi_k(x)\right) dx \\
&\leq \frac{B}{2}\int_a^{b'} \left[\sum_{k=1}^{\infty} k\left(\frac{2\sqrt{x}}{1+x}\right)^{k-1}\right] \frac{dx}{\sqrt{x(1+x)^3}} \\
&= \frac{B}{2}\int_a^{b'} \frac{\sqrt{1+x}}{\sqrt{x}(1-\sqrt{x})^4}\ dx\,.
\end{aligned}$$

Since every $\mathcal{R}_k$ has a density, one may bound the $K-1$ first terms of the sum by $\int_a^{b'} f_1(x)dx$ for some integrable f_1. Then, since the bound holds true for any $b' > b$, we can let $b' \downarrow b$ and we get the result.

Proof of Proposition 4.2 (2). We have

$$\mathbb{P}(\mathcal{R}_{g+1} \leq x) \leq \mathbb{P}(\mathcal{M}^g \leq x) \leq \mathbb{P}(\mathcal{R}_{g+1} \leq x) + \sum_{j=g+2}^{\infty} \mathbb{P}(\mathcal{R}_j \leq x)\,.$$

On the one hand, from (3.5), we have, for $x \to 0$,

$$\mathbb{P}(\mathcal{R}_{g+1} \leq x) = \frac{\Gamma\left(\frac{2g+3}{2}\right)}{\Gamma\left(\frac{g+2}{2}\right)\Gamma\left(\frac{g+3}{2}\right)}\ x^{(g+1)/2}(1+o(1))\,.$$

On the other hand, a simple computation shows that

$$\sum_{j=g+2}^{\infty} \mathbb{P}(\mathcal{R}_j \leq x) = O(x^{(g+3)/2}).$$

Proof of Proposition 4.2 (3). For $j \geq (g+1)/2$, we have:

$$\left\{\mathcal{M}^g > 1-(2j)^{-1/2}\right\} \subset \bigcap_{i=j}^{2j} \left\{\mathcal{R}_{2i} > 1-(2j)^{-1/2}\right\} \subset \bigcap_{i=j}^{2j} \left\{\mathcal{R}_{2i} > 1-i^{-1/2}\right\},$$

hence, by independence

$$\mathbb{P}\left(\mathcal{M}^g > 1-(2j)^{-1/2}\right) \leq \prod_{i=j}^{2j} \mathbb{P}\left(\mathcal{R}_{2i} > 1-i^{-1/2}\right).$$

From (4.3), we know that $\lim_k \mathbb{P}\left(\mathcal{R}_{2k} > 1-k^{-1/2}\right) = \mathbb{P}(N > -\sqrt{2})$ where $N \stackrel{(d)}{=} \mathcal{N}(0,4)$. Taking $\tau > 0$ with $e^{-\tau} > \mathbb{P}(N > -\sqrt{2})$ we see that for j large enough,

$$\mathbb{P}\left(\mathcal{M}^g > 1-(2j)^{-1/2}\right) \leq e^{-\tau j},$$

which proves (4.2).

Proof of Proposition 4.2 (4). The support of $\mathcal{M}^g$ is $[0,1]$ and $\lim \mathcal{R}_j = 1$ a.s. so that the set $\{j \geq g+1, \mathcal{R}_j = \mathcal{M}^g\}$ is not empty. Moreover since there is no ties ($\mathbb{P}(\mathcal{R}_i = \mathcal{R}_j) = 0$ a.s. for $i \neq j$) this set is a.s. a singleton. □

Proof of Proposition 4.3 (1). Setting

$$\bar{\eta}_k = \frac{\eta_k - k/2}{\sqrt{k}} \quad \text{and} \quad \bar{\eta}'_k = \frac{\eta_{k+1} - (k+1)/2}{\sqrt{k}}$$

the CLT gives $(\bar{\eta}_k, \bar{\eta}'_k) \xrightarrow[k]{(d)} \mathcal{N}(0,1/2) \otimes \mathcal{N}(0,1/2)$ hence $\bar{\eta}_k - \bar{\eta}'_k \xrightarrow[k]{(d)} \mathcal{N}(0,1)$. Since

$$\sqrt{k}\,(\mathcal{R}_k - 1) = \frac{k}{\eta_{k+1}}\left(\bar{\eta}_k - \bar{\eta}'_k - \frac{1}{2\sqrt{k}}\right),$$

and $\eta_{k+1}/k \to 1/2$ a.s., we get the result.

Proof of Proposition 4.3 (2). We have $f_{\mathcal{R}_k}(x) = C_k \Phi_k(x)$ with

$$C_k = 4^{1-\frac{k}{2}} \frac{\Gamma\left(k+\frac{1}{2}\right)}{\Gamma\left(\frac{k}{2}\right)\Gamma\left(\frac{k+1}{2}\right)} = \frac{2}{\sqrt{\pi}} \frac{\Gamma\left(k+\frac{1}{2}\right)}{\Gamma(k)} = \frac{2\sqrt{k}}{\sqrt{\pi}}\,(1+o(1)),$$

where the second equality comes from the Gauss duplication formula, and the $o(1)$ in the last equality tends to zero as k tends to infinity.

Proof of Proposition 4.3 (3). The bounds may be obtained by integration, but also by writing $\mathcal{R}_k$ as ratio of gamma variables and using Chernov's bounds. Since we need bounds holding for ρ depending on k, we use the Markov inequality, independence and (3.8) :

$$\begin{aligned}
\mathbb{P}(\mathcal{R}_k > 1+\rho) &= \mathbb{P}\left(\eta_k - (1+\rho)\eta_{k+1} > 0\right)\\
&\le \mathbb{E}\exp\left(\theta\eta_k - \theta(1+\rho)\eta_{k+1}\right)\\
&= (1-\theta)^{-k/2}\left(1+\theta(1+\rho)\right)^{-(k+1)/2}\\
&= \left(1+\theta(1+\rho)\right)^{-1/2}\Big[(1-\theta)(1+\theta(1+\rho))\Big]^{-k/2},
\end{aligned}$$

for every $\theta \in (0,1)$. The function $\theta \mapsto (1-\theta)(1+\theta(1+\rho))$ reaches its maximum for $\theta = \frac{\rho}{2(1+\rho)} < 1$, so that :

$$\mathbb{P}(\mathcal{R}_k > 1+\rho) \le \left(1 - \frac{\rho^2}{(2+\rho)^2}\right)^{k/2}. \tag{4.10}$$

Similarly

$$\begin{aligned}
\mathbb{P}(\mathcal{R}_k < 1-\rho) &\le E\exp\left(\theta(1-\rho)\eta_{k+1} - \theta\eta_k\right)\\
&= \left((1+\theta)\right)(1-\theta(1-\rho))^{-k/2}\left(1-\theta(1-\rho)\right)^{-1/2}\\
&\le \sqrt{2}\left(1 - \frac{\rho^2}{(2+\rho)^2}\right)^{k/2}.
\end{aligned}$$

Proof of Proposition 4.3 (4). The proof needs similar evaluations for $\mathcal{R}'_k$ and is left to the reader. □

5. Convergences in ℓ^q and consequences for random bases

5.1. **Main result.** The following Proposition 5.1 states a limit behavior for the process $(r_j^{(n)})$ when $n \to \infty$. It is the keystone for the proof of our main result (Theorem 2.2) whose statement is rephrased in Theorem 5.2 below.

Proposition 5.1. *For any $q > 2$, the following convergence in distribution holds in ℓ_q :*

$$(r_j^{(n)} - 1, j \ge 1) \xrightarrow[n]{(d)} (\mathcal{R}_j - 1, j \ge 1).$$

The convergence stated in this proposition is a convergence in distribution. This is due to the fact that the ambient spaces $\mathbb{R}^n, n \ge 1$ are not nested, and then, there is no evident canonical or geometrical consideration providing a stronger convergence (as almost sure convergence or convergence in probability). The proof of this proposition will use a representation of the processes $(r_j^{(n)}, j \ge 1)$ using the gamma distributions.

Since the mapping $\mathsf{x} \mapsto 1 + \min_{i \geq k} \mathsf{x}_i$ is continuous from ℓ_q onto $\mathbb{R}$, it follows that $\mathcal{M}_n^g \wedge 1$ converges in distribution to $\mathcal{M}^g$. We will prove in the next subsection the following rephrasing of Theorem 2.2:

Theorem 5.2. *If (ν_n) is spherical and satisfies Assumption 2.1 then,*

(1) *For every $g \geq 0$, $\mathcal{M}_n^g \xrightarrow[n]{(d)} \mathcal{M}^g$.*
(2) *For every $g \geq 1$, $\mathcal{I}_n^g \xrightarrow[n]{(d)} \mathcal{I}^g$.*
(3) *Let $g : \mathbb{N} \to \mathbb{N}$ such that $g(n) \leq n$ and $g(n) \to \infty$. We have $\mathcal{M}_n^{g(n)} \xrightarrow[n]{(d)} 1$.*

5.2. **Proofs of convergence (Theorem 5.2/2.2, and Proposition 5.1).**

5.2.1. *Construction of a probability space.* In order to prove Proposition 5.1 and Theorem 5.2, we build a probability space on which are defined some copies of the variables $\|b_i^{(n)}\|^2$, $\|\widehat{b}_i^{(n)}\|^2$, $i \geq 0$, $n \geq 0$ (and then also $r_j^{(n)}$) and the process $(\mathcal{R}_k, k \geq 1)$. Thanks to that framework, we will be able to use the strong law of large numbers to get the strong versions of the convergences in distribution stated in Proposition 5.1 and Theorem 5.2. This argumentation follows the coupling method.

From Theorem 3.3 and the representation (3.3) we see that

$$\begin{aligned} \|\widehat{b}_{n-k+1}^{(n)}\|^2 &= Y_{n-k+1}^{(n)} \|b_{n-k+1}^{(n)}\|^2 \\ Y_{n-k+1}^{(n)} \overset{(d)}{=} \frac{\sum_{m=1}^k \xi_m}{\sum_{m=1}^n \xi_m} &\quad , \quad \|b_{n-k+1}^{(n)}\|^2 \overset{(d)}{=} \|b_1^{(n)}\|^2 \end{aligned} \tag{5.1}$$

where the ξ_m's are $\gamma_{1/2}$ distributed, and $\|b_{n-k+1}^{(n)}\|^2$ is independent of the ξ_m's. Since the $\|\widehat{b}_{n-k+1}^{(n)}\|^2$ for $1 \leq k \leq n-1$ are independent, we may consider two double arrays $(\xi_i^k, i \geq 1, k \geq 1)$, $(\zeta_j^k, j \geq 1, k \geq 1)$ of independent random variables (and independent together), such that

$$\begin{aligned} \xi_j^k &\overset{(d)}{=} \gamma(1/2) \ , \quad (j \geq 1, k \geq 1)\, , \\ \zeta_j^k &\overset{(d)}{=} \|b_1^{(j)}\|^2 \ , \quad (j \geq 1, k \geq 1)\, . \end{aligned} \tag{5.2}$$

The common probability space on which are defined all the variables ξ_j^k and ζ_j^k is denoted by Ω. From now on we work exclusively on Ω.

Let us set

$$S_p^k = \sum_{m=1}^p \xi_m^k, \quad k \geq 1, \quad p \geq 1\, .$$

Now, the processes $(S_j^k, j \geq 1)$ for $k \geq 1$ are independent copies of $(S_j^1, j \geq 1)$, and for each $n \geq 1$, we have the following distributional representation :

$$\{\|\widehat{b}_{n-k+1}^{(n)}\|^2 \ , \quad 1 \leq k \leq n-1\} \stackrel{(d)}{=} \left\{ \frac{S_k^k}{S_n^k}\, \zeta_n^k, \quad 1 \leq k \leq n-1 \right\} . \tag{5.3}$$

For $n \geq 2$, set

$$R_k^{(n)} \quad = \quad \begin{cases} \dfrac{S_k^k}{S_{k+1}^{k+1}}\ \dfrac{S_n^{k+1}}{S_n^k}\ \dfrac{\zeta_n^k}{\zeta_n^{k+1}} & \text{if } 1 \leq k \leq n-1, \\ 1 & \text{if } k \geq n. \end{cases} \tag{5.4}$$

We have now, (see (3.24) and (3.25))

$$(r_k^{(n)}, k \geq 1) \stackrel{(d)}{=} (R_k^{(n)}, k \geq 1)\,. \tag{5.5}$$

The processes $r^{(n)}, n \geq 2$ are not defined on a unique probability space, since the ambient spaces are not nested. On the contrary, the sequence $R^{(n)}, n \geq 2$ is defined on the unique probability space Ω. Set also

$$\mathcal{R}_k := \frac{S_k^k}{S_{k+1}^{k+1}}\,. \tag{5.6}$$

Notice that since $\mathcal{R}$ was defined in (3.26), we make in (5.6) a slight abuse of notation but this is consistent in terms of distribution and allows to avoid a new symbol. From now on $(\mathcal{R}_k)$ is then a random variable on Ω.

Setting, for any $g \geq 0$,

$$M_n^g = \min_{g+1 \leq k \leq n-1} R_k^{(n)} \quad \text{and} \quad \mathcal{M}^g = \min_{k \geq g+1} \mathcal{R}_k\,, \tag{5.7}$$

we get

$$\mathcal{M}_n^g \ \stackrel{(d)}{=} \ M_n^g\,, \tag{5.8}$$

and want to prove a convergence (in probability) of M_n^g to $\mathcal{M}^g$. Since the convergence of $R_k^{(n)}$ to $(\mathcal{R}_k)$ for each k is not sufficient to this aim, we need a uniform control.

5.2.2. *Proof of Proposition 5.1.* This is a direct consequence of (5.5) and the following Lemma.

Lemma 5.3. *For some $q > 2$, $(R_k^{(n)} - \mathcal{R}_k, k \geq 1)$ converge a.s. (in Ω) to 0 in ℓ_q, i.e.*

$$\sum_{k=1}^{\infty} |R_k^{(n)} - \mathcal{R}_k|^q \xrightarrow[n]{a.s.} 0. \tag{5.9}$$

Proof of Lemma 5.3. We have

$$\sum_k |R_k^{(n)} - \mathcal{R}_k|^q = \sum_{1\le k\le n-1} |R_k^{(n)} - \mathcal{R}_k|^q + \sum_{k\ge n} |1-\mathcal{R}_k|^q .$$

On the one hand, the second term of the right hand side converges a.s. to zero (see Proposition 4.1). On the other hand, from (5.4) we have

$$R_k^{(n)} - \mathcal{R}_k = \mathcal{R}_k \left(\frac{S_n^{k+1}}{S_n^k} \frac{\zeta_n^k}{\zeta_n^{k+1}} - 1 \right) ,$$

and the sequence $(\mathcal{R}_k)$ is a.s. bounded (by Proposition 4.1). It is then enough to prove that a.s.

$$\lim_n \sum_{k=1}^{n-1} \left| \frac{S_n^{k+1}}{S_n^k} \frac{\zeta_n^k}{\zeta_n^{k+1}} - 1 \right|^q = 0 . \tag{5.10}$$

Let $\delta > 0$. By the union bound and the identity of distributions, we have

$$\begin{aligned} \mathbb{P}\left(\sum_{k=1}^{n-1} \left| \frac{S_n^{k+1}}{S_n^k} \frac{\zeta_n^k}{\zeta_n^{k+1}} - 1 \right|^q > \delta \right) &\le \sum_{k=1}^{n-1} \mathbb{P}\left(\left| \frac{S_n^{k+1}}{S_n^k} \frac{\zeta_n^k}{\zeta_n^{k+1}} - 1 \right|^q > \frac{\delta}{n} \right) \\ &= (n-1)\mathbb{P}\left(\left| \frac{S_n^{(2)}}{S_n^{(1)}} \frac{\zeta_n^1}{\zeta_n^2} - 1 \right| > \frac{\delta^{1/q}}{n^{1/q}} \right) . \end{aligned}$$

Splitting this event, we get easily for $\varepsilon = \frac{\delta^{1/q}}{n^{1/q}} \le 1$

$$\mathbb{P}\left(\left| \frac{S_n^{(2)}}{S_n^{(1)}} \frac{\zeta_n^k}{\zeta_n^{k+1}} - 1 \right| > \varepsilon \right) \le \mathbb{P}\left(\left| \frac{S_n^{(2)}}{S_n^{(1)}} - 1 \right| > \varepsilon/3 \right) + \mathbb{P}\left(\left| \frac{\zeta_n^1}{\zeta_n^2} - 1 \right| > \varepsilon/3 \right) .$$

Recalling Proposition 4.3 (4), the first term is

$$\mathbb{P}(|\mathcal{R}_n' - 1| > \varepsilon/3) = O((1-\varepsilon^2/81)^{n/2}) .$$

. For the second term we need a lemma.

Lemma 5.4. *Let U_1 and U_2 be independent and distributed as $\|x\|^2$ under ν_n. If Assumption 2.1 holds, then there exist $d_1', d_2', \alpha > 0$ and $\rho_0 \in (0,1)$ such that for any $k \ge 1, n \ge 1$ and $\rho \in (0, \rho_0)$*

$$\mathbb{P}\left(\left| \frac{U_1}{U_2} - 1 \right| \ge \rho \right) \le d_1' \exp(-n d_2' \rho^\alpha). \tag{5.11}$$

From (5.2) and Lemma 5.4, the second term is $O\big(\exp(-cn\varepsilon^\alpha)\big)$, where c is some positive constant. Gathering all these bounds we get that for every n

$$\mathbb{P}\left(\sum_{k=1}^{n} \left| \frac{S_n^{k+1}}{S_n^k} \frac{\zeta_n^k}{\zeta_n^{k+1}} - 1 \right|^q > \delta \right) \le c_1 n \exp\left(-c_2 n^{1-\frac{\alpha}{q}} \right) .$$

where c_1 and c_2 are positive constants. For $q > \alpha$, we get a convergent series, so (5.10) holds true, which ends the proof of Lemma 5.3. □

Proof of Lemma 5.4. It is easy to see that for any $\rho \in (0,1)$, $|U_2/U_1 - 1| \geq \rho$ only if $|U_1 - 1| \geq \rho/4$ or $|U_2 - 1| \geq \rho/4$. The lemma now follows from Assumption 2.1 and the union bound. □

5.2.3. *Proof of Theorem 5.2.* (1) From (5.9) and Proposition 4.1, the sequence $\left(R_k^{(n)} - 1, k \geq 1\right)$ converges a.s. in ℓ_q to $(\mathcal{R}_k - 1, k \geq 1)$. Let g be a fixed integer and

$$\widetilde{M}_n^g := \inf_{k \geq g+1} R_k^{(n)},$$

so that $\widetilde{M}_n^g = M_n^g \wedge 1$. This yields $0 \leq M_n^g - \widetilde{M}_n^g = (M_n^g - 1)^+ \leq (R_{n-1}^{(n)} - 1)^+$. Since $R_{n-1}^{(n)} \xrightarrow{P} 1$ (by 3.19), we get

$$M_n^g - \widetilde{M}_n^g \xrightarrow{P} 0, \tag{5.12}$$

and so, M_n^g and $\widetilde{M}_n^g$ have the same limit behavior.

Since the mapping $(c_k)_{k \geq 1} \in \ell_q \longmapsto \inf_{k \geq g} c_k$ is continuous, by Lemma 5.3 one has

$$\widetilde{M}_n^g \xrightarrow[n]{a.s.} \mathcal{M}^g. \tag{5.13}$$

Thanks to (5.12), we obtain $M_n^g \xrightarrow{P} \mathcal{M}^g$ and then by (5.8) $\mathcal{M}_n^g \xrightarrow[n]{(d)} \mathcal{M}^g$.

(2) We take $g = 1$ for the sake of simplicity. Recall that

$$\mathcal{I}_n^1 = \min\{i \in \{1, \ldots, n-2\} : r_i^{(n)} = \min\{r_j^{(n)}, j \in \{1, \ldots, n-1\}\}.$$

For $a \in [0, \infty)^{\mathbb{N}}$, let

$$\min \operatorname{argmin} a := \min\{i \geq 1 : a_i = \inf_{j \geq 1} a_j\}$$

where as usual set $\min \emptyset = \infty$. If we set $I_n^1 = \min \operatorname{argmin} \{R_j^{(n)}, j \geq 1\}$, we have

$$I_n^1 \wedge n \stackrel{(d)}{=} \mathcal{I}_n^1. \tag{5.14}$$

We know that a.s. $\mathcal{M}^0 < 1$ so that for n large enough, we have $M_n^0 < 1$, hence $I_n^1 \wedge n = I_n^1$. Now, from Lemma 5.3, a.s $\lim R^{(n)} = \mathcal{R}$ in ℓ_q, and from Proposition 4.2(4), $\#\text{argmin}\ (\mathcal{R}) = 1$. It is straightforward that the convergence of y_n to y in ℓ_q implies the convergence of $\min \operatorname{argmin}\ (y_n)$ to $\operatorname{argmin}\ (y)$ if $\#\text{argmin}\ (y) = 1$. Hence, a.s. $\lim I_n^1 \wedge n = \mathcal{I}^1$. Thanks to (5.14), we conclude $\mathcal{I}_n^1 \xrightarrow[n]{(d)} \mathcal{I}^1$.

(3) Since a.s. $(\mathcal{R}_k - 1, k \geq 1) \in \ell_q$, it is clear that $\mathcal{M}^K$ tends to 1 a.s. as K tends to infinity. For every $\varepsilon > 0$ it is then possible to find K such that

$$\mathbb{P}(\mathcal{M}^K \leq 1 - \varepsilon) \leq \varepsilon\,.$$

For n large enough, one then has, by (5.13) and (5.12),

$$\mathbb{P}(M_n^K \leq 1 - 2\varepsilon) \leq 2\varepsilon\,.$$

Since the function $k \mapsto M_n^k$ is non-decreasing, one has, for n large enough such that $g(n) \geq K$,

$$\mathbb{P}(M_n^{g(n)} \leq 1 - \varepsilon) \leq 2\varepsilon\,,$$

i.e. $M_n^{g(n)} \xrightarrow{P} 1$. With the help of (5.8), we conclude $\mathcal{M}_n^{g(n)} \xrightarrow[n]{(d)} 1$. $\square$

6. LLL reductions and QR decompositions

6.1. **LLL reduction of a lattice.** If $B = [b_1^{(n)}, \cdots, b_p^{(n)}]$ is the $n \times p$ matrix with column vectors $b_1^{(n)}, \cdots, b_p^{(n)}$ in the canonical basis, it can be decomposed in a unique way as $B = QR$ where

- $R = [R_{i,j}] \in \mathbb{R}^{p \times p}$ is upper-triangular, $R_{i,j} = 0$ for $j < i$ and $R_{i,i} > 0$,
- $Q \in \mathbb{R}^{n \times p}$ is isometric i.e. $Q'Q = I_p$.

The relation with the Gram-Schmidt orthogonalization is

$$Q = \left[\frac{\widehat{b}_1^{(n)}}{\|\widehat{b}_1\|}, \dots, \frac{\widehat{b}_p^{(n)}}{\|\widehat{b}_p\|}\right]$$

$$R_{jj} = \|\widehat{b}_j\|, \quad R_{k,j} = \frac{\langle b_j^{(n)}, \widehat{b}_k^{(n)}\rangle}{\|\widehat{b}_k^{(n)}\|}\ ,\ 1 \leq k < j \leq p\,. \tag{6.1}$$

Let us consider the differences between the definition of LLL reduction we consider here and the original definition introduced by Lenstra-Lenstra-Lovász in [**?**].

Firstly in the original definition the basis has also to be *proper*[2] or *size-reduced*, i.e.

$$|R_{k,j}| \leq \frac{1}{2} R_{k,k}\ ,\ 1 \leq k < j \leq p\,. \tag{6.2}$$

But from any basis satisfying (1.2) one efficiently obtains a proper basis still satisfying (1.2) by a straightforward sequence of integer translations provided in subsection 6.3.

[2]Considering the notion of *flag* ([**?**]) rather than basis for lattices, makes it possible to skip the notion of properness.

Secondly the approximation parameter of the original LLL in [**?**] is slightly different from ours and the reduction we consider here is indeed Siegel reduction as called in [**?**, **?**]. Our main Theorem 2.2 is still true with the original definition of a LLL reduced basis as detailed in subsection 6.2.

6.2. **LLL(δ)-reduced basis versus Siegel(s)-reduced basis.**

Definition 6.1. *Let $\delta \in (1/4, 1]$. The basis $\mathbf{b}_p^{(n)}$ is called truly–LLL(δ) reduced if it is proper (see* (6.2)*) and if*

$$\delta R_{k,k}^2 \le R_{k,k+1}^2 + R_{k+1,k+1}^2 \quad \textit{for} \quad k = 1, \ldots, p-1\,, \tag{6.3}$$

or equivalently

$$\delta \|\widehat{b}_k^{(n)}\|^2 \le R_{k,k+1}^2 + \|\widehat{b}_{k+1}^{(n)}\|^2 \quad \textit{for} \quad k = 1, \ldots, p-1\,. \tag{6.4}$$

From the above definition and the definition of a LLL(s)-reduced basis (1.1), and since $4R_{k,k+1}^2 \le \|\widehat{b}_k^{(n)}\|^2$ (thanks to properness) one deduces immediately:

Proposition 6.2. (*i*) *If a basis is LLL(s) reduced with $s \in (0, 1)$ and proper, then it is truly–LLL(δ) reduced with $\delta = s$.*

(*ii*) *If a basis is truly–LLL(δ) reduced then it is LLL(s) reduced with $s = \sqrt{\delta - 1/4}$.*

6.3. **How to make a basis proper while preserving its LLL reduceness.**

The Make–proper algorithm:

Input: A basis $\mathbf{b} = (b_1, \ldots, b_p)$ of a lattice L.
Output: A proper basis $\mathbf{b}$ of the lattice L.
Initialization: Compute the orthogonalized system $\widehat{\mathbf{b}}$ and the matrix R.
For i from 2 to n do
  For j from (i-1) downto 1 do
    $b_i := b_i - \lfloor \frac{R_{j,i}}{R_{j,j}} \rceil b_j$ ($\lfloor x \rceil$ is the integer nearest to x).

Clearly the Gram-Schmidt basis associated with the input basis is preserved under the integer translations of the above algorithm. So the Gram Schmidt basis associated with the output basis is the same as the one associated with the input basis and the Make–proper algorithm preserves LLL(s)-reduceness and truly–LLL(s)-reduceness.

6.4. **A brief description of the LLL algorithm.**

In this subsection, we provide a simple formulation of the LLL(δ) algorithm. Clearly, from Proposition 6.2 if the input basis is LLL(s)-reduced the following algorithm will stop after one iteration of the **while** loop (which makes the basis proper).

The LLL(δ)-reduction algorithm:

Input: A basis $\mathbf{b} = (b_1, \ldots, b_p)$ of a lattice L.
Output: A $LLL(\delta)$-reduced basis $\mathbf{b}$ (or a truly LLL(s)-reduced basis) of the lattice L.
Initialization: Compute the orthogonalized system $\widehat{\mathbf{b}}$ and the matrix R.
$\mathbf{i := 1}$;
While $\mathbf{i < n}$ **do**
  $b_{i+1} := b_{i+1} - \lfloor \frac{R_{i,i+1}}{R_{i,i}} \rceil b_i$ ($\lfloor x \rceil$ is the integer nearest to x).
  Test: $\|\widehat{b}_{i+1}\| > s\|\widehat{b}_i\|$? (or $\|\widehat{b}_{i+1}\|^2 + R^2_{i,i+1} > \delta\|\widehat{b}_i\|^2$?)
    If true, make $(b_1, \ldots, b_{i+1})$ proper by **Make-proper**; **set** $\mathbf{i := i + 1}$;
    If false, swap b_i and b_{i+1}; update $\widehat{\mathbf{b}}$ and R; if $i \neq 1$ then **set** $\mathbf{i := i - 1}$;.

7. Extensions

We quote here two possibilities of extension of the above considerations on random bases. We do not give proofs since they are straightforward and do not bring any new concept or technical difficulty.

7.1. **Segment reduction.** In [**?**], Koy and Schnorr proposed the concept of segment LLL-reduction in which a basis $b_1^{(n)}, \ldots, b_n^{(n)}$ of dimension $n = dm$ is partitioned into m segments $B_\ell = [b_{d\ell+1}^{(n)}, \ldots b_{(d+1)\ell}^{(n)}]$, $\ell = 1, \ldots, m$ of d consecutive basis vectors. They adapt the LLL algorithm, improving the time bound. They perform local reduction of consecutive segments B_{r-1}, B_r. They defined the local Gramian determinant of B_r as

$$D(r) = \|\widehat{b}_{d(r-1)+1}^{(n)}\|^2 \cdots \|\widehat{b}_{dr}^{(n)}\|^2$$

and are interested in the quotients $D(r)/D(r+1)$, $r \geq 1$. It is straightforward to extend our results, thanks to the strong independence of vector lengths. Let

$$\mathcal{M}_{d,n}^g = \inf_{r:(r+1)d \leq n-g} \frac{D(r+1)}{D(r)} \tag{7.1}$$

As in Theorem 2.2, under a spherical model, if $g = g(n)$ tends to ∞ and the block size d is fixed, then for any $s \in [0, 1]$

$$\mathbb{P}\Big(\mathcal{M}_{d,n}^g \geq s^2\Big) \to 1\,;$$

if g is constant, then this probability tends to a constant in $[0, 1]$ (depending on s, g and d), or in other words, the random variable $\mathcal{M}_{d,n}^g$ converges in distribution.

Proposition 5.1 and Theorem 5.2 have their analogous for the reduction by segments. Set

$$r_{d,j}^{(n)} := \frac{D(m-j)}{D(m-j-1)} \quad \text{(recall } n = dm)$$

for j such that $g+1 \leq dj \leq dm-1$ and $r_{d,j}^{(n)} := 1$ for j such that $dj \geq dm$. Then when $m \to \infty$ (hence $n \to \infty$), we have convergence of $(r_{d,j}^{(n)},\ j \geq 1)$ to a process $(\mathcal{R}_{d,j},\ j \geq 1)$ with

$$\mathcal{R}_{d,j} = \frac{\eta_{d,j}}{\eta_{d,j+1}}\ ,\ \eta_{d,j} \stackrel{(d)}{=} \gamma(j/2)\gamma((j+1)/2)\cdots\gamma((j+d-1)/2)\,,$$

where the $\eta_{d,j}, j \geq 1$ are independent, and the gamma variables too. Then by setting

$$\mathcal{M}_{d,n}^{g} = \min_{j: g+1 \leq dj \leq n-1} r_{d,j}^{(n)}\ ,\quad \widetilde{\mathcal{M}}_{d}^{g} := \inf\left\{\mathcal{R}_{d,j}, dj \geq g+1\right\}.$$

one obtains also an analogous to Theorem 5.2.

7.2. **Complex or quaternionic bases.** In the complex LLL (see [**?**]) vectors are chosen in $\mathbb{C}^n$. If we consider random basis, we have similar results but the square length of a vector is now γ_n distributed and in all our results, the $\gamma_{1/2}$ distribution has to be replaced by a γ_1 (i.e. exponential) distribution. It is also possible to study quaternionic vectors and the LLL algorithm in the same framework (see [**?**]). The distribution involved would be γ_2 distributed.

8. Orthogonality Defect and Random Matrix Theory

If $\mathbf{b}_p^{(n)}$ is picked with distribution $\mathbb{G}_n$, the matrix $B'B$ has a Wishart distribution. If it is picked with distribution $\mathbb{U}_n^S$, the matrix $B'B$ has the so-called Uniform Gram distribution. These distributions are well known in statistics ([**?**], [**?**]) and the studies of these random matrices have recently been the topic of many papers[3]. It is straightforward from Definition 1.4 that the orthogonality index has the same distribution under all spherical models. It is then sufficient to consider $\mathbb{U}_n^S$, and in this case $\rho_{p,n}^{-2} = \det B'B$. The random matrix $B'B$ has a distribution called Uniform Gram Ensemble and its determinant was studied in [**?**]. The decomposition (1.4) in a product of independent random variables with beta distribution (Theorem 3.2), known as a Bartlett-type decomposition, makes possible, taking logarithms, to apply limit theorems on triangular arrays. The regime used (as frequently in recent works in Random Matrix Theory) is $p, n \to \infty$ such that $p/n \to t \in [0,1]$.

We now translate some of the results obtained there to get the asymptotic behavior of $\rho_{p,n}$ as $n \to \infty$. The first result corresponds to $g(n) = n - \lfloor nt \rfloor \to \infty$ and the second one corresponds to $g = 0$. It is clear that for $g \neq 0$ fixed, we would obtain results similar to (2). Notice that the result of simulation in Tab. 8.1 p.147 of [**?**] is in accordance with (8.4).

Theorem 8.1 (Rouault [**?**] Theorem 3.1)**.** *The following convergences hold*

[3]For the algorithmic point of view see an excellent survey in [**?**]

(1) *For $t \in [0,1)$, as $n \to \infty$,*

$$\mathbb{E}(\log \rho_{[nt],n}) = \frac{n}{2}\mathcal{A}(t) + O(1) \tag{8.1}$$

where $\mathcal{A}(t) := t + (1-t)\log(1-t)$. Moreover

$$\lim_n \sup_{t\in[0,1]} \left| \frac{\log \rho_{\lfloor nt \rfloor}}{n} - \frac{\mathcal{A}(t)}{2} \right| = 0\,, \tag{8.2}$$

in distribution.

(2) *For the full basis, we have*

$$\mathbb{E}(\log \rho_{n,n}) - \frac{n}{2} - \frac{1}{4}\log n \quad \xrightarrow[n]{} \quad C \quad \text{where } C \text{ is some constant.} \tag{8.3}$$

$$(\rho_{n,n})^{1/n} \quad \xrightarrow[n]{(d)} \quad e^{1/2}\,. \tag{8.4}$$

Theorem 8.2 (Rouault [?] Theorem 3.2)**.** *Let*

$$\xi_n(t) := \log \rho_{[nt],n} - E \log \rho_{[nt],n} \quad , \quad t \in [0,1)\,.$$

1) *The sequence of processes $(\xi_n)_n$ converges in distribution in $D([0,1))$, the space of càdlàg functions on $[0,1)$ equipped with the Skorohod topology to $(G(t), t \in [0,1))$ which is a Gaussian process with continuous paths, independent increments, and variance $v(t) = \frac{1}{2}\log\frac{1}{1-t} - \frac{t}{2}$. If W denotes the standard Brownian motion, we have*

$$\begin{aligned}(G(t), t\in[0,1)) &\stackrel{(d)}{=} \big(W_{v(t)}\ ,\ t \in [0,1)\big)\\ &\stackrel{(d)}{=} \Big(\int_0^t \sqrt{\frac{s}{2(1-s)}}\, dW_s\ ,\ t\in[0,1)\Big)\,.\end{aligned}$$

2) *Let*

$$\xi_n := \frac{\log \rho_{n,n} - \frac{n}{2} - \frac{1}{4}\log n}{\sqrt{\log n}}$$

Then, as $n \to \infty$, ξ_n converges in distribution to a random variable N independent of the process G and $\mathcal{N}(0,1/2)$ distributed.

There is also a principle of large deviations but we omit it here, not to lengthen this paper.

References

LIAFA, Université Denis Diderot- Case 7014, 2 place Jussieu, 75251 Paris Cedex 05

E-mail address, A. Akhavi: akhavi@liafa.jussieu.fr

LABRI, Université Bordeaux I, 351 cours de la Libération, 33405-Talence cedex

E-mail address, J-F. Marckert: marckert@labri.fr

LMV UMR 8100, Université Versailles-Saint-Quentin, 45 Avenue des Etats-Unis, 78035-Versailles Cedex

E-mail address, A. Rouault: Alain.Rouault@math.uvsq.fr