COMMENT ON "SUM OF SQUARES OF UNIFORM RANDOM VARIABLES" BY I. WEISSMAN

PETER J. FORRESTER

Abstract. The recent paper by I. Weissman, "Sum of squares of uniform random variables", [Statist. Probab. Lett. **129** (2017), 147–154] is compared to earlier work of B. Tibken and D. Constales relating to the area of the intersection of a centred ball and cube in $\mathbb{R}^n$, published in the Problems and Solutions section of SIAM Review in 1997. Some recent applications of explicit formulas for the corresponding probabilities from these references, to problems in lattice reduction, and to the study of Lyapunov exponents of products of random matrices, are noted.

1. Introduction

A recent paper in this journal by Weissman [13] addresses the question of the distribution of the sum of the squares of n independent uniform random variables in $[0, 1]$. It is stated in the Introduction of [13] that there is nothing in the published literature dealing with this problem. While this may be true in literal terms, the solution to an equivalent question within geometrical probability has been available in the literature since 1997, in the form of two answers to a particular problem posed in the section "Problems and Solutions" of SIAM Review [10].

The purpose of this note is to explicitly connect [10] with the topic of [13], to isolate from [10] formulas which supplement those obtained in [13], and to indicate some recent developments in the form of both applications and new theory.

2. Comparison of results

Let U_i, $1 \le i \le N$ be independent, uniformly distributed random variables on $[0, 1]$, and set

$$S_N = \sum_{i=1}^{N} U_i^2. \tag{2.1}$$

With $\chi_J = 1$ for J true, $\chi_J = 0$ otherwise, one sees immediately that [13, Eq. (7)]

$$\begin{aligned} F_N(s) := \Pr\left(S_N \le s\right) &= \int_0^1 dx_1 \cdots \int_0^1 dx_N \, \chi_{\sum_{j=1}^N x_j^2 \le s} \\ &= \mathrm{Vol}\left(C_N([0,1]) \cap B_N(\sqrt{s})\right), \end{aligned} \tag{2.2}$$

where $C_N([a,b])$ denotes the cube in $\mathbb{R}^N$, $[a,b]^N$, and $B_N(r)$ denotes the ball in $\mathbb{R}^N$, centred at the origin and of radius r. By symmetry and scaling this can be written

$$\begin{aligned} F_N(s) &= 2^{-N}\mathrm{Vol}\left(C_N([-1,1]) \cap B_N(\sqrt{s})\right) \\ &= 2^{-N} s^{N/2} \mathrm{Vol}\left(C_N([-1/\sqrt{s}, 1/\sqrt{s}]) \cap B_N(1)\right). \end{aligned} \tag{2.3}$$

The Problems and Solutions section of volume 39 of SIAM Review, published in 1997 [10], contained solutions by B. Tibken and D. Constales of Problem 96-19 as posed by Liqun Xu: "What is the volume of the intersection of a cube and a ball in N-space? Assume that the cube and the ball have a common centroid and that neither of the two bodies is large enough to contain the other completely? This problem arises in the study of certain probability distributions." One sees that (2.3) is precisely the geometric quantity as sought by Xu.

The explicit form for $N = 2$,

$$F_N(s) = \begin{cases} \frac{1}{4}\pi s, & 0 \le s \le 1 \\ \sqrt{s-1} + (\pi/4 - \arccos\left(1/\sqrt{s}\right))s, & 1 \le s \le 2 \\ 1, & 2 \le s. \end{cases} \tag{2.4}$$

was derived in both the solutions of Tibken and Constales (for the latter use needs to be made of the second equality in (2.3)). This is [13, Eq. (10)]. In relation to $N = 3$, let

$$h(a) = 8a^2\sqrt{1-2a^2} + 2(3a - a^3)\Big(4\mathrm{arcsin}\left(\frac{a}{\sqrt{1-a^2}}\right) - \pi\Big) - 8\mathrm{arcsin}\left(\frac{a^2}{1-a^2}\right) + \frac{4\pi}{3}.$$

From the solution of Tibken, Eq. (23), we read off that

$$\mathrm{Vol}\left(C_N([-a,a]) \cap B_N(1)\right) = \begin{cases} 8a^3, & 0 \le a < 1/\sqrt{3} \\ h(a), & 1/\sqrt{3} \le a < 1/\sqrt{2} \\ \pi(6a - 2a^3 - 8/3), & 1/\sqrt{2} \le a \le 1 \\ 4\pi/3, & 1 \le a. \end{cases} \tag{2.5}$$

Recalling the 2nd equality in (2.3), we see this is equivalent to [13, Eq. (13)].

For general N, using a method based on Fourier series, it was proved by Constales[1] that

$$F_N(s) = \left(\frac{1}{6} + \frac{s}{N} + \frac{1}{\pi}\mathrm{Im}\sum_{k=1}^{\infty}\Big(\frac{C(\sqrt{2\pi k/N}) - iS(\sqrt{2\pi k/N})}{\sqrt{2\pi k/N}}\Big)^N \frac{e^{2\pi i k s/N}}{k}\right). \tag{2.6}$$

[1] after the correction $2\sqrt{k/N} \mapsto \sqrt{2\pi k/N}$ for all quantities relating to the power of N in the sum, as alerted to me by E. Postlethwaite, and as is consistent with [1, Th. 4]

Here $S(x) = \int_0^x (\sin t^2)\,\mathrm{d}t$ and $C(x) = \int_0^x (\cos t^2)\,\mathrm{d}t$ denote the Fresnel integrals. Let $\mathcal{L}(F_N)(s) := \int_0^\infty F_N(t)e^{-st}\,\mathrm{d}t$ denote the Laplace transform of F_N. Constales also remarks that

$$\mathcal{L}(F_N)(s) = \frac{2^{-N}\pi^{N/2}(\operatorname{erf}\sqrt{s})^N}{s^{N/2+1}},$$

and thus by the inversion formula for the Laplace transform

$$F_N(t) = 2^{-N}\frac{\pi^{N/2}}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{(\operatorname{erf}\sqrt{s})^N}{s^{N/2+1}}e^{st}\,\mathrm{d}s, \qquad c > 0. \tag{2.7}$$

It is commented too that the central limit theorem applied to (2.1) implies that for large N, $F_N'(s)$ has the form of the normal distribution $\mathrm{N}[N/3, 2\sqrt{N/45}]$ cf. the first sentence of [13, §2].

Using a method based on the Fourier integral rather than Fourier series, it was proved by Tibken that for general N

$$F_N(s) = s^{N/2}\Big(\frac{1}{2\pi}\Big)^{N/2}\int_{\mathbb{R}^N}\frac{J_{N/2}((\sum_{j=1}^N y_j^2)^{1/2})}{(\sum_{j=1}^N y_j^2)^{N/4}}\prod_{j=1}^N\frac{\sin(y_j/\sqrt{s})}{y_j}\,\mathrm{d}y_1\cdots\mathrm{d}y_N \tag{2.8}$$

(this is Eq. (13) in Tibken with use required too of (2.3) since Tibken computes the quantity $\mathrm{Vol}\,(C_N([-a,a])\cap B_N(1))$). Here $J_p(z)$ denotes the Bessel function of order p. Moreover, with

$$I_a(\lambda,0) = \Big(\pi\operatorname{erf}\Big(\frac{a}{2\sqrt{\lambda}}\Big)\Big)^n, \qquad I_a(\lambda,k) = (-1)^k\frac{\partial^k}{\partial\lambda^k}I_a(\lambda,0),$$

and $L_n^{(k)}(x)$ denoting the classical Laguerre polynomial, it was shown in Eq. (33) of Tibken's work that (2.8) can be reduced to

$$2^N s^N F_N(1/s^2) = \pi^{-N/2}\bigg(\frac{I_s(1/(2N+4),0)}{\Gamma(N/2+1)} + \sum_{k=2}^\infty\frac{L_k^{N/2}(N/2+1)I_s(1/(2N+4),k)}{\Gamma(k+N/2+1)(2N+4)^k}\bigg). \tag{2.9}$$

3. Applications

3.1. **Complex lattice reduction.** Let $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ be a basis in $\mathbb{R}^n$. Associated with $\mathcal{B}$ is the lattice

$$\mathcal{L}_\mathcal{B} = \Big\{n_1\mathbf{b}_1 + n_2\mathbf{b}_2 + \cdots + n_N\mathbf{b}_N \,\Big|\, n_i \in \mathbb{Z}\ (i = 1,\ldots,N)\Big\}. \tag{3.1}$$

For dimensions $N \geq 2$, there are an infinite number of bases giving the same lattice. A basic question is to determine a basis — referred to as a reduced basis — consisting of short and/ or near orthogonal vectors. In two dimensions the Lagrange–Gauss lattice reduction

algorithm (see e.g. [2]) performs this task, and converges to basis vectors $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ with the property that

$$||\boldsymbol{\alpha}|| \le ||\boldsymbol{\beta}||, \qquad \Big| \frac{\boldsymbol{\alpha} \cdot \boldsymbol{\beta}}{||\boldsymbol{\alpha}||^2} \Big| \le \frac{1}{2}. \tag{3.2}$$

It is well known, and straightforward to verify, that the inequalities (3.2) imply that these basis vectors are the shortest possible. Probabilities and volumes can be introduced into this setting by introducing the notion of a random basis, as then the reduced basis is given by a probability distribution. The most natural meaning of a random basis, normalised to have a unit cell with volume unity, is to choose the matrix M of lattice vectors from $\mathrm{SL}_N(\mathbb{R})$, endowed with a Haar measure as identified by Siegel [12].

The problem of computing (2.2) shows itself for $N = 2$ in this context by considering the lattice reduction problem for a complex analogue of (3.1) in two-dimensions. Specifically, one requires that $\mathbf{b}_1$, $\mathbf{b}_2$ be linearly independent vectors in $\mathbf{C}^2$, and chooses $n_1, n_2 \in \mathbb{Z}[i]$, and thus as Gaussian integers. In a QR (Gram-Schmidt) parametrisation, the matrix of basis vectors is decomposed $M = UT$, where $U \in \mathrm{SU}(2)$ and

$$T = \begin{bmatrix} t_{11} & t_{12}^{(r)} + i t_{12}^{(i)} \\ 0 & t_{22} \end{bmatrix}, \qquad t_{11} > 0, \quad t_{22} = 1/t_{11}.$$

Here we think of U as rotating the lattice so that $\mathbf{b}_1 = (r_{11}, 0)$, $\mathbf{b}_2 = (t_{12}^{(r)} + i t_{12}^{(i)}, t_{22})$. After integrating over the variables associated with U, and t_{22}, and introducing $t_{11} = t$, $t_{12}^{(r)} = y_1$, $t_{12}^{(i)} = y_2$, for notational convenience, the invariant measure restricted to the domain of the shortest reduced basis is equal to [6, Eq. (4.26)]

$$(2\pi^2) t \chi_{\|\mathbf{y}\|^2 \ge t^2 - 1/t^2} \chi_{|y_1| \le t/2} \chi_{|y_2| \le t/2} \mathrm{d}t \mathrm{d}y_1 \mathrm{d}y_2. \tag{3.3}$$

As noted in [6], with $V_2(a, b)$ denoting the area of overlap between a disk of radius a, and a square of side length b, both centred at the origin, (3.3) upon integration over y_1 and y_2 can be written

$$(2\pi^2) \Big(t^3 \chi_{0<t<1} + \chi_{t>1} t \left(t^2 - V_2 \left((t^2 - 1/t^2)^{1/2}, t/2 \right) \right) \Big) \mathrm{d}t. \tag{3.4}$$

Use of (2.4) and (2.3) in (3.4) allows for the determination of the explicit functional form of V_2, which up to normalisation corresponds to the PDF of the length of the shortest lattice vector. The latter quantity can be realised as a numerically generated histogram, by Monte Carlo sampling from $\mathrm{SL}_2(\mathbb{C})$ with Haar measure, and then use of the complex Lagrange–Gauss lattice reduction algorithm to determine the shortest basis for each sample; see [6, §6].

3.2. **Lyapunov exponents.** Let $\mathbf{r}_i \in \mathbb{R}^3$ $(i = 1, 2, 3)$ be sampled uniformly from the unit sphere in $\mathbb{R}^3$; this can be done for example by setting $\mathbf{r}_i = (x_i, y_i, z_i)/\sqrt{x_i^2 + y_i^2 + z_i^2}$, where each of x_i, y_i, z_i are independent standard normal random variables. Specify an element of the ensemble of 2×2 random matrices U_2^B by forming $\begin{bmatrix} x_1 & y_1 \\ x_2 & y_2 \end{bmatrix}$, and thus restricting $\mathbf{r}_1$, $\mathbf{r}_2$ to the first two components along each row. Specify an element of the ensemble of 3×3 random matrices U_3^S by forming

$$\begin{bmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{bmatrix},$$

and so placing the components of $\mathbf{r}_i$ along each row in order. The ensembles U_2^B and U_3^S both have the property that the distribution of any member, X_i say, is unchanged by multiplication by an appropriately sized real orthogonal matrix on the right. As such, the Lyapunov exponent μ_1, defined as

$$\mu_1 = \lim_{m\to\infty} \frac{1}{m} \log \max_{||\mathbf{v}||=1} ||X_m X_{m-1} \cdots X_1 \mathbf{v}||, \tag{3.5}$$

is given by the simple formula [3]

$$2\mu_1 = \int_0^\infty (\log t) p(t)\, \mathrm{d}t,$$

where $p(t)$ is the PDF for $\sum_{i=1}^p x_i^2$, $(p = 2, 3)$, corresponding to the sum of the squares of the entries in the first column of any X_i.

We know from [7, Prop. 6] that both the ensembles U_2^B and U_3^S have each x_i uniformly distributed on $[-1, 1]$ and thus $p(s) = F_N'(s)$ for $N = 2$, $N = 3$ respectively. Consequently for U_2^B, using (2.4)

$$\begin{aligned} 2\mu_1 &= \frac{\pi}{4} \int_0^1 \log s \, \mathrm{d}s + \int_1^2 \Big(\arcsin\Big(\frac{1}{\sqrt{s}}\Big) - \frac{\pi}{4} \Big) \log s \, \mathrm{d}s \\ &\approx -0.736056. \end{aligned} \tag{3.6}$$

And for U_3^S, as implied by (2.5) and (2.3), or more explicitly by [13, Eq. (14)], with the notation

$$\begin{aligned} f_{3,2}(s) &= 3\Big(\arcsin\Big(\frac{1}{\sqrt{s-1}}\Big) - \frac{\pi}{4}\Big) + \sqrt{s}\Big(\arctan\sqrt{\frac{s-2}{s}} - \arctan\sqrt{\frac{1}{s(s-2)}}\Big), \\ &= 3\Big(\arcsin\Big(\frac{1}{\sqrt{s-1}}\Big) - \frac{\pi}{4}\Big) + \sqrt{s}\Big(\frac{\pi}{4} - \frac{3}{2}\arcsin\Big(\frac{1}{s-1}\Big)\Big) \end{aligned}$$

we have

$$2\mu_1 = \frac{\pi}{4}\int_0^1 s^{1/2}\log s\,\mathrm{d}s + \frac{\pi}{4}\int_1^2 (3-2s^{1/2})\log s\,\mathrm{d}s + \int_2^3 f_{3,2}(s)\log s\,\mathrm{d}s$$
$$\approx -0.187705. \tag{3.7}$$

Numerical methods similar to those used in [5, §4], which are based on the definition (3.5), can be used to obtain Monte Carlo estimates of (3.6) and (3.7), and so realising the numerical values to several decimal places.

3.3. **Random sampling — lattice enumeration with discrete pruning.** In subsection 3.1, attention was drawn to the problem of determining a reduced basis for a general lattice (3.1). A more modest aim, but one with wide applicability — for example to lattice based cryptography [9] — is to find a nonzero lattice vector of the smallest norm. This is the so-called shortest vector problem. In the enumeration approach to the shortest vector problem [4], the basic idea is to perform a depth-first search on a tree whose leaves correspond to lattice points, and internal nodes to coefficients of the integer combination practical improvement is to restrict the exhaustive search to a subset of possible solutions, by pruning subtrees of the tree for which the "probability" of finding the shortest vector is small [11]. In [1] a different pruning set to that in [11] is introduced. Analysis of the algorithm requires computing

$$\mathrm{Vol}\Big(\prod_{l=1}^N [\alpha_l,\beta_l]\cap B_N(1)\Big), \qquad \prod_{l=1}^N [\alpha_l,\beta_l] := \{(x_1,\dots,x_N):\ x_l\in[\alpha_l,\beta_l]\ (l=1,\dots,N)\}$$

(cf. (2.3)). Aono and Nguyen [1] give generalisations of each of Constales formulas (2.6), (2.7), and Tibken's formula (2.9). The simplest is the generalisation of (2.7), which reads

$$\mathrm{Vol}\Big(\prod_{l=1}^N [\alpha_l,\beta_l]\cap B_N(1)\Big) = \frac{\pi^{N/2}}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{e^s}{s^{N/2+1}}\prod_{j=1}^N \frac{(\mathrm{erf}(\beta_j\sqrt{s})-\mathrm{erf}(\alpha_j\sqrt{s}))}{2(\beta_j-\alpha_j)}\,\mathrm{d}s, \tag{3.8}$$

for suitable c. The efficient numerical computation of (3.8) is discussed in detail in [1].

Acknowledgements

This research project is part of the program of study supported by the ARC Centre of Excellence for Mathematical & Statistical Frontiers, and the Australian Research Council Discovery Project grant DP170102028. The referee of the published form of this work [Statist. Probab. Lett. **129** (2018), 147–154] is to be thanked for picking up a number of errors relative to the original arXiv posting. However, this report was unfortunately missed at the time, and not acted on until now. Most recently (11$^{\text{th}}$ August, 2022) Eamonn Postlethwaite alerted

me to the error in the form of (2.6) as reported in Constales article from 1997, which was copied into my original arXiv posting, and is now fixed.

References

[1] Y. Aono Y. and P.Q. Nguyen, *Random Sampling Revisited: Lattice Enumeration with Discrete Pruning*. In: Coron JS., Nielsen J. (eds) Advances in Cryptology — EUROCRYPT 2017. Lecture Notes in Computer Science, vol 10211. Springer, Cham, 2017.

[2] M.R. Bremner, *Lattice basis reduction: an introduction to the LLL algorithm and its applications*, CRC Press, Boca Raton, FL, 2012.

[3] J.E. Cohen and C.M. Newman, *The stability of large random matrices and their products*, The Annals of Prob. **12** (1984), 283–310.

[4] U. Finke and M. Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comp. **44** (1985), 463–471.

[5] P.J. Forrester, *Lyapunov exponents for products of complex Gaussian random matrices*, J. Stat. Phys. **151** (2013) , 796–808.

[6] P.J. Forrester and J. Zhang, *Volumes and distributions for random unimodular complex and quaternion lattices*, J. Numb. Th. **190** (2018), 1–39.

[7] P.J. Forrester and J. Zhang, *Lyapunov exponents for some isotropic random matrix ensembles*, J. Stat. Phys. **180** (2020), 558–575.

[8] N. Gama, P.Q. Nguyen, O. Regev, *Lattice Enumeration Using Extreme Pruning*. In: Gilbert H. (eds) Advances in Cryptology. EUROCRYPT 2010. Lecture Notes in Computer Science, vol 6110. Springer, Berlin, Heidelberg, 2010

[9] P.Q. Nguyen, *Public-key cryptoanalysis*. In: Luengo, I. (ed.) Recent trends in Cryptography. Contemporary Mathematics, vol. 477, AMS-RSMEm 2009.

[10] C.C. Rousseau and O.G. Ruehr, *Problems and solutions. subsection: The volume of the intersection of a cube and a ball in N-space. two solutions by Bernd Tibken and Denis Constales.*, SIAM Review **39** (1997), 779–786.

[11] C.P. Schnorr and M. Eucher, *Lattice basis reduction: improved practical algorithms and solving subset sum problems*, Math. Programming **66**, (1994) 181–199.

[12] C.L. Siegel *A mean value theorem in geometry of numbers*, Ann. Math. **46** (1945), 340–347.

[13] I. Weissman, *Sum of squares of uniform random variables*, Statist. Probab. Lett. **129** (2017), 147–154

ARC Centre of Excellence for Mathematical and Statistical Frontiers, School of Mathematics and Statistics, The University of Melbourne, Victoria 3010, Australia.

Email address: pjforr@unimelb.edu.au