

Rotatable random sequences in local fields*

Steven N. Evans[†]

Daniel Raban[‡]

Abstract

An infinite sequence of real random variables (ξ_1, ξ_2, \dots) is said to be rotatable if every finite subsequence (ξ_1, \dots, ξ_n) has a spherically symmetric distribution. A celebrated theorem of Freedman states that (ξ_1, ξ_2, \dots) is rotatable if and only if $\xi_j = \tau\eta_j$ for all j , where (η_1, η_2, \dots) is a sequence of independent standard Gaussian random variables and τ is an independent nonnegative random variable. Freedman's theorem is equivalent to a classical result of Schoenberg which says that a continuous function $\phi: \mathbb{R}_+ \rightarrow \mathbb{C}$ with $\phi(0) = 1$ is completely monotone if and only if $\phi_n: \mathbb{R}^n \rightarrow \mathbb{R}$ given by $\phi_n(x_1, \dots, x_n) = \phi(x_1^2 + \dots + x_n^2)$ is nonnegative definite for all $n \in \mathbb{N}$. We establish the analogue of Freedman's theorem for sequences of random variables taking values in local fields using probabilistic methods and then use it to establish a local field analogue of Schoenberg's result. Along the way, we obtain a local field counterpart of an observation variously attributed to Maxwell, Poincaré, and Borel which says that if $(\zeta_1, \dots, \zeta_n)$ is uniformly distributed on the sphere of radius \sqrt{n} in \mathbb{R}^n , then, for fixed $k \in \mathbb{N}$, the distribution of $(\zeta_1, \dots, \zeta_k)$ converges to that of a vector of k independent standard Gaussian random variables as $n \rightarrow \infty$.

Keywords: p -adic; p -series; exchangeable; spherically symmetric; Gaussian; total variation; completely monotone; nonnegative definite.

AMS MSC 2010: Primary 60B99; 60G09, Secondary 12J25.

Submitted to ECP on March 6, 2019, final version accepted on April 3, 2019.

Supersedes arXiv:1903.02058.

1 Introduction

An n -vector ξ of real-valued random variables is *rotatable* if $U\xi$ has the same distribution as ξ for every $n \times n$ orthogonal matrix U ; that is, the distribution of ξ is spherically symmetric. Similarly, an infinite sequence $(\xi_i)_{i \in \mathbb{N}}$ of real-valued random variables is rotatable if the vectors $(\xi_i)_{i \in [n]}$ are rotatable for every $n \in \mathbb{N}$ (here we use the notation $[n] := \{1, \dots, n\}$). Because permutation matrices are orthogonal, it follows that a rotatable infinite sequence is exchangeable and hence, by de Finetti's theorem, distributed as a mixture of independent, identically distributed sequences. A famous result of Maxwell [17, 18] says that if a real random vector is spherically symmetric and has independent (necessarily identically distributed) entries, then the distribution of the entries is centered Gaussian. Combining these two observations makes plausible the celebrated theorem of Freedman [10] (see, also, [13, 14, 6, 15, 21]) that a rotatable

*SNE supported in part by NSF grant DMS-1512933 and NIH grant 1R01GM109454-01.

[†]University of California at Berkeley, United States of America. E-mail: evans@stat.berkeley.edu

[‡]University of California at Los Angeles, United States of America. E-mail: danielraban@math.ucla.edu

infinite sequence of real-valued random variables is a scale mixture of sequences of independent standard Gaussian random variables; that is, if ξ is an infinite rotatable sequence, then $\xi = \tau\eta$, where $(\eta_i)_{i \in \mathbb{N}}$ is a sequence of independent standard Gaussian random variables and τ is a nonnegative random variable that is independent of η .

We refer the reader to the *Historical and Bibliographical Notes* in [12] for an indication of the later literature around Freedman's theorem and for remarks on the connection between this result and the classical theorem of Schoenberg [20] which says that a continuous function $\phi : \mathbb{R}_+ \rightarrow \mathbb{C}$ with $\phi(0) = 1$ is completely monotone if and only if $\phi_n : \mathbb{R}^n \rightarrow \mathbb{R}$ given by $\phi_n(x_1, \dots, x_n) = \phi(x_1^2 + \dots + x_n^2)$ is nonnegative definite for all $n \in \mathbb{N}$.

Our primary goal, realized in Theorem 3.3, is to obtain an analogue of Freedman's theorem for sequences of random variables taking values in fields other than the fields of real and complex numbers. More specifically, we consider the *local fields*; a local field is any locally compact, non-discrete topological field other than \mathbb{R} or \mathbb{C} (a local field is, for some prime p , a finite algebraic extension of either the field of p -adic numbers or the field of Laurent series over the finite field of integers modulo p). We recall some facts about the structure of local fields and vector spaces over them in Section 2. Just as in the real case, Freedman's theorem is equivalent to a structure theorem for nonnegative definite functions, and we present such a result in Section 4.

In order to search for a counterpart Freedman's theorem we need to have a parallel for the group of orthogonal matrices so that we can say what it means for a distribution to be "spherically symmetric" in the local field setting. The $n \times n$ orthogonal matrices are, of course, the matrices that preserve the Euclidean metric on n -dimensional space and so, denoting our local field by \mathcal{K} , we take as our parallel of the orthogonal matrices those matrices that are isometries of \mathcal{K}^n , where \mathcal{K}^n is equipped with the natural metric described in Subsection 2.2 – see Subsection 2.3.

Not surprisingly, our counterpart of Freedman's theorem also involves a suitable parallel of the class of Gaussian measures in a local field setting. Such an analogue was considered in [7, 8]. The idea is that, given one has a notion of spherical symmetry, one can take the property embodied in Maxwell's theorem to be the definition of Gaussianity for local fields. We recall some of the elementary properties of Gaussian probability measures on local fields in Subsection 2.6 after we have laid some groundwork on Haar measure and Fourier theory on local fields in Subsection 2.4 and Subsection 2.5, respectively.

2 Local fields

From now on, let \mathcal{K} be a fixed local field. We refer the reader to [19, 23, 22] for in-depth treatments of various aspects of analysis on local fields. Any result that we state without a proof or a bibliographic citation may be found in these references.

2.1 Basics

There is a distinguished real-valued mapping on \mathcal{K} which we denote by $|\cdot|$; this map has the properties

$$|x| = 0 \iff x = 0, \quad (2.1)$$

$$|xy| = |x||y|, \quad (2.2)$$

$$|x + y| \leq |x| \vee |y|, \quad (2.3)$$

and takes the values $\{0\} \cup \{q^m : m \in \mathbb{Z}\}$, where $q = p^c$ for some prime p and positive integer c .

A map with properties (1.1)-(1.3) is called a *non-Archimedean valuation*. Property (1.3) is known as the *ultrametric inequality* or the *strong triangle inequality*. The mapping $(x, y) \mapsto |x - y|$ on $\mathcal{K} \times \mathcal{K}$ is a metric on \mathcal{K} which induces the topology of \mathcal{K} . The metric space \mathcal{K} is a complete, totally disconnected, *ultrametric space* under this metric.

Write \mathcal{D} for the closed unit ball $\{x : |x| \leq 1\}$. Choosing $\rho \in \mathcal{K}$ so that $|\rho| = q^{-1}$, we have

$$\rho^k \mathcal{D} = \{x : |x| \leq q^{-k}\} = \{x : |x| < q^{-(k-1)}\}$$

for each $k \in \mathbb{Z}$; in particular, $\rho^k \mathcal{D}$ is both open and closed for each $k \in \mathbb{Z}$.

The set \mathcal{D} is a ring, called the *ring of integers* of \mathcal{K} . Each of the sets $\rho^k \mathcal{D}$, $k \in \mathbb{Z}$, is a compact \mathcal{D} -submodule of \mathcal{K} , and every non-trivial compact \mathcal{D} -submodule of \mathcal{K} is of this form. For $\ell < k$ the additive quotient group $\rho^\ell \mathcal{D} / \rho^k \mathcal{D}$ has order $q^{k-\ell}$. Consequently, \mathcal{D} is the union of q disjoint translates (that is, cosets) of $\rho \mathcal{D}$. Each of these cosets is, in turn, the union of q disjoint translates of $\rho^2 \mathcal{D}$, and so on.

Remark 2.1. We can thus think of the collection of balls contained in \mathcal{D} as being arranged in an infinite rooted q -ary tree: the root is \mathcal{D} itself, the nodes at level k are the balls of radius q^{-k} (cosets of $\rho^k \mathcal{D}$), and the q “children” of such a ball are the q cosets of $\rho^{k+1} \mathcal{D}$ that it contains. We can uniquely associate each point in \mathcal{D} with the sequence of balls that contain it, and so we can think of the points in \mathcal{D} as the boundary of this tree.

2.2 Norms

A *norm* on a vector space \mathcal{E} over the local field \mathcal{K} is a real-valued mapping $\|\cdot\|$ on \mathcal{E} with the properties

$$\|x\| = 0 \iff x = 0, \tag{2.4}$$

$$\|\lambda x\| = |\lambda| \|x\|, \quad \lambda \in \mathcal{K}, \tag{2.5}$$

$$\|x + y\| \leq \|x\| \vee \|y\|. \tag{2.6}$$

The norm induces a metric on \mathcal{E} by $(x, y) \mapsto \|x - y\|$. The resulting metric space is an ultrametric space. We always take the norm on \mathcal{K}^n to be the one given by

$$\|(x_i)_{i \in [n]}\| := \bigvee_{i \in [n]} |x_i|.$$

The space \mathcal{K}^n is complete under this metric. In general, a *\mathcal{K} -Banach space* is a vector space \mathcal{E} over \mathcal{K} that is equipped with a norm such that the resulting metric space is complete.

2.3 Orthogonality

The following definition of orthogonality in a normed vector space over \mathcal{K} mimics a characterization of orthogonality in an inner product space over \mathbb{R} that does not explicitly involve the inner product and instead is in terms of the induced metric.

Definition 2.2. Given a subset G of a normed vector space \mathcal{E} over \mathcal{K} , write $\langle G \rangle$ for the linear span of G . A subset F of \mathcal{E} is *\mathcal{K} -orthogonal* if $\|x - y\| \geq \|x\|$ for all $x \in F$ and $y \in \langle F \setminus \{x\} \rangle$; that is, the best approximation of x in the vector space $\langle F \setminus \{x\} \rangle$ is 0. Equivalently, a subset F is *\mathcal{K} -orthogonal* if for any finite subset $\{x_1, \dots, x_n\} \subseteq F$ and collection of scalars $\alpha_1, \dots, \alpha_n \in \mathcal{K}$,

$$\left\| \sum_{i \in [n]} \alpha_i x_i \right\| = \bigvee_{i \in [n]} |\alpha_i| \|x_i\|.$$

A subset F of \mathcal{E} is *\mathcal{K} -orthonormal* if it is \mathcal{K} -orthogonal and $\|x\| = 1$ for all $x \in F$.

Remark 2.3. If F is \mathcal{K} -orthonormal, then, for any finite subset $\{x_1, \dots, x_n\} \subseteq F$ and collection of scalars $\alpha_1, \dots, \alpha_n \in \mathcal{K}$, $\left\| \sum_{i \in [n]} \alpha_i x_i \right\| = \bigvee_{i \in [n]} |\alpha_i| \|x_i\| = \bigvee_{i \in [n]} |\alpha_i|$. Conversely, suppose that for any finite subset $\{x_1, \dots, x_n\} \subseteq F$ and collection of scalars $\alpha_1, \dots, \alpha_n \in \mathcal{K}$ we have $\left\| \sum_{i \in [n]} \alpha_i x_i \right\| = \bigvee_{i \in [n]} |\alpha_i|$. Taking $\alpha_j = 1$ and $\alpha_i = 0$ for $i \neq j$, $j \in [n]$, we see that $\|x_j\| = 1$ for $j \in [n]$ and hence $\left\| \sum_{i \in [n]} \alpha_i x_i \right\| = \bigvee_{i \in [n]} |\alpha_i| \|x_i\|$; that is, F is \mathcal{K} -orthonormal.

Theorem 2.4. *The following are equivalent for an $n \times n$ matrix U .*

- (i) *The matrix U is an isometry of \mathcal{K}^n .*
- (ii) *The matrix U is invertible and the entries of both U and U^{-1} lie in \mathcal{D} .*
- (iii) *The columns of U are \mathcal{K} -orthonormal.*
- (iv) *The rows of U are \mathcal{K} -orthonormal.*
- (v) *The entries of U lie in \mathcal{D} and $|\det U| = 1$.*

Proof. (i) \iff (ii): See Remark 3.2 in [9].

(i) \iff (iii): Note that

$$\begin{aligned} \|Ux\| &= \|x\|, \quad \forall x \in \mathcal{K}^n, \\ \iff \bigvee_{i \in [n]} |(Ux)_i| &= \bigvee_{i \in [n]} |x_i|, \quad \forall x \in \mathcal{K}^n, \\ \iff \bigvee_{i \in [n]} \left| \sum_{j \in [n]} U_{i,j} x_j \right| &= \bigvee_{i \in [n]} |x_i|, \quad \forall x \in \mathcal{K}^n, \\ \iff \left\| \sum_{j \in [n]} x_j (U_{i,j})_{i \in [n]} \right\| &= \bigvee_{i \in [n]} |x_i|, \quad \forall x \in \mathcal{K}^n, \\ \iff \text{the columns of } U &\text{ are orthonormal,} \end{aligned}$$

where we applied Remark 2.3 for the last equivalence.

(i) \iff (iv): We have already shown that (i), (ii), and (iii) are equivalent. It remains to observe that U is invertible with U and U^{-1} both having entries in \mathcal{D} if and only if the transpose U^\top is invertible with U^\top and $(U^\top)^{-1}$ both having entries in \mathcal{D} .

(ii) \iff (v): If (ii) holds, then it follows from the properties of the valuation that $|\det U| \leq 1$ and $|\det U|^{-1} = |(\det U)^{-1}| = |\det U^{-1}| \leq 1$, so that $|\det U| = 1$ and (v) holds. Conversely, if (v) holds, then (ii) follows from Cramer's rule. \square

Notation 2.5. *In light of Theorem 2.4, we write $\text{GL}_n(\mathcal{D})$ for the group of matrices that satisfy the equivalent conditions of the theorem and say that these matrices are \mathcal{K} -orthogonal.*

Notation 2.6. *For $n \in \mathbb{N}$, denote the unit sphere $\{x \in \mathcal{K}^n : \|x\| = 1\} = \mathcal{D}^n \setminus (\rho\mathcal{D})^n$ by $\mathcal{S}^{(n)}$.*

Lemma 2.7. *The group of matrices $\text{GL}_n(\mathcal{D})$ acts transitively on the set $\mathcal{S}^{(n)}$; that is, given $x, y \in \mathcal{K}^n$ with $\|x\| = \|y\| = 1$, there is exists $U \in \text{GL}_n(\mathcal{D})$ such that $Ux = y$.*

Proof. Let $e_i, i \in [n]$, be the coordinate vectors in \mathcal{K}^n ; that is e_i is the vector with 1 in the i^{th} coordinate and 0 elsewhere. Because $\text{GL}_n(\mathcal{D})$ is a group, it suffices to show that for any $x \in \mathcal{K}^n$ with $\|x\| = 1$ there exists a matrix $U \in \text{GL}_n(\mathcal{D})$ such that $Ue_1 = x$.

Fix such an x . Because $\|x\| = 1$, there is at least one coordinate, say i , such that $|x_i| = 1$. Let U be an $n \times n$ matrix that has first column equal to x and remain columns given by the $n - 1$ vectors $e_j, j \neq i$, listed in some order. Note that $Ue_1 = x$. Clearly, $\det U = \pm x_i$ so that $|\det U| = |x_i| = 1$ and $U \in \text{GL}_n(\mathcal{D})$. \square

2.4 Haar measure

There is a unique measure λ on \mathcal{K} which has the properties

$$\lambda(x + A) = \lambda(A)$$

and

$$\lambda(xA) = |x|\lambda(A)$$

for each $x \in \mathcal{K}$, and

$$\lambda(\mathcal{D}) = 1;$$

the measure λ is just the suitably normalized Haar measure on the additive group of \mathcal{K} .

For $n \in \mathbb{N}$, the measure $\lambda^{\otimes n}$ on \mathcal{K}^n has the properties

$$\lambda^{\otimes n}(x + A) = \lambda^{\otimes n}(A)$$

for each $x \in \mathcal{K}^n$ and

$$\lambda^{\otimes n}(MA) = |\det M| \lambda^{\otimes n}(A)$$

for each $n \times n$ matrix M . In particular, $\lambda^{\otimes n}$ is $\text{GL}_n(\mathcal{D})$ -invariant.

Notation 2.8. Write γ for the restriction of the measure λ to \mathcal{D} and, for $n \in \mathbb{N}$, set $\gamma_n := \gamma^{\otimes n}$. Denote by σ_n the probability measure obtained by conditioning the probability measure γ_n on the set $\mathcal{S}^{(n)}$; that is, σ_n is $\gamma_n(\cdot \cap \mathcal{S}^{(n)})$ normalized to be a probability measure.

Proposition 2.9. The probability measure σ_n is the unique probability measure on $\mathcal{S}^{(n)}$ that is invariant under the action of $\text{GL}_n(\mathcal{D})$.

Proof. It is clear that γ_n is invariant under the action of $\text{GL}_n(\mathcal{D})$. Because $\mathcal{S}^{(n)}$ is a subset of \mathcal{D}^n that has positive γ_n measure (namely, $1 - q^{-n}$) that is invariant under the action of $\text{GL}_n(\mathcal{D})$, it follows that σ_n is invariant under the action of $\text{GL}_n(\mathcal{D})$. It therefore remains to establish the uniqueness claim. This, however, is immediate from Theorem 2.11 below and Lemma 2.7. \square

Remark 2.10. (i) The uniqueness claim in Proposition 2.9 may be established by an alternative route. Because $\text{GL}_n(\mathcal{D})$ is a compact, second countable, Hausdorff group, it possesses a Haar measure which is unique if we normalize it to be a probability measure. Denote this probability measure by μ . Suppose that ν is a $\text{GL}_n(\mathcal{D})$ -invariant probability measure on $\mathcal{S}^{(n)}$. For any positive Borel function f on $\mathcal{S}^{(n)}$ and $U \in \text{GL}_n(\mathcal{D})$ we have $\int f(x) \nu(dx) = \int f(Ux) \nu(dx)$ and so $\int f(x) \nu(dx) = \int \int f(Ux) \nu(dx) \mu(dU) = \int \int f(Ux) \mu(dU) \nu(dx)$. From Lemma 2.7 we know for each $x \in \mathcal{S}^{(n)}$ that there is a matrix $V \in \text{GL}_n(\mathcal{D})$ such that $x = V\mathbf{e}_1$, where $\mathbf{e}_1 = (1, 0, \dots, 0)^\top$. Therefore, by the invariance of μ , $\int f(Ux) \mu(dU) = \int f(UV\mathbf{e}_1) \mu(dU) = \int f(U\mathbf{e}_1) \mu(dU)$ and hence $\int f(x) \nu(dx)$ is necessarily $\int f(U\mathbf{e}_1) \mu(dU)$.

(ii) It is possible to describe the Haar measure on $\text{GL}_n(\mathcal{D})$ quite concretely. Let $\gamma_{n \times n}$ be the probability measure on $n \times n$ matrices given by $\gamma_{n \times n}((dm_{i,j})_{i,j \in [n]}) = \bigotimes_{i,j \in [n]} \gamma(dm_{i,j})$; that is, if M is distributed according to $\gamma_{n \times n}$, then the entries of M are independent and each is distributed according to γ . The Haar measure on $\text{GL}_n(\mathcal{D})$ is just $\gamma_{n \times n}$ conditioned on the set $\text{GL}_n(\mathcal{D})$; that is, the Haar measure is the restriction of $\gamma_{n \times n}$ to $\text{GL}_n(\mathcal{D})$ normalized to be a probability measure. Because we don't need this result in what follows, we leave the (straightforward) proof to the reader. We note in passing that the $\gamma_{n \times n}$ measure of $\text{GL}_n(\mathcal{D})$ is $\prod_{i \in [n]} (1 - q^{-i})$ – see [9, Theorem 4.1].

(iii) As we have seen, the probability measure γ_n is $\text{GL}_n(\mathcal{D})$ -invariant. On the other hand, if the push-forward of γ_n by an $n \times n$ matrix M is again γ_n , then property (v) of Theorem 2.4 holds and $M \in \text{GL}_n(\mathcal{D})$. We may therefore add another equivalent property to the list in Theorem 2.4. A similar remark holds with γ_n replaced by σ_n .

For the sake of completeness, we state the following classical result on the existence and uniqueness of measures invariant under the action of a group (see, for example, [11, Theorem 2.29]).

Theorem 2.11. *Let G be a locally compact, second countable, Hausdorff group of measurable transformations on a locally compact, second countable, Hausdorff space S . Suppose that G acts properly (that is, the set $\{g \in G : gs \in K\} \subseteq G$ is compact for all $s \in S$ and compact $K \subseteq S$) and transitively (that is, given $s, t \in S$ there exists $g \in G$ such that $gs = t$). Then, up to normalization, there is a unique non-zero G -invariant Radon measure on S .*

The following corollary is an easy consequence of Proposition 2.9, but we include the proof for the sake of completeness.

Corollary 2.12. *Let ξ be a \mathcal{K}^n -valued random variable such that $U\xi$ has the same distribution as ξ for all $U \in \text{GL}_n(\mathcal{D})$. Possibly on some extension $(\bar{\Omega}, \bar{\mathcal{F}}, \bar{\mathbb{P}})$ of $(\Omega, \mathcal{F}, \mathbb{P})$ there is a σ_n -distributed, $\mathcal{S}^{(n)}$ -valued random variable ϑ and a $\{\rho^m : m \in \mathbb{Z}\} \cup \{0\}$ -valued random variable R independent of ϑ such that $\xi = R\vartheta$. Consequently, if ν is a $\text{GL}_n(\mathcal{D})$ -invariant probability measure on \mathcal{K}^n , then ν is the push-forward of $\pi \otimes \sigma_n$ by the map $(r, x) \mapsto rx$ for some probability measure π on $\{\rho^m : m \in \mathbb{Z}\} \cup \{0\}$.*

Proof. Define events $A_m, m \in \mathbb{Z}$, by $A_m := \{\omega \in \Omega : \|\xi(\omega)\| = q^{-m}\}$ and set $A_\infty := \{\omega \in \Omega : \|\xi(\omega)\| = 0\}$. Let $(\bar{\Omega}, \bar{\mathcal{F}})$ be $\Omega \times \mathcal{S}^{(n)}$ equipped with the product of the σ -field \mathcal{F} and the Borel σ -field on $\mathcal{S}^{(n)}$. Let $\bar{\mathbb{P}} := \mathbb{P} \otimes \sigma_n$. Extend the definition of ξ to $\bar{\Omega}$ by, with the usual abuse of notation, taking $\xi(\omega, x)$ to be $\xi(\omega)$.

Set $R := \rho^m$ on the event $A_m \times \mathcal{S}^{(n)}, m \in \mathbb{Z}$, and $R := 0$ on the event $A_\infty \times \mathcal{S}^{(n)}$. Put

$$\vartheta(\omega, x) := \begin{cases} \rho^{-m}\xi(\omega, x), & \omega \in A_m, m \in \mathbb{Z}, \\ x, & \omega \in A_\infty. \end{cases}$$

It is clear that $\xi = R\vartheta$. For any $r \in \{\rho^m : m \in \mathbb{Z}\} \cup \{0\}$ the conditional distribution of ϑ given the event $\{R = r\}$ is obviously invariant under the action of $\text{GL}_n(\mathcal{D})$ and so, by Proposition 2.9, the random variable ϑ is independent of R with distribution σ_n . \square

A classical theorem often attributed to Poincaré says that for fixed $k \in \mathbb{N}$ the distribution of the first k coordinates of a point uniformly distributed over the sphere of radius \sqrt{n} in \mathbb{R}^n converges to the distribution of a vector of k independent standard Gaussian variables as $n \rightarrow \infty$. See Section 6 of [4] for a discussion of the history of this result leading to the conclusion that a more appropriate attribution is to the work of Borel in [1] (see also Chapter V of [2]). It is shown in [4] that indeed the total variation distance between the distribution of the first k coordinates of a point uniformly distributed over the sphere of radius \sqrt{n} in \mathbb{R}^n and the distribution of a vector of k independent standard Gaussian variables converges to zero as $n \rightarrow \infty$ provided that $k = o(n)$.

The analogue of such a result in the local field setting is the following. Note that the relevant total variation distance converges to zero as $n \rightarrow \infty$ regardless of the relative size of k with respect to n .

Theorem 2.13. *For $n \in \mathbb{N}$ and $k \in [n]$, let $\sigma_{n,k}$ be the push-forward of σ_n by the map that sends $(x_i)_{i \in [n]} \in \mathcal{K}^n$ to $(x_i)_{i \in [k]} \in \mathcal{K}^k$. The total variation distance between the probability measures $\sigma_{n,k}$ and γ_k is $q^{-n}(1 - q^{-k})/(1 - q^{-n})$.*

Proof. Let $(\xi_{n,i})_{i \in [n]}$ have distribution σ_n and let $(\eta_i)_{i \in [n]}$ have distribution γ_n so that $(\xi_{n,i})_{i \in [k]}$ has distribution $\sigma_{n,k}$ and $(\eta_i)_{i \in [k]}$ has distribution γ_k .

By definition, the distribution of $(\xi_{n,i})_{i \in [n]}$ is the same as the distribution of $(\eta_i)_{i \in [n]}$ conditioned on the event $\{\|(\eta_i)_{i \in [n]}\| = 1\}$. Write $\delta_{n,i}$ for the indicator of the event

$\{|\xi_{n,i}| = 1\}$ and ϵ_i for the indicator of the event $\{|\eta_i| = 1\}$. Let ν_0 (resp. ν_1) be γ conditioned on the event $\{x \in \mathcal{K} : |x| < 1\}$ (resp. $\{x \in \mathcal{K} : |x| = 1\}$); that is, ν_0 (resp. ν_1) is the conditional distribution of η_i given the event $\{|\eta_i| < 1\}$ (resp. $\{|\eta_i| = 1\}$).

If $(e_i)_{i \in [n]} \in \{0, 1\}^n \neq 0$, then the conditional distribution of $(\xi_{n,i})_{i \in [k]}$ given the event $\{(\delta_{n,i})_{i \in [k]} = (e_i)_{i \in [k]}\}$ is the same as that of $(\eta_i)_{i \in [k]}$ given the event $\{(\epsilon_k)_{i \in [k]} = (e_i)_{i \in [k]}\}$; both conditional distributions are $\otimes_{i \in [k]} \nu_{e_i}$. It follows that the total variation distance we seek is the same as the total variation distance between the distribution of $(\delta_{n,i})_{i \in [k]}$ and the distribution of $(\epsilon_i)_{i \in [k]}$. Furthermore, the conditional distribution of $(\delta_{n,i})_{i \in [k]}$ given the event $\{\sum_{i \in [k]} \delta_{n,i} = j\}$ is the same as the conditional distribution of $(\epsilon_i)_{i \in [k]}$ given the event $\{\sum_{i \in [k]} \epsilon_i = j\}$. Thus, it further suffices to compute the total variation distance between the distribution of $\sum_{i \in [k]} \delta_{n,i}$ and the distribution of $\sum_{i \in [k]} \epsilon_i$.

Put $X = \sum_{i \in [n]} \epsilon_i$ and $Y = \sum_{i \in [k]} \epsilon_i$. Noting that the distribution of $\sum_{i \in [k]} \delta_{n,i}$ is the same as the conditional distribution of Y given the event $\{X \neq 0\}$, the total variation distance we seek is

$$\frac{1}{2} \sum_{y=0}^k |\mathbb{P}\{Y = y\} - \mathbb{P}\{Y = y | X \neq 0\}|.$$

For $y \neq 0$ we have

$$\mathbb{P}\{Y = y | X \neq 0\} = \frac{\mathbb{P}\{Y = y, X \neq 0\}}{\mathbb{P}\{X \neq 0\}} = \frac{\mathbb{P}\{Y = y\}}{\mathbb{P}\{X \neq 0\}},$$

and so

$$\begin{aligned} \sum_{y=1}^k |\mathbb{P}\{Y = y\} - \mathbb{P}\{Y = y | X \neq 0\}| &= \left(\frac{1}{1 - q^{-n}} - 1 \right) \sum_{y=1}^k \mathbb{P}\{Y = y\} \\ &= \left(\frac{1}{1 - q^{-n}} - 1 \right) (1 - \mathbb{P}\{Y = 0\}) \\ &= \frac{q^{-n}}{1 - q^{-n}} (1 - q^{-k}). \end{aligned}$$

Also,

$$\mathbb{P}\{Y = 0\} = q^{-k}$$

and

$$\mathbb{P}\{Y = 0 | X \neq 0\} = \frac{q^{-k}(1 - q^{-(n-k)})}{1 - q^{-n}},$$

so that

$$\begin{aligned} |\mathbb{P}\{Y = 0\} - \mathbb{P}\{Y = 0 | X \neq 0\}| &= q^{-k} - \frac{q^{-k}(1 - q^{-(n-k)})}{1 - q^{-n}} \\ &= \frac{q^{-k}(q^{-(n-k)} - q^{-n})}{1 - q^{-n}}. \end{aligned}$$

Therefore,

$$\begin{aligned} \frac{1}{2} \sum_{y=0}^k |\mathbb{P}\{Y = y\} - \mathbb{P}\{Y = y | X \neq 0\}| &= \frac{1}{2} \frac{q^{-n}(1 - q^{-k}) + q^{-k}(q^{-(n-k)} - q^{-n})}{1 - q^{-n}} \\ &= \frac{1}{2} \frac{2q^{-n} - 2q^{-(n+k)}}{1 - q^{-n}} \\ &= \frac{q^{-n}(1 - q^{-k})}{1 - q^{-n}}, \end{aligned}$$

as claimed. □

2.5 Fourier theory

Recall that a *character* on a locally compact Abelian group G with the group operation written additively is a map $\kappa : G \rightarrow \mathbb{T} := \{z \in \mathbb{C} : |z| = 1\}$ such that $\kappa(g + h) = \kappa(g)\kappa(h)$ for all $g, h \in G$.

It is possible to fix a character χ for \mathcal{K} such that χ restricted to the subgroup \mathcal{D} is trivial (that is, always takes the value 1) while χ restricted to the subgroup $\rho^{-1}\mathcal{D}$ is non-trivial. Fixing any such choice of the character χ , an arbitrary character on \mathcal{K} is of the form $x \mapsto \chi(ax)$ for some $a \in \mathcal{K}$. More generally, an arbitrary character on \mathcal{K}^n is of the form $x \mapsto \chi(a \cdot x)$ for some $a \in \mathcal{K}^n$, where $a \cdot x$ is the usual dot product of the vectors a and x .

A probability measure μ on \mathcal{K}^n has a Fourier transform $\hat{\mu}(t) := \int \chi(t \cdot x) \mu(dx)$, $t \in \mathcal{K}^n$. For example, $\hat{\gamma}_n = \mathbb{1}_{\mathcal{D}^n}$.

2.6 Gaussian random variables

For an introduction to the/an analogue of Gaussian probability measures on local fields and the proofs of any results stated without proof in this subsection, see [7, 8].

The following definition mimics a standard definition/characterization of Gaussian random variables taking values in a Banach spaces over the real numbers.

Definition 2.14. *Let \mathcal{E} be a separable \mathcal{K} -Banach, and let ξ be an \mathcal{E} -valued random variable. The random variable ξ is \mathcal{K} -Gaussian if whenever ξ_1 and ξ_2 are independent copies of ξ and $(\alpha_{1,1}, \alpha_{1,2}), (\alpha_{2,1}, \alpha_{2,2}) \in \mathcal{K}^2$ are \mathcal{K} -orthonormal, then (ξ_1, ξ_2) has the same distribution as $(\alpha_{1,1}\xi_1 + \alpha_{1,2}\xi_2, \alpha_{2,1}\xi_1 + \alpha_{2,2}\xi_2)$.*

Theorem 2.15. *Let \mathcal{E} be a separable \mathcal{K} -Banach space and let ξ be an \mathcal{E} -valued random variable.*

- (i) *The random variable ξ is \mathcal{K} -Gaussian if and only if the distribution of ξ is Haar measure on some compact \mathcal{D} -module of \mathcal{E} . In particular, if $\mathcal{E} = \mathcal{K}$, then ξ is \mathcal{K} -Gaussian if and only if the distribution of ξ is either the point mass at 0 or the restriction of the Haar measure λ to one of the sets $\rho^m\mathcal{D}$, $m \in \mathbb{Z}$, normalized to be a probability measure.*
- (ii) *The random variable ξ is \mathcal{K} -Gaussian if and only if the \mathcal{K} -valued random variable $T\xi$ is \mathcal{K} -Gaussian for all $T \in \mathcal{E}^*$, where \mathcal{E}^* is the dual space of continuous, linear maps from \mathcal{E} to \mathcal{K} .*
- (iii) *If ξ is \mathcal{K} -Gaussian, then the compact \mathcal{D} -module in (i) is the set*

$$\{x \in \mathcal{E} : |Tx| \leq \|T\xi\|_\infty \quad \forall T \in \mathcal{E}^*\},$$

where $\|\zeta\|_\infty := \text{ess sup}\{|\zeta(\omega)| : \omega \in \Omega\}$ for a \mathcal{K} -valued random variable ζ .

- (iv) *The random variable ξ is \mathcal{K} -Gaussian if and only if $\|T\xi\|_\infty$ is finite for all $T \in \mathcal{E}^*$ and, for all $t \in \mathcal{K}$,*

$$\mathbb{P}[\chi(tT\xi)] = \begin{cases} 1, & |t|\|T\xi\|_\infty \leq 1, \\ 0, & \text{otherwise.} \end{cases}$$

Definition 2.16. *A \mathcal{K} -valued random variable is standard \mathcal{K} -Gaussian if its distribution is γ .*

3 Rotatable random sequences

The following analogue of Theorem 2 in [4] follows from a combination of Corollary 2.12 and Theorem 2.13.

Proposition 3.1. Suppose that ν is a $GL_n(\mathcal{D})$ -invariant probability measure on \mathcal{K}^n so that ν is the push-forward of $\pi \otimes \sigma_n$ by the map $(r, x) \mapsto rx$ for some probability measure π on $\{\rho^m : m \in \mathbb{Z}\} \cup \{0\}$. The total variation distance between ν and the push-forward of $\pi \otimes \gamma_n$ by the map $(r, x) \mapsto rx$ is at most q^{-n} .

Definition 3.2. An infinite sequence $(\xi_i)_{i \in \mathbb{N}}$ of \mathcal{K} -valued random variables is rotatable if $U(\xi_i)_{i \in [n]}$ has the same distribution as $(\xi_i)_{i \in [n]}$ for every $n \in \mathbb{N}$ and $U \in GL_n(\mathcal{D})$.

Theorem 3.3. A \mathcal{K} -valued random infinite sequence $\xi = (\xi_i)_{i \in \mathbb{N}}$ is rotatable if and only if $\sup_{i \in \mathbb{N}} |\xi_i|$ is almost surely finite and (possibly on some extension of $(\Omega, \mathcal{F}, \mathbb{P})$) $\xi_i = \tau \eta_i$, $i \in \mathbb{N}$, where

- η_1, η_2, \dots are independent, identically distributed, standard \mathcal{K} -Gaussian random variables,
- τ is the random variable taking values in $\{\rho^m : m \in \mathbb{Z}\} \cup \{0\}$ given by

$$\tau := \begin{cases} \rho^m, & \sup_j |\xi_j| = q^{-m}, \quad m \in \mathbb{Z}, \\ 0, & \sup_j |\xi_j| = 0. \end{cases}$$

- the random variable τ is independent of the sequence $\eta = (\eta_i)_{i \in \mathbb{N}}$.

Proof. For each $n \in \mathbb{N}$, let

$$\tau_n := \begin{cases} \rho^m, & \|(\xi_i)_{i \in [n]}\| = q^{-m}, \quad m \in \mathbb{Z}, \\ 0, & \|(\xi_i)_{i \in [n]}\| = 0, \end{cases}$$

and let $(\tilde{\xi}_{n,i})_{i \in [n]}$ be distributed according to σ_n and independent of τ_n . Observe that, by Corollary 2.12, $(\xi_i)_{i \in [n]}$ has the same distribution as $\tau_n(\tilde{\xi}_{n,i})_{i \in [n]}$. Now let $\tilde{\eta}$ be an infinite sequence of independent, identically distributed, standard \mathcal{K} -Gaussian random variables independent of $(\tau_n)_{n \in \mathbb{N}}$. Writing $\mathcal{L}(\zeta)$ for the distribution of a random variable ζ and $\|\cdot - \cdot\|_{TV}$ for the total variation distance, we have

$$\begin{aligned} \|\mathcal{L}((\xi_i)_{i \in [k]}) - \mathcal{L}(\tau_n(\tilde{\eta}_i)_{i \in [k]})\|_{TV} &= \|\mathcal{L}(\tau_n(\tilde{\xi}_{n,i})_{i \in [k]}) - \mathcal{L}(\tau_n(\tilde{\eta}_i)_{i \in [k]})\|_{TV} \\ &\leq \|\mathcal{L}((\tilde{\xi}_{n,i})_{i \in [k]}) - \mathcal{L}((\tilde{\eta}_i)_{i \in [k]})\|_{TV}, \end{aligned}$$

which goes to 0 as $n \rightarrow \infty$ by Theorem 2.13. So $\tau_n \tilde{\eta}$ certainly converges in distribution to ξ .

Now $|\tau_n| = \|(\xi_i)_{i \in [n]}\| = \bigvee_{i \in [n]} |\xi_i|$ is increasing with $n \in \mathbb{N}$, and

$$\begin{aligned} 0 &= \inf_{m \in \mathbb{Z}} \mathbb{P}\{|\xi_1| > q^m\} \\ &= \inf_{m \in \mathbb{Z}} \lim_{n \in \mathbb{N}} \mathbb{P}\{|\tau_n \tilde{\eta}_1| > q^m\} \\ &= \inf_{m \in \mathbb{Z}} \sup_{n \in \mathbb{N}} \mathbb{P}\{|\tau_n \tilde{\eta}_1| > q^m\} \\ &= \inf_{m \in \mathbb{Z}} \sup_{n \in \mathbb{N}} \sum_{\ell=0}^{\infty} \mathbb{P}\{|\tau_n| > q^{m+\ell}\} \mathbb{P}\{|\tilde{\eta}_1| = q^{-\ell}\} \\ &= \sum_{\ell=0}^{\infty} \inf_{m \in \mathbb{Z}} \sup_{n \in \mathbb{N}} \mathbb{P}\{|\tau_n| > q^{m+\ell}\} \mathbb{P}\{|\tilde{\eta}_1| = q^{-\ell}\} \\ &= \sum_{\ell=0}^{\infty} \inf_{m \in \mathbb{Z}} \mathbb{P}\left\{ \sup_{n \in \mathbb{N}} |\tau_n| > q^{m+\ell} \right\} \mathbb{P}\{|\tilde{\eta}_1| = q^{-\ell}\} \\ &= \mathbb{P}\left\{ \sup_{n \in \mathbb{N}} |\tau_n| = \infty \right\}, \end{aligned}$$

so that $\tau_n \rightarrow \tau$ almost surely for some random variable τ taking values in $\{\rho^m : m \in \mathbb{Z}\} \cup \{0\}$.

Thus ξ has the same distribution as $\tau\tilde{\eta}$. The almost sure result then follows from the transfer lemma (Corollary 6.11 from [11]); we thus have random variables $\eta, \check{\tau}$ such that $(\tau, \tilde{\eta})$ has the same distribution as $(\check{\tau}, \eta)$ and $\check{\tau}\eta = \xi$ almost surely. It remains to observe that

$$\begin{aligned} |\tau| &= \sup_{n \in \mathbb{N}} \|(\xi_i)_{i \in [n]}\| \\ &= \sup_{n \in \mathbb{N}} \|(\check{\tau}(\eta_i))_{i \in [n]}\| \\ &= \sup_{n \in \mathbb{N}} |\check{\tau}| \|(\eta_i)_{i \in [n]}\| \\ &= |\check{\tau}| \sup_{n \in \mathbb{N}} \|(\eta_i)_{i \in [n]}\| \\ &= |\check{\tau}| \end{aligned}$$

almost surely, so that $\check{\tau} = \tau$ almost surely. □

There are several extensions and variants of Freedman’s theorem in the literature – see [5] for a review. One extension is to consider infinite random sequences where the individual entries take values in \mathbb{R}^m for some $m \in \mathbb{N}$ or, more generally, in some separable Banach space over \mathbb{R} as in [3]. The analogue of the result in [3] holds in the local field setting, as we now explain. We say that a random sequence ξ with entries in a separable \mathcal{K} -Banach space \mathcal{E} is *rotatable* if for any $n \in \mathbb{N}$ and $U \in GL_n(\mathcal{D})$ we have that $(\sum_{j \in [n]} U_{i,j} \xi_j)_{i \in [n]}$ has the same distribution as $(\xi_i)_{i \in [n]}$. Write $\Gamma(\mathcal{E})$ for the set of Gaussian probability measures on \mathcal{E} . The set $\Gamma(\mathcal{E})$ is a closed subset of the Polish space of probability measures on the Polish space \mathcal{E} , where we equip the space of probability measures with the topology of weak convergence. By Theorem 2.15, $\Gamma(\mathcal{E})$ is in a bijective correspondence with the set of compact \mathcal{D} -modules in \mathcal{E} . The analytic content of Theorem 3.3 is that the distribution of a rotatable sequence of \mathcal{K} -valued random variables is $\int_{\Gamma(\mathcal{K})} \mu^{\otimes \mathbb{N}} \pi(d\mu)$ for some probability measure on $\Gamma(\mathcal{K})$ and it is not too difficult to establish the following generalization that is a local field counterpart to the result in [3]. We omit the proof.

Theorem 3.4. *An infinite sequence ξ of random variables in a separable \mathcal{K} -Banach space \mathcal{E} is rotatable if and only if the distribution of ξ is $\int_{\Gamma(\mathcal{E})} \mu^{\otimes \mathbb{N}} \pi(d\mu)$ for some probability measure π on $\Gamma(\mathcal{E})$.*

Other variants of Freedman’s theorem involve considering infinite random sequences ξ such that for all $n \in \mathbb{N}$ the random vector $U(\xi_i)_{i \in [n]}$ has the same distribution as $(\xi_i)_{i \in [n]}$ for all $U \in G_n$, where G_n is some subgroup of the $n \times n$ orthogonal group that contains the subgroup of permutation matrices. For example, [21] considers the case where G_n is the subgroup that fixes the vector $(1, \dots, 1)^T$ and shows that in this case $\xi = \alpha + \beta\eta$, where η is an independent, identically distributed, standard Gaussian sequence and (α, β) is an independent $\mathbb{R} \times \mathbb{R}_+$ -valued random vector. It would be interesting to investigate the counterparts of such results in the local field setting, but we leave this to a future paper.

4 A local field analogue of Schoenberg’s theorem

In the case of real-valued rotatable random variables over \mathbb{R} , Freedman’s theorem is equivalent to a result about nonnegative definite functions (see Theorem 1.31 and Appendix 4 in [12]) which we recalled in the Introduction. Here, we provide an analogue of the latter result in the local field setting.

Recall that a function ϕ defined on an Abelian group G is *nonnegative definite* if $\sum_{i,j \in [n]} \phi(g_i - g_j) z_i \bar{z}_j \geq 0$ for all $g_1, \dots, g_n \in G$, $z_1, \dots, z_n \in \mathbb{C}$, and $n \in \mathbb{N}$.

Theorem 4.1. *Let $\phi : \{0\} \cup \{q^m : m \in \mathbb{Z}\} \rightarrow \mathbb{R}$ be such that $\lim_{m \rightarrow \infty} \phi(q^{-m}) = \phi(0) = 1$. For $n \in \mathbb{N}$, define $\phi_n : \mathcal{K}^n \rightarrow \mathbb{R}$ by*

$$\phi_n(x_1, \dots, x_n) := \phi(|x_1| \vee \dots \vee |x_n|).$$

Then ϕ_n is nonnegative definite for every $n \in \mathbb{N}$ if and only if ϕ is nonnegative and nonincreasing.

Proof. By Bochner’s theorem for locally compact groups (see Section 36 of [16], also see [24]), the function ϕ_n is nonnegative definite if there exists some \mathcal{K}^n -valued random variable $\xi^{(n)}$ such that $\phi_n(t) = \mathbb{E}[\chi(t \cdot \xi^{(n)})]$ for $t \in \mathcal{K}^n$; that is, ϕ_n is the characteristic function of $\xi^{(n)}$. Using the definition of ϕ_n , this is

$$\mathbb{E}[\chi(t \cdot \xi^{(n)})] = \phi(\|t\|).$$

We claim for $n \in \mathbb{N}$ and $m \in [n]$ that $(\xi_i^{(n)})_{i \in [m]}$ has the same distribution as $\xi^{(m)}$. Indeed, for $t \in \mathcal{K}^m$,

$$\begin{aligned} \mathbb{E}[\chi(t \cdot \xi^{(m)})] &= \phi(|t_1| \vee \dots \vee |t_m|) \\ &= \phi(|t_1| \vee \dots \vee |t_m| \vee 0 \vee \dots \vee 0) \\ &= \mathbb{E}[\chi((t_1, \dots, t_m, 0, \dots, 0) \cdot \xi^{(n)})] \end{aligned}$$

and the uniqueness of characteristic functions completes the proof of the claim. By the Kolmogorov extension theorem, there exists an infinite \mathcal{K} -valued random sequence ξ such that $(\xi_i)_{i \in [n]}$ has the same distribution as $\xi^{(n)}$ for each $n \in \mathbb{N}$.

We next claim that the random sequence ξ is rotatable. Given $n \in \mathbb{N}$ and $U \in \text{GL}_n(\mathcal{D})$,

$$\begin{aligned} \mathbb{E}[\chi(t \cdot U(\xi_i)_{i \in [n]})] &= \mathbb{E}[\chi(U^\top t \cdot (\xi_i)_{i \in [n]})] \\ &= \phi(\|U^\top t\|) \\ &= \phi(\|t\|) \\ &= \mathbb{E}[\chi(t \cdot (\xi_i)_{i \in [n]})], \end{aligned}$$

which shows that $U(\xi_i)_{i \in [n]}$ has the same distribution as $(\xi_i)_{i \in [n]}$.

Using Theorem 3.3, we have that $\xi = \tau\eta$ almost surely, where η is a sequence of independent, identically distributed, standard \mathcal{K} -Gaussian random variables. So ϕ_n is nonnegative definite for each $n \in \mathbb{N}$ if and only if $\phi(\|t\|) = \mathbb{E}[\chi(t \cdot \tau(\eta_i)_{i \in [n]})]$ for each $n \in \mathbb{N}$. Thus

$$\begin{aligned} \phi(\|t\|) &= \mathbb{E}[\chi(t \cdot \tau(\eta_i)_{i \in [n]})] \\ &= \mathbb{E}[\chi((\tau t) \cdot (\eta_i)_{i \in [n]})] \\ &= \mathbb{E}[\mathbb{1}_{\{\|\tau t\| \leq 1\}}] \\ &= \begin{cases} 1, & \|t\| = 0, \\ \mathbb{P}\{|\tau| \leq \frac{1}{\|t\|}\}, & \|t\| \neq 0. \end{cases} \end{aligned}$$

This is equivalent to ϕ having the desired properties. □

References

- [1] E. Borel, *Sur les principes de la théorie cinétique des gaz*, Annales scientifiques de l’É.N.S. 3^e serie **23** (1906), 9–32.

Rotatable sequences

- [2] E. Borel, *Introduction géométrique à quelques théories physiques*, Gauthier-Villars, Paris, 1914.
- [3] A. P. Dawid, *Extendibility of spherical matrix distributions*, J. Multivariate Anal. **8** (1978), no. 4, 559–566. MR-520963
- [4] Persi Diaconis and David Freedman, *A dozen de Finetti-style results in search of a theory*, Ann. Inst. H. Poincaré Probab. Statist. **23** (1987), no. 2, suppl., 397–423. MR-898502
- [5] Persi W. Diaconis, Morris L. Eaton, and Steffen L. Lauritzen, *Finite de Finetti theorems in linear models and multivariate analysis*, Scand. J. Statist. **19** (1992), no. 4, 289–315. MR-1211786
- [6] Morris L. Eaton, *On the projections of isotropic distributions*, Ann. Statist. **9** (1981), no. 2, 391–400. MR-606622
- [7] Steven N. Evans, *Local field Gaussian measures*, Seminar on Stochastic Processes, 1988 (Gainesville, FL, 1988), Progr. Probab., vol. 17, Birkhäuser Boston, Boston, MA, 1989, pp. 121–160. MR-990478
- [8] Steven N. Evans, *Local fields, Gaussian measures, and Brownian motions*, Topics in probability and Lie groups: boundary theory, CRM Proc. Lecture Notes, vol. 28, Amer. Math. Soc., Providence, RI, 2001, pp. 11–50. MR-1832433
- [9] Steven N. Evans, *Elementary divisors and determinants of random matrices over a local field*, Stochastic Process. Appl. **102** (2002), no. 1, 89–102. MR-1934156
- [10] David A. Freedman, *Invariants under mixing which generalize de Finetti's theorem*, Ann. Math. Statist **33** (1962), 916–923. MR-0156369
- [11] Olav Kallenberg, *Foundations of modern probability*, second ed., Probability and its Applications (New York), Springer-Verlag, New York, 2002. MR-1876169
- [12] Olav Kallenberg, *Probabilistic symmetries and invariance principles*, Probability and its Applications (New York), Springer, New York, 2005. MR-2161313
- [13] Douglas Kelker, *Distribution theory of spherical distributions and a location-scale parameter generalization*, Sankhyā Ser. A **32** (1970), 419–438. MR-0287628
- [14] J. F. C. Kingman, *On random sequences with spherical symmetry*, Biometrika **59** (1972), 492–494. MR-0343420
- [15] Gérard Letac, *Isotropy and sphericity: some characterisations of the normal distribution*, Ann. Statist. **9** (1981), no. 2, 408–417. MR-606624
- [16] Lynn H. Loomis, *An introduction to abstract harmonic analysis*, D. Van Nostrand Company, Inc., Toronto-New York-London, 1953. MR-0054173
- [17] J. C. Maxwell, *Theory of heat*, 4th ed., Longmans, London, 1875.
- [18] J. C. Maxwell, *On Boltzmann's theorem on the average distribution of energy in a system of material points*, Trans. Cambridge Phil. Soc. **12** (1878), 547.
- [19] W. H. Schikhof, *Ultrametric calculus*, Cambridge Studies in Advanced Mathematics, vol. 4, Cambridge University Press, Cambridge, 2006, An introduction to p -adic analysis, Reprint of the 1984 original [MR0791759]. MR-2444734
- [20] I. J. Schoenberg, *Metric spaces and positive definite functions*, Trans. Amer. Math. Soc. **44** (1938), no. 3, 522–536. MR-1501980
- [21] A. F. M. Smith, *On random sequences with centred spherical symmetry*, J. Roy. Statist. Soc. Ser. B **43** (1981), no. 2, 208–209. MR-626767
- [22] M. H. Taibleson, *Fourier analysis on local fields*, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1975. MR-0487295
- [23] A. C. M. van Rooij, *Non-Archimedean functional analysis*, Monographs and Textbooks in Pure and Applied Math., vol. 51, Marcel Dekker, Inc., New York, 1978. MR-512894
- [24] André Weil, *L'intégration dans les groupes topologiques et ses applications*, Actual. Sci. Ind., no. 869, Hermann et Cie., Paris, 1940, [This book has been republished by the author at Princeton, N. J., 1941.]. MR-0005741

Acknowledgments. We thank Persi Diaconis and an anonymous referee for a number of helpful suggestions.