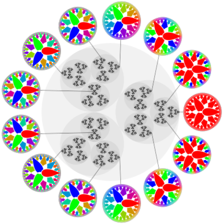
Rotatable random sequences in local fields

Steven N. Evans

U.C. Berkeley

October, 2017



Collaborator

Daniel Raban, U.C. Berkeley

Recall that the linear isometries of $\mathbb{R}^n$ are given by matrices $U \in O(n, \mathbb{R})$ (i.e. $U^\top U = UU^\top = I$).

Definition

A real random vector $\xi = (\xi_1, \ldots, \xi_n)$ is rotatable if $U\xi \stackrel{d}{=} \xi$ for all $U \in O(n, \mathbb{R})$ (i.e. the distribution of ξ is spherically symmetric).

Theorem (Maxwell)

Let $\xi_1, \ldots, \xi_n$, $n \geq 2$, be i.i.d. real random variables. Then $(\xi_1, \ldots, \xi_n)$ is rotatable if and only if the ξ_k are centered Gaussian.

Theorem (Maxwell, Borel)

For each $n \in \mathbb{N}$, let the random vector $(\xi_{n1}, \ldots, \xi_{nn})$ be uniform on the unit sphere in $\mathbb{R}^n$, and let $\eta_1, \eta_2, \ldots$ be i.i.d. standard normal random variables. Then, for each $k \in \mathbb{N}$,

$$\lim_{n \to \infty} \|\mathcal{L}(\sqrt{n}(\xi_{n1}, \ldots, \xi_{nk})) - \mathcal{L}(\eta_1, \ldots, \eta_k)\|_{\mathrm{TV}} = 0.$$

Rotatable real random sequences

Definition

A real random infinite sequence $\xi = (\xi_1, \xi_2, \ldots)$ is rotatable if $(\xi_1, \ldots, \xi_n)$ is rotatable for all $n \in \mathbb{N}$.

Theorem (Freedman)

A real random infinite sequence $\xi = (\xi_1, \xi_2, \ldots)$ is rotatable if and only if $\xi_j = \sigma \eta_j$ a.s. for all $j \in \mathbb{N}$ for some i.i.d. standard normal random variables $\eta_1, \eta_2, \ldots$ (possibly defined on an extension of the original probability space) and an a.s. unique nonnegative random variable σ that is independent of $\eta_1, \eta_2, \ldots$.

Definition

- Fix a positive prime p.
- We can write any non-zero rational number $r \in \mathbb{Q}\backslash\{0\}$ uniquely as $r = p^s(a/b)$, where a and b are not divisible by p. Set $|r| := p^{-s}$ and $|0| := 0$.
- The valuation map $|\cdot|$ has the properties:

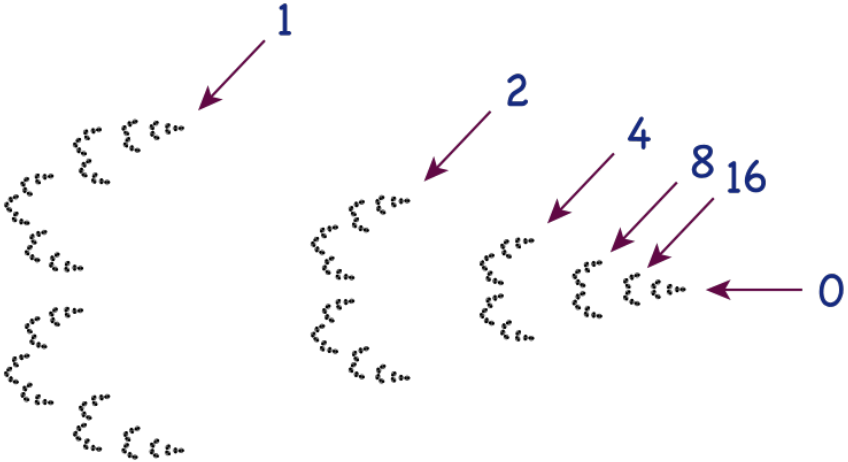
$$
\begin{aligned}
|x| = 0 &\iff x = 0 \\
|xy| &= |x||y| \\
|x + y| &\le |x| \vee |y|
\end{aligned}
$$

- The map $(x, y) \mapsto |x - y|$ defines a metric on $\mathbb{Q}$.
- We denote the completion of $\mathbb{Q}$ in this metric by $\mathbb{Q}_p$.
- The field operations on $\mathbb{Q}$ extend continuously to make $\mathbb{Q}_p$ a topological field called the p-adic numbers.
- The map $|\cdot|$ also extends continuously.

Properties of $\mathbb{Q}_p$

- The closed unit ball around 0, $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x| \le 1\}$ (= the closure in $\mathbb{Q}_p$ of the integers $\mathbb{Z}$), is a ring called the p-adic integers.
- As $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x| < p\}$, the set $\mathbb{Z}_p$ is also open.
- Any ball around 0 is of the form $\{x \in \mathbb{Q}_p : |x| \le p^{-k}\} = p^k \mathbb{Z}_p$ for some integer k.
- Such a ball is the closure of the rational numbers divisible by p^k and is a $\mathbb{Z}_p$-module (in particular, an additive subgroup of $\mathbb{Q}_p$).
- Arbitrary balls are translates (cosets) of these closed and open subgroups.
- As the topology of $\mathbb{Q}_p$ has a base of closed and open sets, $\mathbb{Q}_p$ is totally disconnected.
- As these balls are compact, $\mathbb{Q}_p$ is locally compact.

A picture of $\mathbb{Z}_2$



Definition

A local field is any locally compact, non-discrete field other than $\mathbb{R}$ or $\mathbb{C}$.

Theorem

A local field is totally disconnected, and is either a finite algebraic extension of the field of p-adic numbers or a finite algebraic extension of the p-series field ($:=$ the field of formal Laurent series with coefficients drawn from the finite field with p elements).

- Let $\mathcal{K}$ be a local field.
- There is a valuation map $|\cdot| : \mathcal{K} \to \{q^k : k \in \mathbb{Z}\} \cup \{0\}$, where $q = p^c$ for some prime p and $c \in \mathbb{N}$, such that

$$|x| = 0 \iff x = 0$$
$$|xy| = |x||y|$$
$$|x + y| \le |x| \vee |y|$$

- The metric $(x, y) \mapsto |x - y|$ induces the topology on $\mathcal{K}$.
- The ring of integers $\mathcal{D} := \{x \in \mathcal{K} : \|x\| \le 1\}$ is a compact, open ring.
- Fix $\rho \in \mathcal{K}$ with $|\rho| = q^{-1}$.
- All balls are of the form $x + \rho^k \mathcal{D}$ for $x \in \mathcal{K}$ and $k \in \mathbb{Z}$.

Definition

For $x = (x_1, \dots, x_n) \in \mathcal{K}^n$ set $\|x\| := \bigvee_{i=1}^n |x_i|$.

Definition

Say that the vectors $x_1 = (x_{11}, \dots, x_{1n}), \dots, x_k = (x_{k1}, \dots, x_{kn})$ are orthogonal if

$$\left\| \sum_{j=1}^k \alpha_j x_j \right\| = \bigvee_{j=1}^k |\alpha_j| \|x_j\|$$

for all $\alpha_1, \dots, \alpha_k \in \mathcal{K}$.

Definition

Say that the vectors $x_1 = (x_{11}, \dots, x_{1n}), \dots, x_k = (x_{k1}, \dots, x_{kn})$ are orthonormal if they are orthogonal and $\|x_j\| = 1$ for all j.

Linear isometries

Theorem

The following are equivalent for an $n \times n$ *matrix* U *with entries in* $\mathcal{K}$.

- $\|Ux\| = \|x\|$ *for all* $x \in \mathcal{K}^n$,
- *the columns of* U *are orthonormal,*
- *the rows of* U *are orthonormal,*
- U *is invertible and the entries of* U *and* U^{-1} *belong to* $\mathcal{D}$ *(i.e.* $M \in \mathrm{GL}(n, \mathcal{D})$*),*
- *the entries of* U *belong to* $\mathcal{D}$ *and* $|\det(U)| = 1$.

Haar measure

- There is a unique Borel measure λ on $\mathcal{K}$ such that
  - $\lambda(x + A) = \lambda(A)$ for $x \in \mathcal{K}$ and $A \in \mathcal{B}(\mathcal{K})$,
  - $\lambda(xA) = |x|\lambda(A)$ for $x \in \mathcal{K}$ and $A \in \mathcal{B}(\mathcal{K})$,
  - $\lambda(\mathcal{D}) = 1$.

Local field Gaussian random variables

Definition

A $\mathcal{K}$-valued random variable η is $\mathcal{K}$-Gaussian if either $\eta = 0$ a.s. or for some $k \in \mathbb{Z}$

$$\mathbb{P}\{\eta \in A\} = \frac{\lambda(A \cap \rho^k \mathcal{D})}{\lambda(\rho^k \mathcal{D})}.$$

Say that η is standard $\mathcal{K}$-Gaussian if

$$\mathbb{P}\{\eta \in A\} = \lambda(A \cap \mathcal{D}).$$

What???

We will see why this is the "right" analogue in a moment, but note the following.

- A standard (real) Gaussian has distribution

$$\frac{1}{\sqrt{2\pi}} \exp\left(-\frac{x^2}{2}\right)\, dx.$$

- Any group character for $\mathbb{R}$ is of the form $x \mapsto \exp(izx)$, $z \in \mathbb{R}$.
- A standard (real) Gaussian has Fourier transform

$$z \mapsto \int_{\mathbb{R}} \exp(izx) \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{x^2}{2}\right)\, dx = \exp\left(-\frac{z^2}{2}\right).$$

- A standard $\mathcal{K}$-Gaussian has distribution

$$\mathbb{1}_{\mathcal{D}}(x)\, \lambda(dx).$$

- Any group character for $\mathcal{K}$ is of the form $x \mapsto \chi(zx)$, $z \in \mathbb{K}$, where χ is some fixed character that is 1 on $\mathcal{D}$ but not constant on $\rho^{-1}\mathcal{D}$
- A standard $\mathcal{K}$-Gaussian has Fourier transform

$$z \mapsto \int_{\mathcal{D}} \chi(zx) \mathbb{1}_{\mathcal{D}}(x)\, \lambda(dx) = \mathbb{1}_{\mathcal{D}}(z).$$

Definition

A $\mathcal{K}$-valued random vector $\xi = (\xi_1, \ldots, \xi_n)$ is rotatable if $U\xi \stackrel{d}{=} \xi$ for all $U \in \mathrm{GL}(n, \mathcal{D})$.

Theorem (E.)

Let $\xi_1, \ldots, \xi_n$, $n \geq 2$, be i.i.d. $\mathcal{K}$-valued random variables. Then $(\xi_1, \ldots, \xi_n)$ is rotatable if and only if the ξ_k are $\mathcal{K}$-Gaussian.

Uniform distribution on the "unit sphere"

Corollary (E. & Raban)

The following are equivalent:

- ν *is the unique probability measure supported on* $\{x \in \mathcal{K}^n : \|x\| = 1\}$ *such that* $\nu(UA) = \nu(A)$ *for all* $U \in \mathrm{GL}(n, \mathcal{D})$ *and* $A \in \mathcal{B}(\mathcal{K}^n)$,
- ν *is the distribution of* $\tau(\eta)^{-1}\eta$, *where* $\eta = (\eta_1, \ldots, \eta_n)$ *with* $\eta_1, \ldots \eta_n$ *i.i.d. standard* $\mathcal{K}$*-Gaussian random variables and* $\tau : \mathcal{K}^n \to \{\rho^k : k \in \mathbb{Z}\} \cup \{0\}$ *is defined by*

$$\tau(x) := \begin{cases} \rho^k, & \text{if } \|x\| = q^{-k}, \\ 0, & \text{if } \|x\| = 0. \end{cases}$$

- ν *is the conditional distribution of* η *given the event* $\{\|\eta\| = 1\}$, *where* $\eta = (\eta_1, \ldots, \eta_n)$ *with* $\eta_1, \ldots \eta_n$ *i.i.d. standard* $\mathcal{K}$*-Gaussian random variables.*

Asymptotics of uniforms on the “unit sphere”

Theorem (E. & Raban)

For each $n \in \mathbb{N}$, let the random vector $(\xi_{n1}, \ldots, \xi_{nn})$ be uniform on $\{x \in \mathcal{K}^n : \|x\| = 1\}$ and let $\eta_1, \eta_2, \ldots$ be i.i.d. standard $\mathcal{K}$-Gaussian random variables. Then, for $1 \le k \le n$,

$$\|\mathcal{L}(\xi_{n1}, \ldots, \xi_{nk}) - \mathcal{L}(\eta_1, \ldots, \eta_k)\|_{\mathrm{TV}} = \frac{q^{-n}(1 - q^{-k})}{1 - q^{-n}}.$$

Definition

A $\mathcal{K}$-valued random infinite sequence $\xi = (\xi_1, \xi_2, \ldots)$ is rotatable if $(\xi_1, \ldots, \xi_n)$ is rotatable for all $n \in \mathbb{N}$.

Theorem (E. & Raban)

A $\mathcal{K}$-valued random infinite sequence $\xi = (\xi_1, \xi_2, \ldots)$ is rotatable if and only if $\xi_j = \sigma\eta_j$ a.s. for all $j \in \mathbb{N}$ for some i.i.d. standard $\mathcal{K}$-Gaussian random variables $\eta_1, \eta_2, \ldots$ (possible defined on an extension of the original probability space) and a random variable σ that is independent of $\eta_1, \eta_2, \ldots$, takes values in $\{\rho^k : k \in \mathbb{Z}\} \cup \{0\}$, and is given by

$$\sigma := \begin{cases} \rho^k, & \text{if } \sup_j |\xi_j| = q^{-k}, \\ 0, & \text{if } \sup_j |\xi_j| = 0. \end{cases}$$

(In particular, $\sup_j |\xi_j|$ is almost surely finite for any rotatable random infinite sequence $\xi = (\xi_1, \xi_2, \ldots)$.)

Proof

- Put
$$\sigma_n := \tau(\xi_1, \ldots, \xi_n) = \begin{cases} \rho^k, & \text{if } \|(\xi_1, \ldots, \xi_n)\| = q^{-k}, \\ 0, & \text{if } \|(\xi_1, \ldots, \xi_n)\| = 0. \end{cases}$$
- Let $(\tilde{\xi}_{n1}, \ldots, \tilde{\xi}_{nn})$ be uniform on $\{x \in \mathcal{K}^n : \|x\| = 1\}$ and independent of σ_n.
- Observe that $(\xi_1, \ldots, \xi_n) \stackrel{d}{=} \sigma_n(\tilde{\xi}_{n1}, \ldots, \tilde{\xi}_{nn})$ be rotatability.
- Let $\tilde{\eta}_1, \tilde{\eta}_2, \ldots$ be i.i.d. standard $\mathcal{K}$-Gaussian random variables independent of $\sigma_1, \sigma_2, \ldots$.
- Note that
$$\begin{aligned} &\|\mathcal{L}(\xi_1, \ldots, \xi_k) - \mathcal{L}(\sigma_n(\tilde{\eta}_1, \ldots, \tilde{\eta}_k))\|_{\mathrm{TV}} \\ &\quad = \|\mathcal{L}(\sigma_n(\tilde{\xi}_{n1}, \ldots, \tilde{\xi}_{nk})) - \mathcal{L}(\sigma_n(\tilde{\eta}_1, \ldots, \tilde{\eta}_k))\|_{\mathrm{TV}} \\ &\quad \leq \|\mathcal{L}(\tilde{\xi}_{n1}, \ldots, \tilde{\xi}_{nk}) - \mathcal{L}(\tilde{\eta}_1, \ldots, \tilde{\eta}_k)\|_{\mathrm{TV}} \\ &\quad \to 0 \quad \text{as } n \to \infty. \end{aligned}$$
- Thus, $\sigma_n \tilde{\eta} \xrightarrow{d} \xi$.

Proof – continued

Now $|\sigma_n| = \|(\xi_1, \ldots, \xi_n)\| = \bigvee_{i=1}^n |\xi_i|$ is increasing with n and

$$
\begin{aligned}
0 &= \inf_m \mathbb{P}\{|\xi_1| > q^m\} \\
&= \inf_m \lim_n \mathbb{P}\{|\sigma_n \tilde{\eta}_1| > q^m\} \\
&= \inf_m \sup_n \mathbb{P}\{|\sigma_n \tilde{\eta}_1| > q^m\} \\
&= \inf_m \sup_n \sum_{\ell=0}^{\infty} \mathbb{P}\{|\sigma_n| > q^{m+\ell}\}\mathbb{P}\{|\tilde{\eta}_1| = q^{-\ell}\} \\
&= \sum_{\ell=0}^{\infty} \inf_m \sup_n \mathbb{P}\{|\sigma_n| > q^{m+\ell}\}\mathbb{P}\{|\tilde{\eta}_1| = q^{-\ell}\} \\
&= \sum_{\ell=0}^{\infty} \inf_m \mathbb{P}\{\sup_n |\sigma_n| > q^{m+\ell}\}\mathbb{P}\{|\tilde{\eta}_1| = q^{-\ell}\} \\
&= \mathbb{P}\{\sup_n |\sigma_n| = \infty\}
\end{aligned}
$$

so that $\sigma_n \stackrel{a.s.}{\to} \sigma$ for some random variable σ taking values in $\{\rho^k : k \in \mathbb{Z}\} \cup \{0\}$.

Proof – completed

- Therefore, $\xi \stackrel{d}{=} \sigma\tilde{\eta}$.
- The "transfer theorem" gives $\xi = \breve{\sigma}\eta$ with $(\breve{\sigma}, \eta) \stackrel{d}{=} (\sigma, \tilde{\eta})$.
- It remains to observe that

$$\begin{aligned} |\sigma| &= \sup_n \|(\xi_1, \ldots, \xi_n)\| \\ &= \sup_n \|\breve{\sigma}(\eta_1, \ldots, \eta_n)\| \\ &= \sup_n |\breve{\sigma}| \|(\eta_1, \ldots, \eta_n)\| \\ &= |\breve{\sigma}| \sup_n \|(\eta_1, \ldots, \eta_n)\| \\ &= |\breve{\sigma}|, \end{aligned}$$

so that $\breve{\sigma} = \sigma$.

Theorem (Schoenberg)

Let $f : \mathbb{R}_+ \to \mathbb{R}$ *be a continuous function with* $f(0) = 1$. *For* $n \in \mathbb{N}$ *define* $f_n : \mathbb{R}^n \to \mathbb{R}$ *by*

$$f_n(x_1, \ldots, x_n) := f(x_1^2 + \cdots + x_n^2).$$

Then f_n *is nonnegative definite for every* $n \in \mathbb{N}$ *if and only if* f *is completely monotone.*

Theorem (E. & Raban)

Let $f : \{q^k : k \in \mathbb{Z}\} \cup \{0\} \to \mathbb{R}$ *be such that* $\lim_{k \to \infty} f(q^{-k}) = f(0) = 1$. *For* $n \in \mathbb{N}$ *define* $f_n : \mathcal{K}^n \to \mathbb{R}$ *by*

$$f_n(x_1, \ldots, x_n) := f(|x_1| \vee \cdots \vee |x_n|).$$

Then f_n *is nonnegative definite for every* $n \in \mathbb{N}$ *if and only if* f *is nonnegative and nonincreasing.*

Reminder: transfer theorem / stochastic equations (Kallenberg)

Lemma

Fix two Borel spaces S and T, a measurable mapping $f : S \to T$, and random elements α in S and β in T with $\beta \stackrel{d}{=} f(\alpha)$. Then there exists (possibly on an extension of the original probability space) a random element $\hat{\alpha} \stackrel{d}{=} \alpha$ in S with $\beta = f(\hat{\alpha})$ a.s.