THE EXPECTED NUMBER OF ZEROS OF A RANDOM SYSTEM OF p-ADIC POLYNOMIALS

STEVEN N. EVANS

Abstract. We study the simultaneous zeros of a random family of d polynomials in d variables over the p-adic numbers. For a family of natural models, we obtain an explicit constant for the expected number of zeros that lie in the d-fold Cartesian product of the p-adic integers. This expected value, which is

$$\left(1 + p^{-1} + p^{-2} + \cdots + p^{-d}\right)^{-1}$$

for the simplest model, is independent of the degree of the polynomials.

1. Introduction

The distribution of the number of real roots of a random polynomial appears to have been first studied in [Kac43b, Kac43a, Kac49], where the main result is that the expected number of roots of a degree n polynomial with independent standard Gaussian coefficients is asymptotically equivalent to $\frac{2}{\pi}\log n$ for large n. There has since been a huge amount of work on various aspects of the distribution of the roots of random polynomials and systems of random polynomials for a wide range of models with coefficients that are possibly dependent and have distributions other than Gaussian. It is impossible to survey this work adequately, but some of the more commonly cited early papers are [LS68a, LS68b, IM71a, IM71b]. Reviews of the literature can be found in [BRS86, EK95, EK96, Far98], and some recent papers that indicate the level of sophistication that has been achieved in terms of results and methodology are [SV95, IZ97, BR02, Ble99, DPSZ02, SZ03a, SZ04, SZ03b, Wsc05].

1991 *Mathematics Subject Classification.* Primary: 60B99, 30G15; Secondary: 11S80, 30G06.

Key words and phrases. co-area formula, Kac-Rice formula, local field, Gaussian, q-binomial formula, random matrix.

Supported in part by NSF grant DMS-0405778. Part of the research was conducted during a visit to the American Institute of Mathematics for a Workshop on Random Analytic Functions.

In this paper we study the roots of random polynomials over a field other than the real or complex numbers, the field of p-adic numbers for some prime p. Like the reals, the p-adics arise as a completion of the rationals with respect to certain metric – see below. They are the prototypical local fields (that is, non-discrete, locally compact topological fields) and any local field with characteristic zero is a finite algebraic extension of the p-adic numbers (the local fields with non-zero characteristic are finite algebraic extensions of the p-series field of Laurent series over the finite field with p elements).

In order to describe our results we need to give a little background.

We begin with defining the p-adic numbers. 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 $|r| = p^{-s}$. If we set $|0| = 0$, then the map $|\cdot|$ has the properties:

$$\begin{aligned} |x| = 0 &\Leftrightarrow x = 0, \\ |xy| &= |x||y|, \\ |x+y| &\leq |x| \vee |y|. \end{aligned} \tag{1}$$

The map $(x, y) \mapsto |x - y|$ defines a metric on $\mathbb{Q}$, and 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 and the extension has properties (1). The closed unit ball around 0, $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x| \leq 1\}$, is the closure in $\mathbb{Q}_p$ of the integers $\mathbb{Z}$, and is thus a ring (this is also apparent from (1)), 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 other ball around 0 is of the form $\{x \in \mathbb{Q}_p : |x| \leq p^{-k}\} = p^k\mathbb{Z}_p$ for some integer k. Such a ball is the closure of the rational numbers divisible by p^k, and is thus a $\mathbb{Z}_p$-sub-module (this is again also apparent from (1)). In particular, such a ball is an additive subgroup of $\mathbb{Q}_p$. Arbitrary balls are translates (= cosets) of these closed and open subgroups. In particular, the topology of $\mathbb{Q}_p$ has a base of closed and open sets, and hence $\mathbb{Q}_p$ is totally disconnected. Further, each of these balls is compact, and hence $\mathbb{Q}_p$ is also locally compact.

There is a unique Borel measure λ on $\mathbb{Q}_p$ for which

$$\begin{aligned} \lambda(x + A) &= \lambda(A), \quad x \in \mathbb{Q}_p, \\ \lambda(xA) &= |x|\lambda(A), \quad x \in \mathbb{Q}_p, \\ \lambda(\mathbb{Z}_p) &= 1. \end{aligned}$$

The measure λ is just suitably normalized Haar measure on the additive group of $\mathbb{Q}_p$. The restriction of λ to $\mathbb{Z}_p$ is the weak limit as $n \to \infty$

of the sequence of probability measures that at the n-th stage assigns mass p^{-n} to each of the points $\{0, 1, \ldots, p^n - 1\}$.

We have shown in a sequence papers [Eva89, Eva91, Eva93, Eva95, Eva01b, Eva01a, Eva02] that the natural analogues on $\mathbb{Q}_p$ of the centered Gaussian measures on $\mathbb{R}$ are the normalized restrictions of λ to the compact $\mathbb{Z}_p$-sub-modules $p^k\mathbb{Z}_p$ and the point mass at 0. More generally, the natural counterparts of centered Gaussian measures for $\mathbb{Q}_p^d$ are normalized Haar measures on compact $\mathbb{Z}_p$-sub-modules. We call such probability measures $\mathbb{Q}_p$-*Gaussian* and say that a random variable distributed according to normalized Haar measure on $\mathbb{Z}_p^d$ is *standard* $\mathbb{Q}_p$-Gaussian. There is a substantial literature on probability on the p-adics and other local fields. The above papers contain numerous references to this work, much of which concerns Markov processes taking values in local fields. There are also extensive surveys of the literature in the books [Khr97, Koc01, KN04].

If we equip the space of continuous functions $C(\mathbb{Z}_p^d, \mathbb{Q}_p)$ with the map $f \mapsto \|f\| := \sup\{|f(t)| : t \in \mathbb{Z}_p^d\}$, then $\|\cdot\|$ is a p-adic norm in the sense that

$$\begin{aligned}\|f\| &= 0 \Leftrightarrow f = 0,\\ \|af\| &= |a|\|f\|, \quad a \in \mathbb{Q}_p,\ f \in C(\mathbb{Z}_p^d, \mathbb{Q}_p),\\ \|f+g\| &\le \|f\| \vee \|g\|.\end{aligned}$$

Moreover, $C(\mathbb{Z}_p^d, \mathbb{Q}_p)$ is a p-adic Banach space in the sense that it is complete with respect to the metric $(f, g) \mapsto \|f - g\|$.

There is a natural notion of orthogonality on the space $C(\mathbb{Z}_p^d, \mathbb{Q}_p)$. A collection $\{f_0, f_1, \ldots\}$ is *orthogonal* if $\|\sum_{k=0}^n a_k f_k\| = \bigvee_{k=0}^n |a_k|\|f_k\|$ for any n and any $a_k \in \mathbb{Q}_p$. At first glance, this looks completely unlike the notion of orthogonality one is familiar with in real and complex Hilbert spaces, but it can be seen from [Sch84] that there are actually close parallels. It is apparent from [Sch84] that the sequence of functions $\{t \mapsto \binom{t}{k}\}_{k=0}^\infty$, where $\binom{t}{k} := \frac{t(t-1)\cdots(t-k+1)}{k!}$ (the *Mahler basis*) is a very natural *orthonormal* basis for $C(\mathbb{Z}_p, \mathbb{Q}_p)$ (that is, it is orthogonal and each element has unit norm). It is not hard to see that the functions

$$(t_1, t_2, \ldots, t_d) \mapsto \binom{t_1}{k_1}\binom{t_2}{k_2}\cdots\binom{t_d}{k_d}, \quad 0 \le k_1, k_2, \ldots, k_d < \infty,$$

are an orthonormal basis for $C(\mathbb{Z}_p^d, \mathbb{Q}_p)$.

Putting all of these ingredients together, we see that a natural model for a random system of d independent $\mathbb{Q}_p$-valued polynomials in d variables lying in $\mathbb{Z}_p$ is the system

$$F_i(t_1, t_2, \ldots, t_d) := \sum_k a_{i,k} Z_{i,k} \binom{t_1}{k_1}\binom{t_2}{k_2}\cdots\binom{t_d}{k_d}, \quad 1 \le i \le d,$$

where the sum is over multi-indices $k = (k_1, k_2, \ldots, k_d)$, for each i the constants $a_{i,k} \in \mathbb{Q}_p$ are zero for all but finitely many k, and the $\mathbb{Q}_p$-valued random variables are independent and standard $\mathbb{Q}_p$-Gaussian distributed.

To avoid degeneracies, we assume that $a_{i,0} \neq 0$ and $a_{i,e_j} \neq 0$ for $1 \le i, j, \le d$, where $e_1 := (1, 0, 0, \ldots, 0)$, $e_2 := (0, 1, 0, \ldots, 0)$, and so on. By re-scaling, we can assume without loss of generality that $a_{i,0} = 1$ for $1 \le i \le d$. We will also suppose that $a_{i,e_j} = a_{e_j}$ for some $a_{e_j} \in \mathbb{Q}_p$ that does not depend on i (this includes the case where the F_i are identically distributed) and that for each i we have $|a_{i,k}| \ge |a_{i,\ell}|$ when $k \le \ell$ in the usual partial order on multi-indices. It follows from the orthonormality of the products of Mahler basis elements that each $(F_1, F_2, \ldots, F_d)$ maps $\mathbb{Z}_p^d$ into $\mathbb{Z}_p^d$.

Theorem 1.1. *Given $(x_1, x_2, \ldots, x_d) \in \mathbb{Z}_p^d$, the expected number of points in the set*

$$\{(t_1, t_2, \ldots, t_d) \in \mathbb{Z}_p^d : F_i(t_1, t_2, \ldots, t_d) = x_i,\ 1 \le i \le d\}$$

is

$$\left[\prod_{j=1}^d |a_{e_j}|\right] \frac{1 - p^{-1}}{1 - p^{-(d+1)}} = \left[\prod_{j=1}^d |a_{e_j}|\right] \left(1 + p^{-1} + p^{-2} + \cdots + p^{-d}\right)^{-1}.$$

We give the proof in Section 3 after some preliminaries in Section 2. Note that expected value described in the theorem is independent of the degree of the polynomials F_i.

This paper appears to be the first to consider roots of random polynomials over the p-adic field. There has been some work on random polynomials over finite fields, see [Odo92, ABT93, IM96, Pan04, DP04].

2. Preliminaries

Write λ_d for the d-fold product measure $\lambda^{\otimes d}$. Thus λ_d is Haar measure on the additive group of $\mathbb{Q}_p^d$ normalized so that $\lambda_d(\mathbb{Z}_p^d) = 1$. The Euclidean analogue of the following result is well-known.

Lemma 2.1. *For a Borel set $A \subseteq \mathbb{Q}_p^d$ and a $d \times d$ matrix H, the set $H(A)$ has Haar measure $\lambda_d(H(A)) = |\det(H)|\lambda_d(A)$.*

Proof. If H is singular, then the range of H is a lower dimensional subspace of $\mathbb{Q}_p^d$ and the result is obvious.

Suppose then that H is invertible. Write $GL(d, \mathbb{Z}_p)$ for the space of $d \times d$ matrices that have entries in $\mathbb{Z}_p$ and are invertible with the inverse also having entries in $\mathbb{Z}_p$. By Cramer's rule, a matrix W is in $GL(d, \mathbb{Z}_p)$ if and only if it has entries in $\mathbb{Z}_p$ and $|\det(W)| = 1$. Moreover, $GL(d, \mathbb{Z}_p)$ is the set of linear isometries of $\mathbb{Q}_p^d$ equipped with the metric derived from the norm $|(x_1, x_2, \ldots, x_d)| = \bigvee_{i=1}^d |x_i|$ (see Section 3 of [Eva02]). From the representation of H in terms of its elementary divisors, we have

$$H = U\mathrm{diag}(p^{k_1}, p^{k_2}, \ldots, p^{k_d})V,$$

for integers $k_1, \ldots, k_d$ and matrices $U, V \in GL(d, \mathbb{Z}_p)$ (see Theorem 3.1 of [Eva02]). Because $|\det(U)| = |\det(V)| = 1$, it follows that $|\det(H)| = p^{-(k_1+\cdots+k_d)}$.

From the uniqueness of Haar measure, $\lambda_d \circ U$ and $\lambda_d \circ V$ are both constant multiples of λ_d. Both U and V map the ball $\mathbb{Z}_p^d$ bijectively onto itself. Thus $\lambda_d \circ U = \lambda_d \circ V = \lambda_d$.

Again from the uniqueness of Haar measure, $\lambda_d \circ \mathrm{diag}(p^{k_1}, p^{k_2}, \ldots, p^{k_d})$ is a constant multiple of λ_d. Now

$$\begin{aligned}
\lambda_d \circ \mathrm{diag}(p^{k_1}, p^{k_2}, \ldots, p^{k_d})(\mathbb{Z}_p^d) &= \lambda_d\left(\prod_{j=1}^d p^{k_j}\mathbb{Z}_p\right) \\
&= \prod_{j=1}^d \lambda(p^{k_j}\mathbb{Z}_p) \\
&= p^{-(k_1+\cdots+k_d)} \\
&= |\det(H)| \\
&= |\det(H)|\lambda_d(\mathbb{Z}_p^d).
\end{aligned}$$

□

Write $gl(d, \mathbb{Q}_p)$ for the space of $d \times d$ matrices with entries in $\mathbb{Q}_p$. We say that a function f from an open subset X of $\mathbb{Q}_p^d$ into $\mathbb{Q}_p^d$ is *continuously differentiable* if there exists a continuous function $R : X \times X \to gl(d, \mathbb{Q}_p)$ such that $f(x) - f(y) = R(x, y)(x - y)$. This definition is a natural generalization of Definition 27.1 of [Sch84] for the case $d = 1$. Set $Jf(x) = R(x, x)$.

The next result is along the lines of the Euclidean implicit function theorem. It follows from Lemma 2.1 and arguments similar to those which establish the analogous results for $d = 1$ in Proposition 27.3, Lemma 27.4, and Theorem 27.5 of [Sch84].

Lemma 2.2. *Suppose for some open subset X of $\mathbb{Q}_p^d$ that $f : X \to \mathbb{Q}_p^d$ is continuously differentiable.*

(i) *If $Jf(x_0)$ is invertible for some $x_0 \in X$, then, for all sufficiently small balls B containing x_0, the function f restricted to B is a bijection onto its image, $f(B) = Jf(x_0)(B)$, and $|\det(Jf(x))| = |\det(Jf(x_0))|$ for $x \in B$. In particular,*

$$\lambda_d(f(B)) = |\det(Jf(x_0))|\, \lambda_d(B).$$

(ii) *If $Jf(x_0)$ is singular for some $x_0 \in X$, then, for all sufficiently small balls B containing x_0, $\lambda_d(f(B)) = \mathrm{o}(\lambda_d(B))$.*

The following result is an analogue of a particular instance of Federer's co-area formula. The special case of this result for $d = 1$ and an injective function is the substitution formula in Appendix A.7 of [Sch84].

Proposition 2.3. *Suppose for some open subset X of $\mathbb{Q}_p^d$ that $f : X \to \mathbb{Q}_p^d$ is continuously differentiable. Then, for any non-negative Borel function $g : \mathbb{Q}_p^d \to \mathbb{Q}_p^d$,*

$$\int_X g \circ f(x)\, |\det(Jf(x))|\, \lambda_d(dx) = \int_{\mathbb{Q}_p^d} g(y)\, \# f^{-1}(y)\, \lambda_d(dy).$$

Proof. It suffices to consider the case when g is the indicator function of a ball C. Write δ for the diameter of C. Put

$$S := \{x \in X : Jf(x) \text{ is singular}\}$$

and

$$I := \{x \in X : Jf(x) \text{ is invertible}\}.$$

From Lemma 2.2(ii), $\lambda_d(f(S)) = 0$, so that

$$\lambda_d(\{y \in \mathbb{Q}_p^d : f^{-1}(y) \cap S \neq \emptyset\}) = 0$$

and

$$\begin{aligned}\int_{\mathbb{Q}_p^d} g(y)\, \#(f^{-1}(y) \cap S)\, \lambda_d(dy) &= 0 \\ &= \int_S g \circ f(x)\, |\det(Jf(x))|\, \lambda_d(dx).\end{aligned}$$

From Lemma 2.2(iii), we can cover the open set I with a countable collection of balls B_k such that f restricted to B_k is a bijection onto its image, $f(B) = Jf(x_0)(B)$ for some $x_0 \in B$, $|\det(Jf(x))| =$

$|\det(Jf(x_0))|$ for all $x \in B_k$, $\lambda_d(f(B_k)) = |\det(Jf(x_0))|\lambda_d(B_k)$, and $\operatorname{diam} f(B_k) \le \delta$, so that g is constant on $f(B_k)$. Hence

$$\begin{aligned}
&\int_{\mathbb{Q}_p^d} g(y)\,\#(f^{-1}(y) \cap B_k)\,\lambda_d(dy) \\
&\quad = \int_{f(B_k)} g(y)\,\lambda_d(dy) \\
&\quad = \int_{B_k} g \circ f(x)\,|\det(Jf(x))|\,\lambda_d(dx)
\end{aligned}$$

Summing over k gives

$$\int_{\mathbb{Q}_p^d} g(y)\,\#(f^{-1}(y) \cap I)\,\lambda_d(dy) = \int_I g \circ f(x)\,|\det(Jf(x))|\,\lambda_d(dx)$$

and the result follows. □

3. Proof of Theorem 1.1

For $x \in \mathbb{Z}_p^d$, write $N(x)$ for the number of points in the set

$$\{(t_1, t_2, \ldots, t_d) \in \mathbb{Z}_p^d : F_i(t_1, t_2, \ldots, t_d) = x_i,\ 1 \le i \le d\}.$$

Since $Z_{i,0} - (x_1, x_2, \ldots, x_d)$ has the same distribution as $Z_{i,0}$, it follows that $\mathbb{E}[N(\cdot)]$ is constant. Also, by an extension of the argument for $d = 1$ in Theorem 9.3 of [Eva89] (see also Theorem 8.2 of [Eva01b]), the stochastic processes F_i are stationary.

Thus, by Proposition 2.3,

$$\begin{aligned}
\mathbb{E}[N(x)] &= \int_{\mathbb{Z}_p^d} \mathbb{E}[N(x)]\,\lambda_d(dx) \\
&= \mathbb{E}\left[\int_{\mathbb{Z}_p^d} N(x)\,\lambda_d(dx)\right] \\
&= \mathbb{E}\left[\int_{\mathbb{Z}_p^d} |\det(JF(t))|\,\lambda_d(dt)\right] \\
&= \int_{\mathbb{Z}_p^d} \mathbb{E}[|\det(JF(t))|]\,\lambda_d(dt) \\
&= \mathbb{E}[|\det(JF(0))|].
\end{aligned}$$

Now

$$(JF(0))_{ij} = a_{e_j} Z_{i,e_j}$$

and so

$$\det(JF(0)) = \left[\prod_{j=1}^{d} a_{e_j}\right] \det\left(Z_{i,e_j}\right)_{1\le i,j\le d}.$$

From Theorem 4.1 in [Eva02], we find, putting

$$\Pi_k := (1-p^{-1})(1-p^{-2})\cdots(1-p^{-k}),$$

that

$$\begin{aligned}\mathbb{E}[|\det(JF(0))|] &= \left[\prod_{j=1}^{d} |a_{e_j}|\right] \sum_{h=0}^{\infty} p^{-h}\mathbb{P}\{|\det\left(Z_{i,e_j}\right)_{1\le i,j\le d}| = p^{-h}\} \\ &= \left[\prod_{j=1}^{d} |a_{e_j}|\right] \sum_{h=0}^{\infty} p^{-2h}\frac{\Pi_d\Pi_{d+h-1}}{\Pi_h\Pi_{d-1}}.\end{aligned}$$

The result then follows from a consequence of the q-binomial theorem, see Corollary 10.2.2 of [AAR99].

Remark 3.1. (i) Results about level sets of Euclidean processes are often obtained using the Kac-Rice formula. As shown in [AW05], result like the Kac-Rice formula are a consequence of Federer's co-area formula (see also [AT06] for an extensive discussion of this topic). It would be possible to derive a p-adic analogue of the Kac-Rice formula from Proposition 2.3 and use it to prove Theorem 1.1. However, the homogeneity in "space" of $(F_1, F_2, \ldots, F_d)$ makes this unnecessary.
(ii) Because $(F_1, F_2, \ldots, F_d)$ is stationary, its level sets are all stationary point processes on $\mathbb{Z}_p^d$ with intensity the multiple of λ_d given in Theorem 1.1.

References

[AAR99] George E. Andrews, Richard Askey, and Ranjan Roy, *Special functions*, Encyclopedia of Mathematics and its Applications, vol. 71, Cambridge University Press, Cambridge, 1999. MR **MR1688958 (2000g:**33001)

[ABT93] Richard Arratia, A. D. Barbour, and Simon Tavaré, *On random polynomials over finite fields*, Math. Proc. Cambridge Philos. Soc. **114** (1993), no. 2, 347–368. MR **MR1230136 (95a:**60011)

[AT06] Robert J. Adler and Jonathan E. Taylor, *Random fields and geometry*, 2006, Book in preparation, prelimary version at `http://iew3.technion.ac.il/~radler/publications.html`.

[AW05] Jean-Marc Azaïs and Mario Wschebor, *On the distribution of the maximum of a Gaussian field with d parameters*, Ann. Appl. Probab. **15** (2005), no. 1A, 254–278. MR **MR2115043 (2005k:**60117)

[Ble99] Pavel Bleher, *Universality and scaling in random matrix models and random polynomials*, Mathematical results in statistical mechanics (Marseilles, 1998), World Sci. Publishing, River Edge, NJ, 1999, pp. 379–398. MR MR1886266

[BR02] Pavel Bleher and Denis Ridzal, SU(1, 1) *random polynomials*, J. Statist. Phys. **106** (2002), no. 1-2, 147–171. MR **MR1881723 (2002k:**82042)

[BRS86] A. T. Bharucha-Reid and M. Sambandham, *Random polynomials*, Probability and Mathematical Statistics, Academic Press Inc., Orlando, FL, 1986. MR **MR856019 (87m:**60118)

[DP04] John D. Dixon and Daniel Panario, *The degree of the splitting field of a random polynomial over a finite field*, Electron. J. Combin. **11** (2004), no. 1, Research Paper 70, 10 pp. (electronic). MR **MR2097336 (2006a:**11165)

[DPSZ02] Amir Dembo, Bjorn Poonen, Qi-Man Shao, and Ofer Zeitouni, *Random polynomials having few or no real zeros*, J. Amer. Math. Soc. **15** (2002), no. 4, 857–892 (electronic). MR **MR1915821 (2003f:**60092)

[EK95] Alan Edelman and Eric Kostlan, *How many zeros of a random polynomial are real?*, Bull. Amer. Math. Soc. (N.S.) **32** (1995), no. 1, 1–37. MR **MR1290398 (95m:**60082)

[EK96] ———, *Erratum: "How many zeros of a random polynomial are real?" [Bull. Amer. Math. Soc. (N.S.)* **32** *(1995), no. 1, 1–37; MR1290398 (95m:60082)]*, Bull. Amer. Math. Soc. (N.S.) **33** (1996), no. 3, 325. MR MR1376652

[Eva89] 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 **MR990478 (91e:**60121)

[Eva91] ———, *Equivalence and perpendicularity of local field Gaussian measures*, Seminar on Stochastic Processes, 1990 (Vancouver, BC, 1990), Progr. Probab., vol. 24, Birkhäuser Boston, Boston, MA, 1991, pp. 173–181. MR **MR1118442 (93m:**60078)

[Eva93] ———, *Local field Brownian motion*, J. Theoret. Probab. **6** (1993), no. 4, 817–850. MR **MR1245397 (94i:**60098)

[Eva95] ———, *p-adic white noise, chaos expansions, and stochastic integration*, Probability measures on groups and related structures, XI (Oberwolfach, 1994), World Sci. Publishing, River Edge, NJ, 1995, pp. 102–115. MR **MR1414928 (98e:**60083)

[Eva01a] ———, *Local field U-statistics*, Algebraic methods in statistics and probability (Notre Dame, IN, 2000), Contemp. Math., vol. 287, Amer. Math. Soc., Providence, RI, 2001, pp. 75–81. MR **MR1873668 (2003b:**60014)

[Eva01b] ———, *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 **MR1832433 (2003e:**60012)

[Eva02] ———, *Elementary divisors and determinants of random matrices over a local field*, Stochastic Process. Appl. **102** (2002), no. 1, 89–102. MR **MR1934156 (2004c:**15041)

[Far98] Kambiz Farahmand, *Topics in random polynomials*, Pitman Research Notes in Mathematics Series, vol. 393, Longman, Harlow, 1998. MR **MR1679392 (2000d:**60092)

[IM71a] I. A. Ibragimov and N. B. Maslova, *The mean number of real zeros of random polynomials. I. Coefficients with zero mean*, Teor. Verojatnost. i Primenen. **16** (1971), 229–248. MR MR0286157 (44 #3371)

[IM71b] ———, *The mean number of real zeros of random polynomials. II. Coefficients with a nonzero mean*, Teor. Verojatnost. i Primenen. **16** (1971), 495–503. MR MR0288824 (44 #6019)

[IM96] G. I. Ivchenko and Yu. I. Medvedev, *Random polynomials over a finite field*, Teor. Veroyatnost. i Primenen. **41** (1996), no. 1, 204–210. MR **MR1404907 (97e:**60016)

[IZ97] Ildar Ibragimov and Ofer Zeitouni, *On roots of random polynomials*, Trans. Amer. Math. Soc. **349** (1997), no. 6, 2427–2441. MR **MR1390040 (97h:**60050)

[Kac43a] M. Kac, *A correction to "On the average number of real roots of a random algebraic equation."*, Bull. Amer. Math. Soc. **49** (1943), 938. MR MR0009655 (5,179g)

[Kac43b] ———, *On the average number of real roots of a random algebraic equation*, Bull. Amer. Math. Soc. **49** (1943), 314–320. MR MR0007812 (4,196d)

[Kac49] ———, *On the average number of real roots of a random algebraic equation. II*, Proc. London Math. Soc. (2) **50** (1949), 390–408. MR MR0030713 (11,40e)

[Khr97] Andrei Khrennikov, *Non-Archimedean analysis: quantum paradoxes, dynamical systems and biological models*, Mathematics and its Applications, vol. 427, Kluwer Academic Publishers, Dordrecht, 1997. MR **MR1746953 (2001h:**81004)

[KN04] Andrei Yu. Khrennikov and Marcus Nilson, *p-adic deterministic and random dynamics*, Mathematics and its Applications, vol. 574, Kluwer Academic Publishers, Dordrecht, 2004. MR **MR2105195 (2005h:**37102)

[Koc01] Anatoly N. Kochubei, *Pseudo-differential equations and stochastics over non-Archimedean fields*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 244, Marcel Dekker Inc., New York, 2001. MR **MR1848777 (2003b:**35220)

[LS68a] B. F. Logan and L. A. Shepp, *Real zeros of random polynomials*, Proc. London Math. Soc. (3) **18** (1968), 29–35. MR MR0234512 (38 #2829)

[LS68b] ———, *Real zeros of random polynomials. II*, Proc. London Math. Soc. (3) **18** (1968), 308–314. MR MR0234513 (38 #2830)

[Odo92] R. W. K. Odoni, *Zeros of random polynomials over finite fields*, Math. Proc. Cambridge Philos. Soc. **111** (1992), no. 2, 193–197. MR **MR1142739 (92m:**11138)

[Pan04] Daniel Panario, *What do random polynomials over finite fields look like?*, Finite fields and applications, Lecture Notes in Comput. Sci., vol. 2948, Springer, Berlin, 2004, pp. 89–108. MR **MR2092625 (2005f:**11279)

[Sch84] W. H. Schikhof, *Ultrametric calculus*, Cambridge Studies in Advanced Mathematics, vol. 4, Cambridge University Press, Cambridge, 1984, An introduction to p-adic analysis. MR **MR791759 (86j:**11104)

[SV95] Larry A. Shepp and Robert J. Vanderbei, *The complex zeros of random polynomials*, Trans. Amer. Math. Soc. **347** (1995), no. 11, 4365–4384. MR **MR1308023 (96a:**30006)

[SZ03a] Bernard Shiffman and Steve Zelditch, *Equilibrium distribution of zeros of random polynomials*, Int. Math. Res. Not. (2003), no. 1, 25–49. MR **MR1935565 (2003h:**60075)

[SZ03b] ______, *Random polynomials of high degree and Levy concentration of measure*, Asian J. Math. **7** (2003), no. 4, 627–646. MR **MR2074895 (2005e:**32037)

[SZ04] ______, *Random polynomials with prescribed Newton polytope*, J. Amer. Math. Soc. **17** (2004), no. 1, 49–108 (electronic). MR **MR2015330 (2005e:**60032)

[Wsc05] Mario Wschebor, *On the Kostlan-Shub-Smale model for random polynomial systems. Variance of the number of roots*, J. Complexity **21** (2005), no. 6, 773–789. MR MR2182444

Steven N. Evans, Department of Statistics #3860, University of California at Berkeley, 367 Evans Hall, Berkeley, CA 94720-3860, U.S.A.

E-mail address: `evans@stat.Berkeley.EDU`

URL: `http://www.stat.berkeley.edu/users/evans/`