
Counting Zeros of Random Functions

Liviu I. Nicolaescu

Abstract. What is the expected number of roots of a polynomial whose coefficients are random? More generally, what is the expected number of zeros of a random one-variable function? The Kac-Rice formula is meant to answer such questions. This paper is an introduction to this less familiar formula and some of its one-dimensional applications.

1. INTRODUCTION. It is well known that a degree n polynomial

$$P = A_n x^n + \cdots + A_1 x + A_0, \quad (1)$$

has at most n complex roots. Assuming that its coefficients A_k are random real numbers the following vaguely formulated question seems natural.

How many *real* roots should we *expect* (1) to have?

Throughout this paper we will adhere to the probabilists' convention to capitalize the names of random quantities.

To simplify the presentation we assume that the coefficients A_0, \dots, A_n are independent *continuous* random variables. Let $p_k(a)da$ denote the probability distribution of A_k and denote by $Z = Z(A_0, \dots, A_n)$ the number of zeros of the polynomial (1). The number Z is a random variable and the answer to the above question is precisely the expectation of Z , denoted by $E(Z)$. Then

$$E(Z) = \sum_{k=0}^n k \mathbb{P}(Z = k),$$

where $\mathbb{P}(E)$ denotes the probability of an event E .

To proceed further, let us denote by \mathcal{R}_k the region in the space \mathbb{R}^{1+n} consisting of the points (a_0, a_1, \dots, a_n) such that $Z(a_0, \dots, a_n) = k$. Then

$$E(Z) = \sum_{k=0}^n k \int_{\mathcal{R}_k} p_0(a_0) \cdots p_n(a_n) da_0 \cdots da_n.$$

Let us illustrate these ideas on the first nontrivial case, that of random quadratic polynomials. We assume that the coefficients are independent and uniformly distributed in $[-N, N]$, where $N \rightarrow \infty$. In this case the random variables A_0, A_1, A_2 have the same distribution $p(a)da$, where

$$p(a) = \frac{1}{2N} \begin{cases} 1, & |a| \leq N, \\ 0, & |a| > N. \end{cases}$$

Note that $\mathbb{P}(A_2 = 0) = 0$ since A_2 is a continuous random variable, so the polynomial P has almost surely degree 2. Moreover,

$$\mathcal{R}_0 = \{ (a_0, a_1, a_2) \in \mathbb{R}^3; a_1^2 < 4a_0a_2 \},$$

so that

$$\begin{aligned}
\mathbb{P}(Z = 0) &= \mathbb{P}(A_1^2 \leq 4A_0A_2) \\
&= \frac{1}{8N^3} \int_{\substack{0 \leq a_0 a_2 \leq N^2/4 \\ |a_0|, |a_2| \leq N}} \left(\int_{-2\sqrt{a_0 a_2}}^{2\sqrt{a_0 a_2}} da_1 \right) da_0 da_2 + \frac{1}{8N^3} \int_{\substack{a_0 a_2 \geq N^2/4 \\ |a_0|, |a_2| \leq N}} \left(\int_{-N}^N da_1 \right) da_0 da_2 \\
&= \frac{1}{2N^3} \int_{\substack{0 \leq a_0 a_2 \leq N^2/4 \\ |a_0|, |a_2| \leq N}} \sqrt{a_0 a_2} da_0 da_2 + \frac{1}{4N^2} \int_{\substack{a_0 a_2 \geq N^2/4 \\ |a_0|, |a_2| \leq N}} da_0 da_2 \\
(a_0 = Nx_0, a_2 = Nx_2) \\
&= \frac{1}{2} \int_{\substack{0 \leq x_0 x_2 \leq 1/4 \\ |x_0|, |x_2| \leq 1}} \sqrt{x_0 x_2} dx_0 dx_2 + \frac{1}{4} \int_{\substack{x_0 x_2 \geq 1/4 \\ |x_0|, |x_2| \leq 1}} dx_0 dx_2 \\
&= \int_{0 \leq x_0, x_2 \leq 1} \sqrt{x_0 x_2} dx_0 dx_2 + \frac{1}{2} \int_{\substack{x_0 x_2 \geq 1/4 \\ 0 \leq x_0, x_1 \leq 1}} (1 - 2\sqrt{x_0 x_2}) dx_0 dx_2 \\
&= \left(\int_0^1 \sqrt{x} dx \right)^2 + \frac{1}{2} \int_{1/4}^1 \left(\int_{1/(4x_0)}^1 (1 - 2\sqrt{x_0 x_2}) dx_2 \right) dx_0 \\
&= \frac{4}{9} + \frac{1}{2} \int_{1/4}^1 \left(1 - 1/(4x_0) \right) dx_0 - \int_{1/4}^1 \frac{2}{3} \sqrt{x_0} \left(1 - \frac{1}{8} x_0^{-3/2} \right) dx_0 \approx 0.3727.
\end{aligned}$$

This can be alternatively confirmed running a Monte-Carlo simulation using the following R code.

```

#N is the number of samples
N<-250000
a<-c(runif(N,-1,1))
b<-c(runif(N,-1,1))
c<-c(runif(N,-1,1))
sum(b^2-4*a*c<0)/N

```

Observe that $\mathbb{P}(Z = 1) = 0$. Indeed, the event $\{Z = 1\}$ is described by the surface $a_1^2 = 4a_0a_2$ in the Euclidean space with coordinates (a_0, a_1, a_2) and the 3-dimensional volume of this surface is zero.

We deduce that $\mathbb{P}(Z = 2) = 1 - \mathbb{P}(Z = 0) \approx 0.6272$. Thus, with the above concept of randomness, a random degree 2 polynomial, more likely than not, will have two roots. The expected number of real roots of such a polynomial is then

$$E(Z) = 2\mathbb{P}(Z = 2) \approx 1.2544.$$

Can we run the same argument with higher degree polynomials?

First, we need to understand the regions \mathcal{R}_k . The good news is that Sturm’s theorem [3, Sec. 2.2.2] provides explicit descriptions of these regions in terms of polynomial inequalities involving the coefficients a_i . The bad news is that these descriptions are too complicated to be of concrete use in computing the probabilities $\mathbb{P}(\mathcal{R}_k)$.

The Kac-Rice formula is an alternate way of computing $E(Z)$ which is successful in many other instances. In this paper, to avoid delicate probabilistic issues, we discuss only a special, yet sufficiently powerful case of this formula.

Here is briefly the organization of the paper. In Section 2 we introduce the concept of random function and state the general one-dimensional Kac-Rice formula (5). Section 3 presents a few classical examples of random functions, while in Section 4 we present a complete proof of (5) in the Gaussian case, Theorem 8. We conclude with two sections of applications. In Section 5 we discuss the zeros of several classes of random polynomials while in Section 6 we present two geometric applications.

2. RANDOM FUNCTIONS. A random function is really a probability measure on the space of functions from a set of parameters \mathbf{T} to \mathbb{R} . In this paper we will not work in such generality.

The sample space of our story will be a *finite dimensional* vector space \mathcal{F} of smooth functions $\mathbf{T} \rightarrow \mathbb{R}$, where $\mathbf{T} \subset \mathbb{R}$ is a nontrivial interval of the real axis. The randomness is defined by a probability measure $\mathbb{P}(dF)$ on \mathcal{F} . Following the terminology of statistical physics we will refer to the pair $(\mathcal{F}, \mathbb{P})$ as an *ensemble* of functions.

Here is how such ensembles are produced. Fix a basis f_0, f_1, \dots, f_N of \mathcal{F} . Then, any function $f \in \mathcal{F}$ is a linear combination

$$f = \sum_{i=0}^N x_i f_i,$$

and we can identify f with a vector $(x_0, x_1, \dots, x_N) \in \mathbb{R}^{N+1}$. This becomes a random vector once we fix a probability distribution

$$p(x_0, \dots, x_N) dx_0 \dots dx_N \tag{2}$$

on \mathbb{R}^{N+1} . We then think of F as a random linear combination

$$F = \sum_{k=0}^N X_k f_k, \tag{3}$$

where X_0, X_1, \dots, X_n are random variables, and (2) is their joint distribution.

For every $t \in \mathbf{T}$, the *evaluation at t* defines a linear functional

$$\mathbf{ev}_t : \mathcal{F} \rightarrow \mathbb{R}, \quad \mathbf{ev}_t(F) := F(t).$$

If F is a random function as above, then its value $F(t)$ at a point $t \in \mathbf{T}$ is a random variable. This leads to the usual point of view adopted in the theory of stochastic process, namely, a random function is a family of random variables $F(t)$ parametrized by $t \in \mathbf{T}$.

We recall that the distribution of a normal (Gaussian) random variable Y with mean m and variance $v > 0$ is given by the probability density

$$\gamma_{m,v}(y) = \frac{1}{\sqrt{2\pi v}} e^{-\frac{(y-m)^2}{2v}}. \tag{4}$$

A very important case is when the random coefficients X_i are independent, mean zero, Gaussian random variables. In this case we say that F is a (centered) *Gaussian random function*. If F is a Gaussian random function, then $F(t)$, its value at t , is a mean zero Gaussian random variable.

We denote by $Z(F, \mathbf{T})$ the number of zeros of F in the interval \mathbf{T} . This is a non-negative random variable¹ and we denote by $\widehat{Z}(F, \mathbf{T})$ its expectation. More generally, for any continuous bounded function $w : \mathbf{T} \rightarrow \mathbb{R}$ we set

$$Z_w(F) := \sum_{F(t)=0} w(t).$$

This is a weighted count of zeros of F with the function w as weight. Again, $Z_w(F)$ is a random variable and we denote by $\widehat{Z}_w(F)$ its expectation, provided it exists.

The Kac-Rice formula gives a description of $\widehat{Z}_w(F)$ in terms of statistical invariants of the random function F . Some conditions need to be imposed. We mention two of them that are needed to state the formula.

- For any $t \in \mathbf{T}$ the random variable $F(t)$ has a distribution,

$$p_{F(t)}(x)dx,$$

where the density $p_{F(t)}$ is continuous at 0.

- For any $t \in \mathbf{T}$, the random variable $F'(t)$ conditioned on $F(t) = 0$ is a continuous random variable with distribution $q_t(y)dy$. Intuitively, if $p_t(x, y)dx dy$ is the joint distribution of the the random vector $(F(t), F'(t))$, then

$$p_{F(t)}(x) = \int_{\mathbb{R}} p_t(x, y) dy, \quad q_t(y) = \frac{p_t(0, y)}{p_{F(t)}(0)}.$$

We define $C : \mathbf{T} \rightarrow \mathbb{R}$

$$C(t) := \mathbf{E}(|F'(t)| | F(t) = 0) p_{F(t)}(0) = \left(\int_{\mathbb{R}} |y| q_t(y) dy \right) p_{F(t)}(0).$$

Then, the Kac-Rice formula states that

$$\widehat{Z}_w(F) = \int_{\mathbf{T}} w(t) C(t) dt. \tag{5}$$

In particular,

$$\widehat{Z}(F, \mathbf{T}) = \int_{\mathbf{T}} C(t) dt. \tag{6}$$

The applicability of the Kac-Rice formula is limited by our ability of computing the conditional expectation $\mathbf{E}(|F'(t)| | F(t) = 0)$.

When F is a Gaussian random function, this computation simplifies considerably and $C(t)$ can be expressed in terms of the *covariance kernel* of the random function (2). This is the function $K : \mathbf{T} \times \mathbf{T} \rightarrow \mathbb{R}$ defined by

$$K(s, t) := \mathbf{E}(F(s) \cdot F(t)) = \sum_{j,k=0}^N f_j(s) f_k(t) \mathbf{E}(X_j X_k).$$

¹We tacitly assumed that $Z(F, \mathbf{T})$ is measurable. This can be verified directly in each concrete case.

Thus, $K(s, t)$ encodes the correlations between the values of the random function F at the points $s, t \in \mathbf{T}$. Since $\mathbf{E}(X_k^2) = v_k$ and the variables X_k are independent, we have

$$\mathbf{E}(X_j X_k) = \mathbf{E}(X_j)\mathbf{E}(X_k) = 0, \quad \forall j \neq k.$$

We deduce

$$K(s, t) = \sum_{k=0}^N v_k f_k(s) f_k(t). \tag{7}$$

Theorem 8 describes $C(t)$ explicitly in terms of $K(s, t)$.

The Kac-Rice formula was first proved by M. Kac [10] in 1943 in the special case of polynomials with random Gaussian coefficients. In a 1945 report, S.O. Rice, an engineer by profession, considered the case of Gaussian random linear combinations of trigonometric functions of the form $\sin(\lambda t)$ $\cos(\lambda t)$ and gave a “physicist proof” for the expected number of zeros of such functions; see [19, Sec. 3.3]. The first rigorous proofs of the one-dimensional the Gaussian case appeared in 1960s. Proofs of the general case (general random functions in several variables) appeared only in the 1980s; see [1, 2].

In Section 4 we offer a plausibility argument for (5) in general, and a complete proof of a special case that includes both situations considered by M. Kac and S.O. Rice.

3. SOME EXAMPLES OF GAUSSIAN RANDOM FUNCTIONS.

Example 1 (Gaussian random polynomials). Fix $N + 1$ independent normal random variables X_0, \dots, X_N , with mean 0 and variances $\mathbf{var}(X_k) = v_k$, $k = 0, \dots, N$. Then

$$F(t) = X_0 + X_1 t^k + \dots + X_N t^N$$

is a polynomial of degree $\leq N$ whose coefficients are independent random normal variables. Its covariance kernel is

$$K(s, t) = \sum_{k=0}^N v_k (st)^k.$$

Observe that

$$F(-t) = \sum_{k=0}^N (-1)^k X_k t^k.$$

The random variables $(-1)^k X_k$ are also independent normal variables with mean 0 and variances v_k . Thus, the random polynomials $F(t)$ and $F^-(t) = F(-t)$ have the same statistics and we deduce

$$\widehat{Z}(F, [0, \infty)) = \widehat{Z}(F, (-\infty, 0]).$$

Suppose additionally that the variances v_k satisfy the symmetry conditions

$$v_k = v_{N-k}, \quad \forall k = 0, 1, \dots, N. \tag{8}$$

In this case the random polynomials $F(t)$ and

$$F^*(t) = t^N F(t^{-1}) = \sum_{k=0}^n X_{N-k} t^k$$

have the same statistics and we deduce that

$$\widehat{Z}(F, (0, 1)) = \widehat{Z}(F^*, (0, 1)) = \widehat{Z}(F, (1, \infty)).$$

We deduce that if F satisfies the symmetry conditions (8), then

$$\widehat{Z}(F, \mathbb{R}) = 4\widehat{Z}(F, (0, 1)) = 4\widehat{Z}(F, (1, \infty)). \tag{9}$$

□

Example 2 (The Kac ensemble). In this case the random variables have the same variances $v_j = 1, \forall j = 0, \dots, N$. We deduce that the covariance kernel is

$$K(s, t) = \sum_{k=0}^N (st)^k = \frac{1 - (st)^{N+1}}{1 - st}. \tag{10}$$

This ensemble satisfies (8).

□

Example 3 (The Kostlan ensemble). In this case the variances are

$$v_k = \binom{N}{k}, \quad 0 \leq k \leq N,$$

and the covariance kernel is

$$K(s, t) = \sum_{k=0}^N \binom{N}{k} (st)^k = (1 + st)^N. \tag{11}$$

For an explanation of the strange choice of variances in the Kostlan ensemble we refer to [14]. This ensemble also satisfies (8)

□

Example 4 (The Legendre ensemble). Recall that the Legendre polynomials are obtained from the sequence of monomials $(t^k)_{k \geq 0}$ by applying the Gram-Schmidt procedure with respect to the inner product in $L^2([-1, 1], dt)$.

Concretely, the degree n Legendre polynomial is

$$p_n(t) := \sqrt{\frac{2n+1}{2}} \ell_n(t), \quad \ell_n(t) := \frac{1}{2^n n!} \frac{d^n}{dt^n} (t^2 - 1)^n. \tag{12}$$

We can construct a random polynomial

$$F_N(t) = \sum_{k=0}^N X_k p_k(t),$$

where X_k are independent standard normal random variables, $\forall k$. Using the Christoffel-Darboux theorem [20] we deduce that its covariance kernel is given by

$$K_N(s, t) = \sum_{k=0}^N p_k(s)p_k(t) = \frac{N + 1}{2} \cdot \frac{\ell_{N+1}(t)\ell_N(s) - \ell_{N+1}(s)\ell_N(t)}{t - s}. \quad \square$$

Example 5 (Random trigonometric polynomials). We assume $\mathbf{T} = [0, 2\pi]$, N is even, $N = 2m$ and

$$f_0 = 1, \quad f_{2k-1}(t) = \sin(kt), \quad f_{2k}(t) = \cos(kt).$$

Assume that $v_{2k-1} = v_{2k} = 2r_k > 0$. For uniformity we set $r_0 := v_0$. In this case we have

$$\begin{aligned} K(s, t) &= r_0 + \sum_{k=1}^m 2r_0(\cos(ks)\cos(kt) + \sin(ks)\sin(kt)) \\ &= r_0 + 2 \sum_{k=1}^m r_k \cos k(t - s) = r_0 + \sum_{k=1}^m r_k (e^{ik(s-t)} + e^{-ik(t-s)}). \end{aligned} \quad (13)$$

In the special case when $r_0 = r_1 = \dots = r_m = 1$ we deduce

$$K(s, t) = 1 + 2 \sum_{k=1}^m \cos k(t - s) = \frac{\sin \frac{(2m+1)(t-s)}{2}}{\sin \frac{t-s}{2}}. \quad (14)$$

□

4. THE ONE-DIMENSIONAL KAC-RICE FORMULA. We want to present a proof of (5) when F is a Gaussian random function satisfying certain additional conditions. The key to the proof is *Kac's counting formula*, [10]. For any $\varepsilon > 0$ define (see Figure 1 where $\varepsilon = \frac{1}{4}$)

$$\eta_\varepsilon : \mathbb{R} \rightarrow \mathbb{R}, \quad \eta_\varepsilon(y) = \begin{cases} \frac{1}{2\varepsilon}, & |y| < \varepsilon, \\ 0, & |y| \geq \varepsilon. \end{cases}$$

Let us point out that the family η_ε converges as $\varepsilon \rightarrow 0$ to Dirac's δ -function, i.e., for any continuous function $f : \mathbb{R} \rightarrow \mathbb{R}$ we have

$$\lim_{\varepsilon \searrow 0} \int_{\mathbb{R}} \eta_\varepsilon(t)f(t)dt = f(0).$$

For every C^1 -function $F : \mathbf{T} \rightarrow \mathbb{R}$ we set

$$Z_\varepsilon(F, \mathbf{T}) := \int_{\mathbf{T}} \eta_\varepsilon(F(t))|F'(t)|dt.$$

More generally, if $w : \mathbf{T} \rightarrow \mathbb{R}$ is a bounded continuous function, we set

$$Z_\varepsilon(F, w) := \int_{\mathbf{T}} w(t)\eta_\varepsilon(F(t))|F'(t)|dt.$$

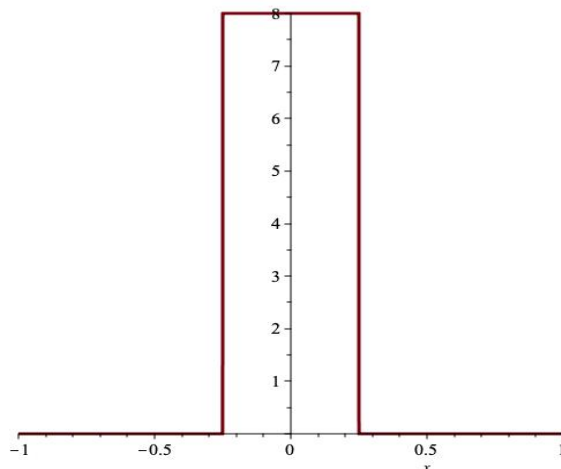


Figure 1. Approximating the Dirac function.

Definition 6. (a) Fix a compact interval $[a, b]$. A C^1 -function $f : [a, b] \rightarrow \mathbb{R}$ is called *convenient* if the following hold.

- $f(a) \cdot f(b) \neq 0$.
- All the zeros of f are *nondegenerate*, i.e., if $f(t) = 0$, then $f'(t) \neq 0$.

(b) We say that a C^1 -function $F : \mathbb{R} \rightarrow \mathbb{R}$ is *convenient* if it is proper and all its zeros are nondegenerate. \square

Lemma 7 (Kac's counting formula). (a) Suppose that the C^1 -function $F : [a, b] \rightarrow \mathbb{R}$ is convenient and $w : [a, b] \rightarrow \mathbb{R}$ is continuous. Then

$$Z_w(F) = \lim_{\varepsilon \searrow 0} Z_\varepsilon(F, w). \quad (15)$$

(b) Suppose that the C^1 -function $F : \mathbb{R} \rightarrow \mathbb{R}$ is convenient and $w : \mathbb{R} \rightarrow \mathbb{R}$ is continuous and bounded. Then

$$Z_w(F) = \lim_{\varepsilon \searrow 0} Z_\varepsilon(F, w). \quad (16)$$

(c) Let $\mathbf{T} = [a, b]$ or $\mathbf{T} = \mathbb{R}$ and suppose that $F : \mathbf{T} \rightarrow \mathbb{R}$ is a C^1 -convenient function with ν zeros and $\kappa < \infty$ critical points. Then, for any $\varepsilon > 0$, we have

$$|Z_\varepsilon(F, w)| \leq \|w\| Z_\varepsilon(F), \quad Z_\varepsilon(F) \leq \nu + 2\kappa, \quad (17)$$

where $\|w\| := \sup_{t \in \mathbf{T}} |w(t)|$.

Proof. (a) Since F is convenient, it has finitely many zeros $\tau_1 < \cdots < \tau_\nu$. The set C of critical points of F is compact and disjoint from the zero set of F because F is convenient. Thus

$$\varepsilon_0 := \min_{x \in C} |F(x)| > 0.$$

Fix $\varepsilon \in (0, \varepsilon_0)$. Then

$$\int_a^b w(t)\eta_\varepsilon(F(t))|F'(t)|dt = \frac{1}{2\varepsilon} \int_{\{|F|<\varepsilon\}} w(t)|F'(t)|dt.$$

The connected components of the open set $\{|F| < \varepsilon\}$ are open intervals $(c, d) \subset [a, b]$ with the following properties:

- i. They are disjoint from the critical set.
- ii. $|F(c)| = |F(d)| = \varepsilon$ and $F(c)F(d) < 0$.

Indeed, if $F(c)F(d) > 0$, then $F(c) = F(d) = \pm\varepsilon$, and Rolle's theorem would imply that the interval (c, d) contains a critical point of f .

Since $\varepsilon < \varepsilon_0$, the derivative $F'(t)$ has constant sign on a connected component of $\{|F| < \varepsilon\}$ and thus F has a unique zero in each such component.

We deduce that the set $\{|F| < \varepsilon\}$ is a disjoint union of open intervals $(c_i(\varepsilon), d_i(\varepsilon))$, $i = 1, \dots, \nu$ such that

$$\tau_i \in (c_i(\varepsilon), d_i(\varepsilon)), \quad \forall i.$$

Moreover, for any connected component (c, d) of $\{|F| < \varepsilon\}$, we have

$$\int_c^d |F'(t)|dt = \left| \int_c^d F'(t)dt \right| = |F(d) - F(c)| = 2\varepsilon.$$

Thus, $\forall \varepsilon \in (0, \varepsilon_0)$, we have

$$\begin{aligned} \int_a^b w(t)\eta_\varepsilon(F(t))|F'(t)|dt &= \frac{1}{2\varepsilon} \sum_{i=1}^{\nu} \int_{c_i(\varepsilon)}^{d_i(\varepsilon)} w(t)|F'(t)|dt \\ &= \sum_{i=1}^{\nu} \frac{\int_{c_i(\varepsilon)}^{d_i(\varepsilon)} w(t)|F'(t)|dt}{\int_{c_i(\varepsilon)}^{d_i(\varepsilon)} |F'(t)|dt}. \end{aligned}$$

Since $c_i(\varepsilon) \nearrow \tau_i$ and $d_i(\varepsilon) \searrow \tau_i$ as $\varepsilon \searrow 0$ we deduce

$$\lim_{\varepsilon \searrow 0} \frac{\int_{c_i(\varepsilon)}^{d_i(\varepsilon)} w(t)|F'(t)|dt}{\int_{c_i(\varepsilon)}^{d_i(\varepsilon)} |F'(t)|dt} = w(\tau_i).$$

(b) The function F is proper so there exists a compact interval $[-a, a]$ such that $|F(t)| > 1$ for $|t| > a$. The restriction of F to $[-a, a]$ is convenient and we have

$$Z(F|_{[-a, a]}, w) = Z(F, w).$$

Next observe that for $\varepsilon \in (0, 1)$ we have $\eta_\varepsilon(F(t)) = 0, \forall |t| > a$ so

$$\int_{\mathbb{R}} w(t)\eta_\varepsilon(F(t))|F'(t)|dt = \int_{-a}^a w(t)\eta_\varepsilon(F(t))|F'(t)|dt.$$

Hence

$$\lim_{\varepsilon \searrow 0} \int_{\mathbb{R}} w(t) \eta_{\varepsilon}(F(t)) |F'(t)| dt = \lim_{\varepsilon \searrow 0} \int_{-a}^a w(t) \eta_{\varepsilon}(F(t)) |F'(t)| dt = Z(F, w).$$

(c) Since F has only finitely many critical points we deduce from Rolle's theorem that for any $c \in \mathbb{R}$ the equation $F(t) = c$ has only finitely many solutions.

Fix an arbitrary $\varepsilon > 0$. The connected components of the set $\{|F| < \varepsilon\}$ are bounded intervals (a, b) such that $|F(a)| = |F(b)| = \varepsilon$. Rolle's theorem shows that the equation $|F(t)| = \varepsilon$ has only finitely many solutions. We deduce that $\{|F| < \varepsilon\}$ has only finitely many components

$$J_{\ell} = (a_{\ell}, b_{\ell}), \quad \ell = 1, \dots, L.$$

We have

$$Z_{\varepsilon}(F, w) = \int_{\mathcal{T}} w(t) \eta_{\varepsilon}(F(t)) |F'(t)| dt = \frac{1}{2\varepsilon} \sum_{\ell=1}^L \int_{J_{\ell}} w(t) |F'(t)| dt.$$

Denote by k_{ℓ} the number of turning points of $F(t)$ in J_{ℓ} , i.e., the number of points where $F'(t)$ changes sign. Let us observe that if J_{ℓ} contains no turning points, then F is either increasing or decreasing on this interval so $F(a_{\ell})F(b_{\ell}) < 0$ and thus J_{ℓ} contains a unique zero of F . In particular, if J_{ℓ} contains no turning point, then

$$\int_{J_{\ell}} |F'(t)| dt = \left| \int_{J_{\ell}} F'(t) dt \right| = 2\varepsilon.$$

We set

$$\mathcal{L}_0 := \{\ell; J_{\ell} \text{ contains no turning point}\}, \quad \mathcal{L}_1 := \{\ell; J_{\ell} \text{ contains turning points}\}.$$

The above discussion shows that $\#\mathcal{L}_0 \leq \nu$, $\#\mathcal{L}_1 \leq \kappa$, and thus

$$\begin{aligned} \frac{1}{2\varepsilon} \sum_{\ell=1}^L \int_{J_{\ell}} |F'(t)| dt &= \frac{1}{2\varepsilon} \sum_{\ell \in \mathcal{L}_0} \int_{J_{\ell}} |F'(t)| dt + \frac{1}{2\varepsilon} \sum_{\ell \in \mathcal{L}_1} \int_{J_{\ell}} |F'(t)| dt \\ &\leq \nu + \frac{1}{2\varepsilon} \sum_{\ell \in \mathcal{L}_1} \int_{J_{\ell}} |F'(t)| dt. \end{aligned}$$

Let $\ell \in \mathcal{L}_1$ and suppose that the turning points of F in J_{ℓ} are $t_1 < \dots < t_{k_{\ell}}$. We set $t_0 := a_{\ell}$ and $t_{k_{\ell}+1} := b_{\ell}$. Then

$$\int_{J_{\ell}} |F'(t)| dt = \sum_{j=1}^{k_{\ell}+1} |F(t_j) - F(t_{j-1})| \leq 2\varepsilon(k_{\ell} + 1).$$

Hence

$$\frac{1}{2\varepsilon} \sum_{\ell \in \mathcal{L}_1} \int_{J_{\ell}} |F'(t)| dt \leq \sum_{\ell \in \mathcal{L}_1} (2k_{\ell} + 1) \leq \kappa + \#\mathcal{L}_1 \leq 2\kappa.$$

□

Let us outline the strategy for proving (5). We want to apply Kac's counting formula to the random function in (3)

$$F : \mathbf{T} \rightarrow \mathbb{R}, \quad F = \sum_{k=0}^N X_k f_k.$$

Here we assume that \mathbf{T} is either a compact interval, or $\mathbf{T} = \mathbb{R}$. We make a first assumption about the random function.

The random function F is almost surely convenient. (18)

Let $w : \mathbf{T} \rightarrow \mathbb{R}$ be continuous and bounded. The Kac's counting formula implies that

$$Z_w(F) = \lim_{\varepsilon \searrow 0} Z_\varepsilon(F, w).$$

Suppose that we can prove that

$$\mathbf{E}\left(\lim_{\varepsilon \searrow 0} Z_\varepsilon(F, w)\right) = \lim_{\varepsilon \searrow 0} \mathbf{E}\left(Z_\varepsilon(F, w)\right). \quad (19)$$

We deduce

$$\begin{aligned} \widehat{Z}_w(F) &= \lim_{\varepsilon \searrow 0} \mathbf{E}\left(\int_{\mathbf{T}} w(t) \eta_\varepsilon(F(t)) |F'(t)| dt\right) dt \\ &= \lim_{\varepsilon \searrow 0} \int_{\mathbf{T}} w(t) \mathbf{E}\left(\eta_\varepsilon(F(t)) |F'(t)|\right) dt. \end{aligned} \quad (20)$$

If $p_t(x, y) dx dy$ is the joint distribution of the random vector $(F(t), F'(t))$, then

$$\mathbf{E}\left(\eta_\varepsilon(F(t)) |F'(t)|\right) = \frac{1}{2\varepsilon} \int_{-\varepsilon}^{\varepsilon} \left(\int_{\mathbb{R}} |y| p_t(x, y) dy\right) dx.$$

Under mild constraints on p_t one can show that, as $\varepsilon \searrow 0$, the last integral converges to

$$\begin{aligned} \int_{\mathbb{R}} |y| p_t(0, y) dy &= \left(\int_{\mathbb{R}} |y| \frac{p_t(0, y)}{p_{F(t)}(0)} dy\right) p_{F(t)}(0) \\ &= \mathbf{E}\left(|F'(t)| \mid F(t) = 0\right) p_{F(t)}(0), \quad p_{F(t)}(0) = \int_{\mathbb{R}} p_t(0, y) dy. \end{aligned}$$

We get (5) by passing to the limit under the integral (19), if this were possible.

The assumption (19) is the tricky part. It happens if we make the additional assumption

$$\exists C > 0 \text{ such that, almost surely, } Z(F, \mathbf{T}) + Z(F', \mathbf{T}) < C. \quad (21)$$

Indeed, with this assumption we can use Lemma 7(c) and Dominated Convergence Theorem to prove (19).

We also need to justify the passage to limit in the second integral of (20). There are other practical issues. For example, determining the joint density $p_t(x, y)$, or the conditional expectation $\mathbf{E}(|F'(t)| | F(t) = 0)$, could be quite difficult if not impossible to compute, thus limiting the usefulness of (5).

Things simplify considerably if we assume that F is a *Gaussian* random function. This is what we assume in the sequel. We also assume that (19) holds for one reason or another, e.g., because (21) holds.

In this case, for each $t \in \mathbf{T}$, the random vector

$$\mathcal{F} \ni F \mapsto (F(t), F'(t)) \in \mathbb{R}^2$$

is Gaussian since it is the limit as $h \rightarrow 0$ of the Gaussian vectors.

$$V_{t,h} = \left(F(t), \frac{F(t+h) - F(t)}{h} \right).$$

Indeed

$$\frac{F(t+h) - F(t)}{h} = \sum_{j=0}^N X_j \frac{f_j(t+h) - f_j(t)}{h} \xrightarrow{L^1} \sum_{j=0}^N X_j f'_j(t) = F'(t).$$

By construction, $\mathbf{E}(F(t)) = 0$. Moreover, $\mathbf{E}(F'(t)) = 0$ since $F'(t)$ is a L^1 -limit of mean zero random variables. Hence, the distribution of the random vector $(F(t), F'(t))$ is determined by its covariance matrix

$$C_t = \begin{bmatrix} a_t & b_t \\ b_t & c_t \end{bmatrix},$$

where

$$a_t = \mathbf{E}(F(t)^2), \quad b_t = \mathbf{E}(F(t)F'(t)), \quad c_t = \mathbf{E}(F'(t)^2).$$

This is a symmetric positive *semidefinite* matrix.

We can describe the entries of C_t in terms of the covariance kernel $K(s, t) = \mathbf{E}(F(s)F(t))$. More precisely, we have

$$a_t = K(t, t), \quad b_t = K'_t(s, t)|_{s=t}, \quad c_t = K''_{st}(s, t)|_{s=t}. \tag{22}$$

We set $\Delta_t := \det C_t = a_t c_t - b_t^2$, and we make another assumption on $F(t)$, namely that C_t is positive *definite*, i.e.,

$$a_t > 0, \quad \Delta_t > 0, \quad \forall t \in \mathbf{T}. \tag{23}$$

The joint distribution of the random vector $(F(t), F'(t))$ is the Gaussian measure $\mathbf{\Gamma}_{C_t}$

$$\mathbf{\Gamma}_{C_t}(dxdy) = \frac{1}{2\pi\sqrt{\Delta_t}} e^{-\frac{1}{2\Delta_t}(c_t x^2 - 2b_t xy + a_t y^2)} dxdy. \tag{24}$$

We then have

$$\mathbf{E}\left(\eta_\varepsilon(F(t)) | F'(t) \right) = \frac{1}{2\varepsilon} \int_{|x| < \varepsilon} |y| \mathbf{\Gamma}_{C_t}(dxdy)$$

$$= \frac{1}{2\varepsilon} \int_{-\varepsilon}^{\varepsilon} \frac{1}{2\pi\sqrt{\Delta_t}} \left(\int_{\mathbb{R}} |y| e^{-\frac{1}{2\Delta_t}(c_t x^2 - 2b_t xy + a_t y^2)} dy \right) dx.$$

A direct elementary computation shows that

$$(c_t x^2 - 2b_t xy + a_t y^2) = a_t \left(y - \frac{b_t x}{a_t} \right)^2 + \frac{\Delta_t}{a_t} x^2.$$

We deduce that

$$\begin{aligned} & \frac{1}{2\pi\sqrt{\Delta_t}} \int_{\mathbb{R}} |y| e^{-\frac{1}{2\Delta_t}(c_t x^2 - 2b_t xy + a_t y^2)} dy \\ &= \frac{1}{\sqrt{2\pi a_t}} e^{-\frac{x^2}{2a_t}} \times \frac{1}{\sqrt{2\pi \frac{\Delta_t}{a_t}}} \int_{\mathbb{R}} |y| e^{-\frac{a_t}{2\Delta_t} \left(y - \frac{b_t x}{a_t} \right)^2} dy \end{aligned}$$

($v_t := \Delta_t/a_t$)

$$\stackrel{(4)}{=} \frac{1}{\sqrt{2\pi a_t}} e^{-\frac{x^2}{2a_t}} \int_{\mathbb{R}} |y| \gamma_{b_t x/a_t, v_t}(dy) =: \Phi_t(x).$$

Thus

$$\mathbf{E} \left(\eta_\varepsilon(F(t)) |F'(t)| \right) = \frac{1}{2\varepsilon} \int_{-\varepsilon}^{\varepsilon} \Phi_t(x) dx.$$

We have

$$\lim_{\varepsilon \searrow 0} \mathbf{E} \left(\eta_\varepsilon(F(t)) |F'(t)| \right) = \Phi_t(0) = \frac{1}{\sqrt{2\pi a_t}} \int_{\mathbb{R}} |y| \gamma_{v_t}(dy). \quad (25)$$

We would like to conclude that

$$\begin{aligned} \widehat{Z}_w(F) &= \lim_{\varepsilon \searrow 0} \int_{\mathcal{T}} w(t) \mathbf{E} \left(\eta_\varepsilon(F(t)) |F'(t)| \right) dt \\ &= \int_{\mathcal{T}} w(t) \lim_{\varepsilon \searrow 0} \mathbf{E} \left(\eta_\varepsilon(F(t)) |F'(t)| \right) dt = \int_{\mathcal{T}} w(t) \Phi_t(0) dt. \end{aligned}$$

To do this we will invoke the Dominated Convergence Theorem.

Any random variable Y with finite mean $\mathbf{E}(Y)$ and finite variance $\mathbf{var}(Y)$ satisfies the inequality

$$\mathbf{E}(|Y|) \leq \sqrt{\mathbf{E}(Y^2)} = \sqrt{\mathbf{var}(Y) + \mathbf{E}(Y)^2}.$$

Applying this inequality in the special case when Y is Gaussian with mean $\frac{b_t x}{a_t}$ and variance v_t we deduce

$$\int_{\mathbb{R}} |y| \gamma_{b_t x/a_t, v_t}(dy) \leq \sqrt{v_t + b_t^2 x^2/a_t^2} \leq \sqrt{v_t} + \frac{|b_t x|}{a_t}.$$

Now observe that $\Phi_t(x)$ is positive and, for any $|x| \leq 1$, we have

$$\Phi_t(x) \leq \frac{1}{\sqrt{2\pi a_t}} \left(\sqrt{v_t} + \frac{|b_t|}{a_t} \right) = \frac{1}{\sqrt{2\pi}} \left(\frac{\sqrt{\Delta_t}}{a_t} + \frac{|b_t|}{a_t^{3/2}} \right) =: \mu(t).$$

We now add another requirement to our random function $F(t)$, namely,

$$\int_{\mathbf{T}} \mu(t) dt < \infty. \tag{26}$$

We deduce

$$\mathbf{E} \left(\eta_\varepsilon(F(t)) |F'(t)| \right) = \frac{1}{2\varepsilon} \int_{-\varepsilon}^\varepsilon \Phi_t(x) dx \leq \mu(t).$$

Invoking (19), (25), (26), and the Dominated Convergence Theorem, we conclude that

$$\begin{aligned} \widehat{Z}_w(F) &= \lim_{\varepsilon \searrow 0} \int_{\mathbf{T}} w(t) \mathbf{E} \left(\eta_\varepsilon(F(t)) |F'(t)| \right) dt \\ &= \int_{\mathbf{T}} w(t) \lim_{\varepsilon \searrow 0} \mathbf{E} \left(\eta_\varepsilon(F(t)) |F'(t)| \right) dt = \int_{\mathbf{T}} w(t) \Phi_t(0) dt. \end{aligned}$$

Observe that

$$\begin{aligned} \Phi_t(0) &= \frac{2}{\sqrt{2\pi a_t}} \int_0^\infty y \gamma_{v_t}(y) dy = \frac{1}{\pi \sqrt{a_t v_t}} \int_0^\infty y e^{-\frac{y^2}{2v_t}} dy = \frac{1}{\pi} \rho_t, \\ \rho_t &:= \frac{\sqrt{\Delta_t}}{a_t}. \end{aligned}$$

Note that we can describe ρ_t in a more compact form,

$$\rho_t^2 = \frac{a_t c_t - b_t^2}{a_t^2} = \frac{K(s, t)_{s=t} K''_{st}(s, t)_{s=t} - K'_t(s, t)_{s=t}^2}{K(s, t)_{s=t}^2} = \partial_{st}^2 \log K(s, t)_{s=t}.$$

We have thus proved the Gaussian Kac-Rice formula.

Theorem 8. *Let $\mathbf{T} = [a, b]$ or $\mathbf{T} = \mathbb{R}$. Suppose that $f_0, f_1, \dots, f_N : \mathbf{T} \rightarrow \mathbb{R}$ are smooth functions and $X_k, k = 0, \dots, N$ are independent normal random variables with mean zero and variance v_k . Consider the random function*

$$F : \mathbf{T} \rightarrow \mathbb{R}, \quad F(t) = \sum_{k=0}^N X_k f_k(t)$$

with covariance kernel $K(s, t) = \mathbf{E}(F(s)F(t))$.

If the random function F satisfies the assumptions (18), (21), (23), (26), then, for any bounded continuous function $w : \mathbf{T} \rightarrow \mathbb{R}$, we have

$$\widehat{Z}_w(F) = \frac{1}{\pi} \int_{\mathbf{T}} w(t) \rho_t dt, \tag{27}$$

where

$$\rho_t = \sqrt{\frac{K(s, t)K''_{st}(s, t) - K'_t(s, t)^2}{K(s, t)^2}} \Big|_{s=t} = \sqrt{\partial_{st}^2 \log K(s, t)_{s=t}}. \quad (28)$$

In particular, the expected number of zeros of F in \mathbf{T} is

$$\widehat{Z}(F, \mathbf{T}) = \frac{1}{\pi} \int_{\mathbf{T}} \rho_t dt. \quad (29)$$

Remark 9. (a) The requirement (26) is easily verifiable. It follows automatically if the interval \mathbf{T} is compact and the random function satisfies the ampleness condition

$$\boxed{a_t > 0, \quad \forall t.} \quad (30)$$

Clearly (30) follows from (23). Note that if (30) holds but (23) is violated, then $\Delta_t = 0$ for some t . For this t the Gaussian measure (24) is degenerate: it is supported on the line $y = \frac{b_t}{a_t}x$.

The requirement (26) is also satisfied for the random polynomials in Example 1 because in this case a_t is a polynomial of degree $2N$, b_t is a polynomial of degree $2N - 2$, c_t is a polynomial of degree $2N - 2$ and Δ_t is an even polynomial of degree $\leq 4N - 3$. In particular, $\deg \Delta_t \leq 4N - 4$ and we deduce

$$\frac{\sqrt{\Delta_t}}{a_t} + \frac{|b_t|}{a_t^{3/2}} = O(t^{-2}) \text{ as } |t| \rightarrow \infty.$$

(b) In the Gaussian case, the assumption (18) follows from the ampleness condition (30) if \mathbf{T} is a compact interval. This is a consequence of a probabilistic version of Sard's theorem, [17, Prop. 1.12].

(c) The assumption (21) is the most difficult to verify in concrete situations. When $\mathbf{T} = \mathbb{R}$, it holds if the functions f_0, \dots, f_N are polynomials. When the interval \mathbf{T} is compact it holds if the functions f_0, \dots, f_N are real analytic on an open interval I that contains \mathbf{T} . For example, it holds if they are trigonometric polynomials. In this case the random function is the random noise considered by S.O. Rice in [19].

(d) Theorem 8 is a very special case of the general Kac-Rice formula. In particular, the general version shows that

if \mathbf{T} is compact, then the equality (27) holds assuming only (30).

The available proofs of this fact avoid the tricky assumption (19) and they are significantly more involved. For details we refer to [1, Chap. 11] or [2, Thm.3.2]. \square

5. ZEROS OF RANDOM POLYNOMIALS. Let us apply Theorem 8 to study the number of real zeros of random polynomials. As we will soon see, the expected number of zeros is sensitive to the concept of randomness we use.

Example 10 (The Kac ensemble). Suppose that $F_N(t)$ is the degree N random Kac polynomial

$$F_N(t) = \sum_{k=0}^N X_k t^k, \tag{31}$$

where the random variables X_k are independent standard normal variables. We denote by Z_N the number of zeros of F_N . In this case the covariance kernel is

$$K_N(s, t) = \frac{1 - (st)^{N+1}}{1 - st}.$$

Then

$$\partial_{st}^2 \log K_N(s, t)_{s=t} = \frac{1}{(t^2 - 1)^2} - \frac{(N + 1)^2 t^{2N}}{(t^{2N+2} - 1)^2} =: f_N(t) dt.$$

We deduce that

$$\widehat{Z}_N := \mathbf{E}(Z_N) = 4\widehat{Z}(F_N, [1, \infty)) = \frac{4}{\pi} \int_1^\infty \sqrt{f_N(t)} dt.$$

For example,

$$\begin{aligned} f_2(t) &= \frac{1}{(t^2 - 1)^2} - \frac{9t^4}{(t^6 - 1)^2} \\ &= \frac{1}{(t^2 - 1)^2} \left(1 - \frac{9t^4}{(t^4 + t^2 + 1)^2} \right) = \frac{t^4 + t^2 + 1}{(t^4 + t^2 + 1)^2}. \end{aligned}$$

Hence

$$Z_2 = \frac{4}{\pi} \int_0^1 \frac{1}{\sqrt{t^4 + t^2 + 1}} dt \approx 0.5055.$$

In particular we deduce that

$$\mathbf{P}(Z_2 > 0) = \frac{1}{2} \mathbf{E}(Z_2) \approx 0.25.$$

Thus the quadratic Kac polynomials are more likely to have no real roots. □

Remark 11. (a) Let Z_N denote the number of zeros of a random Kac polynomial of degree N . As $N \rightarrow \infty$ we have (see [5, §2.5])

$$Z_N = \frac{2}{\pi} (\log N + C) + o(1). \tag{32}$$

Thus, we expect the Kac polynomials of large degree to have relatively few real roots. (b) The graph of

$$\rho_N(t) = \sqrt{\frac{1}{(1 - t^2)^2} - \frac{(N + 1)^2 t^{2N}}{(1 - t^{2N+2})^2}}$$

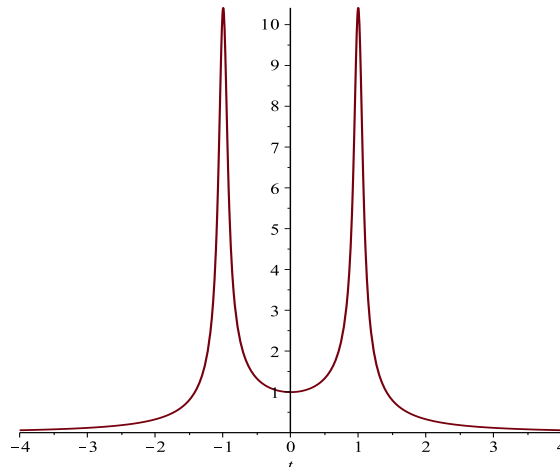


Figure 2. The density of zeros of a random Kac polynomial of degree 25.

is depicted in Figure 2.

It has two “peaks” at $t = \pm 1$ which suggests that the real roots of a Kac random polynomial tend to concentrate near $t = \pm 1$. This statement can be made much more precise.

In [9, §2, Lemma 1] it is shown that, for any $s \in (0, 1)$, the expected number of roots in the interval $(-1 + (\log N)^{-s}, 1 - (\log N)^{-s}) \subset (-1, 1)$ is $\ll \log N$ as $N \rightarrow \infty$. More precisely,

$$\widehat{Z}\left(F_{\text{Kac}}, \left(-1 + \frac{1}{(\log N)^s}, 1 - \frac{1}{(\log N)^s}\right)\right) = O((\log N)^s \log \log N).$$

(b) A weaker version of the asymptotic estimate (32) is valid for more general classes of random polynomials. More precisely, Ibragimov and Maslova have shown in [9] that if $F_n(t)$ is a random degree N polynomial of the form

$$F_N(t) = \sum_{k=0}^N X_k t^k,$$

where $(X_k)_{k \geq 0}$ are independent identically distributed L^2 -random variables and, if we denote by Z_N the number of real zeros of F_N , then

$$E(Z_N) \sim \frac{2}{\pi} \log N \text{ as } N \rightarrow \infty. \quad (33)$$

The proof in [9] is much more complicated and is based on ideas developed by Erdős-Offord [6] where they discuss the special case when X_k are Bernoulli variables taking values ± 1 with equal probability.

The asymptotic behavior of the variance V_N of Z_N was described by N.B. Maslova, [11]. More precisely, she proved that

$$V_N \sim \frac{1}{4\pi} \left(1 - \frac{2}{\pi}\right) \log N \text{ as } N \rightarrow \infty.$$

If $X_k \in L^p$ for some $p > 2$, then the random variables Z_N satisfy a central limit theorem. More precisely, Maslova showed in [12] that if $X_k \in L^p$ for some $p > 0$ then

$$\frac{1}{\sqrt{V_N}} \left(Z_n - \mathbf{E}(Z_N) \right)$$

converges in distribution to a standard normal random variable.

Recently Nguyen-Nguyen-Vu [15] proved that, under the same assumptions,

$$\mu_N := \mathbf{E}(Z_N) = \frac{2}{\pi} \log N + O(1).$$

If the random variables X_k are not identically distributed, then $\mathbf{E}(Z_N)$ can have different asymptotic behavior as the example below shows. Moreover O. Nguyen and V. Vu [16] proved that the central limit result holds (under additional assumptions), even when X_k are merely independent and not necessarily identically distributed, as in the case of Kostlan polynomials. \square

Example 12 (The Kostlan statistics). Consider the Kostlan random polynomials introduced in Example 3. In this case the covariance kernel is $K(s, t) = (1 + st)^N$ and we have

$$\log K(s, t) = N \log(1 + st), \quad \partial_t \log K(s, t) = \frac{Ns}{1 + st},$$

$$\partial_{st}^2 \log K(s, t) = \frac{N}{(1 + st)^2}, \quad \rho_t = \sqrt{\partial_{st}^2 \log K(s, t)|_{s=t}} = \frac{\sqrt{N}}{1 + t^2}.$$

The Kac-Rice formula implies that the expected number of zeros is

$$\mathbf{E}(Z_N) = \frac{2\sqrt{N}}{\pi} \int_0^\infty \frac{1}{1 + t^2} = \sqrt{N}.$$

We see that the Kostlan random polynomials have, on average, more real zeros than the Kac random polynomials. \square

Example 13 (The Legendre statistics). Let $F_n(t)$ denote the random linear combinations of Legendre polynomials described in Example 4. M. Das [4] has shown that the expected number of zeros of $F_N(t)$ in $[-1, 1]$ is asymptotic to $\frac{1}{\sqrt{3}}N$ for large N . The Legendre ensemble displays an even stronger bias towards a relatively large number of real roots. \square

6. GEOMETRIC APPLICATIONS. We want to present some immediate but striking geometric applications of the Kac-Rice formula. We will use the stronger version mentioned in Remark 9(d).

Example 14 (Fáry-Milnor). Suppose that

$$[0, L] \ni s \mapsto \mathbf{r}(s) = (x(s), y(s), z(s)) \in \mathbb{R}^3$$

is the arclength parametrization of a knot K (embedded, smooth, closed curve) in \mathbb{R}^3 .

Consider a random linear function

$$H : \mathbb{R}^3 \rightarrow \mathbb{R}, \quad H(x, y, z) = Ax + By + Cz,$$

where A, B, C are independent standard normal random variables with mean zero and variance 1. Denote by $\mu(H) = \mu(A, B, C)$ the number of critical points of the restriction of H to the knot. These are the points on the knot where the vector (A, B, C) is perpendicular to the tangent vector to the curve at that point.

The restriction of H to K is described by the Gaussian random function

$$F(s) = Ax(s) + By(s) + Cz(s).$$

Note that the critical points of $H|_K$ correspond to the zeros of the derivative.

$$F'(s) = Ax'(s) + By'(s) + Cz'(s).$$

Let (\mathbf{T}, \mathbf{N}) denote a Frenet frame along the curve, where \mathbf{T} is the unit tangent vector and \mathbf{N} a unit normal vector. The derivative $F'(s)$ is a Gaussian random function with covariance kernel

$$K(s_1, s_2) = x'(s_1)x'(s_2) + y'(s_1)y'(s_2) + z'(s_1)z'(s_2) = \mathbf{T}(s_1) \bullet \mathbf{T}(s_2),$$

where \bullet denotes the standard inner product in \mathbb{R}^3 . The Frenet formulæ [21, Sec. 1.9] imply that

$$\partial_{s_2} K(s_1, s_2) = \mathbf{T}(s_1) \bullet \mathbf{T}'(s_2) = \kappa(s_2) \mathbf{T}(s_1) \bullet \mathbf{N}(s_2),$$

where κ denotes the curvature of the curve. Similarly

$$\partial_{s_1 s_2}^2 K(s_1, s_2) = \kappa(s_1) \kappa(s_2) \mathbf{N}(s_1) \bullet \mathbf{N}(s_2).$$

We deduce

$$K(s, s) = 1, \quad \partial_{s_2} K(s, s) = 0, \quad \partial_{s_1 s_2}^2 K(s, s) = \kappa(s)^2, \quad \rho_s = |\kappa(s)|.$$

Hence assumption (30) is satisfied. Remark 9(b) implies that the critical points of $H|_K$ are almost surely nondegenerate. They come in two types: local minima and local maxima. We denote by $m_{\pm}(H)$ the number of local minima/maxima of $H|_K$. Then, almost surely, $m_-(H) = m_+(H)$ and $\mu(H) = m_-(H) + m_+(H)$. The Kac-Rice formula (29) implies that

$$\begin{aligned} \mathbf{E}(\mu(H)) &= 2\mathbf{E}(m_+(H)) = \frac{1}{\pi} \int_0^L |\kappa(s)| ds \\ &= \frac{1}{\pi} \times \text{the total curvature of the curve.} \end{aligned}$$

This result, or rather a version equivalent to it, was first proved independently by I. Fáry [7] and J. Milnor [13]. In particular, Milnor, who was a Freshman at the time, used this to prove a conjecture of K. Borsuk stating roughly that to knot a curve you need to bend it quite a bit. Fáry's proof is also probabilistic in nature, but he used a different approach. \square

Example 15. Suppose that C is a smooth closed curve on the unit n -dimensional sphere

$$S^n := \{ (x_0, x_1, \dots, x_n) \in \mathbb{R}^{n+1}; x_0^2 + x_1^2 + \dots + x_n^2 = 1 \}.$$

Denote by L the length of C . Using the Kac-Rice formula we will prove, in one stroke, two related facts.

- i. If $L < 2\pi$, then C is entirely contained in a hemisphere.
- ii. If $L > 2\pi$, then there exists an Equator of the sphere that intersects C in at least four points.

The case $n = 2$ of (i) seems to be part of the folklore of mathematics; see e.g. [21, Problem 1.10.4]. The case $n = 2$ of (ii) was proved more recently, in a 2008 MONTHLY paper, [8]. The authors refer to it as a 1969 conjecture of Hugo Steinhaus. Here is a probabilistic proof of these facts.

Parametrize C by arclength, $[0, L] \ni s \mapsto \mathbf{x}(s) := (x_0(s), \dots, x_n(s)) \in \mathbb{R}^{n+1}$. Since $C \subset S^n$ we have $|\mathbf{x}(s)| = 1, \forall s$, where $|\cdot|$ denotes the natural Euclidean norm. Moreover, since this is arclength parametrization, we have $|\mathbf{x}'(s)| = 1, \forall s$.

Any vector $\mathbf{u} \in \mathbb{R}^{n+1}$ determines a linear functional $\ell_{\mathbf{u}} : \mathbb{R}^{n+1} \rightarrow \mathbb{R}, \ell_{\mathbf{u}}(\mathbf{x}) = \langle \mathbf{u}, \mathbf{x} \rangle$, where $\langle -, - \rangle$ is the canonical inner product in \mathbb{R}^{n+1} . To prove (i), we have to show that there exists $\mathbf{u} \neq 0$ such that the restriction of $\ell_{\mathbf{u}}$ to C has no zeros. To prove (ii), we have to show that there exists $\mathbf{u} \neq 0$ such that the restriction of $\ell_{\mathbf{u}}$ to C has at least four zeros.

The restriction of $\ell_{\mathbf{u}}$ to C can be identified with the function $f_{\mathbf{u}} : [0, L] \rightarrow \mathbb{R}, f_{\mathbf{u}}(s) = \langle \mathbf{u}, \mathbf{x}(s) \rangle$. Choose independent standard random variables $(U_k)_{0 \leq k \leq n}$ and form the random Gaussian function

$$F_U : [0, L] \rightarrow \mathbb{R}, F_U(s) = \sum_{k=0}^n U_k x_k(s).$$

Its covariance kernel is $K(s, t) = \langle \mathbf{x}(s), \mathbf{x}(t) \rangle$. We deduce

$$a_t = \langle \mathbf{x}(t), \mathbf{x}(t) \rangle = |\mathbf{x}(t)|^2 = 1,$$

$$b_t = K'_t(s, t)|_{s=t} = \langle \mathbf{x}(t), \mathbf{x}'(t) \rangle = \frac{1}{2} \frac{d}{dt} |\mathbf{x}(t)|^2 = 0,$$

$$c_t = K''_{st}(s, t)|_{s=t} = |\mathbf{x}'(t)|^2 = 1.$$

Thus $\Delta_t = 1, \rho_t = 1$. Condition (30) is satisfied so we can apply (29) to deduce that the expected number of zeros of F_U is $Z_C = \frac{L}{\pi}$.

To reach the conclusions (i) and (ii) we need an additional input, topological in nature. Observe that if $f_{\mathbf{u}}$ has only nondegenerate zeros, then it has an even number of them. Indeed, a nondegenerate zero of $f_{\mathbf{u}}$ corresponds to a point where the curve C crosses the hyperplane $\{\ell_{\mathbf{u}} = 0\}$ transversally from one side to the other. Since the curve is closed, it must cross this hyperplane an even number number of times.

As explained in Remark 9(b), condition (30) implies that the zeros of F_U are almost surely nondegenerate. Thus, almost surely, the function F_U has an even number of zeros.

If $L < 2\pi$, then $Z_C < 2$, and the probability that the number of zeros of F_U is < 2 is positive. Since F_U has an even number of zeros we deduce that the probability that F_U has no zeros is positive. This proves (i).

If $L > 2\pi$, then $Z_C > 2$. Hence, the probability that F_U has more than two zeros is positive and we deduce that the probability that F_U has at least four zeros is positive. This proves (ii). \square

Remark 16. The equality $Z_C = \frac{L}{\pi}$ proved in Example 15 is a Crofton-type formula: the quantity Z_C is the average number of intersection points of the curve C with a hyperplane *through the origin*. This is no accident. In [1], the Kac-Rice formula was used to prove wide ranging generalizations of the classical Crofton formulæ, [18, Sec. 9.3].

The Kac-Rice formula, in its higher dimensional incarnations, has other geometric applications. For example, as shown in [17], the classical Gauss-Bonnet formula and all its modern generalizations are special cases of the Kac-Rice formula. \square

ACKNOWLEDGMENT. I want to thank the referees for the useful comments, suggestions and corrections.

REFERENCES

1. Adler, R. J., Jonathan E. Taylor, J. E. (2007). *Random Fields and Geometry*. Springer Monographs in Mathematics, New York, NY: Springer Verlag.
2. Azaïs, J.-M., Mario Wschebor, M. (2009). *Level Sets and Extrema of Random Processes*. Hoboken, NJ: John Wiley & Sons.
3. Basu, S., Pollack, R. P., Roy, M.-F. (2006). *Algorithms in Real Algebraic Geometry*. Berlin: Springer Verlag.
4. Das, M. (1971). Real zeros of a random sum of orthogonal polynomials. *Proc. Amer. Math. Soc.*, 27(1): 147–153.
5. Edelman, A., Kostlan, E. (1995). How many zeros of a random polynomial are real? *Bull. Amer. Math. Soc. (New Series)*, 32(1): 1–37.
6. Erdős, P., Offord, A. C. (1956). On the number of real roots of a random algebraic equation. *Proc. London Math. Soc.*, 6(3): 139–160.
7. Fáry, I. (1949). Sur la courbure totale d'une courbe gauche faisant un noeud, *Bull. Soc. Math. France*, 77: 128–138.
8. Holsztyński, W., Mycielski, J., O'Brien, G. C. , Świerczkowski, S. S. (2008). Closed curves on spheres. *Amer. Math. Monthly*, 115(2): 149–153.
9. Ibragimov, I. A., Maslova, N. B. (1971). On the average number of real zeros of random polynomials I. Coefficients with zero means. *Th. Probab. Appl.* 16(2): 228–248.
10. Kac, M.(1943). On the average number of real roots of a random algebraic equation. *Bull. Amer. Math. Soc.*, 49: 314–320.
11. Maslova, N. B. (1974). On the variance of the number of real roots of random polynomials. *Th. Probab. Appl.*, 19(1): 35–52.
12. Maslova, N. B. (1974). The distribution of the number of real roots of random polynomials. *Th. Probab. Appl.*, 19(3): 461–473.
13. Milnor, J. W. (1950). On the total curvature of knots. *Ann. Math.*, 52(2): 248–237.
14. Newman, D. J., Shapiro, H. S. (1966). Hilbert spaces of entire functions. *Bull. Amer. Math. Soc.*, 72: 971–977.
15. Nguyen, H., Nguyen, O., Vu, V. (2016). On the number of real roots of random polynomials. [arXiv: 1402.4628](https://arxiv.org/abs/1402.4628), *Comm. Contemp. Math.* 18(4): 1550052, 17 pp.
16. Nguyen, O., Van, V. (2021). Random polynomials: central limit theorems for the real roots. [arXiv: 1904.04347](https://arxiv.org/abs/1904.04347), *Duke Math. J.* 170(17): 3745–3813.
17. Nicolaescu, L. I. (2016). A stochastic Gauss-Bonnet-Chern formula. *Probab. Th. Related Fields*, 65(1-2): 235–265.
18. Nicolaescu, L. I. (2020). *Lectures on the Geometry of Manifolds*. 3rd Edition, Singapore: World Scientific.
19. Rice, S. O. (1945). Mathematical analysis of random noise. *Bell System Tech. J.*, 24: 46–156.

20. Szegő, G. (1939). *Orthogonal polynomials*. Colloquium Publications, vol.23, (2003 Reprint), Providence, RI: Amer. Math. Soc..
21. Toponogov, V. A. (2006). *Differential Geometry of Curves and Surfaces. A Concise Guide*. Boston, MA: Birkhäuser.

LIVIU I. NICOLAESCU received his Ph.D. mathematics in 1994 from Michigan State University. He held postdoctoral positions at the University of Michigan and McMaster University before joining the University of Notre Dame where he is currently Professor of Mathematics. He defines himself as a “geometer at large” with eclectic interests. He is the author of over 50 research papers and several monographs.

Department of Mathematics, University of Notre Dame, Notre Dame, IN 46556
lnicolae@nd.edu