

On the asymptotic variance of the number of real roots of random polynomial systems

D. Armentano* J.-M. Azaïs† F. Dalmao‡ J. R. León§

April 6, 2017

Abstract

We obtain the asymptotic variance, as the degree goes to infinity, of the normalized number of real roots of a square Kostlan-Shub-Smale random polynomial system of any size. Our main tools are the Kac-Rice formula for the second factorial moment of the number of roots and a Hermite expansion of this random variable.

Keywords: *Kostlan-Shub-Smale random polynomials, Kac-Rice formula, Hermite expansion.*

AMS subject classification: Primary: 60F05, 30C15. Secondary: 60G60, 65H10

1 Introduction

The study of the roots of random polynomials is among the most important and popular topics in Mathematics and in some areas of Physics. For almost a century a considerable amount of literature about this problem has emerged from fields as probability, geometry, algebraic geometry, algorithm complexity, quantum physics, etc. In spite of its rich history it is still an extremely active field.

There are several reasons that lead to consider random polynomials and several ways to randomize them, see Bharucha-Reid and Sambandham [3].

The case of algebraic polynomials $P_d(t) = \sum_{j=1}^d a_j t^j$ with independent identically distributed coefficients was the first one to be extensively studied and was completely understood during the 70s. If a_1 is centered, $\mathbb{P}(a_1 = 0) = 0$ and $\mathbb{E}(|a_1|^{2+\delta}) < \infty$ for some $\delta > 0$, then, the asymptotic expectation and the asymptotic variance of the number of real roots of P_d , as the degree d tends to infinity, are of order $\log(d)$ and, once normalized, the number of real roots converges in distribution towards a centered Gaussian random variable. See the books by Farahmand [7] and Bharucha-Reid and Sambandham [3] and the references therein for the whole picture.

*CMAT, Universidad de la República, Montevideo, Uruguay. E-mail: diego@cmat.edu.uy.

†IMT, Université de Toulouse, Toulouse, France. Email: jean-marc.azais@math.univ-toulouse.fr

‡DMEL, Universidad de la República, Salto, Uruguay. E-mail: fdalmao@unorte.edu.uy.

§Escuela de Matemática. Facultad de Ciencias. Universidad Central de Venezuela, Caracas, Venezuela. E-mail: jose.leon@ciens.ucv.ve

The case of systems of polynomial equations seems to be considerably harder and has received in consequence much less attention. The results in this direction are confined to the Shub-Smale model and some other invariant distributions. The ensemble of Shub-Smale random polynomials was introduced in the early 90s by Kostlan [9]. Kostlan argues that this is the most natural distribution for a polynomial system. The exact expectation was obtained in the early 90's by geometric means, see Edelman and Kostlan [5] for the one-dimensional case and Shub and Smale [17] for the multi-dimensional one. In 2004, 2005 Azaïs and Wschebor [2] and Wschebor [18] obtained by probabilistic methods the asymptotic variance as the number of equations and variables tends to infinity. Recently, Dalmao [4] obtained the asymptotic variance and a CLT for the number of zeros as the degree d goes to infinity in the case of one equation in one variable. Letendre in [13] studied the asymptotic behavior of the volume of random real algebraic submanifolds. His results include the finiteness of the limit variance, when the degree tends to infinity, of the volume of the zero sets of Kostlan-Shub-Smale systems with strictly less equations than variables. Some results for the expectation and variance of related models are included in [2, 11, 12].

In the present paper we prove that, as the degree goes to infinity, the asymptotic variance of the normalized number of real roots of a Kostlan-Shub-Smale square random system with m equations and m variables exists in $(0, \infty)$. We use Rice Formulas [1] to show the finiteness of the limit variance and Hermite expansions as in Kratz and León [10] to show that it is strictly positive. Furthermore, we strongly exploit the invariance under isometries of the distribution of the polynomials.

The reader may wonder, in view of the results mentioned above, if the normalized number of roots satisfies a CLT when the degree of the system tends to infinity. The answer is affirmative if $m = 1$ [4] but for the time being we cannot give an answer to this question for $m > 1$. The ingredients to prove a CLT for a non linear functional of a Gaussian process are: a) to write a representation in the Itô-Wiener chaos of the normalized functional; b) to demonstrate that each component verifies a CLT (Fourth Moment Theorem [15], [16]) and if the functional has an expansion involving infinitely many terms: c) to prove that the tail of the asymptotic variance tends uniformly (w.r.t. d) to zero. In the present case we lack a proof of c). For $m = 1$ the fact that the invariance by rotations is equivalent with the stationarity allows to build a proof similar to the one made for the number of crossings of a stationary Gaussian process. For $m > 1$ we are not able to reproduce this type of demonstration due to the difficulty of working on the sphere. In particular, the lack of tessellations (or regular partitions) of the sphere is an issue when trying to get the uniform negligibility of the tails.

The rest of the paper is organized as follows. Section 2 sets the problem and presents the main result. Section 3 deals with the proof and Section 4 presents some auxiliary results as well as the explicit form of the asymptotic variance.

2 Main Result

Consider a square system $\mathbf{P} = 0$ of m polynomial equations in m variables with common degree $d > 1$. More precisely, let $\mathbf{P} = (P_1, \dots, P_m)$ with

$$P_\ell(t) = \sum_{|\mathbf{j}| \leq d} a_{\mathbf{j}}^{(\ell)} t^{\mathbf{j}},$$

where

1. $\mathbf{j} = (j_1, \dots, j_m) \in \mathbb{N}^m$ and $|\mathbf{j}| = \sum_{k=1}^m j_k$;
2. $a_{\mathbf{j}}^{(\ell)} = a_{j_1 \dots j_m}^{(\ell)} \in \mathbb{R}$, $\ell = 1, \dots, m$, $|\mathbf{j}| \leq d$;
3. $t = (t_1, \dots, t_m)$ and $t^{\mathbf{j}} = \prod_{k=1}^m t_k^{j_k}$.

We say that \mathbf{P} has the Kostlan-Shub-Smale (KSS for short) distribution if the coefficients $a_{\mathbf{j}}^{(\ell)}$ are independent centered normally distributed random variables with variances

$$\text{Var} \left(a_{\mathbf{j}}^{(\ell)} \right) = \binom{d}{\mathbf{j}} = \frac{d!}{j_1! \dots j_m! (d - |\mathbf{j}|)!}.$$

We are interested in the number of real roots of \mathbf{P} that we denote by $N_d^{\mathbf{P}}$. Shub and Smale [17] proved that $\mathbb{E}(N_d^{\mathbf{P}}) = d^{m/2}$. Our main result is the following.

Theorem 1. *Let \mathbf{P} be a KSS random polynomial system with m equations, m variables and degree d . Then, as $d \rightarrow \infty$ we have*

$$\lim_{d \rightarrow \infty} \frac{\text{Var}(N_d^{\mathbf{P}})}{d^{m/2}} = V_\infty^2,$$

where $0 < V_\infty^2 < \infty$.

An explicit expression of V_∞^2 is given in Theorem 2 in the Appendix.

3 Proof

3.1 Preliminaries

It is customary and convenient to homogenize the polynomials. That is, to add an auxiliary variable t_0 and to multiply the monomial in P_ℓ corresponding to the index \mathbf{j} by $t_0^{d-|\mathbf{j}|}$. Let $\mathbf{Y} = (Y_1, \dots, Y_m)$ denote the resulting vector of m homogeneous polynomials in $m + 1$ real variables with common degree $d > 1$. We have,

$$Y_\ell(t) = \sum_{|\mathbf{j}|=d} a_{\mathbf{j}}^{(\ell)} t^{\mathbf{j}}, \quad \ell = 1, \dots, m,$$

where this time $\mathbf{j} = (j_0, \dots, j_m) \in \mathbb{N}^{m+1}$; $|\mathbf{j}| = \sum_{k=0}^m j_k$; $a_{\mathbf{j}}^{(\ell)} = a_{j_0 \dots j_m}^{(\ell)} \in \mathbb{R}$; $t = (t_0, \dots, t_m) \in \mathbb{R}^{m+1}$ and $t^{\mathbf{j}} = \prod_{k=0}^m t_k^{j_k}$.

Since \mathbf{Y} is homogeneous, its roots consist of lines through 0 in \mathbb{R}^{m+1} . Then, it is easy to check that each root of \mathbf{P} corresponds exactly to two (opposite) roots of \mathbf{Y} on the unit sphere S^m of \mathbb{R}^{m+1} . Furthermore, one can prove that the subset of homogeneous polynomials \mathbf{Y} with roots lying in the hyperplane $t_0 = 0$ has Lebesgue measure zero. Then, denoting by $N_d^{\mathbf{Y}}$ the number of roots of \mathbf{Y} on S^m , we have $N_d^{\mathbf{P}} = N_d^{\mathbf{Y}}/2$ almost surely.

From now on we work with the homogenized version \mathbf{Y} . Standard multinomial formula shows that for all $s, t \in \mathbb{R}^{m+1}$ we have

$$r_d(s, t) := \mathbb{E}(Y_\ell(s)Y_\ell(t)) = \langle s, t \rangle^d,$$

where $\langle \cdot, \cdot \rangle$ is the usual inner product in \mathbb{R}^{m+1} . As a consequence, we see that the distribution of the system \mathbf{Y} is invariant under the action of the orthogonal group in \mathbb{R}^{m+1} . For the ease of notation we omit the dependence on d of \mathbf{Y} .

In the sequel we need to consider the derivative of Y_ℓ , $\ell = 1, \dots, m$. Since the parameter space is the sphere S^m , the derivative is taken in the sense of the sphere, that is, the spherical derivative $Y'_\ell(t)$ of $Y_\ell(t)$ is the orthogonal projection of the free gradient on the tangent space t^\perp of S^m at t . The k -th component of $Y'_\ell(t)$ at a given basis of the tangent space is denoted by $Y'_{\ell k}(t)$.

The covariances between the derivatives and between the derivatives and the process are obtained via routine computations from the covariance of Y_ℓ . In particular, the invariance under isometries is preserved after derivation and for each $t \in S^m$ $\mathbf{Y}(t)$ is independent from $\overline{\mathbf{Y}}'(t)$.

3.2 Finiteness of the limit variance

In this section we prove that

$$\lim_{d \rightarrow \infty} \frac{\text{Var}(N_d^{\mathbf{P}})}{d^{m/2}} < \infty.$$

Recall that $\mathbb{E}(N_d^{\mathbf{P}}) = d^{m/2}$, we write

$$\text{Var}(N_d^{\mathbf{P}}) = \text{Var}\left(\frac{N_d^{\mathbf{Y}}}{2}\right) = \frac{1}{4} [\mathbb{E}(N_d^{\mathbf{Y}}(N_d^{\mathbf{Y}} - 1)) - \mathbb{E}^2(N_d^{\mathbf{Y}})] + \frac{d^{m/2}}{2}. \quad (3.1)$$

The quantity $\mathbb{E}(N_d^{\mathbf{Y}}(N_d^{\mathbf{Y}} - 1))$ is computed via Rice formula [1].

$$\begin{aligned} \mathbb{E}(N_d^{\mathbf{Y}}(N_d^{\mathbf{Y}} - 1)) &= \int_{(S^m)^2} \mathbb{E}[|\det \mathbf{Y}'(s) \det \mathbf{Y}'(t)| | \mathbf{Y}(s) = \mathbf{Y}(t) = 0] \\ &\quad \cdot p_{\mathbf{Y}(s), \mathbf{Y}(t)}(0, 0) ds dt. \end{aligned}$$

Here ds and dt are the m -geometric measure on S^m but we will use in other parts ds and dt for the Lebesgue measure.

Let $\{e_0, e_1, \dots, e_m\}$ be the canonical basis of \mathbb{R}^{m+1} . Because of the invariance by isometries we can assume without loss of generality that

$$s = e_0, \quad t = \cos(\psi)e_0 + \sin(\psi)e_1. \quad (3.2)$$

For s^\perp we choose as basis $\{e_1, \dots, e_m\}$ and $\{\sin(\psi)e_0 - \cos(\psi)e_1, e_2, \dots, e_m\}$ for t^\perp . Finally, take $\psi = z/\sqrt{d}$ and use Lemma 3. Hence,

$$\begin{aligned} &d^{-m/2} \mathbb{E}(N_d^{\mathbf{Y}}(N_d^{\mathbf{Y}} - 1)) \\ &= \frac{\kappa_m \kappa_{m-1}}{(2\pi)^m \sqrt{d}} \int_0^{\sqrt{d}\pi} \sin^{m-1}\left(\frac{z}{\sqrt{d}}\right) \frac{d^{m/2}}{\left(1 - \cos^{2d}\left(\frac{z}{\sqrt{d}}\right)\right)^{m/2}} \mathcal{E}\left(\frac{z}{\sqrt{d}}\right) dz, \end{aligned}$$

where $\mathcal{E}(z/\sqrt{d})$ is the conditional expectation written for s, t as in (3.2) and κ_m is the m -geometric volume of the sphere S^m .

Now, we deal with the conditional expectation $\mathcal{E}(z/\sqrt{d})$. Introduce the following notation

$$\begin{aligned}\mathcal{A}\left(\frac{z}{\sqrt{d}}\right) &= -\sqrt{d}\cos^{d-1}\left(\frac{z}{\sqrt{d}}\right)\sin\left(\frac{z}{\sqrt{d}}\right); \\ \mathcal{B}\left(\frac{z}{\sqrt{d}}\right) &= \cos^d\left(\frac{z}{\sqrt{d}}\right) - (d-1)\cos^{d-2}\left(\frac{z}{\sqrt{d}}\right)\sin^2\left(\frac{z}{\sqrt{d}}\right); \\ \mathcal{C}\left(\frac{z}{\sqrt{d}}\right) &= \cos^d\left(\frac{z}{\sqrt{d}}\right); \\ \mathcal{D}\left(\frac{z}{\sqrt{d}}\right) &= \cos^{d-1}\left(\frac{z}{\sqrt{d}}\right);\end{aligned}$$

and -omitting the (z/\sqrt{d}) -

$$\sigma^2 = 1 - \frac{\mathcal{A}^2}{1 - \mathcal{C}^2}, \quad \rho = \frac{\mathcal{B}(1 - \mathcal{C}^2) - \mathcal{A}^2\mathcal{C}}{1 - \mathcal{C}^2 - \mathcal{A}^2}.$$

Thus, we can write the variance-covariance matrix of the vector $(Y_\ell(s), Y_\ell(t), \frac{Y'_\ell(s)}{\sqrt{d}}, \frac{Y'_\ell(t)}{\sqrt{d}})$ in the following form

$$\left[\begin{array}{c|c|c} A_{11} & A_{12} & A_{13} \\ \hline A_{12} & I_m & A_{23} \\ \hline A_{13} & A_{23} & I_m \end{array} \right],$$

where I_m is the $m \times m$ identity matrix,

$$A_{11} = \begin{bmatrix} 1 & \mathcal{C} \\ \mathcal{C} & 1 \end{bmatrix}, \quad A_{12} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ -\mathcal{A} & 0 & \cdots & 0 \end{bmatrix}, \quad A_{13} = \begin{bmatrix} \mathcal{A} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{bmatrix},$$

and $A_{23} = \text{diag}([\mathcal{B}, \mathcal{D}, \dots, \mathcal{D}])_{m \times m}$.

Regression formulas imply that the conditional distribution of the vector $(\frac{Y'_\ell(s)}{\sqrt{d}}, \frac{Y'_\ell(t)}{\sqrt{d}})$ (conditioned on $\mathbf{Y}(s) = \mathbf{Y}(t) = 0$) is centered normal with variance-covariance matrix:

$$\left[\begin{array}{c|c} B_{11} & B_{12} \\ \hline B_{12} & B_{22} \end{array} \right], \quad (3.3)$$

with $B_{11} = B_{22} = \text{diag}([\sigma^2, 1, \dots, 1])$ and $B_{12} = \text{diag}([\sigma^2\rho, \mathcal{D}, \dots, \mathcal{D}])$.

It is important to remark that if $A = (A_1 A_2 \dots A_m)$ is a matrix with columns vectors A_j , it holds that $\det(A) = Q_m(A_1, A_2, \dots, A_m)$ for a certain polynomial Q_m of degree m from \mathbb{R}^{m^2} to \mathbb{R} . Using representation of Gaussian vectors from a standard one we can write

$$\begin{aligned}\mathcal{E}\left(\frac{z}{\sqrt{d}}\right) &= \int_{(\mathbb{R}^{m^2})^2} \phi_{m^2}(\mathbf{x})\phi_{m^2}(\mathbf{y}) \left| Q_m \left(\left(\begin{array}{c} \sigma x_{11} \\ x_{12} \\ \vdots \\ x_{1m} \end{array} \right), \dots, \left(\begin{array}{c} \sigma x_{m1} \\ x_{m2} \\ \vdots \\ x_{mm} \end{array} \right) \right) \right| \\ &\left| Q_m \left(\left(\begin{array}{c} \sigma(\rho x_{11} + \sqrt{1-\rho^2}y_{11}) \\ \mathcal{D}x_{12} + \sqrt{1-\mathcal{D}^2}y_{12} \\ \vdots \\ \mathcal{D}x_{1m} + \sqrt{1-\mathcal{D}^2}y_{1m} \end{array} \right), \dots, \left(\begin{array}{c} \sigma(\rho x_{m1} + \sqrt{1-\rho^2}y_{m1}) \\ \mathcal{D}x_{m2} + \sqrt{1-\mathcal{D}^2}y_{m2} \\ \vdots \\ \mathcal{D}x_{mm} + \sqrt{1-\mathcal{D}^2}y_{mm} \end{array} \right) \right) \right| dx dy,\end{aligned}$$

where ϕ_{m^2} is the standard normal density in \mathbb{R}^{m^2} . Because of the homogeneity of the determinant we have

$$\mathcal{E}\left(\frac{z}{\sqrt{d}}\right) = \sigma^2 \int_{(\mathbb{R}^{m^2})^2} Q_m(\mathbf{x})Q_m(\mathbf{z})\phi_{m^2}(\mathbf{x})\phi_{m^2}(\mathbf{y})d\mathbf{x}d\mathbf{y} =: \sigma^2 G(\rho, \mathcal{D}),$$

where $\mathbf{z} = \text{diag}([\rho, \mathcal{D}, \dots, \mathcal{D}])\mathbf{x} + \text{diag}([\sqrt{1-\rho^2}, \sqrt{1-\mathcal{D}^2}, \dots, \sqrt{1-\mathcal{D}^2}])\mathbf{y}$.
Now, we return to the expression of the variance in (3.1). We have

$$\begin{aligned} d^{-m/2}\text{Var}\left(N_d^{\mathbf{P}}\right) &= \frac{1}{4d^{m/2}}\left[\mathbb{E}\left(N_d^{\mathbf{Y}}\left(N_d^{\mathbf{Y}}-1\right)\right)-\left(\mathbb{E}\left(N_d^{\mathbf{Y}}\right)\right)^2\right]+\frac{1}{2} \\ &= \frac{1}{2}+\frac{\kappa_m\kappa_{m-1}}{4(2\pi)^m}\int_0^{\sqrt{d}\pi}\sin^{m-1}\left(\frac{z}{\sqrt{d}}\right)d^{(m-1)/2} \\ &\quad \left[\frac{\sigma^2\left(\frac{z}{\sqrt{d}}\right)}{\left[1-\cos^{2d}\left(\frac{z}{\sqrt{d}}\right)\right]^{m/2}}G\left(\rho\left(\frac{z}{\sqrt{d}}\right),\mathcal{D}\left(\frac{z}{\sqrt{d}}\right)\right)-G(0,0)\right]dz. \end{aligned} \quad (3.4)$$

The proof of the convergence of this integral is done in several steps.

In the rest of this section \mathbf{C} denotes an unimportant constant, its value can change from one occurrence to another. It can depend on m , but recall that m is fixed.

Step 1: Bounds for G .

- $G(\rho, \mathcal{D}) = \int_{(\mathbb{R}^{m^2})^2} Q_m(\mathbf{x})Q_m(\mathbf{z})\phi_{m^2}(\mathbf{x})\phi_{m^2}(\mathbf{y})d\mathbf{x}d\mathbf{y}$;
- $G(0, 0) = \int_{(\mathbb{R}^{m^2})^2} Q_m(\mathbf{x})Q_m(\mathbf{y})\phi_{m^2}(\mathbf{x})\phi_{m^2}(\mathbf{y})d\mathbf{x}d\mathbf{y}$;
- $|\sqrt{1-\rho^2}-1| \leq \mathbf{C}|\rho|$; $|\sqrt{1-(\mathcal{D})^2}-1| \leq \mathbf{C}|\mathcal{D}|$;
- $|Q_m(\mathbf{x})| \leq \mathbf{C}(1+\|\mathbf{x}\|_\infty)^m$;
- any partial derivative of $Q_m(\mathbf{w})$ is a polynomial of degree $m-1$ and thus it is bounded by $\mathbf{C}(1+\|\mathbf{w}\|_\infty)^{m-1}$;

Applying that to a point between \mathbf{y} and \mathbf{z} , we get

$$\begin{aligned} |Q_m(\mathbf{z})-Q_m(\mathbf{y})| &\leq \mathbf{C}(1+\|\mathbf{y}\|_\infty+\|\mathbf{z}\|_\infty)^{m-1}(|\rho|+|\mathcal{D}|) \\ &\leq \mathbf{C}(1+\|\mathbf{x}\|_\infty+\|\mathbf{y}\|_\infty)^{m-1}(|\rho|+|\mathcal{D}|), \end{aligned}$$

and

$$\begin{aligned} |Q_m(\mathbf{x})\cdot Q_m(\mathbf{z})-Q_m(\mathbf{x})\cdot Q_m(\mathbf{y})| \\ \leq \mathbf{C}(1+\|\mathbf{x}\|_\infty)^m(1+\|\mathbf{x}\|_\infty+\|\mathbf{y}\|_\infty)^{m-1}(|\rho|+|\mathcal{D}|). \end{aligned}$$

The finitude of all the moments of the supremum of Gaussian random variables finally yields

$$|G(\rho, \mathcal{D})-G(0, 0)| \leq \mathbf{C}(|\rho|+|\mathcal{D}|).$$

Step 2: Point-wise convergence. It is a direct consequence of the expansions of sine and cosine functions. As d tends to infinity:

1. $\mathcal{A}\left(\frac{z}{\sqrt{d}}\right) \rightarrow -z \exp(-z^2/2)$;
2. $\mathcal{B}\left(\frac{z}{\sqrt{d}}\right) \rightarrow (1-z^2) \exp(-z^2/2)$;
3. $\mathcal{C}\left(\frac{z}{\sqrt{d}}\right)$ and $\mathcal{D}\left(\frac{z}{\sqrt{d}}\right)$ tend to $\exp(-z^2/2)$;
4. $\sigma^2\left(\frac{z}{\sqrt{d}}\right) \rightarrow \frac{1-(1+z^2)\exp(-z^2)}{1-\exp(-z^2)}$;
5. $\rho\left(\frac{z}{\sqrt{d}}\right) \rightarrow \frac{(1-z^2)^2(1-\exp(-z^2))\exp(-z^2)}{1-(1+z^2)\exp(-z^2)}$.

This, in view of the continuity of the function G , implies the point-wise convergence of the integrand in (3.4).

Step 3: Symmetrization. We have $\mathcal{A}(\pi - z/\sqrt{d}) = (-1)^{d-1}\mathcal{A}(z/\sqrt{d})$, $\mathcal{B}(\pi - z/\sqrt{d}) = (-1)^d\mathcal{B}(z/\sqrt{d})$, $\mathcal{C}(\pi - z/\sqrt{d}) = (-1)^d\mathcal{C}(z/\sqrt{d})$, $\mathcal{D}(\pi - z/\sqrt{d}) = (-1)^{d-1}\mathcal{D}(z/\sqrt{d})$, $\sigma^2(\pi - z/\sqrt{d}) = \sigma^2(z/\sqrt{d})$ and $\rho(\pi - z/\sqrt{d}) = (-1)^d\rho(z/\sqrt{d})$. Hence, $B_{12}(\pi - z/\sqrt{d})$ in (3.3) becomes

$$((-1)^d\sigma^2(z/\sqrt{d})\rho(z/\sqrt{d}), (-1)^{d-1}\mathcal{D}(z/\sqrt{d}), \dots, (-1)^{d-1}\mathcal{D}(z/\sqrt{d})),$$

the rest being unchanged. This corresponds, for example to performing some change of signs (depending on the parity of d) on the coordinates of $Y'_\ell(t)$. Gathering the different ℓ this may imply a change of sign in $\det(\mathbf{Y}'(t))$ that plays no role because of the absolute value. As a consequence

$$\mathcal{E}(\pi - z/\sqrt{d}) = \mathcal{E}(z/\sqrt{d}).$$

In conclusion, for the next step it suffices to dominate the integral in the r.h.s of (3.4) restricted to the interval $[0, \sqrt{d}\pi/2]$.

Step 4: Domination. The following lemma gives bounds for the different terms, its proof is given in the appendix.

Lemma 1. *There exists some constant α , $0 < \alpha \leq 1/2$ and some integer d_0 such that for $\frac{z}{\sqrt{d}} \leq \frac{\pi}{2}$ and $d > d_0$:*

1. $\mathcal{C} \leq \mathcal{D} \leq \cos^{d-2}(\frac{z}{\sqrt{d}}) \leq \exp(-\alpha z^2)$;
2. $|\mathcal{A}| \leq z \exp(-\alpha z^2)$;
3. $\mathcal{B} \leq (1 + z^2) \exp(-\alpha z^2)$;
4. for $z \geq z_0$, $1 - \mathcal{C}^2 \geq 1 - \mathcal{C}^2 - \mathcal{A}^2 \geq \mathbf{C} > 0$;
5. $0 \leq 1 - \sigma^2 \leq \mathbf{C} \exp(-2\alpha z^2)$;
6. $|\rho| \leq \mathbf{C}(1 + z^2)^2 \exp(-2\alpha z^2)$.

We have to find a dominant and to prove the convergence of the integral at zero and at infinity.

At zero, since the function G is bounded we have to give bounds for

$$\frac{d^{\frac{m-1}{2}} \sin^{m-1}\left(\frac{z}{\sqrt{d}}\right) \sigma^2\left(\frac{z}{\sqrt{d}}\right)}{(1 - \cos^{2d}(\frac{z}{\sqrt{d}}))^{m/2}}.$$

Clearly, $d^{\frac{m-1}{2}} \sin^{m-1}(z/\sqrt{d}) \leq z^{m-1}$. Besides,

$$\frac{\sigma^2\left(\frac{z}{\sqrt{d}}\right)}{(1 - \cos^{2d}(\frac{z}{\sqrt{d}}))^{\frac{m}{2}}} = \frac{1 - c_d^2(z) - c_d'^2(z)}{(1 - c_d^2(z))^{\frac{m}{2}+1}},$$

where $c(z) = \mathcal{C}(z/\sqrt{d})$.

For the denominator, using Lemma 1, we have

$$1 - c_d^2(z) \geq \mathbf{C}(1 - \exp(-2\alpha z^2)). \quad (3.5)$$

We turn now to the numerator, let $X_d(\cdot)$ be a formal Gaussian stationary process on the line with covariance c_d . Hence,

$$\begin{aligned} 1 - c_d^2(z) - c_d'^2(z) &= \text{Var}(X_d(z)|X_d(0), X_d'(0)) \\ &= \text{Var}(X_d(z) - X_d(0) - zX_d'(0)|X_d(0), X_d'(0)) \\ &\leq \text{Var}(X_d(z) - X_d(0) - zX_d'(0)) = z^4 \text{Var}\left(\int_0^1 (1-t)X_d''(ut)dt\right), \end{aligned}$$

where we used the Taylor formula with integral rest. The covariance function $\cos(z/\sqrt{d})$ corresponds to the spectral measure $\mu = \frac{1}{2}(\delta_{-d^{-1/2}} + \delta_{d^{-1/2}})$, see [1]. The spectral measure associated to $c_d(z) = \cos^d(z/\sqrt{d})$ is the d -th convolution of μ and a direct computation shows that its fourth spectral moment exists and is bounded uniformly in d . As a consequence, $\text{Var}(X'_d(t))$ is bounded uniformly in d , yielding that

$$1 - c_d^2(z) - c_d'^2(z) \leq \mathbf{C}z^4. \quad (3.6)$$

Using (3.5) and (3.6) we get the convergence at zero.

At infinity, define

$$\begin{aligned} \mathcal{H}\left(\sigma^2\left(\frac{z}{\sqrt{d}}\right), \mathcal{C}\left(\frac{z}{\sqrt{d}}\right), \rho\left(\frac{z}{\sqrt{d}}\right), \mathcal{D}\left(\frac{z}{\sqrt{d}}\right)\right) \\ = \frac{\sigma^{2\left(\frac{z}{\sqrt{d}}\right)}}{\left(1 - \cos^{2d}\left(\frac{z}{\sqrt{d}}\right)\right)^{m/2}} G\left(\rho\left(\frac{z}{\sqrt{d}}\right), \mathcal{D}\left(\frac{z}{\sqrt{d}}\right)\right) dz. \end{aligned}$$

Multiplication of bounded Lipschitz functions gives a Lipschitz function, thus

$$\begin{aligned} \left| \mathcal{H}\left(\sigma^2\left(\frac{z}{\sqrt{d}}\right), \mathcal{C}\left(\frac{z}{\sqrt{d}}\right), \rho\left(\frac{z}{\sqrt{d}}\right), \mathcal{D}\left(\frac{z}{\sqrt{d}}\right)\right) - \mathcal{H}(1, 0, 0, 0) \right| \\ \leq \mathbf{C}(|\sigma^2 - 1| + |\mathcal{C}| + |\rho| + |\mathcal{D}|). \end{aligned}$$

The proof is achieved with Lemma 1.

3.3 Positivity of the limit variance

3.3.1 Hermite expansion of the number of real roots

We introduce the Hermite polynomials $H_n(x)$ by $H_0(x) = 1$, $H_1(x) = x$ and $H_{n+1}(x) = xH_n(x) - nH_{n-1}(x)$. The multi-dimensional versions are, for multi-indexes $\alpha = (\alpha_\ell) \in \mathbb{N}^m$ and $\beta = (\beta_{\ell,k}) \in \mathbb{N}^{m^2}$, and vectors $\mathbf{y} = (y_\ell) \in \mathbb{R}^m$ and $\mathbf{y}' = (y'_{\ell,k}) \in \mathbb{R}^{m^2}$

$$\mathbf{H}_\alpha(\mathbf{y}) = \prod_{\ell=1}^m H_{\alpha_\ell}(y_\ell), \quad \overline{\mathbf{H}}_\beta(\mathbf{y}') = \prod_{\ell,k=1}^m H_{\beta_{\ell,k}}(y'_{\ell,k}).$$

It is well known that the standardized Hermite polynomials $\{\frac{1}{\sqrt{n!}}H_n\}$, $\{\frac{1}{\sqrt{\alpha!}}\mathbf{H}_\alpha\}$ and $\{\frac{1}{\sqrt{\beta!}}\overline{\mathbf{H}}_\beta\}$ form orthonormal bases of the spaces $L^2(\mathbb{R}, \phi_1)$, $L^2(\mathbb{R}^m, \phi_m)$ and $L^2(\mathbb{R}^{m^2}, \phi_{m^2})$ respectively. Here, ϕ_j stands for the standard Gaussian measure on \mathbb{R}^j ($j = 1, m, m^2$) and $\alpha! = \prod_{\ell=1}^m \alpha_\ell!$, $\beta! = \prod_{\ell,k=1}^m \beta_{\ell,k}!$. See [15, 16] for a general picture of Hermite polynomials.

Before stating the Hermite expansion for the normalized number of roots of \mathbf{Y} we need to introduce some coefficients. Let f_β ($\beta \in \mathbb{R}^{m^2}$) be the coefficients in the Hermite's basis of the function $f : \mathbb{R}^{m^2} \rightarrow \mathbb{R}$ such that $f(\mathbf{y}') = |\det(\mathbf{y}')|$. That is $f(\mathbf{y}') = \sum_{\beta \in \mathbb{R}^{m^2}} f_\beta \overline{\mathbf{H}}_\beta(\mathbf{y}')$ with

$$\begin{aligned} f_\beta &= f_{(\beta_1, \dots, \beta_m)} = \frac{1}{\beta!} \int_{\mathbb{R}^{m^2}} |\det(\mathbf{y}')| \overline{\mathbf{H}}_\beta(\mathbf{y}') \phi_{m^2}(\mathbf{y}') d\mathbf{y}' \\ &= \frac{1}{\beta_1! \dots \beta_m!} \int_{\mathbb{R}^{m^2}} |\det(\mathbf{y}')| \prod_{l=1}^m H_{\beta_l}(\mathbf{y}'_l) \frac{\exp\left(-\frac{\|\mathbf{y}'_l\|^2}{2}\right)}{(2\pi)^{\frac{m}{2}}} d\mathbf{y}'_l, \end{aligned}$$

with $\beta_l = (\beta_{l1}, \dots, \beta_{lm})$ and $\mathbf{y}'_l = (y'_{l1}, \dots, y'_{lm})$: $l = 1, \dots, m$.

Parseval's Theorem entails $\|f\|_2^2 = \sum_{q=0}^{\infty} \sum_{|\beta|=q} f_{\beta}^2 \beta! < \infty$. Moreover, since the function f is even w.r.t. each column, the above coefficients are zero whenever $|\beta_l|$ is odd for at least one $l = 1, \dots, m$.

To introduce the next coefficients let us consider first the coefficients in the Hermite's basis in $L^2(\mathbb{R}, \phi_1)$ for the Dirac delta $\delta_0(x)$. They are $b_{2j} = \frac{1}{\sqrt{2\pi}} (-\frac{1}{2})^j \frac{1}{j!}$, and zero for odd indices [10]. Introducing now the distribution $\prod_{j=1}^m \delta_0(y_j)$ and denoting as b_{α} its coefficients it holds

$$b_{\alpha} = \frac{1}{[\frac{\alpha}{2}]!} \prod_{j=1}^m \frac{1}{\sqrt{2\pi}} \left[-\frac{1}{2} \right]^{\lfloor \frac{\alpha_j}{2} \rfloor}$$

or $b_{\alpha} = 0$ if at least one index α_j is odd.

Since the formulas for the covariances of Hermite polynomials work in a neater way when the underlying random variables are standardized, we define the standardized derivative as

$$\bar{Y}'_{\ell}(t) := \frac{Y'_{\ell}(t)}{\sqrt{d}}, \quad \text{and} \quad \bar{\mathbf{Y}}'(t) := (\bar{Y}'_1(t), \dots, \bar{Y}'_m(t)),$$

where $Y'_{\ell}(t)$ denotes the spherical derivative of Y_{ℓ} at $t \in S^m$. As said above, the k -th component of $\bar{\mathbf{Y}}'(t)$ in a given basis is denoted by $\bar{Y}'_{\ell k}(t)$.

Proposition 1. *Let the above notations prevail. We have, in the L^2 sense, that*

$$\bar{N}_d := \frac{N_d^{\mathbf{Y}} - 2d^{m/2}}{2d^{m/4}} = \sum_{q=1}^{\infty} I_{q,d},$$

where

$$I_{q,d} = \frac{d^{m/4}}{2} \int_{S^m} \sum_{|\gamma|=q} c_{\gamma} \mathbf{H}_{\alpha}(\mathbf{y}) \bar{\mathbf{H}}_{\beta}(\mathbf{y}') dt,$$

with $\gamma = (\alpha, \beta) \in \mathbb{N}^m \times \mathbb{N}^{m^2}$ and $|\gamma| = |\alpha| + |\beta|$ and $c_{\gamma} = b_{\alpha} f_{\beta}$.

Remark 1. *Hermite polynomials' properties imply that for $q \neq q'$*

$$\mathbb{E}(I_{q,d} I_{q',d}) = 0.$$

Proposition 1 is a direct consequence of the following lemma.

Lemma 2. *For $\varepsilon > 0$ define*

$$N_{\varepsilon} := \int_{S^m} |\det(\mathbf{Y}'(t))| \delta_{\varepsilon}(\mathbf{Y}(t)) dt,$$

where $\delta_{\varepsilon}(\mathbf{y}) := \prod_{\ell=1}^m \frac{1}{2\varepsilon} \mathbf{1}_{\{|y_{\ell}| < \varepsilon\}}$ and \mathbf{Y}' is the spherical derivative of \mathbf{Y} . Then,

1. For $\mathbf{v} \in \mathbb{R}^m$, let $N_d^{\mathbf{Y}}(\mathbf{v})$ denote the number of real roots in S^m of the equation $\mathbf{Y}(t) = \mathbf{v}$. Then, $N_d^{\mathbf{Y}}(\mathbf{v})$ is bounded above by $2d^m$ almost surely.
2. $N_{\varepsilon} \rightarrow N_d^{\mathbf{Y}}$ almost surely and in the L^2 sense as $\varepsilon \rightarrow 0$.
3. The random variable $N_d^{\mathbf{Y}}$ admits a Hermite's expansion.

Proof. Since the paths of \mathbf{Y} are smooth, Proposition 6.5 of [1] implies that for every $v \in \mathbb{R}^m$ almost surely there is no point $t \in S^m$ such that $\mathbf{Y}(t) = v$ and the spherical gradient is singular. Using the local inversion theorem, this implies that the roots of $\mathbf{Y} = v$ are isolated and by compactness they

are finitely many. As a consequence, $N_d^{\mathbf{Y}}(v)$ is well defined and a.s. finite. Moreover, for every $t \in \mathbb{R}^{m+1}$ such that $Y(t) = v$, $\|t\| = 1$, we have that the set $\{Y_1'(t), \dots, Y_m'(t), t\}$ is almost surely linearly independent in \mathbb{R}^{m+1} . This implies that $N_d^{\mathbf{Y}}(v)$ is uniformly bounded by the Bézout's number $2d^m$ concluding 1 (see for example Milnor [14, Lemma 1, pag. 275]).

By the inverse function theorem, a.s. for every regular value $v \in \mathbb{R}^m$, $N_d^{\mathbf{Y}}(\cdot)$ is locally constant in a neighborhood of v . Furthermore, by the Area Formula (see Federer [8], or [1] Proposition 6.1), for small $\varepsilon > 0$ we have

$$N_\varepsilon = \frac{1}{(2\varepsilon)^m} \int_{[-\varepsilon, \varepsilon]^m} N_d^{\mathbf{Y}}(\mathbf{v}) d\mathbf{v}, \quad a.s. \quad (3.7)$$

Hence,

$$N_d^{\mathbf{Y}}(0) = \lim_{\varepsilon \rightarrow 0} N_\varepsilon, \quad a.s. \quad (3.8)$$

From 1. and (3.7) we have $N_\varepsilon \leq 2d^m$ a.s. Then, the convergence in (3.8) also happens in L^2 .

This convergence allows us getting a Hermite's expansion. We have

$$\begin{aligned} \delta_\varepsilon(\mathbf{y}) &= \sum_{\alpha \in \mathbb{N}^m} b_\alpha^\varepsilon \mathbf{H}_\alpha(\mathbf{y}), \\ \left| \det \left(\frac{\mathbf{y}'}{\sqrt{d}} \right) \right| &= \sum_{\beta \in \mathbb{N}^{m^2}} f_\beta \overline{\mathbf{H}}_\beta \left(\frac{\mathbf{y}'}{\sqrt{d}} \right), \end{aligned}$$

where b_α^ε are the Hermite coefficients of $\delta_\varepsilon(\mathbf{y})$ and the f_β have been already defined. Furthermore, we know that $\lim_{\varepsilon \rightarrow 0} b_\alpha^\varepsilon = b_\alpha$. Now, taking limit and regrouping terms we get as in Estrade and León [6] that

$$N_d = d^{m/2} \sum_{q=0}^{\infty} \sum_{|\alpha|+|\beta|=q} b_\alpha f_\beta \int_{S^m} \mathbf{H}_\alpha(\mathbf{Y}(t)) \overline{\mathbf{H}}_\beta(\overline{\mathbf{Y}}'(t)) dt.$$

This concludes the proof. \square

3.3.2 $V_\infty > 0$

To prove that $V_\infty > 0$ we use the Hermite expansion. In fact,

$$V_\infty^2 = \lim_{d \rightarrow \infty} \sum_{q=2}^{\infty} \text{Var}(I_{q,d}) \geq \lim_{d \rightarrow \infty} \text{Var}(I_{2,d}).$$

By Proposition 1, we have,

$$I_{2,d} = \frac{d^{m/4}}{2} \sum_{|\gamma|=2} c_\gamma \int_{S^m} H_\alpha(\mathbf{Y}(t)) H_\beta(\overline{\mathbf{Y}}'(t)) dt.$$

The coefficients vanish for any odd coefficient $\alpha_\ell, \beta_{\ell,k}$, thus the only possibility to satisfy the condition $|\gamma|=2$ is that only one of the coefficients be 2 and the rest vanish. Hence,

$$I_{2,d} = \frac{d^{m/4}}{2} \int_{S^m} \sum_{\ell=1}^m \left[b_2 b_0^{m-1} f_{(0, \dots, 0)} H_2(Y_\ell(t)) + \sum_{\ell, k=1}^m b_0^m \tilde{f}_{ik2} H_2(\overline{\mathbf{Y}}'_{\ell,k}(t)) \right] dt,$$

where $\tilde{f}_{ik2} = f_{(0, \dots, \beta_{ik}, 0, \dots, 0)}$, $\beta_{ik} = 2$. By Mehler Formula, $\mathbb{E}(H_2(\xi)H_2(\eta)) = 2(\mathbb{E}(\xi\eta))^2 \geq 0$ for jointly normal variables ξ, η . Hence,

$$\begin{aligned} \text{Var}(I_{2,d}) &\geq \frac{d^{m/2}}{4} \int_{(S^m)^2} b_2^2 b_0^{2m-2} f_{(0, \dots, 0)}^2 (\mathbb{E}(Y_1(s)Y_1(t)))^2 ds dt + o(1) \\ &= c_m \int_{S^m} \langle e_0, t \rangle^{2d} dt + o(1). \end{aligned} \quad (3.9)$$

The term $o(1)$ comes from the covariance between the two terms of the sum. In fact, in this case

$$(\mathbb{E} Y_1(s) \overline{Y}'_{1,k}(t))^2 = \delta_{1,k} \left(d^{1/2} \langle s, t \rangle^{d-1} \sqrt{1 - \langle s, t \rangle^2} \right)^2,$$

and after the rescaling this tends to zero. Now, the integral in (3.9) is dealt with as in Section 3.2. In fact, we already have the domination and the point-wise limit of the integrand. Its limit is an integral on $[0, \infty)$ of a positive function, thus, it is strictly positive.

4 Appendix

4.1 Explicit expression of the variance

For $k = 1, \dots, m$ let ξ_k, η_k be independent standard normal random vectors on \mathbb{R}^k . Let us define

- $m_{k,j} = \mathbb{E} (\|\xi_k\|^j) = 2^{j/2} \frac{\Gamma((j+k)/2)}{\Gamma(k/2)}$, where $\|\cdot\|$ is the Euclidean norm on \mathbb{R}^k ;
- for $k = 1, \dots, m-1$, $M_k(t) = \mathbb{E} \left[\|\xi_k\| \|\eta_k + \frac{e^{-t^2/2}}{(1-e^{-t^2})^{1/2}} \xi_k\| \right]$;
- for $k = m$, $M_m(t) = \mathbb{E} \left[\|\xi_m\| \|\eta_m + \frac{\tau(t)}{(\sigma^4(t) - \tau^2(t))^{1/2}} \xi_m\| \right]$.

Using the method of section 12.1.2 of [1] the following result can be proved.

Theorem 2. *We have*

$$V_\infty^2 = \frac{1}{2} + \frac{\kappa_m \kappa_{m-1}}{2(2\pi)^m} \int_0^\infty t^{m-1} \left[\frac{\sigma^4(t)(1-\rho^2(t))}{1-e^{-t^2}} \right]^{1/2} \left[\prod_{k=1}^m M_k(t) - \prod_{k=1}^m m_{k,1}^2 \right] dt.$$

4.2 Integration on the sphere

Lemma 3. *Let \mathcal{H} be a measurable function defined on \mathbb{R} . Then, we have*

$$\begin{aligned} \int_{(S^m)^2} \mathcal{H}(\langle s, t \rangle) ds dt &= \kappa_m \kappa_{m-1} \int_0^\pi \sin(\psi)^{m-1} \mathcal{H}(\cos(\psi)) d\psi \\ &= \frac{\kappa_m \kappa_{m-1}}{\sqrt{d}} \int_0^{\sqrt{d}\pi} \sin\left(\frac{z}{\sqrt{d}}\right)^{m-1} \mathcal{H}\left(\cos\left(\frac{z}{\sqrt{d}}\right)\right) dz. \end{aligned}$$

Proof. The proof is a direct consequence of the formula of integration over sub-manifolds.

$$\int_{S^m} \mathcal{H}(\langle t, e_0 \rangle) dt = \kappa_{m-1} \int_0^\pi \sin(\psi)^{m-1} \mathcal{H}(\cos(\psi)) d\psi.$$

□

4.3 Proof of Lemma 1

Proof. We give the proof of 1, the other cases are similar or easier. On $[0, \pi/2]$ there exists α_1 , $0 < \alpha_1 < 1/2$ such that

$$\cos(\psi) \leq 1 - \alpha_1 \psi^2.$$

Thus,

$$\cos^{d-2} \left(\frac{z}{\sqrt{d}} \right) \leq \left(1 - \frac{\alpha_1 z^2}{d} \right)^{d-2} \leq \exp \left(-\frac{\alpha_1 z^2 (d-2)}{d} \right) \leq \exp \left(-\alpha z^2 \right),$$

as soon as $\alpha < \alpha_1$ and d is big enough. \square

References

- [1] J-M Azaïs and M. Wschebor. Level sets and extrema of random processes and fields. John Wiley & Sons Inc., Hoboken, NJ, (2009), ISBN: 978-0-470-40933-6.
- [2] J-M Azaïs and M. Wschebor. On the roots of a random system of equations. The theorem on Shub and Smale and some extensions. *Found. Comput. Math.* 5 (2005), no. 2, 125-144.
- [3] A.T. Bharucha-Reid and M. Sambandham. Random polynomials. Probability and Mathematical Statistics. Academic Press, Inc., Orlando, FL, (1986), xvi+206 pp. ISBN: 0-12-095710-8.
- [4] F. Dalmao. Asymptotic variance and CLT for the number of zeros of Kostlan Shub Smale random Polynomials. *C.R. Acad. Sci. Paris Ser. I* 353 (2015), 1141-1145.
- [5] A. Edelman and E. Kostlan. How many zeros of a random polynomial are real? *Bull. Amer. Math. Soc. (N.S.)* 32 (1995), no. 1, 1-37.
- [6] A. Estrade and J.R. León. A central limit theorem for the Euler characteristic of a Gaussian excursion set. *Ann. Probab.* 44 (2016), no. 6, 3849-3878.
- [7] K. Farahmand. Topics in random polynomials. Pitman Research Notes in Mathematics Series, 393. Longman, Harlow, (1998), x+163 pp. ISBN: 0-582-35622-9.
- [8] H. Federer. Two theorems in geometric measure theory. *Bull. Amer. Math. Soc.*, 72, (1966), 719.
- [9] E. Kostlan. On the distribution of roots of random polynomials. *From Topology to Computation: Proceedings of the Smalefest (Berkeley, CA, 1990)*, 419-431, Springer, New York, 1993.
- [10] M. F. Kratz and J. R. León. Hermite polynomial expansion for non-smooth functionals of stationary Gaussian processes: crossings and extremes. *Stochastic Process. Appl.*, 66(2), (1997), 237-252.
- [11] A. Lerario and E. Lundberg. On the zeros of random harmonic polynomials: the truncated model. *J. Math. Anal. Appl.* 438 (2016), no. 2, 1041-1054.
- [12] T. Letendre. Expected volume and Euler characteristic of random submanifolds. *J. Funct. Anal.* 270 (2016), no. 8, 3047-3110.

- [13] T. Letendre. Variance of the volume of random real algebraic submanifolds. Preprint (2016) arXiv:1608.05658.
- [14] J. Milnor. On the Betti numbers of real varieties. Proc. Amer. Math. Soc (1964), 15, 275-280.
- [15] I. Nourdin and G. Peccati. Normal approximations with Malliavin calculus. From Stein's method to universality. Cambridge Tracts in Mathematics, 192. Cambridge University Press, Cambridge, (2012), xiv+239 pp. ISBN: 978-1-107-01777-1
- [16] G. Peccati and M. Taqqu. Wiener chaos: moments, cumulants and diagrams. A survey with computer implementation. Supplementary material available online. Bocconi & Springer Series, 1. Springer, Milan; Bocconi University Press, Milan, (2011), xiv+274 pp. ISBN: 978-88-470-1678-1.
- [17] M. Shub and S. Smale. Complexity of Bézout's theorem. II. Volumes and Computational algebraic geometry (Nice, 1992), 267-285, Progr. Math., 109, Birkhäuser Boston, Boston, MA, 1993.
- [18] M. 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.