



Low-Degree Approximation of Random Polynomials

Daouda Niang Diatta¹ · Antonio Lerario²

Received: 14 February 2019 / Revised: 30 January 2021 / Accepted: 11 February 2021 /
Published online: 25 March 2021
© The Author(s) 2021

Abstract

We prove that with “high probability” a random Kostlan polynomial in $n + 1$ many variables and of degree d can be approximated by a polynomial of “low degree” *without* changing the topology of its zero set on the sphere \mathbb{S}^n . The dependence between the “low degree” of the approximation and the “high probability” is quantitative: for example, with overwhelming probability, the zero set of a Kostlan polynomial of degree d is isotopic to the zero set of a polynomial of degree $O(\sqrt{d} \log d)$. The proof is based on a probabilistic study of the size of C^1 -stable neighborhoods of Kostlan polynomials. As a corollary, we prove that certain topological types (e.g., curves with deep nests of ovals or hypersurfaces with rich topology) have exponentially small probability of appearing as zero sets of random Kostlan polynomials.

Keywords Random polynomials · Real algebraic geometry · Harmonic analysis

Mathematics Subject Classification 14P25 · 14P05 · 60G15

1 Introduction

Over the past few years, there has been an intense activity around the field of *Random Algebraic Geometry*, whose main interest has been studying topological properties of the zero set of *random* real algebraic equations.

This approach goes back to the classical work of Kac [15], who studied the expected number of real zeroes of a random polynomial in one variable whose coefficients are

Communicated by Felipe Cucker.

✉ Antonio Lerario
lerario@sissa.it

Daouda Niang Diatta
nddiatta@univ-zig.sn

¹ LMA, University Assane Seck of Ziguinchor, BP 523, Ziguinchor, Senegal

² SISSA, Mathematics area, via Bonomea 265, 34131 Trieste, Italy

Gaussian random variables, and was later extended and generalized in the 1990s to systems of equations in a sequence of influential papers by Edelman, Kostlan, Shub, and Smale [6,7,17,31–33]. More recently, in 2011, Sarnak [28] suggested to look at the connected components of a real algebraic curve from the random point of view, proposing a random version of Hilbert’s Sixteenth Problem (to investigate the “number, shape, and position” of the connected components of a real algebraic hypersurface [35]). Since then, the area has seen much progress [9,11–13,18–21,24,25,28,29], with a focus on the expectation of topological quantities such as the Betti numbers of random algebraic hypersurfaces [9,12,13].

In this paper, we concentrate on the so-called *Kostlan* model: we sample a random polynomial according to the rule

$$P(x) = \sum_{|\alpha|=d} \xi_\alpha \cdot \left(\left(\frac{d!}{\alpha_0! \cdots \alpha_n!} \right)^{1/2} x_0^{\alpha_0} \cdots x_n^{\alpha_n} \right),$$

with $\{\xi_\alpha\}_{|\alpha|=d}$ a family of independent, standard Gaussian variables (see Sect. 3 for more details). A main feature of this probabilistic model, in the univariate case, is that the expectation of the number of real zeroes of a Kostlan polynomial equals \sqrt{d} [6]. This phenomenon is called “square-root law”: essentially the Kostlan polynomial seems to behave as if its degree is \sqrt{d} rather than d . In higher dimensions, a similar phenomenon happens to the Betti numbers of its zero set: their expectation is of the order $O(d^{n/2})$, while the deterministic upper bound is $O(d^n)$. In this paper, we give a further contribution in this direction, by proving the following theorem (see Theorem 7).

Theorem A (Low-degree approximation) *Let P be a random Kostlan polynomial in $n + 1$ many variables and of degree d . Denote by $p = P|_{\mathbb{S}^n}$ its restriction to the unit sphere $\mathbb{S}^n \subset \mathbb{R}^{n+1}$ and by $Z(p) \subset \mathbb{S}^n$ its zero set on the sphere. With probability that goes to one as $d \rightarrow \infty$, the pair $(\mathbb{S}^n, Z(p))$ is diffeomorphic to a pair $(\mathbb{S}^n, Z(q))$ where q is the restriction to the sphere of a polynomial of degree $O(\sqrt{d \log d})$.*

Remark 1 Let us comment on the meaning of this theorem, by looking at the example of real algebraic curves on the sphere \mathbb{S}^2 . As d goes to infinity, the number $D(d)$ of rigid isotopy classes of smooth real curves of degree d on \mathbb{S}^2 grows as $e^{\Theta(d^2)}$ [26]. This means that in the space of curves (i.e., in the space of homogeneous polynomials of degree d) the real discriminant (i.e., the set of curves which are singular) separates the space into super-exponentially many connected components (i.e., rigid isotopy classes, also called *chambers*). Inside the space of curves of degree d , there are the curves of degree $O(\sqrt{d \log d})$; the number of rigid isotopy classes of these curves is much smaller, “only” $e^{\Theta(d \log d)}$. Let us denote by $\mathcal{C}_d = \{c_i\}_{i=1}^{D(d)}$ the set of rigid isotopy classes of smooth curves of degree d on \mathbb{S}^2 . If we put on \mathcal{C}_d the uniform probability distribution (i.e., we set $\mathbb{P}(c_i) = D(d)^{-1}$ for all i), then with probability that goes to one as $d \rightarrow \infty$, curves are not isotopic to curves of smaller degree. However, if we put on \mathcal{C}_d the probability measure such that $\mathbb{P}(c_i)$ equals the Kostlan probability of the corresponding chamber, then most of the mass comes from $\mathcal{C}_{O(\sqrt{d \log d})} \subset \mathcal{C}_d$ and with probability that goes to one as $d \rightarrow \infty$, curves are isotopic to curves of smaller

degree. From the point of view of random Kostlan polynomials, curves which are not isotopic to curves of smaller degree are inaccessible.

The idea of the proof of the previous theorem is the following. Thom’s First Isotopy Lemma implies that, given a function $p : \mathbb{S}^n \rightarrow \mathbb{R}$ whose zero set $Z(p) \subset \mathbb{S}^n$ is nonsingular, there is a small C^1 neighborhood (we call it a “stable neighborhood”) such that all functions in this neighborhood have zero sets diffeomorphic to $Z(p)$. However, how large this neighborhood can be depends on p and in Proposition 3 we prove that it contains a C^1 -ball:

$$\left\{ \|f - p\|_{C^1} < \frac{\delta(p)}{2} \right\} \implies (\mathbb{S}^n, Z(p)) \sim (\mathbb{S}^n, Z(f)), \tag{1.1}$$

where $\delta(p)$ denotes the distance, in the Bombieri–Weyl norm, from p to the set of polynomials with a singular zero set (the “discriminant,” see Sect. 4). In order to produce a low-degree approximation of p , we first write it as $p = \sum_{\ell} p_{\ell}$, where each p_{ℓ} denotes the projection of p to the space of spherical harmonics of degree ℓ , and then take only the part of degree smaller than L of this expansion:

$$p|_L = \sum_{\ell \leq L} p_{\ell}.$$

We will prove that, choosing $L = O(\sqrt{d \log d})$, with probability that goes to one as $d \rightarrow \infty$, the difference $p - p|_L$ has small enough C^1 -norm to be contained in the above stable neighborhood.

From the technical point of view, this last step requires three estimates: we first bound the C^1 -norm of $p - p|_L$ with its Sobolev norm (Proposition 1), then the Sobolev norm with the Bombieri–Weyl norm of the original polynomial (which is the norm endowing the space of polynomials with the Kostlan Gaussian measure, Proposition 2) and finally we estimate the size (i.e., the probability) of a small neighborhood of the discriminant (Proposition 4).

1.1 Consequences

All the previous estimates are quantitative and produce different outcomes for different choices of the degree L to which we truncate the expansion of p . The most general bound that we obtain is the following (Theorem 5): there exists $c_5(n) > 0$ such that for every $L, \sigma > 1$ we have:

$$\mathbb{P} \left\{ \|p - p|_L\|_{C^1} < \frac{\delta(p)}{2} \right\} \geq 1 - \left(c_5(n) d^{\frac{5n}{2} + 2} e^{-\frac{L^2}{4d}} \sigma^2 + \frac{1}{\sigma} \right).$$

For example, choosing L to be a fraction of $d = \deg(p)$, the above σ can be tuned so that the probability from the statement of Theorem 1 goes exponentially fast to one as $d \rightarrow \infty$.

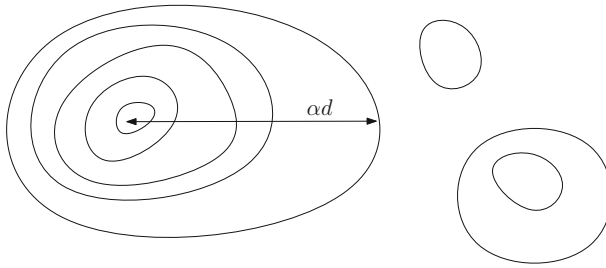


Fig. 1 A random Kostlan curve has $\Theta(d)$ many connected components, however the probability that it has a nest of depth αd decays exponentially fast as $d \rightarrow \infty$ by Theorem 9

We use this idea to constraint the typical topology of $(\mathbb{S}^n, Z(p))$ as follows: (i) we identify a “family” of topological types (e.g., hypersurfaces of the sphere \mathbb{S}^n with more than αd^n many components); (ii) we show that we need at least degree L_d to realize this topological type (e.g., we need degree at least $c(\alpha)d$ to have αd^n many components); (iii) we prove that with “high probability” p can be stably approximated by a polynomial of degree *smaller* than L_d (which implies its zero set *cannot* have that topological type). Here are two examples of the application of this strategy.

(Theorem 8) The probability that the zero set on \mathbb{S}^n of a Kostlan polynomial of degree d has total Betti number larger than αd^n is bounded by $\gamma_1(\alpha)e^{-\gamma_2(\alpha)d}$ for some constants $\gamma_1(\alpha), \gamma_2(\alpha) > 0$. This was known for the case $n = 1$ (points on \mathbb{S}^1) and for the case $n = 2$ (algebraic curves) [10], but only in the case of maximal curves, see Remark 10.

(Theorem 9) The probability that the zero set on \mathbb{S}^n of a Kostlan polynomial of degree d contains a nest of depth αd^n is bounded by $\gamma_1(\alpha)e^{-\gamma_2(\alpha)d}$ for some constants $\gamma_1(\alpha), \gamma_2(\alpha) > 0$, see Fig. 1. For example, hyperbolic hypersurfaces of degree d (whose isotopy class is the one of a nest of spheres of depth d) have exponentially small probability.

Remark 2 Gichev has proved a result with a flavor similar to Theorem 1: in [14, Theorem 5.3] he shows that with probability that goes to one as $d \rightarrow \infty$, a random Kostlan polynomial of degree d can be approximated *in the Sobolev norm* with a polynomial of degree $O(\sqrt{d \log d})$. Unfortunately, we cannot use directly Gichev’s result, essentially because how close should the approximation be in order to guarantee that the zero sets are diffeomorphic depends on p (note that in (1.1) the distance of p from the discriminant is involved). The precise point where the current paper gets close to [14] is in Proposition 2, which is responsible for the similarities. The difference with Gichev’s result relies on the fact that we are not showing only that lower-degree polynomials are “near,” but they are “near enough” so that the zero sets are diffeomorphic. The main practical difference is that Gichev compares the Sobolev norm of the tail with the *Sobolev* norm of p , while in Proposition 2 we compare the Sobolev norm of the tail with the *Bombieri–Weyl* norm of p . This difference is crucial for the final estimate that we will use in Proposition 4. (However, the use of the Sobolev norm is often practical for us too, because it is quite easy to handle it.)

Remark 3 Since the low-degree approximation from Theorem 1 is the projection of p to low-degree harmonics, this could be used, in the case $n = 1$ and with high probability, to improve the complexity of a certain class of algorithms in real algebraic geometry (e.g., adaptive algorithms for real root isolation), essentially showing that “for most polynomials” the bound on the complexity of these algorithms is better than the absolute deterministic bound. We plan to elaborate on this idea in a forthcoming work.

Remark 4 After this paper was written, building on our results, there was some development on the low-degree approximation theme. In [2], Breiding, Keneshlou and the second named author of the current paper generalized Theorem 5 from the case of zero sets on the sphere to more general “singularities” of polynomial maps from the sphere to \mathbb{R}^k ; in [1], Ancona extended our method to the case of zero sets of Gaussian random sections of high tensor power of real line bundles on a general real algebraic manifold.

2 Spaces of Polynomials and Norms

We denote by $\mathcal{P}_{n,d} = \mathbb{R}[x_0, \dots, x_n]_{(d)}$ the space of real homogeneous polynomials of degree d . We endow $\mathcal{P}_{n,d}$ with the Bombieri–Weyl norm, which is defined as follows: writing a homogeneous polynomial in the monomial basis we set:

$$\left\| \sum_{|\alpha|=d} \gamma_\alpha x_0^{\alpha_0} \cdots x_n^{\alpha_n} \right\|_{\text{BW}} = \left(\sum_{|\alpha|=d} \gamma_\alpha^2 \frac{\alpha_0! \cdots \alpha_n!}{d!} \right)^{1/2}.$$

For every $\ell = 0, \dots, d$, we will also consider the space $\mathcal{H}_{n,\ell} \subset \mathcal{P}_{n,\ell}$ of homogeneous harmonic polynomials, i.e., polynomials H such that $\Delta_{\mathbb{R}^{n+1}} H = 0$. It turns out that the space $\mathcal{P}_{n,d}$ can be decomposed as:

$$\mathcal{P}_{n,d} = \bigoplus_{d-\ell \in 2\mathbb{N}} \|x\|^{d-\ell} \mathcal{H}_{n,\ell}. \tag{2.1}$$

The decomposition (2.1) has two important properties (see [16]):

- (i) Given a scalar product which is invariant under the action of $O(n + 1)$ on $\mathcal{P}_{n,d}$ by change of variables, the decomposition (2.1) is orthogonal for this scalar product.
- (ii) The action of $O(n + 1)$ on $\mathcal{P}_{n,d}$ preserves each $\mathcal{H}_{n,\ell}$ and the induced representation on the space of harmonic polynomials is irreducible. In particular, there exists a unique, up to multiples, scalar product on $\mathcal{H}_{n,\ell}$ which is $O(n + 1)$ -invariant.

The space $\mathcal{P}_{n,d}$ injects (by taking restrictions of polynomials) into the space $C^\infty(\mathbb{S}^n, \mathbb{R})$ of smooth functions on the unit sphere $\mathbb{S}^n \subset \mathbb{R}^{n+1}$. We denote by

$$\mathcal{S}_{n,d} = \{p : \mathbb{S}^n \rightarrow \mathbb{R} \mid p = P|_{\mathbb{S}^n} \text{ with } P \in \mathcal{P}_{n,d}\} = \mathcal{P}_{n,d}|_{\mathbb{S}^n}.$$

the image of such injection. In particular, the two vector spaces $\mathcal{P}_{n,d}$ and $\mathcal{S}_{n,d}$ are isomorphic:

$$\mathcal{P}_{n,d} \simeq \mathcal{S}_{n,d} \simeq \mathbb{R}^N \quad \text{where } N = \binom{n+d}{d}.$$

We introduce the following convention: given $P \in \mathcal{P}_{n,d}$, we denote by $p = P|_{\mathbb{S}^n}$ (i.e., we will use capital letters for polynomials in $\mathcal{P}_{n,d}$ and small letters for their restrictions in $\mathcal{S}_{n,d}$). Restricting polynomials in $\mathcal{H}_{n,\ell}$ to the unit sphere, we obtain exactly eigenfunctions of the spherical Laplacian:

$$V_{n,\ell} = \{h : \mathbb{S}^n \rightarrow \mathbb{R} \mid \Delta_{\mathbb{S}^n} h = -\ell(\ell + n - 1)h\} = \mathcal{H}_{n,\ell}|_{\mathbb{S}^n}.$$

We will consider various norms on $\mathcal{S}_{n,d}$:

- (1) The Bombieri–Weyl norm, simply defined for $p = P|_{\mathbb{S}^n}$ as $\|p\|_{\text{BW}} = \|P\|_{\text{BW}}$. Note that the same $p : \mathbb{S}^n \rightarrow \mathbb{R}$ can be the restriction of two different $P_1 \in \mathcal{P}_{n,d_1}$ and $P_2 \in \mathcal{P}_{n,d_2}$ (for example: take $P_2(x) = \|x\|^2 P_1(x)$), it is therefore important for the computation of the Bombieri–Weyl norm to specify the space where p comes from, i.e., its original homogeneous degree.
- (2) The C^1 -norm defined for $p \in \mathcal{S}_{n,d}$ as:

$$\|p\|_{C^1} = \max_{\theta \in \mathbb{S}^n} |p(\theta)| + \max_{\varphi \in \mathbb{S}^n} \|\nabla_{\mathbb{S}^n} p(\varphi)\|,$$

where $\nabla_{\mathbb{S}^n} p$ denotes the *spherical gradient*, i.e., the orthogonal projection on the unit sphere of the gradient of p .

- (3) The L^2 -norm, defined for $p \in \mathcal{S}_{n,d}$ as:

$$\|p\|_{L^2} = \left(\int_{\mathbb{S}^n} p(\theta)^2 \, d\theta \right)^{1/2},$$

where “ $d\theta$ ” denotes integration with respect to the standard volume form of the sphere. In the sequel, we will denote by $\{y_{\ell,j}\}_{j \in J_\ell}$ a chosen L^2 -orthonormal basis of $V_{n,\ell}$.

- (4) The Sobolev q -norm, defined for $p = \sum_{\ell} p_{\ell}$ (decomposed as in (2.1)) by:

$$\|p\|_{H^q} = \left(\|p_0\|^2 + \sum_{d-\ell \in 2\mathbb{N}} \ell^{2q} \|p_{\ell}\|_{L^2}^2 \right)^{1/2}.$$

Note that $\|p_0\|^2 = 0$ when d is odd; moreover, $\|\cdot\|_{H^0} = \|\cdot\|_{L^2}$.

The decomposition (2.1) induces a decomposition:

$$\mathcal{S}_{n,d} = \bigoplus_{d-\ell \in 2\mathbb{N}} V_{n,\ell}. \tag{2.2}$$

By property (i) above, this decomposition is orthogonal, at the same time, for the Bombieri–Weyl, the L^2 and the Sobolev scalar products. Moreover, because of property (ii) above, the Bombieri–Weyl scalar product, the L^2 and the Sobolev one are one multiple of the others on $V_{n,\ell}$ (viewed as a subspace of $\mathcal{P}_{n,d}$):

$$\begin{aligned} \|h_{n,\ell}\|_{L^2} &= w_{n,d}(\ell)\|h_{n,\ell}\|_{\text{BW}}, \quad \|h_{n,\ell}\|_{H^q} \\ &= \ell^q w_{n,d}(\ell)\|h_{n,\ell}\|_{\text{BW}} \quad \forall h_{n,\ell} \in V_{n,\ell} \subset \mathcal{S}_{n,\ell}. \end{aligned}$$

In particular, $\|h_{n,\ell}\|_{H^q} = \ell^q \|h_{n,\ell}\|_{L^2}$.

The rescaling weights are given by (see [9, Example 1]):

$$w_{n,d}(\ell) = \left(\text{vol}(\mathbb{S}^n) \Gamma\left(\frac{n+1}{2}\right) \frac{\Gamma\left(\frac{d+\ell}{2} + 1\right)}{\Gamma\left(\frac{n+1}{2} + \frac{d+\ell}{2}\right)} \frac{1}{2^d} \left(\frac{d}{2}\right) \right)^{1/2}. \tag{2.3}$$

We observe also the following important fact: writing $P = \sum_{\ell} P_{\ell}$ with each $P_{\ell} \in \|x\|^{d-\ell} \mathcal{H}_{n,\ell}$ as in (2.1), when taking restrictions to the unit sphere we have $p = \sum_{\ell} p_{\ell}$ with each p_{ℓ} the restriction to \mathbb{S}^n of a polynomial of degree ℓ : in other words, the restriction to the unit sphere “does not see” the $\|x\|^{d-\ell}$ factor, which is constant on the unit sphere.

Proposition 1 *There exists $c_1(n) > 0$ such that for every $q \geq \frac{n+1}{2}$ and for every $p \in \mathcal{S}_{n,d}$ we have:*

$$\|p\|_{C^1} \leq c_1(n) d^{\frac{1}{2}} \|p\|_{H^q}.$$

Proof Given $p \in \mathcal{S}_{n,d}$, we write $p = \sum_{\ell} h_{\ell}$ with each $h_{\ell} \in V_{n,\ell}$, as in (2.2). We can estimate for $\theta, \varphi \in \mathbb{S}^n$:

$$\begin{aligned} |p(\theta)| + \|\nabla_{\mathbb{S}^n} p(\varphi)\| &\leq \sum_{d-\ell \in 2\mathbb{N}} (|h_{\ell}(\theta)| + \|\nabla_{\mathbb{S}^n} h_{\ell}(\varphi)\|) \\ &\leq C_5(n) \sum_{d-\ell \in 2\mathbb{N}} \ell^{\frac{n+1}{2}} \|h_{\ell}\|_{L^2} \quad (\text{by [30, Theorem 4]}) \\ &\leq C_6(n) \left(\sum_{d-\ell \in 2\mathbb{N}} \ell^{n+1} \|h_{\ell}\|_{L^2}^2 \right)^{1/2} \left(\frac{d}{2}\right)^{1/2} \\ &\quad (\text{by Cauchy–Schwartz inequality}) \\ &\leq c_1(n) \sqrt{d} \|p\|_{H^q} \quad \text{for } q \geq \frac{n+1}{2}. \end{aligned}$$

By taking the supremum over $\theta \in \mathbb{S}^n$ then over $\varphi \in \mathbb{S}^n$, the proof concludes.

3 Gaussian Measures and Random Polynomials

The space $\mathcal{P}_{n,d}$ can be turned into a Gaussian space by sampling a random polynomial according to the rule:

$$P(x) = \sum_{|\alpha|=d} \xi_\alpha \cdot \left(\left(\frac{d!}{\alpha_0! \cdots \alpha_n!} \right)^{1/2} x_0^{\alpha_0} \cdots x_n^{\alpha_n} \right),$$

with $\{\xi_\alpha\}_{|\alpha|=d}$ a family of independent, standard Gaussian variables. A random polynomial defined in this way is called a *Kostlan* polynomial. An alternative way for writing a random Kostlan polynomial is to expand it in the spherical harmonic basis:

$$P(x) = \sum_{d-\ell \in 2\mathbb{N}} \sum_{j \in J_\ell} \xi_{\ell,j} \cdot \left(w_{n,d}(\ell) \|x\|^{d-\ell} y_{\ell,j} \left(\frac{x}{\|x\|} \right) \right),$$

where $\{\xi_{\ell,j}\}_{\ell,j}$ is a family of independent, standard Gaussian variables and $\{w_{n,d}(\ell)\}_{d-\ell \in 2\mathbb{N}}$ are given by (2.3).

Remark 5 Observe that both

$$\left\{ \left(\frac{d!}{\alpha_0! \cdots \alpha_n!} \right)^{1/2} x_0^{\alpha_0} \cdots x_n^{\alpha_n} \right\}_{|\alpha|=d} \quad \text{and} \\ \left\{ w_{n,d}(\ell) \|x\|^{d-\ell} y_{\ell,j} \left(\frac{x}{\|x\|} \right) \right\}_{d-\ell \in 2\mathbb{N}, j \in J_\ell}$$

are Bombieri–Weyl orthonormal bases for $\mathcal{P}_{n,d}$. More generally, given a basis $\{F_k\}_{k=1}^N$ for $\mathcal{P}_{n,d}$ which is orthonormal for the Bombieri–Weyl scalar product, a random Kostlan polynomial can be defined by:

$$F(x) = \sum_{k=1}^N \xi_k F_k(x),$$

where $\{\xi_k\}_{k=1}^N$ is a family of independent, standard Gaussian variables.

Given $L \in \{0, \dots, d\}$, we consider the projection $\mathcal{S}_{n,d} \rightarrow \mathcal{S}_{n,L}$ defined by expanding p in spherical harmonics and taking only the terms of degree at most L of this expansion given by:

$$p := \sum_{d-\ell \in 2\mathbb{N}} p_\ell \quad \mapsto \quad p|_L := \sum_{d-\ell \in 2\mathbb{N}, \ell \leq L} p_\ell.$$

Proposition 2 *There exists $c_2(n) > 0$ such that for all $t, q \geq 0$ and for every $L \in \{0, \dots, d\}$ we have:*

$$\mathbb{P} \left\{ \|p - p|_L\|_{H^q} \leq t \|p\|_{\text{BW}} \right\} \geq 1 - c_2(n) \frac{d^{2q - \frac{n}{2} - 1} e^{-\frac{t^2}{4d}}}{t^2}. \tag{3.1}$$

Remark 6 As already noted, this proposition is similar to [14, Theorem 5.3], which would provide a lower bound for the probability of the event $\{\|p - p|_L\|_{H^q} \leq t\|p\|_{H^q}\}$, with an estimate which has a shape similar to (3.1).

Proof First observe that, since $\{\|p - p|_L\|_{H^q} \leq t\|p\|_{\text{BW}}\} \subset \mathcal{P}_{n,d}$ is a cone, denoting by \mathbb{S}^{N-1} the unit sphere in the Bombieri–Weyl norm, the required probability equals:

$$\begin{aligned} \mathbb{P}\left\{\|p - p|_L\|_{H^q} \leq t\|p\|_{\text{BW}}\right\} &= \frac{\text{vol}\left(\{\|p - p|_L\|_{H^q} \leq t\|p\|_{\text{BW}}\} \cap \mathbb{S}^{N-1}\right)}{\text{vol}\left(\mathbb{S}^{N-1}\right)} \\ &= \frac{\text{vol}\left(\{\|p - p|_L\|_{H^q} \leq t\} \cap \mathbb{S}^{N-1}\right)}{\text{vol}\left(\mathbb{S}^{N-1}\right)} \\ &= 1 - \frac{\text{vol}\left(\{\|p - p|_L\|_{H^q} > t\} \cap \mathbb{S}^{N-1}\right)}{\text{vol}\left(\mathbb{S}^{N-1}\right)}. \end{aligned}$$

We will estimate the quantity

$$Q(t) = \frac{\text{vol}\left(\{\|p - p|_L\|_{H^q} > t\} \cap \mathbb{S}^{N-1}\right)}{\text{vol}\left(\mathbb{S}^{N-1}\right)}$$

from above using Markov’s inequality:

$$Q(t) \leq \frac{\mathbb{E}_{p \in \mathbb{S}^{N-1}} \|p - p|_L\|_{H^q}^2}{t^2}, \tag{3.2}$$

where the expectation is computed sampling a polynomial p uniformly from the unit Bombieri–Weyl sphere.

More precisely, expanding p in an L^2 -orthonormal basis $\{y_{\ell,j}\}$ (so that $\{w_{n,d}(\ell)y_{\ell,j}\}$ is a Bombieri–Weyl orthonormal basis)

$$p = \sum_{d-\ell \in 2\mathbb{N}} \sum_{j \in J_\ell} \gamma_{\ell,j} w_{n,d}(\ell) y_{\ell,j},$$

the condition that $p \in \mathbb{S}^{N-1}$ writes $\sum_{\ell,j} \gamma_{\ell,j}^2 = 1$. Consequently, denoting as before “ $d\theta$ ” the integration with respect to the standard volume form of the sphere, we obtain by moments computation [8]:

$$\begin{aligned} \mathbb{E}_{p \in \mathbb{S}^{N-1}} \|p - p|_L\|_{H^q}^2 &= \frac{1}{\text{vol}(\mathbb{S}^{N-1})} \int_{\mathbb{S}^{N-1}} \sum_{\ell > L} \sum_{j \in J_\ell} \ell^{2q} w_{n,d}(\ell)^2 \gamma_{\ell,j}(\theta)^2 d\theta \\ &= \sum_{\ell > L} \sum_{j \in J_\ell} \ell^{2q} w_{n,d}(\ell)^2 \frac{1}{\text{vol}(\mathbb{S}^{N-1})} \int_{\mathbb{S}^{N-1}} \gamma_{\ell,j}(\theta)^2 d\theta \\ &= \sum_{\ell > L} \sum_{j \in J_\ell} \ell^{2q} w_{n,d}(\ell)^2 N^{-1} = (*). \end{aligned}$$

We use now the fact that the cardinality of J_ℓ is $O(\ell^{n-1})$ and that $N \leq (2d)^n$, obtaining the estimate:

$$(*) \leq C_1(n)d^{-n} \sum_{\ell > L} \ell^{2q+n-1} w_{n,d}(\ell)^2. \tag{3.3}$$

Moreover, from (2.3) we easily get:

$$w_{n,d}(\ell)^2 \leq C_2(n)d^{-\frac{n}{2}} \frac{d^{\frac{1}{2}}}{2^{d-1}} \left(\frac{d}{\frac{d-\ell}{2}} \right). \tag{3.4}$$

Substituting (3.4) into (3.3), we get:

$$(*) \leq C_3(n)d^{-\frac{3n}{2}} \sum_{\ell > L} \ell^{2q+n-1} \frac{d^{\frac{1}{2}}}{2^{d-1}} \left(\frac{d}{\frac{d-\ell}{2}} \right) = (**).$$

For $y \in \mathbb{R}$, let us denote now by $\{y\}$ the nearest integer to y with the same parity as d . Then, we can rewrite:

$$(**) = C_3(n)d^{-\frac{3n}{2}} \int_L^\infty \{y\}^{2q+n-1} \frac{d^{\frac{1}{2}}}{2^{d-1}} \left(\frac{d}{\frac{d-\{y\}}{2}} \right) dy.$$

We apply now the change of variable $y = x\sqrt{d}$ in the above integral, and obtain:

$$\begin{aligned} (**) &= C_3(n)d^{-\frac{3n}{2}} \int_{\frac{L}{\sqrt{d}}}^\infty \{x\sqrt{d}\}^{2q+n-1} \frac{d^{\frac{1}{2}}}{2^{d-1}} \left(\frac{d}{\frac{d-\{x\sqrt{d}\}}{2}} \right) \sqrt{d} dx \\ &\leq C_4(n)d^{-\frac{3n}{2} + \frac{2q+n}{2}} \int_{\frac{L}{\sqrt{d}}}^\infty x^{2q+n-1} \frac{d^{\frac{1}{2}}}{2^{d-1}} \left(\frac{d}{\frac{d-\{x\sqrt{d}\}}{2}} \right) dx \\ &\leq C_4(n)d^{-n+q} \int_{\frac{L}{\sqrt{d}}}^\infty x^{2q+n-1} \frac{d^{\frac{1}{2}}}{2^{d-1}} \left(\frac{d}{\frac{d-\{x\sqrt{d}\}}{2}} \right) dx. \end{aligned}$$

We need now to estimate the function:

$$g_d(x) = x^{2q+n-1} \frac{d^{1/2}}{2^{d-1}} \left(\frac{d}{\frac{d-\{x\sqrt{d}\}}{2}} \right).$$

Observe first that $g_d(x) = 0$ whenever $x > \sqrt{d}$, therefore our estimate needs to be done only for $0 \leq x \leq \sqrt{d}$.

To this end, we assume that d is even (the odd case work in an analogous way) and establish the bound:

$$\left(\frac{d}{\frac{d-k}{2}} \right) \leq \left(\frac{d}{2} \right) e^{-\frac{k^2}{4d}} \quad \forall 0 \leq k \leq d \text{ (} k \text{ with the same parity as } d \text{)}. \tag{3.5}$$

Let us set

$$\begin{aligned}
 B &:= \frac{\binom{d}{\frac{d-k}{2}}}{\binom{d}{\frac{d}{2}}} = \frac{(\frac{d}{2})! (\frac{d}{2})!}{(\frac{d+k}{2})! (\frac{d-k}{2})!} \\
 &= \prod_{j=1}^{\frac{k}{2}} \frac{\frac{d}{2} + 1 - j}{\frac{d}{2} + j}.
 \end{aligned}$$

From this, it follows that:

$$\begin{aligned}
 \log(B) &= \sum_{j=1}^{\frac{k}{2}} \log\left(\frac{\frac{d}{2} + 1 - j}{\frac{d}{2} + j}\right) \\
 &= \sum_{j=1}^{\frac{k}{2}} \log\left(1 - 2 \cdot \frac{2j - 1}{d + 2j}\right) \\
 &\leq \sum_{j=1}^{\frac{k}{2}} -2 \cdot \frac{2j - 1}{d + 2j} && \text{(since } \log(1 - x) \leq -x \text{)} \\
 &\leq -\frac{2}{d + k} \sum_{j=1}^{\frac{k}{2}} (2j - 1) && \text{(since } j \leq k/2 \text{)} \\
 &= -\frac{2}{d + k} \frac{k^2}{4} \\
 &\leq -\frac{k^2}{4d} && \text{(since } k \leq d \text{)}.
 \end{aligned}$$

In particular:

$$B = e^{\log(B)} \leq e^{-\frac{k^2}{4d}},$$

which gives the desired claim (3.5).

We also record the asymptotic:

$$\binom{d}{\frac{d}{2}} = \sqrt{\frac{2}{\pi}} \frac{2^d}{\sqrt{d}} (1 + o(1)),$$

which gives:

$$\frac{d^{1/2}}{2^{d-1}} \binom{d}{\frac{d}{2}} \leq A \tag{3.6}$$

for some constant $A > 0$.

We finally turn to the estimate of our function g_d :

$$g_d(x) \leq x^{2q+n-1} \frac{d^{1/2}}{2^{d-1}} \left(\frac{d}{2}\right) e^{-\frac{x^2}{4}} \quad \text{by (3.5)}$$

$$\leq A \cdot x^{2q+n-1} e^{-\frac{x^2}{4}} \quad \text{by (3.6).} \quad (3.7)$$

Using the upper bound (3.7), we have:

$$\begin{aligned} C_4(n)d^{-n+q} \int_{\frac{L}{\sqrt{d}}}^{\infty} x^{2q+n-1} \frac{d^{1/2}}{2^{d-1}} \left(\frac{d}{2}\right) dx \\ = C_4(n)d^{-n+q} \int_{\frac{L}{\sqrt{d}}}^{\sqrt{d}} g_d(x) dx \\ \leq C_5(n)d^{-n+q} \int_{\frac{L}{\sqrt{d}}}^{\sqrt{d}} x^{2q+n-1} e^{-\frac{x^2}{4}} dx \quad \text{by (3.7)} \\ \leq C_6(n)d^{-n+q} \int_{\frac{L^2}{4d}}^{\frac{d}{4}} t^{\frac{2q+n}{2}-1} e^{-t} dt \\ \leq C_7(n)d^{2q-\frac{n}{2}-1} \int_{\frac{L^2}{4d}}^{\infty} e^{-t} dt \\ \leq C_8(n)d^{2q-\frac{n}{2}-1} e^{-\frac{L^2}{4d}}. \end{aligned} \quad (3.8)$$

Finally, using the estimate (3.8) into (3.2) gives the desired inequality.

Remark 7 The final estimate (3.8) from Proposition 2 takes the following interesting shapes:

– If $L = b\sqrt{d}$ with $b > 0$, then:

$$d^{2q-\frac{n}{2}-1} e^{-\frac{L^2}{4d}} \leq d^{2q-\frac{n}{2}-1} e^{-\frac{b^2}{4}}.$$

– If $L = \sqrt{bd \log d}$ with $b > 0$, then:

$$d^{2q-\frac{n}{2}-1} e^{-\frac{L^2}{4d}} \leq d^{2q-\frac{n}{2}-\frac{b}{4}-1}.$$

– If $L = d^b$ with $b \in (\frac{1}{2}, 1)$, then there exist c_1 (depending on b, q and n), $c_2 > 0$ (depending exclusively on b) such that:

$$d^{2q-\frac{n}{2}-1} e^{-\frac{L^2}{4d}} \leq c_1 e^{-\frac{dc_2}{4}}.$$

- If $L = bd$ with $b \in (0, 1)$, then there exist c_1 (depending on b, q and n), $c_2 > 0$ (depending exclusively on b) such that:

$$d^{2q-\frac{n}{2}-1} e^{-\frac{L^2}{4d}} \leq c_1 e^{-c_2 d}. \tag{3.9}$$

4 Stability

Let us consider the discriminant set $\Sigma_{n,d} \subset \mathcal{S}_{n,d}$ consisting of all those polynomials whose zero set on the sphere is singular:

$$\Sigma_{n,d} = \{p \in \mathcal{S}_{n,d} \text{ such that there exists } x \in \mathbb{S}^n \text{ with } p(x) = 0 \text{ and } \nabla_{\mathbb{S}^n} p(x) = 0\}.$$

Given $p \in \mathcal{S}_{n,d}$, we denote by $\delta(p)$ its distance, in the Bombieri–Weyl norm, to $\Sigma_{n,d}$:

$$\delta(p) = \min_{s \in \Sigma_{n,d}} \|s - p\|_{\text{BW}}.$$

If $Z_1, Z_2 \subset \mathbb{S}^n$ are two smooth hypersurfaces, we will write $(\mathbb{S}^n, Z_1) \sim (\mathbb{S}^n, Z_2)$ to denote that the two pairs (\mathbb{S}^n, Z_1) and (\mathbb{S}^n, Z_2) are diffeomorphic. Given $f \in C^1(\mathbb{S}^n, \mathbb{R})$ we denote by $Z(f) \subset \mathbb{S}^n$ its zero set. A small perturbation in the C^1 -norm of a function $f \in C^1(\mathbb{S}^n, \mathbb{R})$ whose zero set $Z(f)$ is nondegenerate does not change the class of the pair $(\mathbb{S}^n, Z(f))$; the next proposition makes this more quantitative.

Proposition 3 *Let $p \in \mathcal{S}_{n,d} \setminus \Sigma_{n,d}$. Given $f \in C^1(\mathbb{S}^n, \mathbb{R}) \mid \|f - p\|_{C^1} < \frac{\delta(p)}{2}$, we have:*

$$(\mathbb{S}^n, Z(p)) \sim (\mathbb{S}^n, Z(f)).$$

Proof For $t \in [0, 1]$, let us consider now the function $f_t = p + t(f - p)$. Since $\|f - p\|_{C^1} < \frac{\delta(p)}{2}$, for all $\theta \in \mathbb{S}^n$ we have:

$$|f_t(\theta) - p(\theta)| < \frac{\delta}{2}.$$

Moreover, since $d \geq 1$, from $\|f - p\|_{C^1} < \frac{\delta(p)}{2}$ we also deduce $\frac{\|f - p\|_{C^1}}{\sqrt{d}} < \frac{\delta(p)}{2}$, which in turn implies for every $t \in [0, 1]$ and $\theta \in \mathbb{S}^n$:

$$\left| \frac{\|\nabla_{\mathbb{S}^n} f_t(\theta)\|}{\sqrt{d}} - \frac{\|\nabla_{\mathbb{S}^n} p(\theta)\|}{\sqrt{d}} \right| < \frac{\delta(p)}{2}. \tag{4.1}$$

Recall from [27, Theorem 5.1] the following explicit expression¹ for $\delta(p)$:

$$\delta(p) = \min_{\theta \in \mathbb{S}^n} \left(|p(\theta)|^2 + \frac{\|\nabla_{\mathbb{S}^n} p(\theta)\|^2}{d} \right)^{1/2}. \tag{4.2}$$

¹ This expression can also be derived from [4, Theorem 19.3], where it is proved that the distance from the real discriminant equals the reciprocal of the condition number. We prefer to quote directly [27] because it seems that this nice work of Raffalli has been forgotten from the literature on the subject.

Note that $\left(|p(\theta)|^2 + \frac{\|\nabla_{\mathbb{S}^n} p(\theta)\|^2}{d}\right)^{1/2}$ equals the distance in \mathbb{R}^2 between the two vectors $v_1(\theta) = (|p(\theta)|, 0)$ and $v_2(\theta) = \left(0, \frac{\|\nabla_{\mathbb{S}^n} p(\theta)\|}{\sqrt{d}}\right)$. Observe also that the two vectors $w_1(t, \theta) = (|f_t(\theta)|, 0)$ and $w_2(t, \theta) = \left(0, \frac{\|\nabla_{\mathbb{S}^n} f_t(\theta)\|}{\sqrt{d}}\right)$, in virtue of (4.1) and (4.2), satisfy:

$$w_1(t, \theta) \in B_1(\theta) = B_{\mathbb{R}^2}\left(v_1(\theta), \frac{\delta(p)}{2}\right)$$

$$\text{and } w_2(t, \theta) \in B_2(\theta) = B_{\mathbb{R}^2}\left(v_2(\theta), \frac{\delta(p)}{2}\right).$$

In particular:

$$\begin{aligned} \left(|f_t(\theta)|^2 + \frac{\|\nabla_{\mathbb{S}^n} f_t(\theta)\|^2}{d}\right)^{1/2} &= \|w_1(t, \theta) - w_2(t, \theta)\| \\ &> d_{\mathbb{R}^2}(B_1(\theta), B_2(\theta)) \\ &= \|v_1(\theta) - v_2(\theta)\| - \delta(p), \end{aligned}$$

where the strict inequality comes from the fact that w_1 and w_2 belong to the interior of the balls.

Taking the minimum over $\theta \in \mathbb{S}^n$ in the above expression gives:

$$\min_{\theta \in \mathbb{S}^n} \left(|f_t(\theta)|^2 + \frac{\|\nabla_{\mathbb{S}^n} f_t(\theta)\|^2}{d}\right)^{1/2} > 0 \quad \forall t \in [0, 1]. \tag{4.3}$$

In particular, the equation $\{f_t = 0\}$ on \mathbb{S}^n is regular for all $t \in [0, 1]$: whenever $f_t(\theta) = 0$, then $\nabla_{\mathbb{S}^n} f_t(\theta)$ cannot vanish because of the strict inequality in (4.3). The result follows now from Thom’s First Isotopy Lemma [22, Proposition 11.1] (see also [34, Théorème 2.D.2]).

Next proposition quantifies how large is the set of stable polynomials in the Bombieri–Weyl norm. This is a special case of [3, Theorem 21.1] (see also [5, Theorem 5.1]), applied to the case of the real discriminant, which has degree $(n + 1)(d - 1)^n$.

Proposition 4 *There exist $c_3(n), c_4(n) > 0$ such that for every $s \geq c_4(n)d^{2n}$ and for $p \in \mathcal{P}_{n,d}$:*

$$\mathbb{P}\left\{\|p\|_{\text{BW}} \leq s\delta(p)\right\} \geq 1 - c_3(n)\frac{d^{2n}}{s}.$$

5 Low-Degree Approximation

Theorem 5 *There exists $c_5(n) > 0$ such that for every $L, \sigma > 1$ we have:*

$$\mathbb{P}\left\{\|p - p|_L\|_{C^1} < \frac{\delta(p)}{2}\right\} \geq 1 - \left(c_5(n)d^{\frac{5n}{2}+2}e^{-\frac{L^2}{4d}}\sigma^2 + \frac{1}{\sigma}\right).$$

Moreover, denoting by $\alpha(d, L) = c_5(n)d^{\frac{5n}{2}+2}e^{-\frac{L^2}{4d}}$, there exist $c_6(n), c_7(n) > 0$ such that for every L, d satisfying $\alpha(d, L) < \frac{1}{2}$, we have:

$$\mathbb{P} \left\{ \|p - p|_L\|_{C^1} < \frac{\delta(p)}{2} \right\} \geq 1 - c_6(n)d^{c_7(n)}e^{-\frac{L^2}{12d}}.$$

Remark 8 Of course, the previous statement is interesting if we can choose $L, \sigma > 0$ in such a way that $\frac{1}{\sigma}$ goes to zero, but not too fast, and L is significantly smaller than d , but not too small, because we still want the exponential term $e^{-\frac{L^2}{4d}}$ to kill the other factors and make the probability go to one.

Proof Let $p \in \mathcal{S}_{n,d}$ and $L \in \{0, \dots, d\}$. We have the following chain of inequalities:

$$\begin{aligned} \|p - p|_L\|_{C^1} &\leq c_1(n)d^{\frac{1}{2}}\|p - p|_L\|_{H^q} && \text{(Proposition 1)} \\ &\leq c_1(n)d^{\frac{1}{2}}t\|p\|_{\text{BW}} && \text{(Proposition 2)} \\ &\leq c_1(n)d^{\frac{1}{2}}ts\delta(p) && \text{(Proposition 4)} \end{aligned} \tag{5.1}$$

which hold for every $q \geq \frac{n+1}{2}, t > 0$ and $s \geq c_4(n)d^{2n}$, with probability

$$\mathbb{P} \geq 1 - \left(c_2(n)\frac{d^{2q-\frac{n}{2}-1}e^{-\frac{L^2}{4d}}}{t^2} + c_3(n)\frac{d^{2n}}{s} \right).$$

We now make the choices:

$$s = c_4(n)d^{2n}\sigma, \quad t = \frac{1}{3c_1(n)c_4(n)d^{2n+1/2}\sigma} \quad \text{and} \quad q = \frac{n+1}{2}.$$

With these choices, we have:

$$s \geq c_4(n)d^{2n} \tag{5.2}$$

$$c_1(n)d^{\frac{1}{2}}ts < \frac{1}{2} \tag{5.3}$$

$$c_2(n)\frac{d^{2q-\frac{n}{2}-1}e^{-\frac{L^2}{4d}}}{t^2} + c_3(n)\frac{d^{2n}}{s} \leq c_5(n)d^{\frac{5n}{2}+2}e^{-\frac{L^2}{4d}}\sigma^2 + \frac{1}{\sigma}, \tag{5.4}$$

where we have set $c_5(n) = c_2(n)(3c_1(n)c_4(n))^2$.

Because of (5.2), we can apply the estimate in (5.1) which, using (5.3), becomes:

$$\|p - p|_L\|_{C^1} \leq c_1(n)d^{\frac{1}{2}}ts\delta(p) < \frac{\delta(p)}{2}.$$

Using (5.4), the last chain of inequalities holds with probability:

$$\mathbb{P} \geq 1 - \left(c_5(n)d^{\frac{5n}{2}+2}e^{-\frac{L^2}{4d}}\sigma^2 + \frac{1}{\sigma} \right).$$

Now denote $\alpha(d, L) = c_5(n)d^{\frac{5n}{2}+2}e^{-\frac{L^2}{4d}}$. We have:

$$\mathbb{P} \left\{ \|p - p|_L\|_{C^1} < \frac{\delta(p)}{2} \right\} \geq 1 - \left(\alpha(d, L)\sigma^2 + \frac{1}{\sigma} \right)$$

for all $\sigma > 1$. In particular,

$$\mathbb{P} \left\{ \|p - p|_L\|_{C^1} < \frac{\delta(p)}{2} \right\} \geq 1 - \inf_{\sigma>1} \left(\alpha(d, L)\sigma^2 + \frac{1}{\sigma} \right).$$

It is not hard to check that this infimum is a minimum. It is attained at $\sigma_0 = \left(\frac{1}{2\alpha(d, L)}\right)^{1/3}$ and is equal to $\frac{2}{3}(2\alpha(d, L))^{\frac{1}{3}}$. Hence, if $\sigma_0 > 1$ (i.e., $\alpha(d, L) < \frac{1}{2}$), we have:

$$\mathbb{P} \left\{ \|p - p|_L\|_{C^1} < \frac{\delta(p)}{2} \right\} \geq 1 - c_6(n)d^{c_7(n)}e^{-\frac{L^2}{12d}},$$

where we have set $c_6(n) = \frac{2}{3}(2c_5(n))^{\frac{1}{3}}$ and $c_7(n) = \frac{5n}{6} + \frac{2}{3}$.

Proposition 6 *For every $a > 0$, there exists $b > 0$ such that for sufficiently large d :*

$$\|p - p|_{\sqrt{bd \log d}}\|_{C^1} < \frac{\delta(p)}{2} \tag{5.5}$$

with probability greater than $1 - O(d^{-a})$.

Proof Let $a > 0$ and $L = \sqrt{bd \log d}$. Then, we have:

$$c_6(n)d^{c_7(n)}e^{-\frac{L^2}{12d}} \leq d^{c_7(n)-\frac{b}{12}} \leq O(d^{-a}),$$

where the last inequality holds for $b > 0$ large enough. We apply now Theorem 5 with this choice and have:

$$\mathbb{P} \left\{ \|p - p|_{\sqrt{bd \log d}}\|_{C^1} < \frac{\delta(p)}{2} \right\} \geq 1 - \left(d^{c_7(n)-\frac{b}{12}} \right) \geq 1 - O(d^{-a}).$$

6 Applications to Random Topology

In this section, we show how the previous results can be used to put constraints on the topological type of the pair $(S^n, Z(p))$ for p a random Kostlan polynomial. The first result is the following more detailed version of Theorem 1 from the Introduction, which we reformulate here making the constants and the quantifiers more precise.

Theorem 7 For every $d \in \mathbb{N}$ and $b > 0$, consider the event $E_d(b) \subset \mathcal{P}_{n,d}$ consisting of the set of Kostlan polynomials p such that $(\mathbb{S}^n, Z(p)) \sim (\mathbb{S}^n, Z(q))$, with q of degree $\sqrt{bd \log d}$. For every $a > 0$, there exist $b > 0$ and $c > 0$ such that $E_d(b)$ holds with probability at least $1 - \frac{c}{d^a}$.

Proof Let $a > 0$ and consider the $b > 0$ given by Proposition 6. Then, Proposition 3, (5.5) implies that the pairs $(\mathbb{S}^n, Z(p))$ and $(\mathbb{S}^n, Z(p|_{\sqrt{bd \log d}}))$ are diffeomorphic and the conclusion follows from Proposition 6.

6.1 Hypersurfaces with Rich Topology

For a topological space X , we denote by $b(X)$ the sum of its \mathbb{Z}_2 -Betti numbers (sometimes also called the homological complexity of X). Recall by [23] that if $P \in \mathbb{R}[x_0, \dots, x_n]_d$, then the zero set of $p = P|_{\mathbb{S}^n}$ has homological complexity bounded by $b(Z(p)) \leq O(d^n)$.

Theorem 8 For $\alpha > 0$, let $M_{\alpha,d} \subset \mathcal{S}_{n,d}$ be the set:

$$M_{\alpha,d} := \{p \in \mathcal{S}_{n,d} | b(Z(p)) \geq \alpha d^n\}.$$

Then, there exist $\gamma_1(\alpha), \gamma_2(\alpha) > 0$ such that:

$$\mathbb{P}(M_{\alpha,d}) \leq \gamma_1(\alpha)e^{-\gamma_2(\alpha)d}.$$

Proof Observe first that if $q \in \mathbb{R}[x_0, \dots, x_n]_L$ (q is just a polynomial of degree L , not necessarily homogeneous), then $b(Z(q)) \leq cL^n$ for some $c > 0$, again by [23]. Hence, if we want $b(Z(q)) > \alpha d^n$ we must have:

$$L > \left(\frac{\alpha}{c}\right)^{\frac{1}{n}} d.$$

Arguing as in the proof of Theorem 5, where now we take the projection $\lambda = \lambda_L : \mathcal{S}_{n,d} \rightarrow \mathcal{S}_{n,L}$ choosing the value $L = \left(\frac{\alpha}{c}\right)^{\frac{1}{n}} d$, we see that for every $t > 0$ and $s \geq c_4(n)d^{2n}$:

$$\|p - p|_L\|_{C^1} \leq c_1(n)d^{\frac{1}{2}}ts\delta(p)$$

with probability

$$\begin{aligned} \mathbb{P} &\geq 1 - \left(c_2(n) \frac{d^{2q - \frac{n}{2} - 1} e^{-\frac{L^2}{4d}}}{t^2} + c_3(n) \frac{d^{2n}}{s} \right) && \text{(Propositions 1, 2, 4)} \\ &\geq 1 - \left(c_5(n, \alpha) \frac{e^{-c_6(\alpha)d}}{t^2} + c_3(n) \frac{d^{2n}}{s} \right) && \text{by (3.9).} \end{aligned}$$

Observe now that:

$$t = c_5(n, \alpha)^{1/2} e^{-\frac{c_6(\alpha)d}{4}} \implies c_5(n, \alpha) \frac{e^{-c_6(\alpha)d}}{t^2} \leq \gamma_3(\alpha) e^{-\gamma_4(\alpha)d} \tag{6.1}$$

for some constants $\gamma_3(\alpha), \gamma_4(\alpha) > 0$, and

$$s = \frac{e^{\frac{c_6(\alpha)d}{4}}}{3c_1(n)d^{1/2}c_5(n, \alpha)^{1/2}} \implies c_3(n) \frac{d^{2n}}{s} \leq \gamma_5(\alpha) e^{-\gamma_6(\alpha)d} \tag{6.2}$$

for some constants $\gamma_5(\alpha), \gamma_6(\alpha) > 0$.

Choosing s as in (6.2) and t as in (6.1), for $d > 0$ large enough we have $s \geq c_4(n)d^{2n}$, and $c_1(n)d^{1/2}ts < \frac{1}{2}$; it follows that there exist constants $\gamma_1(\alpha), \gamma_2(\alpha) > 0$ such that

$$\|p - p|_L\|_{C^1} < \frac{\delta(p)}{2} \quad \text{with probability } \mathbb{P} \geq 1 - \gamma_1(\alpha) e^{-\gamma_2(\alpha)d}. \tag{6.3}$$

The condition $b(Z(p)) > \alpha d^n$ implies that with the choice of $L < \left(\frac{\alpha}{c}\right)^{\frac{1}{n}} d$ we must have $\|p - p|_L\|_{C^1} \geq \frac{\delta(p)}{2}$, for otherwise the zero set of p would be diffeomorphic to the zero set of $p - p|_L$ which, since $\text{deg}(p - p|_L) < L$, has homological complexity bounded by $b(Z(p - p|_L)) < cL^n < \alpha d^n$. In particular:

$$\left\{ b(Z(p)) > \alpha d^n \right\} \subset \left\{ \|p - p|_L\|_{C^1} \geq \frac{\delta(p)}{2} \right\},$$

which combined with (6.3) implies the statement.

Remark 9 Notice that, using Theorem 5 and Remark 7, similar rarefaction estimates can be produced for the set of hypersurface with less rich topology. For instance, those with $b(Z(p)) \geq (d^{1/2+\epsilon})^n$ would have probability smaller than $c_1 e^{-d^{c_2}/2}$, for some constant $c_1(\epsilon), c_2(\epsilon) > 0$.

Remark 10 It is not difficult to derive from Theorem 8 a similar result for random zero projective sets $Z(p) \subset \mathbb{RP}^n$. In this context, the previous result should be compared with [10, Theorem 1], where the authors prove that the Kostlan measure of the set of curves $C \subset \mathbb{RP}^2$ of degree d whose number of components is more than $\frac{(d-1)(d-2)}{2} + 1 - ad$ is $O(e^{-c_2 d})$. Theorem 8 is stronger in two senses: it applies to the general case of hypersurfaces in \mathbb{RP}^n and it gives exponential rarefaction for all sets of the form $\{b_0(Z(p)) \geq \alpha d^n\}$ (i.e., not necessarily a linear correction from the maximal bound).

6.2 Depth of a Nest

Given $p \in \mathcal{S}_{n,d} \setminus \Sigma_{n,d}$, its zero set $Z(p) \subset \mathbb{S}^n$ consists of a finite union of connected, smooth and compact hypersurfaces. Fixing a point $y_\infty \in \mathbb{S}^n$ (with $\mathbb{P} = 1$, this point does not belong to $Z(p)$), every such component of $Z(p)$ separates the sphere \mathbb{S}^n

into two open sets: a “bounded” one (the open set which does not contain y_∞) and an “unbounded” one (the open set which contains y_∞). The nesting graph of $Z(p)$ (with respect to y_∞) is a graph whose vertices are the components of $Z(p)$ and there is an edge between two components if and only if one is contained in the bounded component of the other. The resulting graph is a forest (a union of trees) and we say that $(\mathbb{S}^n, Z(p))$ has a nest of depth m if this forest contains a tree of depth m .

Theorem 9 For $\alpha > 0$, let $N_{\alpha,d} \subset \mathcal{S}_{n,d}$ be the set:

$$N_{\alpha,d} := \{p \in \mathcal{S}_{n,d} \mid Z(p) \text{ has a nest of depth } \geq \alpha d\}.$$

Then, there exist $c_1(\alpha), c_2(\alpha) > 0$ such that:

$$\mathbb{P}(N_{\alpha,d}) \leq c_1(\alpha)e^{-c_2(\alpha)d}.$$

Proof The proof is essentially the same as the proof of Theorem 8, after observing that the depth of every nest of the zero set of a polynomial of degree L is smaller than L .

Acknowledgements We are indebted to Marie-Françoise Roy, who has played a crucial role for the existence of this paper. We also wish to thank the anonymous referees for their constructive comments which helped improving the presentation of the paper.

Funding Open access funding provided by Scuola Internazionale Superiore di Studi Avanzati - SISSA within the CRUI-CARE Agreement.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Michele Ancona. Exponential rarefaction of maximal real algebraic hypersurfaces, 2020.
2. Paul Breiding, Hanieh Keneshlou, and Antonio Lerario. Quantitative Singularity Theory for Random Polynomials. *International Mathematics Research Notices*, 10 2020. rnaa274.
3. Peter Bürgisser and Felipe Cucker. *Condition*, volume 349 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer, Heidelberg, 2013. The geometry of numerical algorithms.
4. Peter Bürgisser and Felipe Cucker. *Condition: The geometry of numerical algorithms*, volume 349 of *Grundlehren der Mathematischen Wissenschaften*. Springer, Heidelberg, 2013.
5. Felipe Cucker, Teresa Krick, and Michael Shub. Computing the homology of real projective sets. *Found. Comput. Math.*, 18(4):929–970, 2018.
6. Alan Edelman and Eric Kostlan. How many zeros of a random polynomial are real? *Bull. Amer. Math. Soc. (N.S.)*, 32(1):1–37, 1995.
7. Alan Edelman, Eric Kostlan, and Michael Shub. How many eigenvalues of a random matrix are real? *J. Amer. Math. Soc.*, 7(1):247–267, 1994.

8. Gerald B. Folland. How to integrate a polynomial over a sphere. *Am. Math. Mon.*, 108(5):446–448, 2001.
9. Y. V. Fyodorov, A. Lerario, and E. Lundberg. On the number of connected components of random algebraic hypersurfaces. *J. Geom. Phys.*, 95:1–20, 2015.
10. Damien Gayet and Jean-Yves Welschinger. Exponential rarefaction of real curves with many components. *Publ. Math. Inst. Hautes Études Sci.*, (113):69–96, 2011.
11. Damien Gayet and Jean-Yves Welschinger. Lower estimates for the expected Betti numbers of random real hypersurfaces. *J. Lond. Math. Soc. (2)*, 90(1):105–120, 2014.
12. Damien Gayet and Jean-Yves Welschinger. Expected topology of random real algebraic submanifolds. *J. Inst. Math. Jussieu*, 14(4):673–702, 2015.
13. Damien Gayet and Jean-Yves Welschinger. Betti numbers of random real hypersurfaces and determinants of random symmetric matrices. *J. Eur. Math. Soc. (JEMS)*, 18(4):733–772, 2016.
14. V. Gichev. Decomposition of the Kostlan-Shub-Smale model for random polynomials. In *Complex analysis and dynamical systems VII*, volume 699 of *Contemp. Math.*, pages 103–120. Amer. Math. Soc., Providence, RI, 2017.
15. M. Kac. On the average number of real roots of a random algebraic equation. *Bull. Amer. Math. Soc.*, 49:314–320, 1943.
16. E. Kostlan. On the distribution of roots of random polynomials. In *From Topology to Computation: Proceedings of the Smalefest (Berkeley, CA, 1990)*, pages 419–431. Springer, New York, 1993.
17. Eric Kostlan. On the expected number of real roots of a system of random polynomial equations. In *Foundations of computational mathematics (Hong Kong, 2000)*, pages 149–188. World Sci. Publ., River Edge, NJ, 2002.
18. Antonio Lerario. Random matrices and the average topology of the intersection of two quadrics. *Proc. Amer. Math. Soc.*, 143(8):3239–3251, 2015.
19. Antonio Lerario and Erik Lundberg. Statistics on Hilbert’s 16th problem. *Int. Math. Res. Not. IMRN*, (12):4293–4321, 2015.
20. Antonio Lerario and Erik Lundberg. Gap probabilities and Betti numbers of a random intersection of quadrics. *Discrete Comput. Geom.*, 55(2):462–496, 2016.
21. Antonio Lerario and Erik Lundberg. On the geometry of random lemniscates. *Proc. Lond. Math. Soc. (3)*, 113(5):649–673, 2016.
22. John Mather. Notes on topological stability john mather, 1970.
23. J. Milnor. On the Betti numbers of real varieties. *Proc. Amer. Math. Soc.*, 15:275–280, 1964.
24. F. Nazarov and M. Sodin. Asymptotic laws for the spatial distribution and the number of connected components of zero sets of Gaussian random functions. *Zh. Mat. Fiz. Anal. Geom.*, 12(3):205–278, 2016.
25. Fedor Nazarov and Mikhail Sodin. On the number of nodal domains of random spherical harmonics. *Amer. J. Math.*, 131(5):1337–1357, 2009.
26. S. Yu. Orevkov and V. M. Kharlamov. Growth order of the number of classes of real plane algebraic curves as the degree grows. *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, 266(Teor. Predst. Din. Sist. Komb. i Algoritm. Metody. 5):218–233, 339, 2000.
27. Christophe Raffalli. Distance to the discriminant. *preprint on arXiv*, 2014. <https://arxiv.org/abs/1404.7253>.
28. Peter Sarnak. Letter to b. gross and j. harris on ovals of random planes curve. *handwritten letter*, 2011. available at <http://publications.ias.edu/sarnak/section/515>
29. Peter Sarnak and Igor Wigman. Topologies of nodal sets of random band limited functions. In *Advances in the theory of automorphic forms and their L-functions*, volume 664 of *Contemp. Math.*, pages 351–365. Amer. Math. Soc., Providence, RI, 2016.
30. R. T. Seeley. Spherical harmonics. *Amer. Math. Monthly*, 73(4, part II):115–121, 1966.
31. M. Shub and S. Smale. Complexity of Bezout’s theorem. II. Volumes and probabilities. In *Computational algebraic geometry (Nice, 1992)*, volume 109 of *Progr. Math.*, pages 267–285. Birkhäuser Boston, Boston, MA, 1993.
32. Michael Shub and Steve Smale. Complexity of Bézout’s theorem. I. Geometric aspects. *J. Amer. Math. Soc.*, 6(2):459–501, 1993.
33. Michael Shub and Steve Smale. Complexity of Bezout’s theorem. III. Condition number and packing. *J. Complexity*, 9(1):4–14, 1993. Festschrift for Joseph F. Traub, Part I.
34. R. Thom. Ensembles et morphismes stratifiés. *Bull. Amer. Math. Soc.*, 75:240–284, 1969.
35. George Wilson. Hilbert’s sixteenth problem. *Topology*, 17(1):53–73, 1978.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.