Condition Numbers for the Cube. I: Univariate Polynomials and Hypersurfaces

Josué Tonelli-Cueto, Elias Tsigaridas

Condition Numbers for the Cube. I: Univariate Polynomials and Hypersurfaces

Josué Tonelli-Cueto
Inria Paris & IMJ-PRG
Sorbonne Université
Paris, France
josue.tonelli.cueto@bizkaia.eu

Elias Tsigaridas
Inria Paris & IMJ-PRG
Sorbonne Université
Paris, France
elias.tsigaridas@inria.fr

ABSTRACT

The condition-based complexity analysis framework is one of the gems of modern numerical algebraic geometry and theoretical computer science. One of the challenges that it poses is to expand the currently limited range of random polynomials that we can handle. Despite important recent progress, the available tools cannot handle random sparse polynomials and Gaussian polynomials, that is polynomials whose coefficients are i.i.d. Gaussian random variables.

We initiate a condition-based complexity framework based on the norm of the cube, that is a step in this direction. We present this framework for real hypersurfaces. We demonstrate its capabilities by providing a new probabilistic complexity analysis for the Plantinga-Vegter algorithm, which covers both random sparse (alas a restricted sparseness structure) polynomials and random Gaussian polynomials. We present explicit results with structured random polynomials for problems with two or more dimensions. Additionally, we provide some estimates of the separation bound of a univariate polynomial in our current framework.

CCS CONCEPTS

• **Theory of computation** → *Design and analysis of algorithms*; *Computational geometry*; • **Mathematics of computing** → Numerical analysis; Computations on polynomials.

KEYWORDS

condition number; probabilistic complexity; sparse polynomials; subdivision methods; numerical algebraic geometry

ACM Reference Format:
Josué Tonelli-Cueto and Elias Tsigaridas. 2020. Condition Numbers for the Cube. I: Univariate Polynomials and Hypersurfaces. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The complexity of numerical algorithms is not uniform. It depends on a measure of the numerical sensitivity of the output with respect to perturbations of the input, called *condition number*. This motivates the condition-based complexity analysis of numerical algorithms. As this analysis is not input-independent, a usual technique is to randomize the input to obtain a probabilistic complexity analysis that reflects the behaviour of the algorithm in practice. We refer the reader to [3] for more details about this paradigm of complexity for numerical algorithms.

After the complete solution of Smale's 17th problem [17], the main challenge in numerical algebraic geometry is to extend the current algorithms and their analysis to more general inputs, sparse and structured polynomials. Regarding the solution of sparse polynomial systems over the complex numbers, there is the groundbreaking work of Malajovich [19, 20] and Malajovich and Rojas [21, 22]. Additionally, there is significant progress in the probabilistic analysis of the condition number for solving some structured polynomial systems by Armentano and Beltrán [1], by Beltrán and Kozhasov [2], and by Ergür, Paouris and Rojas [13, 14].

A common problem with many of the current techniques is that they rely on unitary/orthogonal invariance. Developing techniques that do not rely on this invariance is therefore a central task in the goal of being able to deal with sparse/structured polynomials and more general probability distributions. We make another step in this research direction by developing a condition-based complexity framework that relies on the ∞-norm of the cube, and so it does not rely on the above invariance.

In this paper, we develop the above framework for univariate polynomials and hypersurfaces. We hope to extend it for polynomial systems in future work. To illustrate its advantages we apply it to the study of the complexity of the Plantinga-Vegter algorithm [6, 23] and the separation bounds for the roots of a real univariate polynomials.

In the case of the Plantinga-Vegter algorithm, we are able to show that this algorithm is efficient (i.e., takes polynomial time on the average) for a wide class of random sparse polynomials (Theorem 2.10). This significantly extends the results of [7] (cf. [9]). Additionally, we also cover Gaussian polynomials, in which all coefficients have the same variance.

We note that our aim is not to show that the Plantinga-Vegter is the most efficient algorithm for random sparse polynomials, but that it remains efficient when we restrict it to a wide class of random sparse polynomials. A similar approach was employed in [13] for the algorithm for finding real zeros of real polynomial systems from [10]. However, unlike [13], our analysis applies to structured

polynomials that are sparse, but with a combinatorial restriction on the support. We note that our condition is similar to that in [24] and so is the bound we obtain; the latter is polynomial in the degree and the size of the support and exponential in the number of variables.

We also note that our bounds depend polynomially on the degree and not logarithmically. The latter would be ideal in view of the results of Khovanskiĭ [16] and Kushnirenko's hypothesis, which bound the size of the Betti numbers of zero sets of sparse polynomials independently of the degree. However, few progress have been made in this direction beyond the univariate case [15]. Moreover, many computational problems in real algebraic geometry lack algorithms that are polynomial in the degree, so such bounds contribute to the state-of-the-art.

In the case of univariate polynomials, our results imply that the complex roots of a random real univariate sparse polynomial around the unit interval are well-separated with high probability. Given than the logarithm of the separation bound is an important parameter that controls the complexity of many univariate solvers, this will lead to interesting probabilistic complexity bounds for these solvers.

Our framework is based on variational properties of the polynomials and considered condition numbers and probabilistic techniques from geometric functional analysis. The former follows the variational approach to condition numbers of [27, $2^{\S 2}$] and extends [8] to new norms. The latter has been already applied in [13, 14] and [7], but our applications these methods takes them to the maximum development.

The 1-norm on the space of polynomials behaves as the "dual"norm to the ∞-norm on the cube. This norm is naturally suited for subdivision methods on the cube. The analysis of the Plantinga-Vegter subdivision process using our framework serves the purpose to convince the reader of the advantages of the new framework for the analysis of algorithms. It also has the ambition to bring new insights in the study of algorithms in numerical algebraic geometry. Our approach continues the trend started by [7] of bringing further interactions between the communities of numerical algebraic geometry and symbolic computation.

Notation. Let $\mathcal{P}_{n,d}$ be the space of polynomials in n variables of total degree at most d, $I^n := [-1,1]^n \subset \mathbb{R}^n$ the unit cube and $B_{\mathbb{C}}(x,r)$ complex disk centered at x of radius r. A polynomial $f \in \mathcal{P}_{n,d}$, is $f = \sum_{|\alpha|\leq d} f_\alpha X^\alpha$, even though we commonly omit the summation index. For $X \subseteq \mathbb{R}^n$, we denote by $\mathcal{B}(X)$ the set of boxes (i.e., cubes) contained in X. For any $B \in \mathcal{B}(\mathbb{R}^n)$, we denote by $m(B)$ its *midpoint* and by $w(I)$ its *width*, so that $B = m(B) + w(B)/2[-1,1]^n$.

Organization. In the next section, we introduce the randomness model that we will consider, zintzo random polynomials, and how our framework applies to the subdivision routine of the Plantinga-Vegter algorithm. In Section 3, we introduce the norms with which we will be working and their main properties. In Section 4, we introduce a new condition number adapted to the introduced norms and we prove its main properties. In Section 5, we develop a probabilistic analysis of the introduced condition number for zintzo random polynomials. Finally, in Section 6, we perform the complexity analysis of the subdivision routine of the Plantinga-Vegter algorithm; and in Section 7, we introduce the separation bound.

2 MAIN RESULTS

In this paper, the main result is a different condition-based framework that allows to control the probability of numerical algorithms with respect random polynomials that are sparse and don't have any scaling in their coefficients, as it has been usual with the so-called KSS or dobro random polynomials introduced in [7]. We showcase our techniques with the Plantinga-Vegter algorithm.

2.1 Randomness model

We introduce a new class of random polynomials that is similar to the class of dobro random polynomials [7]. The main difference is that we require a scaling in the coefficients of the random polynomials. In this way, the new class is a more natural model of random polynomials. Moreover, we explicitly include sparseness in the model of randomness.

Let us recall some basic definitions.

(SG) We call a random variable X *subgaussian*, if there exist a $K > 0$ such that for all $t \geq K$,

$$\mathbb{P}(|X| > t) \leq 2\exp(-t^2/K^2).$$

The smallest such K is the *subgaussian constant* of X.

(AC) A random variable X has the *anti-concentration property*, if there exists a $\rho > 0$, such that for all $\varepsilon > 0$,

$$\max\{\mathbb{P}(|X-u| \leq \varepsilon) \mid u \in \mathbb{R}\} \leq 2\rho\varepsilon.$$

The smallest such ρ is the anti-concentration constant of X.

Definition 2.1. Let $M \subseteq \mathbb{N}^n$ be a finite set such that $0, e_1, \ldots, e_n \in M$. A *zintzo random polynomial supported on* M is a random polynomial $\mathfrak{f} = \sum_{\alpha\in M} \mathfrak{f}_\alpha X^\alpha \in \mathcal{P}_{n,d}$ such that the coefficients $\mathfrak{f}_\alpha$ are independent subgaussian random variables with the anti-concentration property.

Remark 2.2. The word "zintzo" is a Basque word that means honest, upright, righteous. We use this word instead of a variation of dobro to emphasize that this class of random polynomials is different from the class of dobro polynomials.

Remark 2.3. The technical condition $0, e_1, \ldots, e_n \in M$ is there because is needed in our proofs. In layman's terms, this technical condition states that all the terms of the first order approximation of $\mathfrak{f}$ at 0, $\mathfrak{f}_0 + \mathfrak{f}_{e_1}X_1 + \cdots + \mathfrak{f}_{e_n}X_n$, appear with probability one. In terms of the Newton polytope, this condition implies that the tangent cone of the Newton polytope at 0 is a simple cone.

Given a zintzo random polynomial, the complexity estimates that we present in the sequel depend on the product of the following two parameters:

(1) the *subgaussian constant* of $\mathfrak{f}$ which is given by

$$K_{\mathfrak{f}} := \sum\nolimits_{\alpha\in M} K_\alpha, \tag{2.1}$$

where K_α is the subgaussian constant of $\mathfrak{f}_\alpha$, and

(2) the *anti-concentration constants* of $\mathfrak{f}$ which is given by

$$\rho_{\mathfrak{f}} := \sqrt[n+1]{\rho_0\rho_{e_1}\cdots\rho_{e_n}}, \tag{2.2}$$

where ρ_0 is the anti-concentration constant of $\mathfrak{f}_0$ and for each i, ρ_{e_i} is the anti-concentration constant of $\mathfrak{f}_{e_i}$.

We note that the product $K_{\mathfrak{f}}\rho_{\mathfrak{f}}$ that will appear in our estimates is invariant under multiplication of $\mathfrak{f}$ by non-zero scalars. It also satisfies the following inequality, which we will prove in Section 5.

Proposition 2.4. *Let $\mathfrak{f}$ be a zintzo random polynomial supported on M. Then $K_{\mathfrak{f}}\rho_{\mathfrak{f}} > (n+1)/4 \geq 1/2$.*

Let $M \subseteq \mathbb{N}^n$ be such that it contains $0, e_1, \ldots, e_n$. The following are the two most important examples of our randomness model.

- G A *Gaussian polynomial supported on M* is a zintzo random polynomial $\mathfrak{f}$ supported on M, the coefficients of which are i.i.d. Gaussian random variables. In this case, it holds that $\rho_{\mathfrak{f}} = 1/\sqrt{2\pi}$ and $K_{\mathfrak{f}} \leq |M|$.
- U A *uniform random polynomial supported on M* is a zintzo random polynomial $\mathfrak{f}$ supported on M, the coefficients of which are i.i.d. uniform random variables on $[-1,1]$. In this case, $\rho_{\mathfrak{f}} = 1/2$ and $K_{\mathfrak{f}} \leq |M|$.

An important feature of our randomness model is that it includes the smoothed analysis inside the probabilistic analysis. We recall that the smoothed case, as introduced by Spielman and Teng [26], considers a fixed polynomial on which we perform a random perturbation. Recall that $\|f\|_1 := \sum_\alpha |f_\alpha|$. The presence of the norm in the following statement is to make the random perturbation of size proportional to the size of the polynomial.

Proposition 2.5. *Let $\mathfrak{f}$ be a zintzo random polynomial supported on M, $f \in \mathcal{P}_{n,d}$ a polynomial supported on M, and $\sigma > 0$. Then, $\mathfrak{f}_\sigma := f + \sigma\|f\|_1\mathfrak{f}$ is a zintzo random polynomial supported on M such that $K_{\mathfrak{f}_\sigma} \leq \|f\|_1(1+\sigma K_{\mathfrak{f}})$ and $\rho_{\mathfrak{f}_\sigma} \leq \rho_{\mathfrak{f}}/(\sigma\|f\|_1)$. In particular,*

$$K_{\mathfrak{f}_\sigma}\rho_{\mathfrak{f}_\sigma} = (K_{\mathfrak{f}} + 1/\sigma)\rho_{\mathfrak{f}}.$$

The proof of the proposition appears in Section 5. Note that

$$\lim_{\sigma\to 0} K_{\mathfrak{f}_\sigma}\rho_{\mathfrak{f}_\sigma} = \infty \quad \text{and} \quad \lim_{\sigma\to\infty} K_{\mathfrak{f}_\sigma}\rho_{\mathfrak{f}_\sigma} = K_{\mathfrak{f}}\rho_{\mathfrak{f}},$$

so that we have that the smoothed case recovers both the worst and the average case. In particular, the worst case emerges as the perturbation becomes zero and the average case as the perturbation becomes of infinite magnitude.

Remark 2.6. We use the term subgaussian constant instead of the ψ_2-norm since our choice may not agree with the usual definition of ψ_2-norm which is

$$\|X\|_{\psi_2} := \inf\{t > 0 \mid \mathbb{E}\exp(-X^2/t^2) \leq 2\},$$

see [28, Definition 2.5.6]. However, one can see that what we call subgaussian constant is always bounded from above by the ψ_2-norm.

Remark 2.7. Our methods also apply if we replace the subgaussian property by the more general subexponential property [28, 2.7] or by probability distributions having stronger tail decays (see [28, Exercise 2.7.3]).

Remark 2.8. Saying that X has the anti-concentration property with anti-concentration constant ρ is the same as saying that X has a density (with respect the Lebesgue measure) bounded almost everywhere by ρ. See [25] for more details on this.

Remark 2.9. By Proposition 2.5, any probabilistic average complexity analysis includes the smoothed complexity analysis. Because of this, we will only provide complexity estimates in the average case.

2.2 Complexity results

Our main complexity result is the following probabilistic complexity analysis for the subdivision routine of the Plantinga-Vegter, PV-Subdivsion, that we prove in Section 6.

Theorem 2.10. *Let $\mathfrak{f} \in \mathcal{P}_{n,d}$ be a zintzo random polynomial supported on M. The average number of boxes of the final subdivision of PV-Subdivsion using the interval approximations* (6.1) *and* (6.2) *on input $\mathfrak{f}$ is at most*

$$n^{\frac{3}{2}} d^{2n} |M| \left(80\sqrt{n(n+1)}K_{\mathfrak{f}}\rho_{\mathfrak{f}}\right)^{n+1}.$$

Let us particularize the result for the two main examples of zintzo random polynomials.

Corollary 2.11. *Let $\mathfrak{f} \in \mathcal{P}_{n,d}$ be a random polynomial supported on M. The average number of boxes of the final subdivision of PV-Subdivsion using the interval approximations* (6.1) *and* (6.2) *on input $\mathfrak{f}$ is at most*

$$n^{\frac{3}{2}} \left(40\sqrt{n(n+1)}\right)^{n+1} d^{2n}|M|^{n+2}$$

if $\mathfrak{f}$ is Gaussian or uniform.

We observe that in all these results the bound is polynomial in the degree, as in [7], providing further theoretical justification of the practical success of the Plantinga-Vegter algorithm. However, unlike the estimates in [7], the above results justify the success of the Plantinga-Vegter algorithm for sparse random polynomials. As mentioned in the introduction, this is one of the first such probabilistic complexity estimates in numerical algebraic geometry.

3 A NORM TO WORK IN THE CUBE

To work in the cube I^n, we will use the ∞-norm which is

$$\|x\|_\infty := \max_i |x_i|,$$

for $x \in \mathbb{R}^n$. Motivated by duality, we will consider the following norm on $\mathcal{P}_{n,d}$, the space of affine polynomials of degree at most d in n variables:

$$\|f\|_1 := \sum_\alpha |f_\alpha|, \tag{3.1}$$

for $f := \sum_{|\alpha|\leq d} f_\alpha X^\alpha \in \mathcal{P}_{n,d}$.

The motivation to choose the 1-norm emanates from the following proposition which shows that we can control the evaluation of f at $x \in I^n$, that is $f(x)$, using 1-norm for f.

Proposition 3.1. *Let $f \in \mathcal{P}_{n,d}$ and $x \in I^n$. Then $|f(x)| \leq \|f\|_1$.*

Proof. It holds $|f(x)| = |\sum_\alpha f_\alpha x^\alpha| \leq \sum_\alpha |f_\alpha| \|x\|_\infty^{|\alpha|} \leq \|f\|_1$; as $x \in I^n$ implies that $\|x\|_\infty \leq 1$. □

Remark 3.2. A reader might wonder why we do not choose another norm. For example, if we choose $\|f\|_2 := \sqrt{\sum_\alpha |f_\alpha|^2}$, then we can prove that for all $x \in I^n$, it holds $|f(x)| \leq \sqrt{N}\|f\|_2$. Unfortunately, the inequality depends on $\sqrt{N}$. This $\sqrt{N}$ factor will spread throughout the analysis and it will take away any gain we obtain from choosing the Euclidean norm. Because of this, we pick the norm that makes our analysis as simple as possible, that is the 1-norm.

An important feature of the 1-norm is that, using the norm of a polynomial, we can control the norm of its derivative. Proposition 3.4 and its Corollary 3.5 quantify this feature.

Remark 3.3. We use the convention of writing ∇f to refer to the formal gradient vector, whose entries are the formal partial derivatives of f. We write $\nabla_x f$ to refer to the gradient vector of f at x, whose entries are the partial derivatives of f evaluated at x. In this way, for $v \in \mathbb{R}^n$, $\langle \nabla f, v\rangle = \sum_i v_i \partial_i f$ is a polynomial, while $\langle \nabla_x f, v\rangle = \sum_i v_i \partial_i f(x)$ is a number.

Proposition 3.4. *Let $f \in \mathcal{P}_{n,d}$, $x \in I^n$, and $v \in \mathbb{R}^n$. Then, it holds $\|\langle \nabla f, v\rangle\|_1 \leq d\|f\|_1\|v\|_\infty$.*

Proof. We have $d\|f\|_1\|v\|_\infty = \sum_\alpha d|f_\alpha|\|v\|_\infty$ and $\|\langle \nabla f, v\rangle\|_1 \leq \sum_\alpha |f_\alpha|\|\langle \nabla(X^\alpha, v\rangle\|_1$. Therefore, it is enough to prove the claim for X^α. But then $\langle \nabla X^\alpha, v\rangle = \sum_{i=1}^n \alpha_i v_i X^\alpha / X_i$ and so $\|\langle \nabla X^\alpha, v\rangle\|_1 \leq \left(\sum_{i=1}^n \alpha_i\right)\|v\|_\infty \leq d\|v\|_\infty$. □

Corollary 3.5. *The map $\hat{f} : I^n \to \mathbb{R}$, given by $x \mapsto \hat{f}(x) = f(x)/\|f\|_1$, is d-Lipschitz with respect the ∞-norm.*

Proof. By the fundamental theorem of calculus, $|f(x) - f(y)| \leq \int_0^1 |\langle \nabla_{x+t(x-y)} f, x - y\rangle|\, dt$. Now, by Proposition 3.1, the integrand is bounded from above by $d\|f\|_1\|x - y\|_\infty$. Hence $|f(x) - f(y)| \leq d\|f\|_1\|x - y\|_\infty$, as desired. □

Recall that, by duality, it is natural to measure the gradient of f with the 1-norm, which, for $y \in \mathbb{R}^n$ is

$$\|y\|_1 := \sum_{i=1}^n |y_i|.$$

This is so, because this norm is the optimal norm satisfying the condition that for all $x, y \in \mathbb{R}^n$,

$$\langle y, x\rangle \leq \|y\|_1\|x\|_\infty.$$

This motivates the choice of norms in corollary below.

Corollary 3.6. *The map $\widehat{\nabla f} : I^n \to \mathbb{R}$, given by $x \mapsto \widehat{\nabla f}(x) := \nabla_x f/(d\|f\|_1)$, is $(d-1)$-Lipschitz with respect the ∞-norm in the domain and the 1-norm on the codomain.*

Proof. By Proposition 3.4 and Corollary 3.5, the map $x \mapsto \langle \nabla_x f, v\rangle/(d\|f\|_1\|v\|_\infty)$ is $(d-1)$-Lipschitz with respect the ∞-norm. Hence for all $v \in \mathbb{R}^n \setminus 0$, it holds

$$\frac{1}{\|v\|_\infty}\left|\left\langle \frac{\nabla_x f}{d\|f\|_1} - \frac{\nabla_y f}{d\|f\|_1}, v\right\rangle\right| \leq (d-1)\|x - y\|_\infty.$$

If we maximize the left hand side, then we obtain the 1-norm (as it is the dual norm of the ∞-norm) and so

$$\left\|\frac{\nabla_x f}{d\|f\|_1} - \frac{\nabla_y f}{d\|f\|_1}\right\|_1 \leq (d-1)\|x - y\|_\infty,$$

which concludes the proof. □

4 CONDITION AND ITS PROPERTIES

The following definition adapts the real local condition number [3, Chapter 19] to our setting.

Definition 4.1. Let $f \in \mathcal{P}_{n,d}$ and $x \in I^n$, the *local condition number of f at x* is the quantity

$$\mathtt{C}(f, x) := \frac{\|f\|_1}{\max\left\{|f(x)|, \frac{1}{d}\|\nabla_x f\|_1\right\}}.$$

Remark 4.2. We note that $\mathtt{C}(f, x)$ is infinity only when f has a singular zero at x. In all the other cases, it is finite and it measures how close is f to having a singularity at x.

Following [27, $2^{\S 2}$], a condition number should satisfy the following properties: regularity inequality, the 1st and the 2nd Lipschitz property, and the Higher Derivative Estimate. These properties are the ones that we usually need to bound the various quantities when we analyze algorithms in real numerical algebraic geometry.

Proposition 4.3 (Regularity inequality). *Let $f \in \mathcal{P}_{n,d}$ and $x \in I^n$. Then,*

$$\textit{either } |f(x)|/\|f\|_1 \geq 1/\mathtt{C}(f, x) \textit{ or } \quad \|\nabla_x f\|_1/(d\|f\|_1) \geq 1/\mathtt{C}(f, x).$$

Proof. This follows from the observation that $1/\mathtt{C}(f, x)$ is the maximum of $|f(x)|/\|f\|_1$ and $\|\nabla_x f\|_1/(d\|f\|_1)$. □

Proposition 4.4 (1st Lipschitz property). *The map $\mathcal{P}_{n,d} \ni f \mapsto \|f\|_1/\mathtt{C}(f, x)$ is 1-Lipschitz.*

Proof. If we apply the reverse triangle inequality several times, we get

$$\begin{aligned}
&|\|f\|_1/\mathtt{C}(f, x) - \|g\|_1/\mathtt{C}(g, x)| \\
&\leq |\max\{|f(x)| - |g(x)|, \|\nabla_x f\|_1/d - \|\nabla_x g\|_1/d\}| \\
&\leq |\max\{|f(x) - g(x)|, \|\nabla_x f - \nabla_x g\|_1/d\}| \\
&\leq |\max\{|(f-g)(x)|, \|\nabla_x (f-g)\|_1/d\}|\,.
\end{aligned}$$

Finally, Propositions 3.1 and 3.4 conclude the proof. □

Let $\Sigma_x \leq \mathcal{P}_{n,d}$ be the subspace of polynomials that are singular at 0, that is

$$\Sigma_x := \{g \in \mathcal{P}_{n,d} \mid g(x) = 0,\ \nabla_x g = 0\}.$$

We cannot prove a Condition Number Theorem where the condition number is (the inverse of) the distance to the discriminantal variety. However, bound the condition number, in both directions, with this distance.

Corollary 4.5 (Condition Number Theorem). *For all $f \in \mathcal{P}_{n,d}$ and $x \in I^n$,*

$$\|f\|_1/\mathrm{dist}_1(f, \Sigma_x) \leq \mathtt{C}(f, x) \leq 2d\,\|f\|_1/\mathrm{dist}_1(f, \Sigma_x)$$

where dist_1 is the distance induced by the 1-norm.

Proof. The left hand side follows from Proposition 4.4. For the right hand side, consider the polynomial

$$g := f - f(x) - \textstyle\sum_{i=1}^n \partial_i f(x) X_i.$$

It is clear that $g \in \Sigma_x$ and that $\|f - g\|_1 \leq |f(x)| + \|\nabla_x f\|_1$. Hence $\mathrm{dist}_1(f, \Sigma_x) \leq \|f - g\|_1 \leq 2d \max\{|f(x)|, \|\nabla_x f\|_1/d\} = 2d\|f\|_1/\mathtt{C}(f, x)$, as desired. □

Proposition 4.6 (2nd Lipschitz property). *The map $I^n \ni x \mapsto 1/\mathtt{C}(f, x)$ is d-Lipschitz.*

Proof. Without loss of generality, we can assume that $\|f\|_1 = 1$. The proof is analogous, mutatis mutandis, to the proof of Proposition 4.4. By using the reverse triangular inequality, we have

$$\left|\frac{1}{\mathtt{C}(f, x)} - \frac{1}{\mathtt{C}(f, y)}\right| \leq \max\left\{|f(x) - f(y)|, \frac{1}{d}\|\nabla_x f - \nabla_y f\|\right\}.$$

Now, Corollaries 3.5 and 3.6 conclude the proof. □

We recall that Smale's gamma, γ, is the invariant given by

$$\gamma(f,x) := \sup_{k\geq 2} \left\| \frac{1}{k!} \mathrm{D}_x f^\dagger \, \mathrm{D}_x^k f \right\|^{\frac{1}{k-1}} = \sup_{k\geq 2} \left(\frac{1}{\|\nabla_x f\|_2^2} \left\| \frac{1}{k!} (\nabla_x f)^* \, \mathrm{D}_x^k f \right\| \right)^{\frac{1}{k-1}},$$

where the $\dagger$ is the pseudoinverse, and the norm the operator norm with respect the Euclidean norm. We also notice that the second equality follows from computing the pseudoinverse for a covector. The following proposition serves the purpose of the Higher Derivative Estimate [3, Prop. 16.45] in our setting.

Proposition 4.7 (Higher Derivative Estimate). *Let $x \in I^n$ be such that $\mathtt{C}(f,x)\hat{f}(x) < 1$. Then*

$$\gamma(f,x) \leq \frac{1}{2}(d-1)\sqrt{n}\,\mathtt{C}(f,x).$$

Proof. Let $\mathrm{D}_X^k f(v_1,\dots,v_k)$ stand for the polynomial obtained by evaluating the formal kth derivative of f evaluated at $v_1, \dots, v_k \in \mathbb{R}^n$. Then, by Proposition 3.4 and induction, we have

$$\left\| \frac{1}{k!} \mathrm{D}_X f(v_1,\dots,v_k) \right\|_1 \leq \binom{d}{k} \|f\|_1 \|v_1\|_\infty \cdots \|v_k\|_\infty.$$

Now, by the above inequality, $\|v\|_\infty \leq \|v\|_2$ and submultiplicativity of operator norms, we have that

$$\frac{1}{\|\nabla_x f\|_2^2} \left\| \frac{1}{k!} (\nabla_x f)^* \, \mathrm{D}_x^k f \right\| \leq \frac{\|f\|_1}{\|\nabla_x f\|_2} \binom{d}{k}.$$

Since $\|\nabla_x f\|_2 \geq \|\nabla_x f\|_1/\sqrt{n}$, we deduce that can bound the previous inequality by

$$\binom{d}{k}\sqrt{n}\frac{\|f\|_1}{\|\nabla_x f\|_1} \leq \frac{1}{d}\binom{d}{k}\sqrt{n}\,\mathtt{C}(f,x),$$

where the inequality follows from the Regularity Inequality (Proposition 4.3). Finally, we observe that $\frac{1}{d}\binom{d}{k} \leq (d-1)^{k-1}/2^{k-1}$; then, the claim follows by taking the $(k-1)$th root and the supremum. □

5 PROBABILITY ESTIMATES

We refine the techniques of [7] to obtain explicit constants in the bounds and to deal with a restricted class of sparse polynomials.

5.1 Probabilistic toolbox

Our probabilistic toolbox should control, on the one hand, the norm and, on the other hand, the size of the projection. For the former we need a variant of the Hoeffding inequality, and for latter we need a bound on small ball probabilities.

Proposition 5.1. *Let $\mathfrak{x} \in \mathbb{R}^M$ be a random vector such that for each $\alpha \in M$, $\mathfrak{x}_\alpha$ is subgaussian with subgaaussian constant K_α. Then for all $t \geq \sum_\alpha K_\alpha$, it have*

$$\mathbb{P}(\|\mathfrak{x}\|_1 \geq t) \leq 2|M| \exp\left(-t^2 / \left(\sum_{\alpha\in M} K_\alpha \right)^2 \right).$$

Proof. We have that

$$\begin{aligned}\mathbb{P}\left(\textstyle\sum_{\alpha\in M} |\mathfrak{x}_\alpha| \geq t\right) &= \mathbb{P}\left(\textstyle\sum_{\alpha\in M} |\mathfrak{x}_\alpha| \geq \sum_{\alpha\in M} K_\alpha t/(\sum_{\alpha\in M} K_\alpha)\right) \\ &\leq \mathbb{P}\left(\exists \alpha \in M \mid |\mathfrak{x}_\alpha| \geq K_\alpha t/(\textstyle\sum_{\alpha\in M} K_\alpha)\right) \\ &\leq |M| \max_{\alpha\in M} \mathbb{P}\left(|\mathfrak{x}_\alpha| \geq K_\alpha t/(\textstyle\sum_{\alpha\in M} K_\alpha)\right) \\ &\leq 2|M| \exp\left(-t^2/(\textstyle\sum_{\alpha\in M} K_\alpha)^2\right),\end{aligned}$$

where the first inequality follows from the implication bound –note that for $x, y \in \mathbb{R}^n_+$, we have that if $\sum_{i=1}^n x_i \geq \sum_{i=1}^n y_i$, then for some i, $x_i \geq y_i$, as otherwise the first claim would be false– the second one from the union bound, and the third one by hypothesis. □

Proposition 5.2. *Let $A \in \mathbb{R}^{k\times N}$ be a surjective linear map and $\mathfrak{x} \in \mathbb{R}^N$ be a random vector such that the $\mathfrak{x}_i$'s are independent random variables with densities (with respect the Lebesgue measure) bounded almost everywhere by ρ. Then, for all measurable $U \subseteq \mathbb{R}^k$,*

$$\mathbb{P}(A\mathfrak{x} \in U) \leq \mathrm{vol}(U) \left(\sqrt{2}\rho\right)^k / \sqrt{\det AA^*}.$$

Proof. Using SVD, write $A = QSP$ where, $P \in \mathbb{R}^{k\times N}$ is an orthogonal projection, S a diagonal matrix containing the singular values of A, and Q an orthogonal matrix.

By [25, Theorem 1.1], see also [18, Theorem 1.1] for the explicit constant, we have that $P\mathfrak{x} \in \mathbb{R}^k$ is a random vector with density bounded, almost everywhere, by $(\sqrt{2}\rho)^k$. Hence

$$\mathbb{P}(A\mathfrak{x} \in U) = \mathbb{P}(P\mathfrak{x} \in (QS)^{-1}U) \leq \mathrm{vol}\left((QS)^{-1}U\right)(\sqrt{2}\rho)^k.$$

This suffices to conclude the proof, since we have $\mathrm{vol}\left((QS)^{-1}U\right) = \mathrm{vol}(U)/\det(QS)$ and $\det(QS) = \sqrt{\det AA^*}$. □

5.2 Condition of zintzo random polynomials

We apply our probabilistic toolbox to zintzo random polynomials.

Theorem 5.3. *Let $\mathfrak{f} \in \mathcal{P}_{n,d}$ a zintzo random polynomial supported on M. Then for all $t \geq e$,*

$$\mathbb{P}(\mathtt{C}(\mathfrak{f},x) \geq t) \leq \sqrt{n} d^n |M| \left(8K_{\mathfrak{f}}\rho_{\mathfrak{f}}\right)^{n+1} \frac{\ln^{\frac{n+1}{2}} t}{t^{n+1}}.$$

Lemma 5.4. *Let $M \subseteq \mathbb{N}^n$ as in Definition 2.1 and $\mathcal{P}_{n,d}(M)$ the set of polynomials in $\mathcal{P}_{n,d}$ supported on M. Let $R_x : \mathcal{P}_{n,d}(M) \to \mathbb{R}^{n+1}$ be the linear map given by*

$$R_x : f \mapsto \begin{pmatrix} f(x) & \frac{1}{d}\partial_1 f(x) & \cdots & \frac{1}{d}\partial_n f(x) \end{pmatrix}^*,$$

and $S : \mathcal{P}_{n,d}(M) \to \mathcal{P}_{n,d}(M)$ be the linear map given by

$$S : f = \sum_{\alpha\in M} f_\alpha X^\alpha \mapsto \sum_{\alpha\in M} \rho_\alpha f_\alpha X^\alpha,$$

where $\rho \in \mathbb{R}^M_+$. Then for $\tilde{R}_x := R_x S^{-1}$ we have that

$$\sqrt{\det \tilde{R}_x \tilde{R}_x^*} \geq \frac{1}{d^n \rho_0 \rho_{e_1} \cdots \rho_{e_n}},$$

with respect to coordinates induced by the standard monomial basis.

Proof of Theorem 5.3. We write $\mathtt{C}(\mathfrak{f},x) = \|f\|_1/\|R_x\mathfrak{f}\|$, where R_x is as in Lemma 5.4 and the norm $\|\cdot\|$ in the denominator is

given by $\|y\| = \max\{|y_1|, |y_2| + \cdots + |y_{n+1}|\}$. By the union bound, we have that for $u, s > 0$, it holds

$$\mathbb{P}(\mathtt{C}(\mathtt{f}, x) \geq t) \leq \mathbb{P}(\|\mathtt{f}\| \geq u) + \mathbb{P}(\|A_x \mathtt{f}\| \leq u/t). \tag{5.1}$$

By Propositions 5.1, we have that for $u \geq K_{\mathtt{f}}$,

$$\mathbb{P}(\|\mathtt{f}\| \geq u) \leq 2|M| \exp\left(-u^2/K_{\mathtt{f}}^2\right). \tag{5.2}$$

Let $S : \mathcal{P}_{n,d}(M) \to \mathcal{P}_{n,d}(M)$ be as in Lemma 5.4 with ρ_α the anti-concentration constant of $\mathtt{f}_\alpha$. Then, we have that $S\mathtt{f}$ has independent random coefficients with densities bounded (almost everywhere) by 1 and so we can apply to it to the Proposition 5.2. We do so with the help of Lemma 5.4, so that we obtain

$$\mathbb{P}(\|R_x \mathtt{f}\| \leq u/t) = \mathbb{P}(\|\tilde{R}_x(S\mathtt{f})\| \leq u/t) \leq \frac{2^{n+1}}{n!} d^n (\sqrt{2}\rho_{\mathtt{f}} u/t)^{n+1}, \tag{5.3}$$

where $\tilde{R}_x$ is as in Lemma 5.4.

Combining (5.1), (5.2), and (5.3) with $u = K_{\mathtt{f}}\sqrt{(n+1)\ln t}$, we get

$$\mathbb{P}(\mathtt{C}(\mathtt{f}, x) \geq t) \leq \frac{2|M|}{t^{n+1}} + \frac{2^{n+1}}{n!} d^n (\sqrt{2} K_{\mathtt{f}} \rho_{\mathtt{f}} (n+1))^{n+1} \frac{\ln^{\frac{n+1}{2}} t}{t^{n+1}}.$$

By Stirling's formula,

$$(n+1)^{n+1}/n! \leq \sqrt{n} e^n (1 + 1/n)^{n+1}/\sqrt{2\pi} \leq \sqrt{n} e^{n+1},$$

and so the desired claim follows for $t \geq e$, by Proposition 2.4. □

Proof of Lemma 5.4. The maximal minor of A_x is given by

$$\begin{pmatrix} 1 & x^* \\ 0 & \frac{1}{d}\mathbb{I} \end{pmatrix}.$$

This is precisely the minor associated to the subset $\{1, X_1, \ldots, X_n\}$ of the standard monomial basis of $\mathcal{P}_{n,d}(M)$. Note that at this point we require the assumption that $0, e_1, \ldots, e_n \in M$.

By the Cauchy-Binet identity, $\sqrt{\det A_x A_x^*}$ is lower-bounded by the absolute value of the determinant of the given maximal minor. Hence the lemma follows. □

Proof of Proposition 2.4. Using the positivity of the subgaussian constants, K_α, of the coefficients of the zintzo polynomial $\mathtt{f}$ and the arithmetic-geometric inequality,

$$K_{\mathtt{f}}\rho_{\mathtt{f}} \geq (n+1)\sqrt[n+1]{(K_0\rho_0)(K_{e_1}\rho_{e_1})\cdots(K_{e_n}\rho_{e_n})}.$$

Hence, it suffices to show that for a random variable with X with subgaussian constant K and anti-concentration constant ρ, $K\rho \geq 1/4$. Now, by definition,

$$3K\rho \geq \mathbb{P}(|X| \leq 1.5K) = 1 - \mathbb{P}(|X| > 1.5K) \geq 1 - \exp(-2.25).$$

Calculating we get $K\rho \geq 1/4$, as desired. □

Corollary 5.5. *Let $\mathtt{f} \in \mathcal{P}_{n,d}$ be a zintzo random polynomial supported on M. Then,*

$$\mathbb{E}_{\mathtt{f}}\mathbb{E}_{\mathtt{f}\in I^n} \mathtt{C}(f, x)^n \leq 2n^2 d^n |M| \left(10\sqrt{n+1} K_{\mathtt{f}}\rho_{\mathtt{f}}\right)^{n+1}.$$

Proof. By the Fubini-Tonelli theorem, we have

$$\mathbb{E}_{\mathtt{f}}\mathbb{E}_{\mathtt{f}\in I^n} \mathtt{C}(f, x)^n = \mathbb{E}_{\mathtt{f}\in I^n}\mathbb{E}_{\mathtt{f}} \mathtt{C}(f, x)^n,$$

so it is enough to compute $\mathbb{E}_{\mathtt{f}} \mathtt{C}(f, x)^n = \int_1^\infty \mathbb{P}(\mathtt{C}(\mathtt{f}, x)^n \geq t)$. The latter, by Theorem 5.3, is bounded from above by

$$e^n \sqrt{n} d^n |M| \left(\frac{8K_{\mathtt{f}}\rho_{\mathtt{f}}}{\sqrt{n}}\right)^{n+1} \int_1^\infty \frac{\ln^{\frac{n+1}{2}} t}{t^{1+\frac{1}{n}}} \, \mathrm{d}t.$$

After straightforward calculations, we obtain

$$\int_1^\infty \frac{\ln^{\frac{n+1}{2}} t}{t^{1+\frac{1}{n}}} \, \mathrm{d}t = n^{\frac{n+3}{2}} \Gamma\left(\frac{n+3}{2}\right) \leq e\sqrt{\pi} n^{\frac{n+4}{2}} \left(\frac{n+1}{2e}\right)^{\frac{n+1}{2}},$$

where Γ is Euler's Gamma function and the second inequality follows from Striling's approximation. Hence, the bound follows. □

We can also bound the *global condition number*, that is

$$\mathtt{C}(f) := \max\{\mathtt{C}(f, x) \mid x \in I^n\}. \tag{5.4}$$

Corollary 5.6. *Let $\mathtt{f} \in \mathcal{P}_{n,d}$ be a zintzo random polynomial supported on M. Then, for all $t > 2e$,*

$$\mathbb{P}(\mathtt{C}(\mathtt{f}) \geq t) \leq \frac{1}{4}\sqrt{n} d^{2n} |M| \left(64 K_{\mathtt{f}}\rho_{\mathtt{f}}\right)^{n+1} \frac{\ln^{\frac{n+1}{2}} t}{t}.$$

Proof. The idea is to use an efficient ε-net of I^n and the 2nd Lipschitz property to turn our local estimates into global ones, as is done in [27, Theorem 1§2 19]. Recall, that an ε-net of I^n (with respect to the ∞-norm) is a finite subset $\mathcal{G} \subseteq I^n$ such that, for all $y \in I^n$, $\mathrm{dist}_\infty(y, \mathcal{G}) \leq \varepsilon$.

Note that for every $\varepsilon > 0$, we have an ε-net $\mathcal{G}_\varepsilon \subseteq I^n$ of size $\leq 2^n \varepsilon^{-n}$. To construct it, we take the uniform grid in the cube.

Now, we notice that if $\mathtt{C}(\mathtt{f}) \geq t$, then

$$\max\{\mathtt{C}(\mathtt{f}, x) \mid x \in \mathcal{G}_{1/(2dt)}\} \geq t/2$$

by the 2nd Lipschitz property (Proposition 4.6). In this way, by the implication and the union bound, we obtain

$$\mathbb{P}(\mathtt{C}(\mathtt{f}) \geq t) \leq \left|\mathcal{G}_{1/(2dt)}\right| \max\{\mathbb{P}(\mathtt{C}(\mathtt{f}, x) \geq t/2) \mid x \in I^n\}.$$

By Theorem 5.3 and the bound on $\left|\mathcal{G}_{1/(2dt)}\right|$, we conclude. □

Now we have all the tools to prove Proposition 2.5 which shows that the smoothed case is included in the above average cases.

Proof of Proposition 2.5. It is enough to show that for $x, s \in \mathbb{R}$ and a random variable $\mathfrak{x}$ with subgaussian constant K and anti-concentration constant ρ, $x + s\mathfrak{x}$ is a random variable with subgaussian constant $\leq |x| + sK$ and anti-concentration constant $\leq \rho/s$. We note that the latter follows directly from the definition, so we only prove the former.

Now, for all $t \geq |x| + sK$,

$$\mathbb{P}(|x + s\mathfrak{x}| \geq t) \leq \mathbb{P}(|\mathfrak{x}| \geq (t - |x|)/s) \leq 2\exp(-(t - |x|)^2/(sK)^2).$$

We can easily check that $t \geq |x| + sK$ implies $(t - |x|)/(sK) \geq t/(|x| + sK)$. Hence, the claim follows. □

6 PLANTINGA-VEGTER ALGORITHM

The Plantinga-Vegter algorithm [23] is a subdivision-based algorithm that computes an isotopically correct approximation of the zeros of a univariate polynomial in an interval, of a curve in the plane, or of a surface in 3-dimensional space. Following [6] and [7], we will focus on the subdivision procedure, which is extended for an arbitrary number of variables, and bound the complexity by bounding the number of boxes that the algorithm produces. We

Algorithm 1: PV-Subdivsion

Input : $f \in \mathcal{P}_{n,d}$ which is non-singular in I^n
Output : A subdivision $\mathcal{S}$ of I^n into boxes such that for all $B \in \mathcal{S}$, $C_f(B)$ holds

$\mathcal{S}_0 \leftarrow \{I^n\}, \mathcal{S} \leftarrow \emptyset$;
while $\mathcal{S}_0 \neq \emptyset$ **do**
  Take $B \in \mathcal{S}_0$;
  if $C_f(B)$ *holds* **then**
    $\mathcal{S} \leftarrow \mathcal{S} \cup \{B\}, \mathcal{S}_0 \leftarrow \mathcal{S}_0 \setminus \{B\}$;
  else
    $\mathcal{S}_0 \leftarrow \mathcal{S}_0 \setminus \{B\} \cup$ StandardSubdivsion(B);
return $\mathcal{S}$;

refer to [6], [7] and [27, 5$^{\S 2}$] for further justification of the approach taken here.

Remark 6.1. Even though we present our results for the unit cube I^n, we note that our tools apply for a cube of arbitrary size (up to the technical assumption on the support). To do so, we need to normalize evaluations appropiately by a power of $\max\{1, \|x\|_\infty\}$ for $\|x\|_\infty > 1$. However, this would obfuscate many of the ideas presented in this paper. Hence, for the sake of simplicity, we analyze Algorithm PV-Subdivsion only in the unit cube.

6.1 PV Algorithm and its interval version

The subdivision routine of the PV algorithm, PV-Subdivsion, relies on subdividing the unit cube I^n until each box B in the subdivision satisfies the condition

$$C_f(B) : \text{ either } 0 \notin f(B) \text{ or } 0 \notin \{\langle \nabla_x f, \nabla_y f\rangle \mid x, y \in B\}.$$

To implement this algorithm one uses interval arithmetic. Recall that an *interval approximation* of a map $g : I^n \to \mathbb{R}^q$ is a map $\square[g] : \mathcal{B}(I^n) \to \mathcal{B}(\mathbb{R}^q)$, where $\mathcal{B}(X)$ is the set of (coordinate) boxes contained in X, such that for all $B \in \mathcal{B}(I^n)$, we have

$$g(B) \subseteq \square[g](B).$$

Using the language of Xu and Yap [29], we will consider only the interval level of the algorithm, leaving the effective version to an extended version of this work.

We note that Corollaries 3.5 and 3.6 establish Lipschitz properties for both f and ∇f, with respect the ∞-norm. This is ideal for constructing interval approximations to implement PV-Subdivsion. In our case, our interval approximations will be:

$$\square[f](B) := f(m(B)) + d\|f\|_1 w(B)/2[-1, 1] \tag{6.1}$$

and

$$\square[\|\nabla f\|_1](B) := \|\nabla_{m(B)} f\|_1 + \sqrt{2n}d(d-1)\|f\|_1 w(B)[-1, 1]. \tag{6.2}$$

For these interval approximations, we can interpret the stopping criterion as follows:

Proposition 6.2. *The condition $C_f(B)$ is implied by the condition*

$$C'_f(B) : \begin{cases} |f(m(B))| & > d\|f\|_1 w(B)/2 \\ \text{or} & \|\nabla_{m(B)} f\|_1 > \sqrt{2n}d(d-1)\|f\|_1 w(B) \end{cases}.$$

Hence, PV-Subdivsion with the interval approximations given in (6.1) *and* (6.2) *is correct if we substitute the condition $C_f(B)$ by*

$$C_f^{\square}(B) : \text{ either } 0 \notin \square[f](B) \text{ or } 0 \notin \square[\|\nabla f\|_1](B).$$

Proof. The statement follows from Corollaries 3.5 and 3.6, [7, Lemma 4.4] and the fact that for $y \in \mathbb{R}^n$, $\|y\|_1/\sqrt{n} \leq \|y\|_2$. □

For now on, the interval version of PV-Subdivsion will be a variant that exploits the interval approximations in (6.1) and (6.2).

6.2 Complexity analysis

As in [6] and [7], our complexity analysis relies on the construction of a local size bound for PV-Subdivsion and the application of the continuous amortization developed by Burr, Krahmer and Yap [4, 5].

We recall the definition of the local size bound and the result that we will exploit in our complexity analysis.

Definition 6.3. A *local size bound* for the interval version of PV-Subdivsion on input f is a function $b_f : I^n \to [0, 1]$ such that for all $x \in \mathbb{R}^n$,

$$b_f(x) \leq \inf\{\text{vol}(B) \mid x \in B \in \mathcal{B}(I^n) \text{ and } C_f^{\square}(B) \text{ false}\}.$$

Theorem 6.4. *[4–6] The number of boxes of the final subdivision of the interval version of PV-Subdivsion on input f is at most*

$$4^n \mathbb{E}_{\mathbf{x} \in I^n}\left(b_f(x)^{-1}\right).$$

Also, the bound is finite if and only if PV-Subdivsion terminates. □

Theorem 6.5. *The function*

$$x \mapsto \left(2d\sqrt{n}\,\mathtt{C}(f, x)\right)^{-n}$$

is a local size bound for PV-Subdivsion on input f.

Proof. Let $x \in B \in \mathcal{B}(I^n)$. Then $\|m(B) - x\|_\infty \leq w(B)/2$ and so, by Corollaries 3.5 and 3.6 and the regularity inequality (Propsoition 4.3), we have that

$$|f(m(B))| > \|f\|_1 \left(\mathtt{C}(f, x)^{-1} - dw(B)/2\right), \tag{6.3}$$

and

$$\|\nabla_{m(B)} f\|_1 > d\|f\|_1 \left(\mathtt{C}(f, x)^{-1} - (d-1)w(B)/2\right). \tag{6.4}$$

Hence, $C_f(B)$ is true as long as, either $\mathtt{C}(f, x)^{-1} \geq dw(B)$, or $\mathtt{C}(f, x)^{-1} > 2\sqrt{n}dw(B)$. The result follows, since $\text{vol}(B) = w(B)^n$. □

Theorem 6.4 and Theorem 6.5 result the following corollary:

Corollary 6.6. *The number of boxes of the final subdivision of the interval version of PV-Subdivsion on input f is at most*

$$8^n n^{\frac{n}{2}} d^n \mathbb{E}_{\mathbf{x} \in I^n} \mathtt{C}(f, \mathbf{x})^n.$$

Theorem 2.10 follows now from Corollaries 5.5 and 6.6.

Remark 6.7. A similar argument as in the proof of [7, Theorem 6.4] shows that we can bound the local size bound of [6] in terms of $1/\mathtt{C}(f, x)^n$. Since the interval approximation of the analyzed version is simpler, requiring a single evaluation, we only analyze the complexity of this.

Remark 6.8. Our tools apply for a cube of arbitrary size (up to the technical assumption on the support). To do so, we need to normalize evaluations by a power of $\max\{1, \|x\|_\infty\}$ for $\|x\|_\infty > 1$. However, this would obfuscate many of the ideas presented. Hence, for the sake of simplicity, we restrict our analysis to the unit cube.

7 CONDITION AND SEPARATION BOUNDS

The following theorem is a variation of a result due to Dedieu [11, Theorem 3.2 and Theorem 5.1]. It relates the condition number with the separation bound, that is the minimum distance between the roots, in the univariate case.

Theorem 7.1. *Let $f \in \mathcal{P}_{1,d}$ be a univariate polynomial and $x \in I$. Then, for any two distinct and non-singular roots, α and $\tilde{\alpha}$, such that $\alpha, \tilde{\alpha} \in B_{\mathbb{C}}(x, 1/(2(d-1)\,\mathsf{C}(f,x)))$,*

$$|\alpha - \tilde{\alpha}| \geq 1/(16(d-1)\,\mathsf{C}(f,x)).$$

Proof. By [12, Théorème 91], the Newton method converges for any point in $B_{\mathbb{C}}(\alpha, 1/(6\gamma(f,\alpha))$, where γ is Smale's gamma. This means that for any two roots α and $\tilde{\alpha}$ of f, we must have

$$|\alpha - \tilde{\alpha}| \geq 1/\max\{3\gamma(f,\alpha), 3\gamma(f,\tilde{\alpha})\}.$$

Now, by [12, Lemme 98], for any $y \in B_{\mathbb{C}}(x, 1/(4\gamma(f,x)))$,

$$\gamma(f,y) \leq 32\gamma(f,x)/3.$$

Hence, for any distinct roots $\alpha, \tilde{\alpha} \in B_{\mathbb{C}}(x, 1/(4\gamma(f,x)))$ that are not singular, and because Smale's gamma is finite at them, we have

$$|\alpha - \tilde{\alpha}| \geq 1/(32\gamma(f,x)).$$

Using the Higher Derivative Estimate (Prop. 4.7) we conclude. □

Recall that the local separation at a root α is given by $\Delta_\alpha := \min_{\beta \in f^{-1}(0)\setminus\{\alpha\}} |\alpha - \beta|$. The following corollary controls the local separation of the roots near an interval I.

Corollary 7.2. *Let $f \in \mathcal{P}_{1,d}$. Then, for every complex $\alpha \in f^{-1}(0)$ such that $\operatorname{dist}(\alpha, I) \leq 1/(3(d-1)\,\mathsf{C}(f))$,*

$$\Delta_\alpha \geq 1/(16(d-1)\,\mathsf{C}(f)).$$

Corollary 7.2 together with Corollary 5.6 allows us to give probabilistic estimates of the separation bound for roots that lie near the unit interval.

Acknowledgements. Both authors are grateful to Alperen Ergür for various discussions and suggestions. The first author is grateful to Evgenia Lagoda for moral support. Both authors are partially supported by ANR JCJC GALOP (ANR-17-CE40-0009), the PGMO grant ALMA, and the PHC GRAPE.

REFERENCES

[1] Diego Armentano and Carlos Beltrán. 2019. The polynomial eigenvalue problem is well conditioned for random inputs. *SIAM J. Matrix Anal. Appl.* 40, 1 (2019), 175–193. https://doi.org/10.1137/17M1139941

[2] Carlos Beltrán and Khazhgali Kozhasov. 2019. The Real Polynomial Eigenvalue Problem is Well Conditioned on the Average. *Foundations of Computational Mathematics* On-line First (2019), 19. https://doi.org/10.1007/s10208-019-09414-2

[3] Peter Bürgisser and Felipe Cucker. 2013. *Condition.* Grundlehren der mathematischen Wissenschaften, Vol. 349. Springer-Verlag, Berlin. https://doi.org/10.1007/978-3-642-38896-5

[4] Michael Burr, Felix Krahmer, and Chee Yap. 2009. Continuous amortization: A non-probabilistic adaptive analysis technique. *Electronic Colloquium on Computational Complexity* 16, Report. No. 136 (Dec. 2009), 22.

[5] Michael A. Burr. 2016. Continuous amortization and extensions: with applications to bisection-based root isolation. *J. Symbolic Comput.* 77 (2016), 78–126. https://doi.org/10.1016/j.jsc.2016.01.007

[6] Michael A. Burr, Shuhong Gao, and Elias P. Tsigaridas. 2017. The complexity of an adaptive subdivision method for approximating real curves. In *ISSAC'17—Proceedings of the 2017 ACM International Symposium on Symbolic and Algebraic Computation.* ACM, New York, 61–68. https://doi.org/10.1145/3087604.3087654

[7] Felipe Cucker, Alperen A. Ergür, and Josué Tonelli-Cueto. 2019. Plantinga-Vegter Algorithm Takes Average Polynomial Time. In *Proceedings of the 2019 on International Symposium on Symbolic and Algebraic Computation (ISSAC '19).* ACM, New York, Beijing, China, 114–121. https://doi.org/10.1145/3326229.3326252

[8] Felipe Cucker, Alperen A. Ergür, and Josué Tonelli-Cueto. 2020. Functional norms, condition numbers and numerical algorithms in algebraic geometry. Manuscript.

[9] Felipe Cucker, Alperen A. Ergür, and Josué Tonelli-Cueto. 2020. On the Complexity of the Plantinga-Vegter Algorithm. arXiv:2004.06879.

[10] Felipe Cucker, Teresa Krick, Gregorio Malajovich, and Mario Wschebor. 2008. A numerical algorithm for zero counting. I: Complexity and accuracy. *J. Complexity* 24 (2008), 582–605. https://doi.org/10.1016/j.jco.2008.03.001

[11] Jean-Pierre Dedieu. 1997. Estimations for the Separation Number of a Polynomial System. *Journal of Symbolic Computation* 24, 6 (Dec. 1997), 683–693.

[12] Jean-Pierre Dedieu. 2006. *Points fixes, zéros et la méthode de Newton.* Mathématiques & Applications (Berlin) [Mathematics & Applications], Vol. 54. Springer, Berlin. xii+196 pages.

[13] Alperen A. Ergür, Grigoris Paouris, and J. Maurice Rojas. 2018. Probabilistic Condition Number Estimates for Real Polynomial Systems II: Structure and Smoothed Analysis. (Sept. 2018), 22 pages. arXiv:1809.03626.

[14] Alperen A. Ergür, Grigoris Paouris, and J. Maurice Rojas. 2019. Probabilistic Condition Number Estimates for Real Polynomial Systems I: A Broader Family of Distributions. *Found. Comput. Math.* 19, 1 (2019), 131–157. https://doi.org/10.1007/s10208-018-9380-5

[15] Gorav Jindal and Michael Sagraloff. 2017. Efficiently computing real roots of sparse polynomials. In *ISSAC'17—Proceedings of the 2017 ACM International Symposium on Symbolic and Algebraic Computation.* ACM, New York, 229–236. https://doi.org/10.1145/3087604.3087652

[16] Askold G. Khovanskiĭ. 1991. *Fewnomials.* Translations of Mathematical Monographs, Vol. 88. American Mathematical Society, Providence, RI. viii+139 pages. Trans. from the Russian by S. Zdravkovska.

[17] Pierre Lairez. 2017. A deterministic algorithm to compute approximate roots of polynomial systems in polynomial average time. *Found. Comput. Math.* 17, 5 (2017), 1265–1292. https://doi.org/10.1007/s10208-016-9319-7

[18] Galyna Livshyts, Grigoris Paouris, and Peter Pivovarov. 2016. On sharp bounds for marginal densities of product measures. *Israel Journal of Mathematics* 216, 2 (2016), 877–889. https://doi.org/10.1007/s11856-016-1431-5

[19] Gregorio Malajovich. 2019. Complexity of sparse polynomial solving: homotopy on toric varieties and the condition metric. *Found. Comput. Math.* 19, 1 (2019), 1–53. https://doi.org/10.1007/s10208-018-9375-2

[20] Gregorio Malajovich. 2020. Complexity of Sparse Polynomial Solving 2: Renormalization. (May 2020), 84 pages. arXiv:2005.01223.

[21] Gregorio Malajovich and J. Maurice Rojas. 2002. Polynomial systems and the momentum map. In *Foundations of computational mathematics (Hong Kong, 2000).* World Sci. Publ., River Edge, NJ, 251–266.

[22] Gregorio Malajovich and J. Maurice Rojas. 2004. High probability analysis of the condition number of sparse polynomial systems. *Theoret. Comput. Sci.* 315, 2-3 (2004), 524–555. https://doi.org/10.1016/j.tcs.2004.01.006

[23] Simon Plantinga and Gert Vegter. 2004. Isotopic Approximation of Implicit Curves and Surfaces. In *Proceedings of the 2004 Eurographics/ACM SIGGRAPH Symposium on Geometry Processing (SGP '04).* ACM, New York, NY, USA, 245–254. https://doi.org/10.1145/1057432.1057465

[24] J. Renegar. 1987. On the efficiency of Newton's method in approximating all zeros of a system of complex polynomials. *Math. Oper. Res.* 12, 1 (1987), 121–148. https://doi.org/10.1287/moor.12.1.121

[25] Mark Rudelson and Roman Vershynin. 2015. Small ball probabilities for linear images of high-dimensional distributions. *Int. Math. Res. Not. IMRN* 19 (2015), 9594–9617. https://doi.org/10.1093/imrn/rnu243

[26] Daniel A. Spielman and Shang-Hua Teng. 2002. Smoothed Analysis of Algorithms. In *Proceedings of the International Congress of Mathematicians, Vol. I (Beijing, 2002).* Higher Ed. Press, Beijing, 597–606.

[27] Josué Tonelli-Cueto. 2019. *Condition and Homology in Semialgebraic Geometry.* Doctoral Thesis. Technische Universität Berlin, DepositOnce Repository. https://doi.org/10.14279/depositonce-9453

[28] Roman Vershynin. 2018. *High-dimensional probability: An introduction with applications in data science.* Cambridge Series in Statistical and Probabilistic Mathematics, Vol. 47. Cambridge University Press, Cambridge. https://doi.org/10.1017/9781108231596

[29] Juan Xu and Chee Yap. 2019. Effective subdivision algorithm for isolating zeros of real systems of equations, with complexity analysis. In *ISSAC'19—Proceedings of the 2019 ACM International Symposium on Symbolic and Algebraic Computation.* ACM, New York, 355–362.