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

Josué Tonelli-Cueto (Inria Paris & IMJ-PRG)
together with
Elias Tsigaridas (Inria Paris & IMJ-PRG)

June 30, 2020

Slides at *https://tonellicueto.xyz/pdf/ISSAC20_slides.pdf*

This presentation is about the accepted paper

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

authored by

- Elias Tsigaridas (Inria Paris & IMJ-PRG), and
- Josué Tonelli-Cueto (Inria Paris & IMJ-PRG)

The authors were partially supported by

- ANR JCJC GALOP (ANR-17-CE40-0009),
- the PGMO grant ALMA, and
- the PHC GRAPE.

The long-term goal

Grid and subdivision methods: What are they for?

Grid methods:

- Feasibility of real polynomial systems (Cucker & Smale; 1999)
- Approximating and counting real zeros (Cucker, Krick, Malajovich & Wschebor; 2008, 2009, 2012)
- Homology of real algebraic sets (Cucker, Krick & Shub; 2012)
- Homology of semialgebraic sets (Bürgisser, Cucker & Lairez; 2018) (Bürgisser, Cucker & T.-C.; 2019, 2020+)

Subdivision methods:

- Root isolation of univariate polynomials (Pan, Davenport, Yap, Sagraloff, Mehlhorn, Rouillier, Mourrain, Yakoubsohn...) Too many to write them all!
- Root isolation of polynomial systems (Dedieu & Yakoubsohn; 1991) (Mourrain& Pavone; 2009) (Mantzaflaris, Mourrain & Tsigaridas; 2011)
- PL approximation of curves and surfaces (Plantinga & Vegter; 2004) (Galehouse; 2009) (Burr, Gao & Tsigaridas; ISSAC'17)

Grid and subdivision methods: What is their complexity?

Techniques for controlling complexity:

- Root separation bounds (Davenport, Mahler & Mignotte) (Emiris, Mourrain & Tsigaridas; 2010) $\rightarrow$ Bit-complexity bounds
- Variety separation bounds (D'Andrea, Krick & Sombra; 2013) (Burr, Gao & Tsigaridas; ISSAC'17) $\rightarrow$ Bit-complexity bounds
- Continuous amortization (Burr, Krahmer & Yap; 2009) (Burr; 2016) + Condition-based complexity + Probabilistic analysis (Cucker, Ergür & T.-C.;2019) $\rightarrow$ Average and smoothed complexity bounds

Condition-based complexity

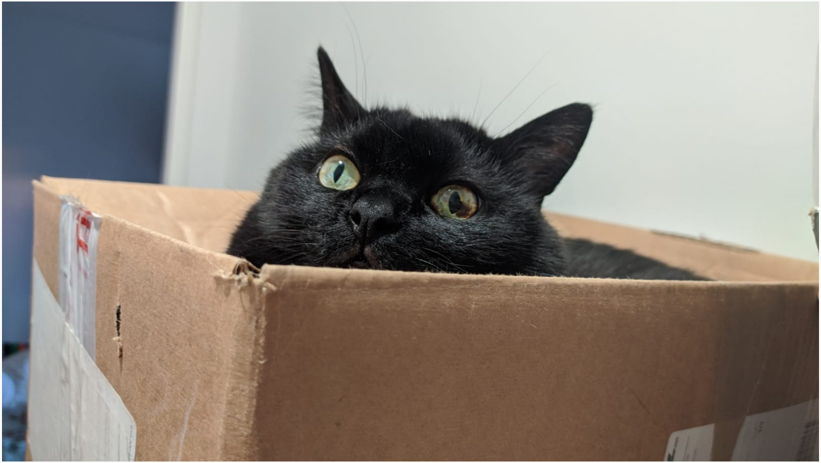
Average and smoothed complexity bounds!

Main issue:

Condition numbers are designed for the sphere,
but the algorithms work in the cube!

Example:
Covering the cube efficiently is easy,
but covering the sphere is not so easy.

Condition numbers for the cube?



This is our objective!

The plan

$$\begin{array}{rcll} \text{Geometry on the sphere} & = & \text{Euclidean norm} & \|x\| := \sqrt{\sum_i |x_i|^2} \\ \text{Geometry on the cube} & = & \infty\text{-norm} & \|x\|_\infty := \max_i |x_i| \end{array}$$

Goal:

$$\begin{array}{rcl} \text{Geometry on the sphere} & \to & \text{Geometry on the cube} \\ \text{Euclidean norm} & \to & \infty\text{-norm} \end{array}$$

Warning: The ∞-norm does not come from an inner product!

Hopes:

- Better complexity estimates
- Faster algorithms
- Better understanding of subdivision methods

Antecedent exploring other norms: (Cucker, Ergür & T.-C.; SIAM AG'19)

Results of the accepted paper

- Condition theory for hypersurfaces in the cube
- Gaussian polynomials
- Polynomials with restricted support (up to assumptions)

We showcase our results with:

- Separation bounds for roots of univariate polynomials in $(0, 1)$
- Plantinga-Vegter algorithm

Polynomial inequalities and condition

Idea

Norm for polynomials control evaluations, variations...

$\updownarrow$

Theory of condition numbers

Our choice:

$$\|f\|_1 := \sum_\alpha |f_\alpha|$$

the 1-norm for polynomials

Why?: $\|f\|_1$ behaves live the dual of $\|x\|_\infty$

In a similar way...

$f \in \mathcal{P}_{n,d} := \{g \in \mathbb{R}[X_0, \dots, X_n] \mid \deg g \leq d\}$, $x, y \in I^n := [-1,1]^n$, $v \in \mathbb{R}^n$

- Control of the evaluation

$$|f(x)| \leq \|f\|_1$$

- Control of the derivative I

$$\|\langle \nabla f, v \rangle\|_1 \leq d\|f\|_1 \|v\|_\infty$$

- Control of the derivative II

$$\|\nabla_x f\|_1 \leq d\|f\|_1$$

- Lipschitz properties for f and its derivatives

$$|f(x) - f(y)| \leq d\|f\|_1 \|x - y\|_\infty$$
$$\|\nabla_x f - \nabla_y f\|_1 \leq d(d-1)\|f\|_1 \|x - y\|_\infty$$

Local condition number

Definition (T.-C., Tsigaridas; ISSAC'20)

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

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

Important observation: $C(f,x) = \infty$ iff x is a singular zero of f

Properties of the local condition number

- Regularity inequality

  either $|f(x)|/\|f\|_1 \geq 1/\, C(f,x)$ or $\|\nabla_x f\|_1/(d\|f\|_1) \geq 1/\, C(f,x)$.

- 1st Lipschitz property

$$f \mapsto \|f\|_1/\, C(f,x) \text{ is 1-Lipschitz}$$

- 2nd Lipschitz property

$$I^n \ni x \mapsto 1/\, C(f,x) \text{ is } d\text{-Lipschitz}$$

- Condition Number Theorem

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

  where $\Sigma_x := \{g \in \mathcal{P}_{n,d} \mid x \text{ is a singular zero of } f\}$

- Higher Derivative Estimate. If $C(f,x)f(x)/\|f\|_1 < 1$, then

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

  where $\gamma(f,x)$ is Smale's γ

All we need for condition-based complexity analyses!

Application 1:
Separation of roots

Separation of roots

Recall...

$$\Delta_\alpha(f) := \mathrm{dist}(\alpha, f^{-1}(0) \setminus \{\alpha\})$$

Theorem (T.-C. & Tsigaridas; ISSAC'20)
Let $f \in \mathcal{P}_{1,d}$. Then, for every complex $\alpha \in f^{-1}(0)$ such that $\mathrm{dist}(\alpha, I) \leq 1/(3(d-1)\,C(f))$,

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

where

$$C(f) := \sup_{x \in I} C(f, x).$$

I.e., the condition number controls the separation of the roots

Probabilistic results

Randomness model I: Two properties

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

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

The smallest such K is the *subgaussian constant* of $\mathfrak{x}$.

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

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

The smallest such ρ is the anti-concentration constant of $\mathfrak{x}$.

Randomness model II: Zintzo random polynomials I

Definition (T.-C. & Tsigaridas; ISSAC'20)

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.

Note: 'zintzo', from Basuqe, means honest, upright, righteous.

Observation: No scaling in the coefficients, as it happens with dobro random polynomials (Cucker, Ergür & T.-C.; ISSAC'19)

Randomness model II: Zintzo random polynomials II

For $\mathfrak{f}$ a zintzo random polynomial, we define:

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

$$K_{\mathfrak{f}} := \sum_{\alpha \in M} K_\alpha, \tag{4.1}$$

   where K_α is the subgaussian constant of $\mathfrak{f}_\alpha$, and
2. the *anti-concentration constants* of $\mathfrak{f}$ which is given by

$$\rho_{\mathfrak{f}} := \sqrt[n+1]{\rho_0 \rho_{e_1} \cdots \rho_{e_n}}, \tag{4.2}$$

   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 $\mathfrak{f}_{e_i}$.

$K_{\mathfrak{f}}$ and $\rho_{\mathfrak{f}}$ will control the complexity estimates

Randomness model II: Zintzo random polynomials III

Let $M \subseteq \mathbb{N}^n$ be such that it contains $0, e_1, \ldots, e_n$. These are two important cases of zintzo random polynomials:

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, $\rho_{\mathfrak{f}} = 1/\sqrt{2\pi}$ 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 $K_{\mathfrak{f}} \leq |M|$.

Randomness model III: Smoothed case

Proposition (T.-C. & Tsigaridas; ISSAC'20)

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

$$K_{\mathfrak{f}_\sigma} \leq \|f\|_1 (1 + \sigma K_{\mathfrak{f}}) \text{ and } \rho_{\mathfrak{f}_\sigma} \leq \rho_{\mathfrak{f}} / (\sigma \|f\|_1).$$

In particular,

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

I.e., the smoothed case is included in our average case!

Probabilistic bound

Theorem (T.-C. & Tsigaridas; ISSAC'20)

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

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

Corollary (T.-C. & Tsigaridas; ISSAC'20)

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

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

Application 2:
Plantinga-Vegter algorithm

The complexity estimate

We had…

Theorem (Cucker, Ergür, T.C.; ISSAC'19)
Let $\mathfrak{f} \in \mathcal{P}_{n,d}$ be a dobro random polynomial with parameters K and ρ. The average number of boxes of the final subdivision of Plantinga-Vegter algorithm on input $\mathfrak{f}$ is at most

$$d^{\frac{n^2+3n}{2}} 2^{\frac{n^2+16n\log(n)}{2}} (c_1 c_2 K \rho)^{n+1}.$$

We get…

Theorem (T.C., Tsigaridas; ISSAC'20)
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 the Plantinga-Vegter algorithm on input $\mathfrak{f}$ is at most

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

An specific bound

Corollary (T.C., Tsigaridas; ISSAC'20)
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 Plantinga-Vegter algorithm 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.

Bere arretagatik eskerrik asko!
Ευχαριστω για την προσοχη σας!

Galderak?
Καμιά ερώτηση?