Polynomial Systems, ℝeal Zeros and Condition Numbers

Josué Tonelli-Cueto
Johns Hopkins University
josue.tonelli.cueto@bizkaia.eu

Elias Tsigaridas
Inria Paris & IMJ-PRG
elias.tsigaridas@inria.fr

Condition Number

Let $f = (f_1, \dots, f_n)$ be a real polynomial system in n variables with f_k of degree at most d_k, its *condition number* is

$$\mathsf{C}(f) := \sup_{x\in[-1,1]^n} \frac{\|f\|}{\max\{\|f(x)\|_\infty, \|\mathrm{D}_x f^{-1}\Delta\|_{\infty,\infty}^{-1}\}}$$

where $\|f\| := \max_k \sum_\alpha |f_{k,\alpha}|$ is the 1-norm, $\| \ \|_\infty$ the ∞-norm, $\| \ \|_{\infty,\infty}$ the matrix norm induced by the ∞-norm and $\Delta := \mathrm{diag}(d_1, \dots, d_n)$.

Meaning? Measures numerical sensitivity of the real zeros of f with respect perturbations of f. it becomes ∞ when f has a singular zero in $[-1,1]^n$.

Geometric Interpretation

Discriminant Variety:

$$\Sigma := \{g \mid \text{there is } x \in [-1,1]^n \text{ s.t. } g(x) = 0, \det \mathrm{D}_x g = 0\}.$$

Condition Number Theorem

Let $f = (f_1, \dots, f_n)$ be a real polynomial system in n variables with f_i of degree at most d_i, then

$$\frac{\|f\|}{\mathrm{dist}(f,\Sigma)} \le \mathsf{C}(f) \le \left(1 + \max_k d_k\right) \frac{\|f\|}{\mathrm{dist}(f,\Sigma)}$$

where dist is the distance induced by $\| \ \|$.

A New ℝeal Phenomenon!

Main Theorem (T.-C., Ts.; '24 +)

Let $f = (f_1, \dots, f_n)$ be a real polynomial system in n variables. Then

$$\#\mathcal{Z}(f,[-1,1]^n) \le \mathcal{O}\left(\log \mathbf{D} \max\{n \log \mathbf{D}, \log \mathsf{C}(f)\}\right)^n$$

where $\mathbf{D}$ is the maximum degree.

Corollary:
Well-posed Real Polynomial Systems
have Few Real Zeros

Observation!
If $\#\mathcal{Z}(f,[-1,1]^n) \ge \Omega(\mathcal{D})$, then $\mathsf{C}(f) \ge 2^{\Omega\left(\frac{\mathcal{D}}{\log \mathbf{D}}\right)}$

Example: Hermitian Matrices

The Question: Given an Hermitian matrix $A \in \mathbb{C}^{d\times d}$, its characteristic polynomial

$$\chi_A := \det(X\mathbb{I} - A)$$

is real-rooted. Is it recommendable to compute the characteristic polynomial of A and then its real roots to obtain the eigenvalues of A?

Numerical Analyst's Answer:

NO!

Our Answer: Effectively no, because, by the theorem below, the characteristic polynomial is ill-posed with respect the perturbation of its coefficients.

Theorem (Moroz, 22) (T.-C., Ts.; '24 +)

Let $A \in \mathbb{C}^{d\times d}$ be a Hermitian matrix, then, for some absolute constant c,

$$\mathsf{C}(\chi_A) \ge 2^{cd/\log d}.$$

What are Polynomial Systems?

Polynomial systems are systems of equations where each equation is the results of adding and multiplying numbers and variables.

One polynomial system:

$$\begin{cases} 1.45X^3 + 5.23XY - 1.23Z^7 &= 0 \\ 2.13XY^2 + 7.23YZ^2 &= 0 \\ 0.12XZ - 1.53Y^2 + 6.45XYZ &= 0 \end{cases}$$

Another polynomial system:

$$\begin{cases} 7.15X^2 + 2.13XY - 1.23Y^2 + 4.34X - 2.34Y + 7.14 &= 0 \\ -1.35X^2 + 4.23XY + 9.45Y^2 - 2.13X + 1.24Y - 13.14 &= 0 \end{cases}$$

Probabilistic Consequences

Prob. Theorem (Ver. A) (T.-C., Ts.; '24 +)

Let $\mathfrak{f} = (\mathfrak{f}_1, \dots, \mathfrak{f}_n)$ be a random real polynomial system in n variables whose coefficients are i.i.d. uniform in $[-1,1]$. Then for $\ell \ge 1$,

$$\mathbb{E}_{\mathfrak{f}} \#\mathcal{Z}_r(\mathfrak{f}, \mathbb{R}^n)^\ell \le \mathcal{O}\left(n\ell \log^2 \mathbf{D}\right)^{n\ell}$$

where $\mathcal{Z}(\mathfrak{f}, \mathbb{R}^n)$ is the set of real zeros of $\mathfrak{f}_1 = \dots = \mathfrak{f}_n = 0$, and $\mathbf{D}$ is the maximum degree.

Prob. Theorem (Ver. B) (T.-C., Ts.; '24 +)

Let $\mathfrak{f} = (\mathfrak{f}_1, \dots, \mathfrak{f}_n)$ be a random real polynomial system in n variables whose coefficients are independent and uniformly distributed in $[-1,1]$. Then there is an absolute constant C such that, for $t \ge 1$,

$$\mathbb{P}_{\mathfrak{f}}\left(\sqrt[n]{\#\mathcal{Z}(\mathfrak{f}, \mathbb{R}^n)} \ge t\right) \le \exp\left(\frac{-t}{Cn \log^2 \mathbf{D}}\right)$$

where $\mathcal{Z}_r(\mathfrak{f}, \mathbb{R}^n)$ is the set of real zeros of $\mathfrak{f}_1 = \dots = \mathfrak{f}_n = 0$, and $\mathbf{D}$ is the maximum degree.

Corollary:
Fewnomial systems with many zeros
are very improbable

More generally...
We can cover a wide range of probabilistic assumptions

Why these bounds?

Condition numbers have nice probabilistic properties!

Prob. Theorem (T.-C., Ts.; '24 +)

Let $\mathfrak{f} = (\mathfrak{f}_1, \dots, \mathfrak{f}_n)$ be a random real polynomial system in n variables whose coefficients are independent and uniformly distributed in $[-1,1]$. Then for $\ell \ge 1$,

$$\mathbb{E}_{\mathfrak{f}} \log^\ell \mathsf{C}(\mathfrak{f}) \le \mathcal{O}\left(n\ell \log \mathbf{D}\right)^{n\ell}$$

where $\mathcal{Z}(\mathfrak{f}, \mathbb{R}^n)$ is the set of real zeros of $\mathfrak{f}_1 = \dots = \mathfrak{f}_n = 0$, and $\mathbf{D}$ is the maximum degree.

Other Valid Distributions:

- Exponential.
- Gaussian.
- Integer variables uniformly distributed on an interval.

Evaluation Reduction
If
$\mathsf{C}(f)$ is large,
then
$\mathbb{P}(|f(\mathfrak{x})|$ is small$)$ is large,
where $\mathfrak{x} \in [-1,1]^n$ random.

And where do these appear?

Polynomial systems appear in many applications, since they are among non-linear equations the most simple ones.

Biochemical Reaction Networks:
How many equilibria
does a biochemical reaction network have?
Counting Solutions of a Polynomial System!

Statistics:
How can we compute the parameters
of a distribution out of sample values?
Solving a Polynomial System!

Algorithmic Consequences

Fully constructible Proof!

Alg. Theorem (T.-C., Ts.; '24 +)

There is a explicit partition

$$\mathcal{B}$$

of $[-1,1]^n$ into

$$\mathcal{O}(\log \mathbf{D})^n$$

boxes such that for all real polynomial system

$$f = (f_1, \dots, f_n)$$

in n variables of degree at most $\mathbf{D}$ and all $\mathrm{B} \in \mathcal{B}$, there is a polynomial

$$\phi_{f,\mathrm{B}}$$

of degree $\mathcal{O}(\max\{n \log \mathbf{D}, \log \mathsf{C}(f)\})$ such that

$$\#\mathcal{Z}(f, \mathrm{B}) \le \#\mathcal{Z}(\phi_{f,\mathrm{B}}, \mathbb{R}^n).$$

Moreover, every real zero of f in B has a zero of $\phi_{f,\mathrm{B}}$ that converges quadratically to it under Newton's method.

Proof idea: Well-conditioned polynomials are fast converging Taylor series

What's the issue?
We need an estimate of $\mathsf{C}(f)$
to make the scheme effective,
can we get the estimate fast?
Or can we go around it?

A New Goal

Is there a
Montecarlo numerical algorithm
that,
given a real polynomial system f,
outputs an approximation of

$$\mathcal{Z}(f, [-1,1]^n)$$

with run-time at most

$$\mathcal{O}_{n,\mathbf{D}}\left(\log \mathsf{C}(f) + \log\log \frac{1}{\varepsilon}\right)^{\mathcal{O}(n)} \mathrm{L}(f)$$

with ε being the failure probability and $\mathrm{L}(f)$ the evaluation cost of f?

On the sphere...
We can cover also random polynomial system with the Weyl scaling. However, we only get probabilistic bounds of the form $\mathcal{O}\left(\sqrt{\mathbf{D}} \log \mathbf{D}\right)^n$ appears in the bound.