

NEW CONDITION-BASED BOUNDS FOR THE NUMBER OF ~~R~~ REAL ZEROS

Joint work with
Elias Tsigaridas

Josué TONELLI-CUETO
Inria Paris & IMJ-PRG

Which questions are we interested in?

- Given a real polynomial system,
how many real zeros does it have?

↙
what are the
possibilities?

↘
what are the
restrictions?

- Given a random real polynomial system,
what are the statistics of its number of real zeros?

↙
how robust
are our estimates?

↓
how do the estimates
depend on the structures?

\mathbb{R} is the real complex, not \mathbb{C} Complex !

Let

$$g: \begin{cases} g_1 = \sum_{|\alpha| \leq d_1} g_{1,\alpha} X^\alpha \\ \vdots \\ g_n = \sum_{|\alpha| \leq d_n} g_{n,\alpha} X^\alpha \end{cases}$$

have generic \mathbb{C} complex / \mathbb{R} real coefficients,
then:

$$\#Z(g, \mathbb{R}^n) \leq \#Z(g, \mathbb{C}^n) = D := \prod_{i=1}^n d_i$$

Bézout

\mathbb{R} is the real complex, not \mathbb{C} Complex II

Let $A_1, \dots, A_n \subseteq \mathbb{N}^n$,

$$g: \begin{cases} g_1 = \sum_{\alpha \in A_1} g_{1,\alpha} X^\alpha \\ \vdots \\ g_n = \sum_{\alpha \in A_n} g_{n,\alpha} X^\alpha \end{cases}$$

have generic complex/ \mathbb{R} coefficients,
then:

$$\# Z(g, (\mathbb{R}^*)^n) \leq \# Z(g, (\mathbb{C}^*)^n) = MV(\text{conv}(A_1), \dots, \text{conv}(A_n))$$

Bernstein-Khovanskii-Kushnirenko

Real is the real complex, not Complex III

Kushnirenko Hypothesis III

Let $A_1, \dots, A_n \subseteq \mathbb{N}^n$,

$$g: \begin{cases} g_i = \sum_{\alpha \in A_i} g_{i,\alpha} X^\alpha \end{cases} \quad (i=1, \dots, n)$$

THE HOLY GRAIL
OF RAG

Then:

$$\#Z_v(g, (\mathbb{R}^*)^n) \leq \text{poly}(n, \sum_{i=1}^n \#A_i)^n$$

Widely open!

($n=1$) $\#Z_v(g, \mathbb{R}^*) \leq 2\#A_1$ (Descartes' rule of signs)

($n=2$) ($A_2 = \{(\alpha_1, \alpha_2) \mid \alpha_1 + \alpha_2 \leq d_2\}$) $\#Z_v(g, (\mathbb{R}^*)^2) \leq O(\#A_1 d_2^3 + (\#A_1)^3 d_2^2)$
(Sevast'yanov) (Koiran, Portier, Tavenas)

($A_2 = \{(0,0), (1,0), (0,1)\}$) $\#Z_v(g, (\mathbb{R}^*)^2) \leq 6d-7$ (Bihan, El Hilany)

(A_2 arbitrary) Open!

Z_v : regular zeros

Real is the real complex, not Complex IV

Kushnirenko Hypothesis III

Let $A_1, \dots, A_n \subseteq \mathbb{N}^n$,

$$g: \begin{cases} g_i = \sum_{\alpha \in A_i} g_{i,\alpha} X^\alpha \end{cases} \quad (i=1, \dots, n)$$

THE HOLY GRAIL
OF RAG

Then:

$$\#Z_v(g, (\mathbb{R}^*)^n) \leq \text{poly}(n, \sum_{i=1}^n \#A_i)^n$$

Widely open!

$$(\text{General } n) \left(\#(\cup_{i=1}^n A_i) \leq t \right) \#Z_v(g, (\mathbb{R}^*)^n) \leq O\left(2^{n + \binom{t-n-1}{2}} n^{t-n-1} \right)$$

(Bihan, Sottile)

$(A_1 = \dots = A_n, \#A_i \leq t) (g_{i,\alpha} \sim N(0, \sigma(\alpha)) \text{ ind.})$

$$\mathbb{E}_g \#Z_v(g, (\mathbb{R}^*)^n) \leq 2 \binom{t}{n} \leq \frac{2t^n}{n!}$$

(Bürgisser, Ergür, TC)

Z_v : regular zeros

\mathbb{R} real is the real complex, not Complex V

A Concrete Example

$$g: \begin{cases} \alpha_1 + \beta_1 X + \gamma_1 Y + \delta_1 XYZ^d \\ \alpha_2 + \beta_2 X + \gamma_2 Y + \delta_2 XYZ^d \\ \alpha_3 + \beta_3 X + \gamma_3 Y + \delta_3 XYZ^d \end{cases}$$

For generic $\alpha_i, \beta_i, \gamma_i, \delta_i \in \mathbb{C}$,

$$\#Z(g, \mathbb{C}^3) = d$$

LARGE!

For generic $\alpha_i, \beta_i, \gamma_i, \delta_i \in \mathbb{R}$,

$$\#Z(g, \mathbb{R}^3) \leq 1$$

small!

A Random Path towards...

Kushnirenko Hypothesis III

Kushnirenko Random Hypothesis (Unmixed) Let $A \subseteq \mathbb{N}^n$ and a random real polynomial system

$$g: \begin{cases} g_i = \sum_{\alpha \in A} g_{i,\alpha} X^\alpha \quad (i=1, \dots, n) \end{cases}$$

with the $g_{i,\alpha}$ random independent random variables, then for all $e \in \mathbb{N}$,

$$\mathbb{E} \#Z_+(g, \mathbb{R}_+^n)^e \leq \text{poly}(n, \#A)^{ne}$$

- Equivalent to Kushnirenko Hypothesis III
- It creates a continuum between where we are and the Holy Grail of Real Algebraic Geometry

All this is very nice,

but do you have anything new to say?



Condition Numbers I

Def. Let $g \in \mathcal{P}_d[n] := \{g \in \mathbb{R}[x_1, \dots, x_n]^n \mid \deg g_i \leq d_i\}$,
and $x \in I^n := [-1, 1]^n$, the local condition
number of g at x is

$$C(g, x) := \frac{\|g\|_1}{\max\{\|g(x)\|_\infty, S_n(\Delta^{-1} D_x g)\}}$$

where

$$\Delta := \text{diag}(d_1, \dots, d_n)$$

$$\|g\|_1 := \max_i \sum_\alpha |g_{i,\alpha}|$$

$$S_n(A) = \min_{v \neq 0} \frac{\|Av\|_\infty}{\|v\|_\infty} = \|A^{-1}\|_{\infty, \infty}^{-1}$$

Condition Numbers II

Def. Let $g \in \mathcal{P}_d[n] := \{g \in \mathbb{R}[x_1, \dots, x_n]^n \mid \deg g_i \leq d_i\}$,
the condition number of g is

$$C(g) := \sup_{x \in \mathbb{I}^n} C(g, x)$$

Condition Number Theorem. Let $g \in \mathcal{P}_d[n]$,
then

$$\frac{\|g\|_1}{\text{dist}_1(g, \Sigma)} \leq C(g) \leq n(d+1) \frac{\|g\|_1}{\text{dist}_1(g, \Sigma)}$$

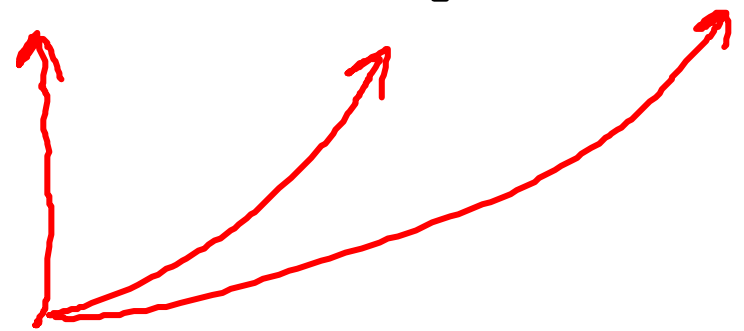
where $\Sigma := \{g \in \mathcal{P}_d[n] \mid \text{every zero of } g \text{ in } \mathbb{I}^n \text{ is regular}\}$

$C(g)$ measures how far is g from the discriminant!

The New Bound

Thm. Let $g \in \mathcal{P}_d[n]$. Then

$$\#Z(g, \mathbb{I}^n) \leq \max \{ O(n \log(2D))^{2n}, O(\log(2D) \log C(g))^n \}$$



Logarithmic!

Cor. Real polynomial systems with many zeros are ill-conditioned.

Proof Ideas I

1. Analytic approximation + Smale's α -theory

Real polynomial systems can be approximated locally by polynomial of degree

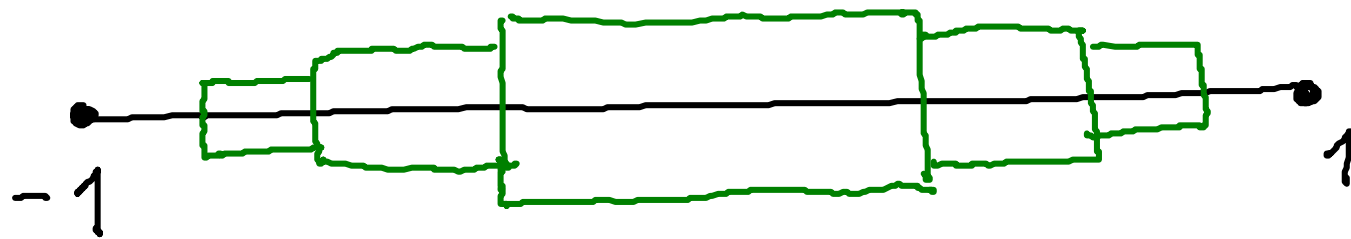
$$\max \{ \mathcal{O}(\log D), \mathcal{O}(\log C(\delta)) \}$$

with the same number of real zeros

Generalizes an idea by Moroz for the univariate case

Proof Ideas II

2. A cover where the local approximation happens can be easily constructed



This cover can be constructed a priori, there is computational content in the proof.

A similar bound
can be obtained
in the projective setting
for the orthogonally invariant
condition number of
Cucker, Krick,
Malajovich & Wschebor!

Random consequences I.

Def. A Kac random polynomial system with support A is a random system

$$g: \left\{ g_i = \sum_{\alpha \in A} g_{i,\alpha} X^\alpha \quad (i=1, \dots, n) \right.$$

where the $g_{i,\alpha} \sim N(0,1)$ i.i.d.



Our probabilistic results hold also if $g_{i,\alpha} \sim \mathcal{U}([-1,1])$ or more general probability distributions.

Random consequences II

Thm. Let $f \in \mathcal{P}_d[n]$ be a random Kac system with support $A \ni 0$. Then

$$\mathbb{P}(\log C(f) \geq t) \leq \text{poly}(n, d, \#A)^n e^{-ct}$$

for some universal constant $c > 0$.

⚠ Condition numbers are easier to control probabilistically

Cor. $\mathbb{E} C(f)^e \leq (\tilde{c} n^2 \log d \log \#A e)^e$

for some universal constant $\tilde{c} > 0$.

Random consequences III

$$\text{Cor. } \mathbb{E} \#Z(f, I^n)^e \leq (\tilde{c} n^3 \log^2 D \#A e)^{en}$$

for some universal constant $\tilde{c} > 0$.

Cor. Random real polynomials with many zeros are extremely rare.

Eskeirik
Asko!

Galderak?

Oder Fragen?