Random polynomials and expected complexity of real solving

Elias TSIGARIDAS

PolSys group
INRIA Paris

joint work with

Ioannis Emiris & André Galligo
U. of Athens, Greece — U. of Nice, France

Outline

1. Intro/Motivation
   - Real solving using STURM
2. Expected Complexity
   - $SO(2)$ polynomials
   - Weyl polynomials
3. Random Bernstein polynomials
4. ToDo list

Outline

Univariate Real Solving

Problem

Given $A \in \mathbb{Z}[X]$ such that

$$A = a_d X^d + \cdots + a_1 X + a_0 \quad \in \mathbb{Z}[X]$$

where

$$\mathbf{d} = \deg(A) \quad \text{and} \quad \mathcal{L}(A) = \max_{0 \leq i \leq d} \{\lg |a_i|\} = \tau$$

Compute isolating intervals for the real roots.

Example

Let

$$f = x^5 - 7x^4 + 22x^3 - 4x^2 - 48x + 36 = (x-1)\cdot(x^2 - 6x + 18)\cdot(x^2 - 2)$$

real roots	$-\sqrt{2}$	1	$+\sqrt{2}$
output	$(-49, 0)$	$(\frac{49}{64}, \frac{147}{128})$	$(\frac{147}{128}, 49)$

How hard is the problem?

Definition (Separation bound)

$$\Delta = sep(A) = \min_{i \neq j} |\gamma_i - \gamma_j| \sim 2^{-d\,\tau} = 2^{-s}$$

Example

Consider the Wilkinson polynomial

$$A = (x-1)(x-2)\cdots(x-20)$$

$$\Delta \sim 10^{-344}$$

actual $\quad sep(A) = 1$

Experimental motivation

		300	400	500	600	700	800	900	1000
L	CF	9.14	25.27	55.86	110.13	214.99	407.09	774.22	1376.34
	#roots	300	400	500	600	700	800	900	1000
C1	CF	3.16	8.61	19.67	38.23	77.75	139.18	247.11	414.51
	#roots	300	400	500	600	700	800	900	1000
W	CF	2.54	6.09	12.07	21.43	34.52	53.35	81.88	120.21
	#roots	300	400	500	600	700	800	900	1000
R1	CF	0.07	0.33	0.06	0.37	0.66	0.76	1.03	1.77
	#roots	2	6	2	4	4	2	4	4

(Emiris, T.; 2007)

Outline

1. Intro/Motivation
   - Real solving using STURM
2. Expected Complexity
   - $SO(2)$ polynomials
   - Weyl polynomials
3. Random Bernstein polynomials
4. ToDo list

Subdivision solvers

General strategy

- Compute an interval containing all the real roots
- Subdivide the interval until is certified that contains 0 or 1 real roots

Subdivision solvers $\sim$ Binary search

Two main categories:

Sturm (-Habicht)

Descartes' rule of sign

Subdivision solvers

General strategy

- Compute an interval containing all the real roots
- Subdivide the interval until is certified that contains 0 or 1 real roots

Subdivision solvers $\sim$ Binary search

Two main categories:

Sturm (-Habicht)

Descartes' rule of sign

Theorem

Using STURM, *we isolate the real roots of A with worst-case complexity*

$$\widetilde{O}_B(r d^2(s^2 + \tau s)),$$

where r is the number of real roots.

The history of (expected) complexity bounds

	CF	STURM	DESCARTES	BERNSTEIN
$<$ 1980	$\widetilde{\mathcal{O}}_B(2^\tau)$ (Uspensky;1948)	$\widetilde{\mathcal{O}}_B(d^7\tau^3)$ (Heidel;1971)	$\widetilde{\mathcal{O}}_B(d^6\tau^2)$ (Collins,Akritas;1976)	(L,R;81)
$<$ 2005	$\mathcal{O}_B(d^5\tau^3)$ (Akritas;1980)	$\widetilde{\mathcal{O}}_B(d^6\tau^3)$ (Davenport;1988)	$\widetilde{\mathcal{O}}_B(d^5\tau^2)$ (Krandick;95,Johnson;98)	$\widetilde{\mathcal{O}}_B(d^6\tau^3)$ (MVY;2004)
$\leq$2006	$\widetilde{\mathcal{O}}_B(d^4\tau^2)$ (Emiris,T.;2006)	$\widetilde{\mathcal{O}}_B(d^4\tau^2)$ (Du,Sharma,Yap;2005) (Emiris,Mourrain,T.;2006)	$\widetilde{\mathcal{O}}_B(d^4\tau^2)$ (Eigenwillig,Sharma,Yap;06)	$\widetilde{\mathcal{O}}_B(d^4\tau^2)$ (ESY;2006) (EMT;2006)
2006+	$\widetilde{\mathcal{O}}_B(d^3\tau)$ (E,T.; 09) $\widetilde{\mathcal{O}}_B(d^5\tau^2)$ (S;08) $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ (M,R;09) $\widetilde{\mathcal{O}}_B(d^4\tau^2)$ (T;11)	$\widetilde{\mathcal{O}}_B(r\, d^2\tau)$ (Emiris,Galligo,T.;10)		

Numerical bound $\widetilde{\mathcal{O}}_B(d^3\tau)$ (Pan; 2001)

Outline

Random polynomials

$$A = \sum_{i=0}^{d} a_i x^i$$

Distribution	$\mathbf{E}[\#\{\text{real roots}\}]$	
i.i.d Gaussians, $N(0,1)$ or Uniform(0,1)	$\frac{2}{\pi}\log d + \mathcal{O}(1)$	[Kac; 43]
i.d Gaussians, $N(0, \binom{d}{i})$	$\sqrt{d}$	
i.d Gaussians, $N(0, 1/\sqrt{i!})$	$\frac{2}{\pi}\sqrt{d} + \mathcal{O}(1)$	

Outline

1. Intro/Motivation
   - Real solving using STURM
2. Expected Complexity
   - $SO(2)$ polynomials
   - Weyl polynomials
3. Random Bernstein polynomials
4. ToDo list

$SO(2)$ polynomials

Definition

$A = \sum_{i=0}^{d} a_i x^i$ $\qquad a_i$ i.i.d Gaussians with $N(0, \binom{d}{i})$

$A = \sum_{i=0}^{d} \sqrt{\binom{d}{i}}\, a_i\, x^i$ $\qquad a_i$ i.i.d Gaussians with $N(0, 1)$

(Edelman-Kostlan;95)

``the more natural definition of a random polynomial...''

Expected number of real roots

$$\rho(t) = \frac{\sqrt{d}}{\pi(1+t^2)}$$ ("true" density of real roots)

$$r = \int_{\mathbb{R}} \rho(t)dt = \sqrt{d}$$ (Edelman,Kostlan;1995)

Definition (Straightened Zeros)

$$\zeta_j = \mathcal{P}(\alpha_j) = \sqrt{d}\ \mathtt{arctan}(\alpha_j)/\pi,\ j = 1, \ldots, r,$$

- $\mathcal{P}(t) = \int_0^t \rho(u)\, du$.
- Bijection between α_j and ζ_j.
- The ordering is preserved.
- The ζ_j uniformly distributed on the circle of length $2\sqrt{d}$ (Bleher,Di;1997)

Definition (Straightened Zeros)

$$\zeta_j = \mathcal{P}(\alpha_j) = \sqrt{d}\ \arctan(\alpha_j)/\pi,\ j = 1, \ldots, r,$$

- $\mathcal{P}(t) = \int_0^t \rho(u)\, du$.
- Bijection between α_j and ζ_j.
- The ordering is preserved.
- The ζ_j uniformly distributed on the circle of length $2\sqrt{d}$ (Bleher,Di;1997)

Lemma ((Bleher,Di;1997))

As $d \to \infty$ the limit 2-point correlation of ζ_j, when $s_1 - s_2 \to 0$, is

$$k(s_1, s_2) \to \pi^2 |s_1 - s_2|/4$$

A joint pdf of two ζ_j.

Computations with the joint pdf

$$\Pr[\Delta(\zeta) \leq l] \to \int_Z k(s_1, s_2)\, ds_1\, ds_2$$
$$= 2 \int_0^{2\sqrt{d}} ds_1 \int_{s_1}^{s_1+l} k(s_1, s_2)\, ds_2$$
$$= \frac{\pi^2}{2} \int_0^{2\sqrt{d}} ds_1 \int_{s_1}^{s_1+l} |s_1 - s_2|\, ds_2 = \frac{\pi^2\sqrt{d}}{2}\, l^2$$

$$\mathrm{E}[\Delta(\zeta)] \geq l \Pr[\Delta(\zeta) \geq l] = l - l \Pr[\Delta(\zeta) < l] > l - \frac{\pi^2\sqrt{d}}{2}\, l^3$$

Remember

$$\alpha_j = \mathcal{P}^{-1}(\zeta_j)$$

Divide the world to two parts

- $\Delta \leq l = 1/(d^c \tau)$
  - worst case bound for isolation, $\widetilde{\mathcal{O}}_B(d^4 \tau^2)$.
  - Occurs $\Pr[\Delta \leq l] = \sqrt{d}\, l^2 = \frac{1}{d^{2c-1/2}\,\tau^2}$,
- $\Delta > 1/(d^c \tau)$
  - $s = \mathcal{O}(\lg d + \lg \tau)$ (Markov's inequality)
  - $\Pr[\Delta > l] = 1 - \sqrt{d}\, l^2 = 1 - \frac{1}{d^{2c-1/2}\,\tau^2} \rightarrow 1$

Divide the world to two parts

- $\Delta \leq l = 1/(d^c \tau)$
  - worst case bound for isolation, $\widetilde{\mathcal{O}}_B(d^4 \tau^2)$.
  - Occurs $\Pr[\Delta \leq l] = \sqrt{d}\, l^2 = \frac{1}{d^{2c-1/2}\, \tau^2}$,
- $\Delta > 1/(d^c \tau)$
  - $s = \mathcal{O}(\lg d + \lg \tau)$ (Markov's inequality)
  - $\Pr[\Delta > l] = 1 - \sqrt{d}\, l^2 = 1 - \frac{1}{d^{2c-1/2}\, \tau^2} \to 1$

$$\widetilde{\mathcal{O}}_B\left((1 - \frac{1}{d^{2c-1/2}\, \tau^2}) \cdot r d^2 \tau + \frac{1}{d^{2c-1/2}\, \tau^2} \cdot d^4 \tau^2 \right) = \widetilde{\mathcal{O}}_B(r d^2 \tau)$$

Outline

Weyl polynomials (Ginibre random matrices)

Definition

$A = \sum_{i=0}^{d} a_i x^i$ $\quad a_i$ i.i.d Gaussians with $N(0, 1/\sqrt{i!})$

$A = \sum_{i=0}^{d} \frac{1}{1/\sqrt{i!}} a_i x^i$ $\quad a_i$ i.i.d Gaussians with $N(0, 1)$

- Density (Schehr,Majumdar;2008)

$$\rho(t) = \frac{1}{\pi}\sqrt{1 + \frac{t^{2d}(t^2 - d - 1)}{e^{t^2}\Gamma(n+1,t)} - \frac{t^{4d+2}}{(e^{t^2}\Gamma(n+1,t))^2}} \to \begin{cases} \pi^{-1}, & |t| \ll \sqrt{d} \\ \frac{d}{\pi t^2}, & |t| \gg \sqrt{d} \end{cases}$$

- Real roots (Schehr,Majumdar;2008)

$$r = \int_{\mathbb{R}} \rho(t) dt \sim \frac{2}{\pi}\sqrt{d}$$

- Limit 2-point correlation of straightened zeros

$$w(s_1, s_2) \to |s_1 - s_2| / (4\pi)$$

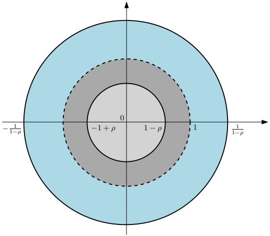
Theorem

For $SO(2)$ and Weyl random polynomials
the expected complexity of STURM *is*

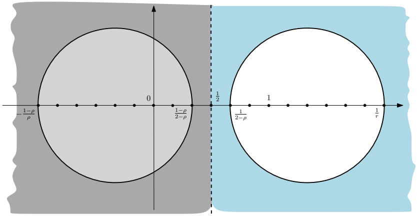
$$\widetilde{O}_B(r\, d^2 \tau)$$

Outline

Random polynomials



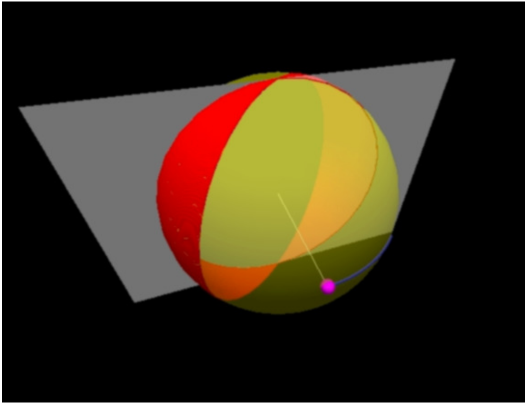
$$x \mapsto \frac{x}{x+1}$$



(equi-)distribution of the roots (Erdos,Turán;1950), (Hughes,Nikeghbali;2004)

	$\mathbf{E}[\#\text{real roots}]$		
monomial	$\frac{2}{\pi}\log(d) + o(1)$	$N(0,1)$	(Kac;1943) (Edelman,Kostlan;1995)
Bernstein	$\sqrt{d}$	$N(0,d^d)$	(Dedieu,Armentano;2009)
Bernstein	$\sqrt{2\,d} \pm \mathcal{O}(1)$	$N(0,d)$	

Integral Geometry



$$\mathbf{a} \cdot \mathbf{x} = (a_2, a_1, a_0) \cdot (x^2, x, 1) = \sum_{i=0}^{d=2} a_i\, x^i = 0$$

#(real roots) $\sim$ area $\sim$ length of the curve

(Edelman,Kostlan;1995)

Images and video by (George Koulieris; 2009)

Theorem (Expected number of real roots (Kac) (Edelman-Kostlan))

$$v(t) = (f_o(t), \ldots, f_n(t))^\top$$

is a vector of differentiable functions and $c_0, \ldots, c_n$ *elements of a multivariate normal distribution with zero mean and covariance matrix* C.

The expected number of real zeros on an interval (or a measurable set) I *of the equation*

$$c_0 \cdot f_0(t) + c_1 \cdot f_1(t) \cdots + c_n \cdot f_n(t) = 0$$

is

$$\int_I \frac{1}{\pi} \|\mathbf{w}'(t)\| dt, \quad \mathbf{w} = w(t)/\|w(t)\|.$$

where $w(t) = C^{1/2} v(t)$. *In logarithmic derivative notation, this is*

$$\frac{1}{\pi} \int_I \sqrt{\frac{\partial^2}{\partial x \partial y} \log \left(v(x)^\top C v(x) \right)\Big|_{x=y=t}} dt.$$

Theorem (Expected number of real roots (Kac) (Edelman-Kostlan))

$$v(t) = (1, t, \ldots, t^n)^\top$$

is a vector of differentiable functions and $c_0, \ldots, c_n$ *elements of a multivariate normal distribution with zero mean and covariance matrix* C.

The expected number of real zeros on an interval (or a measurable set) I *of the equation*

$$c_0 \cdot 1 + c_1 \cdot t + \cdots + c_n \cdot t^n = 0$$

is

$$\int_I \frac{1}{\pi} \|\mathbf{w}'(t)\| dt, \quad \mathbf{w} = w(t)/\|w(t)\|.$$

where $w(t) = C^{1/2} v(t)$. *In logarithmic derivative notation, this is*

$$\frac{1}{\pi} \int_I \sqrt{\frac{\partial^2}{\partial x \partial y} \log \left(v(x)^\top C v(x) \right)|_{x=y=t}} dt.$$

Change the polynomial

The coefficients b_k are standard normal r.v.

$$\widehat{P} := \sum_{k=0}^{k=d} b_k \binom{d}{k} z^k (1-z)^{d-k}$$

$$P = \sum_{k=0}^{k=d} b_k \binom{d}{k} y^k$$

$$P = \sum_{k=0}^{k=d} b_k \binom{d}{k} x^{2k}$$

$$\binom{d}{k} \sim \sqrt{\sqrt{\frac{d}{\pi}} \sqrt{\frac{1}{k(d-k)}} \sqrt{\binom{2d}{2k}}} = \sqrt{S} \sqrt{\binom{2d}{2k}}$$

$$P = \sum_{k=0}^{k=d} b_k \sqrt{\binom{2d}{2k}} x^{2k}$$

Change the polynomial

The coefficients b_k are standard normal r.v.

$$\widehat{P} := \sum_{k=0}^{k=d} b_k \binom{d}{k} z^k (1-z)^{d-k}$$

$$P = \sum_{k=0}^{k=d} b_k \binom{d}{k} y^k$$

$$P = \sum_{k=0}^{k=d} b_k \binom{d}{k} x^{2k}$$

$$\binom{d}{k} \sim \sqrt{\sqrt{\frac{d}{\pi}}\sqrt{\frac{1}{k(d-k)}}}\sqrt{\binom{2d}{2k}} = \sqrt{S}\sqrt{\binom{2d}{2k}}$$

$$P = \sum_{k=0}^{k=d} b_k \sqrt{\binom{2d}{2k}} x^{2k}$$

Put $S \leq \sqrt{d}$ in the variance

The curve and some tricks

$$P = \sum_{k=0}^{k=d} a_k \sqrt{\binom{2d}{2k}} x^{2k}$$

$$\frac{1}{\pi} \int_I \sqrt{\frac{\partial^2}{\partial x \partial y} \log \left(v(x)^\top \sqrt{C} \sqrt{C} v(x) \right) \Big|_{x=y=t}} dt$$

$$v(x)^\top C v(y) = \sum_{k=0}^{d} \binom{2d}{2k} (xy)^{2k}$$

The curve and some tricks

$$P = \sum_{k=0}^{k=d} a_k \sqrt{\binom{2d}{2k}} x^{2k}$$

$$\frac{1}{\pi} \int_I \sqrt{\frac{\partial^2}{\partial x \partial y} \log \left(v(x)^\top \sqrt{C} \sqrt{C} v(x) \right) \Big|_{x=y=t}} dt$$

$$v(x)^\top C v(y) = \sum_{k=0}^{d} \binom{2d}{2k} (xy)^{2k}$$

The trick

$$\sum_{k=0}^{d} \binom{2d}{2k} z^{2k} = \frac{1}{2}(1+z)^{2d} + \frac{1}{2}(1-z)^{2d}$$

Theorem

The expected number of real roots of a random polynomial (coefficients i.i.d. Gaussians, with 0 mean and moderate variance) in the Bernstein basis, is

$$\sqrt{2d} \pm \mathcal{O}(1)$$

Theorem

The expected number of real roots of a random polynomial (coefficients i.i.d. Gaussians, with 0 mean and moderate variance) in the Bernstein basis, is

$$\sqrt{2d} \pm \mathcal{O}(1)$$

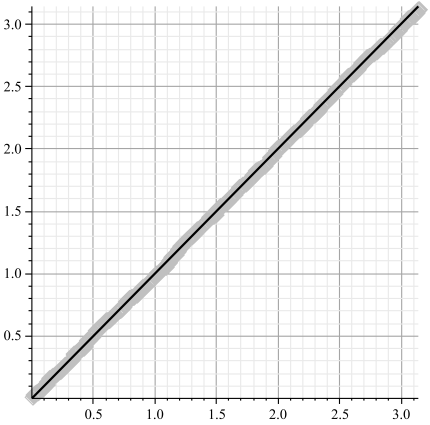
Conjecture

If the coefficients are in $N(0, 1)$ then expected number of real roots is

$$\sqrt{2d} \pm \mathcal{O}(1)$$

Random polynomials in the Bernstein basis

d	$\sqrt{2d}$	$(-\infty, \infty)$	$(-\infty, -1)$	$(-1, 0)$	$(0, 1)$	$(1, \infty)$
100	14.142	13.640	0.760	2.740	6.530	3.610
150	17.321	16.540	0.890	3.260	8.090	4.300
200	20.000	19.740	1.100	3.780	9.740	5.120
250	22.361	21.400	1.350	3.970	10.610	5.470
300	24.495	24.320	1.270	4.760	12.300	5.990
350	26.458	26.540	1.620	5.100	13.400	6.420
400	28.284	27.980	1.490	5.430	14.080	6.980
450	30.000	29.460	1.620	5.890	14.970	6.980
500	31.623	31.200	1.830	5.960	15.620	7.790
550	33.166	32.740	1.770	6.360	16.290	8.320
600	34.641	34.300	1.850	6.570	17.270	8.610
650	36.056	35.480	2.050	6.840	17.240	9.350
700	37.417	37.200	2.160	7.510	18.650	8.880
750	38.730	38.180	2.190	7.300	19.360	9.330
800	40.000	39.160	2.220	7.830	19.490	9.620
850	41.231	40.420	2.130	8.010	20.320	9.960
900	42.426	41.780	2.390	8.070	20.530	10.790
950	43.589	42.680	2.200	8.330	21.570	10.580
1000	44.721	43.540	2.400	8.610	21.770	10.760



Function $\arccos(2t - 1)$ of real roots in $(0, 1)$,
against uniform distribution in $(0, \pi)$

Outline

1. Intro/Motivation
   - Real solving using STURM
2. Expected Complexity
   - $SO(2)$ polynomials
   - Weyl polynomials
3. Random Bernstein polynomials
4. ToDo list

ToDo list

- More random polynomials.

  Kac polynomials! What about sparse or symmetric polys?

- Further improvement of the complexity bounds

  what about DESCARTES *solver ?*

- Similar results for polynomial systems.

  Really hard integrals. What about small/constant degree.

- Exploit further the connections with Stochastic (P)DEs

  !!!!!

- etc...

ToDo list

- More random polynomials.

  Kac polynomials! What about sparse or symmetric polys?

- Further improvement of the complexity bounds

  what about DESCARTES *solver ?*

- Similar results for polynomial systems.

  Really hard integrals. What about small/constant degree.

- Exploit further the connections with Stochastic (P)DEs

  !!!!!

- etc...

Thank you!