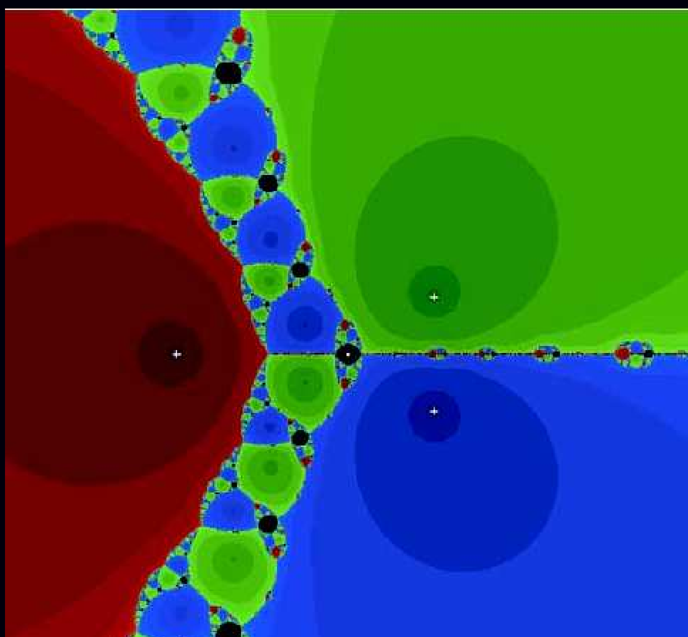
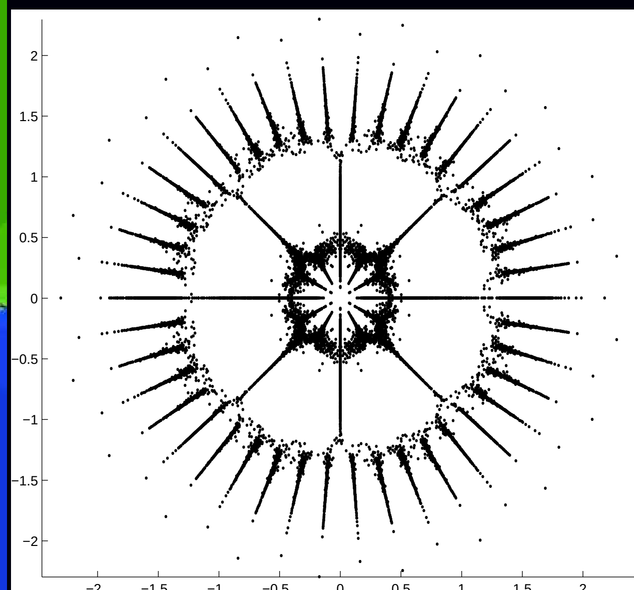
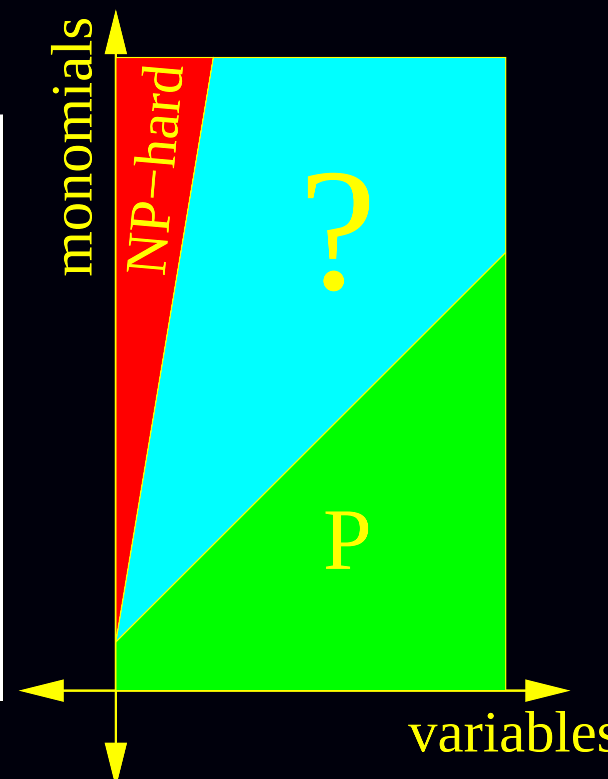
Some New Complexity Bounds for Real Fewnomials

J. Maurice Rojas* (Texas A&M University)

April 13, 2004







* Partially supported by NSF grants DMS-0211458 and DMS-0138446.

OUTLINE

1. **Sharpening Khovanski's Real Fewnomial Theorem** [Li, Rojas, Wang: Disc. & Comp. Geom. 2003]

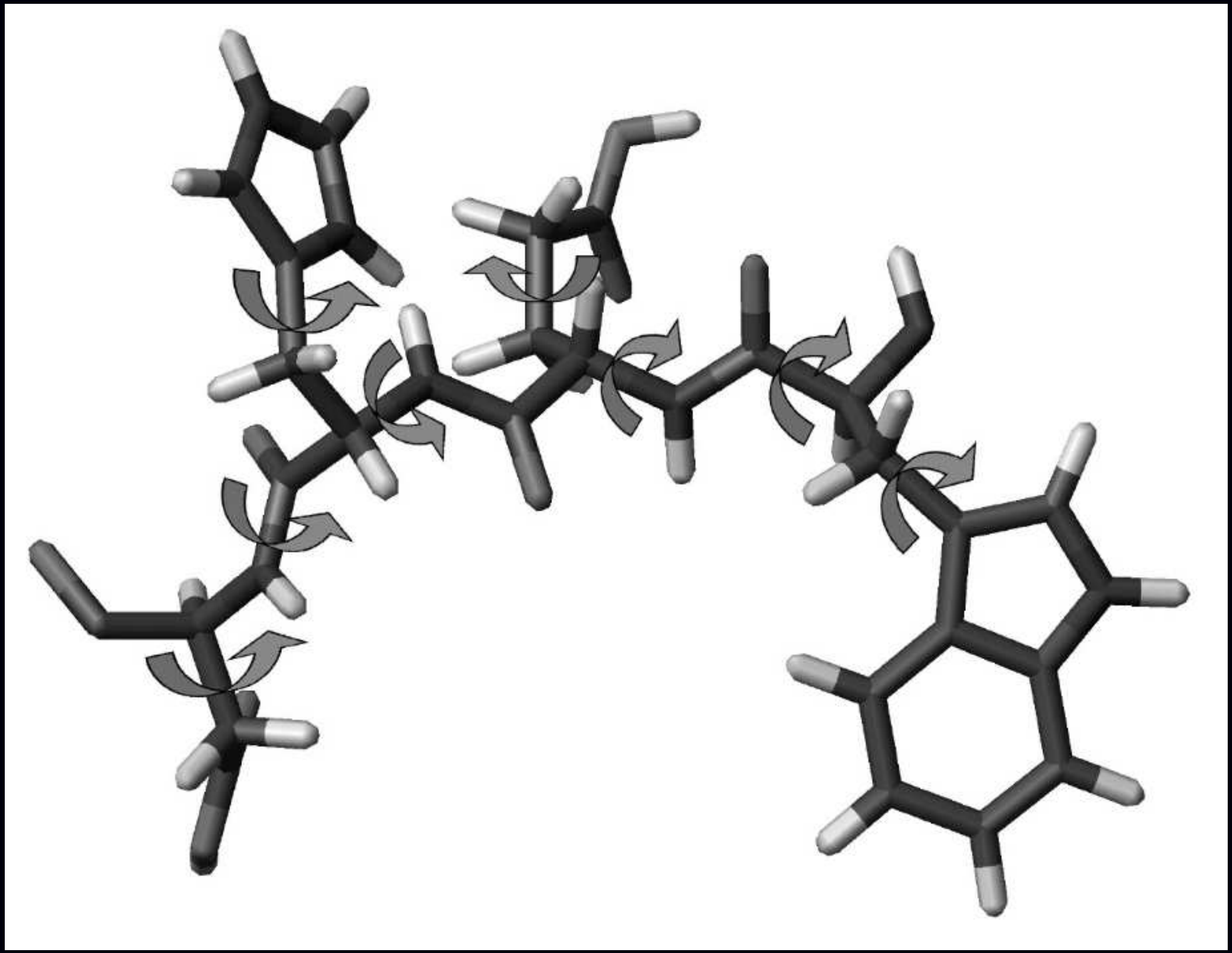
2. **A clearer boundary to NP-hardness for fewnomials** [Rojas, Stella]

3. **Breaking a complexity barrier for counting and approximating the roots of certain fewnomial systems**

   [Rojas, Ye: J. of Complexity, 2004]

APPLICATIONS OVER $\mathbb{R}$

Rational Drug Design...



n twist angles $\Longrightarrow$ $3n$ equations in $3n$ unknowns...

MORE APPLICATIONS OVER $\mathbb{R}$

• **Dynamical Systems:** Arnold's linearized version of Hilbert's 16th Problem [Khovanski, Varchenko 1984].

• **Torsion Points on Algebraic Curves:** Given any number field K, there is an explicit upper bound for the number of $x \in K \setminus \{0,1\}$ satisfying $x^a(1-x)^b = 1$ for some $(a,b) \in \mathbb{Z}^2$ [Cohen & Zannier, 2002].

• **Geometric Model Theory:** Model Completeness and o-minimality for the first order theory of $\langle \mathbb{R}, +, \cdot, -, 0, 1 \exp, < \rangle$ [Wilkie, 1996]

SHARPENING FEWNOMIAL THEORY $/\mathbb{R}$

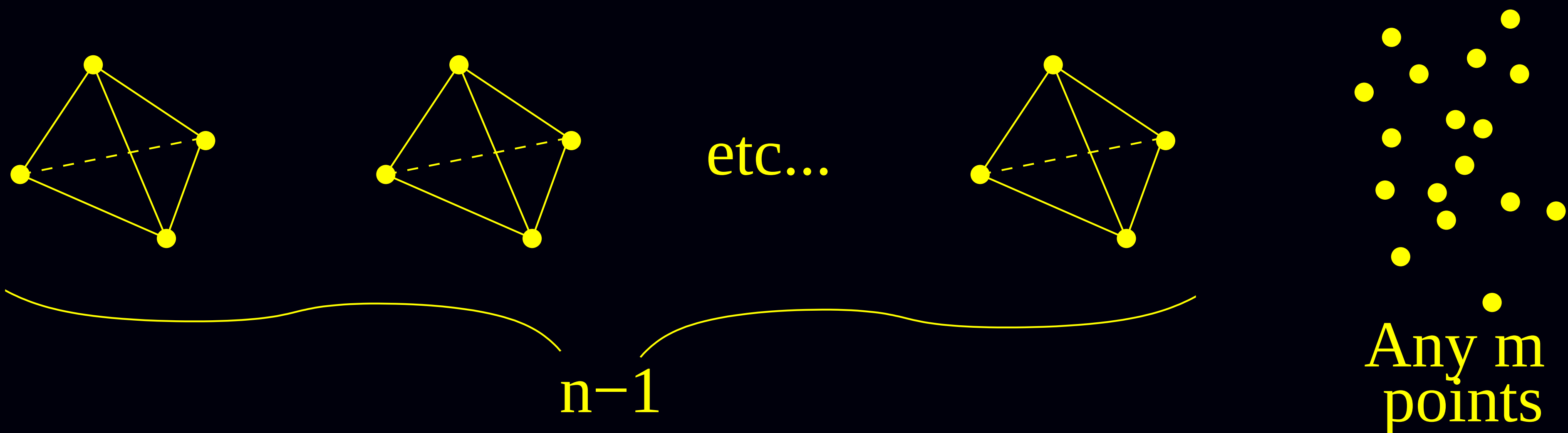
Main Theorem 1 Consider...

$$c_{1,0}x^{a_0} + \cdots + c_{1,n}x^{a_n}$$

$$\vdots$$

$$c_{n-1,0}x^{a_0} + \cdots + c_{n-1,n}x^{a_n}$$

$$c_{n,1}x^{b_1} \quad + \quad \cdots \quad + \quad c_{n,m}x^{b_m}$$



SHARPENING FEWNOMIAL THEORY $/\mathbb{R}$

Main Theorem 1 [Li-Rojas-Wang, DCG 2003]

$$\begin{array}{c} c_{1,0}x^{a_0}+\cdots+c_{1,n}x^{a_n} \\ \vdots \\ c_{n-1,0}x^{a_0}+\cdots+c_{n-1,n}x^{a_n} \\ c_{n,1}x^{b_1} \quad + \quad \cdots \quad + \quad c_{n,m}x^{b_m} \end{array}$$

has $\leq \boxed{\frac{n^m-n}{n-1}}$ isolated roots in $\mathbb{R}^n_+$, where $c_{i,j}\in\mathbb{R}$, $a_i, b_i \in \mathbb{R}^n$ (the a_i affinely independent), and $Z_+(f_1,\ldots,f_{n-1})$ smooth. Moreover...

when $(m,n)=(3,2)$, the maximum number is exactly 5. ■

COMPARISON $/\mathbb{R}$

[Khovanski, 1980+ε] **Suppose $f_1,\ldots,f_n \in \mathbb{R}[x^a \mid a \in \mathbb{R}^n]$ have a total of μ distinct exponent vectors in their monomial term expansions. Then $F := (f_1,\ldots,f_n)$ has $\leq (n+1)^{\mu-1} 2^{(\mu-1)(\mu-2)/2}$ non-degenerate roots in $\mathbb{R}^n_+$.**

COMPARISON $/\mathbb{R}$

[Khovanski, 1980+ε] Suppose $f_1,\ldots,f_n \in \mathbb{R}[x^a \mid a \in \mathbb{R}^n]$ have a total of μ distinct exponent vectors in their monomial term expansions. Then $F := (f_1,\ldots,f_n)$ has $\leq (n+1)^{\mu-1} 2^{(\mu-1)(\mu-2)/2}$ non-degenerate roots in $\mathbb{R}^n_+$.

Example 1: In the setting of Main Theorem 2, $\mu = m+n$ and Khovanski's bound is $2^{\Theta((m+n)^2)} \gg \Theta\left(n^{m-1}\right)$. So we get the first non-trivial improvement — a factor exponential in n — in close to 20 years.

COMPARISON $/\mathbb{R}$

[Khovanski, 1980+ε] Suppose $f_1, \ldots, f_n \in \mathbb{R}[x^a \mid a \in \mathbb{R}^n]$ have a total of μ distinct exponent vectors in their monomial term expansions. Then $F := (f_1, \ldots, f_n)$ has $\leq (n+1)^{\mu-1} 2^{(\mu-1)(\mu-2)/2}$ non-degenerate roots in $\mathbb{R}^n_+$.

Example 1: In the setting of Main Theorem 2, $\mu = m + n$ and Khovanski's bound is $2^{\Theta((m+n)^2)} \gg \Theta\left(n^{m-1}\right)$. So we get the first non-trivial improvement — a factor exponential in n — in close to 20 years.

Example 2: For 2 general trinomials, Khovanski's bound is 5184, while the correct tight bound is 5.

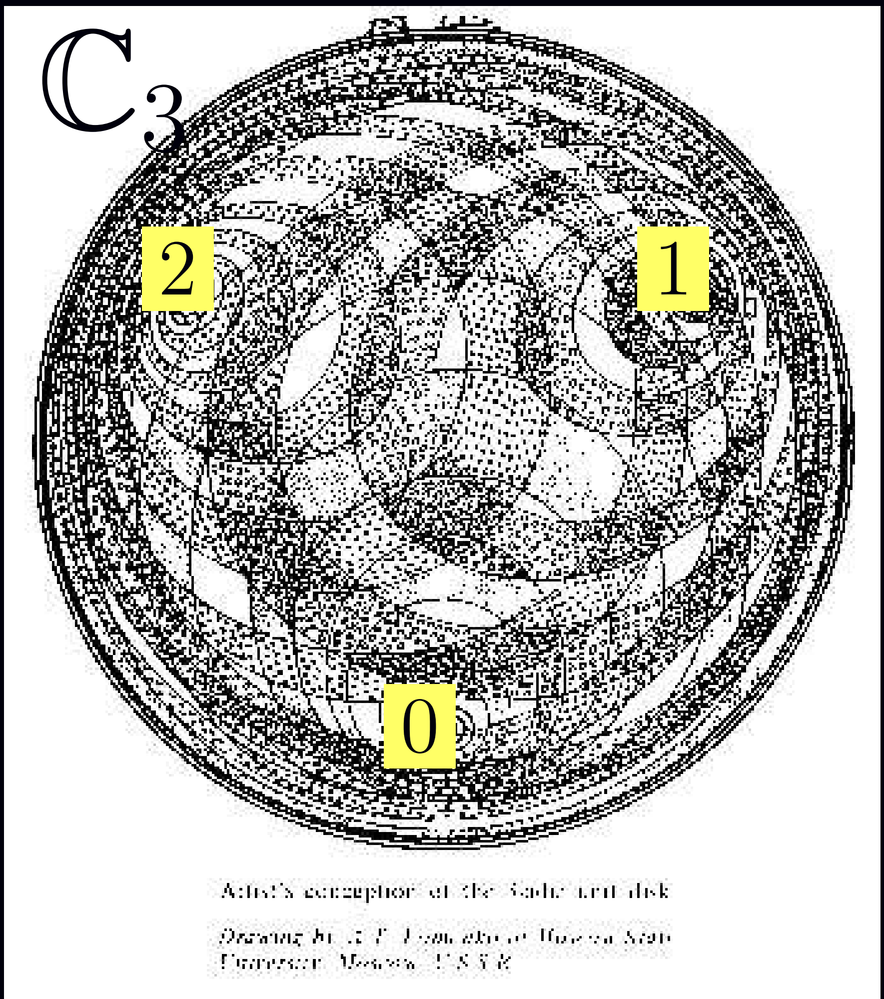
CONJECTURE

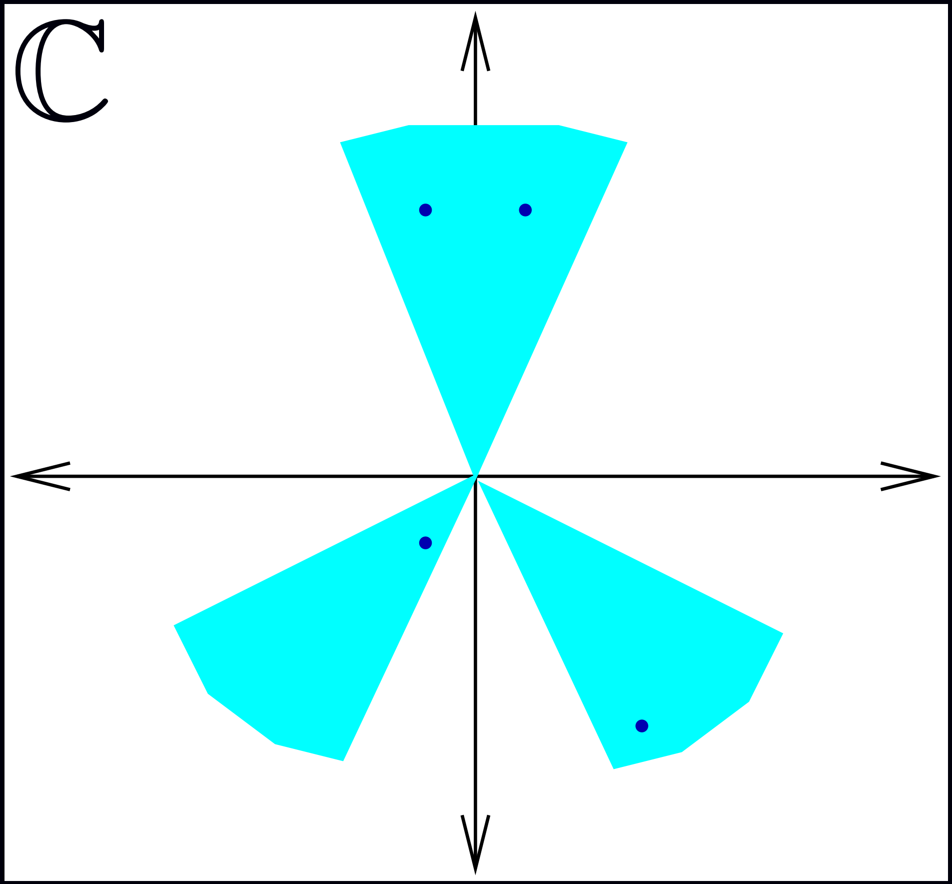
The maximal number of isolated roots in $\mathbb{R}_+^n$ of a μ-sparse $n \times n$ fewnomial system is $\mu^{O(n)}$.

"Meta"-Evidence: The analogue over $\mathbb{Q}_p$ is true! [Rojas, AJM 2004]

$\mathbb{C}$, $\mathbb{C}_p$, AND THE METAPHOR OF ANGLE

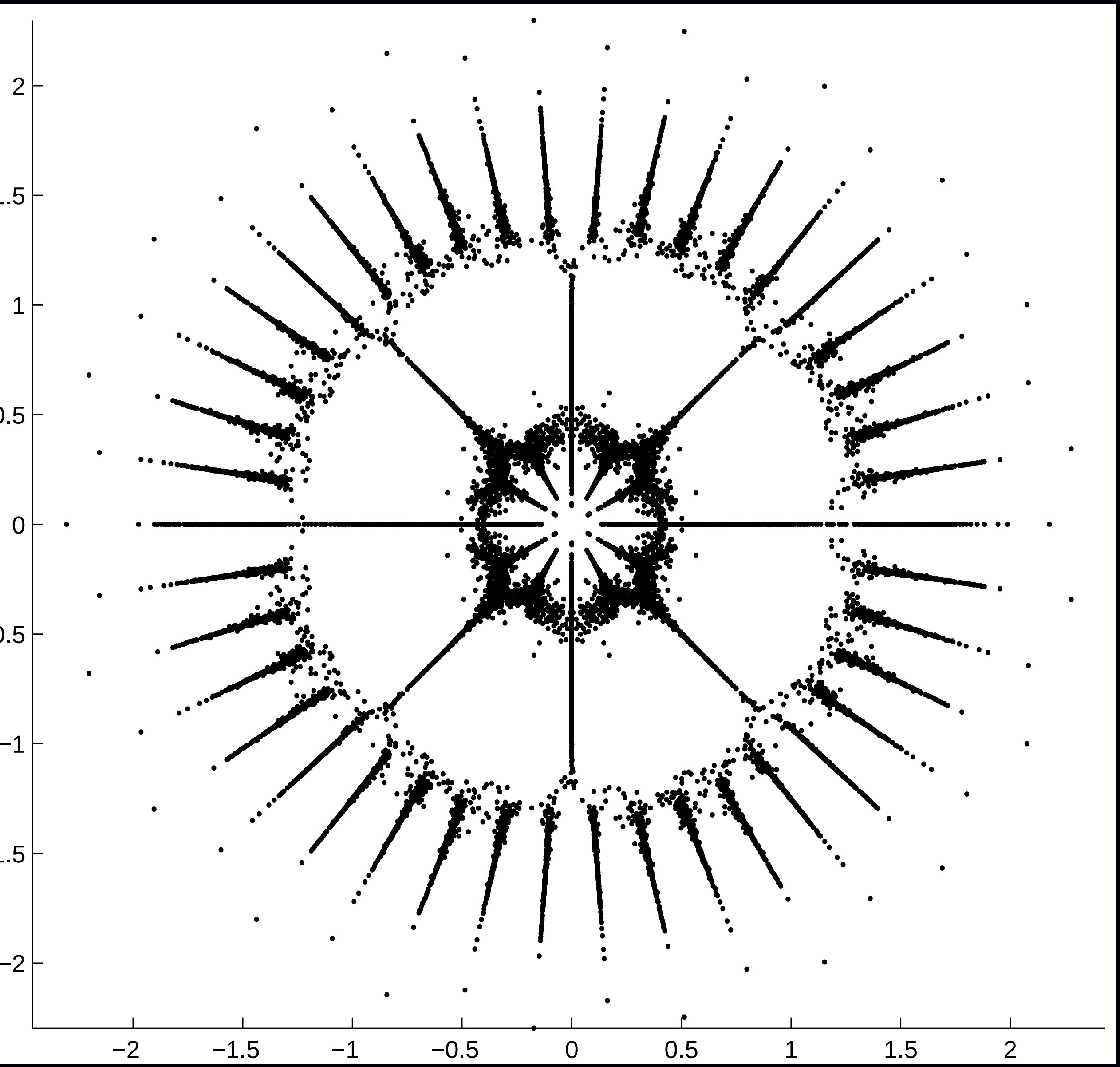
...curious reversal of real case: Khovanski extended his results to counting roots in an angular sector.





$n=1$: [Marc Voorhoeve, 1977]

1000 RANDOM TETRANOMIALS



$a + bx^6 + cx^{10} + dx^{31}$

with a, b, c, d real

indep. centered

Gaussians

Deviation from average number in a sector is very small...

DECIDING EXISTENCE...

Main Theorem 2 [Rojas-Stella, 2004]

For a μ-nomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$, deciding $Z_{\mathbb{R}}(f) \stackrel{?}{=} \emptyset$ is...

1. NP-hard for $\mu \geq 6(n+1)$.
2. in P for $\mu \leq n+1$ (generic exponents).

DECIDING EXISTENCE...

Main Theorem 2 [Rojas-Stella, 2004]

For a μ-nomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$, deciding $Z_{\mathbb{R}}(f) \stackrel{?}{=} \emptyset$ is...

1. NP-hard for $\mu \geq 6(n+1)$.
2. in P for $\mu \leq n+1$ (generic exponents).

E.g., $\text{size}(7x^D - 999y^{37} + 234xy^{12}z) = \Theta(\log D)$, and...

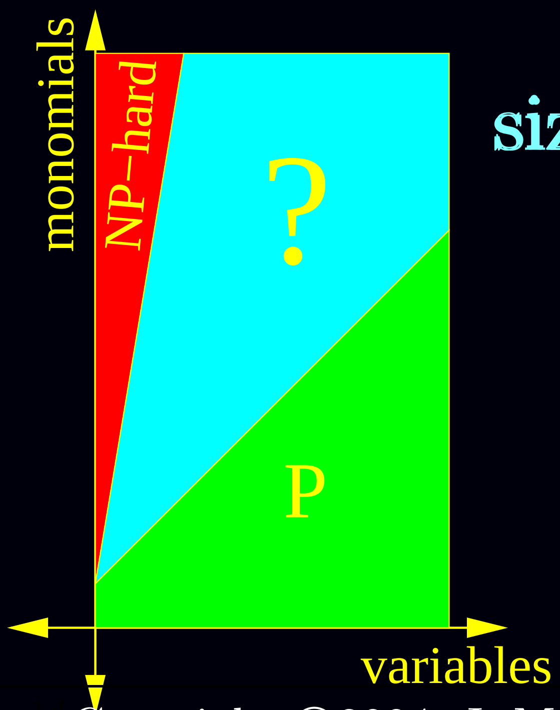
$\text{size}(\text{General Degree } D \text{ Polynomial}) = O(D^n \log D)\text{MaxBitSize}(\text{Coeff of } f)$

DECIDING EXISTENCE...

Main Theorem 2 [Rojas-Stella, 2004]

For a μ-nomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$, deciding $Z_{\mathbb{R}}(f) \stackrel{?}{=} \emptyset$ is...

1. **NP-hard for $\mu \geq 6(n+1)$.**
2. **in P for $\mu \leq n+1$ (generic exponents).**



size(f) := # of bits to write monomial term expansion

High degree is OK!

BEST EARLIER WORK?

1. Deciding $Z_{\mathbb{R}}(f) \stackrel{?}{=} \emptyset$ for a μ-nomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$ is NP-hard for $\mu \geq \frac{13}{3}n^3 - 13n^2 + \frac{26}{3}n + 1$ [Anon, 1980's]. (Fixed n still open, even for $n = 1$!)

2. ...

BEST EARLIER WORK?

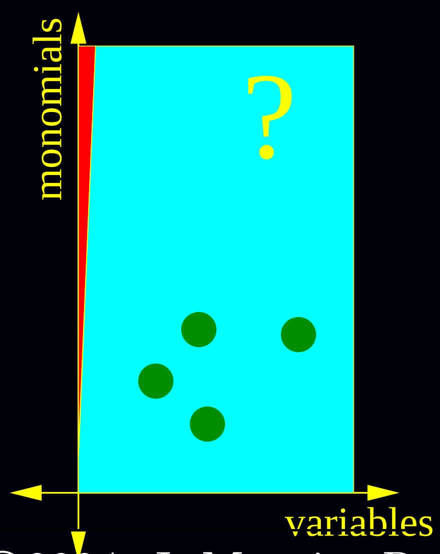
1. Deciding $Z_{\mathbb{R}}(f) \stackrel{?}{=} \emptyset$ for a μ-nomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$ is NP-hard for $\mu \geq \frac{13}{3}n^3 - 13n^2 + \frac{26}{3}n + 1$ [Anon, 1980's]. (Fixed n still open, even for $n=1$!)

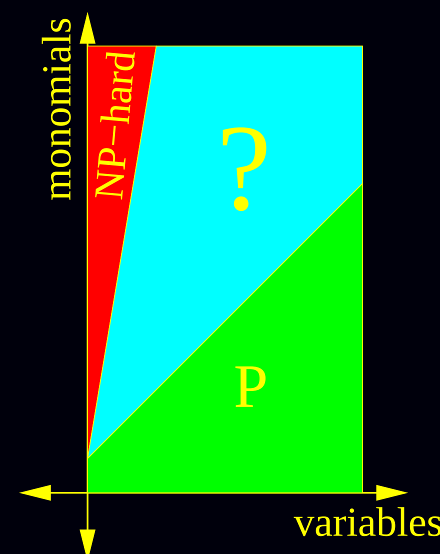
2. Deciding $Z_{\mathbb{R}}(f) \stackrel{?}{=} \emptyset$ for a quadratic $f \in \mathbb{Z}[x_1, \ldots, x_n]$ is in P. (A special case of $\mu = O(n^2)$...) [Barvinok, 1990's; Grigoriev-deKlerk-Pasechnik, 2002]

BEST EARLIER WORK?

1. Deciding $Z_{\mathbb{R}}(f) \stackrel{?}{=} \emptyset$ for a μ-nomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$ is NP-hard for $\mu \geq \frac{13}{3}n^3 - 13n^2 + \frac{26}{3}n + 1$ [Anon, 1980's]. (Fixed n still open, even for $n=1$!)

2. Deciding $Z_{\mathbb{R}}(f) \stackrel{?}{=} \emptyset$ for a quadratic $f \in \mathbb{Z}[x_1, \ldots, x_n]$ is in P. (A special case of $\mu = O(n^2)$...) [Barvinok, 1990's; Grigoriev-deKlerk-Pasechnik, 2002]





COUNTING AND SOLVING?

Main Theorem 3 **For any μ-nomial $f \in \mathbb{R}[x_1]$, of degree D, we can do the following:**

1. With probability $\geq 1 - \varepsilon$, count exactly the number of real roots of f, using just $O\left(\frac{1}{\varepsilon}\mu \log D\right)$ arithmetic operations. Furthermore, for $\mu \leq 3$, $O(\log^2 D)$ suffices for an exact count.

2. ...

COUNTING AND SOLVING?

Main Theorem 3 **For any μ-nomial $f \in \mathbb{R}[x_1]$, of degree D, we can do the following:**

1. With probability $\geq 1 - \varepsilon$, count exactly the number of real roots of f, using just $O\left(\frac{1}{\varepsilon}\mu \log D\right)$ arithmetic operations. Furthermore, for $\mu \leq 3$, $O(\log^2 D)$ suffices for an exact count.

2. [Rojas-Ye, J. of Complexity, 2004] ε-approximate all the roots in $[0, R]$ of a trinomial, using just $O\left(\log(D) \log\left(D \log \frac{R}{\varepsilon}\right)\right)$ arithmetic operations. ■

BEST EARLIER WORK?

1. Counting the number of roots in $[0, R]$ for a general $f \in \mathbb{R}[x_1]$ of degree D takes $\Omega(D \log D)$ arithmetic operations [Lickteig & Roy, 2000], and evaluating already requires $\Omega(m \log D)$.

2. ...

BEST EARLIER WORK?

1. Counting the number of roots in $[0, R]$ for a general $f \in \mathbb{R}[x_1]$ of degree D takes $\Omega(D \log D)$ arithmetic operations [Lickteig & Roy, 2000], and evaluating already requires $\Omega(m \log D)$.

2. ε-approximating all the roots in $\{z \in \mathbb{C} \mid |z| \leq R\}$ of a general $f \in \mathbb{C}[x_1]$ of degree D can be done using just $O\left(D \log^5 D \log\log \frac{R}{\varepsilon}\right)$ arithmetic operations [Neff, Reif, 1996]...

BEST EARLIER WORK?

1. Counting the number of roots in $[0, R]$ for a general $f \in \mathbb{R}[x_1]$ of degree D takes $\Omega(D \log D)$ arithmetic operations [Lickteig & Roy, 2000], and evaluating already requires $\Omega(m \log D)$.

2. ...and approximating square roots within ε already requires at least $\Omega\left(\log\log\frac{1}{\varepsilon}\right)$ arithmetic operations [Bshouty, Mansour, Schieber, & Tiwari, 1997].

♡ Thank you for listening!

- E-mail: rojas@math.tamu.edu

- Please see...
  www.math.tamu.edu/~rojas
  for on-line papers and further information...