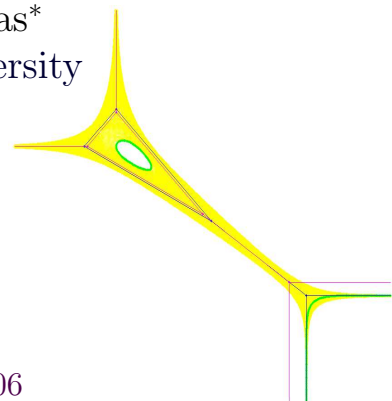
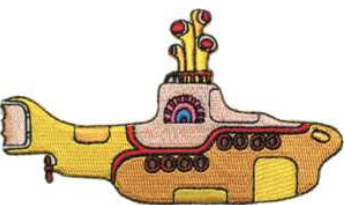


On the Effectiveness of Number Theory in Algorithmic Geometry

J. Maurice Rojas*
Texas A&M University



September 20, 2006

* Partially supported by NSF CAREER grant DMS-0349309.

OUTLINE

How hard is it to decide whether...

- ...a **complex** algebraic set is non-empty?
- ...an algebraic set has a point whose coordinates are complex **roots of unity**, of given order?
- ...a **real** algebraic set is non-empty?

We'll see...

- motivation, examples, algorithms, and upper and lower complexity bounds
- connections to analytic number theory

⁵©J. Maurice Rojas

NP VIA FINITE FIELDS

Would you rather...

- (a) ask your Mom to **decide** a given case of $\mathbf{FEAS}_{\mathbb{F}_2}$?
- or
- (b) ask your Mom to **verify** a given “Yes” instance of $\mathbf{FEAS}_{\mathbb{F}_2}$?

(You should say (b).)

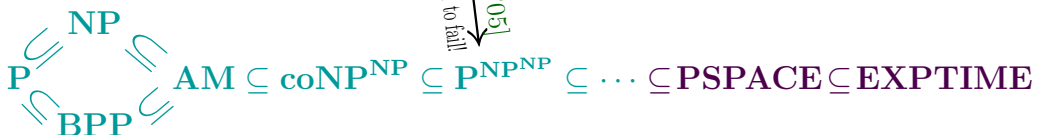
$\mathbf{NP} :=$ Those decision problems where “Yes” always admits a certificate verifiable in \mathbf{P}
 = Decision problems “as hard” as $\mathbf{FEAS}_{\mathbb{F}_2}$

MOTIVATION

- $\mathbf{FEAS}_{\mathbb{C}} :=$ “Decide whether an input system of polynomials in $\mathbb{Z}[x_1, \dots, x_n]$ has a root in \mathbb{C}^n .”

$\mathbf{FEAS}_{\mathbb{C}}$

\subseteq
 [Rojas, '05]
 OK for GRH to fail!



NP VIA KNOT THEORY

Would you rather...

(a) ask your Mom to **decide** a given case of **FEAS \mathbb{F}_2** ?

or

(b) ask your Mom to **verify** a given ‘‘Yes’’ instance of **FEAS \mathbb{F}_2** ?

(You should say (b).)

NP := Those decision problems where ‘‘Yes’’ always admits a certificate verifiable in **P**

= Decision problems ‘‘as hard’’ as **deciding whether a polygonal knot in a 3-manifold* \mathfrak{M} has genus $\leq g$** [Agol-Hass-Thurston, 2006].

\supseteq Knottedness! (via $\mathfrak{M} = S^3$ and $g=0$)

¹⁹©J. Maurice Rojas

*triangulated, compact, and orientable

A SPECIAL CASE OF FEAS \mathbb{C}

TorsionPoint: Given $f_1, \dots, f_k \in \mathbb{Z}[x_1, \dots, x_n]$ and $D_1, \dots, D_n \in \mathbb{N}$, decide whether $f_1(x) = \dots = f_k(x) = x_1^{D_1} - 1 = \dots = x_n^{D_n} - 1 = 0$ has a root in \mathbb{C}^n . \diamond

- ... $k=n=1$ case: deciding whether $\text{Res}(f_1(x_1), x_1^D - 1)$ (a.k.a. a **cyclic resultant**) vanishes.
- ...when $k = n = 1$, recovering f_1 from its cyclic resultant is important in dynamical systems and knot theory [Hillar, 2004].
- ...for $k=1, n \geq 1$, similar (but \neq !) to detecting whether the **(Archimedean) amoeba** of f_1 contains the origin.

²⁴©J. Maurice Rojas

BACKGROUND: NP

Would you rather...

(a) ask your Mom to **decide** a given case of **FEAS \mathbb{F}_2** ?

or

(b) ask your Mom to **verify** a given ‘‘Yes’’ instance of **FEAS \mathbb{F}_2** ?

(You should say (b).)

NP := Those decision problems where ‘‘Yes’’ always admits a certificate verifiable in **P**

= Decision problems ‘‘as hard’’ as **FEAS \mathbb{F}_2**

NP-hard:= ‘‘at least as hard’’ as any problem in **NP**.

NP-complete:= **NP-hard** and in **NP**.

²⁰©J. Maurice Rojas

TorsionPoint \subseteq FEAS \mathbb{C}

TorsionPoint: Given $f_1, \dots, f_k \in \mathbb{Z}[x_1, \dots, x_n]$ and $D_1, \dots, D_n \in \mathbb{N}$, decide whether $f_1(x) = \dots = f_k(x) = x_1^{D_1} - 1 = \dots = x_n^{D_n} - 1 = 0$ has a root in \mathbb{C}^n . \diamond

- Torsion points on a given algebraic sets have a **very** special distribution: they lie on a finite union of **translated subtori** [Chabauty '38, Laurent '84 Ruppert '93, Bombieri-Zannier '95, Remond '02].
- For $k = n = 1$, and **complex** coefficients, [Tao, '03; Meshulam, '06] gave a ‘‘Descartes-like’’ bound for roots of unity.

²⁶©J. Maurice Rojas

TorsionPoint ⊆ FEAS_ℂ

TorsionPoint: Given $f_1, \dots, f_k \in \mathbb{Z}[x_1, \dots, x_n]$ and $D_1, \dots, D_n \in \mathbb{N}$, decide whether $f_1(x) = \dots = f_k(x) = x_1^{D_1} - 1 = \dots = x_n^{D_n} - 1 = 0$ has a root in \mathbb{C}^n . ◊

- Torsion points on a given algebraic sets have a **very** special distribution: they lie on a finite union of **translated subtori** [Chabauty '38, Laurent '84 Ruppert '93, Bombieri-Zannier '95, Remond '02].
- Given the refined structure of torsion points, can we solve **TorsionPoint** in **P**? i.e., within a number of bit operations polynomial in $\sum_{i=1}^k \text{size}(f_i) + \sum_{i=1}^k \text{size}(D_i)$?
- **TorsionPoint**(\mathcal{F}) := "...restriction of **TorsionPoint** to inputs in \mathcal{F} ."

²⁸©J. Maurice Rojas

COMPLEXITY OF TorsionPoint

For $k=n=1$, the best current techniques employing **resultants** (or **Gröbner bases**) yield complexity upper bounds no better than $O((\text{deg}(f_1) + D_1 + \max \log \text{Coefficient})^{1+o(1)})$.

...AND the following new upper bound:

Theorem 1 [Rojas, 2006]

1. Unconditionally, **TorsionPoint**($\mathbb{Z}[x_1]$) ∈ **NP^{NP}**
2. Assuming **APH**, **TorsionPoint** ∈ **AM**. ■



³³©J. Maurice Rojas

COMPLEXITY OF TorsionPoint

For $k=n=1$, the best current techniques employing **resultants** (or **Gröbner bases**) yield complexity upper bounds no better than $O((\text{deg}(f_1) + D_1 + \max \log \text{Coefficient})^{1+o(1)})$.

We also have the following lower bound:

Plaisted's Theorem ('84) **TorsionPoint**($\mathbb{Z}[x_1]$) is **NP-hard**. ■

...in particular, **TorsionPoint**($\mathbb{Z}[x_1]$) ∈ **P** ⇒ **P = NP!**

³¹©J. Maurice Rojas

COMPLEXITY OF TorsionPoint

For $k=n=1$, the best current techniques employing **resultants** (or **Gröbner bases**) yield complexity upper bounds no better than $O((\text{deg}(f_1) + D_1 + \max \log \text{Coefficient})^{1+o(1)})$.

...AND the following new upper bound:

Theorem 1 [Rojas, 2006]

1. Unconditionally, **TorsionPoint**($\mathbb{Z}[x_1]$) ∈ **NP^{NP}**
2. Assuming **APH**, **TorsionPoint** ∈ **AM**. ■

So, assuming **APH**, **TorsionPoint** ∉ **P** ⇒ **P ≠ NP!**
(and, unconditionally, **TorsionPoint**($\mathbb{Z}[x_1]$) ⇒ **P ≠ NP!**)

³⁵©J. Maurice Rojas

COMPLEXITY OF TorsionPoint

For $k=n=1$, the best current techniques employing **resultants** (or **Gröbner bases**) yield complexity upper bounds no better than $O((\deg(f_1) + D_1 + \max \log \text{Coefficient})^{1+o(1)})$.

...AND the following new upper bound:

Theorem 1 [Rojas, 2006]

1. Unconditionally, $\text{TorsionPoint}(\mathbb{Z}[x_1]) \in \mathbf{NP}^{\mathbf{NP}}$
2. Assuming APH, $\text{TorsionPoint} \in \mathbf{AM}$. ■

More concretely, the underlying algorithms appear to be practical. Also, the algorithm is **number-theoretic**, and **totally** different from the usual commutative algebra/homotopy techniques. So let's review a little number theory first...

³⁸©J. Maurice Rojas

PRIMES IN ARITHMETIC PROGRESSION

Fact: [[Iwaniec-Kowalski, '03](#)] A (uniformly) random number chosen from $\{M+1, 2M+1, \dots, xM+1\}$ is **prime** with **probability** $\geq \frac{1}{\log x}$, for $x \geq M^{O(1)}$. ■

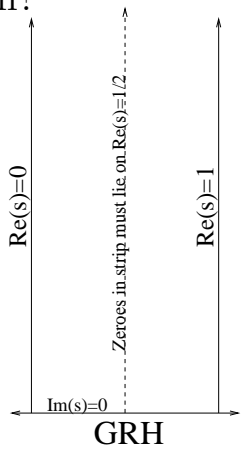
Is $\log^{O(1)} M$ already good enough?

GRH for cyclotomic fields $\supseteq \dots$

$$\bigcup$$

For all M , $\zeta_{Q(\omega_M)}(s) := \sum_{\mathfrak{a} \text{ an ideal of } \mathbb{Z}[\omega_M]} \frac{1}{(\mathcal{N}\mathfrak{a})^s}$

$\implies x = \Omega(\log M)$ is good enough!



⁴⁴©J. Maurice Rojas

PRIMES IN ARITHMETIC PROGRESSION

Observe that a (uniformly) random number chosen from $\{4849845 + 1, 2 \cdot 4849845 + 1, \dots, x \cdot 4849845 + 1\}$ is **prime** with (apparent) **probability** $\geq \frac{1}{\log x}$, for $x \geq 42$ ($\approx 3 \log 4849845$)...

The probability is in fact $\geq \frac{1}{\log x}$, for all $x \gg 0$, so...

When exactly does this density kick in?!

⁴¹©J. Maurice Rojas

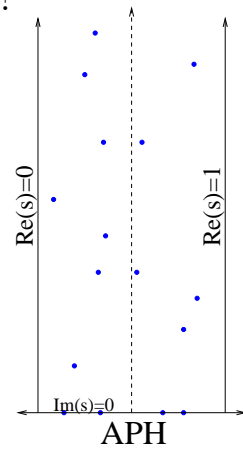
PRIMES IN ARITHMETIC PROGRESSION

Fact: [[Iwaniec-Kowalski, '03](#)] A (uniformly) random number chosen from $\{M+1, 2M+1, \dots, xM+1\}$ is **prime** with **probability** $\geq \frac{1}{\log x}$, for $x \geq M^{O(1)}$. ■

Is $\log^{O(1)} M$ already good enough?

APH: There is an absolute $C \geq 1$ such that for any $n, M \in \mathbb{N}$ with $n \geq 2^{\log^C \log M}$, the set $\{1 + kM \mid k \in \{1, \dots, 2^{n^C}\}\}$ contains at least $\frac{2^{n^C}}{n}$ primes.

So APH can still hold under bad failures of GRH!



⁴⁵©J. Maurice Rojas

ALGORITHM 1

(For TorsionPoint in general, assuming APH)

Input: $F \in (\mathbb{Z}[x_1, \dots, x_n])^k$ and $d_1, \dots, d_n \in \mathbb{N}$.

Output: A true declaration of whether $Z(f_1, \dots, f_k)$ contains a $\zeta = (\zeta_1, \dots, \zeta_n)$ with $\zeta_i^{d_i} = 1 \forall i$.

Description:

1. Let S be the total input size and $J = \Theta(S^C)$ and $M := \text{lcm}\{d_1, \dots, d_n\} \max\{\sum_i |f_i|_1, \max_i \{1 + \deg f_i\}\}$.
2. Pick no more than $6J$ random $j \in \{1, \dots, 2^{J^C}\}$ until one either has $q := jM + 1$ prime, or $6J$ such numbers that are all composite. In the latter case, stop and output ‘‘I HAVE FAILED. PLEASE FORGIVE ME.’’.
3. Nondeterministically, decide whether the mod q reduction of $F(x) = x_1^{d_1} - 1 = \dots = x_n^{d_n} - 1 = 0$ has a root in $(\mathbb{Z}/q\mathbb{Z})^n$.
4. If there is such a solution then stop and output ‘‘YES.’’. Otherwise, stop and output ‘‘NO.’’. ■

⁵⁰©J. Maurice Rojas

EXAMPLE

Is there a pair of 4849845th roots of unity, (x, y) , such that*

$$\begin{aligned}
& 2 - x^{285285} + x^{969969} + x^{3879876} + x^{1939938} + x^{2909907} + y^{255255} + y^{4594590} + y^{4084080} + y^{4339335} + y^{3828825} \\
& + y^{3573570} + y^{3318315} + y^{3063060} + y^{2807805} + y^{2552550} + y^{2297295} + y^{2042040} + y^{1786785} + y^{1531530} + y^{1276275} \\
& + y^{1021020} + y^{765765} + y^{510510} + y^{255255} x^{2909907} + y^{765765} x^{969969} + y^{510510} x^{3879876} + y^{4594590} x^{3879876} \\
& + y^{4594590} x^{2909907} + y^{4594590} x^{1939938} + y^{4594590} x^{969969} + y^{4339335} x^{3879876} + y^{4339335} x^{2909907} \\
& + y^{4339335} x^{1939938} + y^{4339335} x^{969969} + y^{4084080} x^{3879876} + y^{4084080} x^{2909907} + y^{4084080} x^{1939938} \\
& + y^{4084080} x^{969969} + y^{3828825} x^{3879876} + y^{3828825} x^{2909907} + y^{3828825} x^{1939938} + y^{3828825} x^{969969} \\
& + y^{3573570} x^{3879876} + y^{3573570} x^{2909907} + y^{3573570} x^{1939938} + y^{3573570} x^{969969} + y^{3318315} x^{3879876} \\
& + y^{3318315} x^{2909907} + y^{3318315} x^{1939938} + y^{3318315} x^{969969} + y^{3063060} x^{3879876} + y^{3063060} x^{2909907} \\
& + y^{3063060} x^{1939938} + y^{3063060} x^{969969} + y^{2807805} x^{3879876} + y^{2807805} x^{2909907} + y^{2807805} x^{1939938} \\
& + y^{2807805} x^{969969} + y^{2552550} x^{3879876} + y^{2552550} x^{2909907} + y^{2552550} x^{1939938} + y^{2552550} x^{969969} \\
& + y^{2297295} x^{3879876} + y^{2297295} x^{2909907} + y^{2297295} x^{1939938} + y^{2297295} x^{969969} + y^{2042040} x^{3879876} \\
& + y^{2042040} x^{2909907} + y^{2042040} x^{1939938} + y^{2042040} x^{969969} + y^{1786785} x^{3879876} + y^{1786785} x^{2909907} \\
& + y^{1786785} x^{1939938} + y^{1786785} x^{969969} + y^{1531530} x^{3879876} + y^{1531530} x^{2909907} + y^{1531530} x^{1939938} \\
& + y^{1531530} x^{969969} + y^{1276275} x^{3879876} + y^{1276275} x^{2909907} + y^{1276275} x^{1939938} + y^{1276275} x^{969969} \\
& + y^{1021020} x^{3879876} + y^{1021020} x^{2909907} + y^{1021020} x^{1939938} + y^{1021020} x^{969969} + y^{510510} x^{2909907} + y^{510510} x^{969969} \\
& + y^{510510} x^{1939938} + y^{510510} x^{969969} + y^{765765} x^{3879876} + y^{765765} x^{2909907} + y^{765765} x^{1939938} + y^{765765} x^{969969} \\
& + y^{255255} x^{2909907} + y^{255255} x^{1939938} + y^{255255} x^{969969}
\end{aligned}$$

AND

$$\begin{aligned}
& -2 + x^{2552550} y^{285285} + x^{1786785} y^{285285} - x^{255255} x^{4594590} - x^{4084080} - x^{4339335} - x^{3828825} - x^{3573570} \\
& - x^{3318315} - x^{3063060} - x^{2807805} - x^{2552550} - x^{2297295} - x^{2042040} - x^{1531530} - x^{1276275} - x^{1021020} - x^{1786785} \\
& - x^{765765} - x^{510510} - 18 y^{4849845} + y^{285285} - 3 y^{969969} - 15 y^{3879876} - 6 y^{1939938} - 10 y^{2909907} + x^{4594590} y^{285285} \\
& + x^{4339335} y^{285285} + x^{4084080} y^{285285} + x^{3828825} y^{285285} + x^{3573570} y^{285285} + x^{3318315} y^{285285} + x^{3063060} y^{285285} \\
& + x^{2807805} y^{285285} + x^{2297295} y^{285285} + x^{2042040} y^{285285} + x^{1531530} y^{285285} + x^{1276275} y^{285285} + x^{1021020} y^{285285} \\
& + x^{765765} y^{285285} + x^{510510} y^{285285} + x^{255255} y^{285285} - 15 y^{7759752} - 18 y^{6789783} - 19 y^{5819814} - 10 y^{8729721} \\
& - y^{11639628} - 3 y^{10669659} - 6 y^{9699690}
\end{aligned}$$

both vanish?

On the other hand, trying to compute the resultant of $(f, g, x^{4849845} - 1)$ takes awfully long...

⁵⁴©J. Maurice Rojas

*...even after reduction, the respective degrees are 8474466 and 4879875.

EXAMPLE

Is there a pair of 4849845th roots of unity, (x, y) , such that*

$$\begin{aligned}
& 2 - x^{285285} + x^{969969} + x^{3879876} + x^{1939938} + x^{2909907} + y^{255255} + y^{4594590} + y^{4084080} + y^{4339335} + y^{3828825} \\
& + y^{3573570} + y^{3318315} + y^{3063060} + y^{2807805} + y^{2552550} + y^{2297295} + y^{2042040} + y^{1786785} + y^{1531530} + y^{1276275} \\
& + y^{1021020} + y^{765765} + y^{510510} + y^{255255} x^{2909907} + y^{765765} x^{969969} + y^{510510} x^{3879876} + y^{4594590} x^{3879876} \\
& + y^{4594590} x^{2909907} + y^{4594590} x^{1939938} + y^{4594590} x^{969969} + y^{4339335} x^{3879876} + y^{4339335} x^{2909907} \\
& + y^{4339335} x^{1939938} + y^{4339335} x^{969969} + y^{4084080} x^{3879876} + y^{4084080} x^{2909907} + y^{4084080} x^{1939938} \\
& + y^{4084080} x^{969969} + y^{3828825} x^{3879876} + y^{3828825} x^{2909907} + y^{3828825} x^{1939938} + y^{3828825} x^{969969} \\
& + y^{3573570} x^{3879876} + y^{3573570} x^{2909907} + y^{3573570} x^{1939938} + y^{3573570} x^{969969} + y^{3318315} x^{3879876} \\
& + y^{3318315} x^{2909907} + y^{3318315} x^{1939938} + y^{3318315} x^{969969} + y^{3063060} x^{3879876} + y^{3063060} x^{2909907} \\
& + y^{3063060} x^{1939938} + y^{3063060} x^{969969} + y^{2807805} x^{3879876} + y^{2807805} x^{2909907} + y^{2807805} x^{1939938} \\
& + y^{2807805} x^{969969} + y^{2552550} x^{3879876} + y^{2552550} x^{2909907} + y^{2552550} x^{1939938} + y^{2552550} x^{969969} \\
& + y^{2297295} x^{3879876} + y^{2297295} x^{2909907} + y^{2297295} x^{1939938} + y^{2297295} x^{969969} + y^{2042040} x^{3879876} \\
& + y^{2042040} x^{2909907} + y^{2042040} x^{1939938} + y^{2042040} x^{969969} + y^{1786785} x^{3879876} + y^{1786785} x^{2909907} \\
& + y^{1786785} x^{1939938} + y^{1786785} x^{969969} + y^{1531530} x^{3879876} + y^{1531530} x^{2909907} + y^{1531530} x^{1939938} \\
& + y^{1531530} x^{969969} + y^{1276275} x^{3879876} + y^{1276275} x^{2909907} + y^{1276275} x^{1939938} + y^{1276275} x^{969969} \\
& + y^{1021020} x^{3879876} + y^{1021020} x^{2909907} + y^{1021020} x^{1939938} + y^{1021020} x^{969969} + y^{510510} x^{2909907} + y^{510510} x^{969969} \\
& + y^{510510} x^{1939938} + y^{510510} x^{969969} + y^{765765} x^{3879876} + y^{765765} x^{2909907} + y^{765765} x^{1939938} + y^{765765} x^{969969} \\
& + y^{255255} x^{2909907} + y^{255255} x^{1939938} + y^{255255} x^{969969}
\end{aligned}$$

AND

$$\begin{aligned}
& -2 + x^{2552550} y^{285285} + x^{1786785} y^{285285} - x^{255255} x^{4594590} - x^{4084080} - x^{4339335} - x^{3828825} - x^{3573570} \\
& - x^{3318315} - x^{3063060} - x^{2807805} - x^{2552550} - x^{2297295} - x^{2042040} - x^{1531530} - x^{1276275} - x^{1021020} - x^{1786785} \\
& - x^{765765} - x^{510510} - 18 y^{4849845} + y^{285285} - 3 y^{969969} - 15 y^{3879876} - 6 y^{1939938} - 10 y^{2909907} + x^{4594590} y^{285285} \\
& + x^{4339335} y^{285285} + x^{4084080} y^{285285} + x^{3828825} y^{285285} + x^{3573570} y^{285285} + x^{3318315} y^{285285} + x^{3063060} y^{285285} \\
& + x^{2807805} y^{285285} + x^{2297295} y^{285285} + x^{2042040} y^{285285} + x^{1531530} y^{285285} + x^{1276275} y^{285285} + x^{1021020} y^{285285} \\
& + x^{765765} y^{285285} + x^{510510} y^{285285} + x^{255255} y^{285285} - 15 y^{7759752} - 18 y^{6789783} - 19 y^{5819814} - 10 y^{8729721} \\
& - y^{11639628} - 3 y^{10669659} - 6 y^{9699690}
\end{aligned}$$

both vanish?

A suitable random q is 106696591 = 22 · 4849845 + 1. Moreover, a suitable $(x, y) \in \mathbb{F}_q^2$ is (75770298, 4468374).

⁵³©J. Maurice Rojas

*...even after reduction, the respective degrees are 8474466 and 4879875.

ALGORITHMIC LANG CONJECTURE?

That torsion points on algebraic sets have a special distribution (Laurent’s Theorem) is really just the $(\mathbb{C}^*)^n$ case of Lang’s Conjecture. The Abelian variety case contains the Faltings-Mordell Theorem as a special case.

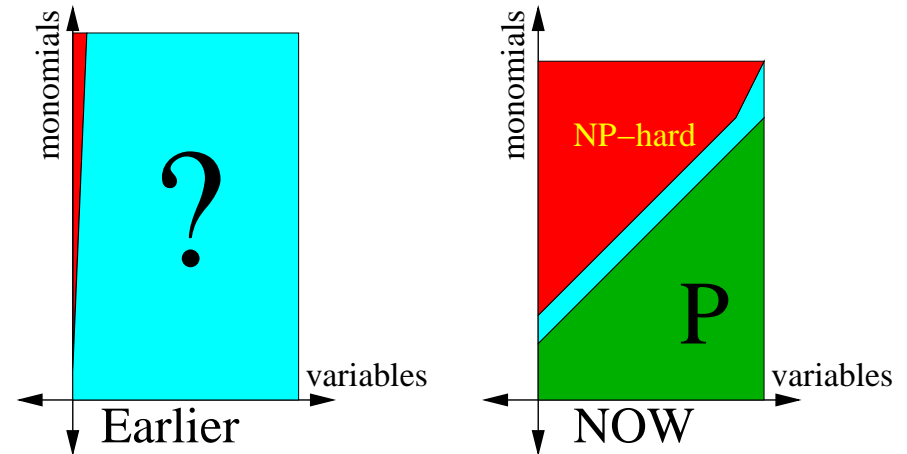
Ruppert, Bombieri, and Zannieri have found quantitative versions of Laurent’s Theorem, and we now have an algorithmic analogue.

Can we do the same for semi-Abelian varieties?

⁵⁸©J. Maurice Rojas

FINAL MAIN RESULT...

The complexity of deciding whether a polynomial in n variables (with exactly $n+k$ monomial terms) has a real root, can be summarized as follows:



⁶¹©J. Maurice Rojas

MOTIVATING PUZZLE

Given positive numbers c and D , how many bit operations does it take to decide if

$$1 + (c + 71)x^{6D} + 3y^{6D^2} - c^2x^Dy^Dz^D + 2006z^{4D^3}$$

has a real root?

1. This puzzle was **completely open** until 2005.

2. Many applications:

...quantifier elimination [Basu-Pollack-Roy, '03],
robotics (via road-maps of semi-algebraic sets) [Canny '87],
computing homology [Basu, '02],...

⁶⁶©J. Maurice Rojas

Let's now switch from \mathbb{C} to \mathbb{R} ...

⁵⁹©J. Maurice Rojas

MOTIVATING PUZZLE

Given positive numbers c and D , how many bit operations does it take to decide if

$$1 + (c + 71)x^{6D} + 3y^{6D^2} - c^2x^Dy^Dz^D + 2006z^{4D^3}$$

has a real root?

WHY DO WE CARE?

⁶³©J. Maurice Rojas

HISTORY

Given positive numbers c and D , how many bit operations does it take to decide if

$$1 + (c + 71)x^{6D} + 3y^{6D^2} - c^2x^Dy^Dz^D + 2006z^{4D^3}$$

has a real root?

[Tarski, ≤1948] Some function of c and D .

[Collins, ≤1975] $2^{O(c+D)}$.

[Chistov, Grigoriev, ≤1984] $(D + c)^{O(1)}$.

[Basu, Pollack, Roy, ≤1994] $(D + \log c)^{O(1)}$.

[Bihan, Rojas, Stella, 2005] $(\log(D) + \log(c))^{O(1)}$.

⁷¹©J. Maurice Rojas

LINEAR FORMS IN LOGS

...the hardest cases of **FEAS_ℝ** we can do in **P** reduce to deciding the sign of **circuit discriminants**:

$$a_1^{b_1} \dots a_k^{b_k} \stackrel{?}{>} (-c)^c \alpha_1^{\beta_1} \dots \alpha_\ell^{\beta_\ell}$$

...and this can be done in **P** by approximating the logs of the coefficients above to bit-precision polynomial in $\text{size}(f)$, thanks to **Baker's Theorem**:

Suppose $a_i \in \mathbb{N}$, $c_i \in \mathbb{Z}$, $A := \log^s \max\{4, a_1, \dots, a_s\}$, $C := \max\{4, c_1, \dots, c_s\}$, and $\Lambda := c_1 \log(a_1) + \dots + c_s \log(a_s)$.

Then

$$\Lambda \neq 0 \implies |\Lambda| > (CA)^{-(16s)^{200s} A \log A}. \blacksquare$$

⁷⁷©J. Maurice Rojas

A TRINOMIAL EXAMPLE

If a, b, c are positive real numbers, then

$$f(x) := c - bx^{39} + ax^{2006}$$

has 0, 1, or 2 positive roots, according as the **A-discriminant**

$$\Delta_{\{0,39,2006\}} := 1967^{1967} 39^{39} b^{2006} - 2006^{2006} c^{1967} a^{39}$$

is < 0 , $= 0$, or > 0 .

Also,

$$\nabla_{\{0,39,2006\}} := \{(a, b, c) \in \mathbb{R}^3 \mid \Delta_{\{0,39,2006\}}(a, b, c) = 0\}$$

splits the orthant \mathbb{R}_+^3 into exactly 2 chambers, and the roots are continuous functions of the coefficients (away from $\nabla_{\{0,39,2006\}}$)!

⁷⁵©J. Maurice Rojas

THE PHASE TRANSITION

Theorem 3 [Bihan-Rojas-Stella, 2005]



FEAS_ℝ($\{(n + 1)\text{-nomials}\}_{n \in \mathbb{N}}\}) \in \mathbf{NC}_1$ and **FEAS_ℝ**($\{(n + 2)\text{-nomials}\}_{n \in \mathbb{N}}\}) \in \mathbf{P}$ for any **fixed** n .*




For any **fixed** $\varepsilon > 0$, **FEAS_ℝ**($\{(n + n^\varepsilon)\text{-nomials}\}_{n \in \mathbb{N}}\})$ is **NP-hard**.


⁷⁹©J. Maurice Rojas

*...restricting to $\text{Vol}(\text{Newt}(f)) > 0$

THE p -ADIC PARALLEL

Theorem $3\frac{1}{2}$ [Poonen-Rojas, 2006]

 **FEAS** $_{\mathbb{Q}_p}$ (n -variate $(n + 1)$ -nomials) \in **RP** for any fixed $n, *$ and the dependence on the prime p is **polynomial** in $\log p$.

 For any fixed $\varepsilon > 0$ and prime p , **FEAS** $_{\mathbb{Q}_p}$ ($\{n^\varepsilon$ -nomials $\}_{n \in \mathbb{N}}$) is **NP-hard**.

Conjecture **FEAS** $_{\mathbb{Q}_p}$ ($\{\text{Univariate Trinomials}\}$) \in **BQP**, and the dependence on the prime p is **polynomial** in $\log p$.

⁸²©J. Maurice Rojas
*...restricting to $\text{Vol}(\text{Newt}(f)) > 0$

$(n+3)$ -NOMIALS AND SYSTEMS...

Let's restrict to

$$\begin{aligned} x^6 + ay^3 - y \\ y^6 + bx^3 - x, \end{aligned}$$

and let $\mathcal{H}(3) := \left\{ \begin{bmatrix} 0 \\ 6 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 6 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \right\}$.

⁸⁶©J. Maurice Rojas

What about n -variate $(n + 3)$ -nomials?

...and what about **systems** of equations?

⁸⁴©J. Maurice Rojas

A BIG DISCRIMINANT...

$$\begin{aligned} &1102507499354148695951786433413508348166942596435546875 \\ &+ 143179068880953778932665444119482631585536972924672 a^{33}b^{12} \\ &+ 236627403090264575474785219707184968001345670463360 a^7b^{28} \\ &- 21034640556603101797073088972187333790660436864 a^{41}b^{34} \\ &- 64692524354845875214754581881148274484815004672 a^{28}b^{42} \\ &+ 412135181350390183442816324226955474457329028451840 a^{31}b^{24} \\ &+ 74268630326294559239611631031564286630254733223424 a^{30}b^{30} \\ &+ 143179068880953778932665444119482631585536972924672 a^{12}b^{33} \\ &+ 1816274895843482705708030487016037960921088 a^{45}b^{45} \\ &+ 45707486651439559266284202160587828803602159296 a^{22}b^{43} \\ &+ 818616116909248137227768928071007988989779492250000 a^{22}b^8 \\ &+ 236627403090264575474785219707184968001345670463360 a^{28}b^7 \\ &+ 48642180526070778429206216629487443546990203515625000 a^2b^{23} \end{aligned}$$

⁸⁷©J. Maurice Rojas

MORE...

- +82754024941868680778822139064668229594467072 $a^{47}b^{33}$
- + 41207664199903653076991000690234985094533094566144 $a^{38}b^{17}$
- + 2218314692460666836925542429565491177644708007287488 $a^{25}b^{25}$
- + 41207664199903653076991000690234985094533094566144 $a^{17}b^{38}$
- + 3748225467651453229201948457758388644676161761600 $a^{29}b^{36}$
- + 8821163670466338815738170064779601944777780404750000 $a^{29}b$
- + 3868355234950754259360595357692756784447296591507264 $a^{26}b^{19}$
- + 516440160351044111358464119738658142157348733522052 a^{35}
- + 516440160351044111358464119738658142157348733522052 b^{35}
- + 785145092246909876150591435521602332059258264670112 $a^{13}b^{27}$
- + 24519711093887016527058411574716512472434688 $a^{39}b^{46}$
- + 24941314853111247935885131129664284932525713375712 $a^{23}b^{37}$
- + 48642180526070778429206216629487443546990203515625000 $a^{23}b^2$

⁸⁸©J. Maurice Rojas

STILL STILL MORE...

- +1398733594760368236093256811269504896377517856840320 $a^{14}b^{21}$
- + 17631004810327637966335552676449435712814331054687500 $a^{11}b^4$
- + 87388579975718405520742649542672056483735351562500000 a^3b^{17}
- + 87388579975718405520742649542672056483735351562500000 $a^{17}b^3$
- + 91600550371393246059947540351710510253906250000000000 a^5b^5
- + 282899832910494363044397530137205019165966367950000 $a^{15}b^{15}$
- + 827275071884277891574270307523957502500000000000000 $a^{10}b^{10}$
- + 1398733594760368236093256811269504896377517856840320 $a^{21}b^{14}$
- + 24519711093887016527058411574716512472434688 $a^{46}b^{39}$
- + 45707486651439559266284202160587828803602159296 $a^{43}b^{22}$
- + 3868355234950754259360595357692756784447296591507264 $a^{19}b^{26}$
- + 6928958745160627098972661174706927675938439861357568 $a^{20}b^{20}$
- 21034640556603101797073088972187333790660436864 $a^{34}b^{41}$

⁹⁰©J. Maurice Rojas

STILL MORE...

- +8415197276745089043520547466937512136683223717776 $a^{39}b^{11}$
- + 24941314853111247935885131129664284932525713375712 $a^{37}b^{23}$
- + 702895423288031690919605187889043797831187902752768 $a^{18}b^{32}$
- 7262663129907778310522865630114322908083751120 $a^{35}b^{35}$
- + 1427268903613031358591879727444818722481000000000000 a^9b^{16}
- + 8821163670466338815738170064779601944777780404750000 ab^{29}
- + 8415197276745089043520547466937512136683223717776 $a^{11}b^{39}$
- + 1427268903613031358591879727444818722481000000000000 b^9a^{16}
- + 412135181350390183442816324226955474457329028451840 $a^{24}b^{31}$
- + 785145092246909876150591435521602332059258264670112 $a^{27}b^{13}$
- + 3748225467651453229201948457758388644676161761600 $a^{36}b^{29}$
- + 17631004810327637966335552676449435712814331054687500 a^4b^{11}
- + 818616116909248137227768928071007988989779492250000 a^8b^{22}

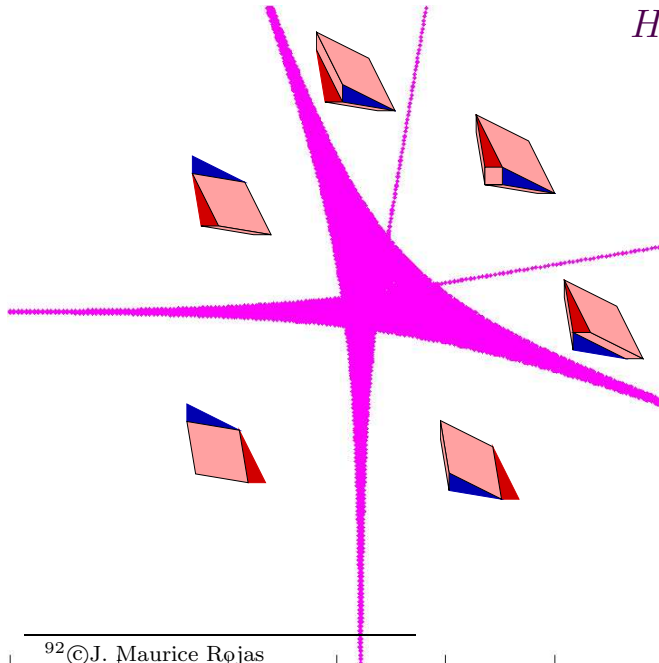
⁸⁹©J. Maurice Rojas

DONE

- +17458752420081093875109627316025221604311252224096 $a^{34}b^6$
- + 702895423288031690919605187889043797831187902752768 $a^{32}b^{18}$
- + 82754024941868680778822139064668229594467072 $a^{33}b^{47}$
- 64692524354845875214754581881148274484815004672 $a^{42}b^{28}$
- 1382857482588991594621856281744153452803994624 $a^{40}b^{40}$
- + 17458752420081093875109627316025221604311252224096 a^6b^{34}

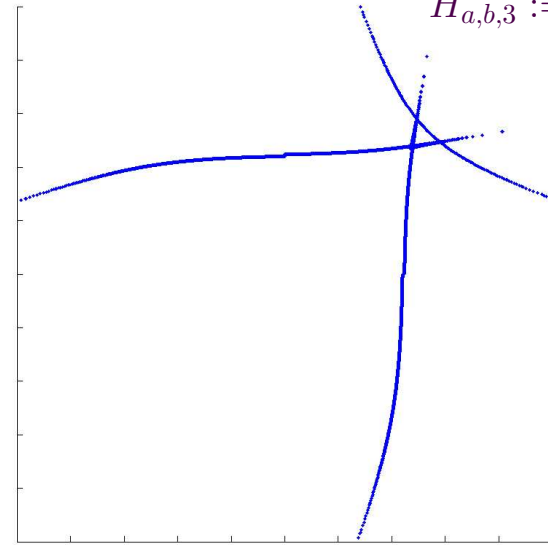
⁹¹©J. Maurice Rojas

$$H_{a,b,3} := \begin{cases} x^6 + ay^3 - y \\ y^6 + bx^3 - x \end{cases}$$



⁹²©J. Maurice Rojas

$$H_{a,b,3} := \begin{cases} x^6 + ay^3 - y \\ y^6 + bx^3 - x \end{cases}$$



⁹³©J. Maurice Rojas

ARE WE MISSING SOMETHING?

$$H_{a,b,3} := \begin{cases} x^6 + ay^3 - y \\ y^6 + bx^3 - x \end{cases}$$

...let's **magnify** the discriminant variety! <./movie1>

⁹⁴©J. Maurice Rojas



Thank you for listening!

Please see...

www.math.tamu.edu/~rojas

for on-line papers and further information, and...

www.ima.umn.edu

for an April 2007 workshop on the state of the art on Complexity, Coding, and Communication (organized by [Mulumley](#), [Rojas](#), [Rosenthal](#), and [Sudan](#)).

This talk is downloadable from:

www.math.tamu.edu/~rojas/ima.pdf