Counting the p-adic valuations of the roots of multivariate systems of polynomials

Cory Saunders

Haverford College

July 18, 2016

Paths of Glory before ours

- 1637: Descarte's Rule. Suppose $f \in \mathbb{R}[x_1]$ and has t terms. Then there are at most $2t+1$ real roots.
- 1980s: van den Dries and (?). Suppose $f_i, \cdots f_n \in \mathbb{Q}[x_1, \cdots, x_n]$ with $\leq t$ terms each. Then there exists a finite number of isolated roots in $\mathbb{Q}_p^n$. No explicit formula found yet!
- 2000s: p-adic tropical geometry can help with finding explicit bounds on the number of roots in $\mathbb{Q}_p$. Complexity theorey gets involved!

Our goal this summer

Use p-adic techniques to help bound the number of integers roots of certain polynomial systems.

p-adic fields

Let p be prime.

- $\mathbb{Z}$: Field of integers. An integer in base 3 is a finite sequence. Ex: 1012 (base 3)$= 1 \cdot 3^3 + 0 \cdot 3^2 + 1 \cdot 3^1 + 2 \cdot 3^0$ (base 10)
- $\mathbb{Z}_3$: All sequences terminating on the right. $\cdots 1012 = \cdots + 1 \cdot 3^3 + 0 \cdot 3^2 + 1 \cdot 3^1 + 2 \cdot 3^0$
- $\mathbb{Q}_3$: All sequences with a finite number of digits after the decimal point. $\cdots 1012.22 = \cdots + 1 \cdot 3^3 + 0 \cdot 3^2 + 1 \cdot 3^1 + 2 \cdot 3^0 + 2 \cdot 3^{-1} + 2 \cdot 3^{-2}$
- $\mathbb{C}_3$: The completion of the algebraic closure of $\mathbb{Q}_3$.

Motivating example: 3-adic roots of $162 - x + 63x^3$

Let $p = 3$. Consider the polynomial $162 - x + 63x^3$.
One real root ($\approx -1.373...$), but three 3-adic roots. Found in Maple:

$$3^{-1} + 2 + 2 \cdot 3 + 2 \cdot 3^4 + 2 \cdot 3^5 + \text{higher order terms}$$
$$2 \cdot 3^{-1} + 2 \cdot 3^2 + 2 \cdot 3^3 + 3^4 + \text{higher order terms}$$
$$2 \cdot 3^4 + 2 \cdot 3^{14} + 3^{15} + \text{higher order terms}$$

The power of 3 of the first non-zero term is its *p-adic valuation*.

Upshot

The polynomial $162 - x + 63x^3$ has three 3-adic roots. Two roots have valuation -1 and one root has valuation 4.

Drawing pictures

You could also draw a picture to get to the same upshot.

$$f(x) = 162 - x + 63x^3 = 2 \cdot 3^4 - x + 7 \cdot 3^2$$

For $f \in \mathbb{C}_p[x_1, \cdots, x_n]$ written $f = \sum_i c_i x^{a_i}$:

Definition (Newton polytope of f)

The *Newton polytope*, $\mathrm{Newt}(f)$, is the convex hull of the set $\{a_i\}$.

Definition (p-adic Newton polytope of f)

The *p-adic Newton polytope*, $\mathrm{Newt}_p(f)$, is the convex hull of the set $\{a_i, \mathrm{ord}_p(c_i)\}$.

Definition (p-adic Tropical Variety of f)

The *p-adic Tropical Variety*, $\mathrm{Trop}_p(f)$, is the set $\{v \in \mathbb{R}^n \,|\, (v, 1) \text{ is an inner normal of a positive-dim. face of } \mathrm{Newt}_p(f)\}$

Generalizing to higher dimensions

Let $p = 3$. Consider the polynomial $g = 1 + x^2 - 54xy$.

What does $\text{Trop}_p(g)$ look like? (Demonstration)

Upshot

We can derive the Y-shape of $\text{Trop}_p(g)$ by $\text{Newt}(g)$ (independent of coefficients).

If you want the position of $\text{Trop}_p(g)$, you need $\text{Newt}_p(g)$ (dependent of coefficients).

Cory-jargon: The Y-shape in $\text{Trop}_p(f_i)$ will occur if $\text{Newt}(f_i)$ is a triangle. They are "hyper-Y's."

Link to bounding integer roots: Kapranov's Theorem

Theorem (Kapranov)

For a system $F := (f_1, \cdots, f_n) \in C_p[x_1, \cdots, x_n]$,
$ord_p \left(\mathcal{Z}_{\mathbb{C}_p}(f_1, \cdots, f_n) \right) \subseteq \bigcap_{i=1} Trop_p(f_i) \bigcap \mathbb{Q}^n$.

Let $t :=$ the number of exponent vectors, $\{a_i\}$ in the system.

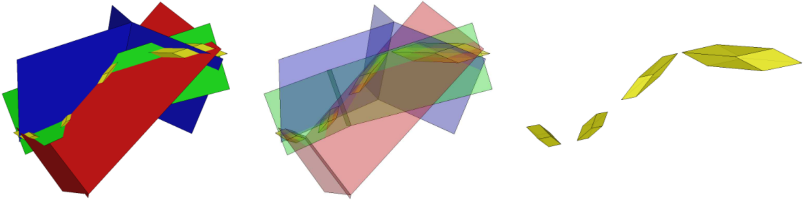
Special case (the "circuit case"): When $t = n + 2$ (with some mild conditions). Use Gaussian Elimination and reduce problem to looking at a collection of hyper-Y's.

Goal

Find a sufficiently good upper bound on the number of intersections of the $\text{Trop}_p(f_i)$ in the case where $t = n + 2$.

Higher dimensional hyper-Y's and why we choose p-adics

$F := (f_1, f_2, f_3) := (xy - x^2 - 1/16^6, yz - 1 - x^2, z - 1 - x^2/16^{18})$
We have $t = n + 2$. $\quad xy, x^2, 1, yz, z$
Look at intersections of
$\mathrm{ArchTrop}(f_1) \cap \mathrm{ArchTrop}(f_2) \cap \mathrm{ArchTrop}(f_3)$. (Image: Dr. Rojas.)



$\mathrm{ArchTrop}(f_i)$ is the real analog to $\mathrm{Trop}_p(f_i)$.

Old Bounds and New

Theorem (Koiran, Portier, Rojas)

Suppose $F := (f_1, \cdots, f_n)$ *with* $f_i \in \mathbb{C}_p(x_1, \cdots x_n)$*. In the "circuit case" (*$\#$ *exponent vectors* $= n+2$*), then the maximum number of valuations of the roots of* F *is at most* $\max\{2, \lfloor \frac{n}{2} \rfloor^n + n\}$*.*

Short-term goal

Achieve an upper bound polynomial in n. For certain case nice cases, we can prove a bound of $n+1$. For certain less-nice cases, a bound of $2n+1$ (S).

Conjecture (Koiran, Portier, Rojas)

The bound can be improved to $n+1$. This bound is sharp.

Conclusions

Same goal, new friend

Find sufficiently good bounds on the number of integer roots for a system of multivariate polynomials.

Bounding p-adic valuations is a step towards bounding integer roots. We do this by looking at intersections of the $\text{Trop}_p(f_i)$'s.

In the "circuit case," we want to bound the number of intersections (=upper bound on number of valuations of the roots of F) by $n + 1$.

Thank you

Thank you for listening!

References

[1] Gouvêa, Fernando Q., *p-adic Numbers: An Introduction*. Second edition. Universitext. *Springer-Verlag, Berlin*, 1997.

[2] Koiran, Pascal; Portier, Natacha; Rojas, J. Maurice, *Counting Tropically Degenerate Valuations and p-adic Approaches to the Hardness of the Permanent*, Math ArXiv 1309.0486v1

[3] Rojas, J. Maurice, *Efficiently Estimating Norms of Complex Roots of Multivariate Polynomials.*