Root Separation for Sparse Polynomials

Yuyu Zhu

Department of Mathematics, Texas A&M University

Objective

- What is the largest t such that all univariate t-nomials have well-separated roots in $\mathbb{C}$ and $\mathbb{C}_p$?
- Use knowledge of root separation, and recent fast algorithms for counting in $\mathbb{Z}/p^r\mathbb{Z}$, to count roots in $\mathbb{Q}_p$ faster.

Detecting roots in $\mathbb{Q}_p$ for univariate polynomials is **NP**-hard (with respect to the sparse input size)[1]; the minimal number of variables making real root detection **NP**-hard is also unknown. So it is natural to restrict to study fine-grained complexity: univariate t-nomials. For example, deciding if a trinomial has a root in $\mathbb{R}$ (resp. $\mathbb{Q}_p$) is proven to be in **P** [2] (resp. **NP** [1]).

Asymptotically sharp root separation bounds for sparse polynomials remain unknown to this day. For a field K, let

$$\sigma_K(f) = \min \|x_1 - x_2\|_K ,$$

where x_1, x_2 are distinct roots of f in K. A classical result due to Mahler [4] states that $\log \sigma_{\mathbb{C}}^{-1}(f)$ can be exponential in the **sparse size** of f (denoted by s):

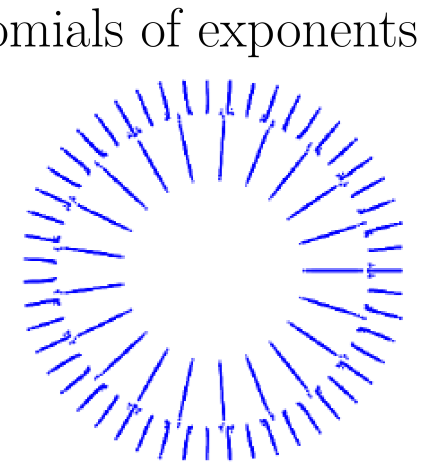
$$\log \sigma_{\mathbb{C}}^{-1}(f) = O(d \log d + d \log H) = O(\exp(s)),$$

where d is the degree and H denotes the height of the coefficients.

We discuss root separation for trinomials and tetranomials over $\mathbb{C}$ and $\mathbb{C}_p$. A natural consequence of our results is faster root counting for trinomials over $\mathbb{Q}_p$.

Trinomials

The picture illustrates how complex roots of random real Gaussian trinomials of exponents $[0, 51, 72]$ are evenly spaced on two circles.



- Phases of the roots strongly cluster.
- Often, roots can be split into "small" norm and "big" norm.

Koiran improved Mahler's bound for trinomial over $K = \mathbb{C}, \mathbb{R}$ [3]:

$$\log \sigma_K^{-1}(f) = O(s^3).$$

We prove a p-adic analogue of his results.

Root Spacing for Trinomials

Theorem 1. (Zhu) Let $f(x) := a + bx^\beta + cx^\gamma \in \mathbb{Z}[x]$ be square-free with $abc \neq 0$, $0 < \beta < \gamma$, and set $s := \log|a| + \log|b| + \log|c| + \log\beta + \log\gamma$. For any prime p, we embed f in $\mathbb{Z}_p[x]$. Then

$$\log \sigma_{\mathbb{C}_p}^{-1}(f) = O(p s_p^4/(\log p)^4),$$

where $s_p = \min(s, \log p)$.

Tetranomials

However, when f is a tetranomial, $\log_{\mathbb{C}}^{-1}(f)$, $\log_{\mathbb{C}_p}^{-1}(f)$ can be **exponential** in the sparse size of f, as shown by the following family of examples:

$$f_\varepsilon(x) = x^d - \left(\frac{x}{\varepsilon^s} - \frac{1}{\varepsilon}\right)^2.$$

for $s > 2$ and $2 < d$ an even integer bounded from above by $\exp(s)$.

Theorem 2. (Zhu)

- **Over** $\mathbb{C}$ take $\varepsilon = 1/2$: there exist x_1, x_2 distinct $\mathbb{C}$ roots of f such that
$$|x_1 - x_2| < 2^{-\Omega(ds)} = 2^{-\Omega(2^s)}.$$
- **Over** $\mathbb{C}_p$ take $\varepsilon = p$: there exist x_1, x_2 distinct $\mathbb{C}_p$ roots of f such that
$$\|x_1 - x_2\|_p \leq p^{-\Omega(ds)} = p^{-\Omega(2^s)}.$$

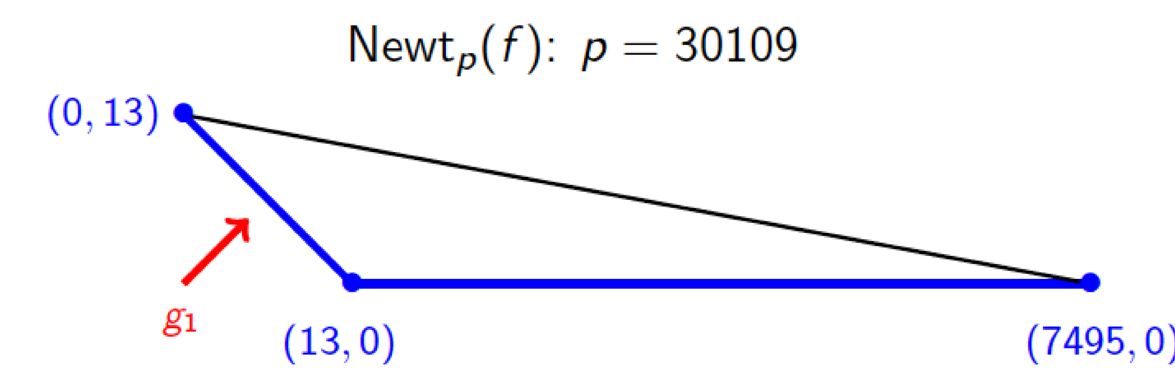
Root Counting

- ***p*-adic Newton polygon** of $f(x) := a_0 + a_1 x + \cdots + a_d x^d$ is
$$\mathrm{Newt}_p(f) := \mathrm{Conv}(\{(i, \mathrm{ord}_p(a_i)) : i \in \{0, 1, \cdots, d\}\}).$$
- f is **regular** with respect to p, if p does not divide the difference of exponents, and for any lower edge E of $\mathrm{Newt}_p(f)$, there are no points of the form $(i, \mathrm{ord}_p(a_i))$ on E other than the two endpoints.
- **Counting roots** in $\mathbb{Q}_p$ can be reduced to counting roots in $\mathbb{Z}/p^r\mathbb{Z}$, where $r = O(\log^{-1} \sigma_{\mathbb{C}_p}(f))$.

Root Counting for Trinomials

Theorem 3. (Zhu) Let $f(x) \in \mathbb{Z}[x]$ be a square-free, regular trinomial. For any prime p, we embed $f \in \mathbb{Z}_p[x]$. Then the number of roots of f in $\mathbb{Q}_p$ can be computed in time polynomial in $s + \log p$.

- **Example:** Let $p = 30109$. Then the number of roots of the **regular** trinomial $f = 3313x^{7495} + 26224x^{13} - 30109^{13} \cdot 293$ in $\mathbb{Q}_p$ can be computed as follows:



This is a regular polynomial, and thus by our algorithm, it suffices to compute the number of roots respectively of

$$g_1 = x^{13} - 9083 \mod 30109, \text{ and}$$
$$g_2 = x^{7482} + 14040 \mod 30109$$

As -9083 is a 13-th root modulo 30109, whereas 14040 is not a 7482-th root, the number of roots of f is equal to that of g_1, which is 13.

- **Conjecture:** We can count the number of $\mathbb{Q}_p$ roots in polynomial time for **any** trinomial.

Theorem 4. (Zhu) For **any** trinomial $f = a + bx^\beta + cx^\gamma \in \mathbb{Z}_p[x]$ with $p \nmid (\gamma - \beta)$, counting $\mathbb{Q}_p$ roots can be done in time polynomial in the sparse size of f.

References

[1] Martín Avendano, Ashraf Ibrahim, J. Maurice Rojas, and Korben Rusek, *Faster p-adic feasibility for certain multivariate sparse polynomials*, Journal of Symbolic Computation **47** (2012), no. 4, 454–479.

[2] Frédéric Bihan, J. Maurice Rojas, and Casey E. Stella, *Faster real feasibility via circuit discriminants*, Proceedings of ISSAC 2009, 2009.

[3] Pascal Koiran, *Root separation for trinomials*, arXiv:1709.03294, December 2017.

[4] Kurt Mahler, *An inequality for the discriminant of a polynomial*, The Michigan Mathematical Journal **11** (1964), no. 3, 257–262.

TEXAS A&M UNIVERSITY