Bounding the Number of Distinct p-adic Valuations of Integer Roots of Certain SPS-Polynomials

Kayla Cummings

Pomona College

July 18, 2016

Motivation

Definition

For $f \in \mathbb{Z}[x]$, $\tau(f)$ is the minimum number of steps required to build f from 1 and x.

Motivation

Definition

For $f \in \mathbb{Z}[x]$, $\tau(f)$ is the minimum number of steps required to build f from 1 and x.

Example. Let $f = (1+x)^8$. Then $\tau(f) \leq 4$.

$$1, x \to 1+x \to (1+x)^2 \to (1+x)^4 \to (1+x)^8$$

Motivation

Definition

For $f \in \mathbb{Z}[x]$, $\tau(f)$ is the minimum number of steps required to build f from 1 and x.

Example. Let $f = (1+x)^8$. Then $\tau(f) \leq 4$.

$$1, x \to 1+x \to (1+x)^2 \to (1+x)^4 \to (1+x)^8$$

Shub-Smale τ Conjecture (1993)

If there exists an absolute constant c such that for all $f \in \mathbb{Z}[x]$, the number of integer roots of f is bounded above by $\tau(f)^c$, then $P_{\mathbb{C}} \neq NP_{\mathbb{C}}$.

Motivation

Definition *(Koiran, Portier, Rojas)*

An SPS-polynomial g is a polynomial expressible as $\sum_{i=1}^{k} \prod_{j=1}^{m} g_{i,j}$ with nonzero, univariate $g_{i,j}$ having at most t monomial terms for all i, j.

Motivation

Definition *(Koiran, Portier, Rojas)*

An SPS-polynomial g is a polynomial expressible as $\sum_{i=1}^{k} \prod_{j=1}^{m} g_{i,j}$ with nonzero, univariate $g_{i,j}$ having at most t monomial terms for all i, j.

Theorem *(Koiran, Portier, Rojas)*

Let f be an SPS-polynomial. If there exists a prime p such that, for all f, the cardinality of the set of distinct p-adic valuations of the integer roots is $(kmt)^{O(1)}$, then the permanent of square matrices cannot be computed in polynomial time.

Project Goal

Conjecture

Let $f \in \mathbb{Z}[x]$ defined as $f = (x+a)^M(x+b)^N + c$ be a univariate polynomial with a and b distinct nonzero integers, c an integer, and M and N positive integers. Then f has $O(\log_p(M+N))$ distinct p-adic valuations of the integer roots.

Background

Definition

Let $f \in \mathbb{Z}[x_1]$ with $f = \sum_k \gamma_k x^k$. Then define the p-adic Newton Polygon of f to be the convex hull of $(k, \operatorname{ord}_p(\gamma_k))$ for all k.

Background

Definition

Let $f \in \mathbb{Z}[x_1]$ with $f = \sum_k \gamma_k x^k$. Then define the p-adic Newton Polygon of f to be the convex hull of $(k, \text{ord}_p(\gamma_k))$ for all k.

Definition

The lower hull of $\text{Newt}_p(f)$ is the set of all edges of $\text{Newt}_p(f)$ whose inner normals have positive y-coordinates.

Background

Definition

Let $f \in \mathbb{Z}[x_1]$ with $f = \sum_k \gamma_k x^k$. Then define the p-adic Newton Polygon of f to be the convex hull of $(k, \text{ord}_p(\gamma_k))$ for all k.

Definition

The lower hull of $\text{Newt}_p(f)$ is the set of all edges of $\text{Newt}_p(f)$ whose inner normals have positive y-coordinates.

Theorem (Hensel, Dumas, 1903)

Let $-m$ be the slope of the edge of $\text{Newt}_p(f)$ with scaled inner normal $(v, 1)$. Then f has at most v integer roots with valuation m, counting multiplicities.

A Concise Case: p divides neither a nor b

Theorem *(Saunders)*

Assume $\text{ord}_p(a) = \text{ord}_p(b) = 0$ and $\text{ord}_p(M) > \text{ord}_p(N) > 0$. Then there are no more than $\text{ord}_p(N) + 2$ edges in the lower hull of $\text{Newt}_p(f)$.

A Concise Case: p divides neither a nor b

Theorem *(Saunders)*

Assume $\text{ord}_p(a) = \text{ord}_p(b) = 0$ and $\text{ord}_p(M) > \text{ord}_p(N) > 0$. Then there are no more than $\text{ord}_p(N) + 2$ edges in the lower hull of $\text{Newt}_p(f)$.

Intuition

- We have $\text{ord}_p(\gamma_1) = \text{ord}_p(N)$. Consider the first j such that $\text{ord}_p(\gamma_j) = 0$ and the y-axis projections of the lower edges: there are at most $\text{ord}_p(N)$ edges between $(1, \text{ord}_p(N))$ and $(j, 0)$.

A Concise Case: p divides neither a nor b

Theorem *(Saunders)*

Assume $\text{ord}_p(a) = \text{ord}_p(b) = 0$ and $\text{ord}_p(M) > \text{ord}_p(N) > 0$. Then there are no more than $\text{ord}_p(N) + 2$ edges in the lower hull of $\text{Newt}_p(f)$.

Intuition

- We have $\text{ord}_p(\gamma_1) = \text{ord}_p(N)$. Consider the first j such that $\text{ord}_p(\gamma_j) = 0$ and the y-axis projections of the lower edges: there are at most $\text{ord}_p(N)$ edges between $(1, \text{ord}_p(N))$ and $(j, 0)$.
- There is at most one edge between $(0, \text{ord}_p(\gamma_0)$ and $(1, \text{ord}_p(N))$.

A Concise Case: p divides neither a nor b

Theorem *(Saunders)*

Assume $\text{ord}_p(a) = \text{ord}_p(b) = 0$ and $\text{ord}_p(M) > \text{ord}_p(N) > 0$. Then there are no more than $\text{ord}_p(N) + 2$ edges in the lower hull of $\text{Newt}_p(f)$.

Intuition

- We have $\text{ord}_p(\gamma_1) = \text{ord}_p(N)$. Consider the first j such that $\text{ord}_p(\gamma_j) = 0$ and the y-axis projections of the lower edges: there are at most $\text{ord}_p(N)$ edges between $(1, \text{ord}_p(N))$ and $(j, 0)$.
- There is at most one edge between $(0, \text{ord}_p(\gamma_0)$ and $(1, \text{ord}_p(N))$.
- Suppose $j \neq M + N$. There is at most one edge between $(j, 0)$ and $(M + N, 0)$.

A Concise Case: Example

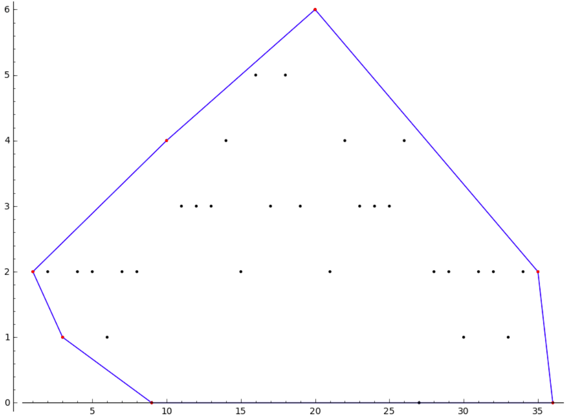

Figure 1: $\text{Newt}_3((x+14)^{3^3}(x+4)^{3^2} - 14^{27}4^9)$

A Base Polytope: p divides a or b

Theorem *(C.)*

Let p divide a or b with $\text{ord}_p(a) \geq \text{ord}_p(b)$ and $c = 0$.

A Base Polytope: p divides a or b

Theorem *(C.)*

Let p divide a or b with $\text{ord}_p(a) \geq \text{ord}_p(b)$ and $c = 0$. Then $h : [0, M+N] \to \mathbb{Z}$ describes the lower hull of $\text{Newt}_p(f)$ and is defined by

$$h(x) = \begin{cases} -\text{ord}_p(a)x + (M \cdot \text{ord}_p(a) + N \cdot \text{ord}_p(b)) & \text{if } 0 \leq x \leq M \\ -\text{ord}_p(b)x + (M+N) \cdot \text{ord}_p(b) & \text{if } M \leq x \leq M+N \end{cases}$$

Example: Base Polygon and Constant Term

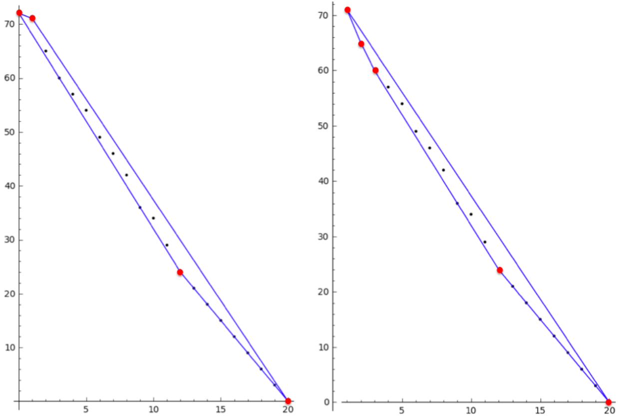

Figure 2: $\text{Newt}_3((x + 4 \cdot 3^4)^{12}(x + 3^3)^8)$ and $\text{Newt}_3((x + 4 \cdot 3^4)^{12}(x + 3^3)^8 - (4 \cdot 3^4)^{12}(3^3)^8$

Using the Theorem

Anchoring the Linear Term

If we can guarantee $\text{ord}_p(\gamma_1) = h(1)$, then $\text{Newt}_p(f)$ will have at most 3 edges.

Example: Anchored Linear Term

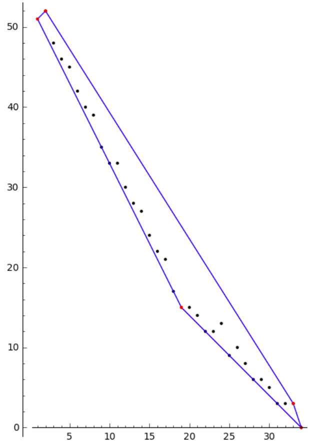

Figure 3: $\text{Newt}_3((x + 5 \cdot 3^2)^{19}(x + 2 \cdot 3)^{5 \cdot 3} - 45^{19}6^{15})$

Anchoring the Linear Term

Guaranteeing the point $(1, h(1))$

Let $a = \alpha p^j$ and $b = \beta p^k$ with $p \nmid \alpha$, $p \nmid \beta$, and $j \geq k$.

Anchoring the Linear Term

Guaranteeing the point $(1, h(1))$

Let $a = \alpha p^j$ and $b = \beta p^k$ with $p \nmid \alpha$, $p \nmid \beta$, and $j \geq k$.

$$\text{ord}_p(\gamma_1) = h(1) + \text{ord}_p(N\alpha p^{j-k} + M\beta)$$

Anchoring the Linear Term

Guaranteeing the point $(1, h(1))$

Let $a = \alpha p^j$ and $b = \beta p^k$ with $p \not| \alpha$, $p \not| \beta$, and $j \geq k$.

$$\text{ord}_p(\gamma_1) = h(1) + \text{ord}_p(N\alpha p^{j-k} + M\beta)$$

When does $\text{ord}_p(N\alpha p^{j-k} + M\beta) = 0$?

Anchoring the Linear Term

Guaranteeing the point $(1, h(1))$

Let $a = \alpha p^j$ and $b = \beta p^k$ with $p \nmid \alpha$, $p \nmid \beta$, and $j \geq k$.

$$\text{ord}_p(\gamma_1) = h(1) + \text{ord}_p(N\alpha p^{j-k} + M\beta)$$

When does $\text{ord}_p(N\alpha p^{j-k} + M\beta) = 0$?

- $\text{ord}_p(a) > \text{ord}_p(b), p \nmid M$
- $\text{ord}_p(a) = \text{ord}_p(b), p \mid M, p \nmid N$
- $\text{ord}_p(a) = \text{ord}_p(b), p \nmid M, p \mid N$

Remaining Cases

Case 1: $\text{ord}_p(a) > \text{ord}_p(b)$, $p \mid M$

Vertices only occur on points whose x-coordinates are powers of p between 1 and M. We can bound the number of edges by $\text{ord}_p(M) + 3$.

Remaining Cases

Case 1: $\text{ord}_p(a) > \text{ord}_p(b)$, $p \mid M$

Vertices only occur on points whose x-coordinates are powers of p between 1 and M. We can bound the number of edges by $\text{ord}_p(M) + 3$.

Case 2: $\text{ord}_p(a) = \text{ord}_p(b)$, $\text{ord}_p(M) > \text{ord}_p(N) > 0$

Vertices only occur on points whose x-coordinates are powers of p between 1 and N. Then $\text{Newt}_p(f)$ has a max of $\text{ord}_p(N) + 2$ lower edges.

Example: Remaining Case

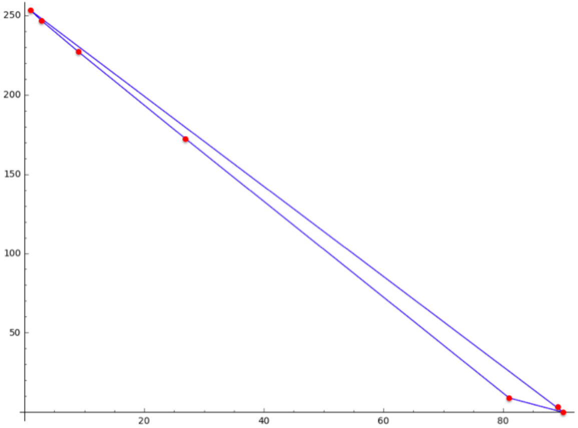

Figure 4: $\text{Newt}_3((x+5\cdot 3^3)^{3^4}(x+2\cdot 3)^{3^2} - 135^{81}6^9)$

A Tricky Case: $\text{ord}_p(a) = \text{ord}_p(b), p \nmid M, p \nmid N$

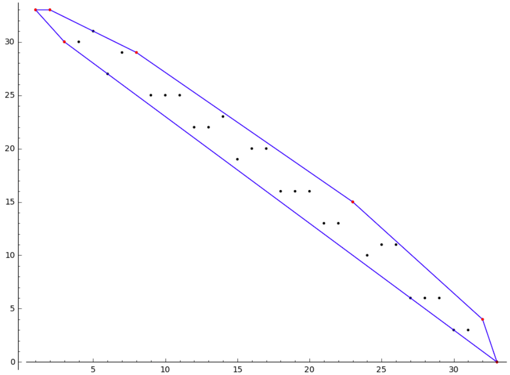

Figure 5: $\text{Newt}_3((x+15)^{14}(x+6)^{19} - 15^{14}6^{19})$

Summary

Our bound of $O(log_p(M+N))$ is within reach!

Conclusion

Thank you for listening!

References

- L. Blum, F. Cucker, M. Shub, S. Smale. *Complexity and Real Computation.* New York: Springer-Verlag, 1998. Print.
- Gouvêa, Fernando Q. *p-adic Numbers: An Introduction*, 2nd ed. New York: Springer-Verlag, 1997.
- P. Koiran, N. Portier, J. M. Rojas. "Counting Tropically Degenerate Valuations and p-adic Approaches to the Hardness of the Permanent," submitted for publication.
- Rojas, J. Maurice. "Arithmetic Multivariate Descartes' Rule," American Journal of Mathematics, vol. 126, no. 1, February 2004, pp. 1-30.
- Weiss, Edwin. *Algebraic Number Theory.* New York: McGraw-Hill Book Company, Inc., 1963. Print.