AN UPPER BOUND ON THE NUMBER OF INTEGER ROOTS OF CERTAIN SUM-PRODUCT-SPARSE POLYNOMIALS

KAYLA CUMMINGS AND CORY SAUNDERS

July 21, 2016

Abstract. An SPS-polynomial is a polynomial expressible as a sum of products of sparse univariate polynomials. SPS-polynomials are closely related to depth-4 arithmetic circuits (of recent interest in complexity theory), and Koiran has shown earlier that new lower bounds for the complexity of the permanent hold if SPS-polynomials of low complexity have few integer roots. Some effort has been made toward bounding the number of real roots of SPS-polynomials, but bounding the number of integer roots still appears out of reach.

Bounding p-adic valuations of the integer roots is a potentially promising, alternative approach that has yet to be explored. We show that an upper bound for the number of p-adic valuations, in line with Koiran's conjectures, can be proven for a particular family of SPS-polynomials. We then point out a larger family of SPS-polynomials where p-adic methods may be more tractable than real analytic methods.

1. Introduction

The solutions to large systems of polynomials are oftentimes the algebraic analogues to important open problems. We study the integer solutions to a particular family of sum-product-sparse polynomials. We relate the number of p-adic valuations of the integer roots to the complexity of computing the permanent of square matrices.

Definition 1.1. Let $k, m, t \in \mathbb{N}$. Define a *sum-product-sparse* polynomial $g \in \mathrm{SPS}(k, m, t)$ to be a polynomial that can be expressed in the form

$$\sum_{i=1}^{k} \prod_{j=1}^{m} g_{i,j}$$

where $g_{i,j} \in \mathbb{Z}[x_1]\backslash\{0\}$ is a t-nomial for all i, j. [2]

Theorem 1.2. Define a set S as follows.

$$S := \{i \in \mathbb{N} \mid x \in \mathbb{Z},\ g(x) = 0,\ p^i \mid x,\ p^{i+1} \nmid x\}$$

If there exists some p such that $|S| = (kmt)^{O(1)}$ for all $k, m, t \in \mathbb{N}$ and $g \in SPS(k, m, t)$, then the permanent of square matrices cannot be computed by constant-free, division-free arithmetic circuits in polynomial time. [2]

The bound $(kmt)^{O(1)}$ itself remains unproven for many cases, including $k = 2$. Therefore, we are interested in bounding the number of p-adic valuations of the integer roots for a specific polynomial $f \in \mathrm{SPS}(2, m, t)$. We are interested to see whether the bound we find for our specific case agrees with the desired generalized bound.

Conjecture 1.3. Let $f = (x + a)^M (x + b)^N + c$ with $c \in \mathbb{Z}$, $M, N \in \mathbb{N}$, and distinct $a, b \in \mathbb{Z}\backslash\{0\}$. Then there are $O(\log_p(M + N))$ distinct p-adic valuations of the integer roots.

We make use of a classical result that relates p-adic Newton polygons and p-adic valuations of the integer roots.

Definition 1.4. Let $f \in \mathbb{Z}[x_1]$ with $f = \sum_{i=0}^{M+N} \gamma_i x^i$. Then define the *$p$-adic Newton Polygon* of f, denoted $\mathrm{Newt}_p(f)$, to be the convex hull of the set $\{(i, \mathrm{ord}_p(\gamma_i)) \mid i \in \{0, M + N\} \cap \mathbb{Z}\}$.

Definition 1.5. Given a p-adic Newton Polygon, we call an edge a *lower edge* if its inner normal vector has a positive y-coordinate. We rescale the inner normal to be of the form $(v, 1)$. The *lower hull* of $\text{Newt}_p(f)$ is the set of all lower edges of $\text{Newt}_p(f)$.

Theorem 1.6. *(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 v integer roots with valuation m, counting multiplicities. [4]

2. Results

The results of our case study are organized by the table in Figure (1).

Case	a, b	M, N	More assumptions	Conjectured bound	Proof
1.A	$\text{ord}_p(a) = 0$	$p \mid M, p \nmid N$		2	✓
1.B	$\text{ord}_p(b) = 0$	$p \nmid M, p \nmid N$		$\log_p(M) + \log_p(N) + 3$	✓
1.C.i		$p \mid M, p \mid N$	$\text{ord}_p(M) > \text{ord}_p(N)$	$\text{ord}_p(N) + 2$	✓
1.C.ii			$\text{ord}_p(M) = \text{ord}_p(N)$	$\log_p(M) + \log_p(N) + 3$	✓
2.A.i	$\text{ord}_p(a) = \text{ord}_p(b)$	$p \mid M, p \mid N$	$\text{ord}_p(M) > \text{ord}_p(N)$	$\text{ord}_p(N) + 2$	✗
2.A.ii	$p \mid a \quad p \mid b$		$\text{ord}_p(M) = \text{ord}_p(N)$	sufficiently small	✗
2.B		$p \mid M, p \nmid N$		2	✓
2.C		$p \nmid M, p \nmid N$		sufficiently small	✗
3.A	$\text{ord}_p(a) > \text{ord}_p(b)$	$p \nmid M$		3	✓
3.B.i		$p \mid M$	$\text{ord}_p(M) \neq \text{ord}_p(N) + \text{ord}_p(a) - \text{ord}_p(b)$	$\text{ord}_p(M) + 3$	✗
3.B.ii			$\text{ord}_p(M) = \text{ord}_p(N) + \text{ord}_p(a) - \text{ord}_p(b)$	sufficiently small	✗

Figure 1. An exhaustive table of cases and conjectures.

We first outline important ideas we use in the discussion of our sub-cases.

Lemma 2.1. Let $f = \sum_{i=0}^{M+N} \gamma_i x^i$ with $\gamma_i \in \mathbb{Z}$ and $i \in \mathbb{N}$. Then every point in the set $\{(i, \text{ord}_p(\gamma_i) \mid i \in \{0, M+N\} \cap \mathbb{Z}\}$ will lie on the integer lattice in the first quadrant of the plane.

Proof. We study a family of polynomials whose coefficients γ_i are integers for all i. Consequently, the p-adic valuations of every coefficient will be positive. Each coefficient corresponds to a non-negative-degree term. Thus, $(i, \text{ord}_p(\gamma_i))$ will be an ordered pair of non-negative integers for all i.

■

Lemma 2.2. The rightmost vertex of $\text{Newt}_p(f)$ is $(M + N, 0)$.

Proof. For all f, $\gamma_{M+N} = 1$. Then for any prime p, $\text{ord}_p(\gamma_{M+N}) = 0$.

■

Lemma 2.3. $\text{Newt}_p(f)$ has a maximum of $\text{ord}_p(\gamma_i) + (i + 1)$ lower edges.

Proof. We consider the y-axis projections of the lower edges between $(i, \text{ord}_p(\gamma_i))$ and $(M+N, 0)$ and observe there are at most $\text{ord}_p(\gamma_i))$ edges between these two points. Then we consider the x-axis projections of the lower edges between $(0, \text{ord}_p(\gamma_0))$ and $(i, \text{ord}_p(\gamma_i)$ and observe there are at most i edges between these two points. If there is some $j \neq M + N$ such that $\text{ord}_p(\gamma_j) = 0$, then there is at most one edge adjoining $(j, 0)$ and $(M + N, 0)$.

■

Lemma 2.4. If all but one term in a sum S is divisible by p, then $\text{ord}_p(S) = 0$.

Proof. Assume all but one term in a sum S is divisible by p. Then $S \not\equiv 0 \pmod{p}$ and S is indivisible by p. Thus, $\text{ord}_p(S) = 0$.

■

We also provide a short study of a simpler SPS-polynomial.

Theorem 2.5. (S.) Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g = (x+1)^M - 1$ with $M \in \mathbb{N}$. Then for any prime p, there are at most $\log_p(M) + 2$ p-adic valuations of the integer roots.

Proof. Consider expanded g.

$$g = (x^M + \cdots + Mx + 1) - 1$$

By Lemma (2.3), $\text{Newt}_p(g)$ has at most $\text{ord}_p(\gamma_1) + 2 = \text{ord}_p(M) + 2$ lower edges.

■

3. Discussion

3.1. **Case 1.** These are the sub-cases for which we assume $\text{ord}_p(a) = \text{ord}_p(b) = 0$.

(1) **Case 1.A.** This is the sub-case for which we assume $p \mid M$ and $p \nmid N$, without loss of generality.

Claim. (S.) $\text{Newt}_p(f)$ has at most 2 lower edges.

Proof. Consider the valuation of γ_1.

$$\begin{aligned}\text{ord}_p(\gamma_1) &= \text{ord}_p(Na^M b^{N-1} + Ma^{M-1}b^N) \\ &= \text{ord}_p(a^{M-1}b^{N-1}) + \text{ord}_p(Na + Mb) \\ &= 0\end{aligned}$$

Because $\text{ord}_p(a) = \text{ord}_p(b) = 0$, we have $\text{ord}_p(a^{M-1}b^{N-1}) = 0$. Additionally, $\text{ord}_p(Na + Mb) = 0$ by Lemma (2.4).

We have shown $\text{ord}_p(\gamma_1) = 0$. By Lemma (2.3), $\text{Newt}_p(f)$ has a maximum of $\text{ord}_p(\gamma_1) + 2 = 2$ lower edges.

■

(2) **Case 1.B.** This is the sub-case for which we assume $p \nmid M$ and $p \nmid N$.

Claim. (S.) $\text{Newt}_p(f)$ has at most $\log_p(M) + \log_p(N) + 3$ lower edges.

Proof. First assume $\text{ord}_p(\gamma_1) \leq \log(M) + \log(N)$. Then by Lemma (2.3), $\text{Newt}_p(f)$ has at most $\text{ord}_p(\gamma_1) + 2 = \log(M) + \log(N) + 2$ lower edges.

Now assume $\text{ord}_p(\gamma_1) > \log_p(M) + \log_p(N)$.

$$\begin{aligned}\text{ord}_p(\gamma_1) &= \text{ord}_p(Na^M b^{N-1} + Ma^{M-1}b^N) \\ &= \text{ord}_p(Na + Mb)\end{aligned}$$

Then $\text{ord}_p(Na + Mb) > \log_p(M) + \log_p(N)$.

We also have $\text{ord}_p(M + N) \leq \log_p(M) + \log_p(N)$.

$$\begin{aligned}\text{ord}_p(M + N) &\leq \log_p(M + N) \\ &\leq \log_p(MN) \\ &= \log_p(M) + \log_p(N)\end{aligned}$$

Now consider the quadratic coefficient of f.

$$\begin{aligned}\operatorname{ord}_p(\gamma_2) &= \operatorname{ord}_p\left(\frac{a^{M-2}b^{N-2}}{2}\left(N(N-1)a^2+2NMab+M(M-1)b^2\right)\right)\\ &= \operatorname{ord}_p\left((Na+Mb)\cdot(Na+Mb-a-b)+ab\cdot(M+N)\right)\end{aligned}$$

Because $\operatorname{ord}_p(M+N) < \operatorname{ord}_p(Na+Mb)$, we may factor $p^{\operatorname{ord}_p(M+N)}$ out of the sum. By Lemma (2.4), the valuation of the remaining part of the sum becomes zero.

We conclude $\operatorname{ord}_p(\gamma_2) = \operatorname{ord}_p(M+N)$. By Lemma (2.3), $\operatorname{Newt}_p(f)$ has at most $\operatorname{ord}_p(\gamma_2)+3 = \operatorname{ord}_p(M+N)+3$ lower edges. This maximum falls under our conjectured bound of $\log_p(M)+\log_p(N)+3$.

■

(3) **Case 1.C.i.** This is the sub-case for which we assume $\operatorname{ord}_p(M) > \operatorname{ord}_p(N)$ without loss of generality.

Claim. (S.) $\operatorname{Newt}_p(f)$ has at most $\operatorname{ord}_p(N)+2$ lower edges.

Proof. Consider the valuation of the linear coefficient. Let $M = \mu p^m$ and $N = \nu p^n$ with $\operatorname{ord}_p(M) = m$ and $\operatorname{ord}_p(N) = n$. By assumption, $m > n$.

$$\begin{aligned}\operatorname{ord}_p(\gamma_1) &= \operatorname{ord}_p(a^{M-1}b^{N-1}) + \operatorname{ord}_p(Na+Mb)\\ &= \operatorname{ord}_p(\nu p^n a + \mu p^m b)\\ &= \operatorname{ord}_p(N) + \operatorname{ord}_p(\nu a + \mu p^{m-n} b)\\ &= \operatorname{ord}_p(N)\end{aligned}$$

Then by Lemma (2.3) $\operatorname{Newt}_p(f)$ has at most $\operatorname{ord}_p(\gamma_1)+2 = \operatorname{ord}_p(N)+2$ lower edges.

■

(4) **Case 1.C.ii.** This is the sub-case for which we assume $\operatorname{ord}_p(M) = \operatorname{ord}_p(N) \neq 0$.

Claim. (S.) $\operatorname{Newt}_p(f)$ has at most $\log_p(M)+\log_p(N)+3$ lower edges.

Proof. First assume $\operatorname{ord}_p(\gamma_1) \leq \operatorname{ord}_p(M)+\operatorname{ord}_p(N)$. Then, by Lemma (2.3), $\operatorname{Newt}_p(f)$ has a maximum of $\operatorname{ord}_p(\gamma_1)+2 = \log_p(M)+\log_p(N)+2$ lower edges.

Now assume $\operatorname{ord}_p(\gamma_1) > \log_p(M)+\log_p(N)$ and consider the valuation of the quadratic coefficient. Let $M = \mu p^m$ and $N = \nu p^m$ with $\operatorname{ord}_p(M) = \operatorname{ord}_p(N) = m$.

$$\begin{aligned}\operatorname{ord}_p(\gamma_2) &= \operatorname{ord}_p\left(\frac{a^{M-2}b^{N-2}}{2}(N(N-1)a^2+2NMab+M(M-1)b^2)\right)\\ &= \operatorname{ord}_p((N^2a^2+2NMab+M^2b^2)-(Na^2+Nab+Mab+Mb^2)+Nab+Mab)\\ &= \operatorname{ord}_p((Na+Mb)^2-(Na+Mb)(a+b)+ab(N+M))\\ &= m+\operatorname{ord}_p(p^m(\nu a+\mu b)^2-(\nu a+\mu b)(a+b)+ab(\nu+\mu))\\ &= m+\operatorname{ord}_p(\nu+\mu)\end{aligned}$$

We now prove the last line of this computation and show that we can factor $p^{\operatorname{ord}_p(\nu+\mu)}$ out of the sum. After doing so, only the third term is indivisible by p, and the remaining sum's valuation is 0 by Lemma (2.4).

$$\begin{aligned}\operatorname{ord}_p(\nu+\mu)+m &= \operatorname{ord}_p(N+M)\\ &\leq \log_p(N+M)\\ &\leq \log_p(N)+\log_p(M)\end{aligned}$$

By our initial assumption, we also have

$$\begin{aligned}\log_p(M) + \log_p(N) &< \mathrm{ord}_p(\gamma_1)\\ &= \mathrm{ord}_p(Na + Mb)\\ &= \mathrm{ord}_p(\nu a + \mu b) + m\end{aligned}$$

Therefore, $\mathrm{ord}_p(\nu+\mu) \leq \log_p(N) + \log_p(M) - m < \mathrm{ord}_p(\nu a + \mu b)$.

Because $\mathrm{ord}_p(\nu+\mu) < \mathrm{ord}_p(\nu a + \mu b)$, we have $\mathrm{ord}_p(\gamma_2) = m + \mathrm{ord}_p(\nu+\mu)$ and

$$\mathrm{ord}_p(\gamma_2) \leq \log_p(M) + \log_p(N)$$

Thus, by Lemma (2.3), $\mathrm{Newt}_p(f)$ has at most $\mathrm{ord}_p(\gamma_2) + 3 \leq \log_p(N) + \log_p(M) + 3$ lower edges.

■

3.2. **Case 2.** These are the sub-cases for which we assume $\mathrm{ord}_p(a) = \mathrm{ord}_p(b) \neq 0$. We first investigate the shape of $\mathrm{Newt}_p(f)$ when $c = 0$, which we call the "base polygon". Then we let $c = -a^M b^N$, which yields $\gamma_0 = 0$ and $\mathrm{ord}_p(\gamma_0) = \infty$. As $\mathrm{ord}_p(\gamma_0)$ becomes arbitrarily high, the maximum number of lower edges in $\mathrm{Newt}_p(f)$ are revealed.

Claim 3.1. (C.) Let $\mathrm{ord}_p(a) = \mathrm{ord}_p(b) \neq 0$ and $c = 0$. Then $\mathrm{Newt}_p(f)$ has one lower edge described by $g : [0, M+N] \to \mathbb{R}$ defined by:

$$g(x) = -\mathrm{ord}_p(a)x + (M+N)\cdot \mathrm{ord}_p(a) \tag{1}$$

Proof.

(1) We verify that the endpoints are given correctly by g.

$$\begin{aligned}\mathrm{ord}_p(\gamma_0) &= (M+N)\cdot \mathrm{ord}_p(a)\\ &= g(0)\\ \mathrm{ord}_p(\gamma_{M+N}) &= 0\\ &= g(M+N)\end{aligned}$$

(2) We draw a line from $(0, (M+N)\cdot \mathrm{ord}_p(a))$ to $(M+N, 0)$. The slope of this line is $-\mathrm{ord}_p(a)$, which is the slope of g.

(3) We show this line is the lower hull of $\mathrm{Newt}_p(f)$ by verifying $\mathrm{ord}_p(\gamma_i) \geq g(i)$ for all $0 < i < M+N$.

We express γ_i, letting $a = \alpha p^j$ and $b = \beta p^j$ with $\mathrm{ord}_p(a) = \mathrm{ord}_p(b) = j$.

$$\begin{aligned}\gamma_i &= \binom{N}{i} a^M b^{N-i} + \cdots + \binom{M}{i} a^{M-i} b^N\\ &= \binom{N}{i} (\alpha p^j)^M (\beta p^j)^{N-i} + \cdots + \binom{M}{i} (\alpha p^j)^{M-i} (\beta p^j)^N\\ &= (p^j)^{M+N-i} \left(\binom{N}{i} \alpha^M \beta^{N-i} + \cdots + \binom{M}{i} \alpha^{M-i} \beta^N \right)\end{aligned}$$

Now we take the p-adic valuation of γ_i.

$$\begin{aligned}\mathrm{ord}_p(\gamma_i) &= (M+N-i)\cdot \mathrm{ord}_p(a) + \mathrm{ord}_p\left(\binom{N}{i} \alpha^M \beta^{N-i} + \cdots + \binom{M}{i} \alpha^{M-i} \beta^N \right)\\ &\geq (M+N-i)\cdot \mathrm{ord}_p(a)\\ &= g(i)\end{aligned}$$

We have shown that Equation (1) describes $\mathrm{Newt}_p(f)$ for the conditions outlined in Claim (3.1).

■

We may now assume $c = -a^M b^N$.

(1) **Case 2.A.i.** This is the sub-case for which we assume $\text{ord}_p(M) > \text{ord}_p(N)$ with $\text{ord}_p(N) \neq 0$.

Claim. (C.) $\text{Newt}_p(f)$ has at most $\text{ord}_p(N) + 2$ lower edges.

Proof Outline. The vertices of the lower hull of $\text{Newt}_p(f)$ occur at points whose x-coordinates are of the form $x_i = p^i$ with $0 \leq i \leq \text{ord}_p(N)$. There are $\text{ord}_p(N)$ edges adjoining these vertices. The extra 2 edges come from those adjoining (1) the points corresponding to the constant and linear terms, and (2) the points corresponding to $\gamma_{p^{\text{ord}_p(N)}}$ and γ_{M+N}.

First observe the p-adic valuation of γ_1. Let $a = \alpha p^j$ and $b = \beta p^j$ with $\text{ord}_p(a) = \text{ord}_p(b) = j$. Also let $M = \mu p^m$ and $N = \nu p^n$ with $\text{ord}_p(M) = m$ and $\text{ord}_p(N) = n$. We have $m > n$ by assumption.

$$\begin{aligned}
\text{ord}_p(\gamma_1) &= \text{ord}_p(Na^M b^{N-1} + Ma^{M-1}b^N) \\
&= \text{ord}_p(a^{M-1}b^{N-1}) + \text{ord}_p(M\alpha p^j + N\beta p^j) \\
&= (M + N - 1) \cdot j + \text{ord}_p((\mu p^m)\alpha + (\nu p^n)\beta) \\
&= g(1) + n + \text{ord}_p(\mu p^{m-n}\alpha + \nu\beta) \\
&= g(1) + n
\end{aligned}$$

With arbitrarily high $\text{ord}_p(\gamma_0)$, the lower hull of $\text{Newt}_p(f)$ will have a vertex at $(1, g(1) + \text{ord}_p(N))$. For each $x = p^i$ with $1 \leq i \leq \text{ord}_p(N)$, the lower hull of $\text{Newt}_p(f)$ will have a vertex at $(p^i, g(p^i) + \text{ord}_p(N) - i)$. We verify that $\text{ord}_p(\gamma_{p^n})) = g(p^n)$.

$$\begin{aligned}
\text{ord}_p(\gamma_{p^n}) &= \text{ord}_p\left(\binom{N}{p^n}a^M b^{N-p^n} + \cdots + \binom{M}{p^n}a^{M-p^n}b^N\right) \\
&= (M + N - p^n) \cdot \text{ord}_p(a) + \text{ord}_p\left(\binom{N}{p^n}\alpha^{p^n} + \cdots + \binom{M}{p^n}\beta^{p^n}\right) \\
&= g(p^n) + \text{ord}_p\left(\frac{\nu \cdot p^n}{p^n}\binom{N-1}{p^n-1}\alpha^{p^n} + \cdots + \frac{\mu \cdot p^m}{p^n}\binom{M-1}{p^n-1}\beta^{p^n}\right) \\
&= g(p^n) + \text{ord}_p\left(\binom{N-1}{p^n-1}\nu\alpha^{p^n} + \cdots + \binom{M-1}{p^n-1}\beta^{p^n}\mu p^{m-n}\right)
\end{aligned}$$

Every term in the sum is divisible by p except for $\binom{N-1}{p^n-1}\nu\alpha^{p^n}$. By Lemma (2.4), the valuation of the last sum is 0.

Now we consider every x_i with $1 < i < n$. As i increments, the power of p that we are able to factor out of γ_{p^i} decrements. Leftover pieces of the proof involve

- confirming $\text{ord}_p\binom{N-1}{p^n-1} = 0$,
- rigorously verifying $\text{ord}_p(\gamma_{p^i}) = g(p^i) + \text{ord}_p(N) - i$ for $0 < i < \text{ord}_p(N)$, and
- verifying $\text{ord}_p(\gamma_t)$ falls on or above the lines connecting the vertices for all $p^{i-1} < t < p^i$ and for all i.

(2) **Case 2.A.ii.** This is the sub-case for which we assume $\text{ord}_p(M) = \text{ord}_p(N) \neq 0$. *Claim.* (C.) $\text{Newt}_p(f)$ has a sufficiently small number of lower edges.

Discussion. This case is tricky. The bound will be similar to Case 2.A.i, but we cannot use the same methods of determining vertices because the valuations are not as clean.

(3) **Case 2.B.** This is the sub-case for which we assume $p \mid M$ and $p \nmid N$ without loss of generality.

Claim. (C.) $\text{Newt}_p(f)$ has a maximum of two edges.

Proof. If $\mathrm{ord}_p(\gamma_0)$ is arbitrarily high, then $\mathrm{ord}_p(\gamma_i)$ remains unaffected for all i. We show that $\mathrm{ord}_p(\gamma_1) = g(1)$. Let $a = \alpha p^j$ and $b = \beta p^j$ with $\mathrm{ord}_p(a) = \mathrm{ord}_p(b) = j$.

$$\begin{aligned}\mathrm{ord}_p(\gamma_1) &= \mathrm{ord}_p(Na^M b^{N-1} + Ma^{M-1}b^N)\\ &= \mathrm{ord}_p(a^{M-1}b^{N-1}) + \mathrm{ord}_p(N(\alpha p^j) + M(\beta p^j))\\ &= (M+N-1)\cdot j + \mathrm{ord}_p(N\alpha + M\beta)\\ &= g(1) + \mathrm{ord}_p(N\alpha + M\beta)\end{aligned}$$

We have assumed that $p \mid M$ and $p \nmid N$. By Lemma (2.4), $\mathrm{ord}_p(N\alpha + M\beta) = 0$. Thus, $\mathrm{Newt}_p(f)$ has at most two edges described by

$$\begin{aligned}(0, \mathrm{ord}_p(\gamma_0)) &\longleftrightarrow (1, g(1))\\ (1, g(1)) &\longleftrightarrow (M+N, 0)\end{aligned}$$

■

(4) **Case 2.C.** This is the sub-case for which we assume $\mathrm{ord}_p(M) = \mathrm{ord}_p(N) = 0$.

Claim. (C.) The number of edges in the lower hull of $\mathrm{Newt}_p(f)$ is sufficiently small.

Discussion. Consider the p-adic valuation of an arbitrary coefficient. Let $a = \alpha p^j$ and $b = \beta p^j$ with $\mathrm{ord}_p(a) = \mathrm{ord}_p(b) = j$.

$$\begin{aligned}\mathrm{ord}_p(\gamma_i) &= \mathrm{ord}_p\left(\binom{N}{i}a^M b^{N-i} + \cdots + \binom{M}{i}a^{M-i}b^N\right)\\ &= \mathrm{ord}_p(a^{M-i}b^{N-i}) + \mathrm{ord}_p\left(\binom{N}{i}(\alpha p^j)^i + \cdots + \binom{M}{i}(\beta p^j)^i\right)\\ &= (M+N-i)\cdot j + \mathrm{ord}_p\left(\binom{N}{i}\alpha^i + \cdots + \binom{M}{i}\beta^i\right)\\ &= g(i) + \mathrm{ord}_p\left(\binom{N}{i}\alpha^i + \cdots + \binom{M}{i}\beta^i\right)\end{aligned}$$

The valuation of the sum is rather ambiguous. Our usual method of finding the lowest i for which $\mathrm{ord}_p(\gamma_i) = g(i)$ would be highly dependent on individual values of a, b, M, and N.

3.3. **Case 3.** These are the sub-cases for which we assume $\mathrm{ord}_p(a) > \mathrm{ord}_p(b)$. Similarly to Case 2, we investigate our base polygon, the shape of $\mathrm{Newt}_p(f)$ when $c = 0$.

Claim 3.2. (C.) Let $\mathrm{ord}_p(a) > \mathrm{ord}_p(b)$ and $c = 0$. Then $\mathrm{Newt}_p(f)$ has two lower edges described by $h : [0, M+N] \to \mathbb{R}$ defined by:

$$h(x) = \begin{cases} -\mathrm{ord}_p(a)x + (M\cdot\mathrm{ord}_p(a) + N\cdot\mathrm{ord}_p(b)) & \text{if } 0 \le x \le M\\ -\mathrm{ord}_p(b)x + (M+N)\cdot\mathrm{ord}_p(b) & \text{if } M \le x \le M+N\end{cases} \tag{2}$$

Proof. Let $a = \alpha p^j$ and $b = \beta p^k$ with $\mathrm{ord}_p(a) = j$ and $\mathrm{ord}_p(b) = k$. By assumption, $j > k$.

(1) We verify that the endpoints are given correctly by h.

$$\begin{aligned}\mathrm{ord}_p(\gamma_0) &= M\cdot\mathrm{ord}_p(a) + N\cdot\mathrm{ord}_p(b)\\ &= h(0)\\ \mathrm{ord}_p(\gamma_{M+N}) &= 0\\ &= h(M+N)\end{aligned}$$

(2) We show that there is always a point at $(M, N\cdot\mathrm{ord}_p(b))$ by showing $\mathrm{ord}_p(\gamma_M) = N\cdot\mathrm{ord}_p(b)$.

First we express γ_M.

$$\begin{aligned}\gamma_M &= \sum_{j,k|j+k=M} \binom{M}{j}\binom{N}{k}a^{M-j}b^{N-k} \\ &= b^N + \binom{M}{M-1}\binom{N}{1}ab^{N-1} + \cdots + \binom{M}{1}\binom{N}{M-1}a^{M-1}b^{N-M+1} + \binom{N}{M}a^M b^{N-M} \\ &= (p^k)^N\left(\beta^N + MN(\alpha p^{j-k})\beta^{N-1} + \cdots + M\binom{N}{M-1}(\alpha p^{j-k})^{M-1}\beta^{N-M+1} + \binom{N}{M}(\alpha p^{j-k})^M\beta^{N-M}\right)\end{aligned}$$

If $N < M$, note that the final $M - N$ terms will be 0. We take the p-adic valuation of both sides.

$$\operatorname{ord}_p(\gamma_M) = N\cdot\operatorname{ord}_p(b) + \operatorname{ord}_p\left(\beta^N + MN(\alpha p^{j-k})\beta^{N-1} + \cdots + \binom{N}{M}(\alpha p^{j-k})^M\beta^{N-M}\right)$$

The p-adic valuation of the sum will equal 0 by Lemma (2.4). Therefore, $\operatorname{ord}_p(\gamma_M) = N\cdot\operatorname{ord}_p(b)$.

(3) We assume $(M, N\cdot\operatorname{ord}_p(b))$ is a vertex of $\operatorname{Newt}_p(f)$. Thus we draw a line from $(0, M\cdot\operatorname{ord}_p(a) + N\cdot\operatorname{ord}_p(b))$ to $(M, N\cdot\operatorname{ord}_p(b))$, then another line from $(M, N\cdot\operatorname{ord}_p(b))$ to $(M+N, 0)$. The slopes of these two lines are $-\operatorname{ord}_p(a)$ and $-\operatorname{ord}_p(b)$, respectively, which are the slopes of the two pieces of h. We assume these two lines are the lower hull of $\operatorname{Newt}_p(f)$.

(4) We show that $\operatorname{ord}_p(\gamma_i) \geq h(i)$ for $0 < i < M$. First we express γ_i.

$$\begin{aligned}\gamma_i &= \binom{N}{i}a^M b^{N-i} + \cdots + \binom{M}{i}a^{M-i}b^N \\ &= \binom{N}{i}\alpha^M(p^j)^{M-i}(p^{j-k}p^k)^i\beta^{N-i}(p^k)^{N-i} + \cdots + \binom{M}{i}\alpha^{M-i}(p^j)^{M-i}\beta^N(p^k)^N \\ &= (p^j)^{M-i}(p^k)^N\left(\binom{N}{i}\alpha^M\beta^{N-i}(p^{j-k})^i + \cdots + \binom{M}{i}\alpha^{M-i}\beta^N\right)\end{aligned}$$

We take the p-adic valuation of γ_i.

$$\begin{aligned}\operatorname{ord}_p(\gamma_i) &= (M-i)\cdot\operatorname{ord}_p(a) + N\cdot\operatorname{ord}_p(b) + \operatorname{ord}_p\left(\binom{N}{i}\alpha^M\beta^{N-i}(p^{j-k})^i + \cdots + \binom{M}{i}\alpha^{M-i}\beta^N\right) \\ &\geq (M-i)\cdot\operatorname{ord}_p(a) + N\cdot\operatorname{ord}_p(b) \\ &= h(i)\end{aligned}$$

If $p \nmid \binom{M}{i}$, then it is possible for all but one term in the sum to be divisible by p and its valuation could be 0. Thus, $\operatorname{ord}_p(\gamma_i) \geq h(i)$.

(5) We show that $\operatorname{ord}_p(\gamma_i) \geq h(i)$ for $M < i < M + N$. First we express γ_i.

$$\begin{aligned}\gamma_i &= \binom{N}{i}a^M b^{N-i} + \cdots + \binom{M}{i}a^{M-i}b^N \\ &= \binom{N}{i}(\alpha p^{j-k})^M(p^k)^M(\beta p^k)^{N-i} + \cdots + \binom{M}{i}(\alpha p^{j-k})^{M-i}(p^k)^{M-i}(\beta p^k)^N \\ &= (p^k)^{M+N-i}\left(\binom{N}{i}(\alpha p^{j-k})^M\beta^{N-i} + \cdots + \binom{M}{i}(\alpha p^{j-k})^{M-i}\beta^N\right)\end{aligned}$$

We take the p-adic valuation of γ_i.

$$\begin{aligned}\operatorname{ord}_p(\gamma_i) &= (M+N-i)\cdot\operatorname{ord}_p(b) + \operatorname{ord}_p\left(\binom{N}{i}(\alpha p^{j-k})^M\beta^{N-i} + \cdots + \binom{M}{i}(\alpha p^{j-k})^{M-i}\beta^N\right) \\ &\geq (M+N-i)\cdot\operatorname{ord}_p(b)\end{aligned}$$

Because $M < i < M + N$, some monomial term in the sum will have $(p^{j-k})^{M-M} = 1$. Thus, it is possible for all but one term in the sum to be divisible by p and its valuation could feasibly be 0 by Lemma (2.4). Thus, $\operatorname{ord}_p(\gamma_i) \geq h(i)$.

We have shown that Equation (2) describes $\text{Newt}_p(f)$ for the conditions outlined in Claim (3.2).

■

We may now assume $c = -a^M b^N$.

(1) **Case 3.A.** This is the sub-case for which we assume $p \nmid M$.

Claim. (C.) $\text{Newt}_p(f)$ has a maximum of 3 lower edges.

Proof. If $\text{ord}_p(\gamma_0)$ is arbitrarily high, then $\text{ord}_p(\gamma_i)$ remains unaffected for all i. We show that $\text{ord}_p(\gamma_1) = h(1)$. Let $a = \alpha p^j$ and $b = \beta p^k$ with $\text{ord}_p(a)j$ and $\text{ord}_p(b) = k$. By assumption, $j > k$.

$$\begin{aligned}\text{ord}_p(\gamma_1) &= \text{ord}_p(Na^M b^{N-1} + Ma^{M-1}b^N)\\ &= \text{ord}_p(a^{M-1}b^{N-1}) + \text{ord}_p(N(\alpha p^j) + M(\beta p^k))\\ &= (M-1)\cdot j + N\cdot k + \text{ord}_p(N\alpha p^{j-k} + M\beta)\\ &= g(1) + \text{ord}_p(N\alpha p^{j-k} + M\beta)\end{aligned}$$

We have assumed that $p \nmid M$. By Lemma (2.4), $\text{ord}_p(N\alpha p^{j-k} + M\beta) = 0$. Thus, $\text{Newt}_p(f)$ has at most three edges described by

$$\begin{aligned}(0, \text{ord}_p(\gamma_0)) &\longleftrightarrow (1, h(1))\\ (1, h(1)) &\longleftrightarrow (M, N\cdot \text{ord}_p(b))\\ (M, N\cdot \text{ord}_p(b)) &\longleftrightarrow (M+N, 0)\end{aligned}$$

■

(2) **Case 3.B.i.** This is the sub-case for which we assume $p \mid M$. We also make the assumption that $\text{ord}_p(M) \neq \text{ord}_P(N) + \text{ord}_p(a) - \text{ord}_p(b)$.

Claim. (C.) $\text{Newt}_p(f)$ has at most $\text{ord}_p(M) + 3$ lower edges.

Proof Outline. First assume $\text{ord}_p(M) < \text{ord}_p(N) + \text{ord}_p(a) - \text{ord}_p(b)$. Similarly to Case 2.A.i, vertices of $\text{Newt}_p(f)$ occur at points whose x-coordinates are of the form $x_i = p^i$ with $0 \leq i \leq \text{ord}_p(M)$. There are $\text{ord}_p(M)$ edges adjoining these vertices. The extra 3 edges come from those adjoining (1) the points corresponding to the constant and linear terms, (2) the points corresponding to $\gamma_{p^{\text{ord}_p(M)}}$ and γ_M, and (3) the points $(M, N\cdot \text{ord}_p(b))$ and $(M+N, 0)$.

We consider the vertices of $\text{Newt}_p(f)$ whose x-coordinates are of the form $x_i = p^i$ with $0 \leq i \leq \text{ord}_p(M)$. First observe the p-adic valuation of γ_1. Let $a = \alpha p^j$ and $b = \beta p^k$ with $\text{ord}_p(a) = j$ and $\text{ord}_p(b) = k$. By assumption, $j > k$. Also let $M = \mu p^m$ and $N = \nu p^n$ with $\text{ord}_p(M) = m$ and $\text{ord}_p(N) = n$. By assumption, $m < n + j - k$.

$$\begin{aligned}\text{ord}_p(\gamma_1) &= \text{ord}_p(Na^M b^{N-1} + Ma^{M-1}b^N)\\ &= \text{ord}_p(a^{M-1}b^{N-1}) + \text{ord}_p(N(\alpha p^j) + M(\beta p^k))\\ &= (M-1)\cdot \text{ord}_p(a) + N\cdot \text{ord}_p(b) + \text{ord}_p(\nu\alpha p^{n+j-k} + \mu p^m\beta)\\ &= h(1) + m + \text{ord}_p(\nu\alpha p^{n+j-k-m} + \mu\beta)\\ &= h(1) + m\end{aligned}$$

$\text{Newt}_p(f)$ has a vertex at $(1, h(1) + \text{ord}_p(M))$. For each $x_i = p^i$ with $1 \leq i \leq \text{ord}_p(M)$, $\text{Newt}_p(f)$ will have a vertex at $(p^i, h(p^i) + \text{ord}_p(M) - i)$.

The gaps in this proof are identical to those in the proof outline of Case 2.A.i.

Now, if we assume $\text{ord}_p(M) > \text{ord}_p(N) + \text{ord}_p(a) - \text{ord}_p(b)$, the valuation of the linear term changes.

$$\begin{aligned}\text{ord}_p(\gamma_1) &= h(1) + \text{ord}_p(\nu\alpha p^{n+j-k} + \mu\beta p^m)\\ &= h(1) + n + j - k + \text{ord}_p(\nu\alpha + \mu\beta p^{m-n-j+k})\\ &= h(1) + n + j - k\end{aligned}$$

$\text{Newt}_p(f)$ has a vertex at $(1, h(1) + \text{ord}_p(N) + \text{ord}_p(a) - \text{ord}_p(b))$. For each $x_i = p^i$ with $\text{ord}_p(N) + \text{ord}_p(a) - \text{ord}_p(b) + 1 \leq i \leq \text{ord}_p(M)$, $\text{Newt}_p(f)$ will have a vertex at $(p^i, h(p^i) + \text{ord}_p(N) + \text{ord}_p(a) - \text{ord}_p(b) - i)$. This is because, as i increments, the highest power of p that we are able to factor out of γ_{p^i} decrements. There are $\text{ord}_p(N) + \text{ord}_p(a) - \text{ord}_p(b)$ edges adjoining every x_i; thus, we can bound the number of lower edges by $\text{ord}_p(N) + \text{ord}_p(a) - \text{ord}_p(b) + 3$. However, because we have assumed $\text{ord}_p(M) > \text{ord}_p(N) + \text{ord}_p(a) - \text{ord}_p(b)$, we prefer the upper bound of $\text{ord}_p(M) + 3$ that does not rely on $\text{ord}_p(a)$ or $\text{ord}_p(b)$.

(3) **Case 3.B.ii.** This is the sub-case for which we assume $p \mid M$ with $\text{ord}_p(M) = \text{ord}_p(N) + \text{ord}_p(a) - \text{ord}_p(b)$.

Claim. (C.) $\text{Newt}_p(f)$ has a sufficiently small number of lower edges.

Discussion. We can see where this case becomes complicated by reevaluating the p-adic valuation of the linear coefficient. Let $a = \alpha p^j$ and $b = \beta p^k$ with $\text{ord}_p(a) = j$ and $\text{ord}_p(b) = k$. Also let $M = \mu p^m$ and $N = \nu p^n$ with $\text{ord}_p(M) = m$ and $\text{ord}_p(N) = n$. By assumption, $m = n + j - k$.

$$\begin{aligned}\text{ord}_p(\gamma_1) &= \text{ord}_p(Na^M b^{N-1} + Ma^{M-1}b^N) \\ &= (M-1) \cdot \text{ord}_p(a) + N \cdot \text{ord}_p(b) + \text{ord}_p(\nu\alpha p^{n+j-k} + \mu\beta p^m) \\ &= h(1) + m + \text{ord}_p(\nu\alpha + \mu\beta)\end{aligned}$$

The valuation of $\nu\alpha + \mu\beta$ is ambiguous. We also encounter ambiguous valuations at every point that would have been a vertex if not for the assumption $\text{ord}_p(M) = \text{ord}_p(N) + \text{ord}_p(a) - \text{ord}_p(b)$. Although a bound evades us for this case, it seems that the bound will be similar to that of Case 3.B.i.

3.4. **Looking Forward.** We have established some cases towards our desired upper bound of $O(\log_p(M + N))$. In the future, we seek to rigorously prove some of the bounds that we have conjectured and to tighten some of the bounds that we have already proven. We also see potential to generalize our conjectured bound to SPS-polynomials of the form $(x + a_1)^{M_1}(x + a_2)^{M_2} \cdots (x + a_n)^{M_n} + b$.

4. A Multivariate Approach (S.)

We now transition to using p-adic techniques to look at a system of multivariate polynomials. We are again interested in finding an upper bound on the number of unique valuations of the roots. First, let us establish some notation. [2]

Definition 4.1. Let $A_1, \cdots, A_n \in \mathbb{Z}^n$ be finite subsets. Let $F := (f_1, \cdots, f_n)$ be a system of polynomials with $f_i \in \mathbb{C}_p[x_1, \cdots, x_n]$ and $\text{Supp}(f_i) \in A_i$. Let $A := \bigcup_i A_i$ and $t := \#A$.

F is defined as a system of n equations in n variables. Each $f_i \in F$ has supports coming from a finite subset A_i. Let us also define a special set on which we want to find sufficiently good upper bounds.

Definition 4.2. Define $\overline{\mathcal{V}}_p(A_1, \cdots, A_n)$ to be the maximum cardinality of $\text{ord}_p\left(Z^*_{\mathbb{C}_p}(F)\right)$ ranging all F as given in Definition 4.1 with $Z^*_{\mathbb{C}_p}(F)$ finite.

We are particularly interested in the case with $t = n + 2$ because every multivariate system of this form can be reduced to a univariate polynomial in a certain SPS class.

Theorem 4.3. With the notation as in Definitions 4.1 and 4.2, if [$t = n+2$ and for all pairs (i, j) with $i \neq j$ then any n-tuple of vectors emanating from a_i (or a_j) to some a_k (with $k \notin (i, j)$) are linearly independent], then $\overline{\mathcal{V}}_p(A_1, \cdots, A_n) \leq \max\{2, \lfloor \frac{n}{2} \rfloor^n + n\}$. [2]

Note: From now on we refer to "the genericity hypothesis" as the assumption on the linear independence of the support vectors in Theorem 4.3. One point of progress we made this summer was improving the wording of the genericity hypothesis.

4.1. **Reducing the problem.** We may reduce to the problem to looking a specific arrangement of hyperplanes in $\mathbb{R}^n$. We obtain this reduction of the problem by the proof of Theorem (4.3) in [2]. The key ingredients in the proof are Gaussian Elimination and the Fundamental Theorem of Tropical Geometry.

We now describe the particular set-up of the problem. Given $F := (f_1, \cdots, f_n)$ with $f_i \in \mathbb{C}_p[x_1, \cdots, x_n]$ with $A = \bigcup_i \text{Supp}(f_i)$ and $t = n + 2$. We also assume that the system cannot be reduced an earlier case outlined in the paper.

For each pair (i, j) with $i \neq j$ we have a configuration $C_{i,j}$ comprised of n objects each of which we will call a "hyper-Y". First, we apply our Guassian Elimination technique outlined in [2] to the system F and obtain n equations where each of the n other terms may be expressed as linear combinations of x^{a_i} and x^{a_j}. Call these n equations the system $G := (g_1, \cdots, g_n)$.

Now, each hyper-Y is specified by one of the g_i's. More specifically, it is exactly $\text{Trop}_p(g_i)$. We therefore have that $\text{Trop}_p(g_i)$ is dual to a triangle. The rays of the hyper-Y are inner normals of the triangle formed by the three support vectors in g_i. We may regard a hyper-Y as (three rays emanating from a point in a plane)$\times\mathbb{R}^{n-1}$.

In each hyper-Y we make the distinction between the three rays. One we will call the "stem" and the other two will be the "wings." It can be shown based on the geometry of the triangle that the two wings will emanate from opposite halves of the hyperplane given by the stem.

In the configuration $C_{i,j}$, we will have n hyper-Y's in which n stems will be parallel to a common hyperplane. Therefore, we may loosely partition $\mathbb{R}^n$ into up to $n+1$ "slabs" which are separated by up to n hyperplanes. We refer to the up to n hyperplanes that separate these slabs as "slab boundaries." We want to explore bounds on the intersections of these n hyper-Y's.

Lemma 4.4. Any intersection of the $\text{Trop}_p(g_i)$ that does not occur on a slab boundary must be a non-degenerate intersection. [2]

Therefore, we only need to study possible intersections which occur on the slab boundaries. Note that non-degenerate intersections may occur on slab-boundaries.

4.2. **Degenerate intersections within slab boundaries.** We are most concerned about degenerate intersections that occur within the slab boundaries because there are an infinite number of points in the intersection but we want a finite bound.

The first tool is to redo the Gaussian Elimination on a coefficient matrix of F where the terms are permuted, that is consider a different $C_{i',j'}$. This gives a completely different set of tropical varieties. Even if there is a degenerate intersection within this set, we can determine that the valuations of the roots of F is contained in the intersection of degenerate intersections of the different $C_{i,j}$'s. The genericity hypothesis also gives us some information on the linear independence of the hyperplanes in the $C_{i,j}$'s.

We are most interested in proving the following conjecture.

Conjecture 4.5. The bound from Theorem 4.3 can be improved to be sub-exponential. It can be improved to the sharp bound $n + 1$. [2]

Currently, we are working on reducing the possible intersection of the hyper-Y's into manageable cases. One of the nicest cases is the following:

Lemma 4.6. Consider the case in which each configuration $C_{i,j}$ yields that all of the stems of the hyper-Y's lie exactly on the common hyperplane for all pairs (i, j) with $i \neq j$. Then an upper bound on the number of distinct valuations of the roots of F is $2n + 1$.

Proof. Consider such a configuration $C_{i,j}$ in which all stems of the hyper-Y's lie on the common hyperplane. Within each $C_{i,j}$, there is a maximum of one $(n - 1)$-dimensional intersection and two points (one non-degenerate intersection on either half of the common hyperplane). If we take the intersection over n such

$C_{i,j}$, then we have n hyperplanes which intersect in at most one point thanks to the genericity hypothesis. Therefore, there are a maximum of $2n+1$ possible points.

■

We consider other such extreme cases, such as when a configuration yields $\lfloor \frac{n}{2} \rfloor$ slab boundaries where two hyper-Y stems share a slab boundary. The original bound in [2] does not consider the fact that the degenerate intersections possible on the slab boundaries will not be full hyperplanes. In the future, we will use this observation to our benefit as we work towards our overall bound of $n+1$.

5. Acknowledgements

The authors conducted their research at Texas A&M University's 2016 Algorithmic Algebraic Geometry Research Experience for Undergraduates. They deeply thank their P.I. Dr. J. Maurice Rojas and their graduate T.A.s Kaitlyn Phillipson, Yuyu Zhu, and Alperen Ergür for patiently and generously investing in the authors' futures. The authors also thank the National Science Foundation, which funded their research experience via the REU-Site grant DMS-1460766 to Dr. J. Maurice Rojas and Dr. Anne Shiu.

References

[1] Gouvêa, Fernando Q. *p-adic Numbers: An Introduction,* 2nd ed. New York: Springer-Verlag, 1997.
[2] P. Koiran, N. Portier, and J. M. Rojas. "Counting Tropically Degenerate Valuations and p-adic Approaches to the Hardness of the Permanent," submitted for publication.
[3] Rojas, J. Maurice. "Efficiently Estimating Norms of Complex Roots of Multivariate Polynomials."
[4] Weiss, Edwin. *Algebraic Number Theory.* New York: McGraw-Hill Book Company, Inc., 1963. Print.