FEWNOMIAL SYSTEMS WITH MANY ROOTS, AND AN ADELIC TAU CONJECTURE

KAITLYN PHILLIPSON* AND J. MAURICE ROJAS

To Bernd Sturmfels on his $50^{\underline{th}}$ birthday.

Abstract. Consider a system F of n polynomials in n variables, with a total of $n+k$ distinct exponent vectors, over any local field L. We discuss conjecturally tight bounds on the maximal number of non-degenerate roots F can have over L, with all coordinates having fixed phase, as a function of n, k, and L only. In particular, we give new explicit systems with number of roots approaching the best known upper bounds. We also briefly review the background behind such bounds, and their application, including connections to computational number theory and variants of the Shub-Smale τ-Conjecture and the **P** vs. **NP** Problem. One of our key tools is the construction of combinatorially constrained tropical varieties with maximally many intersections.

1. Introduction

Let L be any local field, i.e., $\mathbb{C}$, $\mathbb{R}$, any finite algebraic extension of $\mathbb{Q}_p$, or $\mathbb{F}_q((t))$. Also let $f_1, \ldots, f_n \in L\left[x_1^{\pm 1}, \ldots, x_n^{\pm 1}\right]$ be Laurent polynomials such that the total number of distinct exponent vectors in the monomial term expansions of $f_1, \ldots, f_n$ is $n+k$. We call $F := (f_1, \ldots, f_n)$ an $(n+k)$-*nomial* $n \times n$ *system over* L. We study the distribution of the non-degenerate roots[1] of F in the multiplicative group $(L^*)^n$, as a function of n, k, and L only. This is a fundamental problem in *fewnomial theory over local fields*. Our main focus will be the number of roots in a fixed angular direction from the origin.

Fewnomial theory over $\mathbb{R}$ has since found applications in Hilbert's $16^{\underline{\text{th}}}$ Problem [Kal03], the complexity of geometric algorithms [GV01, VG03, BRS09, PRT09, BS11, BHPR11, Koi11, KPT12], model completeness for certain theories of real analytic functions [Wil99, Ser08], and the study of torsion points on curves [CZ02]. Fewnomial theory over number fields has applications to sharper uniform bounds on the number of torsion points on elliptic curves [Che04], integer factorization [Lip94], additive complexity [Roj02], and polynomial factorization and interpolation [Len99a, KK06, AKS07, GR10, CGKPS12]. In Section 2 we also present an application of general fewnomial bounds to circuit complexity. Since any number field embed in some finite extension of $\mathbb{Q}_p$, we thus have good reason to study fewnomial bounds over non-Archimedean fields. However, for $n, k \geq 2$, *tight* bounds remain elusive [LRW03, Roj04, BS07, AI10, AI11].

Definition 1.1. *Let $y \in L^*$. When $L \in \{\mathbb{R}, \mathbb{C}\}$ we let $|y|$ denote the usual absolute value and define $\phi(y) := \frac{y}{|y|}$ to be the* generalized phase *of y. In the non-Archimedean case, we let $\mathfrak{M}$ denote the unique maximal ideal of the ring of integers of L and call any generator ρ of $\mathfrak{M}$ a* uniformizer *for L. Letting* ord *denote the corresponding valuation on L we then alternatively define the generalized phase as $\phi(y) := \frac{y}{\rho^{\operatorname{ord} y}}$ mod $\mathfrak{M}$. Finally, for general local L, we define*

Key words and phrases. sparse polynomial, tau conjecture, local field, positive characteristic, lower bounds, mixed cell, straight-line program, complexity.

*née Hellenbrand.

K.P. and J.M.R. were partially supported by NSF MCS grant DMS-0915245 and DOE ASCR grant DE-SC0002505. J.M.R. was also partially supported by Sandia National Laboratories.

[1] i.e., roots with Jacobian of rank n

$Y_L(n,k)$ to be the supremum, over all $(n+k)$-nomial $n\times n$ systems F over L, of the number of non-degenerate roots of F in L^n with all coordinates having generalized phase 1. $\diamond$

Note that $y\in\mathbb{C}$ has generalized phase 1 if and only if y is positive. In the non-Archimedean case, $\phi(y)$ can be regarded simply as the first digit of an expansion of y as a Laurent series in ρ. It is well-known in number theory that $\phi(y)$ is a natural extension of the argument (or angle with respect to the positive ray) of a complex number.[2] Our choices of uniformizer and angular direction above are in fact immaterial for the characteristic zero case: see Proposition 5.1 of Section 5, which also discusses the positive characteristic case.

Descartes' classic $17^{\underline{\text{th}}}$ century bound on the number of positive roots of a sparse (a.k.a. lacunary) univariate polynomial [SL54, Wan04], along with some late to post-20th century univariate bounds of Voorhoeve, H. W. Lenstra (Jr.), Poonen, Avendano, and Krick, can then be recast as follows:

Theorem 1.2. *Let p be prime and $k\geq 1$. Then: (1) $Y_{\mathbb{R}}(1,k)=k$ and $Y_{\mathbb{C}}(1,k)=k$, (2) $Y_{\mathbb{Q}_2}(1,1)=2$, (3) $Y_{\mathbb{Q}_2}(1,2)=6$, (4) $Y_{\mathbb{Q}_p}(1,1)=1$ for $p\geq 3$, (5) $Y_{\mathbb{Q}_p}(1,2)=3$ for $p\geq 5$, and (6) $Y_{\mathbb{F}_q((t))}(1,k)=\frac{q^k-1}{q-1}$ for any prime power q. Also: (7) $Y_{\mathbb{Q}_2}(1,k)\geq 2k$, (8) $3\leq Y_{\mathbb{Q}_3}(1,2)\leq 9$, (9) $Y_{\mathbb{Q}_p}(1,k)\geq 2k-1$ for $p\geq 3$, and (10) $Y_{\mathbb{Q}_p}(1,k)\leq k^2-k+1$ for $p>1+k$.* $\blacksquare$

Remark 1.3. *The assertions above are immediate consequences of* [SL54, pg. 160], [Voo76, Cor. 2.1], [Len99b, Example, pg. 286 & pp. 289–290], [AK11, Thm. 1.4, Ex. 1.5, & Thm. 1.6], *and* [Poo98, Sec. 2]. *Also, the polynomials $\prod_{i=1}^{k}(x_1-i)$, $3x_1^{10}+x_1^2-4$, $x_1^{1+p^{p-1}}-(1+p^{p-1})x_1+p^{p-1}$, $\prod\limits_{z_1,\ldots,z_{k-1}\in\mathbb{F}_q}(x_1-z_1-z_2t-\cdots-z_{k-1}t^{k-1})$, and $\prod_{i=1}^{k}(x_1^2-4^{i-1})$ respectively attain the number of roots stated in Assertions (1), (3), (5), (6), and (7).* $\diamond$

$Y_L(1,1)$ can in fact grow without bound if we let L range over arbitrary finite extensions of $\mathbb{Q}_p$.[3] Note also that for any local field $L\neq\mathbb{C}$ and fixed (n,k), the supremum of the *total* number of roots of F in $(L^*)^n$ — with no restrictions on the phase of the coordinates — is easily derivable from $Y_L(n,k)$ (see Proposition 5.1 of Section 5).

We treat the general multivariate case in Sections 1.1 and 1.2, where we state our main results. As a warm-up, let us first unite the simplest multivariate cases (proved in Section 5).

Proposition 1.4. *For any $k\leq 0$, $n\geq 1$, and any local field L, we have $Y_L(n,k)=0$. Also, $Y_L(n,1)=Y_L(1,1)^n$. In particular, $Y_{\mathbb{Q}_2}(n,1)=2^n$ and $Y_L(n,1)=1$ for all $L\in\{\mathbb{C},\mathbb{R}\}\cup\{\mathbb{Q}_3,\mathbb{Q}_5,\ldots\}\cup\{\mathbb{F}_q((t))\mid q$ a prime power$\}$.*

1.1. **New, Simple Systems with Many Roots.** For any $j,N\in\mathbb{N}$ let $[j]_N\in\{0,\ldots,N-1\}$ denote the mod N reduction of j.

Theorem 1.5. *For any local field L, $Y_L(n,2)\geq\max\{Y_L(1,1)^{n-1}Y_L(1,2),n+1\}$. More generally, $Y_L(n,k)\geq\max\left\{Y_L(1,1)^{n-k+1}Y_L(1,2)^{k-1}, Y_L\left(\left\lfloor\frac{n}{k-1}\right\rfloor,2\right)^{k-1-[n]_{k-1}}Y_L\left(\left\lfloor\frac{n}{k-1}\right\rfloor+1,2\right)^{[n]_{k-1}}\right\}$ when $n\geq k-1\geq 1$, and $Y_L(n,k)\geq Y_L\left(1,\left\lfloor\frac{n+k-1}{n}\right\rfloor\right)^{n-[k-1]_n}Y_L\left(1,\left\lfloor\frac{n+k-1}{n}\right\rfloor+1\right)^{[k-1]_n}$ when $1\leq n\leq k-1$. More explicitly, the following lower bounds hold:*

[2]See, e.g., Schikhof's notion of *sign group* in [Sch84, Sec. 24, pp. 65–67].

[3]For instance, when L is the splitting field of $g(x_1):=x_1^p-1$ over $\mathbb{Q}_p$, g has roots $1,1+\mu_1,\ldots,1+\mu_{p-1}$ where the μ_i are distinct elements of L, each with valuation $\frac{1}{p-1}$ (see, e.g., [Rob00, pp. 102–109]).

L	$n\geq k-1\geq 1$	$1\leq n\leq k-1$
$\mathbb{R}$	$\left\lfloor\frac{n+k-1}{k-1}\right\rfloor^{k-1-[n]_{k-1}}\left\lfloor\frac{n+2k-2}{k-1}\right\rfloor^{[n]_{k-1}}$	$\left\lfloor\frac{n+k-1}{n}\right\rfloor^{n-[k-1]_n}\left\lfloor\frac{2n+k-1}{n}\right\rfloor^{[k-1]_n}$
$\mathbb{Q}_2$	2^n3^{k-1}	$2^n\left\lfloor\frac{n+k-1}{n}\right\rfloor^{n-[k-1]_n}\left\lfloor\frac{2n+k-1}{n}\right\rfloor^{[k-1]_n}$
$\mathbb{Q}_p\ (p\geq 3)$	$\left\lfloor\frac{n+k-1}{k-1}\right\rfloor^{k-1-[n]_{k-1}}\left\lfloor\frac{n+2k-2}{k-1}\right\rfloor^{[n]_{k-1}}$	$\left(2\left\lfloor\frac{n+k-1}{n}\right\rfloor-1\right)^{n-[k-1]_n}\left(2\left\lfloor\frac{n+k-1}{n}\right\rfloor+1\right)^{[k-1]_n}$
$\mathbb{F}_q((t))$	$\max\left\{q+1,\left\lfloor\frac{n+k-1}{k-1}\right\rfloor\right\}^{k-1-[n]_{k-1}}\max\left\{q+1,\left\lfloor\frac{n+2k-2}{k-1}\right\rfloor\right\}^{[n]_{k-1}}$	$\left(\frac{q^{\left\lfloor\frac{n+k-1}{n}\right\rfloor}-1}{q-1}\right)^{n-[k-1]_n}\left(\frac{q^{\left\lfloor\frac{2n+k-1}{n}\right\rfloor}-1}{q-1}\right)^{[k-1]_n}$

The lower bound $Y_{\mathbb{R}}(n,2)\geq n+1$ was first proved through an ingenious application of Dessins d'Enfants [Bih07]. We attain our more general lower bound for $Y_L(n,2)$ via an explicit family of polynomial systems instead. Note also that the $L=\mathbb{R}$ case of our general lower bound slightly improves an earlier $\left\lfloor\frac{n+k-1}{\min\{n,k-1\}}\right\rfloor^{\min\{n,k-1\}}$ lower bound from [BRS07]. Non-trivial lower bounds, for $n\geq k-1\geq 2$, were unknown for the non-Archimedean case.

Letting $\mathbb{R}^n_+$ denote the positive orthant, $\bar{L}$ the algebraic closure of L, and defining $\mathrm{ord}\ x := -\log|x|$ in the Archimedean case, our new family of extremal systems can be described as follows:

Theorem 1.6. *For any $n\geq 2$, any local field L, and any $\varepsilon\in L^*$ with generalized phase 1 and $\mathrm{ord}\,\varepsilon$ sufficiently large, the roots in $\bar{L}^n$ of the $(n+2)$-nomial $n\times n$ system G_ε defined by*

$$\left(x_1x_2-\varepsilon\left(1+\frac{x_1^2}{\varepsilon}\right),x_2x_3-\left(1+\varepsilon x_1^2\right),x_3x_4-\left(1+\varepsilon^3x_1^2\right),\ldots,x_{n-1}x_n-\left(1+\varepsilon^{2n-5}x_1^2\right),x_n-\left(1+\varepsilon^{2n-3}x_1^2\right)\right)$$

are all non-degenerate, lie in $(L^*)^n$, and have generalized phase 1 for all their coordinates. In particular, G_ε has exactly $n+1$ non-degenerate roots in $\mathbb{R}^n_+$, $(\mathbb{Q}_p^*)^n$, or $(\mathbb{F}_q((t))^*)^n$ (each with generalized phase 1 for all its coordinates), according as ε is $1/4$, p, or t.

Explicit examples evincing $Y_{\mathbb{R}}(n,2)\geq n+1$ were previously known only for $n\leq 3$ [BRS07]. Our new extremal examples from Theorem 1.6 provide a new and arguably simpler proof that $Y_{\mathbb{R}}(n,2)\geq n+1$. We prove Theorems 1.5 and 1.6 in Sections 4.1 and 4.2, respectively.

Remark 1.7. *By construction, when we are over $\mathbb{Q}_p$ or $\mathbb{F}_q((t))$, the underlying tropical varieties of the zero sets defined by G_ε have a common form: they are each the Minkowski sum of an $(n-2)$-plane and a "Y" lying in a complementary 2-plane. (See Section 3 for further background and Section 3.1 for some illustrations.) Furthermore, all these tropical varieties contain half-planes parallel to a single $(n-1)$-plane. It is an amusing exercise to build such a collection of tropical varieties so that they have at least $n+1$ isolated intersections. However, it is much more difficult to build a collection of polynomials whose tropical varieties have this property, and this constitutes a key subtlety behind Theorem 1.6.* $\diamond$

Another important construction underlying Theorem 1.6 is a particular structured family of univariate polynomials.

Lemma 1.8. *For any $n\geq 2$, the degree $n+1$ polynomial R_n defined by*

$$u(1+\varepsilon u)^2(1+\varepsilon^5u)^2\cdots(1+\varepsilon^{4\lfloor n/2\rfloor-3}u)^2-\varepsilon^2\left(1+\tfrac{u}{\varepsilon}\right)^2(1+\varepsilon^3u)^2(1+\varepsilon^7u)^2\cdots(1+\varepsilon^{4\lceil n/2\rceil-5}u)^2$$

has exactly $n+1$ roots in $\mathbb{R}_+$, $\mathbb{Q}_p^*$, or $\mathbb{F}_p((t))^*$, according as ε is $1/4$, p, or t. In particular, for these choices of ε, all the roots of R_n have generalized phase 1.

We will see in Section 2 how the R_n are part of a more general class of polynomials providing a bridge between fewnomial theory and algorithmic complexity. Lemma 1.8 is proved in Section 4.3.

1.2. **Upper Bounds: Known and Conjectural.** That $Y_{\mathbb{R}}(n,k)<\infty$ for $n\geq 2$ was first proved around 1979 by Khovanskii and Sevastyanov [Kho80, Kho91], yielding an explicit, singly-exponential upper bound. Based on the seminal results [DvdD88, Pg. 105], [Lip88, Thm. 2], and [Len99b], the second author proved in [Roj01, Thm. 1] that $Y_L(n,k)<\infty$ for any fixed n, k, and non-Archimedean field L of characteristic zero. (See [Roj04] and the table below for explicit upper bounds.) The finiteness of $Y_{\mathbb{F}_q((t))}(n,k)$ for $n\geq 2$ remains unknown, in spite of recent results of Avendaño and Ibrahim [AI11] giving explicit upper bounds for the number of roots in L^n of a large class of $n\times n$ systems over any non-Archimedean local field L.

We will use Landau's O-notation for asymptotic upper bounds modulo a constant multiple, along with the companion Ω-notation for asymptotic lower bounds. The best known upper and lower bounds on $Y_L(n,k)$ (as of November 2012), for $L\in\{\mathbb{R},\mathbb{Q}_3,\mathbb{Q}_5,\ldots\}$ and $n,k\geq 2$, can then be summarized as follows:

L	Upper Bound on $Y_L(n,k)$	Lower Bound on $Y_L(n,k)$
$\mathbb{R}$	$2^{O(k^2)}n^{k-1}$ [BS07][4]	$\Omega\left(\left\lfloor\frac{n+k-1}{\min\{n,k-1\}}\right\rfloor\right)^{\min\{n,k-1\}}$ (Theorem 1.5 here)
$\mathbb{Q}_p$	$(O(k^3 n\log k))^n$ [Roj04]	$\Omega\left(\left\lfloor\frac{n+k-1}{\min\{n,k-1\}}\right\rfloor\right)^{\min\{n,k-1\}}$ (Theorem 1.5 here)

Also, Bertrand, Bihan, and Sottile proved the (tight) upper bound $Y_{\mathbb{R}}(n,2)\leq n+1$ in [BBS05]. The implied Ω-constants above can be taken to be 1.

Most importantly, note that for the Archimedean case (resp. the p-adic rational case with $p\geq 3$), $Y_L(n,k)$ is bounded from above by a polynomial in n when k is fixed (resp. a polynomial in k when n is fixed). Based on this asymmetry of upper bounds, the second author posed the following conjecture (mildly paraphrased) at his March 20 Geometry Seminar talk at the Courant Institute in March 2007.

The Local Fewnomial Conjecture.
There are absolute constants $C_2\geq C_1>0$ such that, for any $L\in\{\mathbb{C},\mathbb{R},\mathbb{Q}_3,\mathbb{Q}_5,\ldots\}$ and any $n,k\geq 2$, we have $(n+k-1)^{C_1\min\{n,k-1\}}\leq Y_L(n,k)\leq (n+k-1)^{C_2\min\{n,k-1\}}$.

Remark 1.9. *Should the Local Fewnomial Conjecture be true, it is likely that similar bounds can be asserted for the number of roots counting multiplicity, in the characteristic zero case. This is already known for $(L,n)=(\mathbb{R},1)$* [Wan04], *and* [Len99b, Roj04] *provide evidence for the p-adic rational case. Note, however, that the equality $(x_1+1)^{q^m+1}=x_1^{q^m+1}+x_1^{q^m}+x_1+1$ over $\mathbb{F}_q$ (as observed in* [Poo98]*) tells us that for L of positive characteristic it is impossible to count roots over L^** — with multiplicity — *solely as a function of n, k, and L.* $\diamond$

Theorem 1.5 thus reveals the lower bound of the Local Fewnomial Conjecture to be true (with $C_1=1$) for the special case $k=2$. From our table above we also see that the upper bound from the Local Fewnomial Conjecture holds for $n\leq k-1$ (at least for $C_2\geq 7$), in

[4]While there have been important recent refinements to this bound (e.g., [RSS11]) the asymptotics of [BS07] have not yet been improved in complete generality.

the p-adic rational setting. We intend for our techniques here to be a first step toward establishing the Local Fewnomial Conjecture for $n>k-1$ in the p-adic rational setting.

Note that the maximal number of roots in $(\mathbb{C}^*)^n$ of an $(n+k)$-nomial $n\times n$ system F over $\mathbb{C}$ is undefined for any fixed n and k: consider $((x_1^d-1)\cdots(x_1^d-k), x_2-1,\ldots,x_n-1)$ as $d\longrightarrow\infty$. Nevertheless, the maximal number of roots in $\mathbb{R}^n_+$ is well-defined and finite for any fixed $n,k\geq 1$. The latter assertion is a very special case of Khovanski's *Theorem on Complex Fewnomials* (see [Kho91, Thm. 1 (pp. 82–83), Thm. 2 (pp. 87–88), and Cor. 3′ (pg. 88)]), which estimates the number of roots in angular sub-regions of $\mathbb{C}^n$ for a broad class of analytic functions. [Kho91] does not appear to state any explicit upper bounds for $Y_{\mathbb{C}}(n,k)$, but one can in fact show (see Section 5) that it suffices to study the real case.

Theorem 1.10. *For all $n,k\geq 1$, we have $Y_{\mathbb{C}}(n,k)=Y_{\mathbb{R}}(n,k)$.*

We now discuss the number of roots, over a local field, of certain non-sparse univariate polynomials that nevertheless admit a compact expression, e.g., $(x_1^9+1)^{1000}-(x_1-3)^{2^8}$. This refinement leads us to computational number theory and variants of the famous **P** *vs.* **NP** *Problem*. As we will see shortly, complexity theory leads us to challenging open problems that can be stated entirely within the context of arithmetic geometry.

2. Applications and New Conjectures on Straight-Line Programs

To better discuss the connections between structured polynomials and algorithms let us first introduce the notions of *input size* and *complexity* through a concrete example. [BS96] is an outstanding reference for basic algorithmic number theory and [Sip92, Pap95, AB09, For09, Lip09] are among many excellent sources for further background on complexity theory and the history of the **P** vs. **NP** Problem.

Example 2.1. *Consider the following problem:*

> **A:** *Given any prime p and $f\in\mathbb{F}_p[x_1]$ with degree d and $d<p$, decide whether f has a root in $\mathbb{F}_p$.*

Let us naturally define the input size of an instance (p,f) of Problem A as the number of decimal digits needed to write down p and the monomial term expansion of f. (Thus, for example, $a+bx^{11}+cx^d$ would have size $O(\log p)$ since $a,b,c,d\in\{0,\ldots,p-1\}$.) To measure the complexity of a computation over $\mathbb{F}_p$, we can then simply count the number of digit by digit operations (i.e., addition, subtraction, multiplication, and parity checking) that we use. For instance, via fast mod n arithmetic (e,g., [BS96, Ch. 5]*), it is easy to see that evaluating f at a point in $\mathbb{F}_p$ has complexity near-linear in the input size (a.k.a. near-linear* time*).*

Curiously, no method with complexity polynomial in the input size is known for Problem A, although a putative root can be certainly be verified in polynomial-time.[5] $\diamond$

The complexity of evaluating a polynomial turns out to be a more intrinsic measure of its size than counting digits in monomial term expansions. In particular, many non-sparse polynomials can still be evaluated efficiently since they may admit other kinds of compact expressions. One central notion refining our preceding definition of input size is *straight-line program (SLP) complexity*.

Definition 2.2. *For any field K and $f\in K[x_1]$ let $s(f)$ — the* SLP complexity of f *— denote the smallest n such that $f=f_n$ identically where the sequence $(f_{-N},\ldots,f_{-1},f_0,\ldots,f_n)$*

[5] Technically, Problem A is in **NP**, and is **NP**-hard with respect to randomized reductions [BCR12].

satisfies the following conditions: $f_{-1},\ldots,f_{-N}\in K$, $f_0:=x_1$, *and, for all* $i\geq 1$, f_i *is a sum, difference, or product of some pair of elements* (f_j,f_k) *with* $j,k<i$. *Finally, for any* $f\in\mathbb{Z}[x_1]$, *we let* $\tau(f)$ *denote the obvious analogue of* $s(f)$ *where the definition is further restricted by assuming* $N=1$ *and* $f_{-1}:=1$. $\diamond$

Note that we always have $s(f)\leq\tau(f)$ since s does not count the cost of computing large integers (or any constants).

Example 2.3. *Evaluating* $x_1^{2^k}$ *via recursive squaring (i.e.,* $(\cdots(x_1^2)^2\cdots)^2$*), and employing the binary expansion of* d*, it is easily checked that* $s\left(x_1^d\right)=\tau\left(x_1^d\right)=O\left(\log^2 d\right)$. *One in fact has* $\tau(n)\leq 2\log_2 n$ *for any* $n\in\mathbb{N}$ [dMS96, Prop. 1] *and, when* n *is a difference of two nonnegative integers with at most* δ *nonzero digits in their binary expansions, we also obtain* $s(n)=1$ *and* $\tau(n)=O(\delta(\log\log|n|)^2)$. *See also* [Bra39, Mor97] *for further background.* $\diamond$

Relating SLP complexity to the number of rational roots of polynomials provides a delightfully direct way to go from the theory of sparse polynomials to deep open questions in complexity theory and computational number theory. In what follows, we let $Z_R(f)$ denote the set of roots of f in a ring R, and use $\#S$ for the cardinality of a set S.

Theorem 2.4.

I. *(See* [BCSS98, Thm. 3, Pg. 127] *and* [Bür09, Thm. 1.1]*.) Suppose that for all nonzero* $f\in\mathbb{Z}[x_1]$ *we have* $\#Z_{\mathbb{Z}}(f)\leq(\tau(f)+1)^{O(1)}$. *Then* $\mathbf{P}_{\mathbb{C}}\neq\mathbf{NP}_{\mathbb{C}}$, *and the permanent of* $n\times n$ *matrices cannot be computed by constant-free, division-free arithmetic circuits of size* $n^{O(1)}$.

II. *(Weak inverse to (I)* [Lip94].[6]*) If there is an* $\varepsilon>0$ *and a sequence* $(f_n)_{n\in\mathbb{N}}$ *of polynomials in* $\mathbb{Z}[x_1]$ *satisfying:*

  (a) $\#Z_{\mathbb{Z}}(f_n)>e^{\tau(f_n)^{\varepsilon}}$ *for all* $n\geq 1$ *and (b)* $\deg f_n, \max\limits_{\zeta\in Z_{\mathbb{Z}}(f)}|\zeta|\leq 2^{(\log\#Z_{\mathbb{Z}}(f_n))^{O(1)}}$

  then, for infinitely many n*, at least* $\frac{1}{n^{O(1)}}$ *of the* n *digit integers that are products of exactly two distinct primes (with an equal number of digits) can be factored by a Boolean circuit of size* $n^{O(1)}$.

III. *(Number field analogue of (I) implies Uniform Boundedness* [Che04]*.) Suppose that for any number field* K *and* $f\in K[x_1]$ *we have* $\#Z_K(f)\leq c_1 1.0096^{s(f)}$, *with* c_1 *depending only on* $[K:\mathbb{Q}]$. *Then there is a constant* $c_2\in\mathbb{N}$ *depending only on* $[K:\mathbb{Q}]$ *such that for any elliptic curve* E *over* K*, the torsion subgroup of* $E(K)$ *has order at most* c_2. ■

The hypothesis in Part (I) is known as the *(Shub-Smale)* τ*-Conjecture*, and was also stated as the fourth problem on Smale's list of the most important problems for the 21st century [Sma98, Sma00]. Mike Shub informed the authors in late 2011 that, should the τ-Conjecture hold, its O-constant should be at least 2. The complexity classes $\mathbf{P}_{\mathbb{C}}$ and $\mathbf{NP}_{\mathbb{C}}$ are respective analogues (for the BSS model over $\mathbb{C}$ [BCSS98]) of the well-known complexity classes **P** and **NP**. (Just as in the famous **P** vs. **NP** Problem, the equality of $\mathbf{P}_{\mathbb{C}}$ and $\mathbf{NP}_{\mathbb{C}}$ remains an open question.) The assertion on the hardness of the permanent in Theorem 2.4 is also an open problem and its proof would be a major step toward solving the **VP** *vs.* **VNP** *Problem* — Valiant's algebraic circuit analogue of the **P** vs. **NP** Problem [Val79, Bür00, Koi11, BLMW11].

The hypothesis of Part (II) merely posits a sequence of polynomials violating the τ-Conjecture in a weakly exponential manner. The conclusion in Part (II) would violate a widely-believed version of the cryptographic hardness of integer factorization.

[6] Lipton's main result from [Lip94] is in fact stronger, allowing for rational roots and primes with a mildly differing number of digits.

Some evidence toward the hypothesis of Part (III) is provided by [Roj02, Thm. 1], which gives the upper bound $\#Z_K(f) \leq 2^{O(\sigma(f)\log\sigma(f))}$. The quantity $\sigma(f)$ is the *additive* complexity of f [Gri82, Roj02] and is bounded from above by $s(f)$. The conclusion in Part (III) is the famous *Uniform Boundedness Theorem*, due to Merel [Mer96]. Cheng's conditional proof (see [Che04, Sec. 5]) is dramatically simpler and would yield effective bounds significantly improving known results (e.g., those of Parent [Par99]). In particular, the $K=\mathbb{Q}$ case of the hypothesis of Part (III) would yield a new proof (less than a page long) of Mazur's landmark result on torsion points [Maz78].

A natural approach to the τ-Conjecture would be to broaden it to inspire a new set of techniques, or rule out overly optimistic extensions. For instance, one might suspect that the number of roots of f in a field L containing $\mathbb{Z}$ could also be polynomial in $\tau(f)$, thus allowing us to consider techniques applicable to L. For L a number field, the truth of such an extension of the τ-Conjecture expands its implications into arithmetic geometry, as we already saw in Part (III) of Theorem 2.4. However, the truth of any global field analogue of the τ-Conjecture remains unknown.

Over local fields, we now know that the most naive extensions break down quickly: There are well-known examples $(f_n)_{n\in\mathbb{N}}$, from the dynamical systems and algorithms literature, with $\tau(f_n)=O(n)$ and f_n having 2^n real roots (see, e.g., [BC76, PS07]). Constructing such "small but mighty" polynomials over $\mathbb{Q}_p$ is also possible, even over several such fields at once.

Example 2.5. *Let S be any non-empty finite set of primes, $c_S:=\prod_{p\in S}p$, $k:=\max S$, and consider the recurrence satisfying $h_1:=x_1(1-x_1)$ and $h_{n+1}:=\left(c_S^{3^{n-1}}-h_n\right)h_n$ for all $n\geq 1$. Then $\frac{h_n(x_1)}{x_1(1-x_1)}\in\mathbb{Z}[x_1]$ has degree 2^n-2, exactly 2^n-2 roots in $\mathbb{Z}_p$ for each $p\in S$, and $\tau\left(\frac{h_n(x_1)}{x_1(1-x_1)}\right)=O(n+\#S\log k)$. However, $\frac{h_n(x_1)}{x_1(1-x_1)}$ has no real roots, and thus no integer roots. (Proofs of these facts are provided in Section 4.5.)* $\diamond$

To the best of our knowledge, the τ-Conjecture still has no counter-examples. Indeed, all known families of "small but mighty" polynomials are of a very particular recursive form, and have few (if any) integer roots at all. So let us now formulate a potentially safer extension of the τ-Conjecture to local fields, and apply it to a more restricted family of expressions: *sum-product-sum (SPS) polynomials.*

Definition 2.6. *(See* [Koi11, Sec. 3]*.) Let us define* $\mathrm{SPS}(k,m,t,d,\delta)$ *to be the family of non-constant polynomials presented in the form $\sum_{i=1}^{k}\prod_{j=1}^{m}f_{i,j}$ where, for all i and j,*

(1) $f_{i,j}\in\mathbb{Z}[x_1]\setminus\{0\}$ has degree $\leq d$ and $\leq t$ monomial terms

(2) each coefficient of $f_{i,j}$ has absolute value $\leq 2^d$, and is the difference of two nonnegative integers with at most δ nonzero digits in their binary expansions. $\diamond$

For instance, it is easily checked that the univariate polynomial

$$(7y_1^{97139}-9y^7)\,(24y_1^{45}+1000y_1^{131})+y_1^{99}$$

lies in $\mathrm{SPS}(2,2,2,97139,2)$. The family $\mathrm{SPS}(k,m,t,d,\delta)$ is motivated by recent advances in circuit complexity [AV08, Koi11]. SPS polynomials have also (implicitly) appeared earlier in fewnomial theory: [LRW03, Lemma 2], [BBS05, Prop. 4.2, pg. 375], and [Ave09, Thm. 1], in rather different notation, respectively derived upper bounds on the number of real roots of certain sub-families of $\mathrm{SPS}(k,m,2,1,\delta)$, $\mathrm{SPS}(2,m,d+1,d,\delta)$, and $\mathrm{SPS}(k,2,2,1,\delta)$, independent of δ. Noting that $\tau(f)=(kmt+\delta+\log d)^{O(1)}$ for any $f\in\mathrm{SPS}(k,m,t,d,\delta)$, we see that the following recent result of Koiran significantly strengthens part of Assertion (I) of Theorem 2.4.

Theorem 2.7. [Koi11, Secs. 5–6] *Suppose that for all $k,m,t,d,\delta\in\mathbb{N}$ and $f\in\mathrm{SPS}(k,m,t,d,\delta)$, we have $\#Z_{\mathbb{Z}}(f)=(kmt+\delta+\log d)^{O(1)}$. Then the permanent of $n\times n$ matrices cannot be computed by constant-free, division-free arithmetic circuits of size $n^{O(1)}$.* ■

In [Koi11], Koiran suggests further that the number of real roots may also satisfy a bound like the one above. We propose a more flexible conjecture.

Adelic SPS-Conjecture. *For any $k,m,t,d,\delta\in\mathbb{N}$ and $f\in\mathrm{SPS}(k,m,t,d,\delta)$, there is a field $L\in\{\mathbb{R},\mathbb{Q}_2,\mathbb{Q}_3,\mathbb{Q}_5,\ldots\}$ such that f has no more than $(kmt+\delta+\log d)^{O(1)}$ distinct roots in L.*

The Adelic τ-Conjecture clearly implies the hypothesis of Theorem 2.7. (Some evidence toward the Adelic τ-Conjecture appears in [GKPR12].) So we pose our conjecture mainly to advocate adding p-adic techniques to the real-analytic toolbox put forth in [Koi11, Sec. 6] and [KPT12].

3. Background: From Triangles to Toric Deformations and Tropical Varieties

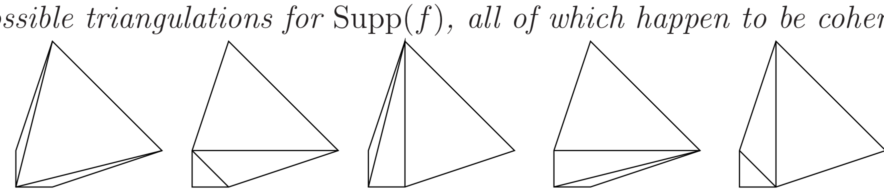
Our first step toward building systems with maximally many roots is a polyhedral construction (Lemma 3.7 below) with several useful algebraic consequences. We refer the reader to the excellent book [LRS10] for further background on triangulations and liftings.

Let $\mathrm{Conv}\mathcal{A}$ denote the convex hull of any set $\mathcal{A}\subseteq\mathbb{R}^n$. Assuming $\mathcal{A}$ is finite, we say that a triangulation of $\mathcal{A}$ is *coherent* (or *regular*) iff its simplices are exactly the domains of linearity for some function $\ell:\mathrm{Conv}\mathcal{A}\longrightarrow\mathbb{R}$ that is convex, continuous, and piecewise linear. (For $n\geq 2$ and $\#\mathcal{A}\geq 6$ one can easily find non-coherent triangulations [LRS10].) We call ℓ a *lifting* of $\mathcal{A}$ (or a lifting of $\mathrm{Conv}\mathcal{A}$), and we let $\hat{\mathcal{A}}:=\{(a,\ell(a))\mid a\in\mathcal{A}\}$. Abusing notation slightly, we also refer to $\hat{\mathcal{A}}$ as a *lifting of $\mathcal{A}$ (with respect to ℓ)*.

Remark 3.1. *It follows directly from our last definition that a lifting function ℓ on $\mathrm{Conv}\mathcal{A}$ is uniquely determined by the values of ℓ on $\mathcal{A}$. So we will henceforth specify such ℓ by specifying just the restricted image $\ell(\mathcal{A})$.* ⋄

Recall also that $\mathrm{Supp}(f)$ denotes the set of exponent vectors (a.k.a. the *support* or *spectrum*) of f.

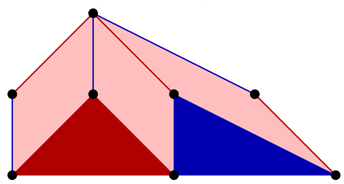
Example 3.2. *Consider $f(x):=1-x_1-x_2+\frac{6}{5}(x_1^4x_2+x_1x_2^4)$. Then $\mathrm{Supp}(f)=\{(0,0),(1,0),(0,1),(1,4),(4,1)\}$ and has convex hull a pentagon. It is then easily checked that there are exactly 5 possible triangulations for $\mathrm{Supp}(f)$, all of which happen to be coherent:*



⋄

Definition 3.3. *(See also [HS95].) For any polytope $\hat{Q}\subset\mathbb{R}^{n+1}$, we call a face $\hat{P}$ of $\hat{Q}$ a* lower face *iff $\hat{P}$ has an inner normal with positive $(n+1)^{\underline{st}}$ coordinate. Letting $\pi:\mathbb{R}^{n+1}\longrightarrow\mathbb{R}^n$ denote the natural projection forgetting the last coordinate, the lower facets of $\hat{Q}$ thus induce a natural polyhedral subdivision Σ of $Q:=\pi\left(\hat{Q}\right)$. In particular, if $\hat{Q}\subset\mathbb{R}^{n+1}$ is a Minkowski* *sum of the form* $\hat{Q}_1 + \cdots + \hat{Q}_n$ *where the* $\hat{Q}_i$ *are polytopes of dimension* $\leq n+1$*,* $\hat{E}_i$ *is a lower edge of* $\hat{Q}_i$ *for all* i*, and* $\hat{P} = \hat{E}_1 + \cdots + \hat{E}_n$ *is a lower facet of* $\hat{Q}$*, then we call* $\hat{P}$ *a* mixed *lower facet of* $\hat{Q}$*. Also, the resulting cell* $\pi\left(\hat{P}\right) = \pi\left(\hat{E}_1\right) + \cdots + \pi\left(\hat{E}_n\right)$ *of* Σ *is called a* mixed cell *of* Σ*.* $\diamond$

Example 3.4. *Let us consider the family of systems* G_ε *from Theorem 1.6 for* $n=2$*. In particular, let* $(\mathcal{A}_1, \mathcal{A}_2)$ *be the pair of supports of* G_ε*, and let* (Q_1, Q_2) *be the corresponding pair of convex hulls in* $\mathbb{R}^2$*. Let us also define a pair of liftings* (ℓ_1, ℓ_2) *via the exponents of the powers of* ε *appearing in the corresponding monomial terms. More precisely,* ℓ_1 *sends* $(0,0)$*,* $(2,0)$*, and* $(1,1)$ *respectively to* 1*,* 0*, and* 1*; and* ℓ_2 *sends* $(1,1)$*,* $(2,0)$*, and* $(0,1)$ *respectively to* 0*,* 1*, and* 0*. These lifting functions then affect the shape of the lower hull of the Minkowski sum* $\hat{Q}_1 + \hat{Q}_2$ *of lifted polygons, which in turn fixes a subdivision* Σ_{ℓ_1,ℓ_2} *of* $Q_1 + Q_2$ *via the images of the lower facets of* $\hat{Q}_1 + \hat{Q}_2$ *under* π*. (See the illustration below.) The mixed cells of* Σ_{ℓ_1,ℓ_2}*, for this particular lifting, correspond to the lighter (pink) parallelograms: from left to right, they are exactly* $E_{1,0} + E_{2,0}$*,* $E_{1,1} + E_{2,0}$*, and* $E_{1,1} + E_{2,1}$*, where* $E_{1,s}$ *(resp.* $E_{2,s}$*) is an edge of* Q_1 *(resp.* Q_2*) for all* s*.*



More precisely, $E_{1,0}$*,* $E_{1,1}$*,* $E_{2,0}$*, and* $E_{2,1}$ *are respectively the convex hulls of* $\{(0,0),(1,1)\}$*,* $\{(1,1),(2,0)\}$*,* $\{(0,0),(0,1)\}$*, and* $\{(0,1),(2,0)\}$*. Note also that these mixed cells, through their expression as edges sums (and the obvious correspondence between vertices and monomial terms), correspond naturally to three binomial systems. In order, they are* $(x_1x_2 - \varepsilon, x_2 - 1)$ *,* $(x_1x_2 - x_1^2, x_2 - 1)$*, and* $(x_1x_2 - x_1^2, x_2 - \varepsilon x_1^2)$*. In particular, the first (resp. second) polynomial of each such pair is a sub-sum of the first (resp. second) polynomial of* G_ε*.* $\diamond$

Definition 3.5. *(See also* [HS95, Ewa96, Roj03a]*.) Let* $\mathcal{A}_1, \ldots, \mathcal{A}_n \subset \mathbb{R}^n$ *be finite point sets with respective convex hulls* $Q_1, \ldots, Q_n$*. Also let* $\ell_1, \ldots, \ell_n$ *be respective lifting functions for* $\mathcal{A}_1, \ldots, \mathcal{A}_n$ *and consider the polyhedral subdivision* $\Sigma_{\ell_1,\ldots,\ell_n}$ *of* $Q := Q_1 + \cdots + Q_n$ *obtained via the images of the lower facets of* $\hat{Q}$ *under* π*. In particular, if* $\dim \hat{P}_1 + \cdots + \dim \hat{P}_n = n$ *for every lower facet of* $\hat{Q}$ *of the form* $\hat{P}_1 + \cdots + \hat{P}_n$*, then we say that* $(\ell_1, \ldots, \ell_n)$ *is* mixed*. For any mixed* n*-tuple of liftings we then define the* mixed volume *of* $(Q_1, \ldots, Q_n)$ *to be* $\mathcal{M}(Q_1, \ldots, Q_n) := \sum\limits_{\substack{C \text{ a mixed cell} \\ \text{of } \Sigma_{\ell_1,\ldots,\ell_n}}} \mathrm{Vol}(C)$*, following the notation of Definition 3.3.* $\diamond$

As an example, the mixed volume of the two triangles from Example 3.4, relative to the stated (mixed) lifting, is the sum of the areas of the three parallelograms in the illustration, i.e., 3.

Theorem 3.6. *(See* [Ewa96, Ch. IV, pg. 126] *and* [HS95]*.) The formula for* $\mathcal{M}(Q_1, \ldots, Q_n)$ *from Definition 3.5 is independent of the underlying mixed* n*-tuple of liftings* $(\ell_1, \ldots, \ell_n)$*. Furthermore, if* $Q'_1, \ldots, Q'_n \subseteq \mathbb{R}^n$ *are any polytopes with* $Q'_i \supseteq Q_i$ *for all* i*, then* $\mathcal{M}(Q_1, \ldots, Q_n) \leq \mathcal{M}(Q'_1, \ldots, Q'_n)$*. Finally, the* n*-dimensional mixed volume satisfies* $\mathcal{M}(Q, \ldots, Q) = n!\mathrm{Vol}(Q)$ *for any polytope* $Q \subset \mathbb{R}^n$*.* $\blacksquare$

Lemma 3.7. *Let* $n \geq 2$*, and let* $\mathbf{O}$ *and* e_i *respectively denote the origin and* $i^{\underline{th}}$ *standard basis vector in* $\mathbb{R}^{n+1}$*. Consider the triangles* $\hat{T}_1 := \mathrm{Conv}\{e_{n+1}, 2e_1, e_1 + e_2\}$*,* $\hat{T}_n := \mathrm{Conv}\{\mathbf{O}, 2e_1 + (2n-3)e_{n+1}, e_n\}$*, and* $\hat{T}_i := \mathrm{Conv}\{\mathbf{O}, 2e_1 + (2i-3)e_{n+1}, e_i + e_{i+1}\}$ *for all* $i \in \{2, \ldots, n-1\}$*. Then the Minkowski sum* $\hat{T} := \hat{T}_1 + \cdots + \hat{T}_n$ *has exactly* $n+1$ *mixed* *lower facets. More precisely, for any* $j \in \{0,\ldots,n\}$, *we can obtain a unique mixed lower facet,* $\hat{P}_j := \hat{E}_{1,1} + \cdots + \hat{E}_{j,1} + \hat{E}_{j+1,0} + \cdots + \hat{E}_{n,0}$, *with* $\mathrm{Vol}\left(\pi\left(\hat{P}_j\right)\right) = 1$, *in the following manner: for all* $i \in \{1,\ldots,n\}$, *define* $\hat{E}_{i,1}$ *(resp.* $\hat{E}_{i,0}$*) to be the convex hull of the second (resp. first) and third listed vertices for* $\hat{T}_i$. *Finally,* $\mathcal{M}\left(\pi\left(\hat{T}_1\right),\ldots,\pi\left(\hat{T}_n\right)\right) = n+1$ *and, for each* $j \in \{0,\ldots,n\}$, *the vector* $v_j := e_{n+1} + e_1 - \sum_{i=1}^{j}(j+1-i)e_i$ *is a nonzero inner normal for the lower facet* $\hat{P}_j$.

Lemma 3.7 is our key polyhedral result and is proved in Section 4.4 and illustrated in Example 3.13 below.

The next result we need is a beautiful generalization, by Bernd Sturmfels, of *Viro's Theorem*. We use ∂Q for the boundary of a polytope Q.

Definition 3.8. *Suppose* $\mathcal{A} \subset \mathbb{Z}^n$ *is finite and* $\mathrm{Vol}(\mathrm{Conv}\mathcal{A}) > 0$. *We call any function* $s : \mathcal{A} \longrightarrow \{\pm\}$ *a* distribution of signs for $\mathcal{A}$, *and we call any pair* (Σ, s) *with* Σ *a coherent triangulation of* $\mathcal{A}$ *a* signed *(coherent) triangulation of* $\mathcal{A}$. *We also call any edge of* Σ *with vertices of opposite sign an* alternating edge.

Given a signed triangulation for $\mathcal{A}$ *we then define a piece-wise linear manifold — the* Viro diagram $\mathcal{V}_{\mathcal{A}}(\Sigma, s)$ *— in the following local manner: For any n-cell* $C \in \Sigma$, *let* L_C *be the convex hull of the set of midpoints of the alternating edges of* C, *and then define* $\mathcal{V}_{\mathcal{A}}(\Sigma, s) := \bigcup\limits_{\substack{C \text{ an } n\text{-cell} \\ \text{of } \Sigma}} L_C \setminus \partial\mathrm{Conv}(\mathcal{A})$. *Finally, when* $\mathcal{A} = \mathrm{Supp}(f)$ *and* s *is the corresponding sequence of coefficient signs, then we call* $\mathcal{V}_{\Sigma}(f) := \mathcal{V}_{\mathcal{A}}(\Sigma, s)$ *the* Viro diagram of f. $\diamond$

Viro's Theorem (see, e.g., Proposition 5.2 and Theorem 5.6 of [GKZ94, Ch. 5, pp. 378–393] or [Vir84]) states that, under certain conditions, one may find a triangulation Σ with the positive zero set of f homeomorphic to $\mathcal{V}_{\Sigma}(f)$. *Sturmfels' Theorem for Complete Intersections* [Stu94, Thm. 4] extends this to polynomial systems, and we will need just the $n \times n$ case.

Definition 3.9. *Suppose* $\mathcal{A}_1,\ldots,\mathcal{A}_n \subset \mathbb{Z}^n$ *and each* $\mathcal{A}_i$ *is endowed with a lifting* ℓ_i *and a distribution of signs* s_i. *Then, following the notation of Definition 3.5, we call a mixed cell* $E_1 + \cdots + E_n$ *of* $\Sigma_{\ell_1,\ldots,\ell_n}$ *an* alternating mixed cell of $(\Sigma_{\ell_1,\ldots,\ell_n}, s_1,\ldots,s_n)$ *iff each edge* E_i *is alternating (as an edge of the triangulation of* $\mathcal{A}_i$ *induced by* ℓ_i*).* $\diamond$

Example 3.10. *Returning to Example 3.4, it is clear that, when* $\varepsilon \in \mathbb{R}^*$, *we can endow the supports of* G_ε *with the distribution of signs corresponding to the underlying coefficients. In particular, when* $\varepsilon > 0$, *each of the* 3 *mixed cells is alternating.* $\diamond$

Sturmfels' Theorem for Complete Intersections (special case). *Suppose* $\mathcal{A}_1,\ldots,\mathcal{A}_n$ *are finite subsets of* $\mathbb{Z}^n$, $(c_{i,a} \mid i \in \{1,\ldots,n\}\ ,\ a \in \mathcal{A}_i)$ *is a vector of nonzero real numbers, and* $(\ell_1,\ldots,\ell_n)$ *is a mixed n-tuple of lifting functions for* $\mathcal{A}_1,\ldots,\mathcal{A}_n$. *Let* $\Sigma_{\ell_1,\ldots,\ell_n}$ *denote the resulting polyhedral subdivision of* $\mathrm{Conv}(\mathcal{A}_1) + \cdots + \mathrm{Conv}(\mathcal{A}_n)$ *(as in Definition 3.5) and let* $s_i := (\mathrm{sign}(c_{i,a}) \mid a \in \mathcal{A}_i)$ *for all* i. *Then, for all* $t > 0$ *sufficiently small, the system of polynomials* $\left(\sum\limits_{a\in\mathcal{A}_1} c_{1,a}t^{\ell_1(a)}x^a, \ldots, \sum\limits_{a\in\mathcal{A}_n} c_{n,a}t^{\ell_n(a)}x^a\right)$ *has exactly* N *roots in* $\mathbb{R}^n_+$, *where* N *is the number of alternating cells of* $(\Sigma_{\ell_1,\ldots,\ell_n}, s_1,\ldots,s_n)$. $\blacksquare$

A final tool we will need is the *non-Archimedean Newton polytope*, along with a recent refinement incorporating generalized phase. In particular, the definition and theorem below are special cases of a non-Archimedean analogue (see [AI11]) of Sturmfel's result above.

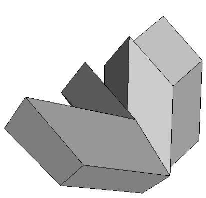
Definition 3.11. *Given any complete non-Archimedean field K with uniformizing parameter ρ, and any Laurent polynomial $f(x) := \sum_{i=1}^{m} c_i x^{a_i} \in K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, we define its* Newton polytope over K *to be* $\mathrm{Newt}_K(f) := \mathrm{Conv}\{(a_i, \mathrm{ord}\ c_i) \mid i \in \{1, \ldots, m\}\}$. *Also, the polynomial associated to summing the terms of f corresponding to points of the form $(a_i, \mathrm{ord}\ c_i)$ lying on a lower face of $\mathrm{Newt}_K(f)$, and replacing each coefficient c by its first digit $\phi(c)$, is called a* lower polynomial. $\diamond$

A remarkable fact true over non-Archimedean algebraically closed fields, but false over $\mathbb{C}$, is that the norms of roots of polynomials can be determined completely combinatorially: see Section 3.1 below and [EKL06]. What is less well-known is that, under certain conditions, the generalized phases can also be found by simply solving some lower binomial systems. Henceforth, we abuse notation slightly by setting $\mathrm{ord}(y_1, \ldots, y_n) := (\mathrm{ord}\ y_1, \ldots, \mathrm{ord}\ y_n)$.

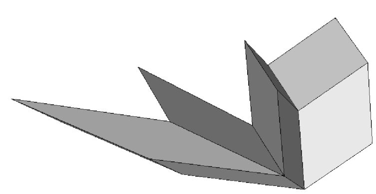
Theorem 3.12. *(Special case of* [AI11, Thm. 3.10 & Prop. 4.4]*.) Suppose K is a complete non-Archimedean field with residue field k and uniformizer ρ. Also let $f_1, \ldots, f_n \in K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, $\hat{Q} := \sum_{i=1}^{n} \mathrm{Newt}_K(f_i)$, and let $(v, 1)$ be an inner normal to a mixed lower facet of $\hat{Q}$ of the form $\hat{E} := \hat{E}_1 + \cdots + \hat{E}_n$ where $\hat{E}_i$ is a lower edge of $\mathrm{Newt}_K(f_i)$ for all i. Suppose also that the lower polynomials $g_1, \ldots, g_n$ corresponding to the normal $(v, 1)$ are all binomials, and that $\pi\left(\hat{E}\right)$ has standard Euclidean volume 1. Then $F := (f_1, \ldots, f_n)$ has 1 or 0 roots $\zeta \in (K^*)^n$ with $\mathrm{ord}\ \zeta = v$ and generalized phase $\theta \in (k^*)^n$ according as $g_1(\theta) = \cdots = g_n(\theta) = 0$ or not. In particular, F has at most one root with valuation vector v.* ■

Note that while the number of roots with given n-tuple of first digits may depend on the uniformizer ρ (see Proposition 5.1 in Section 5), the total number of roots with $\mathrm{ord}\ \zeta = v$ is independent of ρ.

Example 3.13. *Let p be any prime, $n = 3$, and let $(\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ be the triple of supports for the system G_p (see Theorem 1.6). Also let ℓ_1, ℓ_2, ℓ_3 be the respective liftings obtained by using the p-adic valuations of the coefficients of G_p. Lemma 3.7 then tells us that we obtain exactly 4 mixed cells (two views of which are shown below), with corresponding lower facet normals $(1,0,0,1), (0,0,0,1), (-1,-1,0,1), (-2,-2,-1,1)$. In particular, the corresponding lower binomial systems are the following:*



$x_1x_2 - 1$	$x_1x_2 - x_1^2$	$x_1x_2 - x_1^2$	$x_1x_2 - x_1^2$
$x_2x_3 - 1$	$x_2x_3 - 1$	$x_2x_3 - x_1^2$	$x_2x_3 - x_1^2$
$x_3 - 1$	$x_3 - 1$	$x_3 - 1$	$x_3 - x_1^2$



Each mixed cell has volume 1, and each corresponding binomial system has unique solution $(1,1,1) \in (\mathbb{F}_p^*)^3$. Theorem 3.12 then tells us that the roots of G_p in $(\mathbb{Q}_p^*)^3$ are of the following form: $(p(1+O(p)), 1+O(p), 1+O(p))$, $(1+O(p), 1+O(p), 1+O(p))$, $(p^{-1}(1+O(p)), p^{-1}(1+O(p)), 1+O(p))$, and $(p^{-2}(1+O(p)), p^{-2}(1+O(p)), p^{-1}(1+O(p)))$. $\diamond$

3.1. **Some Tropical Visualizations.** A beautiful theorem of Kapranov tells us that, for non-Archimedean K, we can use polyhedral combinatorics to efficiently compute the valuations of the roots of any polynomial.

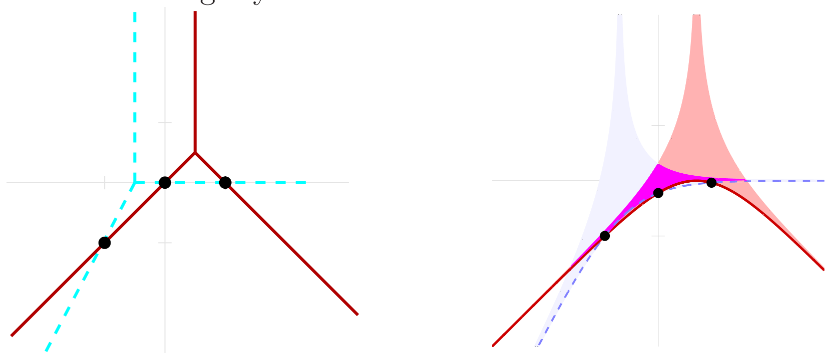
Definition 3.14. *For any complete algebraically closed field K and $f \in K\left[x_1^{\pm 1}, \ldots, x_n^{\pm 1}\right]$ we set $Z_K^*(f) := \{x \in (K^*)^n \mid f(x) = 0\}$. Also, for any subset $S \subseteq \mathbb{R}^n$, we let $\bar{S}$ denote the closure* *of S in the Euclidean topology. Finally, if K is also non-Archimedean, then we define the* tropical variety of f over K, $\mathrm{Trop}_K(f)$, *to be the closure in $\mathbb{R}^n$ of*

$$\{(v_1,\ldots,v_n)\in\mathbb{R}^n \mid (v_1,\ldots,v_n,1) \text{ is an inner edge normal of } \mathrm{Newt}_K(f)\} \qquad \diamond$$

Remark 3.15. $\mathrm{Trop}_K(f)$ *is sometimes equivalently defined in terms of max-plus semi-rings (see, e.g.,* [MS12]*).* $\diamond$

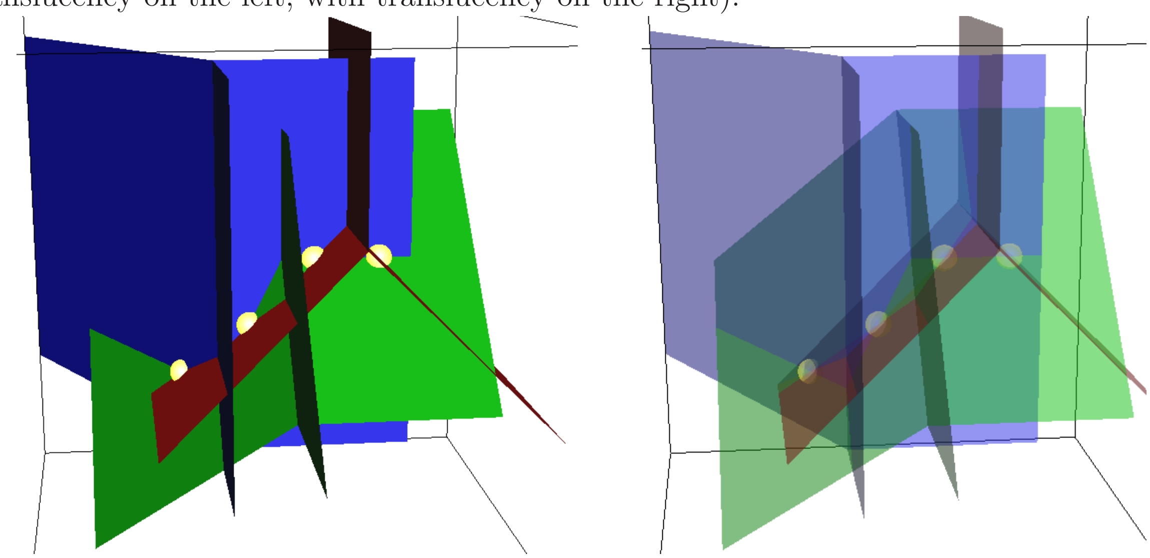
Kapranov's Non-Archimedean Amoeba Theorem. [EKL06] *For any complete, non-Archimedean algebraically closed field K, we have $\overline{\mathrm{ord}(Z^*_K(f))}=\mathrm{Trop}_K(f)$.* ■

We now illustrate these ideas through our earlier examples. Returning to Example 3.4, the underlying tropical varieties (or closures of $\mathrm{ord}(Z^*_L(g_1))$ and $\mathrm{ord}(Z^*_L(g_2))$ for $L\in\left\{\overline{\mathbb{Q}}_p,\overline{\mathbb{F}_q((t))}\right\}$) intersect in exactly 3 points as illustrated below, on the left. (The tropical varieties for the first and second polynomials are respectively colored in solid red and dashed blue.) The right-hand illustration below shows the corresponding plots when $L=\mathbb{C}$ and $\varepsilon=1/4$, with their intersection darkened slightly.



Note that the images of the corresponding positive zero sets under the (complex) ord map are drawn as even darker curves (with 3 marked intersections) in the right-hand illustration above. The negative of the image of a complex algebraic set under the complex ord map is usually called an *amoeba* [PT05].

Returning to Example 3.13, the resulting tropical varieties are illustrated below (without translucency on the left, with translucency on the right):



Note that each tropical variety above is a polyhedral complex of codimension 1, and that all the top-dimensional faces are unbounded, even though they are truncated in the illustrations.

4. Proving our Main Results

4.1. **Theorem 1.5: The Universal Lower Bound.**

First note that since $Y_L(n,k)$ is integer-valued when finite, $Y_L(n,k)$ is actually attained by some $(n+k)$-nomial $n\times n$ system over L when $Y_L(n,k)$ is finite.

Now, any $n\times n$ polynomial system of the form $(b(x_1),\ldots,b(x_{n-1}),r(x_n))$ — with $b\in L[x_1]$ a binomial and $r\in L[x_1]$ a trinomial, both possessing nonzero constant terms — is clearly an $(n+2)$-nomial $n\times n$ system. So we immediately obtain $Y_L(n,2)\geq Y_L(1,2)Y_L(1,1)^{n-1}$ simply by picking b and r (via Theorem 1.2 and Remark 1.3) to have maximally many roots over L with all coordinates of generalized phase 1. That $Y_L(n,2)\geq n+1$ follows immediately from Theorem 1.6, so we obtain the first asserted inequality.

The remaining lower bounds for $Y_L(n,k)$ follow from similar concatenation tricks. First, note that any $n\times n$ polynomial system of the form $(b(x_1),\ldots,b(x_{n-k+1}),r(x_{n-k+2}),\ldots,r(x_n))$ is clearly an $(n+k)$-nomial $n\times n$ system. So, specializing b and r appropriately once again, the inequality $Y_L(n,k)\geq Y_L(1,1)^{n-k+1}Y_L(1,2)^{k-1}$ holds for $n\geq k-1$.

A slightly more intricate construction gives our next lower bound: letting $F_n(x_1,\ldots,x_n)$ denote an $(n+2)$-nomial $n\times n$ system over L possessing a nonzero constant term, observe that when $k-1\leq n$ and $\ell:=\lfloor\frac{n}{k-1}\rfloor$, the block-diagonal system F defined by

$$F_\ell(x_{1,1},\ldots,x_{1,\ell}),\ldots,F_\ell(x_{k-1-[n]_{k-1},1},\ldots,x_{k-1-[n]_{k-1},\ell}),$$
$$F_{\ell+1}(y_{1,1},\ldots,y_{1,\ell+1}),\ldots,F_{\ell+1}(y_{[n]_{k-1},1},\ldots,y_{[n]_{k-1},\ell+1})$$

involves exactly $(k-1-[n]_{k-1})\ell+[n]_{k-1}(\ell+1)=(k-1)\ell+[n]_{k-1}=n$ variables, and n polynomials via the same calculation. Also, the total number of distinct exponent vectors of F is exactly

$(k-1-[n]_{k-1})(\ell+2)+[n]_{k-1}(\ell+3)-(k-1)+1=(k-1)\ell+[n]_{k-1}+2(k-1)-k+2=n+k,$

since all the polynomials share a nonzero constant term. Furthermore, any ordered n-tuple consisting of $k-1-[n]_{k-1}$ non-degenerate roots of F_ℓ in L^ℓ followed by $[n]_{k-1}$ non-degenerate roots of $F_{\ell+1}$ in $L^{\ell+1}$ (with all coordinates having generalized phase 1) is clearly a non-degenerate root of F in L^n with all coordinates having generalized phase 1. Picking F_ℓ and $F_{\ell+1}$ to be appropriate specializations of the systems from Theorem 1.6, we thus obtain $Y_L(n,k)\geq Y_L\left(\lfloor\frac{n}{k-1}\rfloor,2\right)^{k-1-[n]_{k-1}}Y_L\left(\lfloor\frac{n}{k-1}\rfloor+1,2\right)^{[n]_{k-1}}$. So the case $n\geq k-1$ is done.

Now simply note that any $n\times n$ system of the form

$$(m(x_1),\ldots,m(x_{n-[k-1]_n}),\mu(y_1),\ldots,\mu(y_{[k-1]_n}))$$

— with $m\in L[x_1]$ an ℓ-nomial, $\mu\in L[y_1]$ an $(\ell+1)$-nomial, $\ell:=\lfloor\frac{n+k-1}{n}\rfloor$, and $n\leq k-1$ — is easily verified to be an $(n+k)$-nomial $n\times n$ system. So picking m and μ to have maximally many roots with generalized phase 1, we immediately obtain $Y_L(n,k)\geq Y_L\left(1,\lfloor\frac{n+k-1}{n}\rfloor\right)^{n-[k-1]_n}Y_L\left(1,\lfloor\frac{n+k-1}{n}\rfloor+1\right)^{[k-1]_n}$ for $n\leq k-1$.

To conclude, the entries in our table are simply specializations of our recursive lower bounds using the explicit values given by Theorem 1.2. ■

4.2. **Theorem 1.6: Fewnomials Systems with Many Roots Universally.**

First note that all the roots of G_ε in $\bar{L}^n$ lie in $\left(\bar{L}^*\right)^n$. (Clearly, setting any $x_i=0$ results in a pair of univariate polynomials having no roots in common, or a nonzero constant being equal to zero.) Let $(g_1,\ldots,g_n):=G_\varepsilon$ and let $\mathcal{A}$ denote the matrix whose columns are the vectors in the union of the supports of the g_i. More precisely, $\mathcal{A}$ is the $n\times(n+2)$ matrix below:

$$\begin{bmatrix} 0 & 2 & 1 & 0 & & & \\ & & 1 & 1 & & & \\ & & & 1 & & & \\ & & & & \ddots & & \\ & & & & & 1 & \\ & & & & & 1 & 1 \end{bmatrix}$$

Now let $\bar{\mathcal{A}}$ denote the $(n+1)\times(n+2)$ matrix obtained by appending a row of 1s to the top of $\mathcal{A}$. It is then easily checked that $\bar{\mathcal{A}}$ has right null-space of dimension 1, generated by the transpose of $b:=(b_1,\ldots,b_{n+2})\ =(-1,(-1)^n,(-1)^{n+1}2,\ldots,(-1)^{n+n}2)$. Let us rewrite the equation $g_i=0$ as $x^{a_{i+2}}=\beta_i(x_1^2)$, where a_i denotes the $i^{\underline{\text{th}}}$ column of $\mathcal{A}$ and β_i is a suitable degree one polynomial with coefficients that are powers of ε. Since the entries of b sum to 0, we then easily obtain that

$$1^{b_1}u^{b_2}\beta_1(u)^{b_3}\cdots\beta_n(u)^{b_{n+2}}=1$$

when $\zeta=(\zeta_1,\ldots,\zeta_n)$ is a root of G_ε in $\left(\bar{L}^*\right)^n$ and $u:=\zeta_1^2$. In other words, the degree $n+1$ polynomial $R_n(u)$ from Lemma 1.8 must vanish. Furthermore, the value of ζ_n is uniquely determined by the value of u, thanks to the equation $g_n=0$. Proceeding with the remaining equations $g_{n-1}=0,\ldots,g_1=0$ we see that the same holds for $\zeta_{n-1},\ldots,\zeta_2$ and ζ_1 successively. So G_ε has no more than $n+1$ roots, counting multiplicities, in $\left(\bar{L}^*\right)^n$. Note in particular that by Lemma 3.7, combined with *Bernstein's Theorem* (over a general algebraically closed field [Ber75, Dan78]), G_ε having at least $n+1$ distinct roots in $\left(\bar{L}^*\right)^n$ implies that there are *exactly* $n+1$ roots in $\left(\bar{L}^*\right)^n$ and they are all non-degenerate.

To finally prove the first part of our theorem, we separate the Archimedean and non-Archimedean cases: when $L=\mathbb{R}$ we immediately obtain, from Lemma 3.7 and Sturmfels' Theorem, that G_ε has at least $n+1$ positive roots for $\varepsilon>0$ sufficiently small. (This trivially implies the $L=\mathbb{C}$ case as well.)

For the non-Archimedean case, Lemma 3.7 and Theorem 3.12 immediately imply that, when $\phi(\varepsilon)=1$ and $\operatorname{ord}\varepsilon\geq 1$, G_ε has at least $n+1$ roots in L^n with all coordinates having generalized phase 1. In particular, for each vector v_j from Lemma 3.7, it is easily checked that $(1,\ldots,1)$ is a root of the corresponding lower binomial system of G_ε over the residue field of L.

The only assertion left to prove is that $G_{1/4}$ has exactly $n+1$ roots in the positive orthant, and this follows from Lemma 1.8. ■

4.3. **Proof of Lemma 1.8.** Let us first define A_n and B_n respectively as $u(1+\varepsilon u)^2(1+\varepsilon^5u)^2\cdots(1+\varepsilon^{4\lfloor n/2\rfloor-3}u)^2$ and $(\varepsilon+u)^2(1+\varepsilon^3u)^2(1+\varepsilon^7u)^2\cdots(1+\varepsilon^{4\lceil n/2\rceil-5}u)^2$. Clearly, $R_n=A_n-B_n$.

Lemma 4.1. *Assume $\varepsilon=1/4$. Then, for all $n\geq 2$, we have $R_n\left(16^{n-2}/u\right)=\left(\frac{-4^{n-2}}{u}\right)^{n+1}R_n(u)$. Also, for all even $n\geq 2$, we have $R_n(4^{n-2})=0$.*

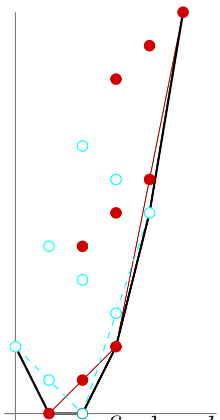
Lemma 4.2. *Assume $\varepsilon=1/4$ and consider R_n as a function on $\mathbb{R}$. Then, for all $n\geq 2$, we have (a) $R_n(0)<0$ and (b) $(-1)^\ell R_n(16^\ell/4)>0$ for all $\ell\in\{0,\ldots,\lceil n/2\rceil-1\}$.*

These subsidiary lemmata are proved in Section 5 below.

Returning to the proof of Lemma 1.8, we now consider two exclusive cases.

Real Case: By Lemma 4.2, R_n has $\lceil\frac{n}{2}\rceil-1$ sign changes in the open interval $\left(0,\frac{16^{\lceil n/2\rceil-1}}{4}\right)$. So by the Intermediate Value Theorem, R_n has $\lceil\frac{n}{2}\rceil-1$ roots in this interval. By Lemma 4.1, for every such root ζ, $\frac{16^{n-2}}{\zeta}$ yields a new root. When n is odd, this gives us $2(\lceil\frac{n}{2}\rceil-1)=n+1$ positive roots. When n is even, we get n positive roots and, by Lemma 4.1, the new positive root 4^{n-2}. So R_n has $n+1$ positive roots. ■

Non-Archimedean Case:



While this case is already implicit in the proof of Theorem 1.6, one can form a direct argument starting from Newton polygons: For $L\in\{\mathbb{Q}_p,\mathbb{F}_q((t))\}$ (and thus $\varepsilon\in\{p,t\}$ respectively), we easily obtain that $P:=\mathrm{Newt}_L(A_n)$ has exactly $1+\lfloor n/2\rfloor$ lower edges, $Q:=\mathrm{Newt}_L(B_n)$ has exactly $\lceil n/2\rceil$ lower edges, and the vertices of P and Q interlace. (The supports of A_4 and B_4 are drawn, respectively as red (filled) and blue (unfilled) circles, at left.) More precisely, $\mathrm{Newt}_L(R_n)=\mathrm{Conv}(P\cup Q)$ has exactly $n+1$ lower edges, each having horizontal length 1. In particular, $\{(1,1),(0,1),\ldots,(1-n,1)\}$ is a representative set of inner normals for the lower edges, and each corresponding lower binomial is a degree one polynomial with pair of coefficients $(\pm 1,\mp 1)$. Also, for any $i\in\{1,0,\ldots,1-n\}$, we can find a $d_i\in\mathbb{Z}$ such that $\varepsilon^{d_i}R_n(\varepsilon^i u)=\pm 1\mp u+O(\varepsilon)$. So by Hensel's Lemma, R_n has exactly $n+1$ roots in $\mathbb{Q}_p$ (resp. $\mathbb{F}_p((t))$) when $\varepsilon=p$ (resp. $\varepsilon=t$), and each such root has first digit 1. ■

4.4. **Proof of Lemma 3.7.** By Theorem 3.6 our mixed volume in question is bounded above by $n!\mathrm{Vol}(Q)$ where Q is the polytope with vertices the columns of the matrix $\mathcal{A}$ from the proof of Theorem 1.6. The vertices of Q form a *circuit*, and the signs of the entries of the vector b from the proof of Theorem 3.6 thereby encode an explicit triangulation of Q (see, e.g., [GKZ94, Prop. 1.2, pg. 217]). More precisely, defining $Q(i)$ to be the convex hull of the points corresponding to all the columns of $\mathcal{A}$ *except* for the $i^{\underline{\text{th}}}$ column, we obtain that $\left\{Q(2),Q(4),\ldots,Q\left(2\left\lfloor\frac{n+2}{2}\right\rfloor\right)\right\}$ (for n even) and $\left\{Q(3),Q(5),\ldots,Q\left(2\left\lceil\frac{n+2}{2}\right\rceil-1\right)\right\}$ (for n odd) form the simplices of a triangulation of Q. Note in particular that the volume of $Q(i)$ is exactly $1/n!$ times the absolute value of the determinant of the submatrix of $\mathcal{A}$ obtained by deleting the first and $i^{\underline{\text{th}}}$ columns. Note also that this submatrix is block-diagonal with exactly 2 blocks: an $(i-2)\times(i-2)$ upper-left upper-triangular block and an $(n-i+2)\times(n-i+2)$ lower-right lower-triangular block. It is then clear that $\mathrm{Vol}(Q(i))$ is 1 or 2, according as $i=2$ or $i\geq 3$. So $\mathrm{Vol}(Q)$ is then $1+2\left(\left\lfloor\frac{n+2}{2}\right\rfloor-1\right)=n+1$ (when n is even) or $2\left(\left\lceil\frac{n+2}{2}\right\rceil-1\right)=n+1$ (when n is odd).

Since any n-tuple of columns chosen from the last $n+1$ columns of $\mathcal{A}$ is linearly independent, each cell $\pi\left(\hat{P}_j\right)$ has positive volume. (The linear independence follows directly from our preceding block diagonal characterization of certain submatrices of $\mathcal{A}$.) So once we show that each such cell is distinct, we immediately obtain that our mixed volume is at least $n+1$ and thus equal to $n+1$. Toward this end, we now check that each v_j is indeed an inner normal to $\hat{P}_j$.

For any $i\in\{1,\ldots,n\}$ let $\hat{\mathcal{A}}_i=(\alpha_i,\beta_i,\gamma_i)$ denote the triple of vertices of the triangle $\hat{T}_i$, ordered so that $\pi(\alpha_i)=\mathbf{O}$ and $\pi(\beta_i)=2e_1$. It then clearly suffices to prove that, for any $j\in\{0,\ldots,n\}$, the inner product $v_j\cdot x$ is minimized on each $\hat{\mathcal{A}}_i$ exactly at the vertices of the edge $\hat{E}_{i,s}$, where s is 1 or 0 according as $i\leq j$ or $i\geq j+1$. Equivalently, this means that the minimum values in the triple $(v_j\cdot\alpha_i,v_j\cdot\beta_i,v_j\cdot\gamma_i)$ must occur exactly at the second and third (resp. first and third) coordinates when $i\leq j$ (resp. $i\geq j+1$). This follows from a direct but tedious computation that we omit. ■

4.5. **Proofs for Example 2.5.** The assertion on the degree of $\frac{h_n(x_1)}{x_1(1-x_1)}$ is obvious from the recurrence for h_n. The upper bound on $\tau\left(\frac{h_n(x_1)}{x_1(1-x_1)}\right)$ follows easily from recursive squaring. In particular, since $\tau(c_S) \leq 2\log_2 c_S$, we easily obtain $\tau(c_S) = O(\#S \log k)$. Expressing $c_S^{3^{n-1}} = (\cdots(c_S^3)^3\cdots)^3$, it is then clear that $\tau\left(c_S^{3^{n-1}}\right) = O(n + \#S \log k)$. Observing that we can easily evaluate $\frac{h_n(x_1)}{x_1(1-x_1)}$ by simply replacing h_2 by $c_S - h_1$ in the recurrence for h_n, we arrive at our bound for $\tau\left(\frac{h_n(x_1)}{x_1(1-x_1)}\right)$. Note also that by construction, $\frac{h_n(x_1)}{x_1(1-x_1)}$ does not vanish at 0 or 1, but does vanish at every other root of h_n.

We now focus on counting the roots of $\frac{h_n(x_1)}{x_1(1-x_1)}$ in the rings $\mathbb{Z}_p$ for $p \in S$. From our last observations, it clearly suffices to show that, for all $n \geq 1$, h_n has exactly 2^n roots in $\mathbb{Z}_p$ for each $p \in S$. We do this by induction, using the following refined induction hypothesis:

> For any prime $p \in S$, h_n has exactly 2^n distinct roots in $\mathbb{Z}_p$. Furthermore, these roots are distinct mod $p^{3^{n-1}}$ and, for any such root ζ, we have $\operatorname{ord} h_n'(\zeta) = \frac{3^{n-1}-1}{2}$.

The case $n=1$ is clear. One also observes $h_1'(x_1) = 1 - 2x_1$, and $h_{n+1}' = (c_S^{3^{n-1}} - h_n)h_n'$ for all $n \geq 1$. So let us now assume the induction hypothesis for any particular n and prove the case $n+1$. In particular, let $\zeta \in \mathbb{Z}_p$ be any of the 2^n roots of h_n. The derivatives of h_n and $c_S^{3^{n-1}} - h_n$ differ only by sign mod $p^{3^{n-1}}$, so by Hensel's Lemma (combined with our induction hypothesis), $c_S^{3^{n-1}} - h_n$ also has 2^n distinct roots in $\mathbb{Z}_p$. However, the roots of $c_S^{3^{n-1}} - h_n$ in $\mathbb{Z}_p$ are all distinct from the roots of h_n in $\mathbb{Z}_p$: this is because $c_S^{3^{n-1}} - h_n$ is nonzero at every root of $h_n(x_1)$ mod $p^{3^{n-1}+1}$. So h_{n+1} then clearly has 2^{n+1} distinct roots in $\mathbb{Z}_p$, and these roots remain distinct mod p^{3^n}. Furthermore, by our recurrence for h_n', the p-adic valuation of h_{n+1}' is exactly $3^{n-1} + \frac{3^{n-1}-1}{2} = \frac{3^n-1}{2}$. So our induction is complete.

To see that $\frac{h_n(x_1)}{x_1(1-x_1)}$ has no real roots, first note that $x_1(1-x_1)$ is strictly increasing on $(-\infty, 1/2)$, strictly decreasing on $(1/2, +\infty)$, and attains a unique maximum of $1/4$ at $x_1 = 1/2$. Since $c_S \geq 2$, we also clearly obtain that $c_S - x_1(1-x_1)$ has range contained in $[3/4, +\infty)$, with minimum occuring at $x_1 = 1/2$. More generally, our recurrence for h_n' implies that any critical point $\zeta \in \mathbb{R}$ of h_n', other than a critical point of h_{n-1}, must satisfy $c_S^{3^{n-1}} = 2h_{n-1}(\zeta)$. So, in particular, h_2 has the same regions of strict increase and strict decrease as h_1, and thus h_2 has maximum $\leq 3/8$. Proceeding by induction, we see thus see that h_n has no critical points other than $1/2$ and thus no real roots other than 0 and 1. Moreover, the latter roots occur with multiplicity 1 from the obvious recursive factorization of h_n. So $\frac{h_n(x_1)}{x_1(1-x_1)}$ has no real roots. ■

5. Wrapping up: Invariance of $Y_L(n,k)$, and the Proofs of Proposition 1.4, Theorem 1.10, and Lemmata 4.1 and 4.2

Let us now see how the value of $Y_L(n,k)$ depends weakly (if at all) on the underlying uniformizer, and how counting roots with coordinates of generalized phase 1 is as good as counting roots in any other direction. In what follows, we let $W_L(n,k)$ denote the supremum, over all $(n+k)$-nomial $n \times n$ systems F over L, of the *total* number of non-degenerate roots of F in $(L^*)^n$.

Proposition 5.1.

(1) *For L any finite extension of $\mathbb{Q}_p$, and $n, k \geq 1$, the value of $Y_L(n,k)$ in Definition 1.1 is independent of the choice of uniformizer ρ. Also, the same holds for $L = \mathbb{F}_q((t))$*

when $n=1$.

(2) $Y_L(n,k)$ *counts the supremum of the number of roots in* any *fixed angular direction in the following sense: let* $\theta_1,\ldots,\theta_n$ *be elements of the complex unit circle, elements of* $\{\pm 1\}$, *or units in the residue field of* L, *according as* L *is* $\mathbb{C}$, $\mathbb{R}$, *or non-Archimedean. Also, letting* F *and* G *denote* $(n+k)$*-nomial* $n\times n$ *systems over* L, *there is an* F *with exactly* N *non-degenerate roots* $(\zeta_1,\ldots,\zeta_n)\in L^n$ *satisfying* $\phi(\zeta_i)=\theta_i$ *for all* i *if and only if there is a* G *with exactly* N *non-degenerate roots in* L^n *with all coordinates having generalized phase* 1.

(3) $W_{\mathbb{C}}(n,k)=+\infty$, $W_{\mathbb{R}}(n,k)=2^nY_{\mathbb{R}}(n,k)$, *and* $W_L(n,k)=(q_L-1)^nY_L(n,k)$ *for any finite extension* L *of* $\mathbb{Q}_p$ *with residue field cardinality* q_L. *Also, we have*
$$W_{\mathbb{F}_q((t))}(n,k)\leq (q-1)^nY_{\mathbb{F}_q((t))}(n,k)\leq (q-1)^nW_{\mathbb{F}_q((t))}(n,k).$$

Proof:
Assertion (2): To prove independence of direction, fix a uniformizer ρ once and for all (for the non-Archimedean case) and assume F has exactly N non-degenerate roots $(\zeta_1,\ldots,\zeta_n)\in L^n$ satisfying $\phi(\zeta_i)=\theta_i$ for all i. Defining $G(x_1,\ldots,x_n)=F(t_1x_1,\ldots,t_nx_n)$ for any $t_1,\ldots,t_n$ of valuation 0 with $\phi(t_i)=\theta_i$ for all i, we then clearly obtain a suitable G with exactly N non-degenerate roots with all coordinates having generalized phase 1. The preceding substitutions can also be inverted to give the converse direction, so we obtain independence of direction, and (in the non-Archimedean case) for any ρ. ■

Assertion (3): The first equality was already observed in Section 1.2.

Now recall that any $y\in\mathbb{R}^*$ (resp. $y\in L$, $y\in\mathbb{F}_q((t))$) can be written in the form $y=uz$ where $u\in\{\pm 1\}$ (resp. u is a unit in the residue field of L or $u\in\mathbb{F}_q^*$), $|y|=|z|$, and z has generalized phase 1. So Assertion (2) then immediately implies $W_{\mathbb{R}}(n,k)\leq 2^nY_{\mathbb{R}}(n,k)$, $W_L(n,k)\leq (q_L-1)^nY_L(n,k)$, and $W_{\mathbb{F}_q((t))}(n,k)\leq (q-1)^nY_{\mathbb{F}_q((t))}(n,k)$. Note also that $Y_{\mathbb{F}_q((t))}(n,k)\leq W_{\mathbb{F}_q((t))}(n,k)$, independent of the underlying uniformizer.

So now we need only prove $W_{\mathbb{R}}(n,k)\geq 2^nY_{\mathbb{R}}(n,k)$ and $W_L(n,k)\geq (q_L-1)^nY_L(n,k)$. Toward this end, note that for any F with N non-degenerate roots in $\mathbb{R}^n$ (resp. L^n), with all coordinates of generalized phase 1, the substitution $x_i=y_i^2$ (resp. $x_i=y_i^{q_L}$) for all i yields a new system with exactly N non-degenerate roots in $\mathbb{R}^n$ (resp. L^n) with n-tuple of generalized phases $(\theta_1,\ldots,\theta_n)$ for *any* $\theta_1,\ldots,\theta_n$ in $\{\pm 1\}$ (resp. units in the residue field). Clearly then, $W_{\mathbb{R}}(n,k)\geq 2^nY_{\mathbb{R}}(n,k)$ and $W_L(n,k)\geq (q_L-1)^nY_L(n,k)$. ■

Assertion (1): For L as in the first part, Assertion (3) tells us that $Y_L(n,k)=\frac{W_L(n,k)}{(q_L-1)^n}$ where q_L is the residue field cardinality of L. $W_L(n,k)$ is independent of ρ, so the first part is proved. The second assertion follows immediately from Section 2 of [Poo98]. ■

5.1. **Proof of Proposition 1.4.** First note that by Gaussian elimination, $k\leq 0$ immediately implies that any $(n+k)$-nomial $n\times n$ system is either equivalent to an $n\times n$ system where all the polynomials are monomials or an $n\times n$ system with at least one polynomial identically zero. Neither type of system can have a root in $(L^*)^n$ with Jacobian of rank n. So we obtain the first equality.

Similarly, any $(n+1)$-nomial $n\times n$ system is either equivalent to an $n\times n$ system consisting solely of binomials or an $n\times n$ system with at least polynomial having 1 or fewer monomial terms. The latter type of system can not have a root in $(L^*)^n$ with Jacobian of rank n, so we may assume that we have an $n\times n$ binomial system. After dividing each binomial by a suitable monomial we can then assume our system has the form $(x^{a_1}-c_1,\ldots,x^{a_n}-c_n)$ for some $a_1,\ldots,a_n\in\mathbb{Z}^n$ and $c_1,\ldots,c_n\in L^*$. Furthermore, via a monomial change of variables, we may in fact assume that $x^{a_i}=x_i^{d_i}$ for all i, for some choice of integers $d_1,\ldots,d_n$. The latter reduction is routine, but we are unaware of a treatment in the literature allowing general fields. So we present a concise version below.

For any integral matrix $A=[a_{i,j}]\in\mathbb{Z}^{n\times n}$ with columns $a_1,\ldots,a_n$, let us write $x^A=(x^{a_1},\ldots,x^{a_n})$ where the notation $x^{a_i}=x_1^{a_{1,i}}\cdots x_n^{a_{n,i}}$ is understood. It is easily checked that $x^{AB}=(x^A)^B$ for any $n\times n$ matrix B.

Recall that an integral matrix $U\in\mathbb{Z}^{n\times n}$ is said to be *unimodular* if and only if its determinant is ± 1. It is easily checked that the substitution $x=y^U$ induces an automorphism on $(L^*)^n$ that also preserves the number of roots with all coordinates having generalized phase 1. From the classical theory of *Smith factorization* [Smi61, Sto00], one can always write $UAV=D$ for some unimodular U and V, and a diagonal matrix D with nonnegative diagonal entries $d_1,\ldots,d_n$.

Applying the last two paragraphs to our binomial system x^A-c, we see that to count the maximal number of roots in $(L^*)^n$ (with all coordinates having generalized phase 1) we may assume that our system is in fact $(x_1^{d_1}-c_1,\ldots,x_n^{d_n}-c_n)$. We thus obtain $Y_L(n,1)=Y_L(1,1)^n$ and, by Assertions (2), (1), (4), and (6) of Theorem 1.2, we are done. ■

5.2. **Proof of Theorem 1.10.** The inequality $Y_{\mathbb{C}}(n,k)\geq Y_{\mathbb{R}}(n,k)$ is immediate since any real $(n+k)$-nomial $n\times n$ system is automatically a complex $(n+k)$-nomial $n\times n$ system. So we need only prove that $Y_{\mathbb{C}}(n,k)\leq Y_{\mathbb{R}}(n,k)$. To do the latter, it clearly suffices to show that for any $(n+k)$-nomial $n\times n$ system $G:=(g_1,\ldots,g_n)$ over $\mathbb{C}$, with N non-degenerate roots in $\mathbb{R}^n_+$, we can find an $(n+k)$-nomial $n\times n$ system $F:=(f_1,\ldots,f_n)$ — with all coefficients *real* — having at least N non-degenerate roots in $\mathbb{R}^n_+$. So, for all i, let us define $f_i:=e^{\sqrt{-1}t}g_i+e^{-\sqrt{-1}t}\bar{g}_i$ where $\bar{(\cdot)}$ denotes complex conjugation, $\bar{g}_i$ is the polynomial obtained from g_i by conjugating all its coefficients, and $t\in[0,2\pi)$ is a constant to be determined later. Clearly, for all i, the coefficients of f_i are all real, and any exponent vector appearing in f_i also appears in g_i.

It is also clear that for any $\zeta\in\mathbb{R}^n_+$ with $G(\zeta)=0$ we have

$$f_i(\zeta)=e^{\sqrt{-1}t}g_i(\zeta)+e^{-\sqrt{-1}t}\bar{g}_i(\zeta)=e^{\sqrt{-1}t}g_i(\zeta)+\overline{e^{\sqrt{-1}t}g_i(\zeta)}=0.$$

So any root of G in $\mathbb{R}^n_+$ is a root of F in $\mathbb{R}^n_+$.

Let $\mathrm{Jac}(F)(\zeta)$ denote the Jacobian determinant of F evaluated at ζ, and assume now that $\zeta\in\mathbb{R}^n_+$ is a non-degenerate root of G. To see that ζ is also a non-degenerate root of F (for a suitable choice of t), note that the multi-linearity of the determinant implies the following:

$$\mathrm{Jac}(F)(\zeta)=\sum_{s=(s_1,\ldots,s_n)\in\{\pm\}^n} e^{\sqrt{-1}(n_+(s)-n_-(s))t}\mathrm{Jac}(g_{1,s_1},\ldots,g_{n,s_n})(\zeta),$$

where $n_\pm(s)$ is the number of $\pm$ signs in s, $g_{i,+}:=g_i$, and $g_{i,-}:=\bar{g}_i$. In particular, we see that $\mathrm{Jac}(F)(\zeta)=J\left(e^{\sqrt{-1}t}\right)$ for some $J\in\mathbb{C}\left[x_1,\frac{1}{x_1}\right]$. Moreover, J is not identically zero since the coefficient of x_1^n is $\mathrm{Jac}(G)(\zeta)\neq 0$. Clearly then, J has at most $2n$ roots in $\mathbb{C}^*$ and thus there are at most $2n$ values of $t\in[0,2\pi)$ for which $\mathrm{Jac}(F)(\zeta)$ vanishes.

Thus, assuming G has N non-degenerate roots in $\mathbb{R}^n_+$, F fails to have at least N non-degenerate roots in $\mathbb{R}^n_+$ for at most $2nN$ values of $t\in[0,2\pi)$. ■

5.3. **Proof of Lemma 4.1.** Recall that in Section 4 we wrote $R_n=A_n-B_n$ where A_n and B_n are suitable monomials. Assuming $n\geq 3$ is odd we obtain the following:

$$A_n\left(\frac{16^{n-2}}{u}\right)=\frac{16^{n-2}}{u}\prod_{i=1}^{\lfloor n/2\rfloor}\left(1+4^{3-4i}\frac{4^{2n-4}}{u}\right)^2=\frac{16^{n-2}}{u}\prod_{i=1}^{\lfloor n/2\rfloor}\left(1+\frac{4^{2n-4i-1}}{u}\right)^2$$

$$= \frac{16^{n-2}}{u} \prod_{i=1}^{\lfloor n/2 \rfloor} \left(\frac{4^{2n-4i-1}}{u} \left(1 + 4^{4i-2n+1} u\right) \right)^2 = \frac{4^{2n-4}}{u} \cdot \frac{4^S}{u^{n-1}} \prod_{i=1}^{\lfloor n/2 \rfloor} \left(1 + 4^{4i-2n+1} u\right)^2,$$

where $S = 2 \sum_{i=1}^{\lfloor n/2 \rfloor} (2n - 4i - 1)$. A minor calculation shows that $S + 2n - 4 = (n-2)(n+1)$, so replacing i by $\lfloor n/2 \rfloor - i + 1$, we get

$$A_n\left(\frac{16^{n-2}}{u}\right) = \left(\frac{4^{n-2}}{u}\right)^{n+1} u \prod_{i=1}^{\lfloor n/2 \rfloor} (1 + 4^{3-4i} u)^2 = \left(\frac{4^{n-2}}{u}\right)^{n+1} A_n(u).$$

An almost identical calculation proves the same transformation law for $B_n(u)$. Since $R_n = A_n - B_n$, we thus obtain our transformation law for odd n.

For even n, a similar calculation yields $A_n\left(\frac{16^{n-2}}{u}\right) = \left(\frac{4^{n-2}}{u}\right)^{n+1} B_n(u)$ and $B_n\left(\frac{16^{n-2}}{u}\right) = \left(\frac{4^{n-2}}{u}\right)^{n+1} A_n(u)$. So we obtain $R_n\left(\frac{16^{n-2}}{u}\right) = -\left(\frac{4^{n-2}}{u}\right)^{n+1} R_n(u)$ and thus the first assertion is proved.

The final assertion follows immediately from our transformation law since $16^{n-2}/4^{n-2} = 4^{n-2}$ and $(-4^{n-2}/4^{n-2})^{n+1} = -1$ for even n. ■

5.4. **Proof of Lemma 4.2.** To prove (a), merely observe that $R_n(0) = -\frac{1}{16} < 0$ for all $n \geq 2$.

To prove (b), the cases $n \leq 4$ can be verified by direct computation. So let us assume $n \geq 5$ and separate into two exclusive cases.

(ℓ even): Let us first observe the following elementary inequality:

(1) $$\prod_{i=1}^{(n-1)/2} \left(1 - \frac{15/16}{1 + 256^{i-2}}\right) \geq \frac{7}{200}\left(1 + \frac{1}{4^{n-1}}\right) \text{ for all odd } n \geq 3.$$

Inequality (1) follows easily by induction, after one first verifies the cases $n \in \{3, 5, 7\}$ directly. The identity $\frac{1+16z}{1+z} = 16\left(1 - \frac{15/16}{1+z}\right)$ then easily implies the following equality:

(2) $$\left(\frac{1 + 4^{2n-8}}{1 + 4^{2n-10}}\right)\left(\frac{1 + 4^{2n-12}}{1 + 4^{2n-14}}\right) \cdots \left(\frac{1 + 4^{-2}}{1 + 4^{-4}}\right) = 16^{(n-1)/2} \prod_{i=1}^{(n-1)/2} \left(1 - \frac{15/16}{1 + 256^{i-2}}\right)$$

Combining (1) and (2) we then obtain, for any odd $n \geq 5$:

$$\begin{aligned}
\frac{A_n(4^{2n-7})}{B_n(4^{2n-7})} &= \frac{4^{2n-7} \cdot 4^{2n-2}}{\left(\frac{1}{4} + 4^{2n-7}\right)^2} \prod_{i=1}^{(n-1)/2} \left(1 - \frac{15/16}{1 + 256^{i-2}}\right)^2 \\
&\geq \frac{4^{2n-7} \cdot 4^{2n-2}}{\left(\frac{1}{4} + 4^{2n-7}\right)^2} \frac{7^2}{200^2} \left(1 + \frac{1}{4^{n-1}}\right)^2 = \frac{4^{2n-7} \cdot 4^{2n-7}}{\left(\frac{1}{4} + 4^{2n-7}\right)^2} \cdot \frac{4^5 \cdot 7^2}{200^2} \left(1 + \frac{1}{4^{n-1}}\right)^2 \\
&= \left(\frac{1 + \frac{1}{4^{n-1}}}{1 + \frac{1}{4^{2n-6}}}\right)^2 \cdot \frac{4^5 \cdot 7^2}{200^2} \geq \frac{4^5 \cdot 7^2}{200^2} = 1.2544 > 1
\end{aligned}$$

We thus obtain

(3) $$A_\ell\left(4^{2\ell-7}\right) > B_\ell\left(4^{2\ell-7}\right) \text{ for all odd } \ell \geq 3$$

Recall that for any odd n, (i) $A_{n+1}(u) = A_n(u)\left(1 + \frac{u}{4^{2n-1}}\right)^2$ and $B_{n+1}(u) = B_n(u)$, and (ii) $A_{n+2}(u) = A_n(u)\left(1 + \frac{u}{4^{2n-1}}\right)^2$ and $B_{n+1}(u) = B_n(u)\left(1 + \frac{u}{4^{2n+1}}\right)^2$. Combining the recurrences (i) and (ii) with Inequality (3), we then easily obtain by induction and re-indexing that $A_n(16^\ell/4) > B_n(16^\ell/4)$ for all $\ell \in \{0, \ldots, n-3\}$ with ℓ even. So we are done. ■

(ℓ odd): This case follows almost identically as the last case, save for minor changes in the indexing. In particular, one first uses Inequality (1) to prove that $A_\ell\left(4^{2\ell-7}\right) < B_\ell\left(4^{2\ell-7}\right)$ for all *even* $\ell \geq 4$. One then increases the subscript from ℓ to n by induction, and re-indexes ℓ, just as before. So we omit the details for brevity. ■

Acknowledgements

We thank Martín Avendaño, Qi Cheng, Pascal Koiran, Jeff Lagarias, Matt Papanikolas, Philippe Pébay, and Bjorn Poonen for useful discussions, some of them p-adic. In particular, Example 2.5 was inspired by a conversation between the second author and Bjorn Poonen at the Extensions of Hilbert's Tenth Problem workshop at the American Institute of Mathematics, March 21–25, 2005. We also thank the anonymous referee for useful commentary. Special thanks go to Richard Lipton for pointing out his earlier result [Lip94] that cryptographic hardness of factoring implies a weakened version of the τ-Conjecture. Finally, we thank the Fields Institute and the Laboratoire de l'Informatique du Parallélisme (at the École Normale Supérieure de Lyon) for their hospitality and great work environment while this paper was completed.

We dedicate this paper in honor of Bernd Sturmfels' $50^{\underline{\text{th}}}$ birthday. Happy 50 Bernd!

References

[AV08] Agrawal, M. and Vinay, V., *"Arithmetic circuits: A chasm at depth four,"* In Proc. 49th IEEE Symposium on Foundations of Computer Science, pp. 67–75, 2008.

[AB09] Arora, Sanjeev and Barak, Boaz, *Computational complexity. A modern approach.* Cambridge University Press, Cambridge, 2009.

[Ave09] Avendaño, Martín, *"The number of roots of a lacunary bivariate polynomial on a line,"* J. Symbolic Comput. 44 (2009), no. 9, pp. 1280–1284.

[AI10] Avendaño, Martín and Ibrahim, Ashraf, *"Ultrametric root counting,"* Houston Journal of Mathematics, vol. 36 (4), pp. 1011–1022, 2010.

[AI11] Avendaño, Martín and Ibrahim, Ashraf, *"Multivariate ultrametric root counting,"* in Randomization, Relaxation, and Complexity in Polynomial Equation Solving, Contemporary Mathematics, vol. 556, pp. 1–24, AMS Press, 2011.

[AK11] Avendaño, Martín and Krick, Teresa, *"Sharp Bounds for the Number of Roots of Univariate Fewnomials,"* Journal of Number Theory 131 (2011), pp. 1209–1228.

[AKS07] Avendaño, Martín; Krick, Teresa; and Sombra, Martin, *"Factoring bivariate sparse (lacunary) polynomials,"* J. Complexity, vol. 23 (2007), pp. 193–216.

[BS96] Bach, Eric and Shallit, Jeff, *Algorithmic Number Theory, Vol. I: Efficient Algorithms,* MIT Press, Cambridge, MA, 1996.

[BHPR11] Bastani, Osbert; Hillar, Chris; Popov, Dimitar; and Rojas, J. Maurice, *"Randomization, Sums of Squares, and Faster Real Root Counting for Tetranomials and Beyond,"* Randomization, Relaxation, and Complexity in Polynomial Equation Solving, Contemporary Mathematics, vol. 556, pp. 145–166, AMS Press, 2011.

[BS11] Bates, Dan and Sottile, Frank, *"Khovanskii-Rolle continuation for real solutions,"* Foundations of Computational Mathematics, October 2011, Vol. 11, Issue 5, pp. 563–587.

[Ber75] Bernshtein, David N., *"The Number of Roots of a System of Equations,"* Functional Analysis and its Applications (translated from Russian), Vol. 9, No. 2, (1975), pp. 183–185.

[BBS05] Bertrand, Benoit; Bihan, Frederic; and Sottile, Frank, *"Polynomial Systems with Few Real Zeroes,"* Mathematisches Zeitschrift, 253 (2006), no. 2, pp. 361–385.

[BCR12] Bi, Jingguo Bi; Cheng, Qi; and Rojas, J. Maurice, *Sub-Linear Root Detection, and New Hardness Results, for Sparse Polynomials Over Finite Fields,* submitted for publication, also available as Math ArXiV preprint `arXiv:1204.1113` .

[Bih07] Bihan, Frederic, *"Polynomial systems supported on circuits and dessins d'enfants,"* J. London Math. Soc. 75 (2007), no. 1, pp. 116–132.

[BRS07] Bihan, Frederic; Rojas, J. Maurice; and Sottile, Frank, *"On the Sharpness of Fewnomial Bounds and the Number of Components of Fewnomial Hypersurfaces,"* IMA Volume 146: Algorithms in Algebraic Geometry (edited by A. Dickenstein, F.-O. Schreyer, and A. J. Sommese), pp. 15–20, Springer, New York, 2007.

[BRS09] Bihan, Frederic; Rojas, J. Maurice; Stella, Case E., *"Faster Real Feasibility via Circuit Discriminants,"* proceedings of International Symposium on Symbolic and Algebraic Computation (ISSAC 2009, July 28–31, Seoul, Korea), pp. 39–46, ACM Press, 2009.

[BS07] Bihan, Frederic and Sottile, Frank, *"New Fewnomial Upper Bounds from Gale Dual Polynomial Systems,"* Moscow Mathematical Journal, 7 (2007), no. 3, pp. 387–407.

[BCSS98] Blum, Lenore; Cucker, Felipe; Shub, Mike; and Smale, Steve, *Complexity and Real Computation,* Springer-Verlag, 1998.

[BC76] Borodin, Alan and Cook, Steve, *"On the number of additions to compute specific polynomials,"* SIAM Journal on Computing, 5(1):146–157, 1976.

[Bra39] Brauer, Alfred, *"On addition chains,"* Bull. Amer. Math. Soc. 45, (1939), pp. 736–739.

[Bür00] Bürgisser, Peter, *"Cook's versus Valiant's Hypothesis,"* Theor. Comp. Sci., 235:71–88, 2000.

[Bür09] ______________, *"On defining integers and proving arithmetic circuit lower bounds,"* Computational Complexity, 18:81–103, 2009.

[BLMW11] Bürgisser, Peter; Landsberg, J. M.; Manivel, Laurent; and Weyman, Jerzy, *"An Overview of Mathematical Issues Arising in the Geometric Complexity Theory Approach to* $\mathbf{VP} \neq \mathbf{VNP}$*,"* SIAM J. Comput. **40**, pp. 1179-1209, 2011.

[CGKPS12] Chattopadhyay, Arkadev; Grenet, Bruno; Koiran, Pascal; Portier, Natacha; and Strozecki, Yann, *"Factoring bivariate lacunary polynomials without heights,"* Math ArXiV preprint arXiv:1206.4224

[Che04] Cheng, Qi, *"Straight Line Programs and Torsion Points on Elliptic Curves,"* Computational Complexity, Vol. 12, no. 3–4 (sept. 2004), pp. 150–161.

[CZ02] Cohen, Paula B. and Zannier, Umberto, *"Fewnomials and intersections of lines with real analytic subgroups in* $\mathbf{G}_m^n$*,"* Bull. London Math. Soc. 34 (2002), no. 1, pp. 21–32.

[Dan78] Danilov, Vladimir Ivanovich, *"The Geometry of Toric Varieties,"* Russian Mathematical Surveys, 33 (2), pp. 97–154, 1978.

[DvdD88] Denef, Jan and van den Dries, Lou, *"p-adic and Real Subanalytic Sets,"* Annals of Mathematics (2) **128** (1988), no. 1, pp. 79–138.

[EKL06] Einsiedler, Manfred; Kapranov, Mikhail; and Lind, Douglas, *"Non-archimedean amoebas and tropical varieties,"* Journal für die reine und angewandte Mathematik (Crelles Journal), Vol. 2006, no. 601, pp. 139–157, December 2006.

[Ewa96] Ewald, Günter, *Combinatorial Convexity and Algebraic Geometry,* Graduate Texts in Mathematics 168, Springer-Verlag, New York, 1996.

[For09] Fortnow, Lance, *"The status of the* **P** *versus* **NP** *problem,"* Commun. ACM **52** (2009), no. 9, pp. 78–86.

[GV01] Gabrielov, Andrei and Vorobjov, Nicolai, *"Complexity of cylindrical decompositions of sub-Pfaffian sets,"* Effective methods in algebraic geometry (Bath, 2000), J. Pure Appl. Algebra 164 (2001), no. 1–2, pp. 179–197.

[GKZ94] Gel'fand, Israel Moseyevitch; Kapranov, Misha M.; and Zelevinsky, Andrei V.; *Discriminants, Resultants and Multidimensional Determinants,* Birkhäuser, Boston, 1994.

[Gri82] Grigor'ev, Dima Yu., *"Lower Bounds in the Algebraic Complexity of Computations,"* The Theory of the Complexity of Computations, I; Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) **118** (1982), pp. 25–82, 214.

[GR10] Giesbrecht, Mark and Roche, Daniel, *"Interpolation of shifted-lacunary polynomials,"* Computational Complexity, vol. 19, no. 3, pp. 333–354, 2010.

[GKPR12] Grenet, Bruno; Koiran, Pascal; Portier, Natacha; and Rojas, J. Maurice, *"An Unreal Approach to Circuit Complexity"* in progress, 2012.

[HS95] Huber, Birkett and Sturmfels, Bernd, *"A Polyhedral Method for Solving Sparse Polynomial Systems,"* Math. Comp. **64** (1995), no. 212, pp. 1541–1555.

[Kal03] Kaloshin, Vadim, *"The existential Hilbert 16-th problem and an estimate for cyclicity of elementary polycycles,"* Invent. Math. 151 (2003), no. 3, pp. 451–512.

[KK06] Kaltofen, Erich and Koiran, Pascal, *"Finding small degree factors of multivariate supersparse (lacunary) polynomials over algebraic number fields,"* in proceedings of ISSAC 2005 (Internat. Symp. Symbolic Algebraic Comput.), pp. 162–168, ACM Press, 2006.

[Kho80] Khovanskii, Askold G., *"On a Class of Systems of Transcendental Equations,"* Dokl. Akad. Nauk SSSR **255** (1980), no. 4, pp. 804–807; English transl. in Soviet Math. Dokl. **22** (1980), no. 3.

[Kho91] __________________, *Fewnomials,* AMS Press, Providence, Rhode Island, 1991.

[Koi11] Koiran, Pascal, *"Shallow Circuits with High-Powered Inputs,"* in Proceedings of Innovations in Computer Science (ICS 2011, Jan. 6–9, 2011, Beijing China), Tsinghua University Press, Beijing.

[KPT12] Koiran, Pascal; Portier, Natacha; and Tavenas, Sébastien, *"A Wronskian Approach to the Real τ-Conjecture,"* math ArXiV preprint `1205.101` .

[Len99a] Lenstra (Jr.), Hendrik W., *"Finding Small Degree Factors of Lacunary Polynomials,"* Number Theory in Progress, Vol. 1 (Zakopane-Kóscielisko, 1997), pp. 267–276, de Gruyter, Berlin, 1999.

[Len99b] ______________________, *"On the Factorization of Lacunary Polynomials,"* Number Theory in Progress, Vol. 1 (Zakopane-Kóscielisko, 1997), pp. 277–291, de Gruyter, Berlin, 1999.

[LRW03] Li, Tien-Yien; Rojas, J. Maurice; and Wang, Xiaoshen, *"Counting Real Connected Components of Trinomial Curves Intersections and m-nomial Hypersurfaces,"* Discrete and Computational Geometry, 30:379–414 (2003).

[Lip88] Lipshitz, Leonard, *"p-adic Zeros of Polynomials,"* J. Reine Angew. Math. **390** (1988), pp. 208–214.

[Lip94] Lipton, Richard, *"Straight-line complexity and integer factorization,"* Algorithmic number theory (Ithaca, NY, 1994), pp. 71–79, Lecture Notes in Comput. Sci., 877, Springer, Berlin, 1994.

[Lip09] Lipton, Richard, *"Gödel's Lost Letter and* $\mathbf{P} = \mathbf{NP}$*,"* blog entry, `http://rjlipton.wordpress.com/the-gdel-letter` .

[LRS10] De Loera, Jesús A.; Rambau, Jörg; Santos, Francisco, *Triangulations,* Structures for algorithms and applications, Algorithms and Computation in Mathematics, 25, Springer-Verlag, Berlin, 2010.

[MS12] Maclagan, Diane and Sturmfels, Bernd, *Introduction to Tropical Geometry,* in progress.

[Maz78] Mazur, Barry, *"Rational Isogenies of Prime Degree,"* Invent. Math., 44, 1978.

[dMS96] de Melo, W. and Svaiter, B. F., *"The cost of computing integers,"* Proc. Amer. Math. Soc. **124** (1996), pp. 1377–1378.

[Mer96] Merel, Loic, *"Bounds for the torsion of elliptic curves over number fields,"* Invent. Math., 124(1–3):437–449, 1996.

[Mor97] T. de Araujo Moreira, Gustavo, *"On asymptotic estimates for arithmetic cost functions,"* Procceedings of the American Mathematical Society, Vol. 125, no. 2, Feb. 1997, pp. 347–353.

[Pap95] Papadimitriou, Christos H., *Computational Complexity,* Addison-Wesley, 1995.

[Par99] Parent, Philippe, *"Effective Bounds for the torsion of elliptic curves over number fields,"* J. Reine Angew. Math, 508:65–116, 1999.

[PT05] Passare, Mikael and Tsikh, August, *"Amoebas: their spines and their contours,"* Idempotent mathematics and mathematical physics, Contemp. Math., v. 377, Amer. Math. Soc., Providence, RI, 2005, pp. 275–288.

[PRT09] Pébay, Philippe P.; Rojas, J. Maurice; and Thompson, David C., *"Optimization and $\mathbf{NP}_{\mathbb{R}}$-Completeness of Certain Fewnomials,"* proceedings of SNC 2009 (August 3–5, 2009, Kyoto, Japan), pp. 133–142, ACM Press, 2009.

[PS07] Perrucci, Daniel and Sabia, Juan, *"Real roots of univariate polynomials and straight line programs,"* J. Discrete Algorithms 5 (2007), no. 3, pp. 471–478.

[Poo98] Poonen, Bjorn, *"Zeros of sparse polynomials over local fields of characteristic p"*, Math. Res. Lett. 5(3), pp. 273–279, 1998.

[Rob00] Robert, Alain M., *A course in p-adic analysis,* Graduate Texts in Mathematics, 198, Springer-Verlag, New York, 2000.

[Roj01] Rojas, J. Maurice, *"Finiteness for Arithmetic Fewnomial Systems,"* in Contemporary Mathematics, vol. 286, (edited by E. Green, S. Hosten, R. Laubenbacher and V. Powers), pp. 107–114, AMS Press, 2001.

[Roj02] ________________, *"Additive Complexity and the Roots of Polynomials Over Number Fields and* $\mathfrak{p}$*-adic Fields,"* Proceedings of ANTS-V (5th Annual Algorithmic Number Theory Symposium, University of Sydney, July 7-12, 2002), Lecture Notes in Computer Science #2369, Springer-Verlag (2002), pp. 506–515.

[Roj03a] ________________, *"Why Polyhedra Matter in Non-Linear Equation Solving,"* paper in Algebraic Geometry and Geometric Modelling (Vilnius, Lithuania, July 29 – August 2, 2002), Contemporary Mathematics, vol. 334, pp. 293–320, AMS Press, 2003.

[Roj04] ________________, *"Arithmetic Multivariate Descartes' Rule,"* American Journal of Mathematics, vol. 126, no. 1, February 2004, pp. 1–30.

[RSS11] Rusek, Korben; Sottile, Frank; and Shakalli-Tang, Jeanette, *"Dense Fewnomials,"* in Randomization, Relaxation, and Complexity in Polynomial Equation Solving, Contemporary Mathematics, vol. 556, pp. 167–186, AMS Press, 2011.

[Sch84] Schikhof, W. H., *Ultrametric Calculus, An Introduction to p-adic Analysis,* Cambridge Studies in Adv. Math. 4, Cambridge Univ. Press, 1984.

[Ser08] Servi, Tamara, *"On the first-order theory of real exponentiation,"* Tesi. Scuola Normale Superiore di Pisa (Nuova Series) [Theses of Scuola Normale Superiore di Pisa (New Series)], 6. Edizioni della Normale, Pisa, 2008.

[Sip92] Sipser, Michael, *"The history and status of the* **P** *versus* **NP** *question,"* in Proceedings STOC '92 (twenty-fourth annual ACM symposium on Theory of computing), pp. 603–618, ACM Press, 1992.

[Sma98] Smale, Steve, *"Mathematical Problems for the Next Century,"* Math. Intelligencer 20 (1998), no. 2, pp. 7–15.

[Sma00] ____________, *"Mathematical Problems for the Next Century,"* Mathematics: Frontiers and Perspectives, pp. 271–294, Amer. Math. Soc., Providence, RI, 2000.

[SL54] Smith, David Eugene and Latham, Marcia L., *The Geometry of René Descartes,* translated from the French and Latin (with a facsimile of Descartes' 1637 French edition), Dover Publications Inc., New York (1954).

[Smi61] Smith, H. J. S., *"On Systems of Integer Equations and Congruences,"* Philos. Trans. 151, pp. 293–326 (1861).

[Sto00] Storjohann, Arne, *"Algorithms for Matrix Canonical Forms,"* doctoral dissertation, Swiss Federal Institute of Technology, Zurich, 2000.

[Stu94] Sturmfels, Bernd, *"Viro's Theorem for Complete Intersections,"* Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 4^e série, tome 21, n^o 3 (1994), pp. 377–386.

[VG03] Vakulenko, Sergey and Grigoriev, Dmitry, *"Complexity of gene circuits, Pfaffian functions and the morphogenesis problem,"* C. R. Math. Acad. Sci. Paris 337 (2003), no. 11, pp. 721–724.

[Val79] Valiant, Leslie G., *"The complexity of computing the permanent,"* Theoret. Comp. Sci., 8:189–201, 1979.

[Vir84] Viro, Oleg Ya., *"Gluing of plane real algebraic curves and constructions of curves of degrees* 6 *and* 7*,"* Topology (Leningrad, 1982), pp. 187–200, Lecture Notes in Math., 1060, Springer, Berlin, 1984.

[Voo76] Voorhoeve, Marc, *"On the Oscillation of Exponential Polynomials,"* Mathematische Zeitschrift, vol. 151, pp. 277–294 (1976).

[Wan04] Wang, Xiaoshen, *"A Simple Proof of Descartes' Rule of Signs,"* The American Mathematical Monthly, Vol. 111, No. 6 (Jun.–Jul., 2004), pp. 525–526, Mathematical Association of America, 2004.

[Wil99] Wilkie, Alex J., *"A theorem of the complement and some new o-minimal structures,"* Selecta Math. (N.S.) 5 (1999), no. 4, pp. 397–421.

Department of Mathematics, Texas A&M University TAMU 3368, College Station, Texas 77843-3368, USA.

E-mail address: `kaitlyn@math.tamu.edu`

E-mail address: `rojas@math.tamu.edu`