

**YEAR 3 (FINAL) REPORT FOR *TEXAS A&M UNIVERSITY GROUP*  
CONTRIBUTION TO DE-FG02-09ER25949/DE-SC0002505:  
TOPOLOGY FOR STATISTICAL MODELING OF PETASCALE DATA  
(AN ASCR-FUNDED COLLABORATION BETWEEN SANDIA  
NATIONAL LABS, TEXAS A&M U, AND U UTAH)**

J. MAURICE ROJAS\*

ABSTRACT. We summarize the contributions of the Texas A&M University Group during 6/9/2011 – 2/27/2013.

## INTRODUCTION

The primary goal of our local team is to develop new theory (and software implementations thereof) for solving large polynomial systems arising from the analysis of petascale data. Some of the notation and background has been detailed in the original project proposal, and the preceding (Year 1 and 2) reports. So let us now summarize more recent progress. (The mentoring of postdocs and graduate students, as well as presentations and conferences organized, are described in Section 4, toward the end of this report.)

Some of the advances of this project during Year 3 include the following:

- (1) An efficient new method to estimate the complex roots of a polynomial system
- (2) Tighter upper and lower bounds for the number of roots of sparse polynomial systems over arbitrary local fields (including the  $p$ -adic rationals, as well as the real and complex numbers)
- (3) New connections between the quantitative behavior of sparse polynomials over local fields and the **VP** vs. **VNP** question

These results, as well as others supported by our current grant, are contained in the 9 papers [PRS11, AIRR12, BHP11, PR13, RSS11, Hau11, KL12, BCR12, AKNR13] (submitted for publication, accepted for publication, or published, during this reporting period), and the recently published AMS proceedings volume [GPRT11] co-edited by Rojas, Sandia Livermore co-PIs Pébay and Thompson, and Sandia Los Alamos scientist Leonid Gurvits.

We now give a brief overview of results (1)–(3).

### 1. FAST TROPICAL APPROXIMATIONS OF COMPLEX ALGEBRAIC SETS

*We show how to define a simple, polyhedral approximation of any complex algebraic hypersurface. Our approximation implies an efficient (albeit coarse) approximation to the roots of any complex polynomial system. [AKNR13] contains further details.*

One of the happiest coincidences in algebraic geometry is the fact that norms of roots of polynomials can be estimated through polyhedral geometry. Perhaps the earliest incarnation of this fact was Newton’s use of a polygon to determine Puiseux series expansions for algebraic functions, as described in a letter to Henry Oldenburg dated October 24, 1676 [New76].

---

*Date:* February 27, 2013.

\* [rojas@math.tamu.edu](mailto:rojas@math.tamu.edu) . Department of Mathematics, Texas A&M University TAMU 3368, College Station, Texas 77843-3368, USA. Partially supported by DOE ASCR grant DE-SC0002505.

Newton's result, in more modern terminology, corresponds to computing norms of roots where the underlying field is  $\mathbb{C}\langle\langle t \rangle\rangle$ .

Newton's result has since been extended to other non-Archimedean fields (e.g.,  $\mathbb{Q}_p$  and  $\mathbb{F}_p((t))$ ); and now tropical geometry [LS09, IMS09, BR10, MS12] continues to deepen the links between algebraic and polyhedral geometry. However, the Archimedean case presents certain subtleties not present in the non-Archimedean case.

**Definition 1.1.** We use the abbreviations  $[N] := \{1, \dots, N\}$ ,  $x := (x_1, \dots, x_n)$ , and let  $\text{Conv}(S)$  denote the convex hull of a set  $S$ . Let us then define the function  $\text{Log}|x|$  to be  $(\log|x_1|, \dots, \log|x_n|)$  and, for any  $f \in \mathbb{C}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ , we define  $\text{Amoeba}(f)$  to be  $\{\text{Log}|x| \mid f(x) = 0, x \in (\mathbb{C}^*)^n\}$ . Also, writing  $f(x) = \sum_{i=1}^t c_i x^{a_i}$  with  $c_i \neq 0$  for all  $i$ , we define the support (or spectrum) of  $f$  to be  $\text{Supp}(f) := \{a_i\}_{i \in [t]}$ , the (ordinary) Newton polytope of  $f$  to be  $\text{Newt}(f) := \text{Conv}(\text{Supp}(f))$ , and the Archimedean Newton polytope of  $f$  to be  $\text{ArchNewt}(f) := \text{Conv}(\{(a_i, -\log|c_i|)\}_{i \in [t]})$ . We also define the Archimedean tropical an outer normal of a positive-dimensional face of  $\text{ArchNewt}(f)$ . Finally, given any subsets  $U, V \subseteq \mathbb{R}^n$ , their Hausdorff distance,  $\Delta(U, V)$ , is defined to be the maximum of  $\sup_{u \in U} \inf_{v \in V} |u - v|$  and  $\sup_{v \in V} \inf_{u \in U} |u - v|$ , where  $|\cdot|$  denotes the usual  $L_2$ -norm on  $\mathbb{R}^n$ .  $\diamond$

**Example 1.2.** When  $t = 2$  it is easy to show that  $\text{Amoeba}(f)$  and  $\text{Trop}(f)$  are identical  $(n-1)$ -flats in  $\mathbb{R}^n$ . More generally,  $\text{Trop}(f)$  is an unbounded  $(n-1)$ -dimensional polyhedral complex and, when  $t \leq \dim(\text{Newt}(f)) + 1$ , it is not hard to show that  $\mathbb{R}^n \setminus \text{Trop}(f)$  is a translate of a disjoint union of exactly  $t$  open  $n$ -dimensional cones.  $\diamond$

**Example 1.3.** Taking  $f(x) = 1 + x_1^3 + x_2^2 - 10x_1x_2$ , an illustration of  $\text{Amoeba}(f) \cap [-7, 7]^2$  and  $\text{Trop}(f) \cap [-7, 7]^2$  appears above. ( $\text{Amoeba}(f)$  is lightly shaded, while  $\text{Trop}(f)$  is the piecewise linear curve.) While  $\text{Trop}(f) \subseteq \text{Amoeba}(f)$ , and  $\text{Trop}(f)$  and  $\text{Amoeba}(f)$  are in fact homotopy equivalent, neither need hold in general.  $\diamond$

The *Newton Majorant*, mentioned by Ostrowski around 1940 [Ost40], is essentially the univariate case of  $\text{Trop}(f)$ .  $\text{Trop}(f)$  has appeared, in different notation and different contexts, in various papers since at least 2000 (e.g., [PR04, Mik05, PRS11, TdW13] to name just a few). Our main contributions here are simple and explicit bounds for how well  $\text{Trop}(f)$  approximates  $\text{Amoeba}(f)$  in arbitrary dimension.

**Definition 1.4.** Let the vertical distance from a point  $(x_1, \dots, x_n, x_{n+1})$  to a set  $S \subseteq \mathbb{R}^{n+1}$  be  $\sup_{(x_1, \dots, x_n, y_{n+1}) \in S} |x_{n+1} - y_{n+1}|$ . We say that a face of  $\text{ArchNewt}(f)$  is a lower face iff it has an outer normal of the form  $(w, -1)$ . Finally, for any  $\sigma > 0$ , we say that  $f$  is  $\sigma$ -bowed iff, for any lower face  $Q$  of  $\text{ArchNewt}(f)$  of dimension  $\dim(\text{Newt}(f))$ , (1)  $Q$  has exactly  $\dim(\text{Newt}(f)) + 1$  vertices and (2) for any  $(a_\ell, -\log|c_\ell|)$  not a vertex of  $Q$ , the vertical distance of  $(a_\ell, -\log|c_\ell|)$  to the flat containing  $Q$  is at least  $\sigma$ .  $\diamond$

In essence,  $\sigma$ -bowedness forces certain monomial term norms  $|c_i \zeta^{a_i}|$  to exceed other  $|c_j \zeta^{a_j}|$  by an increasing function of  $\sigma$ , at any root  $\zeta$  of  $f$ . As detailed further in [AKNR13], this in turn forces  $\text{Amoeba}(f)$  to be close to  $\text{Trop}(f)$ .

**Theorem 1.5.** *For any  $f \in \mathbb{C}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$  with exactly  $t$  monomial terms and  $\text{Newt}(f)$  of dimension  $k$ , we have:*

- (0) *If  $t \leq k + 1$  or  $\text{Newt}(f) \cap \text{Supp}(f) = \text{Supp}(f)$  then both of the following hold:  $\text{Trop}(f) \subseteq \text{Amoeba}(f)$ , and  $\text{Trop}(f)$  and  $\text{Amoeba}(f)$  are homotopy equivalent.*
- (1) *Unconditionally,  $\sup_{u \in \text{Amoeba}(f)} \inf_{v \in \text{Trop}(f)} |u - v| \leq \log(t - 1)$ .*
- (2) *When  $t \geq k + 2$  and  $f$  is  $\log(2(t - k)^2)$ -bowed, we also have  $\sup_{v \in \text{Trop}(f)} \inf_{u \in \text{Amoeba}(f)} |u - v| \leq \log(4(t - k)^2)$ . ■*

An immediate consequence of Assertion (1), for  $n = 1$ , is that the norm of any root of  $f$  is always within a factor of  $t - 1$  of the exponential of the slope of some edge of the lower hull of  $\text{ArchNewt}(f)$ . Alexander Ostrowski proved a similar result in [Ost40, Cor. IX, pg. 143], but his bounds depend on the degree. In particular, for sparse univariate polynomials and roots of near median absolute value (ordering roots by their absolute value), our bounds significantly improve Ostrowski's result.

For multivariate polynomials, our bounds appear to be the first allowing dependence on just the number of terms  $t$ . In particular, letting  $T$  denote the number of lattice points in the Newton polytope of  $f$ , Mikhalkin proved that  $\sup_{u \in \text{Amoeba}(f)} \inf_{v \in \text{Trop}(f)} |u - v| \leq \log(T - 1)$ , in

the special case  $n = 2$  [Mik05, Lemma 8.5, pg. 360]. Assertion (1) of Theorem 1.5 is thus at least sharp and allows  $n$  to be arbitrary.

As far as we are aware, Assertion (2) is the first result asserting that every point of  $\text{Trop}(f)$  is close to some point of  $\text{Amoeba}(f)$ . Based on some computational experiments, we suspect that the assumption of  $\sigma$ -bowedness will eventually be removed.

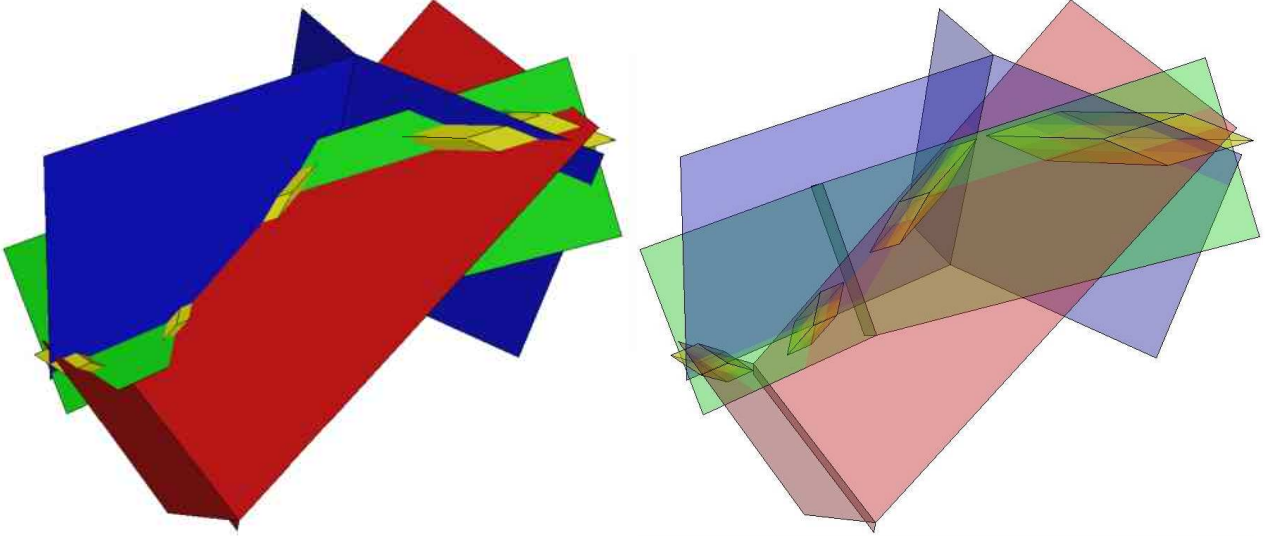
Assertion (0) is included for completeness: the case  $t \leq k + 1$  is likely folkloric, while the case assuming that the support be the vertex set of the Newton polytope was first derived by Passare and Rullgård [PR04, Thm. 2]. It is worth comparing Theorem 1.5 to two other methods for approximating complex amoebae: Purbhoo, in [Pur08], describes a uniformly convergent sequence of outer polyhedral approximations to any amoeba, using cyclic resultants. While  $\text{Trop}(f)$  lacks this refinability, the computation of  $\text{Trop}(f)$  is considerably simpler, with arithmetic complexity polynomial in  $t$  when  $n$  is fixed.  $\text{Trop}(f)$  is in fact closer in spirit to the *spine* of  $\text{Amoeba}(f)$ . The latter construction, based on a multivariate version of Jensen's Formula from complex analysis, is due to Passare and Rullgård [PR04, Sec. 3] and results in a polyhedral complex that is always homotopy equivalent to  $\text{Amoeba}(f)$ . Unfortunately, the computational complexity of the spine is not as straightforward as that of  $\text{Trop}(f)$ . [The02] contains further discussion on the computational complexity of amoebae.

**1.1. Applications: Roots of Polynomial Systems.** An immediate consequence of Assertion (1) of Theorem 1.5 is an estimate for the norms of roots of arbitrary systems of multivariate polynomial equations. In what follows, for any subsets  $A, B \subseteq \mathbb{R}^n$ ,  $A + B$  denotes the *Minkowski sum*  $\{a + b \mid a \in A, b \in B\}$ .

**Corollary 1.6.** *Suppose  $f_1, \dots, f_k \in \mathbb{C}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$  where  $f_i$  has exactly  $t_i$  monomial terms for all  $i$ . Also let  $B_r$  denote the (standard  $L_2$ ) ball of radius  $r$  centered at the origin in  $\mathbb{R}^n$ . Then any root  $\zeta \in (\mathbb{C}^*)^n$  of  $F = (f_1, \dots, f_k)$  satisfies*

$$\text{Log}|\zeta| \in (\text{Trop}(f_1) + B_{\log(t_1 - 1)}) \cap \dots \cap (\text{Trop}(f_k) + B_{\log(t_k - 1)}). \quad \blacksquare$$

**Example 1.7.** Thanks to Corollary 1.6, we can isolate the log-norm vectors of the complex roots of the  $3 \times 3$  system  $F := (f_1, f_2, f_3) := \left(x_1 x_2 - \frac{1}{16^6} - x_1^2, x_2 x_3 - 1 - \frac{x_1^2}{16^6}, x_3 - 1 - \frac{x_1^2}{16^{18}}\right)$  to the intersection of neighborhoods of 3 Archimedean tropical varieties. Here, the intersection  $X := \text{Trop}(f_1) \cap \text{Trop}(f_2) \cap \text{Trop}(f_3)$  consists of exactly 4 points, so the log-norm vectors of the complex roots of  $F$  lie in the union of 4 parallelepipeds that we can easily visualize below (with some transparency in the right-hand illustration):



Truncations of  $\text{Trop}(f_1)$ ,  $\text{Trop}(f_2)$ , and  $\text{Trop}(f_3)$  are respectively drawn in red, green, and blue, while the parallelepipeds are drawn lighter in yellow. In particular, the coordinate-wise exponentials of the coordinates of  $X$  are exactly  $(\frac{1}{16^6}, 1, 1)$ ,  $(1, 1, 1)$ ,  $(16^6, 16^6, 1)$ , and  $(16^{12}, 16^{12}, 16^6)$ . Coordinate by coordinate, these points actually agree to at least 7 digits with the true roots of  $F$ . In particular, the margin of error of the corresponding log-norm vectors is no worse than  $0.11 \times 10^{-6}$  ( $< 0.693 < \log 2$ ), which is well in accordance with Corollary 1.6. (See [PR13] for the relevance of this system to fewnomial theory over local fields.)  $\diamond$

## 2. IMPROVED FEWNOMIAL BOUNDS OVER LOCAL FIELDS AND TROPICAL ILLUSTRATIONS

We study the distribution of the roots of  $F$  in the multiplicative group  $(L^*)^n$  — for  $L$  any local field — as a function of  $n$ ,  $k$ , and  $L$  only. Our main focus will be the number of roots in a fixed angular direction from the origin. See [PR13] for further details.

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  $f_1, \dots, f_n \in L[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$  be Laurent polynomials such that the total number of distinct exponent vectors in the monomial term expansions of  $f_1, \dots, f_n$  is  $n + k$ . We call  $F := (f_1, \dots, f_n)$  an  $(n + k)$ -nomial  $n \times n$  system over  $L$ . The distribution of the roots of  $F$  in  $(L^*)^n$  is a fundamental problem in *fewnomial theory over local fields*. We will sometimes refer to the cases  $L \in \{\mathbb{R}, \mathbb{C}\}$  as the *Archimedean case*.

Fewnomial theory over  $\mathbb{R}$  has since found applications in Hilbert's 16<sup>th</sup> 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 [Len99b, Kal03, AKS07, GR10, CGKPS12]. Since any number field embeds in some finite extension of  $\mathbb{Q}_p$ , we thus have good reason to study fewnomial bounds over non-Archimedean fields. (Applications of general fewnomial bounds to circuit complexity were also mentioned in Section 1 of this report.) However, for  $n, k \geq 2$ , *tight* bounds remain elusive [LRW03, Roj04, BS07, AI10, AI11].

**Definition 2.1.** *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  $\rho$  of  $\mathfrak{M}$  a uniformizer for  $L$ . Letting  $\text{ord}$  denote the corresponding valuation on  $L$  we then alternatively define the generalized phase as  $\phi(y) := \frac{y}{\rho^{\text{ord } y}} \bmod \mathfrak{M}$ . Finally, for general local  $L$ , we define  $Y_L(n, k)$  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  $\rho$ . It is well-known in number theory that  $\phi(y)$  is the natural analogue of the argument (or angle with respect to the positive ray) of a complex number. Our choices of uniformizer and angular direction above are in fact immaterial for the characteristic zero case: see Proposition 2.8 below, which also discusses the positive characteristic case.

Descartes' classic 17<sup>th</sup> century bound on the number of positive roots of a sparse 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 2.2.** *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  $p > 1 + k$ . ■*

**Remark 2.3.** *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  $\prod_{i=1}^k (x_1 - i)$ ,  $3x_1^{10} + x_1^2 - 4$ ,  $x_1^{1+p^{p-1}} - (1 + p^{p-1})x_1 + p^{p-1}$ ,  $\prod_{z_1, \dots, z_{k-1} \in \mathbb{F}_q} (x_1 - z_1 - z_2 t - \dots - z_{k-1} t^{k-1})$ , 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 for finite extensions of  $\mathbb{Q}_p$ : for instance, when  $L$  is the splitting field of  $g(x_1) := x_1^p - 1$  over  $\mathbb{Q}_p$ ,  $g$  has roots  $1, 1 + \mu_1, \dots, 1 + \mu_{p-1}$  where the  $\mu_i$  are distinct elements of  $L$ , each with valuation  $\frac{1}{p-1}$  (see, e.g., [Rob00, pp. 102–109]). 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 2.8 below).

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] and [Lip88, Thm. 2] 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.

---

i.e., roots with Jacobian of rank  $n$

(See [Roj04], and 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  $L$ . Nevertheless, certain cases are easy.

**Proposition 2.4.** [PR13] *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  $L \in \{\mathbb{C}, \mathbb{R}\} \cup \{\mathbb{Q}_3, \mathbb{Q}_5, \dots\} \cup \{\mathbb{F}_q((t)) \mid q \text{ a prime power}\}$ . ■*

For any  $j, N \in \mathbb{N}$  let  $[j]_N \in \{0, \dots, N-1\}$  denote the mod  $N$  reduction of  $j$ . The following theorem summarizes the best general lower bounds on  $Y_L(n, k)$  as of Aug. 2, 2012.

**Theorem 2.5.** [PR13] *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  $n \geq k-1$ , 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  $n \leq k-1$ . More explicitly, the following lower bounds hold:*

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

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 [BRS09]. Non-trivial lower bounds, for  $n \geq k-1 \geq 2$ , were unknown for the non-Archimedean case.

Focussing on  $L \in \{\mathbb{R}, \mathbb{Q}_3, \mathbb{Q}_5, \dots\}$ , we can further condense the best upper and lower bounds on  $Y_L(n, k)$  (as of Aug. 2, 2012) 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] <sup>1</sup>	$\Omega\left(\left\lfloor \frac{n+k-1}{\min\{n, k-1\}} \right\rfloor\right)^{\min\{n, k-1\}}$ (Theorem 2.5 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 2.5 here)

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

<sup>1</sup>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.

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  $L \in \{\mathbb{C}, \mathbb{R}, \mathbb{Q}_3, \mathbb{Q}_5, \dots\}$  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 2.6.** *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  $(x_1 + 1)^{q^m+1} = x_1^2 + 2x_1 + 1$  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  $n$ ,  $k$ , and  $L$ .  $\diamond$*

Theorem 2.5 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 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  $((x_1^d - 1) \cdots (x_1^d - k), x_2 - 1, \dots, x_n - 1)$  as  $d \rightarrow \infty$ . 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 that it suffices to study the real case.

**Theorem 2.7.** [PR13] *For all  $n, k \geq 1$ , we have  $Y_{\mathbb{C}}(n, k) = Y_{\mathbb{R}}(n, k)$ .  $\blacksquare$*

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 number of non-degenerate roots of  $F$  in  $(L^*)^n$ .

**Proposition 2.8.** [PR13]

- (1) *For  $L$  any finite extension of  $\mathbb{Q}_p$ , and  $n, k \geq 1$ , the value of  $Y_L(n, k)$  in Definition 2.1 is independent of the choice of uniformizer  $\rho$ . 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  $\theta_1, \dots, \theta_n$  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  $(\zeta_1, \dots, \zeta_n) \in L^n$  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)  *$W_{\mathbb{C}}(n, k) = +\infty$ ,  $W_{\mathbb{R}}(n, k) = 2^n Y_{\mathbb{R}}(n, k)$ , and  $W_L(n, k) = (q_L - 1)^n Y_L(n, k)$  for any finite extension  $L$  of  $\mathbb{Q}_p$  with residue field cardinality  $q_L$ . Also, we have*

$$W_{\mathbb{F}_q((t))}(n, k) \leq (q - 1)^n Y_{\mathbb{F}_q((t))}(n, k) \leq (q - 1)^n W_{\mathbb{F}_q((t))}(n, k). \quad \blacksquare$$



**2.1. 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 2.9.** Suppose  $K$  is a complete algebraically closed field and  $f \in K[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ . We then define  $\text{Amoeba}_K(f) := \{(\text{ord } x_1, \dots, \text{ord } x_n) \mid f(x_1, \dots, x_n) = 0, x_1, \dots, x_n \in K^*\}$ . Also, if  $K$  is non-Archimedean, we define the tropical variety of  $f$  over  $K$ ,  $\text{Trop}_K(f)$ , to be the closure of  $\{(v_1, \dots, v_n) \in \mathbb{R}^n \mid (v_1, \dots, v_n, 1) \text{ is an inner edge normal of } \text{Newt}_K(f)\}$ .  $\diamond$

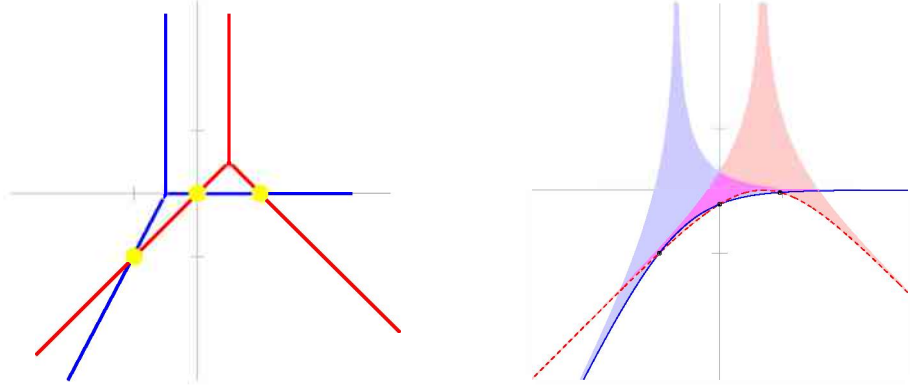
**Remark 2.10.** Note that we've defined  $\text{ord } y = -\text{Log}|y|$  in the Archimedean case, so our  $\text{Amoeba}_{\mathbb{C}}(f)$  is in fact a reflection of the usual Archimedean amoeba as defined in [GKZ94]. We also point out that  $\text{Trop}_K(f)$  is sometimes defined equivalently in terms of max-plus semi-rings (see, e.g., [MS12]).  $\diamond$

**Kapranov's Non-Archimedean Amoeba Theorem.** [EKL06] For  $K$  any complete, non-Archimedean algebraically closed field,  $\text{Amoeba}_K(f) = \text{Trop}_K(f) \cap \mathbb{Q}^n$ .  $\blacksquare$

We now illustrate these ideas through some explicit examples (and some `Matlab` code written for this project). First, consider the following  $2 \times 2$  polynomial system:

$$\begin{aligned} x_1 x_2 &= (\varepsilon + x_1^2) \\ x_2 &= (1 + \varepsilon x_1^2) \end{aligned}$$

Then, according as  $\varepsilon$  is  $p$  or  $t$ , the underlying tropical varieties (or closures of the amoebae over  $\mathbb{Q}_p$  or  $\mathbb{F}_q((t))$ ), intersect in exactly 3 points as illustrated below, on the left. (The amoebae for the first and second polynomials are respectively colored in dashed red and solid blue.) The right-hand illustration below shows the corresponding complex amoebae (with  $\varepsilon = 1/4$ ), with their intersection darkened slightly.



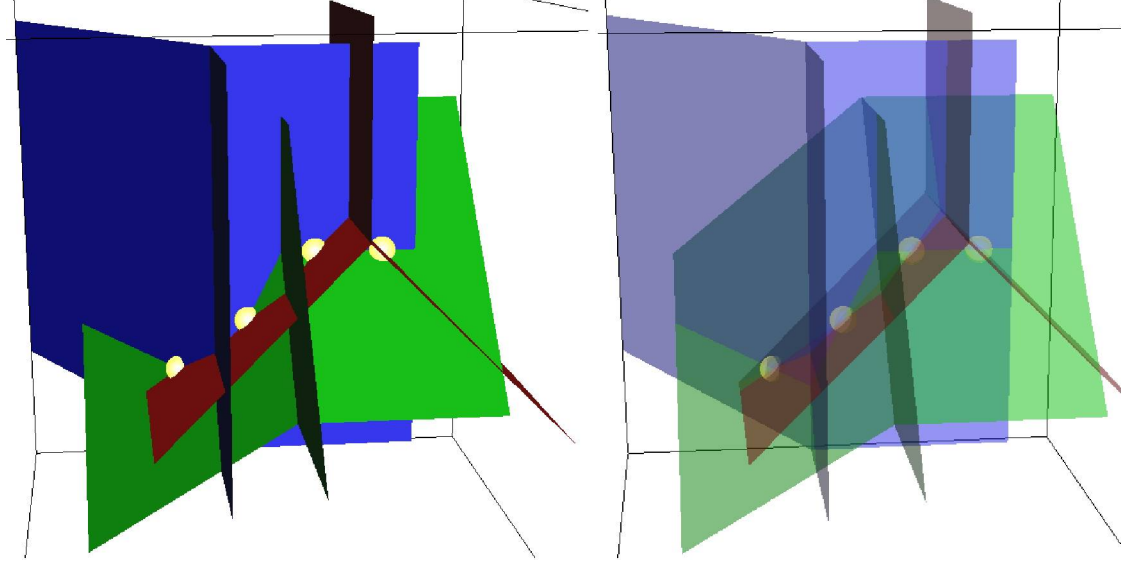
Note that the images of the corresponding positive zero sets under the log-absolute value map are drawn as even darker curves (with 3 marked intersections) in the right-hand illustration above.

Now consider the following  $3 \times 3$  example:

$$\begin{aligned} x_1 x_2 &= (\varepsilon + x_1^2) \\ x_2 x_3 &= (1 + \varepsilon x_1^2) \\ x_3 &= (1 + \varepsilon^3 x_1^2) \end{aligned}$$



The resulting tropical varieties (for  $L$  non-Archimedean and  $\varepsilon$  the underlying uniformizer) 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.

### 3. FROM SPARSE POLYNOMIALS TO **P** VS. **NP**

*Here we detail how sharper upper bounds on the number of roots of certain structured polynomials in one variable imply new complexity lower bounds on the permanent. The upper bounds needed are coming closer to reality, thanks to recent work of PI Rojas and Pascal Koiran. See [PR13, GKPR13] for further details.*

A natural notion refining sparsity (a.k.a. lacunarity) is *straight-line program (SLP) complexity*.

**Definition 3.1.** 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  $(f_{-N}, \dots, f_{-1}, f_0, \dots, f_n)$  satisfies the following conditions:  $f_{-1}, \dots, f_{-N} \in K$ ,  $f_0 := x_1$ , 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 3.2.** Evaluating  $x_1^{2^k}$  via recursive squaring (i.e.,  $(\dots (x_1^2)^2 \dots)^2$ ), and employing the binary expansion of  $d$ , it is easily checked that  $s(x_1^d) = \tau(x_1^d) = O(\log^2 d)$ . 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  $\delta$  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.  $\diamond$

Computing  $s(f)$  and  $\tau(f)$  exactly appears to be quite difficult [GK96]. More to the point, relating SLP complexity to the number of 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 3.3.**

- 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].) 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)  $\deg f_n, \max_{\zeta \in Z_{\mathbb{Z}}(f)} |\zeta| \leq 2^{(\log \#Z_{\mathbb{Z}}(f_n))^{O(1)}}$
 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 (Standard)  $\tau$ -Conjecture, and was also stated as the fourth problem on Smale's list of the most important problems for the 21<sup>st</sup> century [Sma98, Sma00]. Mike Shub informed the authors in late 2011 that, should the  $\tau$ -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  $\mathbb{C}$ ) of the well-known complexity classes  $\mathbf{P}$  and  $\mathbf{NP}$  [BCSS98, AB09]. (Just as in the famous  $\mathbf{P}$  vs.  $\mathbf{NP}$  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 3.3 is also an open problem and its proof would be a major step toward solving the  $\mathbf{VP}$  vs.  $\mathbf{VNP}$  Problem — Valiant's algebraic circuit analogue of the  $\mathbf{P}$  vs.  $\mathbf{NP}$  Problem [Val79, Bür00, Koi11, BLMW11].

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

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  $f$  [GK96, 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  $\tau$ -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  $\tau$ -Conjecture expands its implications into arithmetic geometry, as we

---

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

already saw in Part (III) of Theorem 3.3. However, the truth of any global field analogue of the  $\tau$ -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]). However, no such example has contradicted the  $\tau$ -Conjecture so far. Constructing “small but mighty” polynomials over  $\mathbb{Q}_p$  is also possible, even over several such fields at once.

**Lemma 3.4.** [PR13] *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. ■*

Similar to the real case, no known  $p$ -adic examples contradict the Standard  $\tau$ -Conjecture either. Note that it is possible for a univariate polynomial to have roots in  $\mathbb{R}$ , and  $\mathbb{Q}_p$  for *all* primes  $p$ , but no roots in  $\mathbb{Q}$ :  $(x_1^2 - 2)(x_1^2 - 17)(x_1^2 - 34)$  [Kat07, Pg. 47, Ex. 46] is one of the simplest such examples.

So let us now formulate a potentially safer extension of the  $\tau$ -Conjecture to local fields, and apply it to a more restricted family of expressions: *sum-product-sum* (SPS) expressions.

**Definition 3.5.** (See [Koi11, Sec. 3].) *Let us define  $\text{SPS}(k, m, t, d, \delta)$  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  $\delta$  nonzero digits in their binary expansions.  $\diamond$

The family  $\text{SPS}(k, m, t, d, \delta)$  is motivated by circuit complexity, but has precursors coming from 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  $\text{SPS}(k, m, 2, 1, \delta)$ ,  $\text{SPS}(2, m, d + 1, d, \delta)$ , and  $\text{SPS}(k, 2, 2, 1, \delta)$ , independent of  $\delta$ .

**Adelic  $\tau$ -Conjecture.** [PR13] *For any  $k, m, t, d, \delta \in \mathbb{N}$  and  $f \in \text{SPS}(k, m, t, d, \delta)$ , there is a field  $L \in \{\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \dots\}$  such that  $f$  has no more than  $(kmt + \delta + \log d)^{O(1)}$  distinct roots in  $L$ .*

It is easily checked that  $\tau(f) = (kmt + \delta + \log d)^{O(1)}$  for any  $f \in \text{SPS}(k, m, t, d, \delta)$ . The Standard  $\tau$ -Conjecture then easily implies that we can always find a prime  $p$  such that the number of powers of  $p$  dividing an integer root of  $f$  is  $(kmt + \delta + \log d)^{O(1)}$  [Koi11, Sec. 3]. The latter statement, also implied by the Adelic  $\tau$ -Conjecture, already implies the complexity lower bound on the permanent stated in Part (I) of Theorem 3.3 [GKPR13]. In fact, even the truth of a looser  $2^{(kmt + \delta + \log d)^{O(1)}}$  upper bound would yield new, hitherto unprovable complexity lower bounds for the permanent [GKPR13].

The Adelic  $\tau$ -Conjecture thus allows us expand the real-analytic toolbox suggested by [Koi11, Sec. 6] and [KPT12]. In particular, the key issue now is to find a root count over  $\text{SPS}(k, m, t, d, \delta)$ , with *sub-exponential* dependence on  $t$ , over *some* local field.

#### 4. DISSEMINATION AND DEVELOPMENT OF PERSONNEL

Local co-PI Rojas co-supervised 4 postdocs (Avendaño, Hauenstein, Kadish, and Nisse, with Hauenstein and Kadish receiving funding from this grant) and directly supervised 2 graduate students (Philipson (née Hellenbrand) and Rusek, both receiving funding from this grant). Hauenstein has since gone on to a tenure-track position at NC State (Raleigh) and Kadish has gone on to work as a consultant for Ab Initio. Rusek will finish his Ph.D. degree during summer 2013 and Philipson is on track for completing her Ph.D. by 2015 or earlier.

Some of the presentations resulting from this work are the following:

- (1) \* “An application of quasi-inverse rings,” A&M Algebraic Geometry Seminar, November 2012. (Speaker was postdoc Harlan Kadish.)
- (2) \* “Gradient descent homotopies and real solving,” MAA Mathfest 2012, Madison, August 2012. (Speaker was postdoc Jon Hauenstein.)
- (3) “Arithmetic Approaches to  $\mathbf{P}$  vs.  $\mathbf{NP}$ ,” Microsoft Research (New England), Cambridge, Massachusetts, July 30, 2012.
- (4) “Arithmetic Approaches to  $\mathbf{P}$  vs.  $\mathbf{NP}$ ,” Meeting in honor of Alan Turing’s Centennial, day on model theory and circuits, École Normale Supérieure, Lyon, France, July 4, 2012.
- (5) \* “Real solutions to parameterized polynomial systems,” 2012 SIAM Annual Meeting, Minneapolis, July 2012. (Speaker was postdoc Jon Hauenstein.)
- (6) \* “Approaching the P v. NP problem via algebra and geometry,” MIT Lincoln Laboratories, June 2012. (Speaker was postdoc Harlan Kadish.)
- (7) “Solving a Real Analogue of Smale’s 17th Problem,” Workshop on Dynamics and Complexity in honor of Mike Shub, Fields Institute, University of Toronto, Canada, May 7, 2012.
- (8) \* “Software for numerical algebraic geometry,” Simons Foundation Roundtable on Software for Research, New York City, May 2012. (Speaker was postdoc Jon Hauenstein.)
- (9) “Fast Toric Algorithms Over Local Fields,” number theory seminar, UC Irvine, California, April 12, 2012.
- (10) \* “Polynomial Systems, Random Inputs, and Complexity,” Sandia National Laboratories, Livermore, CA, March 7, 2012. (Speaker was Ph.D. student Korben Rusek.)
- (11) \* “An application of quasi-inverse rings,” Special Session on the Mathematics of Computation, AMS-MAA Joint Mathematics Meeting, January 2012. (Speaker was postdoc Harlan Kadish.)
- (12) \* “Numerical solving of polynomial equations and applications, Mathematics Colloquium,” University of Wisconsin, December 2011. (Speaker was postdoc Jon Hauenstein.)
- (13) \* “Numerical solving of polynomial equations: from 3264 and 1442 to 83200 and 38475,” University of California, Berkeley, December 2011. (Speaker was postdoc Jon Hauenstein.)
- (14) “Petascale Polynomials and a Real Analogue of Smale’s 17th Problem,” Department of Energy Applied Mathematics Program meeting, Washington, D.C., October 17, 2011.
- (15) “Polyhedral Predictions for Polynomial Root Norms,” SIAM Conference on Applied Algebraic Geometry, special session on applications to celestial mechanics, Raleigh, North Carolina, October 8, 2011.

- (16) “Algorithmic Fewnomial Theory Over  $\mathbb{Q}_p$ ,” SIAM Conference on Applied Algebraic Geometry, special session on arithmetic aspects of numerical solving, Raleigh, North Carolina, October 7, 2011.
- (17) \* “On the Topology of p-adic Discriminant Amoebae,” SIAM Conference on Applied Algebraic Geometry, October 7, 2011. (Speaker was Ph.D. student Korben Rusek.)
- (18) “Fast Root Counting Over  $\mathbb{Q}_p$ ,” SIAM Conference on applied algebraic geometry, special session on arithmetic aspects of numerical solving, Raleigh, North Carolina, October 6, 2011.
- (19) “How Number Theory Makes Things Easier (and Harder),” Workshop on Mathematical Aspects of **P** vs. **NP** and its Variants, ICERM, Aug. 4, 2011.
- (20) “Fast Toric Algorithms Over Local Fields,” Toric Geometry and its Applications, Leuven, Belgium, June 9, 2011.

Rojas also helped co-organize the following related conferences and workshops:

- (I) Texas Algebraic Geometry Seminar, co-organized by J.M. Landsberg, J.M. Rojas, and F. Sottile, Texas A&M University, Feb. 28 – Mar. 1, 2012.
- (II) Workshop on Mathematical Aspects of **P** vs. **NP** and its Variants, co-organized by S. Basu, J.M. Landsberg, and J.M. Rojas, ICERM, Rhode Island, Aug. 1–5, 2011.
- (III) Special session on Arithmetic Aspects of Numerical Solving, at SIAM Conference on Applied Algebraic Geometry, Raleigh, North Carolina, Oct. 6–7, 2011.

Also, outreach and educational opportunities growing out of this work include the following:

- (a) Teaching middle school students at 3 weekend Math Circles (Feb. 25, May 5, 2012, and Feb. 16, 2013).
- (b) Giving an expository talk to applied mathematics undergraduates at Texas A&M (Nov. 16).
- (c) Leveraging the work of this project to teach two new summer REU courses (during the summers of 2011 and 2012) to a total of 10 undergraduate students from outside Texas A&M, 5 of whom were female. (The summer 2012 class also included 2 African American students and 2 Hispanic US citizen students.)

## REFERENCES

- [AB09] Arora, Sanjeev and Barak, Boaz, *Computational complexity. A modern approach*. Cambridge University Press, Cambridge, 2009.
- [AKNR13] Avendaño, Martín; Kogan, Roman; Nisse, Mounir; and Rojas, J. Maurice, “Metric Estimates for Archimedean Amoebae and Tropical Hypersurfaces,” submitted for publication.
- [AKS07] Avendaño, Martín; Krick, Teresa; and Sombra, Martin, “Factoring bivariate sparse (lacunary) polynomials,” *J. Complexity*, vol. 23 (2007), pp. 193–216.
- [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.
- [AIRR12] Avendaño, Martín; Ibrahim, Ashraf; Rojas, J. Maurice; and Rusek, Korben, “Faster p-adic Feasibility for Certain Multivariate Sparse Polynomials,” *Journal of Symbolic Computation*, special issue in honor of 60th birthday of Joachim von zur Gathen, vol. 47, no. 4, pp. 454–479 (April 2012).

- [AK11] Avendaño, Martín and Krick, Teresa, “Sharp Bounds for the Number of Roots of Univariate Fewnomials,” *Journal of Number Theory*, vol. 131 (1), pp. 1209–1228, 2011.
- [BS96] Bach, Eric and Shallit, Jeff, *Algorithmic Number Theory, Vol. I: Efficient Algorithms*, MIT Press, Cambridge, MA, 1996.
- [BR10] Baker, Matthew and Rumely, Robert, *Potential theory and dynamics on the Berkovich projective line*, “Mathematical Surveys and Monographs, 159, American Mathematical Society, Providence, RI, 2010.
- [BHPR11] Bastani, Osbert; Hillar, Chris; Popov, Dimitar; and Rojas, J. Maurice, “Randomization, Sums of Squares, Near-Circuits, and Faster Real Root Counting,” in *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.
- [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; Cheng, Qi; and Rojas, J. Maurice, “Sub-Linear Root Detection, and New Hardness Results, for Sparse Polynomials Over Finite Fields,” submitted for publication, 2012.
- [Bih07] Bihan, Frederic, “Polynomial systems supported on circuits and dessins d’enfants,” *J. London Math. Soc.* 75 (2007), no. 1, pp. 116–132.
- [BRS09] Bihan, Frederic; Rojas, J. Maurice; and Stella, Casey, “Faster Real Feasibility via Circuit Discriminants,” proceedings of 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*, vol. 7, no. 3, (July–September, 2007).
- [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.
- [CFKLLS00] Canetti, Ran; Friedlander, John B.; Konyagin, Sergei; Larsen, Michael; Lieman, Daniel; and Shparlinski, Igor E., “On the statistical properties of Diffie-Hellman distributions,” *Israel J. Math.* 120 (2000), pp. 23–46.
- [CZ81] Cantor, David G. and Zassenhaus, Hans, “A new algorithm for factoring polynomials over finite fields,” *Math. Comp.* 36 (1981), no. 154, pp. 587–592.
- [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*, 12:3–4, Sept. 2004, pp. 150–161.
- [CHW11] Cheng, Qi; Hill, Joshua E.; and Wan, Daqing, “Counting Value Sets: Algorithm and Complexity,” *Math ArXiv preprint 1111.1224*.
- [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.
- [Chr56] Christopher, John, “The Asymptotic Density of Some  $k$ -Dimensional Sets,” *the American Mathematical Monthly*, vol. 63, no. 6 (Jun.–Jul., 1956), pp. 399–401.
- [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.
- [DRRS07] Dickenstein, Alicia; Rojas, J. Maurice; Rusek, Korben; Shih, Justin, “Extremal Real Algebraic Geometry and  $\mathcal{A}$ -Discriminants,” *Moscow Mathematical Journal*, vol. 7, no. 3, July–September 2007, pp. 425–452.

- [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.
- [EP05] Emiris, Ioannis Z. and Pan, Victor, “*Improved algorithms for computing determinants and resultants*,” J. Complexity (FOCM 2002 special issue), Vol. 21, no. 1, February 2005, pp. 43–71.
- [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.
- [GJ79] Garey, Michael R. and Johnson, David S. *Computers and Intractability: A Guide to the Theory of NP-Completeness*, A Series of Books in the Mathematical Sciences, W. H. Freeman and Co., San Francisco, Calif., 1979, x+338 pp.
- [vzGat06] von zur Gathen, Joachim, “*Who was who in polynomial factorization*,” Proceedings of ISSAC 2006 (B. M. Trager, ed.), pp. 2–3, ACM Press, 2006.
- [vzGKS96] von zur Gathen, Joachim; Karpinski, Marek; and Shparlinski, Igor E., “*Counting curves and their projections*,” Computational Complexity 6, no. 1 (1996/1997), pp. 64–99.
- [vzGP01] von zur Gathen, Joachim and Panario, Daniel, “*Factoring polynomials over finite fields: A survey*,” J. Symb. Comput., 31(1/2):3–17, 2001.
- [GKZ94] Gel’fand, Israel Moseyevitch; Kapranov, Misha M.; and Zelevinsky, Andrei V.; *Discriminants, Resultants and Multidimensional Determinants*, Birkhäuser, Boston, 1994.
- [GR10] Giesbrecht, Mark and Roche, Daniel, “*Interpolation of shifted-lacunary polynomials*,” Computational Complexity, vol. 19, no. 3, pp. 333–354, 2010.
- [GKPR13] Grenet, Bruno; Koiran, Pascal; Portier, Natacha; and Rojas, J. Maurice, “*An Unreal Approach to Circuit Complexity*” in progress, 2013.
- [GK96] Grigoriev, Dima and Karpinski, Marek, “*Computability of the Additive Complexity of Algebraic Circuits with Root Extracting*,” Theoretical Computer Science, vol. 157, no. 1, April 1996.
- [GPRT11] *Randomization, Relaxation, and Complexity*, (edited by Leonid Gurvits, Philippe Pébay, J. Maurice Rojas, and David C. Thompson), selected papers from a 5-day BIRS workshop on Randomization, Relaxation, and Complexity (co-organized by L. Gurvits, J. M. Rojas, and P. Parrilo), Contemporary Mathematics, vol. 556, American Mathematical Society, 2011.
- [Hab48] Habicht, Walter, “*Eine Verallgemeinerung des Sturmschen Wurzelzhlverfahrens*,” Comment. Math. Helv. **21** (1948), pp. 99–116.
- [Has24] Hasse, H., “*Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper*,” J. Reine Angew. Math. 153 (1924), pp. 113–130.
- [Hau11] Hauenstein, Jon D., “*Numerically computing real points on algebraic sets*,” preprint, 2011.
- [IKW01] Impagliazzo, Russell; Kabanets, Valentine; and Wigderson, Avi, “*In Search of an Easy Witness: Exponential Time vs. Probabilistic Polynomial Time*,” Journal of Computer and System Sciences, 65(4), pp. 672–694, 2002.
- [IP01] Impagliazzo, Russell and Paturi, Ramamohan, “*The Complexity of k-SAT*,” Journal of Computer and System Sciences, Volume 62, Issue 2, March 2001, pp. 367–375.
- [IMS09] Itenberg, Ilia; Mikhalkin, Grigory; and Shustin, Eugenii, *Tropical algebraic geometry*, Second edition, Oberwolfach Seminars, 35, Birkhäuser Verlag, Basel, 2009.
- [KL12] Kadish, Harlan and Landsberg, J.M., “*Padded polynomials, their cousins, and geometric complexity theory*,” submitted to Communications in Algebra, 2012.
- [Kal03] Kaloshin, V., “*The existential Hilbert 16-th problem and an estimate for cyclicity of elementary polycycles*,” Invent. Math. 151 (2003), no. 3, pp. 451–512.
- [Kal03] Kaltofen, Erich, “*Polynomial factorization: a success story*,” In ISSAC 2003 Proc. 2003 Internat. Symp. Symbolic Algebraic Comput. (New York, N.Y., 2003), J. R. Sendra, Ed., ACM Press, pp. 3–4.
- [KK05] Kaltofen, Erich and Koiran, Pascal, “*On the complexity of factoring bivariate supersparse (lacunary) polynomials*,” ISSAC05, Proceedings of 2005 International Symposium Symbolic Algebraic Computation, ACM Press, New York, 2005.
- [KS98] Kaltofen, Erich and Shoup, Victor, “*Subquadratic-time factoring of polynomials over finite fields*,” Math. Comp. 67 (1998), no. 223, pp. 1179–1197.



- [KaShp99] Karpinski, Marek and Shparlinski, Igor E., “On the computational hardness of testing square-freeness of sparse polynomials,” Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999), pp. 492–497, Lecture Notes in Comput. Sci., 1719, Springer, Berlin, 1999.
- [Kat07] Katok, Svetlana, *p-adic Analysis Compared with Real*, Student Mathematical Library, vol. 37, American Mathematical Society, 2007.
- [KU11] Kedlaya, Kiran and Umans, C., “Fast polynomial factorization and modular composition,” SIAM Journal on Computing, Vol. 40, No. 6, pp. 1767–1802, 2011.
- [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.
- [KiSha99] Kipnis, Aviad and Shamir, Adi, “Cryptanalysis of the HFE public key cryptosystem by relinearization,” Advances in cryptology — CRYPTO ’99 (Santa Barbara, CA), pp. 19–30, Lecture Notes in Comput. Sci. 1666, Springer, Berlin, 1999.
- [Koi11] Koiran, Pascal, *personal e-mail communication*, March, 2011.
- [KPT12] Koiran, Pascal; Portier, Natacha; and Tavenas, Sébastien, “A Wronskian Approach to the Real  $\tau$ -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.
- [LLL82] Lenstra, Arjen K.; Lenstra, Hendrik W., Jr.; Lovász, L., “Factoring polynomials with rational coefficients,” Math. Ann. 261 (1982), no. 4, pp. 515–534.
- [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.
- [LS09] *Tropical and Idempotent Mathematics*, International Workshop TROPICAL-07 (Tropical and Idempotent Mathematics, Aug. 25–30, 2007, Independent University, edited by G. L. Litvinov and S. N. Sergeev), Contemporary Mathematics, vol. 495, AMS Press, 2009.
- [MS12] Maclagan, Diane and Sturmfels, Bernd, *Introduction to Tropical Geometry*, in progress.
- [MW99] Maller, Michael and Whitehead, Jennifer, “Efficient p-adic cell decomposition for univariate polynomials,” J. Complexity 15 (1999), pp. 513–525.
- [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.
- [Mes06] Meshulam, Roy, “An uncertainty inequality for finite abelian groups,” European J. of Combinatorics, 27 (2006), pp. 63–67.
- [Mik05] Mikhalkin, Grigory, “Enumerative Tropical Algebraic Geometry in  $\mathbb{R}^2$ ,” Journal of the American Mathematical Society, Vol. 18, No. 2, pp. 313–377, 2005.
- [Mor97] T. de Araujo Moreira, Gustavo, “On asymptotic estimates for arithmetic cost functions,” Proceedings of the American Mathematical Society, Vol. 125, no. 2, Feb. 1997, pp. 347–353.
- [Nes03] Nesterenko, Yuri, “Linear forms in logarithms of rational numbers,” Diophantine approximation (Cetraro, 2000), pp. 53–106, Lecture Notes in Math., 1819, Springer, Berlin, 2003.
- [New76] Newton, Isaac, *letter to Oldenburg dated 1676 Oct 24*, the correspondence of Isaac Newton, II, pp. 126–127, Cambridge University Press, 1960.
- [Ost40] Ostrowski, Alexandre, “Recherches sur la méthode de Graeffe et les zéros des polynomes et des séries de Laurent,” Acta Math. **72**, (1940), pp. 99–155.
- [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.

- [Par03] Parrilo, Pablo A., “*Semidefinite programming relaxations for semialgebraic problems*,” Algebraic and geometric methods in discrete optimization, Math. Program. 96 (2003), no. 2, Ser. B, pp. 293–320.
- [PRS11] Passare, Mikael; Rojas, J. Maurice; and Shapiro, Boris, “*New Multiplier Sequences via Discriminant Amoebae*,” Moscow Mathematical Journal, (special issue in memory of Vladimir Igorevich Arnold), vol. 11, no. 3, July–Sept. 2011, pp. 547–560.
- [PRT09] Pébay, Philippe; Rojas, J. Maurice; 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.
- [PRT11] Pébay, Philippe P.; Rojas, J. Maurice; and Thompson, David C., “*Optimizing  $n$ -variate  $(n+k)$ -nomials for small  $k$* ,” Theoretical Computer Science, Symbolic-Numeric Computation 2009 special issue, Vol. 412, No. 16, 1 April 2011.
- [PR04] Passare, Mikael and Rullgård, “*Amoebas, Monge-Ampère measures, and triangulations of the Newton polytope*,” Duke Math. J., Vol. 121, No. 3 (2004), pp. 481–507.
- [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.
- [PR13] Phillipson, Kaitlyn and Rojas, J. Maurice, “*Fewnomial Systems with Many Roots, and an Adelic Tau Conjecture*,” in proceedings of Bellairs workshop on tropical and non-Archimedean geometry (May 6–13, 2011, Barbados), CRM Monograph Series, AMS Press, to appear. Preliminary version available as Math ArXiv preprint 1011.4128 .
- [Poo98] Poonen, Bjorn, “*Zeros of sparse polynomials over local fields of characteristic  $p$* ,” Math. Res. Lett. 5(3), pp. 273–279, 1998.
- [Pur08] Purbhoo, Kevin, “*A Nullstellensatz for amoebas*,” Duke Mathematical Journal, 141 (2008), no. 3, pp. 407–445.
- [RS02] Rahman, Q. I. and Schmeisser, G., *Analytic Theory of Polynomials*, London Mathematical Society Monographs 26, Oxford Science Publications, 2002.
- [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] Rojas, J. Maurice, “*Additive Complexity and the Roots of Polynomials Over Number Fields and  $p$ -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.
- [Roj03] \_\_\_\_\_, “*Why Polyhedra Matter in Non-Linear Equation Solving*,” paper corresponding to an invited talk delivered at a conference on 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.
- [RY05] Rojas, J. Maurice and Ye, Yinyu, “*On solving sparse polynomials in logarithmic time*,” Journal of Complexity, special issue for the 2002 Foundations of Computation Mathematics (FOCM) meeting, February 2005, pp. 87–110.
- [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.
- [Ser73] Serre, Jean-Pierre, “*A course in arithmetic*,” Graduate Texts in Mathematics, No. 7, Springer-Verlag, New York-Heidelberg, 1973.
- [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.
- [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).
- [Tao05] Tao, Terence, “*An Uncertainty Principle for Cyclic Groups of Prime Order*,” Math. Res. Lett. 12 (1) (2005), pp. 121–127.
- [The02] Theobald, Thorsten, “*Computing Amoebas*,” Experiment. Math. Volume 11, Issue 4 (2002), pp. 513–526.
- [TdW13] Theobald, Thorsten and De Wolff, Timo, “*Amoebas of Genus at Most One*,” Advanced in Mathematics, to appear.
- [Uma08] Umans, Christopher, “*Fast polynomial factorization and modular composition in small characteristic*,” STOC’08, pp. 481–490, ACM, New York, 2008.
- [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.
- [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, A. J., “*A theorem of the complement and some new o-minimal structures*,” Selecta Math. (N.S.) 5 (1999), no. 4, pp. 397–421.