QUANTITATIVE ASPECTS OF SUMS OF SQUARES AND SPARSE POLYNOMIAL SYSTEMS

A Dissertation

by

KAITLYN ROSE PHILLIPSON

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	J. Maurice Rojas
Committee Members,	Laura Matusevich
	Peter Stiller
	Daniele Mortari
Head of Department,	Emil Straube

August 2016

Major Subject: Mathematics

ABSTRACT

Computational algebraic geometry is the study of roots of polynomials and polynomial systems. We are familiar with the notion of degree, but there are other ways to consider a polynomial: How many variables does it have? How many terms does it have? Considering the sparsity of a polynomial means we pay special attention to the number of terms. One can sometimes profit greatly by making use of sparsity when doing computations by utilizing tools from linear programming and integer matrix factorization. This thesis investigates several problems from the point of view of sparsity. Consider a system F of n polynomials over 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 give a complete classification for when an n-variate $n+2$-nomial positive polynomial can be written as a sum of squares of polynomials. Finally, we investigate the problem of approximating roots of polynomials from the viewpoint of sparsity by developing a method of approximating roots for binomial systems that runs more efficiently than other current methods. These results serve as building blocks for proving results for less sparse polynomial systems.

DEDICATION

This work is dedicated to Regina T. Maier and Evelyn C. Hellenbrand, two women who taught me to face the unknown with courage and the satisfaction of a hard day's work.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURE Page

1. INTRODUCTION AND LITERATURE REVIEW

1.1 Introduction

Polynomial equations can be analyzed in many ways. We are familiar with the notion of degree, but there are other ways to consider a polynomial: How many variables does it have? How many terms does it have? Does this affect the solution set?

For example, the univariate polynomial $p(x) = c_0 + c_1x + \cdots + c_{d-1}x^{d-1} + c_dx^d$ with $c_i \in \mathbb{R}$ and $c_d \neq 0$ has exactly d complex roots (counting multiplicities) by the Fundamental Theorem of Algebra. However, what if we assume that some of the coefficients c_i are 0? Consider the polynomial $q(x) = b_1x^{a_1} + b_2x^{a_2} + \cdots + b_tx^{a_t}$ with $a_1 < \cdots < a_t = d$ and $0 \neq b_i \in \mathbb{R}$ for all i. Again, we know that q has d complex roots (counting multiplicities), but we can also use Descartes' Rule of Signs to bound the number of real roots: q has at most $2t-1$ real roots.

The function q is an example of a *sparse* polynomial: Utilizing sparsity means we pay special attention to the number of terms. One can sometimes profit greatly by making use of sparsity when doing computations with polynomials. Sparsity also applies to multi-variate polynomials as well and leads us to some beautiful open problems. This thesis investigates several problems from the point of view of sparsity, using the geometric structure of the exponent set of the polynomials.

The remainder of the dissertation is organized as follows: Section 1 will discuss the relevant background and history to the thesis questions as well as some tools necessary to solve them. Section 2 will discuss bounding the number of roots of an $n \times n$ system with $n+2$ distinct exponent vectors over any local field L. Section 3 gives a complete classification to whether or not a positive n variate $n+2$-nomial can be written as a sum of squares. Section 4 gives a method of quickly approximating roots of certain sparse polynomial systems. Section 5 will summarize the results and discuss some open problems related to these problems.

1.2 Univariate Polynomials

One of the beginning cases to consider for polynomials is single variable polynomial equations. One of the most well-known classical results concerning polynomials is the Fundamental Theorem of Algebra:

Theorem 1.1 (Fundamental Theorem of Algebra)**.** *Let p be the polynomial $p(x) = c_0 + c_1x + \cdots + c_{d-1}x^{d-1} + c_dx^d$, with $c_i \in \mathbb{C}$ for all i and $c_d \neq 0$. The equation $p(x) = 0$ has exactly d solutions counting multiplicities.*

However, this does not tell us exactly how many roots there are or what form they take: How many are real? rational? positive? A result that partially answers these questions is Descartes' Rule of signs:

Theorem 1.2 (Descartes' Rule of Signs)**.** *Let q the polynomial $q(x) = b_1x^{a_1} + b_2x^{a_2} + \cdots + b_tx^{a_t}$, with $a_1 < \cdots < a_t = d$ and $0 \neq b_i \in \mathbb{R}$ for all i. Let $S =$ the number of sign changes of the sequence $(b_1, b_2, \ldots, b_t)$. Then the number of positive solutions (counting multiplicities) of $q(x) = 0$ is either equal to S, or equal to $S \mod 2$. In particular, the number of positive roots of $q(x)$ is at most $t - 1$.*

By replacing $q(x)$ by $q(-x)$, we see that Descartes' Rule of Signs also gives us an upper bound on the number of real roots of q: it has at most $2t - 1$ real roots (0 may also be a root).

Descartes' Rule of Signs is an example of a result that employs *sparsity*: considering the number of terms of the polynomial, or, more generally, the structure of a polynomial system. This can be useful particularly in real world applications, as we see from Descartes' Rule that real or positive solutions may be connected to the number of terms. We will explore this notion further in Section 2. To generalize the notion of sparsity to multi-variate polynomials, we must introduce some geometric notions.

1.3 Newton Polytopes and Mixed Volume

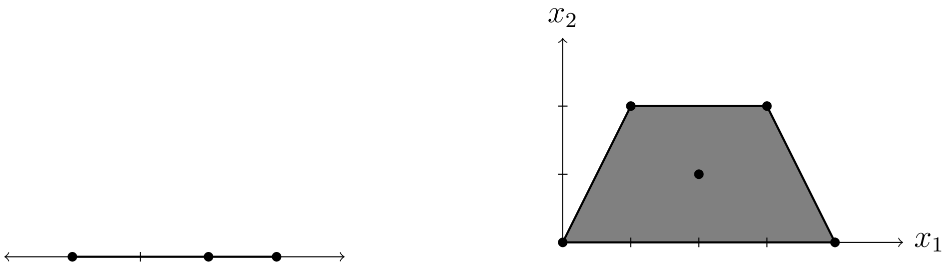
Let K be a field, and $K^* := K \setminus \{0\}$. When considering sparsity, we express a polynomial $f \in K[x_1, \ldots, x_n]$ as $f(x) = \sum_{i=1}^{t} c_i x^{a_i}$, with $c_i \in K^*$, $x = (x_1, \ldots, x_n)$, $a_i \in \mathbb{Z}^n$ are distinct, and if $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$, then $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. We define the *support* of f to be the exponent set $\{a_1, \ldots, a_t\}$ (this set is commonly denoted with the letter $\mathcal{A}$). A geometric object studied in the context of sparsity is the Newton Polytope of a polynomial.

Definition 1.3. Let $f(x) = \sum_{i=1}^{t} c_i x^{a_i}$ as before. We define the *Newton Polytope* of f to be the convex hull of its support:

$$\mathrm{Newt}(f) = \mathrm{Conv}\{a_1, \ldots, a_t\} \subset \mathbb{R}^n.$$

Some examples of Newton Polytopes are given in Figure 1.1. Note that the Newton Polytope only contains information about the exponents of the polynomial. We can also build geometric objects that include information about the coefficients of the polynomial, which will be defined in Section 2. We can see fairly easily through several examples that the geometric structure of the Newton Polytope is intimately related to the overall structure of the polynomial.

Example 1.4. Consider the polynomial $f(x_1, x_2) = 4 - 3x_1x_2 + 20x_1^4x_2^4$. Note that while the Newton Polytope sits in $\mathbb{R}^2$ (see Figure 1.2), its affine dimension is 1; it just a line segment. $f(x_1, x_2)$ is a univariate polynomial in disguise: by the substitution



(a) $\mathrm{Newt}(-5+2x_1^2+10x_1^3)$

(b) $\mathrm{Newt}(7+x_1x_2^2-2x_1^2x_2+5x_1^3x_2^2+8x_1^4)$

Figure 1.1: Examples of Newton Polytopes

$x_1x_2 = y_1$, we get the equivalent polynomial $g(y_1) = 4 - 3y_1 + 20y_1^4$.

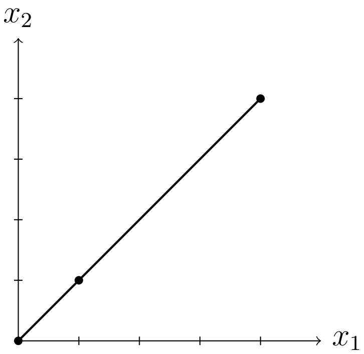


Figure 1.2: $\mathrm{Newt}(f)$

Example 1.5. Consider a polynomial $f(x) := \sum_{a\in\mathcal{A}} c_a x^a$, with $c_a \neq 0, c_a \in \mathbb{R}$. Suppose $f(x)$ is *positive semi-definite*: for all $x \in \mathbb{R}^n$, $f(x) \geq 0$. If $\alpha \in \mathcal{A}$ is a vertex of $\mathrm{Newt}(f)$, then one can show that $\alpha \in (2\mathbb{Z})^n$ and $c_\alpha > 0$:

If α is a vertex of $\mathrm{Newt}(f)$, then there exists $v = (v_1, v_2, \ldots, v_n) \in \mathbb{R}^n$ such that $v \cdot \alpha > v \cdot a$ for all $a \in \mathcal{A}$. Consider the following curve:

$$(x_1, \ldots, x_n) = (z_1 t^{v_1}, z_2 t^{v_2}, \ldots, z_n t^{v_n}), t \in \mathbb{R}, z \in \mathbb{R}^n.$$

Then

$$
\begin{aligned}
F(t) = f(z_1 t^{v_1}, z_2 t^{v_2}, \ldots, z_n t^{v_n}) &= \sum_{a \in \mathcal{A}} c_a z^a t^{v \cdot a} \\
&= c_\alpha z^\alpha t^{v \cdot \alpha} + \text{lower order terms}
\end{aligned}
$$

Since $f(x) \geq 0$ for all x, $F(t) \geq 0$ for all t. As $t \to \infty$, the leading term dominates, so this implies $c_\alpha z^\alpha > 0$ for all $z \in \mathbb{R}^n$. By substituting $z = (1, 1, \ldots, 1)$, we see that $c_\alpha > 0$, and when $z_i = -1$, $z_j = 1$ for $j \neq i$, we see that $\alpha_i \in 2\mathbb{Z}$, so we have $\alpha \in (2\mathbb{Z})^n$.

One of the most well-known results concerning roots of sparse polynomial systems is Bernstein's Theorem, which will be given in Subsection 1.4. To present this result, we need to introduce the notion of mixed volume. A more complete treatment of this material may be found in [59], and will be explored further in Section 4.

Definition 1.6. Given two convex polytopes P and Q, the *Minkowski sum* of P and Q, $P + Q$, is the convex polytope $\{p + q : p \in P, q \in Q\}$.

An example of a Minkowski sum in $\mathbb{R}^2$ is given in Figure 1.3. The vertices of $P+Q$ are sums of vertices of P and Q. If f and g are two polynomials, it easy to check that $\text{Newt}(f \cdot g) = \text{Newt}(f) + \text{Newt}(g)$. When discussing multivariate polynomial systems, we wish to investigate the interaction of the variables in the polynomials.

Definition 1.7. Given n polytopes $Q_1, \ldots, Q_n$ in $\mathbb{R}^n$, their *mixed volume* $\mu(Q_1, \ldots, Q_n)$ equals the following alternating sum of ordinary Euclidean volumes:

$$\sum_{I \subset [n]} (-1)^{n-|I|} \operatorname{vol}\left(\sum_{j \in I} Q_j\right)$$

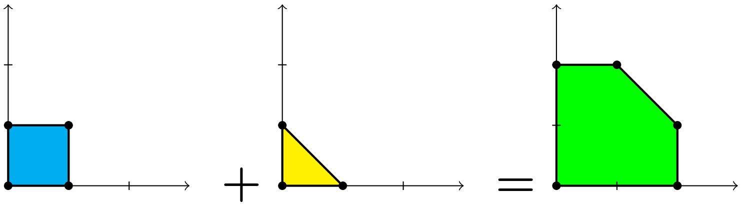


Figure 1.3: Minkowski sum of a square and a triangle

For the example from Figure 1.3, the mixed volume would be

$$(-1)^{2-1}(1) + (-1)^{2-1}(1/2) + (-1)^{2-2}(3 + 1/2) = 2.$$

Another method of computing the mixed volume is by constructing a *lifting* of the polytopes. Let $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_n$ be a collection of supports of polynomials, $\mathcal{A}_i \subset \mathbb{Z}^n$. Let $Q_i := \operatorname{Conv} \mathcal{A}_i$. Note that $Q_i \in \mathbb{R}^n$. For each i, create a lifting function l_i by choosing a random[1] value $l_i(a)$ for each $a \in \mathcal{A}_i$. Consider the polytope

$$\bar{Q}_i := \operatorname{Conv}\{a, l_i(a) : a \in \mathcal{A}_i\}.$$

Note that $\bar{Q}_i \subset \mathbb{R}^{n+1}$. Now compute the lower convex hull L of the Minkowski sum $\bar{Q}_1 + \cdots + \bar{Q}_n$. The facets of L are of the form $\bar{F}_1 + \cdots + \bar{F}_n$, where $\bar{F}_i$ is a face of the corresponding $\bar{Q}_i$ and $\sum_{i=1}^{n} \dim(\bar{F}_i) = n$. We say a facet is *mixed* if $\dim(\bar{F}_i) = 1$ for all i. By projecting the lower hull to $\mathbb{R}^n$, we get a subdivision of the Minkowski sum $Q_1 + \cdots + Q_n$.

Theorem 1.8 (Theorem 1.3.5 [59])**.** *The mixed volume $\mu(Q_1, \dots, Q_n)$ is equal to the sum of the volume of the mixed facets under the previous construction.*

[1] More precisely, we simply need the vector of values of $(l_1, \dots, l_n)$ to lie outside a finite union of hyperplanes $\mathcal{H}$, and $\mathcal{H}$ depends only on the supports $\mathcal{A}_1, \dots, \mathcal{A}_n$.

1.4 Results for Multivariate Polynomials

When discussing roots of multivariate polynomials, we are typically looking at $n \times n$ systems: n polynomials $f_1, \ldots, f_n$ with a total of n variables. A root is *non-degenerate* if the Jacobian matrix of the system at that point has full rank.

1.4.1 Bounds on total number of roots

Now that we have introduced the notion of Newton Polytope and mixed volumes, we can discuss some results on the number of roots of multivariate polynomials.

Theorem 1.9 (Bézout's Theorem [15]). *Let $f_1, f_2, \ldots, f_n$ be n polynomials in n variables, with $\deg f_i = d_i$. If the system $f_1 = \cdots f_n = 0$ has finitely many roots, the total number of roots in $\mathbb{C}^n$ is no more than $d_1 \cdots d_n$.*

For example, the system $x_1^{d_1} - 1 = x_2^{d_2} - 1 = \cdots = x_n^{d_n} - 1 = 0$ attains the upper bound of $d_1 \cdots d_n$ roots. Bézout's theorem does not, however, take into account the interactions of the terms between the equations. The main purpose of defining mixed volume in Subsection 1.3 is for the following result:

Theorem 1.10 (Bernstein's theorem [13]). *Given n subsets $\mathcal{A}_1, \ldots, \mathcal{A}_n$ of $\mathbb{Z}^n$, and $Q_i = \mathrm{Conv}(\mathcal{A}_i)$, consider the sparse polynomial system of equations*

$$\begin{gathered}\sum_{a \in \mathcal{A}_1} c_{1,a} x^a = 0 \\ \sum_{a \in \mathcal{A}_2} c_{2,a} x^a = 0 \\ \vdots \\ \sum_{a \in \mathcal{A}_n} c_{n,a} x^a = 0\end{gathered}$$

For almost all choices of coefficients $(c_{i,a})_{i\in[n],a\in\mathcal{A}_i}$*, the number of roots of this system in* $(\mathbb{C}^*)^n$ *equals the mixed volume* $\mu(Q_1,\ldots,Q_d)$.

Example 1.11. [59] Consider the system

$$c_1x^3y^2 + c_2x + c_3y^2 + c_4 = 0$$
$$c_5xy^4 + c_6x^3 + c_7y = 0$$

Bézout's Theorem gives us a bound of 25 roots. By computing the mixed volume of the Newton Polytopes, Bernstein's Theorem gives us a bound on the number of non-zero roots, which is 18. It can be checked that, for generic coefficients, this is the true bound.

1.4.2 Bounds on number of positive roots

Efforts have been made to come up with a version of Descartes' Rule for multivariate polynomials. The first result was by Khovanskii:

Theorem 1.12 (Khovanskii's bound [45])**.** *Let* $f_1, f_2, \ldots, f_n$ *be* n *polynomials in* n *variables. Suppose that* $n+k+1$ *exponent vectors were used to form all the polynomials in the system* $F = \{f_1,\ldots,f_n\}$*. If* F *has finitely many non-degenerate zeros with all positive coordinates, then this number is no more than*

$$2^{\binom{n+k}{2}}(n+1)^{n+k}.$$

Note that, while this is exponential in $n+k$, this result does not depend on the degree of the f_i. Further efforts were made to find a tighter bound on the number of positive roots of a polynomial system, and while progress was made (see [20]), no sub-exponential bounds have been found. A seemingly reasonable conjecture attributed to Kushnirenko was proposed:

Conjecture 1.13 (Kushnirenko's conjecture)**.** *Let $f_1, f_2, \ldots, f_n$ be n polynomials in n variables. Let m_i = number of terms of f_i, then the number of non-degenerate isolated positive roots of this system is at most*

$$(m_1 - 1)(m_2 - 1)\cdots(m_n - 1).$$

In 2002, Bertrand Haas [39] came up with the first counterexample to Kushnirenko's conjecture. He was able to build a family of bivariate, 2 polynomial systems, with each polynomial having 3 terms, with exactly 5 positive roots, which is more than the proposed $(3-1)\cdot(3-1) = 4$. The smallest such system had degree 106. It was asked whether this is the smallest degree possible in order to break the conjecture. In 2007, Rusek and Shih [31] found a 2×2 system, each with 3 terms, of degree 6 with 5 positive roots. The method for finding such a system involved an important mathematical object called the $\mathcal{A}$-*discriminant* of a polynomial, which will be discussed in Subsection 1.5. General results for a sub-exponential bound are unknown; however, in Section 2, we will discuss some new results giving sharp bounds for certain sparse systems.

1.5 $\mathcal{A}$-Discriminant

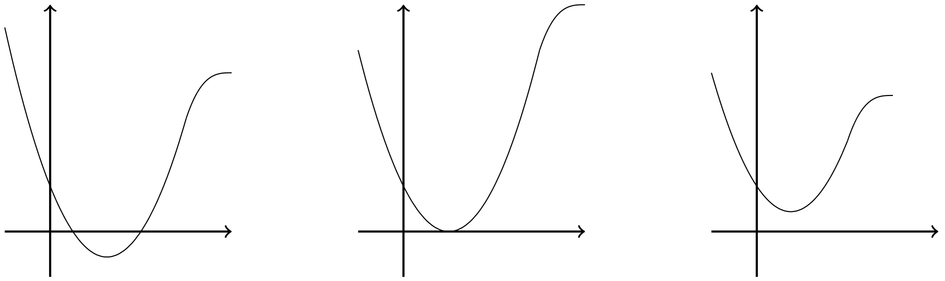
One of the most powerful tools underlying results in sparsity is the $\mathcal{A}$-discriminant. We will begin with a motivating example.

Example 1.14. Consider the univariate polynomial $f(x) = ax^2 + bx + c$. A well-known notion is the *discriminant* of f: $b^2 - 4ac$. We know from the quadratic formula that determining the sign of the discriminant will give us the number of real roots for f: $b^2 - 4ac > 0$ gives us 2 real roots, $b^2 - 4ac = 0$ gives us 1 real root (which is degenerate), and $b^2 - 4ac < 0$ gives us 0 real roots.

These results can be generalized further to any univariate trinomial:

Example 1.15. Consider the polynomial $f(x) = x^D - cx^d + 1, D > d > 0, c > 0$. Note that by Descartes' Rule of signs, this will have 0, 1, or 2 positive roots.

What happens to the graph of $f(x)$ as c varies? In Figure 1.4, we see that the number of positive zeros of f will change as c decreases. When c is sufficiently large, the graph will dip below the x-axis, resulting in 2 positive roots. As c decreases, at some point, it will touch the x-axis resulting in 1 (degenerate) root. We will denote by γ the c-value where this occurs. For $c < \gamma$, the graph will be above the x-axis, resulting in 0 positive roots. Thus, if we want to determine how many positive roots a f will have, we can find the value of γ.



(a) $c > \gamma$ (b) $c = \gamma$ (c) $c < \gamma$

Figure 1.4: Graph of $x^D - cx^d + 1$ as c varies

For f to have a degenerate roots ζ, the system of equations $f(\zeta) = f'(\zeta) = 0$ must be satisfied. Since f has constant term 1, $\zeta \neq 0$, so we can consider the system $f(\zeta) = \zeta f'(\zeta) = 0$ instead. We can represent this as:

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & d & D \end{bmatrix} \begin{bmatrix} 1 \\ -c\zeta^d \\ \zeta^D \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Note that $(1, -c\zeta^d, \zeta^D)^T$ is a vector in the nullspace of $\begin{bmatrix} 1 & 1 & 1 \\ 0 & d & D \end{bmatrix}$. It is easy to compute that the nullspace of this matrix is 1-dimensional, and another vector in its span is $(D-d, -D, d)^T$. Thus, $(1, -c\zeta^d, \zeta^D)$ is a scalar multiple of $(D-d, -D, d)^T$.

Via a clever rearrangement, we get the following relationship:

$$\left(\frac{1}{D-d}\right)^{D-d} \left(\frac{-c}{D}\right)^{-D} \left(\frac{1}{d}\right)^{d} = 1$$

Which we can rewrite as

$$\Delta_{\{0,d,D\}}(c) = \left(\frac{1}{D-d}\right)^{D-d} \left(\frac{-c}{D}\right)^{-D} \left(\frac{1}{d}\right)^{d} - 1 = 0.$$

Solving $\Delta_{\{0,d,D\}}(c) = 0$ gives us γ.

$\Delta_{\{0,d,D\}}$ is called the $\mathcal{A}$-discriminant. The term comes from the common notation of using $\mathcal{A}$ to denote the support set of f. Note that the support $\mathcal{A}$ is fixed, while the coefficient is allowed to vary. More generally, we define the $\mathcal{A}$-discriminant as follows:

Definition 1.16. Let $\mathcal{A} = \{a_1, \ldots, a_t\} \subset \mathbb{Z}^n$ of cardinality t and $c_1, \ldots, c_t \in \mathbb{C}^*$, we define the $\mathcal{A}$-*discriminant variety* $\nabla_{\mathcal{A}} \subset \mathbb{P}_{\mathbb{C}}^{t-1}$ to be the closure of the following set:

$$\{[c_1 : \cdots : c_t] \in \mathbb{P}_{\mathbb{C}}^{t-1} : f(x) = \sum_{i=1}^{t} c_i x^{a_i} \text{ has a degenerate root in } \mathbb{C}^n\}.$$

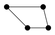
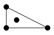
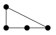
We then define the $\mathcal{A}$-*discriminant* to be the unique (up to sign) irreducible polynomial defining $\nabla_{\mathcal{A}}$.

Note that for Example 1.15, the $\mathcal{A}$-discriminant variety is the point γ where

$$\left(\frac{1}{D-d}\right)^{D-d}\left(\frac{-\gamma}{D}\right)^{-D}\left(\frac{1}{d}\right)^{d}=1.$$

Note that the $\mathcal{A}$-discriminant for the univariate trinomial is quite nice; it is just a binomial. In fact, this result generalizes to any support where $\mathcal{A}$ is a (non-degenerate) circuit:

Definition 1.17. We call $\mathcal{A} \subset \mathbb{R}^n$ a *(non-degenerate) circuit* iff $\mathcal{A}$ is affinely dependent, but every proper subset of $\mathcal{A}$ is affinely independent. Also, we say $\mathcal{A}$ is a *degenerate circuit* iff $\mathcal{A}$ contains a point a and a proper subset $\mathcal{B}$ such that $a \in \mathcal{B}$, $\mathcal{A} \setminus a$ is affinely independent, and $\mathcal{B}$ is a non-degenerate circuit.

For instance, in $n = 2$, both  and  are circuits, but  is a degenerate circuit. For any degenerate circuit $\mathcal{A}$, the subset $\mathcal{B}$ named above is always unique. In this restricted setting, there is a very compact description for $\nabla_{\mathcal{A}}$:

Lemma 1.18. *[Prop. 1.8, pg. 274 [37]] Suppose* $f = \sum_{i=1}^{n+2} c_i x^{a_i}$, $\mathcal{A} = \{a_1, a_2, \ldots, a_{n+2}\} \subset \mathbb{Z}^n$ *is a non-degenerate circuit. Let* $\hat{A}$ *denote the* $(n+1) \times (n+2)$ *matrix whose* $j^{\underline{th}}$ *column is the transpose of* $\{1\} \times a_j$*, i.e.*

$$\hat{A} := \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_{n+2} \end{bmatrix}.$$

Let $b = (b_1, \ldots, b_{n+1}, -1)^T$ *be a generator for the right nullspace of* $\hat{A}$*. Then:*

1. $\Delta(c_1, \ldots, c_{n+2})$ *is, up to a multiple by a nonzero monomial term,* $\prod_{i=1}^{n+2}\left(\frac{c_i}{b_i}\right)^{b_i} - 1$.

2. *For all* $[c_1 : \cdots : c_{n+2}] \in \mathbb{P}^{n+1}_{\mathbb{R}}$*, we have the equivalence* $\prod_{i=1}^{n+2} \left(\operatorname{sign}(b_i c_i) \frac{c_i}{b_i}\right)^{\operatorname{sign}(b_i c_i) b_i} = 1$ *for some* $[c_1 : \cdots : c_{n+2}] \in \mathbb{P}^{n+1}_{\mathbb{R}}$ *with* $\operatorname{sign}(c_1 b_1) = \cdots = \operatorname{sign}(c_{n+2} b_{n+2}) \Leftrightarrow Z_+(\sum_{i=1}^{n+2} c_i x^{a_i})$ *contains a degenerate point* ζ*. In particular,* $Z_+(f)$ *has at most one degenerate point.*

1.6 Factoring Integer Matrices

One of the ways to approach strongly sparse systems is to use a monomial change of variables to rewrite the system in a simpler form. Since the exponents of the system are integer-valued, we need a way to perform operations on the matrix of exponents while keeping the entries as integers.

Definition 1.19. Let $\mathbb{Z}^{n\times n}$ denote the set of $n \times n$ matrices with all entries integral, and let $\mathbb{GL}_n(\mathbb{Z})$ denote the set of all matrices in $\mathbb{Z}^{n\times n}$ with determinant ± 1 (the set of *unimodular* matrices). Recall that any $n \times n$ matrix $[u_{ij}]$ with $u_{ij} = 0$ for all $i > j$ is called *upper triangular.*

Given any $M \in \mathbb{Z}^{n\times n}$, we then call an identity of the form $UM = H$, with $H = [h_{ij}] \in \mathbb{Z}^{n\times n}$ in row echelon form and $U \in \mathbb{GL}_n(\mathbb{Z})$, a *Hermite factorization* of M. Also, if we have the following conditions in addition:

1. the left-most nonzero entry in any row of H is positive.

2. for any i, $h_{i,j}$ the left-most nonzero entry of row $i \implies 0 \leq h_{i',j} < h_{i,j}$ for all $i' < i$.

then we call H *the Hermite normal form* of M.

Also, given any identity of the form $UMV = S$ with $U, V \in \mathbb{GL}_n(\mathbb{Z})$ and S diagonal a *Smith factorization.* In particular, if $S = [s_{i,j}]$ and we require additionally that $s_{i,i} \geq 0$ and $s_{i,i} | s_{i+1,i+1}$ for all $i \in \{1, \ldots, n\}$ (setting $s_{n+1,n+1} := 0$), then S is uniquely determined and is called *the Smith normal form* of M.

Finally, we call any map defined by $x \mapsto x^A$ a *monomial change of variables.*

Note that if $S = \text{diag}(s_1, \ldots, s_n)$ is the Smith Factorization of A, then $|\det(A)| = |\det(S)|$. Moreover, $\max s_i \leq |\det(A)| \leq (\max_{i,j} |a_{ij}|)^n n^{n/2}$ (by Hadamard's inequality).

Proposition 1.20. *We have that $x^{AB} = (x^A)^B$ for any $A, B \in \mathbb{Z}^{n\times n}$. Also, for any field K, the map defined by $m_U(x) = x^U$, for any unimodular matrix $U \in \mathbb{Z}^{n\times n}$, is an automorphism of $(K^*)^n$. Finally, for any column vector $v \in \mathbb{Z}^n$, the smallest valuation of an entry of Uv is k if and only if the smallest valuation of an entry of v is k.*

Theorem 1.21. *[86, Ch. 8, pg. 137] For any $A = [a_{i,j}] \in \mathbb{Z}^{n\times n}$, the Hermite and Smith factorizations of A can be computed within $O\big(n^{3.376}\log^2(n \max_{i,j} |a_{i,j}|)\big)$ bit operations. Furthermore, given a Smith Factorization of A of the form $UMV = S$ with $U, V \in \mathbb{GL}_n(\mathbb{Z})$ and S diagonal, then we have the following bounds for the entries of U and V:*

For V: $\max_{i,j} |v_{ij}| \leq n^{n+1}(|a_{i,j}|)^{2n}$

For U: $\max_{i,j} |u_{ij}| \leq n^{2n+5}(\sqrt{n}\max_{i,j} |a_{i,j}|)^{4n} \max_{i,j} |a_{i,j}|$.

The Hermite and Smith factorization of matrices will be utilized in Sections 4, 3, and 4. Example 1.22 shows how the Smith form can be used to solve binomial systems. This is explored further in Section 4.

Example 1.22. Consider the bivariate binomial system:

$$\begin{cases} x_1^4 x_2^3 = 6 \\ x_1^3 x_2^2 = 2 \end{cases}$$

Then with $A = \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix}$ and $C = (6, 2)$, we can represent the system as $x^A = C$.

We have the following Smith factorization:

$$UAV = \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = S$$

So we can consider the equation $y^{UAV} = C^V$:

$$\begin{cases} y_1 = 6^0 \cdot 2^1 = 2 \\ y_2 = 6^1 \cdot 2^{-1} = 3 \end{cases}$$

Then clearly $(y_1, y_1) = (2, 3)$ is a solution for this system[2].

Now to recover the solutions to the original system, we take $y^U = x$:

$$(x_1, x_2) = (2^1 \cdot 3^{-2}, 2^{-1} \cdot 3^3) = (2/9, 27/2).$$

[2] In general, the Smith factorization will not lead to a linear system.

2. BOUNDING THE NUMBER OF ROOTS OF SPARSE POLYNOMIAL SYSTEMS

2.1 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 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 [43], the complexity of geometric algorithms [35, 90, 19, 64, 8, 7, 48, 49], model completeness for certain theories of real analytic functions [95, 76], and the study of torsion points on curves [28]. Fewnomial theory over number fields has applications to sharper uniform bounds on the number of torsion points on elliptic curves [27], integer factorization [58], additive complexity [71], and polynomial factorization and interpolation [42, 44, 6, 38, 26]. 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. However, for $n, k \geq 2$, *tight* bounds remain elusive [55, 73, 20, 3, 4].

The material in this section is reprinted with permission from "Fewnomial systems with many roots, and an adelic tau conjecture" by Kaitlyn Phillipson and J. Maurice Rojas, In *Proceedings of Bellairs workshop on tropical and non-Archimedean geometry, Contemporary Mathematics*, volume 605, pages 45-71, Copyright 2013 by Kaitlyn Phillipson and J. Maurice Rojas.

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 ρ of $\mathfrak{M}$ a *uniformizer* for L. Letting ord denote the corresponding valuation on L we then alternatively define the generalized phase as $\phi(y) := \frac{y}{\rho^{\text{ord } y}} \mod \mathfrak{M}$. 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.

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.[1] Our choices of uniformizer and angular direction above are in fact immaterial for the characteristic zero case: see Proposition 2.22 of Subsection 2.6, 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 [84, 94], 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 $p > 1 + k$.*

[1] See, e.g., Schikhof's notion of *sign group* in [75, Sec. 24, pp. 65–67].

Remark 1. The assertions above are immediate consequences of [84, pg. 160], [93, Cor. 2.1], [53, Example, pg. 286 & pp. 289–290], [5, Thm. 1.4, Ex. 1.5, & Thm. 1.6], and [66, Sec. 2]. Also, the polynomials $\prod_{i=1}^{k}(x_1 - i)$, $3x_1^{10} + x_1^2 - 4$, $x_1^{1+p^{p-1}} - (1 + p^{p-1})x_1 + p^{p-1}$, $\prod\limits_{z_1,\ldots,z_{k-1}\in\mathbb{F}_q}(x_1 - z_1 - z_2 t - \cdots - z_{k-1}t^{k-1})$, 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).

$Y_L(1,1)$ can in fact grow without bound if we let L range over arbitrary finite extensions of $\mathbb{Q}_p$.[2] 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 2.22 of Subsection 2.6).

2.2 Strongly Sparse Systems

As a warm-up, let us first unite the simplest multivariate case.

Proposition 2.3. *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$\}$.*

Proof. 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

[2] 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., [68, pp. 102–109]).

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. By Proposition 1.20 we know that $x^{AB}=(x^A)^B$ for any $n\times n$ matrix B.

Recall from Subsection 1.6 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. 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 2.2, we are done. □

Example 2.4. Consider the 3-nomial 2×2 system

$$\begin{aligned} x_1^4 - 2x_1^2x_2^2 - 8 &= 0 \\ 3x_1^2x_2^2 - 12 &= 0 \end{aligned}$$

By Gaussian Elimination, we can reduce this to the system to

$$\begin{aligned} x_1^4 &= 16 \\ x_1^2x_2^2 &= 4 \end{aligned}$$

Note that, for our matrix $A = \begin{bmatrix} 4 & 2 \\ 0 & 2 \end{bmatrix}$, the Smith Factorization is:

$$\begin{bmatrix} 0 & 1 \\ 1 & -3 \end{bmatrix} \cdot \begin{bmatrix} 4 & 2 \\ 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}$$

So via the change of variables $x = (x_1, x_2) = y^U = (y_2, y_1y_2^{-3})$, we can solve the equivalent system $y^D = c^V$:

$$\begin{aligned} y_1^2 &= 64 \\ y_2^4 &= 16 \end{aligned}$$

The positive solution for this system is $(y_1, y_2) = (8, 2)$, which gives us the positive solution for the original system: $(x_1, x_2) = (2, 8 \cdot 2^{-3}) = (2, 1)$.

Note that this approach no longer works for $(n+2)$-nomial $n \times n$ systems, as we can no longer separate the variables into individual polynomials. The lower bound $Y_{\mathbb{R}}(n, 2) \geq n+1$ was first proved through an ingenious application of Dessins d'Enfants

[17]. Explicit examples evincing $Y_{\mathbb{R}}(n,2)\geq n+1$ were previously known only for $n\leq 3$ [18].

Theorem 2.5. *For any $n \geq 2$, any local field L, and any $\varepsilon \in L^*$ with generalized phase 1 and* ord ε *sufficiently large, the roots in $\bar{L}^n$ of the $(n+2)$-nomial $n \times n$ system G_ε defined by*

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

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.

Our new extremal examples from Theorem 2.5 provide a new and arguably simpler proof that $Y_{\mathbb{R}}(n,2)\geq n+1$. 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 [18]. Non-trivial lower bounds, for $n\geq k-1\geq 2$, were unknown for the non-Archimedean case. We prove Theorem 2.5 in Subsection 2.4 for the Archimedean case and Subsection 2.5 for the Non-Archimedean case. Another important construction underlying Theorem 2.5 is a particular structured family of univariate polynomials.

Lemma 2.6. *For any $n\geq 2$, the degree $n+1$ polynomial R_n defined by*

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

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.

2.3 Triangulations and Mixed Volume

For less sparse systems, we can utilize the combinatorial structure of the supports of the polynomials to derive results on the number of roots. In Subsection 1.3, we gave the definition of mixed volume. We expand on this further.

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 [59].) 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 2. 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 $\ell(\mathcal{A})$.

Example 2.7. 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 (see Figure 2.1).

Definition 2.8. (See also [40].) 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 $(n+1)^{\underline{\mathrm{st}}}$ 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

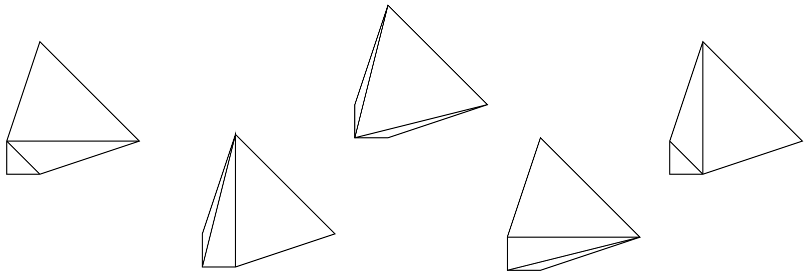


Figure 2.1: Triangulations of $\mathrm{supp}(f)$

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.

Example 2.9. Let us consider the family of systems G_ε from Theorem 2.5 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 Figure 2.2)

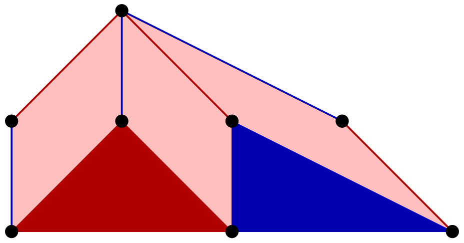


Figure 2.2: Mixed subdivision of supports of G_ε for $n=2$

The mixed cells of Σ_{ℓ_1,ℓ_2}, for this particular lifting, correspond to the lighter 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.

Definition 2.10. (See also [40, 33, 72] and Subsection 1.3.) 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 2.8.

As an example, the mixed volume of the two triangles from Example 2.9, relative to the stated (mixed) lifting, is the sum of the areas of the three parallelograms in the illustration, i.e., 3.

Theorem 2.11. *(See [33, Ch. IV, pg. 126] and [40].) The formula for $\mathcal{M}(Q_1, \ldots, Q_n)$ from Definition 2.10 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 $Q \subset \mathbb{R}^n$. □

Lemma 2.12. *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 $\mathrm{vol}\Big(\pi\Big(\hat{P}_j\Big)\Big) = 1$, 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, $\mathcal{M}\Big(\pi\Big(\hat{T}_1\Big),\ldots,\pi\Big(\hat{T}_n\Big)\Big) = n+1$ 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 $\hat{P}_j$.*

Proof. By Theorem 2.11 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 2.5. The vertices of Q form a *circuit*, and the signs of the entries of the vector b from the proof of Theorem 2.11 thereby encode an explicit triangulation of Q (see, e.g., [37, 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 $\big\{Q(2), Q(4), \ldots, Q\big(2\left\lfloor \frac{n+2}{2}\right\rfloor\big)\big\}$ (for n even) and $\big\{Q(3), Q(5), \ldots, Q\big(2\left\lceil \frac{n+2}{2}\right\rceil - 1\big)\big\}$ (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. $\square$

2.4 Archimedean Local Fields

If L is an Archimedean local field, then $L=\mathbb{R}$ or $\mathbb{C}$. 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 [45, 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. [45] 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 2.13. *For all $n,k\geq 1$, we have $Y_{\mathbb{C}}(n,k)=Y_{\mathbb{R}}(n,k)$.*

Proof. 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 $t \in [0, 2\pi)$. This shows the existence of a real $n \times n$ system F with at least N non-degenerate roots in $\mathbb{R}^n_+$, finishing the proof of the theorem. $\square$

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 2.14. 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.

Viro's Theorem (see, e.g., Proposition 5.2 and Theorem 5.6 of [37, Ch. 5, pp. 378–393] or [92]) 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* [87, Thm. 4] extends this to polynomial systems, and we will need just the $n \times n$ case.

Definition 2.15. 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 2.10, 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).

Example 2.16. Returning to Example 2.9, 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.

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 Subsection 1.3) 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 $(\Sigma_{\ell_1,\ldots,\ell_n}, s_1, \ldots, s_n)$.

2.4.1 Proof of the Archimedean case of Theorem 2.5

Let $\bar{L}$ be the algebraic closure of L. 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 2.6 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 2.12, combined with *Bernstein's Theorem* (over a general algebraically closed field [13, 29]), 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.

When $L = \mathbb{R}$ we immediately obtain, from Lemma 2.12 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.)

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 2.6. □

2.4.2 Proof of Lemma 2.6

Let us first define A_n and B_n respectively as $u(1+\varepsilon u)^2(1+\varepsilon^5 u)^2 \cdots (1+\varepsilon^{4\lfloor n/2 \rfloor - 3}u)^2$ and $(\varepsilon + u)^2(1+\varepsilon^3 u)^2(1+\varepsilon^7 u)^2 \cdots (1+$

$\varepsilon^{4\lceil n/2\rceil-5}u)^2$. Clearly, $R_n = A_n - B_n$.

Lemma 2.17. *Assume $\varepsilon = 1/4$. Then, for all $n \geq 2$, we have*

$$R_n\big(16^{n-2}/u\big) = \left(\frac{-4^{n-2}}{u}\right)^{n+1} R_n(u).$$

Also, for all even $n \geq 2$, we have $R_n(4^{n-2}) = 0$.

Lemma 2.18. *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 below.

Returning to the proof of Lemma 2.6, we now consider two exclusive cases.

Real Case: By Lemma 2.18, 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 2.17, 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 2.17, the new positive root 4^{n-2}. So R_n has $n + 1$ positive roots. □

2.4.3 Proof of Lemma 2.17

Recall that 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. □

2.4.4 Proof of Lemma 2.18

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:

$$\prod_{i=1}^{(n-1)/2} \left(1 - \frac{15/16}{1+256^{i-2}}\right) \quad \geq \quad \frac{7}{200}\left(1+\frac{1}{4^{n-1}}\right) \text{ for all odd } n \geq 3. \qquad (2.1)$$

Inequality (2.1) 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:

$$\left(\frac{1+4^{2n-8}}{1+4^{2n-10}}\right)\left(\frac{1+4^{2n-12}}{1+4^{2n-14}}\right)\cdots\left(\frac{1+4^{-2}}{1+4^{-4}}\right) = 16^{(n-1)/2} \prod_{i=1}^{(n-1)/2} \left(1 - \frac{15/16}{1+256^{i-2}}\right) (2.2)$$

Combining (2.1) and (2.2) 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

$$A_\ell\left(4^{2\ell-7}\right) \;>\; B_\ell\left(4^{2\ell-7}\right) \text{ for all odd } \ell \geq 3 \tag{2.3}$$

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 (2.3), 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 (2.1) 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.

2.5 Non-Archimedean Local Fields

A tool we will need is the *non-Archimedean Newton Polytope*, along with a recent refinement incorporating generalized phase.

Definition 2.19. 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.*

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. 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 2.20. *(Special case of [4, Thm. 3.10 & Prop. 4.4].) Suppose K is a complete non-Archimedean field with residue field $\mathcal{K}$ 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 $\theta\in(\mathcal{K}^*)^n$ 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 2.22 in Subsection 2.6), the total number of roots with $\mathrm{ord}\ \zeta=v$ is independent of ρ.

Example 2.21. 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 2.5). 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 2.12 then tells us that we obtain exactly 4 mixed cells (two views of which are shown in Figure 2.3), 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:

$$\begin{array}{c|c|c|c} x_1x_2-1 & x_1x_2-x_1^2 & x_1x_2-x_1^2 & x_1x_2-x_1^2 \\ x_2x_3-1 & x_2x_3-1 & x_2x_3-x_1^2 & x_2x_3-x_1^2 \\ x_3-1 & x_3-1 & x_3-1 & x_3-x_1^2 \end{array}$$

Each mixed cell has volume 1, and each corresponding binomial system has unique solution $(1,1,1)\in(\mathbb{F}_p^*)^3$. Theorem 2.20 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
$(p^{-2}(1+O(p)),p^{-2}(1+O(p)),p^{-1}(1+O(p)))$.

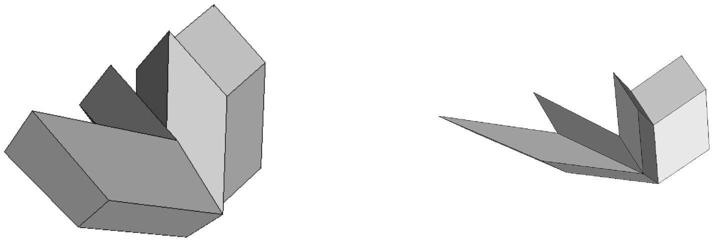


Figure 2.3: Liftings of G_p

2.5.1 Proof of the non-Archimedean case of Theorem 2.5

Due to Theorem 2.20, we can prove Theorem 2.5 two different ways:

Proof directly via construction of G_ε:

By Theorem 2.11 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 2.5. The vertices of Q form a *circuit*, and the signs of the entries of the vector b from the proof of Theorem 2.11 thereby encode an explicit triangulation of Q (see, e.g., [37, 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. □

Lemma 2.12 and Theorem 2.20 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 2.12, 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.

Proof via $R_n(u)$:

Via the same construction as the Archimedean case, $R_n(u) = u(1+\varepsilon u)^2(1+\varepsilon^5 u)^2 \cdots (1+\varepsilon^{4\lfloor n/2\rfloor-3}u)^2 - \varepsilon^2\left(1+\frac{u}{\varepsilon}\right)^2(1+\varepsilon^3 u)^2(1+\varepsilon^7 u)^2\cdots(1+\varepsilon^{4\lceil n/2\rceil-5}u)^2$ must vanish. Recall that $A_n := u(1+\varepsilon u)^2(1+\varepsilon^5 u)^2\cdots(1+\varepsilon^{4\lfloor n/2\rfloor-3}u)^2$ and $B_n := (\varepsilon+u)^2(1+\varepsilon^3 u)^2(1+\varepsilon^7 u)^2\cdots(1+\varepsilon^{4\lceil n/2\rceil-5}u)^2$. For $L\in\{\mathbb{Q}_p,\mathbb{F}_q((t))\}$ (and thus $\varepsilon\in\{p,t\}$ respectively), we easily obtain that $P := \operatorname{Newt}_L(A_n)$ has exactly $1+\lfloor n/2\rfloor$ lower edges, $Q := \operatorname{Newt}_L(B_n)$ has exactly $\lceil n/2\rceil$ lower edges, and the vertices of P and Q interlace. ($\operatorname{Newt}_L(R_4)$ is shown in Figure 2.4) More precisely, $\operatorname{Newt}_L(R_n)=\operatorname{Conv}(P\cup Q)$ has exactly $n+1$ lower edges, each having horizontal length 1. In particular, $\{(2,1),(0,1),\ldots,(2-2n,1)\}$ 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 $i\in\{2,0,\ldots,2-2n\}$, 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.

2.6 Invariance of $Y_L(n,k)$

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*

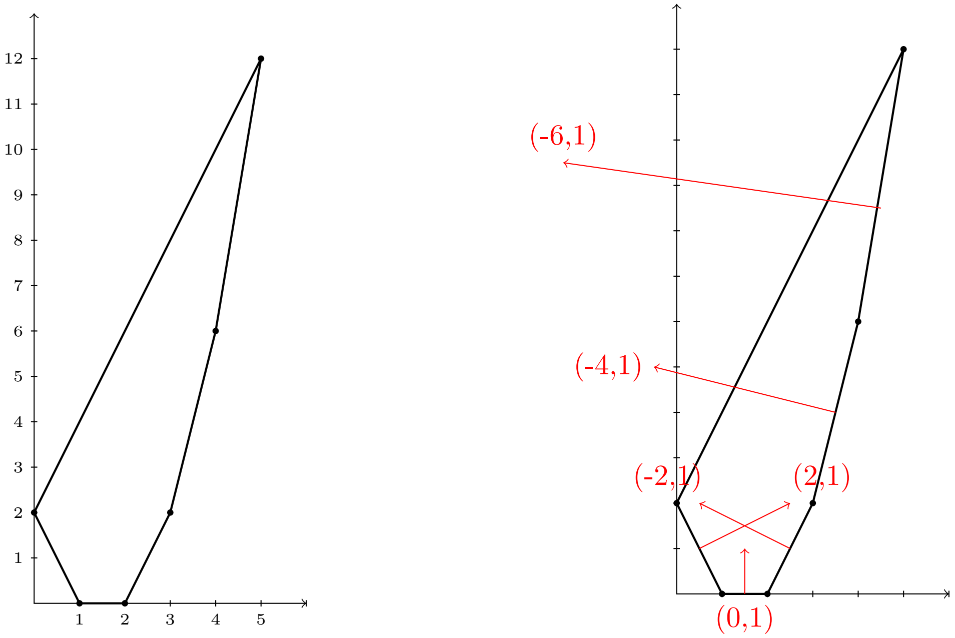


Figure 2.4: $\mathrm{Newt}_L(R_4(u))$ and inner normals

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

Proposition 2.22. *(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 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) $W_{\mathbb{C}}(n,k) = +\infty$, $W_{\mathbb{R}}(n,k) = 2^n Y_{\mathbb{R}}(n,k)$, 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 $W_{\mathbb{F}_q((t))}(n,k) \leq (q-1)^n Y_{\mathbb{F}_q((t))}(n,k) \leq (q-1)^n W_{\mathbb{F}_q((t))}(n,k)$.

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 Subsection 2.4.

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 $W_{\mathbb{R}}(n,k) \leq 2^n Y_{\mathbb{R}}(n,k)$, $W_L(n,k) \leq (q_L-1)^n Y_L(n,k)$, and $W_{\mathbb{F}_q((t))}(n,k) \leq (q-1)^n Y_{\mathbb{F}_q((t))}(n,k)$. 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 $W_{\mathbb{R}}(n,k)\geq 2^n Y_{\mathbb{R}}(n,k)$ and $W_L(n,k)\geq (q_L-1)^n Y_L(n,k)$. 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, $W_{\mathbb{R}}(n,k)\geq 2^n Y_{\mathbb{R}}(n,k)$ and $W_L(n,k)\geq (q_L-1)^n Y_L(n,k)$.

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 [66]. □

2.7 Bounds: Known and Conjectural

Theorem 2.23. *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,*

$$Y_L(n,k) \geq \max\left\{Y_L(1,1)^{n-k+1}Y_L(1,2)^{k-1}, Y_L\left(\left\lfloor \tfrac{n}{k-1}\right\rfloor, 2\right)^{k-1-[n]_{k-1}} Y_L\left(\left\lfloor \tfrac{n}{k-1}\right\rfloor+1, 2\right)^{[n]_{k-1}}\right\}$$

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:

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

Proof. 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 2.2 and Remark 1) 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 2.5, 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 2.5, 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

$$Y_L(n,k) \geq Y_L\left(1, \left\lfloor \frac{n+k-1}{n} \right\rfloor\right)^{n-[k-1]_n} Y_L\left(1, \left\lfloor \frac{n+k-1}{n} \right\rfloor + 1\right)^{[k-1]_n} \quad \text{for } n \leq k-1.$$

To conclude, the entries in our table are simply specializations of our recursive lower bounds using the explicit values given by Theorem 2.2. □

That $Y_{\mathbb{R}}(n,k) < \infty$ for $n \geq 2$ was first proved around 1979 by Khovanskii and Sevastyanov [46, 45], yielding an explicit, singly-exponential upper bound. Based on the seminal results [30, Pg. 105], [57, Thm. 2], and [53], the second author proved in [70, Thm. 1] that $Y_L(n,k) < \infty$ for any fixed n, k, and non-Archimedean field L of characteristic zero. (See [73] 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 [4] 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 $Y_L(n,k)$
$\mathbb{R}$	$2^{O(k^2)}n^{k-1}$ [20][4]	$\Omega\left(\left\lfloor \frac{n+k-1}{\min\{n,k-1\}} \right\rfloor\right)^{\min\{n,k-1\}}$ (Theorem 2.23 here)
$\mathbb{Q}_p$	$(O(k^3 n \log k))^n$ [73]	$\Omega\left(\left\lfloor \frac{n+k-1}{\min\{n,k-1\}} \right\rfloor\right)^{\min\{n,k-1\}}$ (Theorem 2.23 here)

[3] While there have been important recent refinements to this bound (e.g., [74]) the asymptotics of [20] have not yet been improved in complete generality.

Also, Bertrand, Bihan, and Sottile proved the (tight) upper bound $Y_{\mathbb{R}}(n,2) \leq n+1$ in [14]. 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, Rojas posed the following conjecture (mildly paraphrased) at his March 20 Geometry Seminar talk at the Courant Institute in March 2007.

Conjecture 2.24 (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 3. 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 $(L,n) = (\mathbb{R},1)$ [94], and [53, 73] 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 [66]) 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.

Theorem 2.23 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.

3. SPARSITY AND SUMS OF SQUARES

3.1 Introduction and Main Results

Let $H_{n,2d}$ be the space of real polynomials in n variables of degree at most $2d$. Let us define the following cones in $H_{n,d}$:

$$P_{n,2d} = \{f \in H_{n,2d} : f(x) \geq 0 \text{ for all } x \in \mathbb{R}^n\}$$

$$\Sigma_{n,2d} = \{f \in \mathbb{R}[x]_{n,2d} : f = \sum_i f_i^2 \text{ for some } f_i \in H_{n,2d}\}$$

We call polynomials in the set $P_{n,2d}$ *positive semi-definite (or PSD, or non-negative)* polynomials, and polynomials in the set $\Sigma_{n,2d}$ *sums of squares (or SOS)* polynomials. It is a standard exercise to show that the sets $P_{n,2d}$ and $\Sigma_{n,2d}$ are convex cones in the vector space of degree $2d$ polynomials. It is clear that $\Sigma_{n,2d} \subset P_{n,2d}$. It has been established since 1888 by Hilbert that $\Sigma_{n,2d} \subsetneq P_{n,2d}$ except in the following three cases: $n = 1$, $2d = 2$, and $(n = 2, 2d = 4)$.

PSD and SOS polynomials have applications in optimization theory. The problem of minimizing a polynomial ($F = \min_{x \in \mathbb{R}^n} f(x)$) is equivalent to finding the maximum scalar translation that keeps the polynomial positive ($F = \max_{f - \gamma \in P_{n,2d}} \gamma$). The issue is that determining whether or not a polynomial is PSD is NP-Hard. However, determining if a polynomial is SOS is doable in polynomial-time via Semi-Definite Programming [60]. Thus, it would be beneficial to know when it is valid to replace the criteria of the polynomial being positive with the polynomial being SOS, a method known as *relaxation*.

Unfortunately, we cannot assume that most positive polynomials are sums of squares. It was shown in [22] that for a fixed $d \geq 2$, the volumes of the cones $P_{n,2d}$ and $\Sigma_{n,2d}$ are drastically and quantifying different. However, if we instead fix the number of variables, fix the number of terms, and allow d to vary, we could gain some new information.

The main result of this paper is, given a support of a polynomial f supported on a circuit (see Definition 1.17), to completely classify whether or not $f \in P_{n,2d}$ implies $f \in \Sigma_{n,2d}$.

Theorem 3.1. *Given a polynomial $f = \sum_{a \in \mathcal{A}} c_a x^a$, $c_a \neq 0$. Assume that f is PSD and $|\mathcal{A}| = n + 2$. Then if $\mathcal{A}$ is a non-degenerate circuit:*

1. *If $\operatorname{Newt}(f)$ has $n + 2$ vertices, then f is SOS.*
2. *If $\operatorname{Newt}(f)$ has $n + 1$ vertices, then f has an interior point a_i with coefficient c_i. Then we can say that:*
   - a. *If $a_i \in (2\mathbb{Z})^n$ and $c_i > 0$, then f is SOS.*
   - b. *If $a_i \notin (2\mathbb{Z})^n$ or $c_i < 0$, then let $U = \mathcal{A} \setminus a_i$. If $a_i \in$ the maximal mediated set of U, then f is SOS.*

Also, if $\mathcal{A}$ is a degenerate circuit, then f can be reduced to a polynomial with less variables.

Remark 4. Theorem 3.1 and Proposition 3.10 were proved independently in 2013 by Phillipson and by Iliman and de Wolff and published in 2016 in [41] by Iliman and de Wolff. The proofs of Proposition 3.10 [41] and this work are distinct.

3.2 Background

It is natural to consider the support of a polynomial when determining whether or not it is positive. Reznick proved several results concerning the relationship between

PSD polynomials and Newton Polytopes in [67], which will be used later in this section:

Theorem 3.2. *Let $f(x) = \sum_{a \in \mathcal{A}} c_a x^a$ with all c_a nonzero. Assume that $f(x)$ is PSD.*

a. If $0 \leq g \leq f$, then $\mathrm{Newt}(g) \subseteq \mathrm{Newt}(f)$.

b. If $f \in \Sigma_{n,2d}$ with $f = \sum_i f_i^2$, then $\mathrm{Newt}(f_i) \subseteq \frac{1}{2}\mathrm{Newt}(f)$ for all i.

c. If $\alpha \in \mathcal{A}$ is a vertex of $\mathrm{Newt}(f)$, then $c_\alpha > 0$ and $\alpha \in (2\mathbb{Z})^n$.

d. If F is a face of $\mathrm{Newt}\, f$, then $f_F(x) = \sum_{a \in F} c_a x^a$ is PSD.

Note that part (c) of Theorem 3.2 was proved in Example 1.5. Using 3.2, part (c), we have an immediate corollary for $(n+1)$-nomials in sufficiently general position:

Corollary 3.3. *Let $f = \sum_{a \in \mathcal{A}} c_a x^a$, $c_a \neq 0$. Assume that A does not lie in an affine hyperplane in $\mathbb{R}^n$. If $|\mathcal{A}| \leq n+1$, then f is SOS if and only if f is PSD.*

We also have an immediate result for polynomials supported on a non-degenerate circuit that is not a simplex:

Corollary 3.4. *Let $f = \sum_{i=1}^{n+2} c_i x^{a_i}$, $c_i \neq 0$ for all i, $\mathcal{A} = \{a_1, \ldots, a_{n+2}\} \subset \mathbb{Z}^n$ for all i. Suppose f is a PSD polynomial, $\mathcal{A}$ is a non-degenerate circuit, and $\mathrm{Conv}(\mathcal{A})$ is not a simplex. Then f is SOS.*

Proof. It is clear that a_i is a vertex of $\mathrm{Conv}(\mathcal{A})$ for all i, so by 3.2, $a_i \in (2\mathbb{Z})^n$ and $c_i > 0$ for all i, so f is trivially SOS.

□

3.3 Case of Degenerate Circuit

Proposition 3.5. *Suppose $g \in \mathbb{R}[x_1, \dots, x_n]$ and $a \in \mathbb{Z}^{n+1}$ has nonzero last coordinate. Then*

a. $x^a + g(x)$ is PSD $\iff a \in (2\mathbb{Z})^{n+1}$ and g is PSD.

b. $x^a + g(x)$ is SOS $\iff a \in (2\mathbb{Z})^{n+1}$ and g is SOS.

Proof. Define $G(x) = x^a + g(x)$. Note that a is a vertex of $\mathrm{Newt}(G)$ since $a \cdot (0, 0, \dots, 1) > 0 = v \cdot (0, 0, \dots, 1)$ for $v \in \mathrm{supp}(g)$.

For the proof of (a): assume first that $G(x)$ is PSD. Then since a is a vertex of $\mathrm{Newt}(G)$, $a \in (2\mathbb{Z})^{n+1}$, and

$$0 < G(x_1, \dots, x_n, 0) = g(x),$$

so g is PSD.

Now assume that $g(x) > 0$ and $a \in (2\mathbb{Z})^{n+1}$. Then $x^a \geq 0$ for all x, so

$$G(x) = g(x) + x^a \geq g(x) \geq 0.$$

For the proof of (b): First observe that if $g(x)$ is SOS and $a \in (2\mathbb{Z})^{n+1}$, then clearly $G(x)$ is SOS.

Now, let $G(x)$ be SOS. Then $G(x)$ is PSD, so $a \in (2\mathbb{Z})^{n+1}$.

Also, $G(x) = \sum_i (f_i)^2$, so

$$g(x) = G(x_1, \dots, x_n) = \sum_i (f_i(x_1, \dots, x_n, 0)^2,$$

so $g(x)$ is SOS.

□

Lemma 3.6. *Let $\mathcal{A}$ be a degenerate circuit, and let f be a PSD polynomial with* $\operatorname{supp}(f) = \mathcal{A}$*. Then the condition that f is SOS reduces to a polynomial with less variables.*

Proof. Let $\mathcal{A} = \{a_1, \ldots, a_{n+2}\}$ be a degenerate circuit. By dividing by a suitable monomial term, we can assume that $\vec{0} \in \mathcal{A}$. Via the definition of degenerate circuit, there exists $\mathcal{B} \subset \mathcal{A}$ and $a_j \in B$ such that $\mathcal{A} \setminus \{a_j\}$ is affinely independent and B is a non-degenerate circuit. This implies that $|\mathcal{B}| = n + 1$ and $\mathcal{B}$ is contained in a hyperplane of dimension $n - 1$. Moreover, we can assume that $\vec{0} \in \mathcal{B}$.

Without loss of generality, assume that $a_{n+2} \notin \mathcal{B}$. Note that a_{n+2} must be a vertex of $\operatorname{Conv}(\mathcal{A})$. Consider the $n \times (n+2)$ matrix A whose columns are the vectors a_i:

$$A = \begin{bmatrix} \\ a_1 & a_2 & \cdots & a_{n+1} & a_{n+2} \\ \\ \end{bmatrix}.$$

Recall from Section 1.6 that we can compute the Hermite Factorization of A as $UA = H$, with $H = [h_{i,j}] \in \mathbb{Z}^{n \times m}$ upper triangular and $U \in GL_n(\mathbb{Z})$. We claim the first $n + 1$ columns of H have zero in the last row, with the $(n + 2)^{\underline{\text{th}}}$ column having a nonzero entry in the last row. Since $\mathcal{A}$ is a degenerate circuit, $\operatorname{rank} A = n$, so we know that A has no non-zero rows.

Now consider the truncated matrix

$$A' = \begin{bmatrix} \\ a_1 & a_2 & \cdots & a_{n+1} \\ \\ \end{bmatrix}$$

This matrix has rank $n - 1$, so the Hermitian form of A' has one row of zeros. We can compute its Hermite form $U'A' = H'$ with $H' \in \mathbb{Z}^{n \times m}$ upper triangular and

$U' \in GL_n(\mathbb{Z})$. Since U' operates on A' column-by-column, we have that U is either U' itself or U' with the last row multiplied by -1. Either way, we have the desired result.

Thus, if we have a polynomial $f = \sum_{a \in \mathcal{A}} c_a x^a$ with $c_a \neq 0$, then we can introduce a change of coordinates
$(x_1, \ldots, x_n) = (y_1, \ldots, y_n)^U = (y_1^{u_{11}} y_2^{u_{21}} \cdots y_n^{u_{n1}}, \ldots, y_1^{u_{1n}} y_2^{u_{2n}} \cdots y_n^{u_{nn}})$. Then we obtain a polynomial of the form

$$G(y) = c_a y^a + g(y)$$

with $g(y) \in \mathbb{R}[y_1, \ldots, y_{n-1}]$, $c_a = c_{n+2}$, and a is the last column of H, which is assumed to have nonzero last coordinate. Thus, this polynomial is in the form of Proposition 3.5, and we are done.

□

3.4 When Support of Polynomial is a Simplex

When the support of the polynomial is a simplex, positivity need not imply SOS. Consider the Motzkin polynomial:

$$M(x_1, x_2) = 1 - 3x_1^2 x_2^2 + x_1^2 x_2^4 + x_1^4 x_2^2$$

$M(x, y)$ is a bivariate polynomial with support of size 4, with Newton Polytope shown in Figure 3.1. To show $M(x_1, x_2)$ is PSD, we use the Weighted Arithmetic-Geometric Inequality:

Theorem 3.7 (Weighted Arithmetic-Geometric Inequality). *Given weights*

$w_1, w_2, \dots, w_n > 0$, numbers $u_1, \dots, u_n > 0$, if $w = w_1 + \cdots + w_n > 0$, then

$$\frac{w_1u_1 + \cdots + w_nu_n}{w} \geq \sqrt[w]{u_1^{w_1} \cdots u_n^{w_n}}$$

with equality iff $u_1 = u_2 = \cdots = u_n$ and $w_i > 0$ for all i .

Using 3.7, we have that

$$1 + x_1^2x_2^4 + x_1^4x_2^2 \geq 3\sqrt[3]{1 \cdot x_1^2x_2^4 \cdot x_1^4x_2^2} = 3x_1^2x_2^2,$$

which shows that $M(x_1, x_2) \geq 0$ for all $x_1, x_2 \in \mathbb{R}$. However, it can be shown via a simple contradiction argument that $M(x_1, x_2)$ cannot be written as a sum of squares.

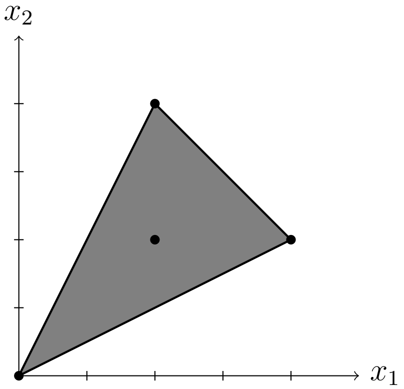


Figure 3.1: Newt(M)

3.4.1 Bounding the coefficients of a PSD polynomial

Assume that $f = \sum_{a \in \mathcal{A}} c_a x^a, \mathcal{A} = \{a_1, a_2, \dots, a_{n+2}\} \subset \mathbb{Z}^n$, with Conv($A$) an n-simplex. Without loss of generality, we can assume that $a_{n+2} \in$ RelInt(Conv(A)). If we fix coefficients $c_1, \dots, c_{n+1}$, we can bound the coefficient a_{n+2}. The lemma below is a special case of Lemma 2.6 in [63]:

Lemma 3.8. *Let $\mathcal{A} = \{a_1, a_2, \ldots, a_{n+2}\} \subset (\mathbb{Z}_+)^n$ be a non-degenerate circuit such that* $\operatorname{Conv}(\mathcal{A})$ *is a simplex with* $a_{n+2} \in \operatorname{RelInt}(\operatorname{Conv}(A))$. *Assume that $a_i \in (2\mathbb{Z})^n$ for all $i \neq n+2$. Let $\hat{A}$ denote the $(n+1) \times (n+2)$ matrix whose $j^{\underline{th}}$ column is the transpose of $\{1\} \times a_j$, i.e.*

$$\hat{A} := \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \\ a_1 & a_2 & \cdots & a_{n+2} \end{bmatrix}.$$

Let $b = (b_1, \ldots, b_{n+1}, -1)^T$ be a generator for the right nullspace of $\hat{A}$. Then for any $c_1, c_2, \ldots, c_{n+1} > 0$, and $x \in \mathbb{R}^n$, we have

$$c_1 x^{a_1} + c_2 x^{a_2} + \cdots + c_{n+1} x^{a_{n+1}} \geq x^{a_{n+2}} \prod_{i=1}^{n+1} \left(\frac{c_i}{b_i} \right)^{b_i}. \tag{3.1}$$

Proof. Note that $b_1 + \cdots + b_{n+1} = 1$ and $b_1 a_1 + \cdots b_{n+1} a_{n+1} = a_{n+2}$. In particular, $(b_1, \ldots, b_{n+1})$ are the barycentric coordinates for a_{n+2}, and $b_i > 0$ for all $i = 1, \ldots, n+1$. To apply the Weighted Arithmetic-Geometric Inequality, let $w_i = b_i$, $u_i = \frac{c_i x^{a_i}}{b_i}$. Then

$$\begin{aligned} c_1 x^{a_1} + c_2 x^{a_2} + \cdots + c_{n+1} x^{a_{n+1}} &\geq (b_1 + \cdots + b_{n+1}) \left(\prod_{i+1}^{n+1} \left(\frac{c_i x^{a_i}}{b_i} \right)^{b_i} \right)^{1/(b_1 + \cdots + b_{n+1})} \\ &\geq x^{b_1 a_1 + \cdots + b_{n+1} a_{n+1}} \prod_{i=1}^{n+1} \left(\frac{c_i}{b_i} \right)^{b_i} \\ &\geq x^{a_{n+2}} \prod_{i=1}^{n+1} \left(\frac{c_i}{b_i} \right)^{b_i}. \end{aligned}$$

□

Note that equality holds in 3.1 if there exists $z \in \mathbb{R}^n$ such that $\frac{c_1 z^{a_1}}{b_1} = \cdots = \frac{c_{n+1} z^{a_{n+1}}}{b_{n+1}}$.

Corollary 3.9. *Let $f = \sum_{i=1}^{n+2} c_i x^{a_i}, c_i \in \mathbb{R}^*, A = \{a_1, a_2, \ldots, a_{n+2}\} \subset \mathbb{Z}^n$, with $\mathrm{Conv}(A)$ an n-simplex. Assume that $a_i \in (2\mathbb{Z})^n$ for all $i \neq n+2$ and $a_{n+2} \in \mathrm{RelInt}(\mathrm{Conv}(A))$. Let $\hat{A}$ be as defined in Lemma 3.8. If $c_i > 0$ for all $i = 1, \ldots, n+1$ and*

$$|c_{n+2}| \leq \prod_{i=1}^{n+1} \left(\frac{c_i}{b_i}\right)^{b_i},$$

then f is PSD.

The converse of Corollary 3.9 also holds, with some additions.

Proposition 3.10. *Let $f = \sum_{i=1}^{n+2} c_i x^{a_i}, c_i \in \mathbb{R}^*, A = \{a_1, a_2, \ldots, a_{n+2}\} \subset \mathbb{Z}^n$, with $\mathrm{Conv}(A)$ an n-simplex. Assume $a_{n+2} \in \mathrm{RelInt}(\mathrm{Conv}(A))$. Let $\hat{A}$ be as defined in Lemma 3.8. If f is PSD, then for all $i = 1, \ldots, n+1$, $a_i \in (2\mathbb{Z})^n$ and $c_i > 0$. We also have one of the following conditions hold for c_{n+2}:*

1. *$a_{n+2} \in (2\mathbb{Z})^n$ and $c_{n+2} > 0$,*
2. *$|c_{n+2}| \leq \prod_{i=1}^{n+1} \left(\frac{c_i}{b_i}\right)^{b_i}$.*

Proof. The first assertions follow from 3.2. Condition (1) is trivial. For Condition (2), we can assume WLOG that $c_{n+2} < 0$. Consider $\gamma = \prod_{i=1}^{n+1} \left(\frac{c_i}{b_i}\right)^{b_i}$. Since $(b_1, \ldots, b_{n+1})$ are the barycentric coordinates for a_{n+2}, we have that $b_i > 0$ for $i \neq n+2$, so we have that $\gamma > 0$ and $1 = \mathrm{sign}(c_1 b_1) = \cdots = \mathrm{sign}(c_{n+1} b_{n+1}) = \mathrm{sign}(-\gamma b_{n+2})$. Also note that $\prod_{i=1}^{n+1} \left(\frac{c_i}{b_i}\right)^{b_i} \left(\frac{-\gamma}{-1}\right)^{-1} = 1$. Thus, by Lemma 1.18, the polynomial $\bar{f} = c_1 x^{a_1} + \cdots + c_{n+1} x^{a_{n+1}} - \gamma x^{a_{n+2}}$ has a degenerate root $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathbb{R}_+^n$. If we plug this into the original polynomial f, we get

$$\begin{aligned} f(\zeta_1,\dots,\zeta_n) &= c_1\zeta^{a_1} + c_{n+2}\zeta^{a_{n+2}} \\ &= c_1\zeta^{a_1} + c_{n+1}\zeta^{a_{n+1}} - \gamma\zeta^{a_{n+2}} + \gamma\zeta^{a_{n+2}} + c_{n+2}\zeta^{a_{n+2}} \\ &= (c_{n+2}+\gamma)\zeta^{a_{n+2}}. \end{aligned}$$

$(c_{n+2}+\gamma)\zeta^{a_{n+2}} > 0$ iff $|c_{n+2}| \leq \gamma$. □

3.4.2 Agiforms

To further discuss PSD polynomials supported on a simplex, we introduce notation first given by Reznick in [67].

Definition 3.11. Given $U \subset (2\mathbb{Z})^n$, Let $C(U) = \mathrm{Conv}(U) \cap \mathbb{Z}^n$, and let $E(U) = \mathrm{Conv}(U) \cap (2\mathbb{Z})^n$. If $B \subset \mathbb{Z}^n$, define $\mathrm{Ave}(B)$ to be the set of averages of even points of B:

$$\mathrm{Ave}(B) = \left\{ \frac{s+t}{2} : s,t \in (B \cap (2\mathbb{Z})^n) \right\},$$

and we let $\overline{\mathrm{Ave}}(B)$ denote the set of averages of *distinct* points of even points of B:

$$\overline{\mathrm{Ave}}(B) = \left\{ \frac{s+t}{2} : s \neq t, s,t \in (B \cap (2\mathbb{Z})^n) \right\}.$$

If $L \subset \mathbb{N}^n$, $U \subseteq L$, and, for every $v \in L \setminus U$, v is the average of two distinct even points in L, then we say that L is *U-mediated.*

Theorem 3.12. *[67] If $U \cup (2\mathbb{Z})^n$ is an affinely independent set, then there exists a U-mediated set U^* satisfying* $\mathrm{Ave}(U) \subseteq U^* \subseteq C(U)$ *which contains every U-mediated set.*

U^* is called the *maximal U-mediated set.* In the proof of Theorem 3.12, an algorithm is given to compute U^*. We now have the following result by Reznick [67]:

Theorem 3.13. *Given $U = \{u_1, u_2, \dots, u_{n+1}\}$, an affinely independent subset of $(2\mathbb{Z})^n$, let $u_{n+2} \in \mathrm{Conv}(U) \cap \mathbb{Z}^n$ with $(\lambda_1, \dots, \lambda_{n+1}) \in \mathbb{R}^{n+1}_{\geq 0}$ the barycentric coordinates of u_{n+2}; i.e., $\sum_{i=1}^{n+1} \lambda_i = 1$ and $u_{n+2} = \sum_{i=1}^{n+1} \lambda_i u_i$. Then if $f(x) := \lambda_1 x^{u_1} + \cdots + \lambda_{n+1} x^{u_{n+1}} - x^{u_{n+2}}$,*

a. $f(x)$ is PSD,

b. $f(x)$ is SOS if and only if $u_{n+2} \in U^*$.

Reznick refers to a polynomial that fits the criteria in 3.13 as an *agiform*[1] . If we consider the Motzkin polynomial $M(x_1, x_2) = 1 - 3x_1^2x_2^2 + x_1^2x_2^4 + x_1^4x_2^2$, we see that $f(x_1, x_2) = \frac{1}{3}M(x_1, x_2)$ is an agiform. Reznick's result was initially given for homogeneous polynomials; however, since de-homogenization does not affect positivity and SOS conditions [60], this theorem holds for non-homogeneous polynomials as stated here.

We claim that Theorem 3.13 can be extended to a *generalized agiform* $f_\mu(x) = \lambda_1 x^{u_1} + \cdots + \lambda_{n+1} x^{u_{n+1}} - \mu x^{u_{n+2}}$ for $0 < \mu < 1$:

Proof. Part (a): We know that $f_1(x) = \lambda_1 x^{u_1} + \cdots + \lambda_{n+1} x^{u_{n+1}} - x^{u_{n+2}}$ and $f_0(x) = \lambda_1 x^{u_1} + \cdots + \lambda_{n+1} x^{u_{n+1}}$ are both PSD. By the earlier remark in Subsection 3.1, the set of PSD polynomials is convex, so any point lying between $(\lambda_1, \dots, \lambda_m, 0)$ and $(\lambda_1, \dots, \lambda_m, 1)$ represents a PSD polynomial. For a given $\mu \in [0, 1]$, this point may be given as

$$(1 - \mu)(\lambda_1, \dots, \lambda_m, 0) + \mu(\lambda_1, \dots, \lambda_m, 1) = (\lambda_1, \dots, \lambda_m, \mu)$$

Thus, $f_\mu(x)$ is PSD, as well.

[1] This term comes from the Arithmetic-Geometric Inequality; sadly, it has no connection to the Texas A&M Aggies.

Part (b): If $u_{n+2} \in U^*$, then $f_1(x)$ is SOS. Since $f_0(x)$ is also clearly SOS, we can use the same argument as part (a) to show $f_\mu(x)$ is SOS.

Now, if $f_\mu(x)$ is SOS, it is not immediately clear that $u_{n+2} \in U^*$; however, we can generalize Reznick's original proof to show this, which we include here:

Suppose $f = f_\mu(x)$ is SOS. Then $f = \sum_{k=1}^{r} h_k^2$ for some r and some polynomials h_k. For each k, let $h_k(x) = \sum_{v \in \mathbb{Z}^n} b_k(v) x^v$. Then

$$f_\mu(x) = \sum_k \left(\sum_v b_k(v) x^v \right)^2 . \tag{3.2}$$

Let R be the union of the supports of the b_k:

$$R = \{v : b_k(v) \neq 0 \text{ for some } k\}.$$

Let $L = 2R \cup U \cup \{u_{n+2}\}$. We will show that L is U-mediated (which shows that $u_{n+2} \in U^*$).

Let $B(v) = (b_1(v), b_2(v), \ldots, b_r(v))$, and let $G(v, v') = B(v) \cdot B(v')$. Note that if we expand the right-hand side of 3.2, we see that the coefficient of x^u is

$$a(u) = \sum_{v+v'=u} G(v, v') = \sum_v G(v, u - v).$$

If $G(v, v') < 0$, then $b_k(v) b_k(v') < 0$ for some k, so $v \neq v'$ and $v, v' \in R$. This show that for $u \in L \setminus U$, if there exists v with $G(v, u-v) < 0$, then we can write u as a sum of distinct points in R (namely, v and $u - v$). Thus, to show L is U-mediated, it suffices to show that for any $u \in L \setminus U$, there exists v with $G(v, u - v) < 0$.

Note that $a(u_i) = \lambda_i$ for $i = 1, \ldots, n+1$, $a(u_{n+2}) = \mu$, and $a(u) = 0$ for all other u. We have that $\mu = a(u_{n+2}) = \sum G(v, u_{n+2})$, so since $\mu < 0$, $G(v_0, u_{n+2} - v_0) < 0$ for some v_0 (which immediately shows that $u_{n+2} \in U^*$). If $u \neq u_{n+2}$, then $u \in$

$L \setminus (U \cup \{u_{n+2}\})(= 2R)$, so $a(u) = 0 = \sum G(v, u - v)$. However, since $u \in 2R$, $b_k(\frac{1}{2}u) \neq 0$ for some k, so $G(\frac{1}{2}u, \frac{1}{2}u) = \sum_k (b_k(\frac{1}{2}u))^2 > 0$, so there must exist v with $G(v, u - v) < 0$ to make the sum vanish.

□

A relatively simple argument can bound the last coefficient of an agiform:

Lemma 3.14. *Let $U = \{u_1, u_2, \ldots, u_{n+1}\}$, an affinely independent subset of $(2\mathbb{Z})^n$, let $u_{n+2} \in \mathrm{Conv}(U) \cap \mathbb{Z}^n$ with $(\lambda_1, \ldots, \lambda_m) \in \mathbb{R}^m_{\geq 0}$ the barycentric coordinates of u_{n+2}; i.e., $\sum_{i=1}^{n+1} \lambda_i = 1$ and $u_{n+2} = \sum_{i=1}^{n+1} \lambda_i u_i$. Then if $f_\mu(x) := \lambda_1 x^{u_1} + \cdots + \lambda_{n+1} x^{u_{n+1}} - \mu x^{u_{n+2}}$ is PSD, either (1) $u_{n+2} \in (2\mathbb{Z})^n$ and $\mu < 0$ or (2) $|\mu| < 1$.*

Proof. (1) is trivial. For (2), suppose $\mu > 1$. Then consider polynomial f evaluated at $x = (1, 1, \ldots, 1)$:

$$f_\mu(1, 1, \ldots, 1) = \lambda_1 + \cdots + \lambda_{n+1} - \mu = 1 - \mu < 0,$$

which contradicts that f is PSD.

For $\mu < -1$, choose index i such that $u_{n+2_i} \notin 2\mathbb{Z}$, and consider the polynomial

$$f_\mu(x_1, \ldots, -x_i, \ldots, x_n) = \lambda_1 x^{u_1} + \cdots + \lambda_{n+1} x^{u_{n+1}} + \mu x^{u_{n+2}}$$

Now repeat the same argument for $\mu > 1$. □

Finally, we will show that any PSD polynomial supported on a simplex can be reduced to an agiform:

Theorem 3.15. *Let $f = \sum_{i=1}^{n+2} c_i x^{a_i}, A = \{a_1, a_2, \ldots, a_{n+2}\} \subset \mathbb{Z}^n$, with $\mathrm{Conv}(A)$ an n-simplex. Assume that $a_{n+2} \in \mathrm{RelInt}(\mathrm{Conv}(A))$. Assume that f is PSD. Then* *there exists a change of coordinates so that f can be considered in the form of theorem 3.13.*

Proof. As in 3.8, let $b = (b_1, \dots, b_{n+1}, -1)^T$ is a generator for the right nullspace of $\hat{A}$. As in the proof of Proposition 3.10, we can compute $\gamma = \prod_{i=1}^{n+1} \left(\frac{c_i}{b_i}\right)^{b_i}$ and define $\bar{f} = c_1 x^{a_1} + \dots + c_{n+1} x^{a_{n+1}} - \gamma x^{a_{n+2}}$. $\bar{f}$ has a degenerate root $\zeta = (\zeta_1, \dots, \zeta_n)$. Moreover, by the Weighted Arithmetic Geometric Inequality, this happens precisely when

$$\frac{c_1 \zeta^{a_1}}{b_1} = \dots = \frac{c_{n+1} \zeta^{a_{n+1}}}{b_{n+1}} = \alpha$$

for some $\alpha \in \mathbb{R}_{>0}$. In other words,

$$(c_1 \zeta^{a_1}, \dots, c_{n+1} \zeta^{a_{n+1}}, -\gamma \zeta^{a_{n+2}}) = \alpha(b_1, \dots, b_{n+1}, -1).$$

If we replace x with $\zeta \odot x = (\zeta_1 x_1, \dots, \zeta_n x_n)$, we get

$$\begin{aligned} f(\zeta_1 x_1, \dots, \zeta_n x_n) &= \sum_{i=1}^{n+2} c_i \zeta^{a_i} x^{a_i} \\ &= \alpha \left(\sum_{i=1}^{n+1} b_i x^{a_i} + \frac{c_{n+2}}{\gamma} x^{a_{n+2}} \right), \end{aligned}$$

and given that the b vector is in the nullspace of $\hat{A}$, it follows that $\sum_{i=1}^{n+1} b_i = 1$ and $\sum_{i=1}^{n+1} a_i b_i = a_{n+2}$. Also, by Proposition 3.10, $|c_{n+2}| \leq \gamma$, so $|\frac{c_{n+2}}{\gamma}| \leq 1$. Thus, $f(\zeta_1 x_1, \dots, \zeta_n x_n)$ is a scalar multiple of a generalized agiform.

□

Since multiplying each variable by a positive scalar affects neither the positivity nor the SOS condition, we see that any polynomial supported on a simplex can be reduced to a generalized agiform.

3.5 Further Discussion on Agiforms

Theorem 3.16. *Let* $U = \{u_1, u_2, u_3\} \subset (2\mathbb{Z})^2$ *form the vertices of a 2-simplex. Then* $\text{Ave}(E(U)) = C(U)$.

Proof. First, consider a lemma:

Lemma 3.17. *Let* $\Delta \subset \mathbb{R}^2$ *be a non-degenerate triangle with vertices* $U_\Delta = \{(a_1, b_1), (a_2, b_2), (a_3, b_3)\}$ *with* $a_i, b_i \in 2\mathbb{Z}$ *such that* $\text{Area}(\Delta) = 2$. *Then* $\text{Ave}(E(U_\Delta)) = C(\Delta)$.

Consider a general $U = \{u_1, u_2, u_3\} \subset (2\mathbb{Z})^2$ such that $S := \text{Conv}(U)$ forms a 2-simplex. I claim that S can be triangulated using triangles with area 2 with even integral vertices.

Consider $\frac{1}{2}U \subset \mathbb{Z}^2$. We can triangulate $\text{Conv}(\frac{1}{2}U)$ using every lattice point of $\text{Conv}(\frac{1}{2}U)$. By Pick's theorem, each triangle will have area 1. Scale the triangulation by 2 to get the desired triangulation.

Now, if $u \in C(U)$, u is a lattice point in some sub-triangle of S of area 2, which I will denote Δ'. By 3.17, $u = \frac{1}{2}(s + t)$, where $s, t \in \Delta' \cap (2\mathbb{Z})^2$. Since $\Delta' \in C(U)$, we have $s, t \in E(U)$. Thus, $u \in \text{Ave}(E(U))$, so $C(U) = \text{Ave}(E(U))$. □

Proof of lemma 3.17. Consider the midpoints of the sides of Δ, which are, without loss of generality,

$$\left(\frac{a_2 - a_1}{2}, \frac{b_2 - b_1}{2}\right), \left(\frac{a_2 - a_3}{2}, \frac{b_2 - b_3}{2}\right), \left(\frac{a_3 - a_1}{2}, \frac{b_3 - b_1}{2}\right)$$

The midpoints are distinct points in $\mathbb{Z}^2$, and they are distinct from the vertices. Hence, there are at least 6 boundary points on Δ.

By Pick's theorem, $\text{Area}(\Delta) = i + \frac{b}{2} - 1$, where i is the number of interior points and b is the number of boundary points. Thus, we have

$$\text{Area}(\Delta) = 2 = i + \frac{b}{2} - 1 \geq i + \frac{6}{2} - 1 = i + 2.$$

Thus, $i = 0$, $b = 6$, so $C(U_\Delta)$ consists solely of the vertices of Δ and the midpoints. Clearly, the midpoints are elements of $\text{Ave}(E(U_\Delta))$, so $C(U_\Delta) = \text{Ave}(E(U_\Delta))$. □

Example 3.18 (Counterexample of Theorem 3.16 for $n \geq 3$)**.** Consider $U = \{(2,0,0), (0,2,0), (0,0,2), (2,2,2)\}$. The convex hull of U is shown in figure 3.2.

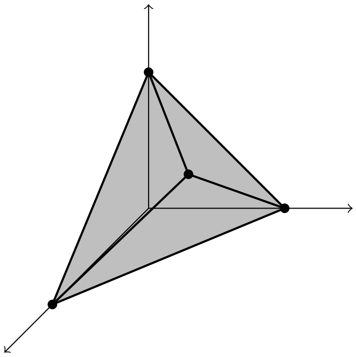


Figure 3.2: Conv(U)

We can compute that $|C(U)| = 11$ and $E(U) = U$; however,

$$|\text{Ave}(U)| \leq \binom{4}{2} + 4 = 10.$$

Thus, $\text{Ave}(U) \neq C(U)$.

Additionally, we can compute $\text{Ave}(U)$ to see that $(1,1,1)$ is the only point not in $\text{Ave}(U)$. It is interesting to compute the mediated set of U: We find that $U^* = \text{Ave}(U)$ in this case.

4. FASTER SOLUTION TO SMALE'S 17TH PROBLEM FOR CERTAIN SPARSE SYSTEMS

4.1 Introduction

Polynomial system solving has occupied a good portion of research in algebraic geometry for centuries, and inspired numerous algorithms in engineering and optimization. In recent years, *homotopy continuation* (see, e.g., [61, 56, 54, 85, 9] and Figure 4.1) has emerged as the most practical and efficient approach to leveraging high performance computing for the approximation of roots of large polynomial systems. A refinement particularly useful for sparse systems is *polyhedral homotopy* [40, 91, 52]. To be brutally concise, polyhedral homotopy reduces the solution of an arbitrary polynomial system to (a) solving a finite collection of *binomial* systems to high precision and then (b) iterating a multivariate rational function.

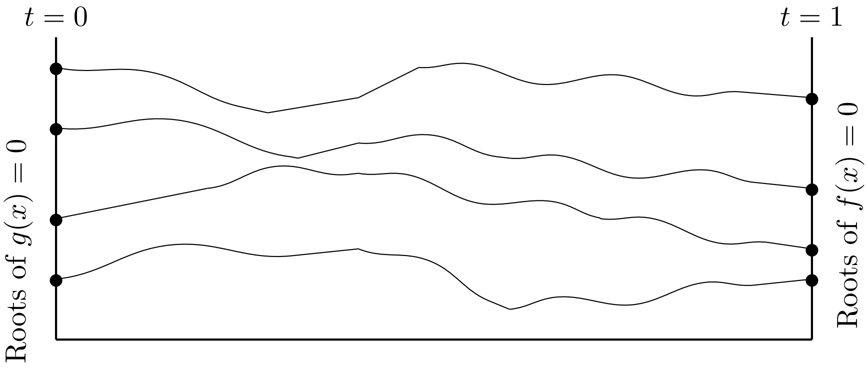


Figure 4.1: Homotopy continuation between two sets of roots

It is thus important to have rigorous and, ideally, optimal complexity estimates for solving binomial systems. Our first main theorem yields an algorithm with near optimal complexity for solving binomial systems.

Definition 4.1. Let $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$. Given $x, \bar{x} \in \mathbb{C}$ with $x \neq 0$, we say that $\bar{x}$ is an *ε-approximation of x* $\Longleftrightarrow |x - \bar{x}| \leq \varepsilon$. When $x, \bar{x} \in \mathbb{C}^n$ with $x = (x_1, \ldots, x_n) \in (\mathbb{C}^*)^n$ and $\bar{x} = (\bar{x}_1, \ldots, \bar{x}_n)$, we say that $\bar{x}$is an *ε-approximation of x* $\Longleftrightarrow |\bar{x} - x| \leq \varepsilon$ with $|\cdot|$ denoting the standard Euclidean norm. We call $f \in \mathbb{C}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ a *binomial* if and only if f has exactly 2 terms in its monomial term expansion. Finally, for any matrix $A = [a_{i,j}] \in \mathbb{Z}^{n \times n}$ we define the n-tuple of monomials $x^A := \left(x_1^{a_{1,1}} \cdots x_n^{a_{n,1}}, \ldots, x_1^{a_{1,n}} \cdots x_n^{a_{n,n}}\right)$, and let ω denote the least real number such that two $n \times n$ complex matrices can always be multiplied using $O(n^\omega)$ arithmetic operations.

Remark 5. The best current estimate on ω (as of July 2014) is $\omega \in [2, 2.3728639)$ [36]. $\diamond$

Theorem 4.2. *Suppose $c = (c_1, \ldots, c_n) \in (\mathbb{C}^*)^n$, $\sigma := \max_i\{|\log|c_i||\}$, $A = [a_{i,j}] \in \mathbb{Z}^{n \times n}$, $d := \max_{i,j}|a_{i,j}|$, and $\det A \neq 0$. We can find an ε-approximation of a root of $F := x^A - c$ in $\mathbb{C}^n$ using $O\big(n^{\omega+1}\log^2(dn)\big)$ bit operations, followed by $O(n^2\log(dn)(n\log(nd\sigma) + \log\log(1/\varepsilon)))$ field operations over $\mathbb{C}$.*

Note that the dependence on the relative accuracy 2^{-N} is *logarithmic* in N. We are unaware of any explicit complexity bounds for $n \geq 2$. Note also that evaluating $x^A - c$ already requires $\Omega(n + \log d)$ multiplications, since there are n monomials to evaluate. Also, ℓ multiplications starting from x_1 yield a power of x_1 with exponent no larger than 2^ℓ.

More importantly, our approach is simple, being based on a careful combination of binary search, Newton iteration, and integer matrix factorization. Estimating Smale's *γ-invariant* (see [81, 23] and Subsection 4.2 below) is a key part to our complexity analysis. Furthermore, Theorem 4.2 strongly implies that a solution of Smale's 17$^{\underline{\text{th}}}$ Problem (see [82, 83] and the next subsection) is possible.

Definition 4.3. Let $F : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ be any analytic function. An *approximate root of F (in the sense of Smale), with associated true root $\zeta \in \mathbb{C}^n$*, is a point $z^{(0)} \in \mathbb{C}^n$ such that the resulting sequence of Newton iterates $\left(z^{(j)}\right)_{j \in \mathbb{N}}$ converges to the root ζ of F fast enough for $|z^{(j)} - \zeta|/|z^{(0)} - \zeta| \leq (1/2)^{2^j}$ to hold for all $j \in \mathbb{N}$.

(a) An approximate root

(b) Not an approximate root

Figure 4.2: Comparison of Newton's method

Remark 6. It is worth noting that the rate of convergence specified above is close to the best one can hope for: For example, it is known that approximating $\sqrt{c}$ within $\varepsilon > 0$ (for any positive $c \in [1, 2]$) takes $\Omega(\log\log(1/\varepsilon))$ arithmetic operations [24].

In Subsection 4.2, we give some well-known methods of certifying a point as being an approximate root of a polynomial system. The proof of Theorem 4.2 contains the following result:

Corollary 4.4. *Suppose $c = (c_1, \ldots, c_n) \in (\mathbb{C}^*)^n$, $\sigma := \max_i\{|\log|c_i||\}$, $A = [a_{i,j}] \in \mathbb{Z}^{n\times n}$, $d := \max_{i,j}|a_{i,j}|$, and* $\det A \neq 0$. *We can find an approximate root of $F := x^A - c$ in $\mathbb{C}^n$ (in the sense of Smale) using $O\left(n^{\omega+1}\log^2(dn)\right)$ bit operations, followed by $O(n^3 \log(dn)\log(dn\sigma))$ field operations over $\mathbb{C}$.*

Corollary 4.4 then suggests the following likely conjecture to solve Smale's $17^{\underline{\text{th}}}$ problem in the case of binomial systems:

Conjecture 4.5. *Suppose* $c=(c_1,\ldots,c_n)\in(\mathbb{C}^*)^n$*, where* c_i *is an independent, standard complex Gaussian random variable.* $\sigma := \max_i\{|\log|c_i||\}$*,* $A=[a_{i,j}]\in\mathbb{Z}^{n\times n}$*,* $d:=\max_{i,j}|a_{i,j}|$*, and* $\det A\neq 0$*. Then there exists some* $K\in\mathbb{N}$ *such that we can find an approximate root of* $F:=x^A-c$ *using* $O\big(n^{\omega+1}\log^2(dn)\big)$ *bit operations, followed by* $O(n^{K+3}\log(d)^{2K+1}\log(n))$ *field operations over* $\mathbb{C}$ *on average.*

4.1.1 Review of Smale's $17^{\underline{\text{th}}}$ Problem and new speed-ups

Smale's $17^{\underline{\text{th}}}$ Problem elegantly summarizes the subtleties behind polynomial system solving, and suggests an advance:

Can **a zero** *of n complex polynomial equations in n unknowns be* **found approximately***,* **on the average***, in polynomial-time with a uniform algorithm?* [Emphases added.]

Let $f_1,\ldots,f_n\in\mathbb{C}[x_1,\ldots,x_n]$ be polynomials with respective degrees d_i and suppose $F:=(f_1,\ldots,f_n)$ is the polynomial system whose complex roots we would like to find. (When all possible coefficients are non-zero, such systems are sometimes referred to as *dense*, in contrast to the setting of *sparse* systems, like those considered in Theorem 4.2 above.) We clarify the notions of "uniform algorithm" and "polynomial-time" below. As motivation, let us first see how the emphasized terms highlight fundamental difficulties in polynomial system solving:

"a zero": We can not expect a fast algorithm approximating *all* the roots since, for $n\geq 2$, there may be infinitely many. In which case, for $d_1\geq 3$ (e.g., the case of elliptic curves [79]), the roots will likely not admit a rational parametrization. When there are only finitely many roots, systems like $(x_1^2-1,\ldots,x_n^2-1)$ show that the number of roots can be exponential in n.

"found approximately": Even restricting to integer coefficients, the number of digits of accuracy needed to separate distinct roots can be exponential in n, e.g.,

$$((2x_1-1)(3x_1-1), x_2-x_1^2, \ldots, x_n-x_{n-1}^2)$$

has roots with $n^{\underline{\text{th}}}$ coordinates $\frac{1}{2^{2^{n-1}}}$ and $\frac{1}{3^{2^{n-1}}}$. So, especially for irrational coefficients, we will need a more robust notion of approximation than digits of accuracy.

"on the average": Restricting to integer coefficients, distinguishing between a system having finitely many or infinitely many roots is **NP**-hard (see, e.g., [65, 47]). Furthermore, as already long known in the numerical linear algebra community (e.g., results on the distribution of eigenvalues of random matrices [32, 88]), even if the number of roots is finite, the accuracy needed to separate distinct roots can vary wildly as a function of the coefficients. So averaging over all inputs allows us to amortize the complexity of potentially intractable instances.

The original statement of Smale's $17^{\underline{\text{th}}}$ Problem measures *time* (or *complexity*) as the total number of (a) (exact) field operations over $\mathbb{R}$, (b) comparisons over $\mathbb{R}$, and (c) bit operations [82]. (The underlying computational model is a *BSS machine over* $\mathbb{R}$ [23], which is essentially a classical *Turing* machine [62, 2, 80], augmented so that it can perform any field operation or comparison over $\mathbb{R}$ in one time step.) *Polynomial-time* was then meant as polynomial in the number of (nonzero) coefficients of F. Smale interpreted the number of coefficients (which can be as high as $\sum_{i=1}^{n}\binom{d_i+n}{n}$ for F as specified above) as the *input size*.

Remark 7. The precise probability distribution over which one averages was never specified in Smale's original statement [82, 83]. In all the literature so far on the problem (see, e.g., [82, 83, 10, 11, 12, 25]), the *Bombieri-Weyl measure* was used: For any F as specified above, replace its coefficients by independent complex Gaussians with mean 0. The variance of the coefficient of $x_1^{a_1} \cdots x_n^{a_n}$ in f_i is then set to be the multinomial coefficient $\frac{d_i!}{a_1! \cdots a_n!(d_i - \sum_j a_j)!}$.

While the Bombieri-Weyl measure satisfies some very nice group invariance properties (see, e.g., [50, 77, 21, 34]), there is currently no widely-accepted notion of a "natural" probability distribution for a random polynomial. For instance, there are several different distributions of interest already for the matrix eigenvalue problem (see, e.g., [32, 69, 1]). More to the point, much work has gone into finding useful properties of the roots of random polynomials that are distribution independent (see, e.g., [16, 89]).

4.1.2 Uniformity and honest solutions of the problem

The meaning of *uniform algorithm* is more technical and is formalized in [23] (see also [62, 2, 80] for the classical Turing case). Roughly, if one imagines that our current computers could do a fixed number of (exact) field operations and comparisons over $\mathbb{R}$ during each clock-cycle, uniformity simply means that we can actually write a program that carries out our algorithm.

For example, aside from a non-constructive step (involving a start system, and initial solution, guaranteed to make homotopy continuation run fast on average) the first partial solution to Smale's 17$^{\underline{\text{th}}}$ Problem [78] ran in polynomial-time. It was precisely this non-constructive step that made the algorithm [78] non-uniform. Beltrán and Pardo then made major advances in [10, 11, 12]. A rough summary is the following result:

Theorem 4.6. *[12, Thm. 13] There is a randomized algorithm that, for an input random polynomial system F (as specified in Remark 7), does the following: After* *sampling a number of independent real standard Gaussians linear in the input size, the algorithm either outputs an approximate root to F (after a finite number of iterations of rational functions) or fails to stop. The probability of success is* 1*, and the average number of arithmetic operations is* $O\left(d^{3/2}n^2\left(\sum_{i=1}^{n}\frac{(d_i+n)!}{d!n!}\right)^2\log(dn)\right)$, *where* $d{:=}\max_i d_i$.

Note in particular that the complexity bound is polynomial in n if d is fixed, and vice-versa. More to the point, were it not for the random sampling, Beltran and Pardo's algorithm would be a full solution to Smale's $17^{\underline{\text{th}}}$ Problem. The next advance was by Bürgisser and Cucker [25] yielding a *deterministic* algorithm with average-case complexity sub-exponential, but super-polynomial in the input size. (The averaging being over the random F.)

Very recently, Lairez [51] developed a deterministic algorithm that is a derandomizatiom of the Beltrán and Pardo's algorithm; this was found to have average-case complexity $O\left(nd^{3/2}\left(\sum_{i=1}^{n}\binom{d_i+n}{n}\right)^2\right)$, which gives a complete solution to Smale's $17^{\underline{\text{th}}}$ Problem.

Conjecture 4.5 thus points to the possibility that the underlying notion of input size might be replaceable by *evaluation complexity*, measured in terms of field operations. Note in particular that the complexity of evaluating a dense F (as in Theorem 4.6) is $O\left(\sum_{i=1}^{n}\frac{(d_i+n)!}{d_i!n!}\log d_i\right)$, while the complexity of evaluating a binomial system (as in Theorem 4.2 and Conjecture 4.5) is $O(n^2\log d)$.

4.2 Background and Preliminary Results

In this subsection, we provide the foundation of the method of approximating roots of binomial systems by first presenting a certification of Newton's method, then giving an algorithm that quickly approximates an root of a univariate binomial.

4.2.1 Gamma theory and certification of Newton's method

The following subsection presents a result that give criteria for a point to be an approximate root of a polynomial system in the sense of Definition 4.3.

Definition 4.7. For any $f : \mathbb{C}^n \to \mathbb{C}^n$ analytic in a neighborhood about $z \in \mathbb{C}^n$, we set

$$\gamma(f, z) := \sup_{k \geq 2} \left| \frac{(f'(z))^{-1} f^{(k)}(z)}{k!} \right|^{1/(k-1)}$$

where for $n > 1$, $f'(z) = \left[\frac{\partial f_i}{\partial z_j} \right]_{i,j}$, $f^{(k)}(z)$ are multi-linear maps, and $| \cdot |$ is the operator norm induced by the 2-norm.

For general n, $f^{(k)}(z)$ is a multi-linear operator, taking $(\mathbb{C}^n)^k \to \mathbb{C}^n$. Further, if $f : \mathbb{C}^n \to \mathbb{C}^n$, $v^{(1)}, \dots, v^{(k)} \in \mathbb{C}^n$, then

$$f^{(k)}(z)(v^{(1)}, \dots, v^{(k)}) = \begin{bmatrix} D_1(v^{(1)}, \dots, v^{(k)}) \\ \\ \vdots \\ \\ D_n(v^{(1)}, \dots, v^{(k)}) \end{bmatrix}, \qquad (4.1)$$

where D_i is a multi-linear polynomial (linear with respect to each $v^{(j)}$) defined as:

for any exponents $\alpha_1^{(1)}, \dots, \alpha_n^{(1)}, \dots, \alpha_1^{(k)}, \dots, \alpha_n^{(k)}$, with $\sum_{l=1}^n \alpha_l^{(j)} = 1$ for all j, then the coefficient of

$(v_1^{(1)})^{\alpha_1^{(1)}} \cdots (v_n^{(1)})^{\alpha_n^{(1)}} \cdots (v_1^{(k)})^{\alpha_1^{(k)}} \cdots (v_n^{(k)})^{\alpha_n^{(k)}}$ (treating the v_i's as variables) is exactly

$$\frac{\partial^k}{\partial x_1^{\sum_{l=1}^k \alpha_1^{(l)}} \cdots \partial x_n^{\sum_{l=1}^k \alpha_n^{(l)}}} f_i(z)$$

Theorem 4.8. *[81] Suppose $f : \mathbb{C}^n \to \mathbb{C}^n$ is analytic in a neighborhood of z containing a root ζ of f, and $f'(\zeta)$ is invertible. If*

$$|z - \zeta| \leq \frac{3 - \sqrt{7}}{2} \cdot \frac{1}{\gamma(f, \zeta)},$$

then z is an approximate root of f (in the sense of Definition 4.3) with associated true root ζ.

Example 4.9. Consider the univariate binomial $f(x_1) = x_1^d - c$ with $c \in \mathbb{C}$. We can compute

$$\begin{aligned}
\gamma(f, z) &= \sup_{k \geq 2} \left| \frac{d(d-1) \cdots (d-k+1) z^{d-k}}{k! d z^{d-1}} \right|^{1/(k-1)} \\
&= \sup_{k \geq 2} \left| \frac{(d-1) \cdots (d-k+1)}{k!} \cdot \frac{1}{z^{k-1}} \right|^{1/(k-1)} \\
&\leq \sup_{k \geq 2} \left| \frac{(d-1)^{k-1}}{2^{k-1}} \cdot \frac{1}{z^{k-1}} \right|^{1/(k-1)} \\
&\leq \sup_{k \geq 2} \left| \left(\frac{d-1}{2z} \right)^{k-1} \right|^{1/(k-1)} \leq \left| \frac{d-1}{2z} \right|.
\end{aligned}$$

This gives us a lower bound for $1/\gamma$: if ζ is a true root of $f(x_1) = x_1^d - c$, and $\tilde{x}$ satisfies

$$|\tilde{x} - \zeta| \leq \frac{(3 - \sqrt{7})|\zeta|}{d - 1} \left(\leq \frac{3 - \sqrt{7}}{2} \cdot \frac{1}{\gamma(f, \zeta)} \right),$$

then $\tilde{x}$ is an approximate root of $f(x_1)$.

4.2.2 Univariate binomials

The first step of our algorithm is ensuring that univariate binomials can be approximated quickly. Approximating $\sqrt[d]{c}$ for $c > 0$ uses a modification of an algorithm first proposed by Ye [96]:

Theorem 4.10 (Hybrid Algorithm [96])**.** *Let $f(x_1) = x_1^d - c$, $c > 0$, $d \geq 2$. We can find an approximate real root $\tilde{x}$ of f with associated true root $\zeta > 0$ such that $|\tilde{x} - \zeta| \leq \varepsilon$ using $O(\log d(\log\log\max\{c, c^{-1}\} + \log\log(1/\varepsilon))$ arithmetic operations. In particular, we can find $\tilde{x}$ in $O(\log(d) + \log\log\max\{c, c^{-1}\})$ field operations such that*

$$|\tilde{x} - \zeta| \leq \frac{|\zeta|}{4d-5}.$$

Remark 8. note that $\frac{1}{4d-5} \leq \frac{(3-\sqrt{7})}{d-1}$ for $d \geq 2$.

Proof. We begin with a proposition proved by Ye in [96]:

Proposition 4.11. *Let $\alpha = \frac{d-1}{2}$. If ζ is a root of $f(x) = x^d - c$, $\zeta \in (0, R)$ for some $R > 0$, and $\zeta \in [(1 - \frac{1}{8\alpha})\hat{x}, \hat{x}] \subset (0, R)$, then $\hat{x}$ is an approximate root of f with associated true root ζ.*

The main goal of Ye's algorithm is to find this interval $[(1 - \frac{1}{8\alpha})\hat{x}, \hat{x}]$.

To begin, let $\beta = \frac{1}{1-\frac{1}{8\alpha}}$, and assume for now that $c > 1$. Note that $f(1) < 0$ and $f(c) > 0$. Define a sequence as follows: For $k \in \{0, 1, 2 \ldots, K\}$, define

$$b(k) := \beta^{2^k},$$

where K is the smallest integer such that $b(K) = \beta^{2^K} \geq c$. Note that $K = O(\log\log c + \log d)$. Now we locate the desired interval by the following method:

Step 0: Let $\hat{x} = 1$ and $\hat{k} = K$.

Step 1: Evaluate $f(b(\hat{k}-1)\hat{x})$.

Step 2: If $f(b(\hat{k}-1)\hat{x}) < 0$ then redefine $\hat{x} := b(\hat{k}-1)\hat{x}$ and $\hat{k} := \hat{k}-1$ and return to Step 1.

Step 3: Otherwise, if $\hat{k} > 0$ then set $\hat{k} := \hat{k}-1$ and return to Step 1.

This terminates in K steps, and each evaluation of f costs $\log(d)$ field operations via recursive squaring. Note that this algorithm is correct since $\zeta \in [\frac{1}{\beta}\hat{x}, \hat{x}]$. Thus, the total cost of computing an approximate root (in the sense of Smale) is $O(\log(d)\log\log c + \log^2(d))$ field operations.

However, this can be sped up: Consider instead computing K such that

$$(\beta^{2^K})^d \geq c.$$

For this K, since $\beta^{2^K} \geq c^{1/d}$, $f(\beta^{2^K}) > 0$, so this interval works, as well. Computing β^d requires $\log(d)$ field operations.

Now compute two sequences: (1) $(\beta^d)^{2^0}, (\beta^d)^{2^1}, \ldots, (\beta^d)^{2^K}$, and (2) $b(k) = \beta^{2^k}$ for $k \in \{0, 1, \ldots, K\}$, where K is the smallest integer such that $(\beta^{2^K})^d = (\beta^d)^{2^K} \geq c$. Since β^d has already been calculated, we no longer need to evaluate x^d each time. Also, note that

$$K = O(\log\log c - \log\log(\beta^d)) = O(\log\log c),$$

since $\log\log(\beta^d)$ is bounded by a constant. This modified algorithm takes $O(\log(d) + \log\log c)$ field operations to find $\hat{x}$. Since $\hat{x}$ is an approximate root of f, we can then use Newton's method to compute an ε-approximate root of f in time
$O(\log d(\log\log(c/\varepsilon)))$.

For $c < 1$, define $g(x_1) = x_1^d - c^{-1}$. Let $\tilde{x}$ be the approximate root of g calculated by the algorithm above with associated true root ζ. In particular, $\zeta < \tilde{x}$ and $|\tilde{x}-\zeta| \leq \frac{|\zeta|}{4d-5}$. Note that ζ^{-1} is a true root of $x_1^d - c$. Now we have, by the Mean Value Theorem, that $|\tilde{x}^{-1} - \zeta^{-1}| \leq \frac{|\tilde{x}-\zeta|}{z^2}$, where $z > 0$ with $\zeta \leq z \leq \tilde{x}$. Note that this implies $\frac{1}{|z|} \leq \frac{1}{|\zeta|}$, so we have

$$\begin{aligned}
|\tilde{x}^{-1} - \zeta^{-1}| &\leq \frac{|\tilde{x}-\zeta|}{z^2} \\
&\leq \frac{|\tilde{x}-\zeta|}{\zeta^2} \\
&\leq \frac{|\zeta|}{4d-5} \cdot \frac{1}{|\zeta|^2} \\
&\leq \frac{|\zeta^{-1}|}{4d-5},
\end{aligned}$$

Which shows that $\tilde{x}^{-1}$ is an approximate root of f with associated true root ζ^{-1}. This takes $O(\log(d) + \log\log c^{-1})$ field operations to compute.

□

Lemma 4.12. *Suppose $d \in \mathbb{N}$, $\varphi \in (0, 2\pi]$. We can approximate $e^{i\varphi/d}$ within accuracy ε using $O(\log\log(1/\varepsilon))$ arithmetic operations.*

Proof. Note that $e^{i\varphi/d} = \cos(\varphi/d) + i\sin(\varphi/d)$. If we approximate $\cos(\varphi/d)$ by x_0 and $\sin(\varphi/d)$ by y_0, each within accuracy $\varepsilon/2$, then we have

$$|e^{i\varphi/d} - (x_0 + iy_0)| = |\cos(\varphi/d) + i\sin(\varphi/d) - (x_0 + iy_0)| \leq |\cos(\varphi/d) - x_0| + |\sin(\varphi/d) - y_0| \leq \varepsilon.$$

Thus, if we approximate $\cos(\varphi/d)$ and $\sin(\varphi/d)$, we approximate $e^{i\varphi/d}$.

To approximate $x = \cos(\varphi/d)$, note that by Taylor's Remainder Theorem, we have

$$\left|\cos(x) - \left(1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \cdots + (-1)^k \frac{x^{2k}}{(2k)!}\right)\right| \leq \left|\frac{d^{k+1}}{dx^{k+1}}\cos(x)\right| \frac{|x^{k+1}|}{(k+1)!}$$
$$\leq \frac{(2\pi/d)^{k+1}}{(k+1)!}$$
$$\leq \frac{(2\pi/d)^{k+1}}{2^{k+1}} \leq \left(\frac{\pi}{d}\right)^{k+1}.$$

For $d > 3$, if we choose $k \geq 9$, then $\left(\frac{\pi}{d}\right)^{k+1} \leq \frac{(3-\sqrt{7})}{d-1}$. For $d = 2, 3$, we can compute that if $k \geq 7$, then $\frac{(2\pi/d)^{k+1}}{(k+1)!} \leq \frac{(3-\sqrt{7})|\zeta|}{d-1}$. Thus, we need only use $k = 9$ steps to compute $x_0 = \left(1 - \frac{(\varphi/d)^2}{2!} + \frac{(\varphi/d)^4}{4!} - \cdots + (-1)^k \frac{(\varphi/d)^{2k}}{(2k)!}\right)$ in order to get the desired approximate root.

The same holds for $\sin(x)$ with $y_0 = \left(\varphi/d - \frac{(\varphi/d)^3}{3!} + \frac{(\varphi/d)^5}{5!} - \cdots + (-1)^k \frac{(\varphi/d)^{2k+1}}{(2k+1)!}\right)$. Thus, $z_0 = x_0 + iy_0$ with give us an approximation for $e^{i\varphi/d}$ that satisfies the γ bound, which ensures that Newton's method from z_0 will converge to $e^{i\varphi/d}$ quadratically.

□

Theorem 4.10 and Lemma 4.12 together give us a method to compute a $d^{\underline{\text{th}}}$ root of a complex number:

Proposition 4.13. *Let $f(x_1) = x_1^d - c, c \in \mathbb{C}^*$. We can find an ε-approximation of a root of f using $O(\log d(\log\log\max\{|c|, |c|^{-1}\} + \log\log(1/\varepsilon)))$ arithmetic operations.*

Proof. Given $c = |c|e^{i\varphi}$ for some $\varphi \in [0, 2\pi)$, one root of f is $|c|^{1/d}e^{i\varphi/d}$. If we have an approximation for $|c|^{1/d}$, called c_0, and an approximation for $e^{i\varphi/d}$, called $\arg_0$, then we can compute that

$$\begin{aligned} ||c|^{1/d}e^{i\varphi/d} - c_0 \arg_0| &= ||c|^{1/d}e^{i\varphi/d} - |c|^{1/d}\arg_0 + |c|^{1/d}\arg_0 - c_0\arg_0| \\ &\leq ||c|^{1/d}e^{i\varphi/d} - |c|^{1/d}\arg_0| + ||c|^{1/d}\arg_0 - c_0\arg_0| \\ &\leq |c|^{1/d}|e^{i\varphi/d} - \arg_0| + |\arg_0||c|^{1/d} - c_0| \\ &\leq \max\{1,|c|\}|e^{i\varphi/d} - \arg_0| + ||c|^{1/d} - c_0| \leq 2\varepsilon, \end{aligned}$$

where if $\varepsilon' = \varepsilon/\max\{1,|c|\}$, then this takes time $O(\log d(\log\log\max\{|c|,|c|^{-1}\} + \log\log(1/\varepsilon)))$.

□

4.3 Binomial Systems

Proposition 4.14. *Let F be a diagonal binomial system $F = (x_1^{d_1} - \psi_1, \ldots, x_n^{d_n} - \psi_n)$ with $\psi \in \mathbb{C}^*$ for all i. Let $d = \max_i d_i$ and $\sigma' = \max_i\{|\log|\psi_i||\}$. We can compute an approximate zero of this system within error ε in time $O(n\log(d)(\log(\sigma') + \log\log(\sqrt{n}/\varepsilon)))$.*

Proof. Given an approximate zero $\tilde{x} = (\tilde{x}_1, \ldots, \tilde{x}_n)$ of F with true root $\zeta = (\zeta_1, \ldots, \zeta_n)$, we can compute each x_i within error $\frac{\varepsilon}{\sqrt{n}}$ in time $O(\log(d_i)\log\log(\sqrt{n}|\psi_i|/\varepsilon))$ by Proposition 4.13. We then have

$$\begin{aligned} |\tilde{x} - \zeta| &\leq \sqrt{n}\max_i\{|\tilde{x}_i - \zeta_i|\} \\ &\leq \sqrt{n}\frac{\varepsilon}{\sqrt{n}} = \varepsilon \end{aligned}$$

Thus, this computation takes time $O(n\log(d)(\log(\sigma') + \log\log(\sqrt{n}/\varepsilon)))$. □

Given a general binomial system:

$$F = \begin{cases} x^{a_1} - c_1 = 0 \\ \vdots \\ x^{a_n} - c_n = 0, \end{cases}$$

where $a_i \in \mathbb{Z}^n$, and $c_i \in \mathbb{C}^*$. Let A be the $n \times n$ matrix whose columns are the vectors a_i. Assume that A has nonzero determinant. We can write this system as $F := x^A = c$, where the notation x^A was given in Subsection 1.6 and $c = (c_1, \ldots, c_n)$. We can compute the Smith Normal Form of A, i.e., we can find matrices $U, V \in \mathbb{GL}_n(\mathbb{Z})$ and D diagonal such that $UAV = D$. Then, via the change of variables $y^U = x$, we can instead solve the equivalent system $G := y^D = c^V$, which is a diagonal system. For a solution y_0 of G, we can find a solution x_0 to F via the map $y_0^U = x_0$.

This approach to solving binomial systems is well-known, but it is believed to be the first time utilizing the Smith Normal Form in an algorithm for approximating roots in the sense of Smale. In particular, it is not immediately clear how close of an approximation we would need for G in order to guarantee an approximate root for F (in the sense of Smale), and how efficient such an algorithm would be.

We will need the following bounds to take into account the monomial change of variables.

Lemma 4.15. *Let $F := x^A = C$ with $C = (c_1, \ldots, c_n) \in (\mathbb{C}^*)^n$, $d := \max_{i,j} a_{ij}$, $\sigma := \max_j\{|\log|c_j||\}$ and let U, V, D be the matrices for the Smith Factorization of A: $UAV = D$. Let $(\psi_1, \ldots, \psi_n) = C^V$. Then the following bounds hold:*

a. $\max_j\{|\log|\psi_j||\} \leq n^4 n^{3n/2} d^{3n} \sigma$.

b. If $\zeta = (\zeta_1, \ldots, \zeta_n)$ is a true root for F, then

$$\max_j |\log|\zeta_j|| \leq n^{O(n)} d^{O(n)} \sigma.$$

Proof. Proof of (a): For a given i, we have

$$\begin{aligned}
|\log|\psi_i|| &= \left|\sum_{j=1}^{n} v_{ij} \log|c_j|\right| \\
&\leq \sum_{j=1}^{n} |v_{ij}| \cdot |\log|c_j|| \\
&\leq \sum_{j=1}^{n} |v_{ij}| \sigma \\
&\leq n(n^3(\sqrt{n}d)^{3n}\sigma = n^4 n^{3n/2} d^{3n} \sigma,
\end{aligned}$$

where the bound for v_{ij} is given in Theorem 1.21.

Proof of (b): Consider the diagonal system $(y_1^{d_1} - \psi_1, \ldots, y_n^{d_n} - \psi_n)$ formed via the change of variables $y^U = x$. Consider a true root $(\eta_1, \ldots, \eta_n)$ of this system. Then we have that $\eta_i^{d_i} = \psi_i$. In particular, we have

$$|\log|\eta_i|| \leq d_i |\log|z_i|| = |\log|\psi_i|| \leq n^4 n^{3n/2} d^{3n} \sigma.$$

From this, if we have a true root $\zeta = z^U$ for the original system F, we have

$$\begin{aligned}
\max_j |\log|\zeta_j|| &= \max_j |\log {z^U}_j| \\
&\leq n \cdot n^{2n+5} (\sqrt{n}d)^{4n} d \cdot (n^4 n^{3n/2} d^{3n} \sigma) \\
&\leq n^{O(n)} d^{O(n)} \sigma.
\end{aligned}$$

□

An important part of our algorithm is ensuring a tight bound on γ for general binomial systems.

Proposition 4.16. *Suppose* $c=(c_1,\ldots,c_n)\in(\mathbb{C}^*)^n$, $\sigma:=\max_i\{|\log|c_i||\}$, $A=[a_{i,j}]\in\mathbb{Z}^{n\times n}$, $d:=\max_{i,j}|a_{i,j}|$, $\det A\neq 0$, *and* $F(x):=x^A-c$. *Then for* ζ *a (true) root of* F,

$$\gamma(F,\zeta)\leq\frac{n^4d^{n+1}\max|\zeta_i|}{2(\min|\zeta_i|)^2}$$

.

Proof. We can write F as

$$F=\begin{cases}x^{a_1}-c_1=0\\ \vdots\\ x^{a_n}-c_n=0,\end{cases}$$

where $a_i\in\mathbb{Z}^n$, and the matrix A whose columns are the vectors a_i are has nonzero determinant. We can compute the Jacobian J at a root ζ as

$$J=\begin{pmatrix}a_{11}\zeta^{a_1-e_1} & \cdots & a_{1n}\zeta^{a_1-e_n}\\ \vdots & \ddots & \vdots\\ a_{n1}\zeta^{a_n-e_1} & \cdots & a_{nn}\zeta^{a_n-e_n},\end{pmatrix}$$

where e_i is the ith standard basis vector. We can decompose J as

$$J = \begin{pmatrix} \zeta^{a_1} & 0 & \cdots & \cdots & 0 \\ 0 & \cdots & \ddots & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & \zeta^{a_n} \end{pmatrix} A \begin{pmatrix} \zeta^{-e_1} & 0 & \cdots & \cdots & 0 \\ 0 & \cdots & \ddots & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & \zeta^{-e_n} \end{pmatrix}$$

So

$$J^{-1} = \begin{pmatrix} \zeta^{e_1} & 0 & \cdots & \cdots & 0 \\ 0 & \cdots & \ddots & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & \zeta^{e_n} \end{pmatrix} A^{-1} \begin{pmatrix} \zeta^{-a_1} & 0 & \cdots & \cdots & 0 \\ 0 & \cdots & \ddots & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & \zeta^{-a_n} \end{pmatrix}$$

Recall that $A^{-1} = \frac{1}{\det A}\text{adj}(A)$, so since A is an integer matrix, we have that

$$||A^{-1}|| = \frac{1}{\det A}||\text{adj}(A)|| \leq \sqrt{n}n \max_{i,j}(\text{adj}(A)_{i,j}) \leq \sqrt{n}nd^{n-1}.$$

Now note that a single coefficient in the polynomial D_i for the monomial with exponent $\alpha_1^{(1)}, \dots, \alpha_n^{(1)}, \dots, \alpha_1^{(k)}, \dots, \alpha_n^{(k)}$ is of the form:

$$\frac{\partial^k}{\partial x_1^{\sum_{l=1}^k \alpha_1^{(l)}} \cdots \partial x_n^{\sum_{l=1}^k \alpha_n^{(l)}}} f_i(z) = \prod_{m: \sum \alpha_m^{(l)} \neq 0} \prod_{t=0}^{\sum_l \alpha_m^{(l)} - 1} (a_{im} - t) z^{a_i - \sum_l \alpha_1^{(l)} e_1 - \cdots \sum_l \alpha_n^{(l)} e_n}.$$

If we apply the matrix $\operatorname{diag}(\zeta^{a_i})$ to $f^{(k)}(\zeta)$, for each D_i, a single coefficient will be reduced to

$$\prod_{m:\sum \alpha_m^{(l)}\neq 0} \prod_{t=0}^{\sum_l \alpha_m^{(l)}-1} (a_{im}-t) z^{-\sum_l \alpha_1^{(l)} e_1 - \cdots \sum_l \alpha_n^{(l)} e_n}.$$

Note that $|\zeta|^{-\sum_l \alpha_1^{(l)} e_1 - \cdots \sum_l \alpha_n^{(l)} e_n} \leq \frac{1}{(\min|\zeta_i|)^k}$, so since D_i has n^k terms, we can utilize the triangle inequality to find:

$$|D_i| \leq \frac{n^k d^k}{(\min|\zeta_i|)^k}.$$

Thus, the norm of the kth derivative is bounded by

$$\frac{\sqrt{n} n^k d^k}{(\min|\zeta_i|)^k}.$$

Putting this together, we have, for ζ a root of f,

$$\begin{aligned}
\gamma(f,\zeta) &\leq \sup_{k\geq 2} \left| \left(\frac{\max|\zeta_i| \cdot \sqrt{n} n d^{n-1}}{k!} \right) \left(\frac{\sqrt{n} n^k d^k}{(\min|\zeta_i|)^k} \right) \right|^{1/(k-1)} \\
&\leq \sup_{k\geq 2} \left| \left(\frac{\max|\zeta_i| \cdot n^2 d^{n-1} n d}{\min|\zeta_i|} \right) \left(\frac{\sqrt{n} n^{k-1} d^{k-1}}{2^{k-1}(\min|\zeta_i|)^{k-1}} \right) \right|^{1/(k-1)} \\
&\leq \sup_{k\geq 2} \left| \frac{\max|\zeta_i| \cdot n^2 d^{n-1} n d}{\min|\zeta_i|} \right|^{1/(k-1)} \cdot \frac{\sqrt{n} n^{k-1} d^{k-1}}{2^{k-1}(\min|\zeta_i|)^{k-1}} \\
&\leq \frac{n^4 d^{n+1} \max|\zeta_i|}{(2\min|\zeta_i|)^2}.
\end{aligned}$$

since $y^{1/(k-1)} < y$ for $y > 1$.

□

4.3.1 The proof of Theorem 4.2

Let $F := x^A = c$, where $x = (x_1, \ldots, x_n)$, $A \in \mathbb{N}^{n\times n}$ is a nonsingular matrix, and $c \in \mathbb{C}^{*n}$. We wish to find an approximate zero for this system.

We find the Smith Normal Form of A: $S = UAV$, and consider the system $y^{UAV} = y^S = c^V = (\psi_1, \ldots, \psi_n)$, where $y^U = x$. By [86], the time to compute the Smith Factorization of A is $O(n^{3.376} \log^2 nd)$ bit operations. Using the method outlined in Proposition 4.14, we can find an approximate root $\tilde{y}$ with associated true zero η for this system within error ε' in time $O(n \log(d')(\log(\sigma') + \log\log(\sqrt{n}/\varepsilon'))$, where $\sigma' = \max_i\{|\log|\psi_i|\}$. Note that by Lemma 4.15, $\log(\sigma') \leq \log(n^4 n^{3n/2} d^{3n}\sigma) = O(n \log(nd\sigma))$ and $d' \leq d^n n^{n/2}$.

We want to show that $\tilde{x} = \tilde{y}^U$ is an approximate zero for $x^A = c$ with associated true zero $\zeta = \eta^U$, so we look at the difference $|\tilde{x} - \zeta| = |\tilde{y}^U - \eta^U|$. Let $f_U(x) = x^U$. By the Mean Value Theorem, we have the following bound:

$$|\tilde{y}^U - \eta^U| \leq |\tilde{y} - \eta| \sup_{z \in l} ||J(f_U)(z)||$$

where $||\cdot||$ denotes the induced Euclidean norm on matrices, $J(f_U)(z)$ denotes the Jacobian of f_U evaluated at a point z, and $l = l(t) = t\tilde{y} + (1-t)\eta$, where $t \in [0,1]$. Note that by the computation of each $\tilde{y}_i$, the line segment joining $\tilde{y}_i$ and η_i does not contain zero; in particular, $|\tilde{y}_i - \eta_i| \leq \frac{|\eta_i|}{4d-5}$. This ensures that $l(t) \neq 0$ for $t \in [0,1]$.

We can compute that

$$J(f_U)(z) = \text{diag}(z^{u_i})U\text{diag}(z^{-e_i}),$$

where u_i is a row of U, e_i is the ith standard basis vector of $\mathbb{R}^n$.

So we have that

$$\begin{aligned}||J(f_U)(z)|| &\leq ||\text{diag}(z^{u_i})|| \cdot ||U|| \cdot ||\text{diag}(z^{-e_i})|| \\ &\leq \max_i |z^{u_i}| \cdot ||U|| \cdot \min_i |z_i|\end{aligned}$$

Note that $\min_i |z_i| \leq \min |\eta_i|$. From [86], we have that $||U|| \leq n||U||_{\max} \leq n^{4n+7}d^{4n+1}$. Let Z satisfy $\sup_{z \in l} \max_i |z^{u_i}| = |Z^{u_i}|$. Putting this all together, we have

$$\begin{aligned}|\tilde{y}^U - \eta^U| &\leq |\tilde{y} - \eta| \sup_{z \in l}\{\max |z^{u_i}| \cdot ||U|| \cdot \min |z_i|\} \\ &\leq \varepsilon' n^{4n+7} d^{4n+1} \cdot |Z^{u_i}| \cdot \min |\eta_i|\}\end{aligned}$$

Via a similar argument as in Lemma 4.15, we can compute that $|\log |Z^{u_i}|| \leq n^{4n+7}d^{4n+1}(\max \log |\eta_i| + \log(d-1)) \leq (dn)^{O(n)}(\sigma + \log(d-1))$. Now, for $|\tilde{y}^U - \eta^U| \leq \frac{3-\sqrt{7}}{2\gamma(\zeta)}$, by our bound for γ in Proposition 4.16, We need

$$\varepsilon' = \frac{2(\min |\zeta_i|)^2}{(dn)^{O(n)} \min_i |\eta_i| \max_i |\zeta_i| \cdot |Z^{u_i}|}.$$

Via our previous bounds for $|\log |\zeta_i||$, $| \, |\log_i |\eta_i||$, and $|\log |Z^{u_i}||$, we can compute that

$$\begin{aligned}\log(1/\varepsilon') =& (nd)^{O(n)}\sigma + \log(n^4 d^{n+1}) + (nd)^{O(n)}\sigma + O(n)\log(nd) \\ &+ O(n)\log(dn)\log(\sigma + \log(d)) + 2(nd)^{O(n)}\sigma.\end{aligned}$$

So $\log\log(1/\varepsilon') = O(n(\log(nd)+\log(\sigma))$. Hence, computing an approximate root for F (in the sense of Smale) requires $O(n^2\log(dn)(n\log(dn\sigma)+n(\log(dn)+\log(\sigma)) = O(n^3\log(dn)\log(dn\sigma))$ arithmetic operations. Since Newton's method is guaranteed to converge quadratically, and each step of Newton's method requires complexity $O(n\log(d))$, we can compute an ε-approximate root via Newton's method using $O(n^2\log(dn)(n\log(nd\sigma)+\log\log(1/\varepsilon)))$ field operations.

$\square$

5. CONCLUSION

When considering polynomials from the point of view of sparsity, one can gain new information about certain properties of polynomials and roots of polynomial systems. In Section 2, we saw that $n \times n$ systems with a total of $n+2$ terms are the first non-trivial case to consider when generalizing Descartes' Rule, and these results not only hold for complex systems but also for any local field. These results gave us a lower bound for larger systems. In Section 3, we gave a complete classification for when a positive polynomial with n variables and $n+2$ terms can be can written as a sum of squares. A general result is still unknown for n-variate polynomials with $n+k$ terms with $k > 2$. It would also be interesting to determine the probability of a positive n-variate polynomial $n+2$-nomial being a sum of squares. Finally, in Section 4, we gave an algorithm for computing approximate roots of binomial systems quickly. Future work will generalize this to any $n \times n$ system with $n+1$ total terms and will used as a building block for approximating roots of $n \times n$ systems with $n+2$ total terms.

REFERENCES

[1] Gernot Akemann, Jinho Baik, and Philippe Di Francesco. *The Oxford Handbook of Random Matrix Theory.* Oxford University Press, 2011.

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

[3] Martín Avendaño and Ashraf Ibrahim. Ultrametric root counting. *Houston Journal of Mathematics*, 36:1011–1022, 2010.

[4] Martín Avendaño and Ashraf Ibrahim. Multivariate ultrametric root counting. *Randomization, Relaxation, and Complexity in Polynomial Equation Solving, Contemporary Mathematics*, 556:1–24, 2011.

[5] Martín Avendaño and Teresa Krick. Sharp bounds for the number of roots of univariate fewnomials. *Journal of Number Theory*, 131:1209–1228, 2011.

[6] Martín Avendaño, Teresa Krick, and Martin Sombra. Factoring bivariate sparse (lacunary) polynomials. *J. Complexity*, 23:193–216, 2007.

[7] Osbert Bastani, Chris Hillar, Dimitar Popov, and J. Maurice Rojas. Randomization, sums of squares, and faster real root counting for tetranomials and beyond. *Randomization, Relaxation, and Complexity in Polynomial Equation Solving, Contemporary Mathematics*, 1556:145–166, 2011.

[8] Dan Bates and Frank Sottile. Khovanskii-Rolle continuation for real solutions. *Foundations of Computational Mathematics*, 11:563–587, 2011.

[9] Daniel Bates, Jonathan D. Hauenstein, Andrew Sommese, and Charles W. Wampler. Numerically solving polynomial systems with bertini. *Environments and Tools*, 2013.

[10] Carlos Beltrán and Luis M. Pardo. On smale's 17th problem: A probabilistic positive answer. *Foundations of Computational Mathematics*, 8:1–43, 2008.

[11] Carlos Beltrán and Luis M. Pardo. Smale's 17th problem: Average polynomial time to compute affine and projective solutions. *Journal of the American Mathematical Society*, 22:363–385, 2009.

[12] Carlos Beltrán and Luis M. Pardo. Efficient polynomial system solving by numerical methods. *in Randomization, Relaxation, and Complexity in Polynomial Equation Solving, Contemporary Mathematics*, 556:37–60, 2011.

[13] David Bernstein. The number of roots of a system of equations. *Functional Analysis and its Applications*, 9:183–185, 1975.

[14] Benoit Bertrand, Frederic Bihan, and Frank Sottile. Polynomial systems with few real zeroes. *Mathematisches Zeitschrift*, 253:361–385, 2006.

[15] Etienne Bézout. *Théorie générale des équations algébriques.* Paris, 1779.

[16] A.T. Bharucha-Reid and M. Sambandham. *Random polynomials.* Academic Press, Orlando, 1986.

[17] Frederic Bihan. Polynomial systems supported on circuits and dessins d'enfants. *J. London Math. Soc.*, 75:116–132, 2007.

[18] Frederic Bihan, J. Maurice Rojas, and Frank Sottile. *On the Sharpness of Fewnomial Bounds and the Number of Components of Fewnomial Hypersurfaces*,

chapter IMA Volume 146: Algorithms in Algebraic Geometry, pages 15–20. Springer, New York, 2007.

[19] Frederic Bihan, J. Maurice Rojas, and Casey E. Stella. Faster real feasibility via circuit discriminants. *Proceedings of International Symposium on Symbolic and Algebraic Computation (ISSAC 2009, July 28–31, Seoul, Korea)*, pages 39–46, 2009.

[20] Frederic Bihan and Frank Sottile. New fewnomial upper bounds from gale dual polynomial systems. *Moscow Mathematical Journal*, 7:387–407, 2007.

[21] Pavel Bleher, Bernard Shiffman, and Steve Zelditch. Poincare-Lelong approach to universality and scaling of correlations between zeros. *Communications in Mathematical Physics*, 208:771–785, 2000.

[22] Grigoriy Blekherman. There are significantly more nonnegative polynomials than sums of squares. *Israel Journal of Mathematics*, 153, 2006.

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

[24] Nader H. Bshouty, Yishay Mansour, Baruch Schieber, and Prasoon Tiwari. A tight bound for approximating the square root. *Information Processing Letters*, 63:211–213, 1997.

[25] Peter Bürgisser and Felipe Cucker. On a problem posed by Steve Smale. *Annals of Mathematics*, 174:1785–1836, 2011.

[26] Arkadev Chattopadhyay, Bruno Grenet, Pascal Koiran, Natacha Portier, and Yann Strozecki. Factoring bivariate lacunary polynomials without heights. *ISSAC*, 2013.

[27] Qi Cheng. Straight line programs and torsion points on elliptic curves. *Computational Complexity*, 12:150–161, 2004.

[28] Paula B. Cohen and Umberto Zannier. Fewnomials and intersections of lines with real analytic subgroups in $\mathbf{G}_m^n$. *Bull. London Math. Soc.*, 34:21–32, 2002.

[29] Vladimir Ivanovich Danilov. The geometry of toric varieties. *Russian Mathematical Surveys*, 33:97–154, 1978.

[30] Jan Denef and Lou van den Dries. p-adic and real subanalytic sets. *Annals of Mathematics*, 128:79–138, 1988.

[31] Alicia Dickenstein, J. Maurice Rojas, Korben Rusek, and Justin Shih. Extremal real algebraic geometry and $\mathcal{A}$-discriminants. *Moscow Mathematical Journal*, 7, 2007.

[32] Alan Edelman. Eigenvalues and condition numbers of random matrices. *SIAM Journal on Matrix Analysis and Applications*, 9:543–560, 1988.

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

[34] Yan V. Fyodorov, Antonio Lerario, and Erik Lundberg. On the number of connected components of random algebraic hypersurfaces. *Journal of Geometry and Physics*, 95:1–20, 2015.

[35] Andrei Gabrielov and Nicolai Vorobjov. Complexity of cylindrical decompositions of sub-pfaffian sets. *J. Pure Appl. Algebra*, 164:179–197, 2001.

[36] François Le Gall. Powers of tensors and fast matrix multiplication. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, pages 296–303, ISSAC 2014, 2014.

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

[38] Mark Giesbrecht and Daniel Roche. Interpolation of shifted-lacunary polynomials. *Computational Complexity*, 19:333–354, 2010.

[39] Bertrand Haas. A simple counterexample to Kouchnirenko's conjecture. *Beiträge zur Algebra und Geometrie*, 43, 2002.

[40] Birk Huber and Bernd Sturmfels. A polyhedral method for solving sparse polynomial systems. *Mathematics of Computation*, 64:1541–1555, 1995.

[41] Sadik Iliman and Timo de Wolff. Amoebas, nonnegative polynomials and sums of squares supported on circuits. *Research in Mathematical Sciences*, 3, 2016.

[42] Hendrik W. Lenstra (Jr.). Finding small degree factors of lacunary polynomials. *Number Theory in Progress*, 1:267–276, 1999.

[43] Vadim Kaloshin. The existential hilbert 16-th problem and an estimate for cyclicity of elementary polycycles. *Inventiones Mathematicae*, 151:451–512, 2003.

[44] Erich Kaltofen and Pascal Koiran. Finding small degree factors of multivariate supersparse (lacunary) polynomials over algebraic number fields. *Proceedings of ISSAC 2005 (Internat. Symp. Symbolic Algebraic Comput.)*, pages 162–168, 2006.

[45] Askold Khovanskii. Fewnomials. *Translations of Mathematical Monographs*, 88, 1991.

[46] Askold G. Khovanskii. On a class of systems of transcendental equations. *Dokl. Akad. Nauk SSSR*, 255:804–807, 1980.

[47] Pascal Koiran. Randomized and deterministic algorithms for the dimension of algebraic varieties. *Proceedings of the 38$^{\underline{th}}$ Annual IEEE Computer Society Conference on Foundations of Computer Science (FOCS)*, 1997.

[48] Pascal Koiran. Shallow circuits with high-powered inputs. *in Proceedings of Innovations in Computer Science (ICS 2011, Jan. 6–9, 2011, Beijing China)*, 2011.

[49] Pascal Koiran, Natacha Portier, and Sébastien Tavenas. A Wronskian approach to the real τ-conjecture. *Journal of Symbolic Computation*, 68:195–214, 2015.

[50] Eric Kostlan. On the distribution of roots of random polynomials. In *From Topology to Computation: Proceedings of the Smalefest (1990)*, pages 419–431, Berkeley, CA, 1993. Springer, New York.

[51] Pierre Lairez. A deterministic algorithm to compute approximate roots of polynomial systems in polynomial average time. *Foundations of computational mathematics*, to appear, 2016.

[52] Tsung-Lin Lee and Tien-Yien Li. Mixed volume computation in solving polynomial systems. *Randomization, Relaxation, and Complexity in Polynomial Equation Solving, Contemporary Mathematics*, 556:97–112, 2011.

[53] Hendrik W. Lenstra. On the factorization of lacunary polynomials. *Number Theory in Progress*, 1:277–291, 1999.

[54] Tien Yien Li. Numerical solution of multivariate polynomial systems by homotopy continuation methods. *Acta numerica*, 6:399–436, 1997.

[55] Tien-Yien Li, J. Maurice Rojas, and Xiaoshen Wang. Counting real connected components of trinomial curves intersections and m-nomial hypersurfaces. *Discrete and Computational Geometry*, 30:379–414, 2003.

[56] Tien Yien Li and Xiaoshen Wang. Solving deficient polynomial systems with homotopies which keep the subschemes at infinity invariant. *Mathematics of Computation*, 56:693–710, 1991.

[57] Leonard Lipshitz. p-adic zeros of polynomials. *J. Reine Angew. Math.*, 390:208–214, 1988.

[58] Richard Lipton. Straight-line complexity and integer factorization, 1994.

[59] Jesús A. De Loera, Jörg Rambau, and Francisco Santos. *Triangulations: Structures for Algorithms and Applications*. Springer, 2010.

[60] Murray Marshall. *Positive Polynomials and Sums of Squares*. American Mathematical Society, 2008.

[61] Alexander Morgan and Andrew Sommese. A homotopy for solving general polynomial systems that respects m-homogeneous structures. *Applied Mathematics and Computation*, 24:101–113, 1987.

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

[63] Philipe Pébay, J. Maurice Rojas, and David C. Thompson. Optimizing n-variate $(n + k)$-nomials for small k. *Theoretical Computer Science, Symbolic-Numeric Computation 2009 special issue*, 412, 2011.

[64] Philippe P. Pébay, J. Maurice Rojas, and David C. Thompson. Optimization and $\mathbf{NP}_{\mathbb{R}}$-completeness of certain fewnomials. *Proceedings of SNC 2009 (August 3–5, 2009, Kyoto, Japan)*, pages 133–142, 2009.

[65] David A. Plaisted. New np-hard and np-complete polynomial and integer divisibility problems. *Theoretical Computer Science*, 31:125–138, 1984.

[66] Bjorn Poonen. Zeros of sparse polynomials over local fields of characteristic p. *Math. Res. Lett.*, 5:273–279, 1998.

[67] Bruce Reznick. Forms derived from the arithmetic-geometric inequality. *Mathematische Annalen*, 283, 1989.

[68] Alain M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, 2000.

[69] J. Maurice Rojas. On the average number of real roots of certain random sparse polynomial systems. In *The Mathematics of Numerical Analysis*, volume 32 of *Lectures in Applied Mathematics*, pages 689–699. American Mathematical Society, 1996.

[70] J. Maurice Rojas. Finiteness for arithmetic fewnomial systems. *Contemporary Mathematics*, 286:107–114, 2001.

[71] J. Maurice Rojas. 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*, pages 506–515, 2002.

[72] J. Maurice Rojas. Why polyhedra matter in non-linear equation solving. *Contemporary Mathematics*, 334:293–320, 2003.

[73] J. Maurice Rojas. Arithmetic multivariate Descartes' rule. *American Journal of Mathematics*, 126:1–30, 2004.

[74] Korben Rusek, Frank Sottile, and Jeanette Shakalli-Tang. Dense fewnomials. *Randomization, Relaxation, and Complexity in Polynomial Equation Solving, Contemporary Mathematics*, 556:167–186, 2011.

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

[76] Tamara Servi. *On the first-order theory of real exponentiation*. Edizioni della Normale, 2008.

[77] Mike Shub and Steve Smale. The complexity of Bezout's theorem II: Volumes and probabilities. *Computational Algebraic Geometry*, pages 267–285, 1992.

[78] Mike Shub and Steve Smale. The complexity of Bezout's theorem V: Polynomial time. *Theoretical Computer Science*, 133:141–164, 1994.

[79] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer, 1994.

[80] Michael Sipser. *Introduction to the Theory of Computation*. Cengage Learning, 3rd edition, 2012.

[81] Steve Smale. Newton's method estimates from data at one point. In *The Merging of Disciplines: New Directions in Pure, Applied, and Computational Mathematics*, pages 185–196. Springer, Laramie, WY, 1986.

[82] Steve Smale. Mathematical problems for the next century. *Math. Intelligencer*, 20:7–15, 1998.

[83] Steve Smale. Mathematical problems for the next century. *Mathematics: Frontiers and Perspectives*, pages 271–294, 2000.

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

[85] Andrew J. Sommese and Charles W. Wampler. The numerical solution to systems of polynomials arising in engineering and science. *World Scientific*, 2005.

[86] Arne Storjohann. *Algorithms for Matrix Canonical Forms.* PhD thesis, Swiss Federal Institute of Technology, Zurich, 2000.

[87] Bernd Sturmfels. Viro's theorem for complete intersections. *Annali della Scuola Normale Superiore di Pisa (4)*, 21:377–386, 1994.

[88] Terence Tao and Van Vu. From the Littlewood-Offord problem to the circular law: Universality of the spectral distribution of random matrices. *Bulletin of the American Mathematical Society*, 46:377–396, 2009.

[89] Terence Tao and Van Vu. Local universality of zeroes of random polynomials. *International Mathematics Research Notices*, 2014.

[90] Sergey Vakulenko and Dmitry Grigoriev. Complexity of gene circuits, pfaffian functions and the morphogenesis problem. *C. R. Math. Acad. Sci. Paris*, 337:721–724, 2003.

[91] Jan Verschelde. Polynomial homotopy continuation with phcpack. *ACM Communications in Computer Algebra*, 2013.

[92] Oleg Ya. Viro. Gluing of plane real algebraic curves and constructions of curves of degrees 6 and 7. *Lecture Notes in Math.*, 1984.

[93] Marc Voorhoeve. On the oscillation of exponential polynomials. *Mathematische Zeitschrif*, 151:277–294, 1976.

[94] Xiaoshen Wang. A simple proof of Descartes' rule of signs. *The American Mathematical Monthly*, 111:525–526, 2004.

[95] Alex J. Wilkie. A theorem of the complement and some new o-minimal structures. *Selecta Math. (N.S.)*, 5:397–421, 1999.

[96] Yinyu Ye. Combining binary search and newton's method to compute real roots for a class of real funcitons. *Journal of Complexity*, 10:271–280, 1994.