# Arithmetic Multivariate Descartes' Rule[1]

J. Maurice Rojas*
Department of Mathematics
Texas A&M University
TAMU 3368
College Station, Texas 77843-3368
USA
e-mail: rojas@math.tamu.edu
Web Page: http://www.math.tamu.edu/~rojas

February 2004

**Abstract**

Let $\mathcal{L}$ be any number field or $\mathfrak{p}$-adic field and consider $F := (f_1, \ldots, f_k)$ where $f_1, \ldots, f_k \in \mathcal{L}[x_1, \ldots, x_n]$ and no more than $\mu$ distinct exponent vectors occur in the monomial term expansions of the $f_i$. We prove that $F$ has no more than $1 + \left(\mathcal{C}n(\mu - n)^3 \log(\mu - n)\right)^n$ geometrically isolated roots in $\mathcal{L}^n$, where $\mathcal{C}$ is an explicit and effectively computable constant depending only on $\mathcal{L}$. This gives a significantly sharper arithmetic analogue of Khovanski's Theorem on Real Fewnomials and a higher-dimensional generalization of an earlier result of Hendrik W. Lenstra, Jr. for the special case of a single univariate polynomial. We also present some further refinements of our new bounds and an explicit generalization of a bound of Lipshitz on $p$-adic complex roots. Connections to non-Archimedean amoebae and computational complexity (including additive complexity and solving for the geometrically isolated rational roots) are discussed along the way. We thus provide the foundations for an effective arithmetic analogue of fewnomial theory.

## 1 Introduction and Main Results

A consequence of Descartes' Rule (a classic result dating back to 1637) is that any real univariate polynomial with exactly $\mu \geq 1$ monomial terms has at most $2\mu - 1$ real roots. This has since been generalized by Askold Georgevich Khovanski during 1979–1987 (see [Kho80] and [Kho91, Pg. 123]) to certain systems of multivariate sparse polynomials and even **fewnomials**. (Sparse polynomials are sometimes also known as lacunary polynomials and, over $\mathbb{R}$, are a special case of fewnomials — a more general class of real analytic functions of parameterized complexity [Kho91].) Here we provide ultrametric and thereby arithmetic

[1] From **American Journal of Mathematics, vol. 126, no. 1, February 2004, pp. 1–30.**
*This research was partially supported by a grant from the Texas A&M College of Science, NSF/DARPA CARGO grant DMS-0138446, and NSF individual grant DMS-0211458.

analogues for both results: we give explicit upper bounds, independent of the degrees of the underlying polynomials, for the number of geometrically isolated roots of sparse polynomial systems over any **$\mathfrak{p}$-adic field** and, as a consequence, over any **number field**. (Recall that a point $x$ in an algebraic set $Z$ defined over a field $\mathcal{L}$ is **geometrically isolated** iff $x$ is a zero-dimensional component of the algebraic set obtained from replacing $\mathcal{L}$ by its algebraic closure $\overline{\mathcal{L}}$.) For convenience, let us henceforth respectively refer to these cases as the **local** case and the **global** case.

Suppose now that $f_1,\ldots,f_k \in \mathcal{L}[x_1^{\pm 1},\ldots,x_n^{\pm 1}]\setminus\{0\}$ where $\mathcal{L}$ is a field to be specified later, and $\mu$ is the total number of distinct exponent vectors appearing in $f_1,\ldots,f_k$, assuming all polynomials are written as sums of monomials. We call $F:=(f_1,\ldots,f_k)$ a **$\mu$-sparse $k\times n$ polynomial system over $\mathcal{L}$** and, for any extension $\mathcal{L}'$ of $\mathcal{L}$, we let $Z_{\mathcal{L}'}(F)$ denote the set of $x\in(\mathcal{L}')^n$ such that $f_1(x)=\cdots=f_k(x)=0$. Khovanski's results take $\mathcal{L}=\mathbb{R}$ and yield an explicit upper bound for the number of non-degenerate roots, in the non-negative orthant, of any $\mu$-sparse $n\times n$ polynomial system [Kho80, Kho91]. With some extra work (e.g., [Roj00b, Cor. 3.2]) his results imply an upper bound of $2^{O(n)}n^{O(\mu)}2^{O(\mu^2)}$ on the number of **topologically** isolated roots (i.e., roots that are themselves connected components of $Z_{\mathbb{R}}(F)$) of $F$ in $\mathbb{R}^n$, and this is asymptotically the best general upper bound currently known. In particular, since it is easy to show that the last bound can in fact be replaced by 1 when $\mu\leq n$ (see, e.g., [LRW03, Thm. 3, Part (b)]), one should focus on understanding the behavior of the maximum number of topologically isolated real roots for $n$ fixed and $\mu\geq n+1$. For example, is the dependence on $\mu$ polynomial for fixed $n$? This turns out to be an open question, but we can answer the arithmetic analogue (i.e., where $\mathcal{L}$ is any $\mathfrak{p}$-adic field or any number field) affirmatively and explicitly. Recall that $\lfloor t\rfloor$ is the greatest integer not exceeding $t$.

**Theorem 1** *Let $p$ be any (rational) prime and $d,\delta$ positive integers. Suppose $\mathcal{L}$ is any degree $d$ algebraic extension of $\mathbb{Q}_p$ or $\mathbb{Q}$, and let $\mathcal{L}^*:=\mathcal{L}\setminus\{0\}$. Also let $F$ be any $\mu$-sparse $k\times n$ polynomial system over $\mathcal{L}$ and define $B(\mathcal{L},\mu,n)$ to be the maximum number of geometrically isolated roots in $(\mathcal{L}^*)^n$ of such an $F$ in the local case, counting multiplicities.*

*Then $B(\mathcal{L},\mu,n)=0$ (if $\mu\leq n$ or $k<n$) and*

$$\boldsymbol{B(\mathcal{L},\mu,n)\leq u(\mu,n)(p^d-1)^n\left\lfloor\left\{c(\mu-n)n\left[1+d\log_p\left(\frac{d(\mu-n)}{\log p}\right)\right]\right\}^n\right\rfloor} \text{ (if } \mu\geq n+1 \text{ and } k\geq n\text{)},$$

*where $u(\mu,n)$ is $\mu-1$, $\max\{1,9(\mu-3)^2\}$, or $((\mu-n)(\mu-n+1)/2)^n$, according as $n=1$, $n=2$, or $n\geq 3$; $c:=\frac{e}{e-1}\leq 1.582$ and $\log_p(\cdot)$ denotes the base $p$ logarithm function.*

*Furthermore, moving to the global case, let us say a root $x\in\mathbb{C}^n$ of $F$ is of* **degree $\leq\delta$ over** $\mathcal{L}$ *iff every coordinate of $x$ lies in an extension of degree $\leq\delta$ of $\mathcal{L}$, and let us define $A(\mathcal{L},\delta,\mu,n)$ to be the maximum number of geometrically isolated roots of $F$ in $(\mathbb{C}^*)^n$ of degree $\leq\delta$ over $\mathcal{L}$, counting multiplicities. Then $A(\mathcal{L},\delta,\mu,n)=0$ (if $\mu\leq n$ or $k<n$) and*

$$\boldsymbol{A(\mathcal{L},\delta,\mu,n)\leq u(\mu,n)2^{nd\delta+1}\left\lfloor\left\{c(\mu-n)n\left[1+2d^2\delta^2\log_2\left(\frac{d^2\delta^2(\mu-n)}{\log 2}\right)\right]\right\}^n\right\rfloor} \text{ (if } \mu\geq n+1 \text{ and } k\geq n\text{)}.$$

Our bounds can be sharpened even further: This is detailed in Corollary 1 and Propositions 1 and 2 of Sections 3 and 3.1, and Corollary 2 and Propositions 3 and 4 of Section 4. The proof of Theorem 1 essentially reduces to a result — Theorem 2 of Section 1.1, our second main theorem — on the distribution of $p$-adic **complex** roots close to the point $(1,\ldots,1)$. The proof of the latter result in turn follows from a beautiful but overlooked result of A. L. Smirnov on the distribution of the norms of $p$-adic complex roots [Smi97, Thm. 3.4] (cf. Section 1.1 below).

**Remark 1** *At the expense of underestimating some multiplicities (e.g., roots on the coordinate hyperplanes may have multiplicities $>1$ counted as $1$ instead), we can easily obtain upper bounds for the number of geometrically isolated roots of $F$ in $\mathcal{L}^n$ (in the local case) and the number of geometrically isolated roots in $\mathbb{C}^n$ of degree $\leq\delta$ over $\mathcal{L}$ (in the global case): By simply setting all possible subsets of variables to zero, we easily obtain respective upper bounds of $1+\sum_{j=1}^{n}\binom{n}{j}B(\mathcal{L},\mu,j)\leq 1+2^nB(\mathcal{L},\mu,n)$ and $1+\sum_{j=1}^{n}\binom{n}{j}A(\mathcal{L},\delta,\mu,j)\leq 1+2^nA(\mathcal{L},\delta,\mu,n)$. Of course, since many of the monomial terms of $F$ will vanish upon setting an $x_i$ to $0$, these bounds will usually be larger than really necessary.* $\diamond$

**Example 1** *Consider the following $2\times 2$ system over $\mathbb{Q}_2$:*

$$\begin{aligned} f_1(x,y) &:= \alpha_1+\alpha_2x^{u_2}y^{v_2}+\alpha_3x^{u_3}y^{v_3} \\ f_2(x,y) &:= \beta_1+\beta_2x^{a_2}y^{b_2}+\cdots+\beta_mx^{a_m}y^{b_m} \end{aligned}$$

*which is $\mu$-sparse for some $\mu\leq m+2$. Theorem 1 and an elementary calculation then tell us that such an $F$ has no more than $\mathbf{90.1}\boldsymbol{m^2(m-1)^2(1+\log_2(1.45m))^2}$ geometrically isolated roots, counting multiplicities, in $(\mathbb{Q}_2^*)^2$ (and $(\mathbb{Q}^*)^2$ as well, via the natural embedding $\mathbb{Q}\hookrightarrow\mathbb{Q}_2$). In particular, $m=3 \Longrightarrow F$ is at worst $5$-sparse and has no more than* **31428** *such roots, regardless of $u_2,v_2,u_3,v_3,a_2,b_2,a_3,b_3$. Explicit bounds independent of the total degrees of $f_1$ and $f_2$ appear to have been unknown before, even for special case $m=3$. Sharper bounds, based on refinements of Theorem 1 (cf. Corollary 1 and Proposition 1) appear in Remark 9 and Example 6, respectively of Sections 3 and 3.1.* $\diamond$

**Remark 2** *If we replace $\mathbb{Q}_2$ by $\mathbb{R}$ in the last example, then the best previous upper bounds were* $\mathbf{4(2^m-2)}$ *for all $m\geq 4$ and a tight bound of* **20** *in the special case $m=3$. Interestingly, the latter bounds, which follow easily from [LRW03, Thm. 1], in fact allow us to take* **real** *exponents and count* **topologically** *isolated roots, but without multiplicities. (Khovanski's Theorem on Real Fewnomials [Kho91, Cor. 7, Sec. 3.12, Pg. 80], which only counts non-degenerate roots, implies an upper bound of $995328$ for $m=3$.) However, this real analytic upper bound exceeds our arithmetic bound for all $m\geq 30$, where both bounds begin to exceed $2.8$ billion.* $\diamond$

**Example 2** *Another consequence of Theorem 1 is that for* **fixed** *$\mathcal{L}$, we now know $\log B(\mathcal{L},\mu,n)$ and $\log A(\mathcal{L},\delta,\mu,n)$ to within a constant factor: the upper bound is clearly $O(n\log\mu)$, with the implied constant depending on $\delta$ and the degree of $\mathcal{L}$ over $\mathbb{Q}_2$ or $\mathbb{Q}$. To get a lower bound, simply consider the $\mu$-sparse $n\times n$ polynomial system $F=(f_1,\ldots,f_n)$ where $f_i=\prod_{j=1}^{m-1}(x_i-j)$ for all $i$ and $\mu=1+n(m-1)$. Clearly then, this $F$ has exactly $(m-1)^n$ geometrically isolated roots in $\mathbb{N}^n$. So $m\geq n+1\geq 3 \Longrightarrow \mu-1\geq n^2$, which in turn implies that $\log B(\mathcal{L},\mu,n)$ and $\log A(\mathcal{L},\delta,\mu,n)$ are never smaller than $\frac{1}{4}n\log\mu$ for all $\mathcal{L}$ as in Theorem 1. Let us emphasize, however, that finding optimal upper bounds for $B(\mathcal{L},\mu,n)$ and $A(\mathcal{L},\delta,\mu,n)$ remains an intriguing open problem. Curiously, much less is known about the analogous growth-rate when $\mathcal{L}$ is replaced by the usual Archimedean completion $\mathbb{R}$ of $\mathbb{Q}$.* $\diamond$

A weaker version of Theorem 1 with non-explicit bounds was derived earlier in [Roj01b]. In particular, explicit bounds were known previously only in the speical case $n=1$ [Len99b, Props. 7.1, 7.2, and 8.1], which we summarize below.

**Lenstra's Theorem** *Following the notation above, we have*

$$B(\mathcal{L},\mu,1)\leq 1.582\cdot(p^d-1)(\mu-1)^2\left(1+\frac{d\log(d(\mu-1)/\log p)}{\log p}\right)$$

*and*

$$A(\mathcal{L},\delta,\mu,1)<4.565\cdot(\mu-1)^2(d\delta+10)2^{d\delta}(\log(d\delta(m-1))+0.367). \qquad \blacksquare$$

All our bounds (save the global case) match the best bounds of [Len99b] in the special case $n=1$. We should also note that the bounds of [Len99b, Props. 7.1 and 7.2; and Sec. 8] are actually slightly sharper than our paraphrase above. Also, to streamline the proof of our multivariate generalization, we left our bound on $A(\mathcal{L},\delta,\mu,n)$ in Theorem 1 a bit loose. To repent for these loosenings, we give a sharper bound for the global case, agreeing with Lenstra's best univariate bound when $n=1$, in Corollary 2 of Section 4.

Philosophically, the approach of [Len99b] was more algebraic (low degree factors of polynomials) while our point of view here is more geometric (geometrically isolated rational points of low degree in a hypersurface intersection). Also, Lenstra derived a higher-dimensional generalization but in a direction different than ours: bounds for the number of hyperplanes (defined over $\mathcal{L}$) in a hypersurface defined by a single $\mu$-sparse $n$-variate polynomial [Len99b, Prop. 6.1].) In particular, the only other results known for $k>1$ or $n>1$ were derived via rigid analytic geometry and model theory, and in our notation imply a non-effective bound of $B(\mathbb{Q}_p,\mu,n)<\infty$ (see the seminal works [DvdD88, Lip88]).

Our approach is simpler and is based on a higher-dimensional generalization (Theorem 2 of the next section) of an earlier root count for univariate sparse polynomials over certain algebraically closed fields [Len99b, Thm. 3]. Indeed, aside from the introduction of some higher-dimensional convex geometry, our proof of Theorem 1 is structurally quite similar to Lenstra's proof of the special case $n=1$ in [Len99b]: reduce the global case to the local case, then reduce the local case to a refined result over the $p$-adic complex numbers.

We now describe two results used in our proofs which may be of broader interest.

**Remark 3** *Throughout this paper, the intersection multiplicity of a geometrically isolated root $x$ of a $k\times n$ polynomial system $F$ is considered in the following sense: For $k=n$ we simply use the coefficient of $x$ in the intersection product of $n$ divisors in the Chow ring of $\left(\overline{\mathcal{L}}^*\right)^n$ [Ful98, Ex. 7.1.10, Pg. 123]. This multiplicity then turns out to always be a positive integer (see, e.g., [Ful98, Prop. 7.1 (a)] or [Roj99b, Thm. 3]). For $k>n$, the theory of [Ful98] no longer applies, but our multiplicities remain positive and integral (cf. Lemma 1).* $\diamond$

**Remark 4** *The numerical calculations and illustrations throughout this paper were done with the assistance of* `Maple`, `Matlab`, *and* `Geomview`, *and the software for these calculations is freely downloadable from the author's web-site at* `http://www.math.tamu.edu/~rojas/list2.html` . $\diamond$

## 1.1 The Distribution of $p$-adic Complex Roots

For any (rational) prime $p$, let $\mathbb{C}_p$ denote the completion (with respect to the extended $p$-adic metric) of the algebraic closure of $\mathbb{Q}_p$. Theorem 1 follows from a careful application of two results on the distribution of roots of $F$ in $(\mathbb{C}_p^*)^n$. The first result strongly limits the number of roots that can be $p$-adically close to the point $(1,\ldots,1)$. The second result strongly limits the number of distinct valuation vectors which can occur for the roots of $F$.

**Theorem 2** *Let $F$ be any $\mu$-sparse $k\times n$ polynomial system over $\mathbb{C}_p$. Also let $r_1,\ldots,r_n>0$, $r:=(r_1,\ldots,r_n)$, and let $\mathrm{ord}_p:\mathbb{C}_p\longrightarrow\mathbb{Q}\cup\{+\infty\}$ denote the usual $p$-adic valuation (cf. Definition 1), normalized so that $\mathrm{ord}_p p=1$, e.g., $\mathrm{ord}_p 0=+\infty$ and $\mathrm{ord}_p(p^k r)=k$ whenever $r$ is a unit in $\mathbb{Z}_p$ and $k\in\mathbb{Q}$. Finally, let $C_p(\mu,n,r)$ denote the maximum number of geometrically isolated roots $(x_1,\ldots,x_n)\in\mathbb{C}_p^n$ of $F$ with $\mathrm{ord}_p(x_i-1)\geq r_i$ for all $i$, counting multiplicities. Then $C_p(\mu,n,r)=0$ (if $\mu\leq n$ or $k<n$) and*

$$\boldsymbol{C_p(\mu,n,r)\leq\left\lfloor\left\{c(\mu-n)\left[r_1+\cdots+r_n+\log_p\left(\frac{(\mu-n)^n}{r_1\cdots r_n\log^n p}\right)\right]\right\}^n\Big/\prod_{i=1}^n r_i\right\rfloor}$$

*(if $\mu\geq n+1$ and $k\geq n$), where $c:=\frac{e}{e-1}\leq 1.582$.*

*Furthermore, when $k=n$ we can obtain a more refined bound as follows: Let $[n]:=\{1,\ldots,n\}$, let $m_i$ denote the number of distinct exponent vectors in $f_i$, $\overline{m}:=(m_1,\ldots,m_n)$, and $\overline{N}:=(N_1,\ldots,N_n)$ where, for each $i$, $N_i\subseteq[n]$ is the set of all $j$ such that $x_j$ appears with nonzero exponent in some monomial term of $f_i$. Then, letting $C_p(\overline{m},\overline{N},r)$ denote the obvious analogue of $C_p(\mu,n,r)$, we have $C_p(\overline{m},\overline{N},r)=0$ (if $m_i\leq 1$ for some $i$) and*

$$\boldsymbol{C_p(\overline{m},\overline{N},r)\leq\left\lfloor c^n\prod_{i=1}^n\left\{(m_i-1)\left[\left(\sum_{j\in N_i}r_j\right)+\log_p\left(\frac{(m_i-1)^{\#N_i}}{\left(\prod_{j\in N_i}r_j\right)\log^{\#N_i}p}\right)\right]\Big/ r_i\right\}\right\rfloor}$$

*(if $m_1,\ldots,m_n\geq 2$), where $\#$ denotes the operation of taking set cardinality.*

A simple corollary of these bounds is that the number of roots in a fixed finite extension of $\mathbb{Q}_p$ with given "first digit" can be bounded solely in terms of $\mu$ (or $\overline{m}$) and $n$ (cf. Section 3). Note also that our upper bounds are decreasing functions of $p$, so we in fact have a **universal** upper bound of $C_2(\mu,n,r)$ (or $C_2(\overline{m},\overline{N},r)$) for the number of geometrically isolated roots of $F$ in $(\mathbb{C}_p^*)^n$ $p$-adically close to $(1,\ldots,1)$.

The bounds above also appear to be new: the only previous results in this direction appear to have been Lenstra's derivation of the special case $n=1$ [Len99b, Thm. 3] and an earlier observation of Leonard Lipshitz [Lip88, Thm. 2] equivalent to the non-explicit bound $C_p(\mu,n,(1,\ldots,1))<\infty$. It is also interesting to note that Theorem 2 gives a sharper and more general p-adic analogue of Khovanski's Theorem on **Complex** Fewnomials [Kho91, Thm. 1, Sec. 3.13, Pg. 82–83]. (The latter result gives an elegant upper bound on the number of non-degenerate roots lying in an angular sector of $(\mathbb{C}^*)^n$.) However, the angular metaphor is reversed here: whereas Khovanski derived his Theorem on Complex Fewnomials via a clever reduction to his Theorem on Real Fewnomials, we prove our $\mathfrak{p}$-adic bound (Theorem 1) from our "digital" bound over $\mathbb{C}_p$ (Theorem 2).

The final bound over $\mathbb{C}_p^n$ we state is a toric arithmetic-geometric result of A. L. Smirnov.

**Definition 1** *For any $a=(a_1,\ldots,a_n)\in\mathbb{Z}^n$, let $x^a:=x_1^{a_1}\cdots x_n^{a_n}$. Writing any $f\in\mathcal{L}[x_1,\ldots,x_n]$ as $\sum_{a\in\mathbb{Z}^n}c_a x^a$, we call $\mathrm{Supp}(f):=\{a\mid c_a\neq 0\}$ the* **support** *of $f$. Also, let $\pi:\mathbb{R}^{n+1}\longrightarrow\mathbb{R}^n$ be the natural projection forgetting the $x_{n+1}$ coordinate and, for any $n$-tuple of polytopes $P=(P_1,\ldots,P_n)$, define $\pi(P):=(\pi(P_1),\ldots,\pi(P_n))$. Finally, a* **non-Archimedean valuation**

**on $\mathcal{L}$** *is any function* $\mathrm{ord} : \mathcal{L} \longrightarrow \mathbb{R} \cup \{+\infty\}$ *satisfying (i)* $\mathrm{ord}(xy) = \mathrm{ord}(x) + \mathrm{ord}(y)$*, (ii)* $\mathrm{ord}(x) = +\infty \Longleftrightarrow x = 0$*, (iii)* $\mathrm{ord}(x+y) \geq \max(\mathrm{ord}(x), \mathrm{ord}(y))$*.* $\diamond$

**Definition 2** *For any $k \times n$ polynomial system $F$ over $\mathcal{L}$, its* ***k*-tuple of Newton polytopes with respect to the valuation ord**, $\widehat{\mathrm{Newt}}(F) := \left(\widehat{\mathrm{Newt}}(f_1), \ldots, \widehat{\mathrm{Newt}}(f_k)\right)$*, is defined as follows:* $\widehat{\mathrm{Newt}}(f_i) := \mathrm{Conv}(\{(a, \mathrm{ord}(c_a)) \mid a \in \mathrm{Supp}(f_i)\}) \subset \mathbb{R}^{n+1}$*, where* $\mathrm{Conv}(S)$ *denotes the convex hull of (i.e., smallest convex set containing) a set $S \subseteq \mathbb{R}^{n+1}$. Also, for any $w \in \mathbb{R}^n$ and any closed subset $B \subset \mathbb{R}^n$, the* **face of *B* with inner normal *w***, $B^w$*, is the set of points $x \in B$ that minimize the inner product $w \cdot x$. We call a face* **lower** *(resp. upper) iff the last coordinate of any of its inner normals is positive (resp. negative). Finally, for any $k$-tuple $(B_1, \ldots, B_k)$ of closed subsets of $\mathbb{R}^n$, we let $(B_1, \ldots, B_k)^w := (B_1^w, \ldots, B_k^w)$.* $\diamond$

**Smirnov's Theorem** *[Smi97, Thm. 3.4] Let $K$ be any algebraically closed field with a non-Archimedean valuation $\mathrm{ord}(\cdot)$. Then, for any $n \times n$ polynomial system $F$ over $K$, the number of geometrically isolated roots $(x_1, \ldots, x_n) \in (K^*)^n$ of $F$ satisfying $\mathrm{ord} x_i = r_i$ for all $i$ (counting multiplicities) is no more than $\mathcal{M}\left(\pi\left(\widehat{\mathrm{Newt}}(F)^{\hat{r}}\right)\right)$, where $\hat{r} := (r_1, \ldots, r_n, 1)$, $\mathcal{M}(\cdot)$ denotes* **mixed volume** *[BZ88, DGH98] (normalized so that $\mathcal{M}(\mathrm{Conv}(\{\mathbf{O}, e_1, \ldots, e_n\}), \ldots, \mathrm{Conv}(\{\mathbf{O}, e_1, \ldots, e_n\})) = 1$), and $e_i$ is the $i^{\underline{\mathrm{th}}}$ standard basis vector of $\mathbb{R}^n$.* ■

**Remark 5** *For convenience, we will use the notation* $\mathrm{Newt}_p$ *in place of* $\widehat{\mathrm{Newt}}$ *when the underlying valuation is* $\mathrm{ord}_p$*.* $\diamond$

**Example 3** *Consider, 3-adically, the following 8-sparse $2 \times 2$ system over $\mathbb{Q}$:*

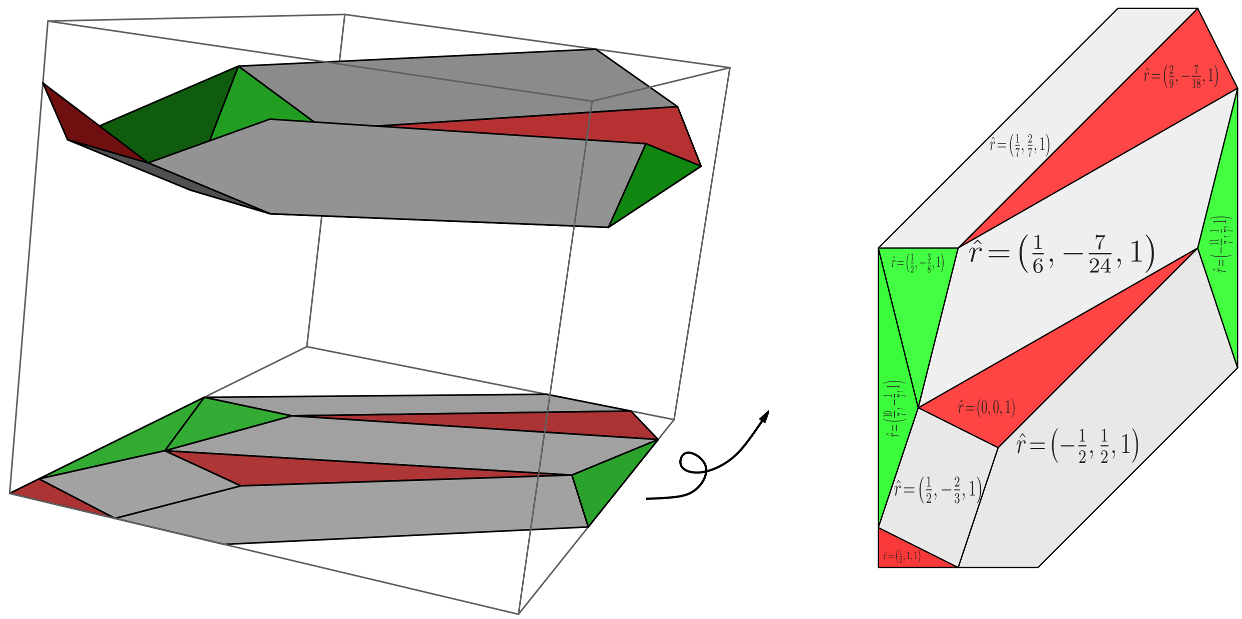
$$f_1(x,y) := 3 + 16x^2 + 7y + 10x^7y^5 + 48x^6y^7$$

$$f_2(x,y) := -48 + 45x^2 - 18y^7 - 49xy^3 + 6x^2y^7$$

*Rather than work with the individual 3-adic Newton polytopes of $F$, it is sometimes convenient to instead work with the* **Minkowski sum**

$$Q := \mathrm{Newt}_3(f_1) + \mathrm{Newt}_3(f_2) := \{q_1 + q_2 \mid q_i \in \mathrm{Newt}_3(f_i) \textit{ for all } i\}.$$

*It is then easily checked that $\mathcal{M}\left(\pi\left(\mathrm{Newt}_3(F)^{\hat{r}}\right)\right) > 0 \Longrightarrow \hat{r}$ is an inner normal of a facet of $Q$ (e.g., via [DGH98, Prop. 2]). So we can use the projections of these facets under $\pi$ to keep track of which valuation vectors are possible for our $F$. In particular, we can illustrate the lower hull of $Q$ and the projections of its facets as follows:*




*Recalling that a vertical segment of length $a$ and a polygon with horizontal width $b$ have mixed area $ab$ (see, e.g., [BZ88, Ch. 4, Sec. 19.4]), one then sees that there are exactly 4 values of $\hat{r}$ for which $\mathcal{M}\left(\pi\left(\mathrm{Newt}_3(F)^{\hat{r}}\right)\right)>0$: $\hat{r}\in\left\{\left(-\frac{1}{2},\frac{1}{2},1\right),\left(\frac{1}{7},\frac{2}{7},1\right),\left(\frac{1}{6},-\frac{7}{24},1\right),\left(\frac{1}{2},-\frac{2}{3},1\right)\right\}$. Also, the corresponding values of $\mathcal{M}\left(\pi\left(\mathrm{Newt}_3(F)^{\hat{r}}\right)\right)$ are 20, 7, 24, and 12. So by Smirnov's Theorem, there are no more than 63 geometrically isolated roots of $F$ in $(\mathbb{C}_3^*)^2$. (Note that the classical Bézout's Theorem gives an upper bound of $13\cdot 9=117$.) Furthermore, any such geometrically isolated root must have valuation vector in $\left\{(-\frac{1}{2},\frac{1}{2}),(\frac{1}{7},\frac{2}{7}),(\frac{1}{6},-\frac{7}{24}),(\frac{1}{2},-\frac{2}{3})\right\}$, and the number of geometrically isolated roots with one of these valuation vectors is no more than 20, 7, 24, or 12, respectively.* $\diamond$

**Remark 6**

1. *The number of possible distinct valuation vectors for a geometrically isolated root of an $n$-variate polynomial system $F$ can thus be combinatorially bounded from above as a function depending solely on $n$ and the number of exponent vectors (cf. Section 3).*

2. *The number of geometrically isolated roots of $F$ in $(\mathbb{C}_p^*)^n$ with given valuation vector thus depends on the support and coefficients of $F$ — not just on the number of exponent vectors.*

3. *It is thus only the* **lower** *faces of the $p$-adic Newton polytopes that matter in counting geometrically isolated roots or valuation vectors thereof.* $\diamond$

We prove Theorem 2 in Section 5. A bit earlier, in Sections 3 and 4, we respectively prove the local and global cases of Theorem 1. However, let us first point out some connections between our results, non-Archimedean amoebae [Kap00], and algorithmic complexity theory [Pap95, Roj00a, Roj01a].

**Remark 7** *Mixed volumes in arbitrary dimensions can be computed by various practical and freely downloadable software implementations, e.g., those by Ioannis Z. Emiris, Birk Huber, Tien-Yien Li, or Jan Verschelde, easily accessible via a search on* `www.google.com` *. One should also be aware that although the Minkowski sum of the* $\mathrm{Newt}_p(f_i)$ *is a useful conceptual device for* $n \leq 3$*, it is almost never used for computing mixed volumes in practice: one usually works with* $n$*-tuples of edges of the* $\mathrm{Newt}_p(f_i)$. $\diamond$

# 2 Applications to Complexity and Connections to Amoebae

Thanks to our results, we now know in particular that the maximum number of geometrically isolated rational roots of any polynomial system over $\mathbb{Q}$ depends polynomially on the number of distinct exponent vectors, provided the number of variables is fixed. Here we point out that similar but looser bounds are possible relative to an even smaller computational invariant called **additive complexity**. Furthermore, we will see that new separations of complexity classes (closely related to **P** and **NP**) will occur if these alternative bounds can be sharpened sufficiently.

We also point out an alternative perspective on Smirnov's Theorem via the recent idea of non-Archimedean amoebae.

## 2.1 Few Integral Roots Implies a Separation

Instead of expansions into monomial terms (a.k.a. the **sparse encoding**), let us consider the **straight-line program (SLP) encoding** for a univariate polynomial [BCSS98, Sec. 7.1]: That is, suppose we have $f \in \mathbb{Z}[x_1]$ expressed as a sequence of the form $(1, x_1, q_2, \ldots, q_N)$, where $q_N = f$ and for all $i \geq 2$ we have that $q_i$ is a sum, difference, or product of some pair of elements $(q_j, q_k)$ with $j, k < i$. Let $\tau(f)$ denote the smallest possible value of $N-1$, i.e., the smallest length for such a computation of $f$. Clearly, $\tau(f)$ is no more than the number of monomial terms of $f$, and is often dramatically smaller.

**The Shub-Smale $\boldsymbol{\tau}$-Theorem** *[BCSS98, Thm. 3, Pg. 127] Suppose there is an absolute constant* $\kappa$ *such that for all nonzero* $f \in \mathbb{Z}[x_1]$*, the number of distinct roots of* $f$ *in* $\mathbb{Z}$ *is no more than* $(\tau(f)+1)^\kappa$*. Then* $\mathbf{P}_{\mathbb{C}} \neq \mathbf{NP}_{\mathbb{C}}$. $\blacksquare$

In other words, an analogue (regarding complexity theory over $\mathbb{C}$) of the famous unsolved $\mathbf{P} \stackrel{?}{=} \mathbf{NP}$ question from computer science (regarding complexity theory over the ring $\mathbb{Z}/2\mathbb{Z}$) would be settled. The question of whether $\mathbf{P}_{\mathbb{C}} \stackrel{?}{=} \mathbf{NP}_{\mathbb{C}}$ remains open as well but it is known that $\mathbf{P}_{\mathbb{C}} = \mathbf{NP}_{\mathbb{C}} \implies \mathbf{NP} \subseteq \mathbf{BPP}$. (This observation is due to Steve Smale and was first published in [Shu93].) The complexity class **BPP** is central in randomized complexity and the last inclusion, while widely disbelieved, is also an open question. (It should also be noted that computer scientists currently believe that **BPP** (not **P**) is the complexity class that truly captures what we can compute. Indeed, it is a basic fact that $\mathbf{BPP} \supseteq \mathbf{P}$ and there is even suspicion that $\mathbf{P} = \mathbf{BPP}$ [IW97].) The implications of $\mathbf{P}_{\mathbb{C}} \neq \mathbf{NP}_{\mathbb{C}}$ for classical complexity are still not clear. However, there are results implying that the truth of $\mathbf{P}_{\mathbb{C}} \neq \mathbf{NP}_{\mathbb{C}}$ would provide some evidence that $\mathbf{P} \neq \mathbf{NP}$ [Koi96, Roj03a].

The truth of the hypothesis of the $\tau$-theorem, also know as the **$\tau$-conjecture**, is yet another open problem, even for $\kappa = 1$. Note however that the $\tau$-conjecture fails for $\kappa < 1$: the polynomial $(x-2)(x-2^2)\cdots(x-2^{2^j})$ clearly has $j+1$ integral roots but SLP complexity $O(j)$.

A reasonable but unsuccessful approach toward the $\tau$-conjecture would be to use the obvious embedding of $\mathbb{Z}$ in $\mathbb{R}$, because over $\mathbb{R}$ there are already results in this direction for univariate polynomials involving an even sharper encoding: For any $f \in \mathbb{R}[x]$, let its **additive complexity**, $\sigma(f)$, be the minimal number of additions and subtractions necessary to express $f$ as an elementary algebraic expression (involving $x$ and any real constants) with integer exponents, where the additions and subtractions in a repeated subexpression are counted only once. For example, $f(x) = (10x^{401} - (x^9+2)^{100})^{97} + 243(x^9+2)^{8736}$ has $\sigma(f) \leq 3$ (since $x^9+2$ occurs twice), and it is clear that $\tau(f) \geq 3$ (since $f(2) \geq 2^{1024}$ and $\tau(n) \geq \log_2 \log_2 n$ for all $n \in \mathbb{N}$). More generally, it is easily checked that $\sigma(f) \leq \tau(f)$ for all $f \in \mathbb{Z}[x_1]$. Remarkably, one can bound the number of non-degenerate **real** roots of $f$ solely in terms of $\sigma(f)$ [BC76, Gri82], and the best current upper bound is Jean-Jacques Risler's $(\sigma(f)+2)^{3\sigma(f)+1} 2^{\left(9\sigma(f)^2+5\sigma(f)+2\right)/2}$ [Ris85, Pg. 181, Line 6]. Unfortunately, there are examples of $f \in \mathbb{Z}[x_1]$ with $\sigma(f) = O(r)$ and at least $2^r$ real roots [Roj00a, Sec. 3, Pg. 13]. So additive complexity, at least over $\mathbb{R}$, is too efficient an encoding to be useful in settling the $\tau$-conjecture.

However, one could embed $\mathbb{Z}$ in another complete field — $\mathbb{Q}_2$ — instead. A consequence of our arithmetic fewnomial bounds here is the following bound which, while still not polynomial in $\sigma(f)$ or $\tau(f)$, is much sharper than its preceding real analogue:

**Theorem 3** *(See [Roj02, Introduction and Thm. 3].) Abusing notation slightly, let $\sigma(f)$ denote the additive complexity of any $f \in \mathbb{Q}_2[x_1] \setminus \{0\}$. Then the maximum number of geometrically isolated roots of $f$ in $\mathbb{Q}_2$ is exactly* 1 *or* 3 *(according as $\sigma(f)$ is* 0 *or* 1*), no greater than* 15, 25089, *or* 3235713 *(according as $\sigma(f)$ is* 2, 3, *or* 4*), and no greater than* $1+\sigma(f)!\sigma(f)^2(22.5)^{\sigma(f)}$ *for $\sigma(f) \geq 5$.* ■

Note that Risler's bound over $\mathbb{R}$ reduces to 4, 20736, 274877906944, 54975581388800000000, or 1263152817442294615051517715315425 28, according as $\sigma(f)$ is 0, 1, 2, 3, or 4. In particular, Theorem 3 yields the sharpest current upper bound on the number of rational and integral roots for a large class of univariate polynomials (see [Roj02] for further discussion). Extensions to multivariate systems of SLP's, as well as other $p$-adic fields and roots of bounded degree over a number field, are also included in [Roj02, Thm. 3]. We also note that the numbers in Theorem 3 above are slightly better than those appearing in the published version of [Roj02] but are derived in the updated version available from the author's web-page.

Unlike the analogous question over $\mathbb{R}$, the existence of a **lower bound exponential in $\boldsymbol{\sigma(f)}$**, on the number of 2-adic rational roots of $f$, is still open. In particular, whether the upper bound from Theorem 3 can be reduced to a quantity **polynomial** in $\sigma(f)$ is an open question of the utmost interest. Indeed, the only obstructions to reworking Theorem 1 in terms of additive complexity appear to be (a) the apparent dependence of the norms of the $p$-adic complex roots on the underlying Newton polytopes (vis-à-vis our application of Smirnov's Theorem) and (b) the unknown existence of an analogue of Theorem 2 for a sharper encoding.

## 2.2 Root Heights Can Be Exponential for the Multivariate Case

As for actually **finding** all the geometrically isolated rational roots of $F$, there is both good news and bad news: The bad news is that one can **not** have a polynomial time algorithm (relative to the sparse encoding) for $n>1$. The good news is that there **is** a polynomial time algorithm (relative to the sparse encoding) for $n=1$, and that the counter-examples for $n>1$ are very simple.

In particular, if we take $\mathcal{L}=\mathbb{Q}$ and measure the input size simply as the number of digits needed to write the coefficients **and** exponents of $F$ in, say, binary; then it possible for a geometrically isolated rational root of $F$ to have bit size exponential in the bit size of $F$. (The bit size of an integer is thus implicitly the number of digits in its binary expansion, and the bit size of a rational number can be taken as the maximum of the bit sizes of its numerator and denominator, written in lowest terms.) For instance, consider $k=n=2$, $\mu=4$, and $F:=(x_1-x_2^D, x_2-2)$. This particular example clearly has bit size $O(\log D)$ but its one rational root $(2^D, 2)$ has a first coordinate of bit size $D$ — exponential in the bit size of $F$. Thus one can't even write the output in polynomial time relative to the sparse encoding.

On the other hand, it is a fortunate accident that the **absolute logarithmic height** of a complex root of $F$ of degree $\leq\delta$ over $\mathcal{L}$ is polynomial in the bit size of $F$ for $n=1$ and $\mathcal{L}$ a number field [Len99a, Prop. 2.3]. This is what permits a clever polynomial time algorithm that finds the roots of $F$ of degree $\leq\delta$ over $\mathcal{L}$ when $n=1$ and $\mathcal{L}$ and $\delta$ are fixed [Len99a, first theorem]. (Lenstra's algorithm has complexity exponential in $\delta$ and the degree of $\mathcal{L}$ over $\mathbb{Q}$, but is considerably faster than the well-known Lenstra-Lenstra-Lovasz factoring algorithm [LLL82]: the latter algorithm would only solve $x^D+ax+b=0$ over the rationals in time **exponential** in $\log D$.) For $n>1$ it thus appears that the only way to achieve a polynomial time algorithm would be to allow a more efficient encoding of the output than expanding into digits. In particular, it is an open question, even for $n=2$, whether one can always find **SLP's** of length polynomial in the bit size of $F$ for the geometrically isolated rational roots of $F$.

Alternatively, one can simplify the question of solving and ask how many geometrically isolated rational roots $F$ has, or whether $F$ has any geometrically isolated rational roots at all. This was addressed in [Roj01a, Thms. 1.3 and 1.4] where it was shown that the truth of the Generalized Riemann Hypothesis implies that detecting a strong form of **non**-solvability over the rationals (transitivity of the underlying Galois group) can be done within the complexity class $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$, provided the underlying complex zero set is finite. In the latter result, $n$ is allowed to be part of the input and can thus vary.

## 2.3 Skinny Amoebae Versus Subdivisions

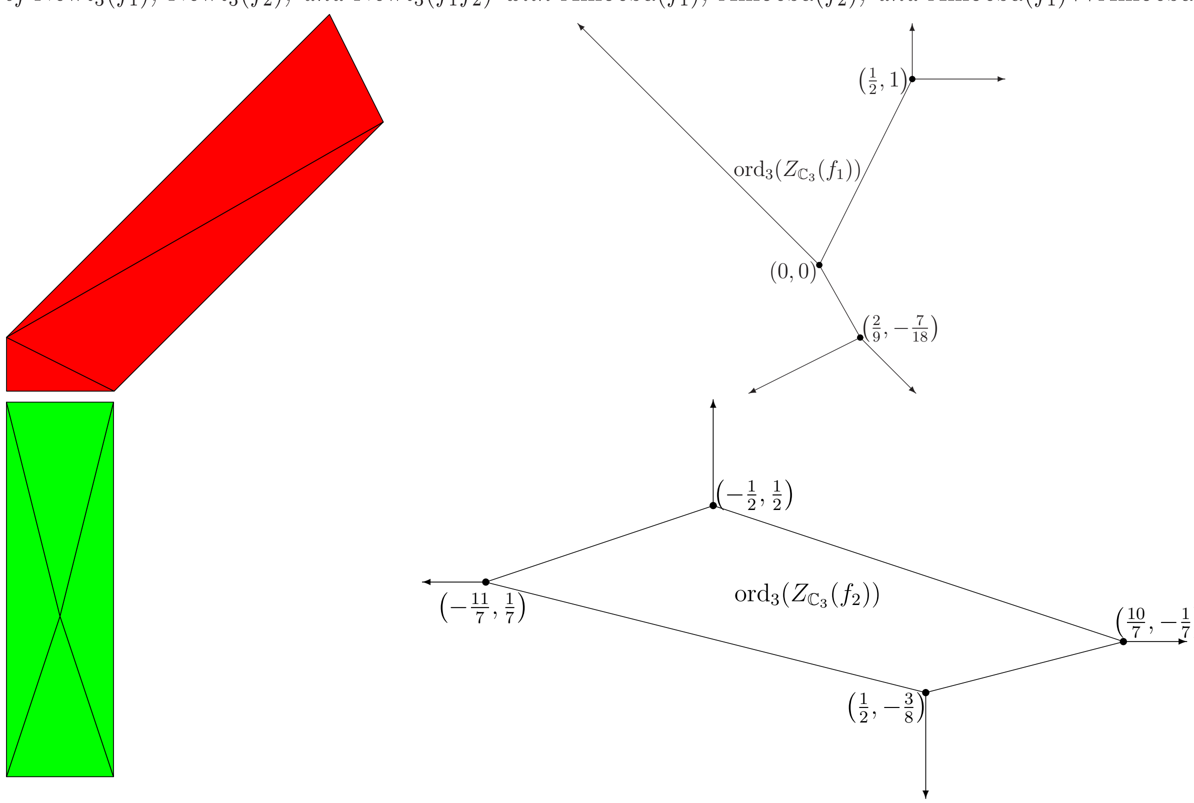
Here we briefly illustrate an alternative, arguably simpler point of view for Smirnov's Theorem. Mikhail M. Kapranov's idea of **non-Archimedean Amoebae** gives an elegant combinatorial description of the valuation vectors determined by a single algebraic hypersurface over any algebraically closed field with a (rational) non-Archimedean valuation. So, to some extent, we can substitute the polyhedral subdivisions from Section 1.1 with an intersection of piecewise linear hypersurfaces in $\mathbb{R}^n$. This approach leads to a much simpler proof of Smirnov's Theorem and is detailed further in [Roj03b].

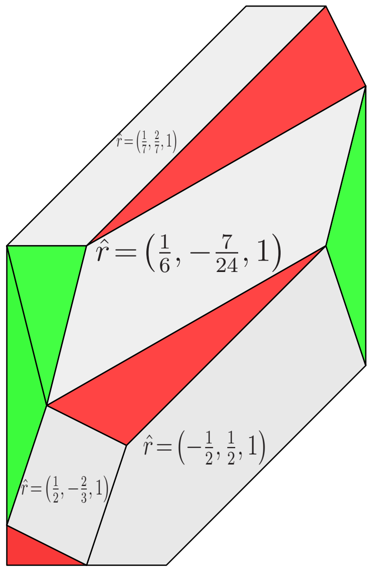
**Definition 3** *Given a polytope $Q \subseteq \mathbb{R}^n$, its* **(inner) normal fan**, $\mathrm{Fan}(Q)$, *is the collection of cones defined by the (inner) normals of the faces of $Q$. The* **codimension 1 skeleton of** $\mathrm{Fan}(Q)$, *denoted* $\mathrm{Fan}^1(Q)$, *is then simply the union of all the cones of* $\mathrm{Fan}(Q)$ *corresponding to the edges of $Q$. Also, following the notation of Definition 1, we call the projected intersection $\pi\left(\mathrm{Fan}^1(Q) \cap \{x_{n+1}=1\}\right)$ the* **amoeba of $Q$**. *Finally, for any algebraically closed field $K$ with a discrete valuation and any polynomial $f \in K[x_1, \ldots, x_n]$, the* **amoeba of $f$**, $\mathrm{Amoeba}(f)$, *is then simply the amoeba of* $\widehat{\mathrm{Newt}}(f)$. $\diamond$

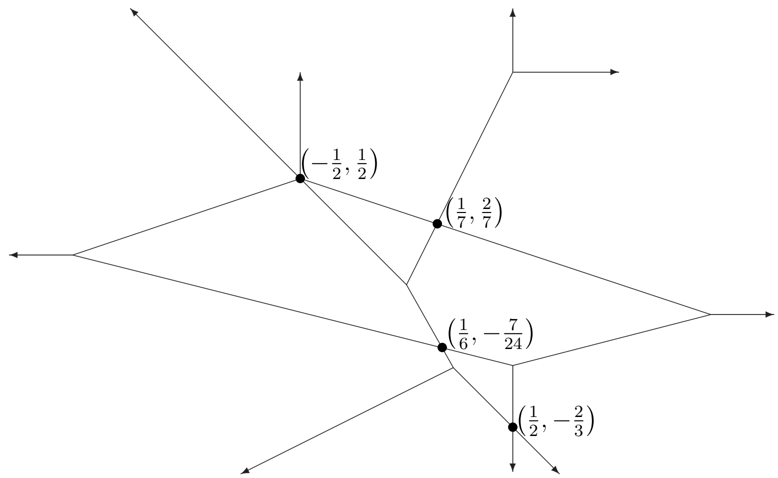
We note that in [Kap00], the amoeba of $f$ was defined via a Legendre transform (a.k.a. support function [Zie95]) of the lower hull of $\widehat{\mathrm{Newt}}(f)$. It is easy to see that both defintions are equivalent.

**Kapranov's Non-Archimedean Amoeba Theorem** *[Kap00] Following the notation above,* $\mathrm{ord}(K) \subseteq \mathbb{Q} \Longrightarrow \mathrm{ord}(Z_K(f) \cap (K^*)^n) = \mathrm{Amoeba}(f) \cap \mathrm{ord}(K)^n$. ■

**Example 4** *Returning to Example 3 of Section 1.1, let us compare the projected lower hulls of* $\mathrm{Newt}_3(f_1)$, $\mathrm{Newt}_3(f_2)$, *and* $\mathrm{Newt}_3(f_1 f_2)$ *with* $\mathrm{Amoeba}(f_1)$, $\mathrm{Amoeba}(f_2)$, *and* $\mathrm{Amoeba}(f_1) \cap \mathrm{Amoeba}(f_2)$*:*








*We thus see that the allowable valuation vectors for the geometrically isolated roots of $F$ in $(\mathbb{C}_3^*)^2$ are contained in the intersection of two piecewise linear curves.* $\diamond$

**Remark 8** *Note that although amoebae provide an elegant conceptual simplification, the assignment of correct multiplicities to amoebic intersections still requires some additional combinatorial work in general: simply consider any $F$ with $\dim \mathbb{Z}_{\mathbb{C}_p}(F)=0$, $\widehat{\mathrm{Newt}}(f_1)=\cdots=\widehat{\mathrm{Newt}}(f_n)$, and $n\geq 2$. For example, the 3-adic amoebae of $x+y-1$ and $2x+4y-8$ are* **identical***, one-dimensional, and thus fail to predict the sole valuation vector of $Z_{\mathbb{C}_3}(x+y-1,2x+4y-8)=\{(-2,3)\}$.* $\diamond$

# 3 Proving the Local Case of Theorem 1

Here we will assume that $\mathcal{L}$ is any degree $d$ algebraic extension of $\mathbb{Q}_p$. The following lemma will help us reduce to the case $k=n$.

**Lemma 1** *Suppose $F:=(f_1,\ldots,f_k)$ is any $k\times n$ polynomial system over $\mathcal{L}$ with $k>n$ and let $D$ be the maximum of the degrees of the $f_i$ and $S\subseteq\mathbb{Z}$ any set of cardinality greater than $kD^n$. Then there is an $n\times k$ matrix $[a_{ij}]$ with entries in $S$ such that*
*$G:=(a_{11}f_1+\cdots+a_{1k}f_k,\ldots,a_{n1}f_1+\cdots+a_{nk}f_k)\Longrightarrow[Z_{\mathbb{C}_p}(F)\subseteq Z_{\mathbb{C}_p}(G)$ and $Z_{\mathbb{C}_p}(G)\setminus Z_{\mathbb{C}_p}(F)$ is finite].*

**Proof:** The analogous statement where one works with roots of $F$ in $\mathbb{C}^n$ instead follows easily from the first assertion of [GH93, Sec. 3.4.1, Pg. 233] and the development there. The proof there only makes use of the fact that $\mathbb{C}$ is algebraically closed, and thus applies to the case at hand over $\mathbb{C}_p$. ■

We will also need the following basic fact on the roots of sparse polynomial systems over most infinite fields.

**Lemma 2** *Suppose $F$ is a $\mu$-sparse $k\times n$ polynomial system over a field $\mathcal{L}$ with an embedded copy of $\mathbb{Z}$ and let $\mathcal{G}(\mathcal{L},\mu,k,n)$ denote the maximum number of geometrically isolated roots in $\mathcal{L}^n$ of such an $F$. Then $[k<n$ or $\mu\leq n]\Longrightarrow\mathcal{G}(\mathcal{L},\mu,k,n)=0$. Also,*

*$\mathcal{G}(\mathcal{L},\mu,k,n) \leq \mathcal{G}(\mathcal{L},(\mu_1,\ldots,\mu_n))$, where $\mu_1,\ldots,\mu_n \leq \mu-n+1$ and $\mathcal{G}(\mathcal{L},(m_1,\ldots,m_n))$ denotes the maximum number of geometrically isolated roots in $\mathcal{L}^n$ of an $n\times n$ polynomial system of type $(m_1,\ldots,m_n)$ over $\mathcal{L}$.*

**Proof:** By [Har77, Affine Dimension Theorem, Prop. 7.1, Pg. 48], $k<n \Longrightarrow Z_{\overline{\mathcal{L}}}(F)$ is positive-dimensional; so it is clear that there are no geometrically isolated roots whatsoever when $k<n$. As for the case $\mu \leq n$, one easily obtains by Gauss-Jordan elimination that $F$ is equivalent to either a system of type $(1,\ldots,1)$ or a system of $k'$ equations in $>k'$ monomials. So the first part of our lemma follows, employing a monomial change of variables in the latter case of our reduction (cf. Section 3.1).

To prove the second assertion, note that we can now assume that $k\geq n$. In the event that $k>n$, Lemma 1 allows us to replace $F$ by a new $n\times n$ polynomial system (with no new exponent vectors) which has at least as many geometrically isolated roots as our original $F$. In fact, by basic linear algebra again (and since $\mathbb{Z}\hookrightarrow\mathcal{L}$ by assumption), we can assume that our new system still has exactly $\mu$ distinct exponent vectors. So we can assume $k=n$.

To conclude, we need only apply another round of Gauss-Jordan elimination to obtain a new system, equivalent to $F$, with $\leq\mu-n+1$ exponent vectors in each of its polynomials. ■

Finally, we will need the following result characterizing when mixed volumes vanish.

**Lemma 3** *[DGH98, Prop. 2]*
*Given polytopes $P_1,\ldots,P_n\subset\mathbb{R}^n$, we have $\mathcal{M}(P_1,\ldots,P_n)>0 \Longleftrightarrow$ there are linearly independent vectors $v_1,\ldots,v_n$ with $v_i$ parallel to an edge of $P_i$ for each $i$.* ■

**Proof of the Local Case of Theorem 1:** The first portion follows immediately from Lemma 2. In particular, we can assume henceforth that $k=n$, $\mu\geq n+1$, and (if desired) that $F$ is of type $(m_1,\ldots,m_n)$ where $m_1,\ldots,m_n\leq\mu-n+1$.

Lemma 3 then tells us that $\mathcal{M}\left(\pi\left(\mathrm{Newt}_p(F)^{\hat{r}}\right)\right)>0 \Longleftrightarrow$ there are linearly independent vectors $v_1,\ldots,v_n$, with $v_i$ parallel to an edge of $\mathrm{Newt}_p(f_i)^{\hat{r}}$ for all $i$. So let $\lambda_i$ be the number of lower edges of $\mathrm{Newt}_p(f_i)$. Clearly then, there are no more than $\lambda_1\cdots\lambda_n$ possible values for an $r\in\mathbb{R}^n$ with $\hat{r}=(r,1)$ and $\mathcal{M}\left(\pi\left(\mathrm{Newt}_p(F)^{\hat{r}}\right)\right)>0$, so let us now find explicit upper bounds on the $\lambda_i$.

If $n=1$ then we clearly have $\lambda_1\leq\mu-1$, and this is a sharp bound for all $\mu$. If $n\geq 3$ then we have the obvious bound of $\lambda_i\leq\mu(\mu-1)/2$ for all $i$, and it is not hard to generate examples showing that this bound is sharp for all $\mu$ as well [Ede87, Thm. 6.5, Pg. 101]. If $n=2$ then note that the number of edges of $\mathrm{Newt}_p(f_i)$ is clearly not decreased if we triangulate the boundary of $\mathrm{Newt}_p(f_i)$. Since each edge of the resulting complex is incident to exactly two 2-faces, Euler's relation [Ede87, Thm. 6.8, Pg. 103] then immediately implies that $\lambda_i\leq 3\mu-6$ for all $i$, which is easily seen to be sharp for all $\mu\geq 3$.

Having an explicit upper bound on $\lambda_1\cdots\lambda_n$, Smirnov's Theorem then tells us that we immediately obtain an explicit upper bound on the number of possible valuation vectors of a geometrically isolated root of $F$ in $(\mathbb{C}_p^*)^n$. To see that $u(\mu,n)$ serves as an upper bound on the number of valuation vectors as well, simply recall that $F$ could also be modified to have at least $n-1$ fewer monomial terms in each of its polynomials, thanks to Lemma 2.

So let us now temporarily fix $(r_1,\ldots,r_n):=r$ and see how many roots of $F$ in $(\mathcal{L}^*)^n$ can have valuation vector $r$. Following the notation of Theorem 2, let $R_p:=\{x\in\mathbb{C}_p \mid |x|_p\leq 1\}$ be the ring of algebraic integers of $\mathbb{C}_p$, let $M_p:=\{x\in\mathbb{C}_p \mid |x|_p<1\}$ be the unique maximal ideal of $R_p$, $\mathbb{F}_{\mathcal{L}} := (R_p \cap \mathcal{L})/(M_p \cap \mathcal{L})$, and let $\rho$ be any generator of the principal ideal $M_p \cap \mathcal{L}$ of $R_p \cap \mathcal{L}$. Also let $e_{\mathcal{L}} := \max_{y \in \mathcal{L}^*} \{|\mathrm{ord}_p y|^{-1}\}$ and $q_{\mathcal{L}} := \#\mathbb{F}_{\mathcal{L}}$. (The last two quantities are respectively known as the **ramification degree** and **residue field cardinality** of $\mathcal{L}$, and satisfy $e_{\mathcal{L}}, \log_p q_{\mathcal{L}} \in \mathbb{N}$ and $e_{\mathcal{L}} \log_p q_{\mathcal{L}} = d$ [Kob84, Ch. III].) Since $\mathrm{ord}_p \rho = 1/e_{\mathcal{L}}$, it is clear that $r$ a valuation vector of a root of $F$ in $(\mathcal{L}^*)^n \Longrightarrow r \in \left(\frac{1}{e_{\mathcal{L}}}\mathbb{Z}\right)^n$.

Fixing a set $A_{\mathcal{L}} \subset R_p$ of representatives for $\mathbb{F}_{\mathcal{L}}$ (i.e., a set of $q_{\mathcal{L}}$ elements of $R_p \cap \mathcal{L}$, exactly **one** of which lies in $M_p$, whose image mod $M_p \cap \mathcal{L}$ is $\mathbb{F}_{\mathcal{L}}$), we can then write any $x_i \in \mathcal{L}$ uniquely as $\sum\limits_{j=e_{\mathcal{L}} r_i}^{+\infty} a_j^{(i)} \rho^j$ for some sequence of $a_j^{(i)} \in A_{\mathcal{L}}$ [Kob84, Corollary, Pg. 68]. Note in particular that $\frac{x_i}{a^{(i)} \rho^{e_{\mathcal{L}} r_i}}$ thus lies in $R_p \setminus M_p$ for any $a^{(i)} \in A_{\mathcal{L}} \setminus M_p$.

Let $r_{\mathcal{L}} := (\underbrace{1/e_{\mathcal{L}}, \ldots, 1/e_{\mathcal{L}}}_{n})$. Theorem 2 then implies that the number of geometrically isolated roots $(x_1, \ldots, x_n) \in (\mathbb{C}_p^*)^n$ of $F$ satisfying

$$(\mathrm{ord}_p x_1, \ldots, \mathrm{ord}_p x_n) = r \textbf{ and } \frac{x_1}{a^{(1)} \rho^{e_{\mathcal{L}} r_1}} \equiv \cdots \equiv \frac{x_n}{a^{(n)} \rho^{e_{\mathcal{L}} r_n}} \equiv 1 \ (\textbf{mod } M_p)$$

is no more than $C_p((\underbrace{\mu - n + 1, \ldots, \mu - n + 1}_{n}), [n]^n, r_{\mathcal{L}})$. Furthermore, since $M_p \cap \mathcal{L} \subset M_p$, we obtain the same statement if we restrict to roots in $(\mathcal{L}^*)^n$ and use congruence **mod** $M_p \cap \mathcal{L}$ instead.

Since there are $q_{\mathcal{L}} - 1$ possibilities for each $a_0^{(i)}$, our last observation tells us that the number of geometrically isolated roots $(x_1, \ldots, x_n) \in (\mathcal{L}^*)^n$ of $F$ satisfying $(\mathrm{ord}_p x_1, \ldots, \mathrm{ord}_p x_n) = r$ is no more than $(q_{\mathcal{L}} - 1)^n C_p((\underbrace{\mu - n + 1, \ldots, \mu - n + 1}_{n}), [n]^n, r_{\mathcal{L}})$. So the total number of geometrically isolated roots of $F$ in $(\mathcal{L}^*)^n$ is no more than

$$u(\mu, n)(q_{\mathcal{L}} - 1)^n C_p((\underbrace{\mu - n + 1, \ldots, \mu - n + 1}_{n}), [n]^n, r_{\mathcal{L}}).$$

Since $e_{\mathcal{L}} \leq d$ and $q_{\mathcal{L}} \leq p^d$, an elementary calculation yields our desired bound. ■

A simple consequence of our last proof is that, when $k = n$, there is a natural injection of the set of possible valuation vectors of the geometricaly isolated roots of $F$ into the set of $n$-tuples of the form $(E_1, \ldots, E_n)$ where $E_i$ is an edge of $\mathrm{Newt}_p(f_i)$ for all $i$. So, noting that we could have also left the supports of $F$ unchanged and applied the second bound from Theorem 2 instead when $k = n$, we also clearly have the following improved bound.

**Corollary 1** *Following the notation above, $k = n$ implies an improved bound of*

$$B(\mathcal{L}, \mu, n) \leq \boldsymbol{\Lambda(F)(q_{\mathcal{L}} - 1)^n \min\left\{C_p(\overline{m}, \overline{N}, r_{e_{\mathcal{L}}}), C_p((\underbrace{\mu - n + 1, \ldots, \mu - n + 1}_{n}), [n]^n, r_{e_{\mathcal{L}}})\right\}},$$

*where $\Lambda(F) = \min\{u(\mu, n), \prod_{i=1}^n \lambda_i\}$, $\lambda_i$ is the number of lower edges of $\mathrm{Newt}_p(f_i)$, $C_p(\overline{m}, \overline{N}, r)$ is as defined in Theorem 2, $r_e := (\underbrace{1/e, \ldots, 1/e}_{n})$, and $q_{\mathcal{L}}$ and $e_{\mathcal{L}}$ are respectively the residue field cardinality and ramification index of $\mathcal{L}$.* ■

**Remark 9** *Returning to Example 1, observe that* $\mathrm{Newt}_2(f_1)$ *has* $\leq 3$ *edges and that* $\mathrm{Newt}_2(f_2)$ *has* $\leq 3(m-2)$ *edges (cf. our use of Euler's formula in the proof of the local case of Theorem 1). So we in fact have* $\Lambda(F) \leq 9(m-2)$ *for all* $m \geq 3$*. Corollary 1 then implies an improved upper bound of* $\mathbf{456(m-1)(m-2)\left(1+\log_2\left(\frac{m-1}{0.693}\right)\right)}$ *for the number of roots of* $F$ *in* $(\mathbb{Q}_2^*)^2$*, e.g.,* **2304** *when* $m=3$*. Note that our refined bound is smaller than the real analytic bound of* $4(2^m-2)$ *(cf. Remark 2 of Section 1) for all* $m \geq 18$*, where the two bounds begin to exceed* 695000. ⋄

**Example 5** *It is entirely possible that the maximum number of geometrically isolated roots in* $(\mathcal{L}^*)^n$ *of a* $\mu$*-sparse* $n \times n$ *polynomial system over* $\mathcal{L}$ *is actually* **larger** *for* $\mathcal{L}=\mathbb{Q}_2$ *than for* $\mathcal{L}=\mathbb{R}$*, for* **small** $\mu$ *and* $n$*. In particular, a univariate trinomial over* $\mathbb{R}$ *clearly has at most* 4 *roots in* $\mathbb{R}^*$*. However,* $3x_1^{10}+x_1^2-4$ *has exactly* 6 *roots in* $\mathbb{Q}_2^*$ *and this is the maximum possible for univariate trinomials over* $\mathbb{Q}_2$ *[Len99b, Prop. 9.2].* ⋄

**Remark 10** *It is easily checked that* $B(\mathcal{L},2,1)$ *is exactly the number of roots of unity in* $\mathcal{L}$*. Lenstra, in an example after Proposition 7.2 of [Len99b], has observed that the latter number in turn is* $(q_{\mathcal{L}}-1)p^{s_{\mathcal{L}}}$*, where* $s_{\mathcal{L}}$ *is a non-negative integer for which* $(p-1)p^{s_{\mathcal{L}}-1}$ *divides* $e_{\mathcal{L}}$*. In particular, the quantity* $p^{s_{\mathcal{L}}}$ *is the number of roots of unity of* $\mathcal{L}$ *that have order a* $p^{\underline{\text{th}}}$ *power [Len99b, final remark].* ⋄

## 3.1 Simpler Sharper Bounds

Before moving on to the global case of Theorem 1, let us point out two simpler and sharper bounds for $B(\mathcal{L},\mu,n)$ when $F$ is of a very special form.

First, defining $x^A := (x_1^{a_{11}}\cdots x_n^{a_{n1}},\ldots,x_1^{a_{1n}}\cdots x_n^{a_{nn}})$, it is easy to see that $x^{AB}=(x^A)^B$ for any $n\times n$ matrices $A=[a_{ij}]$ and $B$ with integer entries. We call the map $x\mapsto x^A$ a **monomial change of variables** and it is easy to see the following:
[The function $m_A(x):=x^A$ is an automorphism of $(\mathcal{L}^*)^n$ and has inverse $m_{A^{-1}}(x)=x^{A^{-1}}$ with all exponents **integral**] $\Longleftrightarrow$ $\det A=\pm 1$.
Let us also call any collection $L_1 \subsetneq \cdots \subsetneq L_n=\mathbb{Q}^n$ of $n$ subspaces of $\mathbb{Q}^n$, with $\dim L_i=i$ for all $i$, a **complete flag**. Note that any integral polytope $Q\subseteq\mathbb{R}^n$ naturally generates a subspace of $\mathbb{Q}^n$ via the set of linear combinations of all differences of its vertices.

It is then clear that the well-known **Hermite factorization** of integer matrices (see, e.g., [Smi61], [Jac85, Ch. 3.7], or [vdK00]) implies that the Newton polytopes of $F$ generate a complete flag iff [$k=n$ and there is an invertible monomial change of variables and a permutation $\sigma$ of $[n]$, such that $f_{\sigma(i)}(x^A)\in\mathcal{L}[x_1,\ldots,x_i]$ for all $i$]. We call such an $F$ **pyramidal** [LRW03, Dfn. 4]. Note also that if $\mu=n+1$, a simple application of Gauss-Jordan elimination will either immediately reduce $F$ to a **binomial** system (i.e., a system of type $(2,\ldots,2)$) or a system of $k'$ equations in $>k'$ monomials. The following refined formula is then immediate.

**Proposition 1** *Following the notation of Theorem 1 and Corollary 1, restricting to* $\mu=n+1$ *or pyramidal* $F$ *respectively yields* $\boldsymbol{B(\mathcal{L},\mu,n)=B(\mathcal{L},2,1)^n}$ *and* $\boldsymbol{B(\mathcal{L},\mu,n)=\prod_{i=1}^n B(\mathcal{L},m_i,1)}$*.* ■

**Example 6** *Taking* $m=2$ *in Example 1 makes* $F$ *at worst* 4*-sparse and* $2\times 2$*, and Theorem 1 thus implies that* $F$ *has no more than* 2304 *geometrically isolated roots in* $(\mathbb{Q}_2^*)^2$*. Corollary 1 gives us an upper bound of* 231*. However, Proposition 1 (along with the bound*

*$B(\mathbb{Q}_2, 2, 1) \leq 2$ (cf. Theorem 1) and the equality $B(\mathbb{Q}_2, 3, 1) = 6$ [Len99b, Prop. 9.2]) implies a sharp bound of* **12***. In particular, note that $F := (3x_1^{10} + x_1^2 - 4, x_2^2 - 1)$ has exactly 12 roots in $(\mathbb{Q}_2^*)^2$ (cf. Example 5), and that the corresponding optimal bound over $(\mathbb{R}^*)^2$ would instead be 8 [LRW03, Thm.3].* $\diamond$

**Example 7** *Let $F$ be any $n \times n$ binomial system over $\mathbb{Q}_2$. Then our pyramidal bound from Proposition 1 is exactly $2^n$, while the upper bound from Corollary 1 is $(c(1-\log_2 \log 2)n)^n \geq (2.418 \cdot n)^n$.* $\diamond$

Now let $\mathrm{Newt}(f_i) := \mathrm{Conv}(\mathrm{Supp}(f_i))$ denote the **Newton polytope of $f_i$ with respect to the trivial valuation**, and set $\mathrm{Newt}(F) := (\mathrm{Newt}(f_1), \ldots, \mathrm{Newt}(f_n))$. Note that this kind of Newton polytope, for an $n$-variate polynomial, lies in $\mathbb{R}^n$ instead of $\mathbb{R}^{n+1}$.

**Proposition 2** *Following the notation of Theorem 1 and Corollary 1, restricting to $F$ with $\mathcal{M}(\mathrm{Newt}(F)) = 0$ yields $\boldsymbol{B(\mathcal{L}, \mu, n) = 0}$.* ■

The proposition of course follows from the fact that there are no roots in $(\mathbb{C}_p^*)^n$ at all for such $F$, which in turn is an immediate consequence of the monotonicity of mixed volume with respect to containment [BZ88] and Smirnov's Theorem.

**Remark 11** *Note that the hypotheses for the two preceding refined bounds can in fact be checked within a number of arithmetic operations polynomial in $\mu$ and $n$: For the pyramidal bound, one can simply use Gaussian elimination to determine the dimensions of the Newton polytopes (corresponding to the trivial valuation) of $F$ and then similarly check the containments in the flag condition if necessary. For the vanishing mixed volume bound, one can use matroid intersection to check the condition from Lemma 3 within $O(\mu n^{1.616})$ arithmetic operations [Roj99a, Lem. 1]. One can even assert polynomial* **bit** *complexity as well (in $\mu$, $n$, and the bit-sizes of the exponents of $F$) for the two preceding hypothesis checks. See, e.g., [BCSS98, Sec. 15.5] and [Ili89] for further details.* $\diamond$

In closing our refinements of the local case of Theorem 1, it should be clear that one can of course combine and interweave Corollary 1 and Propositions 1 and 2 to obtain even sharper upper bounds on $B(\mathcal{L}, \mu, n)$ for various families of $F$, e.g., $F$ which, while not pyramidal, have a subsystem which is pyramidal.

# 4 Proving the Global Case of Theorem 1

Let us start with a construction from [Len99b, Sec. 8] for the univariate case: First, fix a group homomorphism $\mathbb{Q} \longrightarrow \mathbb{C}_2^*$, written $r \mapsto 2^r$, with the property that $2^1 = 2$. To construct $2^r$ for an arbitrary rational $r$, choose $2^{1/n!}$ inductively to be an $n^{\underline{\text{th}}}$ root of $2^{1/(n-1)!}$, and then define $2^{a/n!}$ to be the $a^{\underline{\text{th}}}$ power of $2^{1/n!}$ for any $a \in \mathbb{Z}$. Clearly, $\mathrm{ord}_2(2^r) = r$ for each $r \in \mathbb{Q}$. For $j, e \in \mathbb{N}$ we then define the subgroups $U_e$ and $T_j$ of $\mathbb{C}_2^*$ by $U_e := \{x \mid \mathrm{ord}_p(x-1) \geq 1/e\}$ and $T_j := \{\zeta \mid \zeta^{2^j - 1} = 1\}$. Note that $U_e \subseteq U_{e'}$ if $e \leq e'$, and $T_j \subseteq T_{j'}$ if $j$ divides $j'$.

What we now show is that in addition to having few roots in $(\mathbb{Q}_2^*)^n$, $F$ has few roots in another suprisingly large piece of $(\mathbb{C}_2^*)^n$.

**Lemma 4** *Let $e, j \in \mathbb{N}$. Also let $F$ be a $\mu$-sparse $n \times n$ polynomial system over $\mathbb{C}_2$, $m_i$ the number of exponent vectors of $f_i$, $\overline{m} := (m_1, \ldots, m_n)$, $r_e = (\underbrace{1/e, \ldots, 1/e}_{n})$, $N_i$ the set of all $j$ such that $x_j$ appears with nonzero exponent in some monomial term of $f_i$, and $\overline{N} := (N_1, \ldots, N_n)$. Then, following the notation of Theorem 2 and Corollary 1, $F$ has no more than*

$$\Lambda(F)(2^j - 1)^n \min\left\{C_2(\overline{m}, \overline{N}, r_e), C_2((\underbrace{\mu - n + 1, \ldots, \mu - n + 1}_{n}), [n]^n, r_e)\right\}$$

*geometrically isolated roots in the subgroup $(2^{\mathbb{Q}} \cdot T_j \cdot U_e)^n$ of $(\mathbb{C}_2^*)^n$.*

**Proof:** First note that the case $n = 1$, in slightly different notation, is exactly Lemma 8.2 of [Len99b]. The proof there generalizes quite easily to our higher-dimensional setting.

By Lemma 2 of Section 3, we can assume (if desired) that $F$ is of type $(m'_1, \ldots, m'_n)$ with $m'_1, \ldots, m'_n \leq \mu - n + 1$. So by Theorem 2, $F$ has no more than

$$\min\left\{C_2(\overline{m}, \overline{N}, r_e), C_2((\underbrace{\mu - n + 1, \ldots, \mu - n + 1}_{n}), [n]^n, r_e)\right\}$$

geometrically isolated roots in $U_e^n$. By the change of variables $(x_1, \ldots, x_n) \mapsto (\alpha_1 y_1, \ldots, \alpha_n y_n)$ we then easily obtain the same upper bound for the number of roots of $F$ in any coset of $U_e^n$. Since $T_j^n$ clearly has order $(2^j - 1)^n$, $F$ thus has no more than

$$(2^j - 1)^n \min\left\{C_2(\overline{m}, \overline{N}, r_e), C_2((\underbrace{\mu - n + 1, \ldots, \mu - n + 1}_{n}), [n]^n, r_e)\right\}$$

geometrically isolated roots in any coset $(2^{r_1} T_j U_e) \times \cdots \times (2^{r_n} T_j U_e)$. Smirnov's Theorem then implies, via our proofs of the local case of Theorem 1 and Corollary 1 (cf. Section 3), that a geometrically isolated root $x \in (\mathbb{C}_2^*)^n$ of $F$ can produce no more than $\Lambda(F)$ possible distinct values for $(r_1, \ldots, r_n) := (\mathrm{ord}_2 x_1, \ldots, \mathrm{ord}_2 x_n)$. So we are done. ∎

To at last prove the global case of Theorem 1, let us quote another useful result of Lenstra. Recall that $\lceil x \rceil$ is the least integer greater than $x$.

**Lemma 5** *[Len99b, Lem. 8.3] Let $n \in \mathbb{N}$ and let $L$ be a finite algebraic extension of $\mathbb{Q}_2$ of degree $\leq D$. Then there is a $j \in [D]$ such that $L^* \subseteq 2^{\mathbb{Q}} T_j U_{\lceil d/j \rceil d}$.* ∎

**Proof of the Global Case of Theorem 1:**
Since $\mathbb{Q}$ naturally embeds in $\mathbb{Q}_2$, we can assume that $\mathcal{L}$ is a subfield of $\mathbb{C}_2$ of finite degree over $\mathbb{Q}_2$. Then every root of $F$ in $(\mathbb{C}_2^*)^n$ of degree $\leq \delta$ over $\mathcal{L}$ lies in $(L'^*)^n$, where $L'$ is an extension of $\mathbb{Q}_2$ of degree at most $D := d\delta$. So by Lemma 5, any such root of $F$ also lies in $\bigcup_{j=1}^{D} (2^{\mathbb{Q}} T_j U_{\lceil D/j \rceil D})$. The first part of the global case of Theorem 1 then follows immediately from Lemma 2 of Section 3, and we can assume henceforth that $k = n$, $\mu \geq n + 1$, and (if desired) that $F$ is of type $(m'_1, \ldots, m'_n)$ where $m'_1, \ldots, m'_n \leq \mu - n + 1$.

From Lemma 4 it now follows that the number of roots of $F$ of degree $\leq\delta$ over $\mathcal{L}$ is no more than

$$\sum_{j=1}^{D} u(\mu,n)(2^j-1)^n C_2\left(\underbrace{(\mu-n+1,\ldots,\mu-n+1)}_{n},[n]^n,\left(\frac{1}{\lceil D/j\rceil D},\ldots,\frac{1}{\lceil D/j\rceil D}\right)\right).$$

Since $2^j-1\leq 2^j$ and $C_2(\mu,n,(r,\ldots,r))$ is a decreasing function of $r$, we thus obtain by geometric series that

$$A(\mathcal{L},\delta,\mu,n)\leq u(\mu,n)2^{nd\delta+1}C_2\left(\underbrace{(\mu-n+1,\ldots,\mu-n+1)}_{n},[n]^n,\left(\frac{1}{d^2\delta^2},\ldots,\frac{1}{d^2\delta^2}\right)\right).$$

So by Theorem 2 and an elementary calculation we are done. ■

By leaving the last sum in our proof above unsimplified, and noting that we could have left the supports of $F$ unchanged throughout our proof if $k=n$, we immediately obtain the following improvement of Theorem 2.

**Corollary 2** *Following the notation of Theorem 1 and Lemma 4, if $k=n$ then we have an improved bound of*

$$A(\mathcal{L},\delta,\mu,n)\leq\Lambda(F)\sum_{j=1}^{d\delta}(2^j-1)^n\min\left\{C_2\left(\overline{m},\overline{N},r_{\lceil d\delta/j\rceil d\delta}\right),C_2\left(\overline{m}(\mu,n),[n]^n,r_{\lceil d\delta/j\rceil d\delta}\right)\right\},$$

*where $\Lambda(F)$ is as defined in Corollary 1 of Section 3, $C_p(\overline{m},\overline{N},r)$ is as defined in Theorem 2, and $\overline{m}(\mu,n):=\underbrace{(\mu-n+1,\ldots,\mu-n+1)}_{n}$.* ■

To conclude, note that we can immediately give global analogues of Propositions 1 and 2 from Section 3.1. We omit the proofs since the proofs given for the local versions were in fact independent of the (infinite) field $\mathcal{L}$.

**Proposition 3** *Following the notation of Theorem 1 and Corollary 1, restricting to $\mu=n+1$ or pyramidal $F$ respectively yields $A(\mathcal{L},\delta,\mu,n)\leq A(\mathcal{L},\delta,2,1)^n$ and $A(\mathcal{L},\delta,\mu,n)\leq\prod_{i=1}^n A(\mathcal{L},\delta,m_i,1)$.* ■

**Proposition 4** *Following the notation of Theorem 1 and Corollary 1, restricting to $F$ with $\mathcal{M}(\mathrm{Newt}(F))=0$ yields $A(\mathcal{L},\delta,\mu,n)=0$.* ■

Again, just as for the local case, it should be clear that one can combine and interweave Corollary 2 and Propositions 3 and 4 to obtain even sharper upper bounds on $A(\mathcal{L},\delta,\mu,n)$ for various families of $F$.

# 5 Proving Theorem 2

Conceptually, our proof is fairly direct: We will apply Smirnov's Theorem to the shifted polynomial system $G(x_1,\ldots,x_n):=F(1+x_1,\ldots,1+x_n)$ to count how many roots of $F$ are close to $(1,\ldots,1)$. That the resulting bound is actually independent of the degrees of the $f_i$, for $n=1$, was apparently first observed by Lenstra in [Len99b, Thm. 3]. That this continues to hold for general $n$ is a bit more involved and requires some facts from convex geometry which we will summarize shortly.

However, let us first motivate our approach by seeing a simple illustration of how $C_p(\mu, n, r)$ is well-defined. Smirnov's Theorem and our earlier observations on the vanishing of mixed volume easily imply that $C_p(\mu, n, r)$ will be small provided the lower hull of

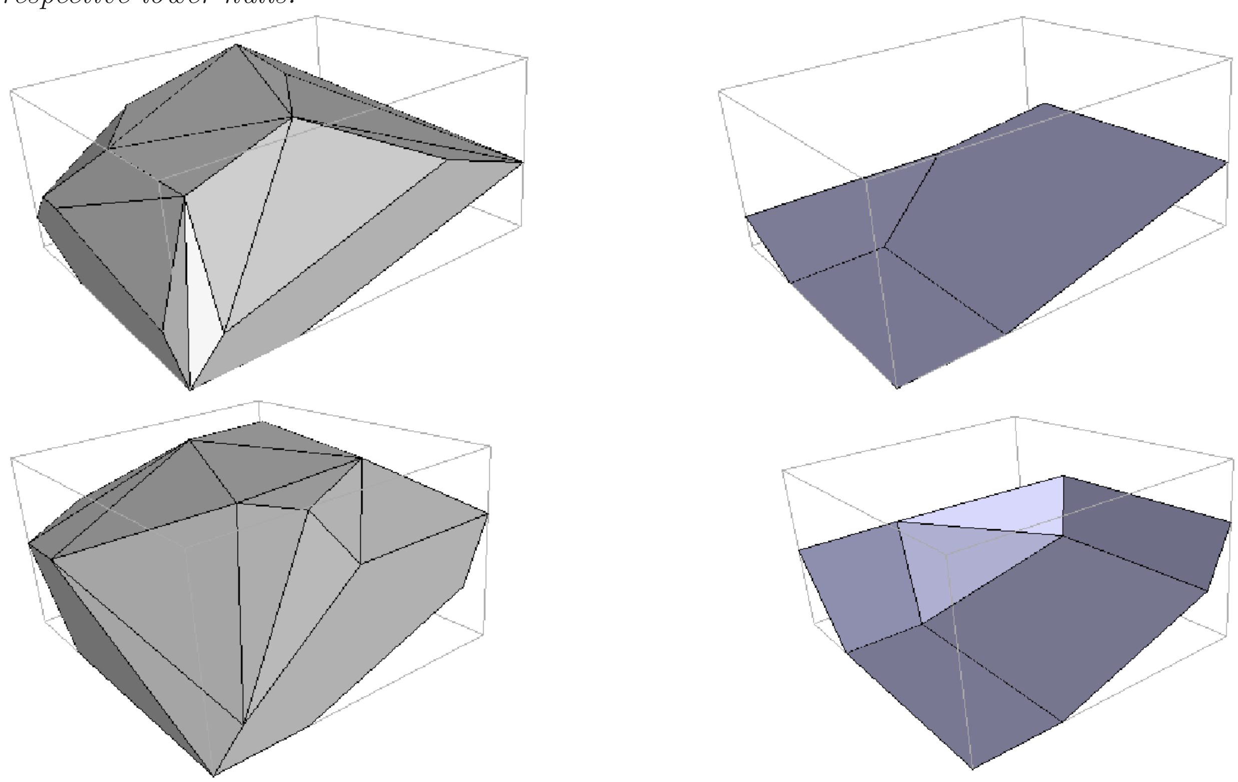
$$\mathrm{Newt}_p\left(\prod_{i=1}^n f_i(1+x_1, \ldots, 1+x_n)\right)$$

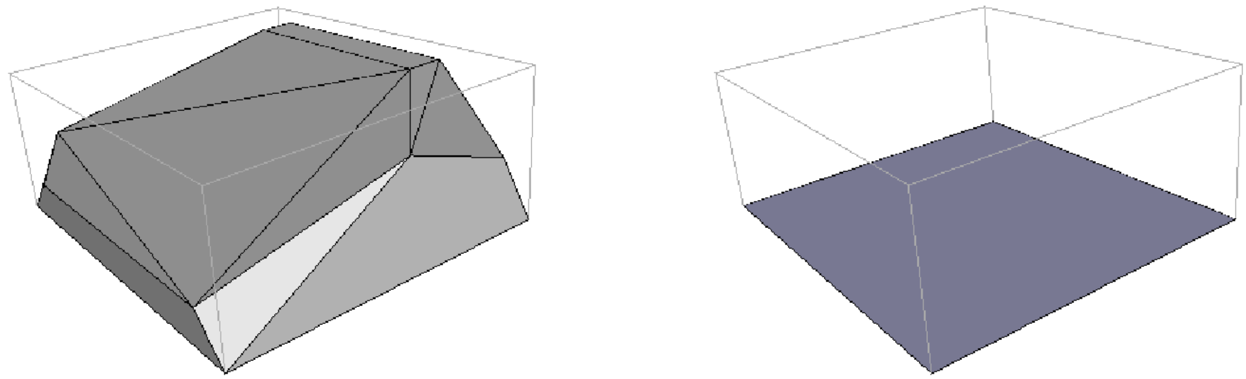
is the graph (in $\mathbb{R}^{n+1}$) of a slowly decreasing function on the non-negative orthant of $\mathbb{R}^n$ (cf. Example 3). That the individual $\mathrm{Newt}_p(f_i)$ are gently "scalloped" on the bottom in this sense can be observed quite easily.

**Example 8** *Let $\{a_i, b_i, c'_i, c''_i\}_{i=1}^7$ be independent uniformly distributed random variables such that the $a_i$ and $b_i$ are chosen from $\{0, \ldots, 11\}$, the $c'_i$ are chosen from $\{0, \ldots, 1000\}$, and the $c''_i$ are chosen from $\{0, \ldots, 11\}$. Consider then the family of* **random** *7-sparse polynomials defined by*

$$f(x, y) := c_1 x^{a_1} y^{b_1} + c_2 x^{a_2} y^{b_2} + c_3 x^{a_3} y^{b_3} + c_4 x^{a_4} y^{a_4} + c_5 x^{a_5} y^{b_5} + c_6 x^{a_6} y^{b_6} + c_7 x^{a_7} y^{b_7},$$

*where $c_i := c'_i 3^{c''_i}$. Clearly, $\mathrm{Newt}_3(f(1+x, 1+y))$ can have many more faces than $\mathrm{Newt}_3(f(x, y))$. However, for arithmetic reasons we will see below, the lower hull of $\mathrm{Newt}_3(f(1+x, 1+y))$ will be surprisingly simple. Here are 3 such random $\mathrm{Newt}_3(f(1+x, 1+y))$ alongside their respective lower hulls:*





*(The origin is the lowest corner in each bounding box, and each bounding box is contained in the non-negative octant.) So we in fact see that for all but one of the above random $f$, the lower hull of* $\mathrm{Newt}_3(f(1+x,1+y))$ *is actually the graph of an* **increasing** *function. Put another way, we have just seen experimental evidence that it is unlikely that a pair of such random $f$ will have roots in the open 3-adic unit polydisc centered at* $(1,1)$. $\diamond$

Let us now recall a clever observation of Lenstra on binomial coefficients, factorials, and least common multiples. Recall that $a|b$ means that $a$ and $b$ are integers with $a$ dividing $b$ and that $\delta_{ij}$ denotes the **Kronecker delta** (which is 0 or 1 according as $i\neq j$ or $i=j$).

**Definition 4** *[Len99b, Sec. 2] For any non-negative integers $m$ and $t$ define $d_m(t)$ to be the least common multiple of all integers that can be written as the product of at most $m$ pairwise distinct positive integers that are at most $t$ (and set $d_m(t):=1$ if $m=0$ or $t=0$).* $\diamond$

**Lemma 6** *[Len99b, Sec. 2] Following the notation of Definition 4, we have the following:*

**(a)** $d_m(t)|t!$

**(b)** $m\geq t \Longrightarrow d_m(t)=t!$

**(c)** $0\leq i\leq m<t \Longrightarrow i!|d_m(t)$

**(d)** $t\geq 1 \Longrightarrow \mathrm{ord}_p d_m(t)\leq m\lfloor \log_p t\rfloor$

*Furthermore, if $A\subset\mathbb{Z}$ is any set of cardinality $m$, then there are rational numbers $\gamma_0(A,t),\ldots,\gamma_{m-1}(A,t)$ such that:*

1. *the denominator of $\gamma_j(A,t)$ divides $d_{m-1}(t)/j!$ if $t\geq m$ and $\gamma_j(A,t)=\delta_{jt}$ otherwise.*
2. $\binom{a}{t}=\sum_{j=0}^{m-1}\gamma_j(A,t)\binom{a}{j}$ *for all $a\in A$.* $\blacksquare$

Note that we set $\binom{0}{0}=1$ and $\binom{a}{t}=0$ for all $t>a$.

Once we show that the $p$-adic Newton polytopes of $G$ are sufficiently well-behaved, Lemmata 7 and 8 below will help us complete the proof of Theorem 2.

**Lemma 7** *Let $c:=\frac{e}{e-1}$ (so $c\leq 1.582$) and $t_1,r_1,\ldots,t_n,r_n>0$. Then*

$$\sum_{i=1}^{n}(r_it_i-(\mu-1)\log_p t_i)\leq(\mu-1)\sum_{i=1}^{n}r_i \Longrightarrow \sum_{i=1}^{n}r_it_i\leq c(\mu-1)\left[\left(\sum_{i=1}^{n}r_i\right)+\log_p\left(\frac{(\mu-1)^n}{r_1\cdots r_n\log^n p}\right)\right].$$

**Proof:** Here we make multivariate extensions of some observations of Lenstra from [Len99b, Prop. 7.1]: First note that it is easily shown via basic calculus that $1-\frac{\log x}{x}$ assumes its minimum (over the positive reals), $1/c$, at $x=e$. So for all $x>0$ we have $x \geq (\log x) + x/c$. Letting $t, r>0$, $w := \frac{\mu-1}{r \log p}$, and $x := t/w$, we then obtain

$$rt \geq rwx \geq rw((\log x) + x/c) = rw(\log t) - rw(\log w) + rt/c = (\mu-1)(\log_p t) - (\mu-1)\log_p\left(\frac{\mu-1}{r\log p}\right) + rt/c.$$

Substituting $r=r_i$, $t=t_i$, and summing over $i$ then implies

$$(\star) \qquad \sum_{i=1}^n r_i t_i \geq (\mu-1)\left(\sum_{i=1}^n \log_p t_i\right) - (\mu-1)\log_p\left(\frac{(\mu-1)^n}{r_1\cdots r_n \log^n p}\right) + \frac{1}{c}\sum_{i=1}^n r_i t_i.$$

Now suppose that

$$(\star\star) \qquad \sum_{i=1}^n r_i t_i > c(\mu-1)\left[\left(\sum_{i=1}^n r_i\right) + \log_p\left(\frac{(\mu-1)^n}{r_1\cdots r_n \log^n p}\right)\right].$$

Substituting $(\star\star)$ into the **last** sum of the **right** hand side of our inequality $(\star)$ then tells us that

$$\sum_{i=1}^n r_i t_i > (\mu-1)\left(\sum_{i=1}^n \log_p t_i\right) - (\mu-1)\log_p\left(\frac{(\mu-1)^n}{r_1\cdots r_n \log^n p}\right) + (\mu-1)\left[\left(\sum_{i=1}^n r_i\right) + \log_p\left(\frac{(\mu-1)^n}{r_1\cdots r_n \log^n p}\right)\right].$$

So we obtain $\sum_{i=1}^n r_i t_i > (\mu-1)\left(\sum_{i=1}^n \log_p t_i\right) + (\mu-1)\left(\sum_{i=1}^n r_i\right)$, which can be rearranged into

$$(\star\star\star) \qquad \sum_{i=1}^n (r_i t_i - (\mu-1)\log_p t_i) > (\mu-1)\sum_{i=1}^n r_i.$$

So $(\star\star) \Longrightarrow (\star\star\star)$, and we conclude simply by taking the contrapositive. ■

The following lemma is a simple consequence of the basic properties of polytopes, their faces, and their mixed volumes [BZ88].

**Lemma 8** *Following the notation of Section 1.1, let* $G := (g_1, \ldots, g_n)$ *be any* $n \times n$ *polynomial system and let* $r := (r_1, \ldots, r_n)$ *be such that* $r_i > 0$ *for all* $i$*. Also let*

$$w(g_i, r) := \pi\left(\bigcup_{\substack{\hat{s} := (s_1, \ldots, s_n, 1) \\ s_i \geq r_i \text{ for all } i}} \mathrm{Newt}_p(g_i)^{\hat{s}}\right) \text{ for all } i.$$

*Then* $\sum_{\substack{\hat{s} := (s_1, \ldots, s_n, 1) \\ s_i \geq r_i \text{ for all } i}} \mathcal{M}\left(\pi\left(\mathrm{Newt}_p(G)^{\hat{s}}\right)\right) \leq \mathcal{M}(\mathrm{Conv}(w(g_1, r)), \ldots, \mathrm{Conv}(w(g_n, r)))$*. In particular, if* $Q_i \subseteq \{(t_1, \ldots, t_n) \in \mathbb{R}^n \mid r_1 t_1 + \cdots r_n t_n \leq \alpha_i \text{ and } t_j \geq 0 \text{ for all } j\}$ *for all* $i \in [n]$*, then* $\mathcal{M}(Q_1, \ldots, Q_n) \leq \prod_{i=1}^n \frac{\alpha_i}{r_i}$. ■

Note that the union and sum above are clearly finite since for a Newton polytope there are only finitely many inner facet normals with last coordinate 1.

**Proof of Theorem 2:**

The first portion follows immediately from Lemma 2 of Section 3, and we can assume henceforth that $k=n$, $\mu\geq n+1$, and (if desired) that $F$ is of type $(m'_1,\ldots,m'_n)$ where $m'_1,\ldots,m'_n\leq\mu-n+1$. In particular, it is now clear that the bound on $C_p(\overline{m},\overline{N},r)$ implies the bound on $C_p(\mu,n,r)$. So it suffices to prove the final bound of the theorem. Noting that $m_i\leq 1$ for some $i\Longrightarrow F$ has no roots in $(\mathbb{C}_p^*)^n$ at all, we can also clearly assume that $m_1,\ldots,m_n\geq 2$.

Let us now set $g_i(x_1,\ldots,x_n):=f_i(1+x_1,\ldots,1+x_n)$ for all $i$ and $G:=(g_1,\ldots,g_n)$. It is then clear that the number of geometrically isolated roots of $F$ with $\mathrm{ord}_p(x_i-1)\geq r_i$ for all $i$ is the same as the number of geometrically isolated roots of $G$ in $(\mathbb{C}_p^*)^n$ with $\mathrm{ord}_p x_i\geq r_i$ for all $i$, and multiplicities are preserved by this change of variables. Smirnov's Theorem then tells us that the latter number (counting multiplicities) is exactly $\sum\limits_{\substack{\hat{s}:=(s_1,\ldots,s_n,1)\\ s_i\geq r_i \text{ for all } i}}\mathcal{M}\left(\pi\left(\mathrm{Newt}_p(G)^{\hat{s}}\right)\right)$.

Now let us define, for any $N\subseteq[n]$, the following scaled $n$-simplex in $\mathbb{R}^n$:

$$S(m,N,r):=\left\{(t_1,\ldots,t_n)\in\mathbb{R}^n \;\middle|\; \sum_{i=1}^n r_it_i\leq c(m-1)\left[\left(\sum_{i\in N} r_i\right)+\log_p\left(\frac{(m-1)^{\#N}}{\left(\prod\limits_{i\in N} r_i\right)\log^{\#N}p}\right)\right] \text{ and } t_i\geq 0 \text{ for } 1\leq i\leq n\right\}.$$

By Lemma 8, and the fact that the mixed volume of integral polytopes is always a non-negative integer, we have that $\mathcal{M}(S(m_1,N_1,r),\ldots,S(m_n,N_n,r))$ is bounded above by

$$\left\lfloor c^n\prod_{i=1}^n\left\{(m_i-1)\left[\left(\sum_{j\in N_i} r_j\right)+\log_p\left(\frac{(m_i-1)^{\#N_i}}{\left(\prod_{j\in N_i} r_i\right)\log^{\#N_i}p}\right)\right]\Big/\, r_i\right\}\right\rfloor$$

where, for all $i$, $N_i$ is as in the statement of Theorem 2. Since $S(m,N,r)$ is always convex, and since $w(g_i,r)$ is a union of convex hulls of subsets of $\mathrm{Supp}(g_i)$, we also have that for all $i$, $w(g_i,r)\cap\mathrm{Supp}(g_i)\subseteq S(m_i,N_i,r)\Longrightarrow\mathrm{Conv}(w(g_i,r))\subseteq S(m_i,N_i,r)$.

Let us now fix any $i\in[n]$ and permute coordinates so that $N_i=[\nu]$. To avoid a profusion of indices, let us temporarily abuse notation slightly for the next 6 paragraphs by respectively writing $f$, $g$, and $m$ in place of $f_i$, $g_i$, and $m_i$. We then observe the following, thanks to the monotonicity of the mixed volume with respect to containment [BZ88]:

**To prove Theorem 2, we need only show that $w(g,r)\cap\mathrm{Supp}(g)\subseteq S(m,[\nu],r)$.**

To do the latter, we will first prove that the valuations of the coefficients of $g$ satisfy a "slow decay" condition, and then use convexity of the gently sloping lower faces of $\mathrm{Newt}_p(f)$ to prove our desired assertion.

Letting $D_i:=\deg_{x_i}f$, it is clear that we can write $g(x):=\sum_{t\in\prod_{i=1}^n\{0,\ldots,D_i\}}b_tx^t$, where $b_t:=\sum_{a\in A}c_a\prod_{i=1}^n\binom{a_i}{t_i}$, $f(x)=\sum\limits_{a=(a_1,\ldots,a_n)\in A}c_ax^a$ (with every $c_a$ nonzero), $t=(t_1,\ldots,t_n)$, and $A:=\mathrm{Supp}(f)$. Since $f\neq 0$ we have $g\neq 0$ and thus not all the $b_t$ vanish. Note also that $D_i>0\Longleftrightarrow i\leq\nu$, thanks to our earlier permutation of coordinates. So $D_1=\cdots=D_n=0\Longrightarrow\nu=0$ and $f$ is a nonzero constant. So in this case, $F$ has no roots in $(\mathbb{C}_p^*)^n$ at all and our asserted formula vanishes in agreement. So we can assume henceforth that $\nu\geq 1$ and $t:=(t_1,\ldots,t_\nu)$, and thus $\mathrm{Supp}(g)\subseteq\prod_{i=1}^\nu\{0,\ldots,D_i\}$.

By Lemma 6 there are rational numbers $\{\gamma^{(i)}_\alpha(t_i)\}$, with $(i,\alpha)\in[\nu]\times\{0,\ldots,\mu-1\}$, such that for all $a=(a_1,\ldots,a_n)\in A$ and $t\in\prod_{i=1}^\nu\{0,\ldots,D_i\}$ we have $\binom{a_i}{t_i}=\sum_{\alpha=0}^{\mu-1}\gamma^{(i)}_\alpha(t_i)\binom{a_i}{\alpha}$ and the denominators of the $\{\gamma^{(i)}_\alpha(t_i)\}$ not too divisible by $p$. To see why, note that for all $t\in\prod_{i=1}^{\nu}\{0,\ldots,D_i\}$,

$$b_t=\sum_{a\in A}c_a\prod_{i=1}^{\nu}\binom{a_i}{t_i}=\sum_{a\in A}c_a\prod_{i=1}^{\nu}\sum_{j_i=0}^{m-1}\left(\gamma^{(i)}_{j_i}(t_i)\binom{a_i}{j_i}\right)=\sum_{a\in A}c_a\sum_{j\in\{0,\ldots,m-1\}^\nu}\prod_{i=1}^{\nu}\left(\gamma^{(i)}_{j_i}(t_i)\binom{a_i}{j_i}\right)$$

$$=\sum_{j\in\{0,\ldots,m-1\}^\nu}\left(\prod_{i=1}^{\nu}\gamma^{(i)}_{j_i}(t_i)\right)\sum_{a\in A}c_a\prod_{i=1}^{\nu}\binom{a_i}{j_i}=\sum_{j\in\{0,\ldots,m-1\}^\nu}\left(\prod_{i=1}^{\nu}\gamma^{(i)}_{j_i}(t_i)\right)b_j.$$

So the coefficients $\{b_t\}_{t\in\prod_{i=1}^{\nu}\{0,\ldots,D_i\}}$ of $g$ are completely determined by a **smaller** set of coefficients corresponding to the exponents of $g$ lying in $\{0,\ldots,m-1\}^\nu$. Even better, Lemma 6 tells us that $t_i\leq m-1\Longrightarrow\gamma^{(i)}_{j_i}(t_i)=0$ for all $j_i\neq t_i$. So we in fact have:
($\heartsuit$) $t_i\leq m-1\Longrightarrow$ the recursive sum for $b_t$ has **no** terms corresponding to any $j$ with $j_i\neq t_i$.

Given this refined recursion for $b_t$ we can then derive that $\mathrm{ord}_p b_t$ decreases slowly and in a highly controlled manner: First note that our recursion, combined with ($\heartsuit$) and the ultrametric inequality, implies that

$$(\star)\qquad \mathrm{ord}_p b_t\geq\min_{j\in J_t}\left\{\mathrm{ord}_p(b_j)+\sum_{i=1}^{\nu}\mathrm{ord}_p\gamma^{(i)}_{j_i}(t_i)\right\}\ \text{ for all } t\in\prod_{i=1}^{\nu}\{0,\ldots,D_i\},$$

where $J_t$ is the set of all $j\in\{0,\ldots,m-1\}^\nu$ with $j_i=t_i$ for all $i\in[\nu]$ satisfying $t_i\leq m-1$. Then, by the definition of a face with inner normal $(s,1)$, we have

$$(t,b_t)\in\mathrm{Newt}_p(g)^{(s,1)}\Longrightarrow\left(\sum_{i=1}^{\nu}s_it_i\right)+\mathrm{ord}_p b_t\leq\left(\sum_{i=1}^{\nu}s_ij_i\right)+\mathrm{ord}_p b_j\ \text{ for all } j\in\prod_{i=1}^{\nu}\{0,\ldots,D_i\}.$$

So for all such $j$ we must have $\mathrm{ord}_p b_j\geq\mathrm{ord}_p b_t+\sum_{i=1}^{\nu}s_i(t_i-j_i)$. In particular, we obtain
($\star\star$) $[(t,b_t)\in\mathrm{Newt}_p(g)^{(s,1)}$ and $t_i\geq j_i$ and $s_i\geq r_i$ for all $i]\Longrightarrow\mathrm{ord}_p b_j\geq\mathrm{ord}_p b_t+\sum_{i=1}^{\nu}r_i(t_i-j_i)$.

Since $t\in\mathrm{Supp}(g)$ and $(t,\mathrm{ord}_p b_t)\in\mathrm{Newt}_p(g)^{(s,1)}$ implies that $\mathrm{ord}_p b_t<\infty$, we can thus combine ($\star$) and ($\star\star$) to obtain that

$$t\in w(g,r)\cap\mathrm{Supp}(g)\Longrightarrow\mathrm{ord}_p b_t\geq\min_{j\in J_t}\left\{\mathrm{ord}_p(b_t)+\sum_{i=1}^{\nu}\left(r_i(t_i-j_i)+\mathrm{ord}_p\gamma^{(i)}_{j_i}(t_i)\right)\right\}.$$

Cancelling and rearranging terms, we thus obtain that $t\in w(g,r)\cap\mathrm{Supp}(g)\Longrightarrow$

$$\sum_{i=1}^{\nu}r_it_i\leq\max_{j\in J_t}\left\{\sum_{i=1}^{\nu}\left(j_ir_i-\mathrm{ord}_p(\gamma^{(i)}_{j_i}(t_i)\right)\right\}.$$

Since Lemma 6 tells us that $-\mathrm{ord}_p\gamma^{(i)}_{j_i}(t_i)\leq(m-1)(\log_p t_i)-\mathrm{ord}_p(j_i!)$ for all $i$ and $t_i\in\{0,\ldots,D_i\}$, we then obtain

$$(\clubsuit)\qquad\sum_{i=1}^{\nu}\left(r_it_i-(m-1)\log_p t_i\right)\leq\max_{j\in J_t}\left\{\sum_{i=1}^{\nu}\left(j_ir_i-\mathrm{ord}_p(j_i!)\right)\right\}\leq(m-1)\sum_{i=1}^{\nu}r_i.$$

So by Lemma 7 we obtain that $w(g,r)\cap \mathrm{Supp}(g)\subseteq S(m,[\nu],r)$ and we are done. ■

It immediately follows that we can give an even sharper bound via the first inequality of (♣) from our last proof:

**Corollary 3** *Following the notation of Theorem 2, let $T(m,N,r)$ be the subset of the non-negative orthant of $\mathbb{R}^n$ defined by*

$$\left\{(t_1,\ldots,t_n)\in\mathbb{R}^n \;\middle|\; \sum_{i\in N}\left(r_it_i-(m-1)\log_p t_i\right)\leq \max_{j\in J_t}\left\{\sum_{i\in N}(j_ir_i-\mathrm{ord}_p(j_i!))\right\} \text{ and } \begin{matrix} t_i\geq 0 \text{ for } i\in N\\ t_i=0 \text{ for } i\not\in N\end{matrix}\right\},$$

*where $J_t$ is the set of all $j\in\{0,\ldots,m-1\}^n$ with $j_i=t_i$ for all $i\in[n]$ satisfying $t_i\leq m-1$. Then we have an improved bound of*

$$C_p(\mu,n,r)\leq\left\lfloor \mathcal{M}(\underbrace{\mathrm{Conv}(T(\mu-n+1,[n],r)),\ldots,\mathrm{Conv}(T(\mu-n+1,[n],r))}_{n})\right\rfloor$$

*and, if $k=n$, a more refined bound of*

$$C_p(\overline{m},\overline{N},r)\leq\lfloor\mathcal{M}(\mathrm{Conv}(T(m_1,N_1,r)),\ldots,\mathrm{Conv}(T(m_n,N_n,r)))\rfloor. \;■$$

For $n=1$ our last corollary agrees with an earlier explicit bound of Lenstra [Len99b, Prop. 7.1]. We also point out that a sufficiently good generalization of mixed volume to $n$-tuples of **non**-convex sets would allow us to sharpen our last bound by removing the convex hulls from its statement.

# Acknowledgements

The author thanks Raphael Hauser and Gregorio Malajovich for useful discussions, and William Fulton and Hal Schenck for clarifying the role of intersection multiplicity in Lemma 1. I also thank Zhigang Zhang for assistance with the `Matlab` code for generating the illustrations. Special thanks go to Mikhail M. Kapranov for sending me a copy of [Kap00]. Finally, I thank the anonymous referee for excellent detailed comments and suggestions.

# References

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

[BC76] Borodin, Allan and Cook, Stephen A., *"On the Number of Additions to Compute Specific Polynomials,"* SIAM J. Comput. **5** (1976), no. 1, pp. 146–157.

[BZ88] Burago, Yu. D. and Zalgaller, V. A., *Geometric Inequalities,* Grundlehren der mathematischen Wissenschaften 285, Springer-Verlag (1988).

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

[DGH98] Dyer, Martin; Gritzmann, Peter; and Hufnagel, Alexander, *"On the Complexity of Computing Mixed Volumes,"* SIAM J. Comput. **27** (1998), no. 2, pp. 356–400.

[Ede87] Edelsbrunner, Herbert, *Algorithms in Combinatorial Geometry,* EATCS Monographs on Theoretical Computer Science, 10, Springer-Verlag, Berlin, 1987.

[Ful98] Fulton, William, *Intersection Theory,* 2nd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete 3, **2**, Springer-Verlag, 1998.

[GH93] Giusti, Marc and Heintz, Joos, *"La détermination des points isolés et la dimension d'une variété algébrique peut se faire en temps polynomial,"* Computational Algebraic Geometry and Commutative Algebra (Cortona, 1991), Sympos. Math. XXXIV, pp. 216–256, Cambridge University Press, 1993.

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

[Har77] Hartshorne, Robin, *Algebraic Geometry,* Graduate Texts in Mathematics, No. 52, Springer-Verlag.

[Ili89] Iliopoulos, Costas S., *"Worst Case Complexity Bounds on Algorithms for Computing the Canonical Structure of Finite Abelian Groups and the Hermite and Smith Normal Forms of an Integer Matrix,"* SIAM Journal on Computing, 18 (1989), no. 4, pp. 658–669.

[IW97] Impagliazzo, Russell and Wigderson, Avi, "**P**=**BPP** if **EXPTIME** Requires Exponential Circuits: Derandomizing the XOR Lemma," STOC '97 (El Paso, TX), pp. 220–229, ACM, New York, 1999.

[Jac85] Jacobson, Nathan, *Basic Algebra I*, 2nd edition, W. H. Freeman and Company, 1985.

[Kap00] Kapranov, Mikhail M., *"Amoebas Over Non-Archimedean Fields,"* manuscript, University of Toronto, 2000.

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

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

[Kob84] Koblitz, Neal I., *p-adic Numbers, p-adic Analysis, and Zeta-Functions,* 2nd ed., Graduate Texts in Mathematics, 58, Springer-Verlag, New York-Berlin, 1984.

[Koi96] Koiran, Pascal, *"Hilbert's Nullstellensatz is in the Polynomial Hierarchy,"* DIMACS Technical Report 96-27, July 1996. (This preprint considerably improves the published version which appeared Journal of Complexity **12** (1996), no. 4, pp. 273–286.)

[LLL82] Lenstra, Arjen K.; Lenstra (Jr.), Hendrik W.; and Lovász, László, *"Factoring Polynomials with Rational Coefficients,"* Math. Ann. 261 (1982), no. 4, 515–534.

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

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

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

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

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

[Ris85] Risler, Jean-Jacques, *"Additive Complexity and Zeros of Real Polynomials,"* SIAM J. Comput. **14** (1985), no. 1, pp. 178–183.

[Roj99a] Rojas, J. Maurice, *"Solving Degenerate Sparse Polynomial Systems Faster,"* Journal of Symbolic Computation, vol. 28 (special issue on elimination theory), no. 1/2, July and August 1999, pp. 155-186.

[Roj99b] _______________, *"Toric Intersection Theory for Affine Root Counting,"* Journal of Pure and Applied Algebra, vol. 136, no. 1, March, 1999, pp. 67–100.

[Roj00a] _______________, *"Algebraic Geometry Over Four Rings and the Frontier to Tractability,"* Contemporary Mathematics, vol. 270, Proceedings of a Conference on Hilbert's Tenth Problem and Related Subjects (University of Gent, November 1-5, 1999), edited by Jan Denef, Leonard Lipschitz, Thanases Pheidas, and Jan Van Geel, pp. 275–321, AMS Press (2000).

[Roj00b] _______________, *"Some Speed-Ups and Speed Limits for Real Algebraic Geometry,"* Journal of Complexity, FoCM 1999 special issue, vol. 16, no. 3 (sept. 2000), pp. 552–571.

[Roj01a] _______________, *"Computational Arithmetic Geometry I: Sentences Nearly in the Polynomial Hierarchy,"* J. Comput. System Sci., STOC '99 special issue, vol. 62, no. 2, march 2001, pp. 216–235.

[Roj01b] _______________, *"Finiteness for Arithmetic Fewnomial Systems,"* invited paper, vol. 286, Contemporary Mathematics, AMS-IMS-SIAM Joint Summer Research Conference Proceedings of "Symbolic Computation: Solving Equations in Algebra, Geometry, and Engineering (June 11–15, 2000, Mount Holyoke College)," edited by Edward L. Green, Serkan Hoşten, Reinhard Laubenbacher, and Vicky Powers, pp. 107–114, AMS Press, 2001.

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

[Roj03a] _______________, *"Dedekind Zeta Functions and the Complexity of Hilbert's Nullstellensatz,"* Math ArXiV preprint `math.NT/0301111`, submitted for publication.

[Roj03b] _______________, *"Tropical Mixed Volumes and non-Archimedean Amoebae,"* preprint.

[Shu93] Shub, Mike, *"Some Remarks on Bézout's Theorem and Complexity Theory,"* From Topology to Computation: Proceedings of the Smalefest (Berkeley, 1990), pp. 443–455, Springer-Verlag, 1993.

[Smi97] Smirnov, A. L., *"Torus Schemes Over a Discrete Valuation Ring,"* St. Petersburg Math. J. **8** (1997), no. 4, pp. 651–659.

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

[vdK00] Van Der Kallen, Wilberd, *"Complexity of the Havas, Majewski, Matthews LLL Hermite normal form algorithm,"* J. Symbolic Comput. 30 (2000), no. 3, pp. 329–337.

[Zie95] Ziegler, Gunter M., *Lectures on Polytopes*, Graduate Texts in Mathematics, Springer Verlag, 1995.