Contemporary Mathematics

Finiteness for Arithmetic Fewnomial Systems

J. Maurice Rojas

To my god-daughter, Monika Althoff.

Abstract. Suppose $\mathcal{L}$ is any finite algebraic extension of either the ordinary rational numbers or the p-adic rational numbers. Also let $g_1, \ldots, g_k$ be polynomials in n variables, with coefficients in $\mathcal{L}$, such that the total number of monomial terms appearing in at least one g_i is exactly m. We prove that the maximum number of isolated roots of $G := (g_1, \ldots, g_k)$ in $\mathcal{L}^n$ is finite and depends solely on $(m, n, \mathcal{L})$, i.e., is independent of the degrees of the g_i. We thus obtain an arithmetic analogue of Khovanski's Theorem on Fewnomials, extending earlier work of Denef, van den Dries, Lipshitz, and Lenstra.

1. Introduction

A consequence of Descartes' Rule (a classic result dating back to 1637) is that any real univariate polynomial with exactly $m \geq 1$ monomial terms has at most $2m - 1$ real roots. In this paper, we extend this result in two directions at once: we bound the number of isolated roots of polynomial **systems** over **$\mathfrak{p}$-adic** fields, independent of the degrees of the underlying polynomials. As a consequence, we also obtain analogous results over any number field. The resulting bounds are, unfortunately, non-explicit. Nevertheless, the existence of such bounds on the number of roots was previously unknown in the multivariate non-Archimedean and number field cases. So let us now detail our results and some important precursors.

Extending the sharp bound of Descartes' Rule to polynomial systems has already proven difficult in the special case of the real numbers $\mathbb{R}$ (perhaps the most familiar metrically complete field): the best general result in this direction, Khovanski's Theorem on Fewnomials [**Kho80, Kho91**], gives an explicit bound on the number of non-degenerate real roots[1] that is independent of the underlying polynomial degrees, but exponential in the number of monomial terms. Whether the number of non-degenerate roots is in fact **polynomial** in the number of monomial

1991 *Mathematics Subject Classification.* Primary 11G25; Secondary 11G35, 14D10, 14G20.
This research was partially supported by Hong Kong UGC Grant #9040469-730 and a grant from the Texas A&M Faculty of Sciences.

[1] One can then extend this to counting isolated roots and connected components via some algebraic tricks. See, e.g., [**Roj00a, LRW01**].

terms for every **fixed** number of equations and variables is an intriguing open question, and the answer is still unknown even in the case of two polynomials in two unknowns. (The polynomial system $(x_1^2-x_1,\ldots,x_n^2-x_n)$ easily shows us that fixing n is necessary if we would like polynomiality in the number of monomial terms.)

As for the $\mathfrak{p}$-adic univariate case, Hendrik W. Lenstra, Jr. has shown that for any degree d algebraic extension L of $\mathbb{Q}_p$, the maximum number of roots in L of a $g\in L[x_1]$ with exactly $m\geq 2$ monomial terms is no more than

$$1+1.582\cdot(p^{f_L}-1)(m-1)^2(1+\tfrac{e_L\log(e_L(m-1)/\log p)}{\log p})$$

[**Len99**, prop. 7.2], where e_L and f_L respectively denote the **ramification degree** and **residue field degree** of L. (Recall that e_L and f_L are integers satisfying $e_Lf_L=d$; see section 3 for their definitions.) In particular, this bound is independent of the degree of g. As a consequence, Lenstra also derived a bound of

$$1+4.566\cdot(m-1)^2(d+10)2^d(\log(d(m-1))+0.367)$$

[**Len99**, prop. 8.1] for the analogous situation where one replaces L by any degree d algebraic extension K of $\mathbb{Q}$.[2]

By recent work of the author [**LRW01**] this polynomiality of the number of roots in the number of monomials can be extended to certain systems of n polynomials in n unknowns, provided we fix n and restrict to real algebraic number fields. (The example from the paragraph before last tells us that fixing n is necessary in the $\mathfrak{p}$-adic and number field cases as well.) However, at the expense of less explicit bounds, one can extend Lenstra's results much farther.

NOTATION. *Let $\mathcal{L}$ be a field and $\mathcal{L}^*:=\mathcal{L}\setminus\{0\}$. If $\boldsymbol{G}:=(g_1,\ldots,g_k)$ where, for all i, $\boldsymbol{g_i}\in\mathcal{L}[x_1,\ldots,x_n]\setminus\{0\}$, and the number of monomial terms appearing in at least one g_i is exactly m, then we call G a* **$(\boldsymbol{k}\times\boldsymbol{n})$ $\boldsymbol{m}$-sparse polynomial system (over $\boldsymbol{\mathcal{L}}$)**. *Also, we say a root ζ of G is* **isolated** *(resp.* **non-degenerate***) iff ζ is an irreducible component of the zero set of G over the algebraic closure of $\mathcal{L}$ (resp. $k=n$ and the Jacobian of G, evaluated at ζ, is invertible).*

THEOREM 1. *For any (rational) prime p and positive integer d, let L be any degree d algebraic extension of $\mathbb{Q}_p$. Also let G be any $k\times n$ m-sparse polynomial system over L. Then there is an absolute constant $\gamma(n,m)$ such that the number of isolated roots of G in L^n is no more than $p^{dn}(1-\frac{1}{p^{f_L}})^n\gamma(n,m)$.*

COROLLARY 1. *Let K be any degree d algebraic extension of $\mathbb{Q}$ and let G be any $k\times n$ m-sparse polynomial system over K. Then the number of isolated roots of G in K^n is no more than $2^{dn}(1-\frac{1}{2^d})^n\gamma(n,m)$.*

Theorem 1 generalizes an analogy over $\mathbb{Z}_p$, initiated by Jan Denef and Lou van den Dries in [**DV88**], of Khovanski's Theorem on Fewnomials. Corollary 1 establishes a higher-dimensional analogue of Lenstra's aforementioned result for univariate sparse polynomials over number fields. We can also extend our finiteness results even further to count isolated roots of bounded degree over L or K (see corollary 2 of section 2).

We prove theorem 1 and corollary 1 in sections 3 and 4 respectively. The proofs, while short, involve deep non-effective results of Jan Denef and Lou van den Dries

[2]In both cases, a bound of 1 is trivial to derive when $m\leq 1$, and the bounds we quoted have the added benefit of counting the multiplicities of the non-zero roots. Furthermore, the result over K is actually a stronger statement which bounds the number of roots of bounded degree over K.

[**DV88**] and Leonard Lipshitz [**Lip88**] on p-adic sub-analytic functions, as well as an elegant extension of the classical p-adic Newton polygon by A. L. Smirnov [**Smi97**]. In particular, aside from the case $n=1$ (which is essentially covered by [**Len99**]), there appear to be no explicit bounds on the function $\gamma(n,m)$ yet. So a more direct and effective approach would be of the utmost interest.

1.1. p-adic Analysis and p-adic Newton Polytopes.

We first state the following paraphrase of a result of Lipshitz:

LIPSHITZ'S THEOREM. *(See* [**Lip88**, thm. 2]*.) For any (rational) prime p, let $\mathbb{C}_p$ denote the completion (with respect to any p-adic metric) of the algebraic closure of $\mathbb{Q}_p$. Also let G be any $n\times n$ m-sparse polynomial system over $\mathbb{C}_p$. Then there is an absolute constant $\beta'(n,m)$ (independent of p) such that G has no more than $\beta'(n,m)$ isolated roots $x:=(x_1,\ldots,x_n)\in\mathbb{C}_p^n$ satisfying $|x_i-1|_p\leq\frac{1}{p}$ for all i, where $|\cdot|_p$ denotes the unique ultra-metric norm on $\mathbb{C}_p$ with $|p|_p=\frac{1}{p}$.* ■

REMARK 1. *In the above $\mathfrak{p}$-adic context, we also have the following equivalent definition of isolation for roots: a root x of G is isolated iff for some $\varepsilon>0$, we have $\max_i|x_i-x_i'|_p>\varepsilon$ for every other root $(x_1',\ldots,x_n')$ of G. So in essence, an isolated root of G in $\mathbb{C}_p^n$ can be contained within a small $\mathfrak{p}$-adic "brick," away from all other roots of G. Lipshitz's original statement in fact dealt with roots with* **algebraic integer** *coordinates in $\mathbb{C}_p^n$, but the statement above is equivalent since the ultra-metric inequality implies $|x|_p\leq\max\{|x-1|_p,|1|_p\}=1$.* ⋄

REMARK 2. *Lenstra has also derived an explicit upper bound on the number of roots x_1 of g_1 in $\mathbb{C}_p$ with $|x_1-1|_p\leq\frac{1}{p^r}$ for any given $r>0$* [**Len99**, prop. 7.1].[3] *Taking $r=1$ one then obtains $\beta'(1,m)\leq 1.582\cdot(m-1)(1+1.443\cdot(\log(m-1)+0.367))$ for $m\geq 2$. (Note that $\beta'(n,0)=\beta'(n,1)=0$ for all n.) Whether Lenstra's explicit bound on the number of roots in $\mathbb{C}_p$ near the identity extends to $n\times n$ sparse polynomial systems is an open problem, even in the case $n=2$. Nevertheless, the proofs of theorem 1 and corollary 1 are structured so that explicit bounds on $\gamma(n,m)$ can be easily derived should such a result become available.* ⋄

Lipshitz's Theorem is based partially on an earlier result of Denef and van den Dries [**DV88**, pg. 105] over the subring $\mathbb{Z}_p$ but also injects model-theoretic techniques (see [**Lip88**] for further details).

The key to proving theorem 1 is to further limit the number of roots defined over a subfield of $\mathbb{C}_p$ by seeing which possible vectors of valuations can occur. In particular, we will use the following extension of the classical univariate p-adic Newton polygon (see, e.g., [**Kob84**, ch. IV, sec. 3] for the latter construction). To clarify the statement, let us make the following definitions:

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 $g\in\mathcal{L}[x_1,\ldots,x_n]$ in the form $\sum_{a\in\mathbb{Z}^n}c_ax^a$, we call $\mathrm{Supp}(\boldsymbol{g}):=\{a \mid c_a\neq 0\}$ the* **support** *of g. Then, for any $n\times n$ polynomial system G over $\mathbb{C}_p$, its* **$\boldsymbol{n}$-tuple of $\boldsymbol{p}$-adic Newton polytopes**, *$\boldsymbol{\Delta_p(G)}=(\Delta_p(g_1),\ldots,\Delta_p(g_n))$, is defined as follows: $\boldsymbol{\Delta_p(g_i)}:=\mathrm{Conv}(\{(a,\mathrm{ord}_pc_a) \mid a\in\mathrm{Supp}(g_i)\})\subset\mathbb{R}^{n+1}$, where $\mathrm{Conv}(S)$ denotes the convex hull of*[4] *a set $S\subseteq\mathbb{R}^{n+1}$ and $\mathrm{ord}_p:\mathbb{C}_p\longrightarrow\mathbb{Q}\cup\{+\infty\}$ is the usual discrete*

[3] The original statement was in terms of ord_p, counted multiplicities, and in fact gave a decreasing function of p.

[4] i.e., smallest convex set containing...

valuation[5] *of* $\mathbb{C}_p$. *Finally, for any* $w \in \mathbb{R}^n$ *and any compact subset* $B \subset \mathbb{R}^n$, *let the* **face of B with inner normal w, B^w**, *be the set of points* $x \in B$ *which minimize the inner product* $w \cdot x$.

EXAMPLE 1. *Consider the* 2×2 6*-sparse polynomial system*

$$F := (50x_1^{18} - 3125x_2^9 - 162x_2, 49x_2^{18} - 35x_1^9 - 109375x_1)$$

over $\mathbb{Q}_5$. *Then the corresponding pair of* 5*-adic Newton polytopes is*

$$\Delta_5(F) = (\mathrm{Conv}(\{(18,0,2),(0,9,5),(0,1,0)\}), \mathrm{Conv}(\{(0,18,0),(9,0,1),(1,0,6)\})).$$

Note that each polytope is in fact a triangle embedded in $\mathbb{R}^3$.

SMIRNOV'S THEOREM. [**Smi97**, thm. 3.4] *Let* $\mathrm{ord}_p x := (\mathrm{ord}_p x_1, \ldots, \mathrm{ord}_p x_n)$ *and let* $v := (v_1, \ldots, v_n) \in \mathbb{R}^n$. *Then for any* $n\times n$ *polynomial system* G *over* $\mathbb{C}_p$, *the number of isolated roots* $x := (x_1, \ldots, x_n)$ *of* G *in* $(\mathbb{C}_p^*)^n$ *satisfying* $\mathrm{ord}_p x = v$ *(counting multiplicities) is no more than* $\mathcal{M}(\pi(\Delta_p^{v'}(g_1)), \ldots, \pi(\Delta_p^{v'}(g_n)))$, *where* $v' := (v_1, \ldots, v_n, 1)$, $\pi : \mathbb{R}^{n+1} \longrightarrow \mathbb{R}^n$ *is the natural projection forgetting the* v_{n+1} *coordinate,* $\mathcal{M}$ *denotes mixed volume* [**BZ88**] *normalized so that*

$$\mathcal{M}(\mathrm{Conv}(\{\mathbf{O}, e_1\}), \ldots, \mathrm{Conv}(\{\mathbf{O}, e_n\})) = 1,$$

and e_i *is the* $i^{\underline{\text{th}}}$ *standard basis vector of* $\mathbb{R}^n$. ■

REMARK 3. *Note that the number of roots of* G *in* $(\mathbb{C}_p^*)^n$ *with given valuation vector thus depends strongly on the individual exponents of* G *— not just on the number of monomial terms. However, the number of possible distinct valuation vectors occuring for any single* G *can be combinatorially bounded from above as a function depending solely on* n *and the number of monomial terms (cf. section 3). In particular, it is only the* **lower**[6] *faces of the Newton polytopes that matter.* ⋄

Note that Smirnov's Theorem provides a non-Archimedean refinement of Bernstein's famous mixed volume bound over $(\mathbb{C}^*)^n$ [**BKK76, Roj99**]. We also point out that aside from a result of Kamel A. Atan and J. H. Loxton in the 2×2 case [**AL86**], Smirnov's result appears to be the first higher-dimensional version of the classical univariate p-adic Newton polygon.

While we will leave the algorithmic issues of p-adic Newton polytopes for another paper, let us at least observe one salient fact before pointing out references to the computational literature: In searching for $v' \in \mathbb{R}^{n+1}$ giving a positive number of roots with valuation vector v, it suffices to restrict one's search to the inner normals of the lower n-dimensional faces of the **Minkowski sum**[7] $\Delta_p(g_1) + \cdots + \Delta_p(g_n)$. The last fact follows from basic convex geometry (see, e.g., [**BZ88**]). While there currently seems to be no direct software implementation of p-adic Newton polytopes, the underlying algorithms have already been implemented in the related context of mixed volume computation, and a detailed description including complexity bounds can be found in [**Emi94, ER01**].

EXAMPLE 2. *A convenient way to visualize how many roots with valuation vector* v *appear for a given* 2×2 *polynomial system is to draw the projected lower faces of the underlying Minkowski sum. For instance, in our last example, we obtain*

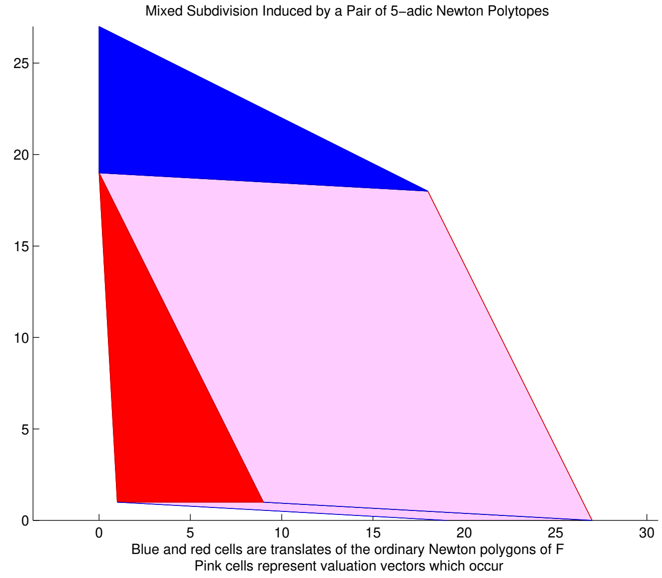
---

[5] So, for example, $\mathrm{ord}_p 0 = +\infty$ and $\mathrm{ord}_p(p^k r) = k$ whenever r is a unit in $\mathbb{Z}_p$ and $k \in \mathbb{Q}$.

[6] Those with positive x_{n+1} coordinate for their inner normals...

[7] The Minkowski sum of any finite collection of subsets $A_1, \ldots, A_k \subseteq \mathbb{R}^n$ is simply the set $\{a_1 + \cdots + a_k \mid a_i \in A_i \text{ for all } i\}$.

the following representation.[8]



It is then easily checked[9] *that among the* 323 *roots* (x_1, x_2) *of* G *in* $(\mathbb{C}_5^*)^2$*, there are exactly* 8 *with* $(\mathrm{ord}_5 x_1, \mathrm{ord}_5 x_2) = (\frac{5}{8}, \frac{53}{4})$ *and* 315 *with* $(\mathrm{ord}_5 x_1, \mathrm{ord}_5 x_2) = (-\frac{1}{9}, 0)$*. In particular, we see that there are roots lying in extensions of* $\mathbb{Q}_5$ *of degree at least* 9*.*

2. Roots of Bounded Degree Over $\mathfrak{p}$-adic Fields and Number Fields

Here we use an observation on p-adic algebraic extensions to prove the following combined strengthening of theorem 1 and corollary 1. First, let us say that a vector $x := (x_1, \ldots, x_n)$ defined over the algebraic closure of a field $\mathcal{L}$ **is of degree $\boldsymbol{\delta}$ over $\boldsymbol{\mathcal{L}}$** iff each x_i is of degree δ over $\mathcal{L}$.

Corollary 2. *Suppose* G *is a* $k \times n$ m*-sparse polynomial system over* $\mathcal{L}$*, where* $\mathcal{L}$ *is a degree* d *algebraic extension of either* $\mathbb{Q}$ *or* $\mathbb{Q}_p$*. Then for any positive integer* δ*, there is an absolute constant* $\gamma'(d, \delta, n, m)$ *(resp.* $\gamma'_p(d, \delta, n, m)$*) such that* G *has no more than* $\gamma'(d, \delta, n, m)$ *(resp.* $\gamma'_p(d, \delta, n, m)$*) isolated roots in* $\mathbb{C}^n$ *(resp.* $\mathbb{C}_p^n$*) of degree* $\leq \delta$ *over* $\mathcal{L}$*, according as* $\mathcal{L}$ *is an algebraic extension of* $\mathbb{Q}$ *or* $\mathbb{Q}_p$*.*

Proof: Focusing first on the case where $\mathcal{L}$ is an algebraic extension of $\mathbb{Q}_p$, note that there are only finitely many algebraic extensions of degree $\leq d\delta$ of $\mathbb{Q}_p$ [**Lan94**, ch. II, prop. 14]. Letting L be the compositum of all these fields, note that L is then also a finite algebraic extension of $\mathbb{Q}_p$. More to the point, any root of G in $\mathbb{C}_p^n$

---

[8]In the illustration, the **ordinary** Newton polygons we refer to are a construction similar to the p-adic Newton polygon, embedded in $\mathbb{R}^2$ instead of $\mathbb{R}^3$, where one essentially uses the **trivial** valuation ($|a| = 1$ for any $a \in \mathbb{C}_p^*$) instead.

[9]In this case, a brute-force search among the cross-products of a pair of edges vectors, one from each triangle, suffices to generate our normal vectors: 2 out of the resulting 9 possibilities are true inner normals of lower 2-dimensional faces of the underlying Minkowski sum. (There are just 2 other lower facet normals and these lead to mixed areas of 0.) Each resulting pair $(\pi(\Delta_5^{v'}(f_1)), \pi(\Delta_5^{v'}(f_2)))$ turns out to be a pair of line segments. The mixed area of any such edge pair (whose Minkowski sum is a lighter-colored cell in our illustration) is simply the absolute value of the determinant of the underlying vectors.

of degree $\leq \delta$ over $\mathcal{L}$ must then also lie in L^n. So the $\mathfrak{p}$-adic case of our corollary follows immediately from theorem 1.

To prove the case where $\mathcal{L}$ is an algebraic extension of $\mathbb{Q}$, note that such an $\mathcal{L}$ embeds naturally as a subfield of the L we just defined for the $\mathfrak{p}$-adic case. Taking $p=2$ to fix ideas, we then see that the degree of $\mathcal{L}\mathbb{Q}_2$ over $\mathbb{Q}_2$ is no more than d, and thus any x_i of degree $\leq \delta$ over $\mathcal{L}$ embeds in an extension of $\mathbb{Q}_2$ of degree $\leq d\delta$. Thus any such x_i can be assumed to lie in L, and we again conclude by theorem 1. ■

REMARK 4. *Note that we immediately obtain from our proof above that* $\gamma'_p(d,\delta,n,m) \leq p^{nD_p}(1-\frac{1}{p^{f_p}})^n\gamma(n,m)$ *and* $\gamma'(d,\delta,n,m) \leq 2^{nD_2}(1-\frac{1}{2^{f_2}})^n\gamma(n,m)$, *where* D_p *(resp.* f_p*) is the degree over* $\mathbb{Q}_p$ *(resp. residue field degree) of the compositum of all algebraic extensions of* $\mathbb{Q}_p$ *of degree* $\leq d\delta$. $\diamond$

3. Proving our Main Local Result (Theorem 1)

The following lemma will allow us to reduce to the case $k=n$.

LEMMA 1. *Following the notation of theorem 1, there is a matrix* $[a_{ij}] \subset \mathbb{Q}_p^{n\times k}$ *such that the zero set of* $G:=(a_{11}g_1+\cdots+a_{1k}g_k,\ldots,a_{n1}g_1+\cdots+a_{nk}g_k)$ *in* $\mathbb{C}_p^n$ *is the union of the zero set of* G *in* $\mathbb{C}_p^n$ *and a finite (possibly empty) set of points.* ■

A stronger version of the above lemma appears in [**GH93**, sec. 3.4.1], but phrased over $\mathbb{C}$ instead. However, the proof there carries over to any algebraically closed field with no difficulty whatsoever.

Returning to the proof of theorem 1, we see that lemma 1 allows us to replace G by a new $n \times n$ polynomial system (clearly still m-sparse) which has at least as many isolated roots as our original G. Abusing notation slightly, let G denote this new $n \times n$ polynomial system.

Applying Smirnov's Theorem to G, recall that $\mathcal{M}(\pi(\Delta_p^{v'}(g_1)),\ldots,\pi(\Delta_p^{v'}(g_n)))>0 \implies v'$ is an inner normal of a lower n-dimensional face of the Minkowski sum $\Sigma_G := \Delta_p(g_1)+\cdots+\Delta_p(g_n)$ (cf. section 1.1). It is then easily checked that Σ_G has at most mn vertices and thus, since any facet normal is uniquely determined by $n+1$ vertices on a facet, Σ_G has at most $\binom{mn}{n+1}$ n-dimensional faces. In particular, this implies that the number of distinct values for the vector $\mathrm{ord}_p x$, where $x \in (\mathbb{C}_p^*)^n$ is a root of G, is no more than $\binom{mn}{n+1}$. So let us fix $v \in \mathbb{R}^n$ and see how many roots of G in $(L^*)^n$ can have valuation vector v.

Let $R_p := \{a \in \mathbb{C}_p \mid |a|_p \geq 1\}$ be the ring of algebraic integers in $\mathbb{C}_p$, M_p the unique maximal ideal of R_p, $\mathbb{F}_L := (R_p \cap L)/(M_p \cap L)$, and let π be any generator of the principal ideal $M_p \cap L$ of $R_p \cap L$. Also let $e := \max_{y\in L^*}\{|\mathrm{ord}_p y|^{-1}\}$ and $f := \log_p \#\mathbb{F}_L$. The last two quantities are respectively known as the **ramification degree** and **residue field degree** of L, and we can in fact pick π so that $\pi^e=p$ as well [**Kob84**, ch. III]. Doing this, then fixing a set $A_L \subset R_p$ of representatives for $\mathbb{F}_L$ (i.e., a set of p^f elements of $R_p \cap L$, exactly **one** of which lies in M_p, whose image mod $M_p \cap L$ is $\mathbb{F}_L$), we can then write any $x_i \in L$ uniquely as $\sum_{j=e\mathrm{ord}_p(x_i)}^{+\infty} a_j^{(i)}\pi^j$ for some sequence of $a_j^{(i)} \in A_L$ [**Kob84**, cor., pg. 68, sec. 3, ch. III].

Intuitively, the numbers in L admit expansions into digits in A_L, where the expansion can go infinitely "to the right" but eventually terminates "on the left." Note in particular that if $\mathrm{ord}_p(x_i)=v_i$, and the first e digits of x_i are $(c^{(i)}_{ev_i},\ldots,c^{(i)}_{ev_i+e-1})$, then $|\frac{x}{\pi^{v_i}(c^{(i)}_{ev_i}+\cdots+c^{(i)}_{ev_i+e-1}\pi^{e-1})}-1|_p\leq\frac{1}{p}$.

Now consider the polynomial system G_c where $G_c(z_1,\ldots,z_n)$ is defined as $G(\pi^{ev_1}(c^{(1)}_{ev_1}+\cdots+c^{(1)}_{ev_1+e-1}\pi^{e-1})z_1,\ldots,\pi^{ev_n}(c^{(n)}_{ev_n}+\cdots+c^{(n)}_{ev_n+e-1}\pi^{e-1})z_n)$, for any fixed vectors $(c^{(1)}_{ev_1},\ldots,c^{(1)}_{ev_1+e-1}),\ldots,(c^{(n)}_{ev_n},\ldots,c^{(n)}_{ev_n+e-1})\in A^e_L$ with $c^{(1)}_{ev_1},\ldots,c^{(n)}_{ev_n}\not\in M_p$. Lipshitz's Theorem then tells us that the number of isolated roots z of G_c in $\mathbb{C}^n_p$ satisfying $|z_1-1|_p,\ldots,|z_n-1|_p\leq\frac{1}{p}$ is no more than $\beta'(n,m)$.

Since there are $(p^f-1)p^{f(e-1)}=p^d(1-\frac{1}{p^f})$ possibilities for each e-tuple $(c^{(i)}_0,\ldots,c^{(i)}_{e-1})$, our preceding observations imply that the number of isolated roots x of G in L^n satisfying $\mathrm{ord}_p x=v$ is no more than $p^{dn}(1-\frac{1}{p^f})^n\beta'(n,m)$. So the total number of isolated roots of G in $(L^*)^n$ is no more than $\binom{mn}{n+1}p^{dn}(1-\frac{1}{p^f})^n\beta'(n,m)$.

To conclude, we simply set all possible subsets of the variables equal to zero (which of course never increases the number of monomial terms) and apply our result recursively to the resulting polynomial systems in fewer variables. We thus obtain our theorem, along with an obvious bound of $\gamma(n,m)\leq 1+\sum^n_{i=1}\binom{n}{i}\binom{mi}{i+1}\beta'(i,m)$ for all $n\in\mathbb{N}$. ■

4. Proving Our Main Global Result (Corollary 1)

Since $\mathbb{Q}$ naturally embeds in $\mathbb{Q}_p$ for any prime p, K embeds in a degree d algebraic extension, L, of $\mathbb{Q}_p$. So let us fix $p=2$, say. Our corollary then follows immediately from theorem 1. ■

Remark 5. *The following improved bound for corollary 1 follows immediately from our proof above:* $2^{dn}(1-\frac{1}{2^{f_L}})^n\gamma(n,m)$, *where* L *is as in the proof.* ◇

Acknowledgements

The author thanks Peter Bürgisser for informing him of the important paper [**DV88**], Angus McIntyre for suggesting this paper to Peter Bürgisser, and Hendrik W. Lenstra, Jr. and Leonard Lipshitz for useful e-mail discussions. Special thanks go to an anonymous referee for graciously and elegantly pointing out some earlier errors of the author which were neither graceful nor elegant. The author is also most grateful to the architects and staff of `MathSciNet` (`http://ams.rice.edu/mathscinet/search`), without which, he wouldn't have found the paper [**Lip88**] until much later.

I dedicate this paper to my god-daughter, Monika Althoff.

References

[AL86] Atan, Kamel A. and Loxton, J. H., *"Newton Polyhedra and Solutions of Congruences,"* Diophantine Analysis (Kensington, 1985), pp. 67–82, London Math. Soc. Lecture Note Ser., 109, Cambridge Univ. Press, Cambridge, 1986.

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

[BKK76] Bernstein, D. N., Kushnirenko, A. G., and Khovanski, A. G., *"Newton Polyhedra,"* Uspehi Mat. Nauk 31 (1976), no. 3(189), pp. 201–202.

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

[DV88] Denef, Jan and van den Dries, Lou, *"p-adic and Real Subanalytic Sets,"* Annals of Mathematics (2) **128** (1988), no. 1, pp. 79–138.

[Emi94] Emiris, Ioannis Z., *"Sparse Elimination and Applications in Kinematics,"* Ph.D. dissertation, Computer Science Division, U. C. Berkeley (December, 1994), available on-line at `http://www.inria.fr/saga/emiris`.

[ER01] Emiris, Ioannis Z. and Rojas, J. Maurice, *"Some Sparse Results on Sparse Elimination,"* preprint.

[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.

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

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

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

[Lan94] Lang, Serge, *"Algebraic Number Theory,"* $2^{\underline{\text{nd}}}$ ed., Springer-Verlag, New York, 1994.

[Len99] ________________, *"On the Factorization of Lacunary Polynomials,"* Number Theory in Progress, Vol. 1 (Zakopane-Kóscielisko, 1997), pp. 277–291, de Gruyter, Berlin, 1999.

[LRW01] Li, Tien-Yien; Rojas, J. Maurice; Wang, Xiaoshen, *"Counting Real Connected Components of Trinomial Curve Intersections and m-nomial Hypersurfaces,"* Math ArXiV preprint `http://xxx.arXiv.org/abs/math.CO/0008069`, submitted for publication.

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

[Roj99] Rojas, J. Maurice, *"Toric Intersection Theory for Affine Root Counting,"* Journal of Pure and Applied Algebra, vol. 136, no. 1, March, 1999, pp. 67–100.

[Roj00a] ________________, *"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.

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

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

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

URL: `http://www.math.tamu.edu/~rojas`