Additive Complexity and Roots of Polynomials Over Number Fields and $\mathfrak{p}$-adic Fields

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

Abstract. Consider any nonzero univariate polynomial with rational coefficients, presented as an elementary algebraic expression (using only integer exponents). Letting $\sigma(f)$ denote the additive complexity of f, we show that the number of rational roots of f is no more than

$$1 + \sigma(f)^2 (22.5)^{\sigma(f)} \sigma(f)!.$$

This provides a sharper arithmetic analogue of earlier results of Dima Grigoriev and Jean-Jacques Risler, which gave a bound of $C^{\sigma(f)^2}$ for the number of real roots of f, for $\sigma(f)$ sufficiently large and some constant C with $22 < C < 32$. We extend our new bound to arbitrary finite extensions of the ordinary **or** p-adic rationals, roots of bounded degree over a number field, and geometrically isolated roots of multivariate polynomial systems. We thus extend earlier bounds of Hendrik W. Lenstra, Jr. and the author to encodings more efficient than expansions into monomial terms. We also mention a connection to complexity theory and note that our bounds hold for a broader class of fields.

1 Introduction

This paper presents another step in the author's program [Roj02] of establishing an effective arithmetic analogue of fewnomial theory. (See [Kho91] for the original exposition of fewnomial theory, which until now has always used the real or complex numbers for the underlying field.) Here, we show that the number of **geometrically isolated** roots (cf. section 2) of a polynomial system over any

* This research was partially supported by a grant from the Texas A&M College of Science.

[0] From **Proceedings of ANTS-V (5th Annual Algorithmic Number Theory Symposium, University of Sydney, July 7-12, 2002), Lecture Notes in Computer Science #2369**, Springer-Verlag (2002), pp. 506-515. (**ANTS** is the premier international conference on algorithmic number theory.) This version, dated April 3, 2003, slightly improves some of the bounds and fixes some minor typos in the published version.

fixed $\mathfrak{p}$-adic field (and thereby any fixed number field) can be bounded from above by a quantity depending solely on the additive complexity of the input equations.

So let us first clarify the univariate case of **additive complexity**: If $\mathcal{L}$ is any field, we say that $f\in\mathcal{L}[x]$ has **additive complexity $\leq s$ (over $\mathcal{L}$)** iff there exist constants $c_1, d_1, \ldots, c_s, d_s, c_{s+1} \in \mathcal{L}$ and arrays of nonnegative integers $[m_{i,j}]$ and $[m'_{i,j}]$ with $f(x)=c_{s+1}\prod\limits_{i=0}^{s} X_i^{m_{i,s+1}}$, where $X_0=x$, $X_1 = c_1X_0^{m_{0,1}} + d_1X_0^{m'_{0,1}}$, and $X_j = c_j\left(\prod\limits_{i=0}^{j-1} X_i^{m_{i,j}}\right) + d_j\left(\prod\limits_{i=0}^{j-1} X_i^{m'_{i,j}}\right)$ for all $j\in\{2,\ldots,s\}$. We then define the **additive complexity (over $\mathcal{L}$) of f, $\sigma_{\mathcal{L}}(f)$**, to be the least s in such a presentation of f as an algebraic expression. Note in particular that additions or subtractions in repeated sub-expressions are thus not counted, e.g., $9(x-7)^{99}(2x+1)^{43} - 11(x-7)^{999}(2x+1)^3$ has additive complexity ≤ 3.

It has been known since the work of Allan Borodin and Stephen A. Cook around 1974 [BC76] that there is a deep connection between additive complexity over the real numbers $\mathbb{R}$ and the number of real roots of a nonzero polynomial in $\mathbb{R}[x]$. For example, they showed that there is a real constant K such that the number of real roots of f is no more than $2^{2^{\cdot^{\cdot^{\cdot^{2^{K\sigma_{\mathbb{R}}(f)}}}}}}$, where the number of exponentiations is $\sigma_{\mathbb{R}}(f)-1$ [BC76]. Jean-Jacques Risler, using Khovanski's famous Theorem on Real Fewnomials [Kho80,Kho91], then improved this bound to $(\sigma_{\mathbb{R}}(f)+2)^{3\sigma_{\mathbb{R}}(f)+1}2^{\left(9\sigma_{\mathbb{R}}(f)^2+5\sigma_{\mathbb{R}}(f)+2\right)/2}$ [Ris85, pg. 181, line 6]. (Dima Grigoriev derived a similar bound earlier [Gri82] and both results easily imply a simplified bound of $C^{\sigma_{\mathbb{R}}(f)^2}$ for the number of real roots of f, for $\sigma_{\mathbb{R}}(f)$ sufficiently large and some constant C with $22<C<32$.)

Here, based on a recent near-optimal **arithmetic** analogue of Khovanski's Theorem on Real Fewnomials found by the author (cf. section 2 below), we give arithmetic analogues of these additive complexity bounds. Our first main result can be stated as follows:

Theorem 1 *Let p be any rational prime and let $\log_p(\cdot)$ denote the base p logarithm function. Also let $c:=\frac{e}{e-1}\leq 1.582$, let $\mathcal{L}$ be any degree d algebraic extension of $\mathbb{Q}_p$, and let $f\in\mathcal{L}[x]\setminus\{0\}$. Then f has no more than $2^{O\left(\sigma_{\mathcal{L}}(f)\log\left(p^d\sigma_{\mathcal{L}}(f)\right)\right)}$ roots in $\mathcal{L}$. More precisely,* $1+\frac{dp(p^d-1)}{p-1}+\frac{4cdp(p^d-1)^2}{p-1}\left(1+d\log_p\left(\frac{2d}{\log p}\right)\right)$

$$+\frac{1}{3}\sum_{j=3}^{\sigma_{\mathcal{L}}(f)} j(6c)^j(p^d-1)^j\left(1+d\log_p\left(\frac{d}{\log p}\right)\right)\left(1+d\log_p\left(\frac{2d}{\log p}\right)\right)^{j-1} j!$$

is a valid upper bound, and just the first $\sigma_{\mathcal{L}}(f)+1$ summands suffice if $\sigma_{\mathcal{L}}(f)\leq 2$.

Remark 1 *Our bounds can be improved further and this is detailed in remark 6 of section 3.* ⋄

Remark 2 *Note that via the obvious embedding $\mathbb{Q}\subset\mathbb{Q}_2$, theorem 1 easily implies a similar statement for $\mathcal{L}$ a number field. A less trivial extension to number fields appears in theorem 2 below.* ⋄

Example 1 *Taking $\mathcal{L}=\mathbb{Q}_2$, we obtain respective upper bounds of* 1, 3, 35, 50195, *and* 6471489 *on the number of roots of f in $\mathbb{Q}_2$, according as $\sigma_{\mathbb{Q}_2}(f)$ is* 0, 1, 2, 3, *or* 4.[1] *For instance, we see that for any non-negative integers $\alpha, \beta, \gamma, \delta, \varepsilon, \lambda, \mu, \nu$ and constants $c_1, d_1, c_2, d_2, c_3 \in \mathbb{Q}_2$, the polynomial*

$$c_3 x^\alpha \left(c_1 x^\beta + d_1 x^\gamma\right)^\delta \left[c_2 \left(c_1 x^\beta + d_1 x^\gamma\right)^\varepsilon + d_2 x^\lambda \left(c_1 x^\beta + d_1 x^\gamma\right)^\mu\right]^\nu$$

has no more than 35 *roots in $\mathbb{Q}_2$ (or $\mathbb{Q}$ obviously). See remark 5 below for improvements of some of these bounds. Note in particular that we can* **not** *count with multiplicities using a function of $\sigma_{\mathcal{L}}(f)$ only, since we can make the multiplicities arbitrarily high by increasing α and/or δ. Note also that for $\sigma_{\mathbb{R}}(f) \in \{0,1,2,3,4\}$ Risler's bound on the number of real roots respectively specializes to* 4, 20736, 274877906944, 5497558138880000000000, *and* 126315281744229461505151771531542528. $\diamond$

The importance of bounds on the number of roots in terms of additive complexity is two-fold: on the one hand, we obtain a new way to bound the number of roots in $\mathcal{L}$ of any univariate polynomial with coefficients in $\mathcal{L}$. Going the opposite way, we can use information about the number of roots in $\mathcal{L}$ of a given univariate polynomial to give a lower bound on the minimal number of additions and subtractions necessary to evaluate it. More to the point, a recent theorem of Shub and Smale establishes a deep connection between the number of integral roots of a univariate polynomial, a variant of additive complexity, and certain fundamental complexity classes.

To make this precise, let us consider another formalization of algebraic expressions. Rather than allowing arbitrary recursive use of integral powers and field operations, let us be more conservative and do the following: Suppose we have $f \in \mathbb{Z}[x_1]$ expressed as a sequence of the form $(1, x_1, f_2, \ldots, f_N)$, where $f_N = f(x_1)$, $f_0 := 1$, $f_1 := x_1$, and for all $i \geq 2$ we have that f_i is a sum, difference, or product of some pair of elements (f_j, f_k) with $j, k < i$. (Such computational sequences are also known as **straight-line programs** or **SLP's**.) Let $\boldsymbol{\tau(f)}$ denote the smallest possible value of $N-1$, i.e., the smallest length for such a computation of f. Clearly, $\tau(f)$ also admits a definition in terms of multivariate polynomial systems much like that of $\sigma_{\mathcal{L}}(f)$. So it is clear that $\tau(f) \geq \sigma_{\mathcal{L}}(f)$ for all $f \in \mathbb{Z}[x_1]$ and $\mathcal{L} \supseteq \mathbb{Z}$, and that $\sigma_{\mathcal{L}}(f)$ is often dramatically smaller than $\tau(f)$.

The Shub-Smale $\boldsymbol{\tau}$ Theorem *(See [SS95] or [BCSS98, theorem 3, pg. 127]) Suppose there is an absolute constant κ 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 $\mathbf{P}_{\mathbb{C}} \neq \mathbf{NP}_{\mathbb{C}}$.* ■

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

[1] All calculations in this paper were done with the assistance of `Maple` and the corresponding `Maple` code can be found on the author's web-page.

observation is due to Steve Smale and was first published in [Shu93].) The complexity class **BPP** is central in randomized complexity and cryptology, and the last inclusion (while widely disbelieved) is also an open question. The truth of the hypothesis of the Shub-Smale τ Theorem, also know as the ***τ*-conjecture**, is yet another open problem, even for $\kappa=1$.

Observing that the number of integral roots of f is no more than $\deg f$ (by the fundamental theorem of algebra), and that $\deg f \leq 2^{\tau(f)}$ (since $\deg f_{i+1} \leq 2\max_{j<i} \deg f_j$), we easily obtain the following crude upper bound.

Proposition *The number of integral roots of $f \in \mathbb{Z}[x_1] \setminus \{0\}$ is no more than $2^{\tau(f)}$.* ∎

As of April 2002, no asymptotically sharper bound in terms of $\tau(f)$ appears to be known![2] However, taking a 2-adic approach via theorem 1, we immediately obtain the following improvement.

Corollary *The number of integral roots of $f \in \mathbb{Z}[x_1] \setminus \{0\}$ is $2^{O\left(\sigma_{\mathbb{Q}_2}(f) \log \sigma_{\mathbb{Q}_2}(f)\right)}$.* ∎

This bound, while apparently not polynomial in $\tau(f)$, at least has the advantage that it is frequently much smaller than $2^{\tau(f)}$. For instance, our corollary tells us that the polynomial from example 1 has no more than 35 integral roots, while the proposition above would give us a non-constant upper bound of at least α, since this example (if not identically zero) has degree $\geq \alpha$.

Whether our 2-adic approach can be pushed farther to solve the τ-conjecture is an intriguing open question. In particular, it isn't even known if there is a family of f with $2^{\Omega\left(\sigma_{\mathbb{Q}_2}(f)\right)}$ roots in $\mathbb{Q}_2$.

Remark 3 *Curiously, using additive complexity over a different complete field — $\mathbb{R}$ — can* **not** *lead to a solution of the τ-conjecture: there are examples of $f \in \mathbb{Z}[x_1]$ with $\sigma_{\mathbb{R}}(f) = O(r)$ and over 2^r real (but irrational) roots [Roj00, sec. 3, pg. 13] (see [BC76] for an even bigger lower bound).* ⋄

Our main results are proved in section 3, where we in fact prove sharper versions. There we also prove a refined number field analogue of theorem 1, which we now state. Recall that if L is a subfield of $\mathbb{C}$ and $x \in \mathbb{C}$ then we say that ***x* is of degree ≤*δ* over *L*** iff x lies in an algebraic extension of L of degree $\leq \delta$.

Theorem 2 *Following the notation of theorem 1, let $\delta \in \mathbb{N}$ and suppose instead now that $\mathcal{L}$ is a degree d algebraic extension of $\mathbb{Q}$. Then the number of roots of f in $\mathbb{C}$ of degree $\leq \delta$ over $\mathcal{L}$ is $2^{O\left(\sigma_{\mathcal{L}}(f)\left(d\delta + \log \sigma_{\mathcal{L}}(f)\right)\right)}$. More precisely,*

$$1 + c(d\delta + 10)2^{d\delta+1} \log_2\left(\frac{d\delta}{\log 2}\right) + c^2(d\delta+10)^2 4^{d\delta+2} \log_2\left(\frac{d\delta}{\log 2}\right) \log_2\left(\frac{2d\delta}{\log 2}\right)$$
$$+ \frac{2}{3} \sum_{j=3}^{\sigma_{\mathcal{L}}(f)} j(6c)^j 2^{d\delta j} \left(1 + 2d^2\delta^2 \log_2\left(\frac{d^2\delta^2}{\log 2}\right)\right) \left(1 + 2d^2\delta^2 \log_2\left(\frac{2d^2\delta^2}{\log 2}\right)\right)^{j-1} j!$$

is a valid upper bound, and just the first $\sigma_{\mathcal{L}}(f)+1$ summands suffice if $\sigma_{\mathcal{L}}(f) \leq 2$.

---

[2] Using Descartes' Rule of Signs instead of the fundamental theorem of algebra does not easily yield a sharper bound: the number of monomial terms of f_i can grow even faster as a function of $\tau(f)$ than $\deg f_i$.

This family of bounds can also be sharpened further and this is also detailed in remark 6 of section 3.

In summary, theorems 1 and 2 are the first bounds on the number of roots in a local field or number field which make explicit use of additive complexity. In particular, our results thus extend an earlier result of Lenstra on polynomials with few monomial terms to the setting of an even sharper input encoding. Recall that for any field L we let $L^* := L \setminus \{0\}$.

Lenstra's Theorem *[Len99, prop. 7.2 and prop. 8.1] Following the notation of theorems 1 and 2, suppose now that $\mathcal{L}$ is a degree d extension of $\mathbb{Q}_p$ (the* **local** *case)* **or** *$\mathbb{Q}$ (the* **global** *case), and that f has exactly m monomial terms. Then f has no more than $c(q_{\mathcal{L}}-1)(m-1)^2\left(1+e_{\mathcal{L}}\log_p\left(\frac{e_{\mathcal{L}}(m-1)}{\log p}\right)\right)$ roots in $\mathcal{L}^*$ in the local case (counting multiplicities), where $e_{\mathcal{L}}$ and $q_{\mathcal{L}}$ respectively denote the ramification index and residue field cardinality of $\mathcal{L}$. Furthermore, f has no more than $c(m-1)^2(d\delta+10)\cdot 2^{d\delta+1}\log_2\left(\frac{d\delta(m-1)}{\log 2}\right)$ roots in $\mathbb{C}^*$ of degree $\leq\delta$ over $\mathcal{L}$ in the global case (counting multiplicities).*

Remark 4 *Recall that $q_{\mathcal{L}}$ is always an integer power of p and $e_{\mathcal{L}}\log_p q_{\mathcal{L}} = d$.* ⋄

Example 2 *Considering the polynomial from example 1 once again, note that Lenstra's Theorem can not even give a constant upper bound for the number of roots in $\mathbb{Q}_2^*$, since the number of monomial terms depends on λ (among other parameters). On the other hand, in the absence of an expression for f more compact than a sum of m monomial terms, Lenstra's bound is quite practical.* ⋄

Remark 5 *Hendrik W. Lenstra has observed that $B(\mathcal{L},2,1)$ is in fact the number of roots of unity in $\mathcal{L}$, which is in turn bounded above by $\frac{e_{\mathcal{L}}p(q_{\mathcal{L}}-1)}{p-1}$ [Len99]. He has also computed $B(\mathbb{Q}_2,3,1)=6$ (giving $3x_1^{10}+x_1^2-4$ as a trinomial which realizes the maximum possible number of nonzero roots in $\mathbb{Q}_2$) [Len99, prop. 9.2]. As a consequence (following easily from our proof of theorem 1), the first three summands of our main formula from theorem 1 can be replaced by $1+\frac{e_{\mathcal{L}}p(q_{\mathcal{L}}-1)}{p-1}+\frac{e_{\mathcal{L}}p(q_{\mathcal{L}}-1)B(\mathcal{L},3,1)}{p-1}$, and our bounds from example 1 can be improved to 3 and 15 in the respective cases $\sigma_{\mathbb{Q}_2}(f)=1$ and $\sigma_{\mathbb{Q}_2}(f)=2$. (This is how we derived the bound cited in the abstract.)* ⋄

As mentioned earlier, our main results follow easily from the author's recent arithmetic multivariate analogue of Descartes' Rule [Roj02]. In fact, Arithmetic Multivariate Descartes' Rule even allows us to derive multivariate extensions of theorems 1 and 2 which we state below. So let us precede our proofs by a brief discussion of this important background result.

2 Useful Multivariate Results

Suppose $\boldsymbol{f_1},\ldots,\boldsymbol{f_k}\in\mathcal{L}[x_1^{\pm1},\ldots,x_n^{\pm1}]\setminus\{0\}$, and $\boldsymbol{m_i}$ is the total number of distinct exponent vectors appearing in f_i (assuming all polynomials are written as sums of monomials). We call $\boldsymbol{F} := (f_1, \ldots, f_k)$ a $\boldsymbol{k \times n}$ polynomial system over $\boldsymbol{\mathcal{L}}$ of **type** $\boldsymbol{(m_1, \ldots, m_k)}$, and we call a root ζ of F **geometrically isolated** iff ζ is a zero-dimensional component of the underlying scheme over the algebraic closure of $\mathcal{L}$ defined by F. If $\mathcal{L}$ is a finite extension of $\mathbb{Q}_p$ (resp. $\mathbb{Q}$) then we say that we are in the **local** (resp. **global**) case.

Arithmetic Multivariate Descartes' Rule (Special Case) *[Roj02, cor. 1 of sec. 2 and cor. 2 of sec. 3] Let p be any (rational) prime and d, δ 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 $m := (m_1, \ldots, m_n) \in \mathbb{N}^n$, $N := (N_1, \ldots, N_n) \in \mathbb{N}^n$, and let F be an $n \times n$ polynomial system over $\mathcal{L}$ of type m such that the number of variables occuring in f_i is exactly N_i. Define $\boldsymbol{B(\mathcal{L}, m, N)}$ to be the maximum number of isolated roots in $(\mathcal{L}^*)^n$ of such an F in the local case, counting multiplicities.[3] Then*

$$B(\mathcal{L}, m, N) \leq \left(\prod_{i=1}^{n} (q_{\mathcal{L}} - 1) m_i (m_i - 1)/2\right) \left\lfloor \prod_{i=1}^{n} \left\{ c(m_i - 1) N_i \left[1 + e_{\mathcal{L}} \log_p \left(\frac{e_{\mathcal{L}}(m_i - 1)}{\log p}\right)\right]\right\}\right\rfloor,$$

where $c := \frac{e}{e-1} \leq 1.582$, and $e_{\mathcal{L}}$ and $q_{\mathcal{L}}$ are respectively the ramfication index and residue field cardinality of $\mathcal{L}$.

Furthermore, moving to the global case, let us say a root $x \in \mathbb{C}^n$ of F is of **degree** $\boldsymbol{\leq \delta}$ **over** $\mathcal{L}$ *iff every coordinate of x is of degree $\leq \delta$ over $\mathcal{L}$, and let us define $\boldsymbol{A(\mathcal{L}, \delta, m, N)}$ to be the maximum number of isolated roots of such an F in $(\mathbb{C}^*)^n$ of degree $\leq \delta$ over $\mathcal{L}$, counting multiplicities.[3] Then*

$$A(\mathcal{L}, \delta, m, N) \leq 2^{d\delta n + 1} \left(\prod_{i=1}^{n} m_i (m_i - 1)/2\right) \prod_{i=1}^{n} \left\{ c(m_i - 1) N_i \left[1 + 2d^2\delta^2 \log_2 \left(\frac{d^2\delta^2(m_i - 1)}{\log 2}\right)\right]\right\}. \blacksquare$$

Various other improvements of these bounds are detailed in [Roj02]. However, let us at least point out that our bound above is nearly optimal: For **fixed** $\mathcal{L}$, $\log B(\mathcal{L}, (\mu, \ldots, \mu), (n, \ldots, n))$ and $\log A(\mathcal{L}, (\mu, \ldots, \mu), (n, \ldots, n))$ are $\Theta(n \log \mu)$, where the implied constant depends on $\mathcal{L}$ (and d and δ) [Roj02, example 2].

Via our definition of additive complexity we will reduce the proofs of our main results to an application of Arithmetic Multivariate Descartes' Rule. In particular, it appears that any further improvement to our main results will have to come from a different technique. For now, we have the following generalization of theorems 1 and 2.

Definition 1 *Following the notation above, given any $k \times n$ polynomial system $F = (f_1, \ldots, f_k)$ over $\mathcal{L}$, let us define its* **additive complexity over** $\boldsymbol{\mathcal{L}}$, $\boldsymbol{\sigma_{\mathcal{L}}(F)}$, *to be the smallest s such that $F(x_1, \ldots, x_n)$ can be written as*
$\left(c^{(1)}_{n+s+1} \prod_{i=1}^{n+s} X_i^{m^{(1)}_{i,n+s+1}}, \ldots, c^{(k)}_{n+s+1} \prod_{i=1}^{n+s} X_i^{m^{(k)}_{i,n+s+1}}\right)$, *where $X_j := x_j$ for all $j \in \{1, \ldots, n\}$, $X_j = c_j \left(\prod_{i=1}^{j-1} X_i^{m_{i,j}}\right) + d_j \left(\prod_{i=1}^{j-1} X_i^{m'_{i,j}}\right)$ for all*

[3] The multiplicity of any isolated root here, which we take in the sense of intersection theory for a scheme over the algebraic closure of $\mathcal{L}$ [Ful98], turns out to always be a positive integer when $k = n$ (see, e.g., [Smi97,Roj99]).

$j \in \{n+1, \ldots, n+s\}$, $c_1, d_1, \ldots, c_{n+s}, d_{n+s}, c^{(1)}_{n+s+1}, \ldots, c^{(k)}_{n+s+1} \in \mathcal{L}$, *and* $[m_{i,j}]$, $[m'_{i,j}]$, *and* $[m^{(\ell)}_{i,j}]$ *are arrays of positive integers.* $\diamond$

Theorem 3 *Following the notation above, F has no more than*

$$1 + B(\mathcal{L},2,1) + (1 + B(\mathcal{L},2,1)B(\mathcal{L},3,1)) + \sum_{\ell=3}^{\sigma_{\mathcal{L}}(F)} \binom{n+\ell-1}{n-1} B(\mathcal{L}, (\underbrace{2,\ldots,2}_{n}, \underbrace{3,\ldots,3}_{\ell-n}), (n+1, n+2 \ldots, n+\ell-1, n+\ell-1))$$

geometrically isolated roots in $\mathcal{L}^n$, or $1 + A(\mathcal{L},\delta,2,1) + (1 + A(\mathcal{L},\delta,2,1)A(\mathcal{L},\delta,3,1))$

$$+ \sum_{\ell=3}^{\sigma_{\mathcal{L}}(F)} \binom{n+\ell-1}{n-1} A(\mathcal{L}, \delta, (\underbrace{2,\ldots,2}_{n}, \underbrace{3,\ldots,3}_{\ell-n}), (n+1, n+2, \ldots, n+\ell-1, n+\ell-1))$$

geometrically isolated roots in $\mathbb{C}^n$ of degree $\leq \delta$ over $\mathcal{L}$, according as we are in the local or global case. In particular, for each bound, the first $\sigma_{\mathcal{L}}(F)+1$ summands suffice if $\sigma_{\mathcal{L}}(F) \leq 2$.

In closing, let us point out a topological anomaly: Over $\mathbb{R}$, one can go even farther and bound the number of connected components of the zero set of a multivariate polynomial in terms of additive complexity [Gri82,Ris85]. Unfortunately, since $\mathbb{Q}_p$ is totally disconnected as a topological space [Kob84], one can not derive any obvious analogous statement in our arithmetic setting. This is why we consider only geometrically isolated roots in the multivariate case. Nevertheless, it would be quite interesting to know if one could bound the number of higher-dimensional **irreducible** components defined over $\mathcal{L}$ in terms of additive complexity, when $\mathcal{L}$ is a $\mathfrak{p}$-adic field.

3 Proving Theorems 1–3

We will give a proof of Theorem 3 which simultaneously yields theorems 1 and 2 for free.

Proof of Theorem 3 (and Theorems 1 and 2): First note that by the definition of additive complexity, $(x_1, \ldots, x_n) \in \mathcal{L}^n$ is a geometrically isolated root of $F \implies (X_1, \ldots, X_{n+s}) \in \mathcal{L}^{n+s}$ is a geometrically isolated root of the polynomial system $G = \mathbf{O}$, where the corresponding equations are exactly

$$c^{(1)}_{n+s+1} \prod_{i=1}^{n+s} X_i^{m^{(1)}_{i,n+s+1}} = 0 \quad , \ldots , \quad c^{(k)}_{n+s+1} \prod_{i=1}^{n+s} X_i^{m^{(k)}_{i,n+s+1}} = 0,$$

$$X_{n+1} = c_{n+1} \left(\prod_{i=1}^{n} X_i^{m_{i,n+1}} \right) + d_{n+1} \left(\prod_{i=1}^{n} X_i^{m'_{i,n+1}} \right)$$

$$\vdots$$

$$X_{n+s} = c_{n+s} \left(\prod_{i=1}^{n+s-1} X_i^{m_{i,n+s}} \right) + d_{n+s} \left(\prod_{i=1}^{n+s-1} X_i^{m'_{i,n+s}} \right),$$

where $s:=\sigma_{\mathcal{L}}(F)$, $X_i=x_i$ for all $i\in\{1,\ldots,n\}$, and the c_i, d_i, $c_i^{(j)}$, $m_{i,j}$, and $m'_{i,j}$ are suitable constants. This follows easily from the fact that corresponding quotient rings $\mathcal{L}[x_1]/\langle f\rangle$ and $\mathcal{L}[X_0,\ldots,X_s]/\langle G\rangle$ are isomorphic, thus making $\mathbb{C}_p[x_1]/\langle f\rangle$ and $\mathbb{C}_p[X_0,\ldots,X_s]/\langle G\rangle$ isomorphic, where $\mathbb{C}_p$ denotes the completion of the algebraic closure of $\mathbb{Q}_p$. In particular, $k\leq n$ easily implies that F has no geometrically isolated roots in $\mathcal{L}^n$ at all, so we can assume that $k\geq n$.

So we now need only count the geometrically isolated roots of G in $\mathcal{L}^{n+s}$ (or the geometrically isolated roots of F in $\mathbb{C}^{n+s}$ of degree $\leq\delta$ over $\mathcal{L}$) precisely enough to conclude. Toward this end, note that the first n equations of $G=\mathbf{O}$ imply that at least n distinct X_i must be 0, for otherwise $(X_1,\ldots,X_{n+s})$ would not be an isolated root. Note also that if we have n of the variables $X_1,\ldots,X_{n+\ell}$ equal to 0, then the first $n+\ell$ equations of G completely determine $(X_1,\ldots,X_{n+\ell})$. Furthermore, by virtue of the last $s-\ell$ equations of G, the value of $(X_1,\ldots,X_{n+\ell})$ **uniquely** determines the value of $(X_{n+\ell+1},\ldots,X_{n+s})$. So it in fact suffices to find the total number of geometrically isolated roots (with all coordinates nonzero) of all systems of the form $G'=\mathbf{O}$, where the equations of G' are exactly $(0=0)$ or

$$\varepsilon_1 X_{n+1}=c_{n+1}\left(\prod_{i=1}^{n}X_i^{m_{i,n+1}}\right)+d_{n+1}\left(\prod_{i=1}^{n}X_i^{m'_{i,n+1}}\right)$$

$$\vdots$$

$$\varepsilon_\ell X_{n+\ell}=c_{n+\ell}\left(\prod_{i=1}^{n+\ell-1}X_i^{m_{i,n+\ell}}\right)+d_{n+\ell}\left(\prod_{i=1}^{n+\ell-1}X_i^{m'_{i,n+\ell}}\right),$$

where $\varepsilon_i\in\{0,1\}$ for all i, $X_{n+\ell}=\varepsilon_\ell=0$, exactly $n-1$ of the variables $X_1,\ldots,X_{n+\ell-1}$ have been set to 0, and ℓ ranges over $\{1,\ldots,n\}$. Note in particular that the $j^{\underline{\text{th}}}$ equation involves no more than $n+j$ variables for all $j\in\{1,\ldots,\ell-1\}$, and that the $\ell^{\underline{\text{th}}}$ equation involves no more than $n+\ell-1$ variables.

To conclude, we thus see that G has no more than

$$1\ \ ,\ \ 1+B(\mathcal{L},2,1)\ \ ,\ \ \rho(\mathcal{L}):=1+B(\mathcal{L},2,1)+(r_n+B(\mathcal{L},2,1)B(\mathcal{L},3,1))\ \ ,\ \ \text{or}$$

$$\rho(\mathcal{L})+\sum_{\ell=3}^{s}\binom{n+\ell-1}{n-1}B(\mathcal{L},(\underbrace{2,\ldots,2}_{n},\underbrace{3,\ldots,3}_{\ell-n}),(n+1,n+2,\ldots,n+\ell-1,n+\ell-1))$$

geometrically isolated roots in $\mathcal{L}^{n+s}$ in the local case, according as s is 0, 1, 2, or ≥ 3, where r_n is 0 or 1 according as $n=1$ or $n\geq 2$. The corresponding statement for the global case, where we replace $B(\mathcal{L},m,N)$ by $A(\mathcal{L},\delta,m,N)$ throughout and count geometrically isolated roots in $\mathbb{C}^{n+s}$ of degree $\leq\delta$ over $\mathcal{L}$ instead, is also clearly true. This proves theorem 3.

Theorems 1 and 2 then follow immediately by specializing the above formulae to $n=1$, applying Arithmetic Multivariate Descartes' Rule, and performing an elementary calculation. ■

Remark 6 *It follows immediately from our proof that we can restate theorems 1 and 2 in sharper intrinsic terms. That is, the bounds from our proof above can* *immediately incorporate any new upper bounds for the quantities* $B(\mathcal{L}, m, N)$ *and* $A(\mathcal{L}, \delta, m, N)$. $\diamond$

Remark 7 *Note that the same proof will essentially work verbatim if we replace* $\mathcal{L}$ *throughout by* **any** *field admitting a multivariate analogue of Descartes' Rule.* $\diamond$[4]

Remark 8 *By taking* $(d, n, p) = (1, 1, 2)$ *in the refined bound from our proof (and recalling remark 5), we get improved upper bounds of* 15, 25089, *or* 3235713 *for the number of* 2*-adic rational roots of an* f *with* $\sigma_{\mathbb{Q}_2}(f)$ *equal to* 2, 3, *or* 4. *Note also that the polynomials* x *and* $x(x^2-1)$ *show that our lower bounds are sharp for* $\sigma_{\mathbb{Q}_2}(f) \in \{0, 1\}$, *for at least half the primes* p. $\diamond$

Acknowledgement

The author thanks the two anonymous referees for their astute comments. Special thanks also go to Mike Shub for help with a bibliographic point.

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.

[Ful98] Fulton, William, *Intersection Theory,* $2^{\underline{\text{nd}}}$ ed., Ergebnisse der Mathematik und ihrer Grenzgebiete 3, **2**, Springer-Verlag, 1998.

[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.

[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.

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

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

[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.

[4] In particular, via the approach of our proofs, it is possible to improve slightly the bounds of [Gri82,Ris85] over $\mathbb{R}$. We leave this as an exercise for the interested reader.

[Roj00] ________________, *"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).

[Roj02] ________________, *"Arithmetic Multivariate Descartes' Rule,"* Math ArXiV preprint `math.NT/0110327`, submitted for publication.

[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.

[SS95] Shub, Mike and Smale, Steve, *"On the Intractibility of Hilbert's Nullstellensatz and an Algebraic Version of 'NP not equal to P?',"* Duke Math J., Vol. 81 (1995), pp. 47–54.

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