New Explicit Root Counts for p-adic Circuit Systems

Joshua Goldstein, J. Maurice Rojas
Texas A&M University
{jgoldstein345,rojas}@tamu.edu
College Station, TX

Henry Stone
henstone@umich.edu
University of Michigan
Ann Arbor, MI

Arnaldo Vera
arnaldo.vera3@upr.edu
University of Puerto Rico
San Juan, Puerto Rico

1 Introduction

Fewnomial theory began by establishing (finite) upper bounds on the number of real non-degenerate roots of any $n \times n$ system of real polynomials, solely as a function of n and the number of distinct exponent vectors in the underlying monomial term expansions. Khovanski and Sevastyanov proved the first explicit bounds around 1980 [5, 6], and then an analogue over the p-adic rationals, $\mathbb{Q}_p$, (with $p \in \mathbb{N}$ prime) was found by Denef and van den Dries around 1988 [3, Sec. 3.4]. However, explicit bounds over $\mathbb{Q}_p$ are known only when $n = 1$ ([3, Sec. 3.5], [8, Thm. 2 & pg. 279]), or when $n \geq 2$ and the underlying zero sets satisfy a very restrictive condition: *tropical genericity (with respect to p)* (see [11] and below). We give the first explicit upper bounds over $\mathbb{Q}_p$ (for $p \geq n+1$) for a broad class of tropically *non*-generic systems with $n+2$ exponent vectors, where no bounds had been available before: See Theorem 1.5 below. Let us first review the simplest systems over $\mathbb{R}$ and $\mathbb{Q}_p$.

1.1 Simplex and Circuit Systems

The analogies between real and p-adic fewnomial theory are still not completely understood, but a good starting point is to define a p-adic analogue of how the positive ray $\mathbb{R}_+$ is embedded in $\mathbb{C}$: We let $\mathbb{Q}_{p,+} := \bigsqcup_{k\in\mathbb{Z}} p^k (1+\mathbb{Z}_p)$, i.e., the set of p-adic rationals with most significant digit 1. For any field K we let $K^* := K \setminus \{0\}$. Just as $(\mathbb{R}^*)^n$ can be partitioned into 2^n cosets of the subgroup $\mathbb{R}_+^n$, $(\mathbb{Q}_p^*)^n$ can be partitioned into $(p-1)^n$ cosets of the subgroup $\mathbb{Q}_{p,+}^n$, and we focus on counting roots there to simplify matters.

Definition 1.1. *Let $A = \{a_1, \ldots, a_t\} \subset \mathbb{Z}^n$ where $a_j = (a_{1,j}, \ldots, a_{n,j})$ for all j, and set $x^{a_j} = x_1^{a_{1,j}} \cdots x_n^{a_{n,j}}$. If $F = (f_1, \ldots, f_n) \in \left(K\left[x_1^{\pm 1}, \ldots, x_n^{\pm 1}\right]\right)^n$, with $f_i(x) = \sum_{j=1}^t c_{i,j} x^{a_j}$ for all i, and t is the number of distinct exponent vectors in the monomial term expansions of $f_1, \ldots, f_n$, then we call F a* t-nomial $n \times n$ system (over K) supported in A. *We call a root $\zeta = (\zeta_1, \ldots, \zeta_n) \in K^n$ of F* non-degenerate *if and only if the Jacobian matrix $\left[\frac{\partial f_i}{\partial x_j}\right]\Big|_{x=\zeta}$ is invertible, and let $N_p^{t,n}$ (resp. $N_\infty^{t,n}$) denote the maximal number of non-degenerate roots of F in $\mathbb{Q}_{p,+}^n$ (resp. $\mathbb{R}_+^n$), over all t-nomial $n \times n$ systems F over K, assuming $K = \mathbb{Q}_p$ (resp. $K = \mathbb{R}$). Finally, we let $\mathbb{C}_p$ denote the p-adic complex numbers [10] and we say a condition $\mathcal{P}(z_1, \ldots, z_N)$, depending on parameters $z_1, \ldots, z_N \in \mathbb{C}_p$, is* generic *(or* generically true*) if and only if there is a polynomial $Q \in \mathbb{C}_p[z_1, \ldots, z_N] \setminus \{0\}$ such that $Q(z_1, \ldots, z_N) \neq 0 \Longrightarrow \mathcal{P}(z_1, \ldots, z_N)$ is true.* $\diamond$

Remark 1.2. *We will assume throughout that A does not lie in an affine $(n-1)$-plane. This is true generically, and implies $t \geq n+1$ as well. Our assumption on A is a simple way to ensure that, under a generic choice of $[c_{i,j}]$, any roots of F in $(\mathbb{C}_p^*)^n$ are non-degenerate.* $\diamond$

The cases $t = n+1$ and $t = n+2$ are respectively known as the *simplex case* and the *circuit case*. We will focus on the circuit case, but it will be helpful to recall the simplex case briefly.

Proposition 1.3. *[4] We have $N_p^{n+1,n} = \max\{1, 4-p\}^n$. In particular, if F is a simplex system with only finitely many roots in $\mathbb{Q}_{p,+}^n$, then all its roots in $\mathbb{Q}_{p,+}^n$ are non-degenerate.* ■

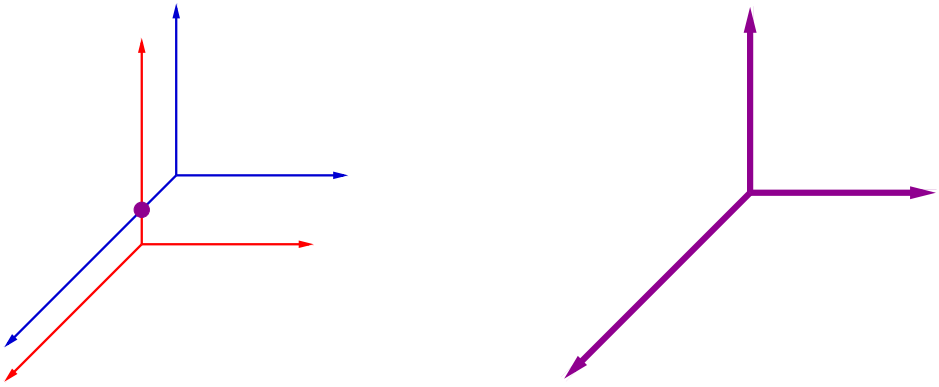
The analogous statement over $\mathbb{R}_+$ is simpler: $N_\infty^{n+1,n} = 1$, and the final assertion on non-degeneracy continues to hold over $\mathbb{R}_+$. (See, e.g., [12].) The aforementioned bounds in the simplex case are tight, both over $\mathbb{R}_+$ and $\mathbb{Q}_{p,+}$ for all prime p: $F = (x_1^2 - 1, \ldots, x_n^2 - 1)$ attains the respective bounds over $\mathbb{R}_+$ and $\mathbb{Q}_{2,+}$ $(= \mathbb{Q}_2)$, while $F = (x_1^{p-1} - 1, \ldots, x_n^{p-1} - 1)$ attains the bounds over $\mathbb{Q}_{p,+}$ for all $p \geq 3$. Moreover, the maximal finite number of roots in $(\mathbb{R}^*)^n$ (resp. $(\mathbb{Q}_p^*)^n$) for a simplex system over $\mathbb{R}$ (resp. $\mathbb{Q}_p$) is 2^n (resp. $\max\{2, p-1\}^n$). The preceding examples also attain these bounds.

For the *circuit* case over $\mathbb{R}$ we have $N_\infty^{n+2,n} = n + 1$ [1]. However, for circuit systems over $\mathbb{Q}_p$, we only know $N_p^{n+2,n} \geq n + 1$ [9, Thm. 1.6], and $N_p^{n+2,n} < \infty$ [3, Sec. 3.4]. For *tropically generic* $n \times n$ circuit systems, we can prove an upper bound of $n + 1$ for the number of non-degenerate roots in $\mathbb{Q}_{p,+}^n$ [9, Rem. 1.7 and Sec. 3.1]. Briefly, we define the *p-adic tropical variety of* f_i, $\mathrm{Trop}_p(f_i)$, to be the Euclidean closure of

$$\{(\mathrm{ord}_p \zeta_1, \ldots, \mathrm{ord}_p \zeta_n) \mid f_i(\zeta) = 0 \text{ and } \zeta \in (\mathbb{C}_p^*)^n\},$$

in $\mathbb{R}^n$, where $\mathrm{ord}_p : \mathbb{C}_p \longrightarrow \mathbb{Q}$ denotes the *p-adic valuation map* [10] which satisfies $\mathrm{ord}_p p = 1$ [9]. We then call F tropically generic (with respect to p) if and only if $\mathrm{Trop}_p(f_1), \ldots, \mathrm{Trop}_p(f_n)$ intersect transversally, i.e., at any $v \in \mathrm{Trop}_p(f_1) \cap \cdots \cap \mathrm{Trop}_p(f_n)$ the underlying tangent spaces of the $\mathrm{Trop}_p(f_i)$ intersect at just 1 point. (That $\mathrm{Trop}_p(f_i)$ is piece-wise linear is a fact due to Mikhail M. Kapranov, from around 2000.)

Example 1.4. *Consider the system* $F := (1 + x_1 + x_2, 1 + 3x_1 + 9x_2)$. *Clearly,* F *has the unique rational root* $\zeta = (\zeta_1, \zeta_2) = (-4/3, 1/3)$. *It is not hard to see that when* $p = 3$ *(resp.* $p \geq 5$*),* $\mathrm{Trop}_p(f_1)$ *and* $\mathrm{Trop}_p(f_2)$ *intersect transversally (resp. non-transversally), as drawn below:*



$p = 3$ $\qquad$ $p \geq 5$

In particular, in the right-hand illustration, the tangent spaces intersect at just one point only when $v = (0, 0)$*, and intersect in a* 1*-dimensional subspace otherwise. More to the point, the intersection of* $\mathrm{Trop}_3(f_1)$ *and* $\mathrm{Trop}_3(f_2)$ *at* $(-1, -1)$ *correctly predicts* $(\mathrm{ord}_3(-4/3), \mathrm{ord}_3(1/3))$. *However, for* $p \geq 5$, $\mathrm{Trop}_p(f_1) \cap \mathrm{Trop}_p(f_2)$ *merely* contains*, and does* not *predict,* $(\mathrm{ord}_p(-4/3), \mathrm{ord}_p(1/3)) = (0, 0)$. $\diamond$

1.2 Our Main Result

With the goal of finding an explicit upper bound for $N_p^{n+2,n}$ we propose a hypothesis which, unlike tropical genericity, *holds with high probability as* $p \longrightarrow \infty$. Our main result makes use of a particular univariate reduction, called a *Gale Dual Form*, for any $n \times n$ circuit system F over $\mathbb{Q}_p$. (We note that the Gale Dual Form was originally used in [2] over $\mathbb{R}$ and $\mathbb{C}$, and we are modifying it slightly for use over $\mathbb{Q}_p$ and $\mathbb{C}_p$.) To describe this reduction, first let $\widehat{A} \in \mathbb{Z}^{(n+1)\times(n+2)}$ be the matrix with ith column the transpose of $(1, a_i)$ (which has rank $n + 1$ thanks to our earlier assumption on A), and let $b \in \mathbb{Z}^{(n+2)\times 1}$ be any generator for the right nullspace of $\widehat{A}$ such that the coordinates of b have gcd 1. By dividing each f_i by $x^{a_{n+2}}$, we may assume a_{n+2} is the origin $\mathbf{O}$. Via row reduction on the monomials of F we may assume that, for generic coefficient matrix $[c_{i,j}]$, we have $F = (x^{a_1} - \gamma_{1,1}x^{a_{n+1}} - \gamma_{1,0}, \ldots, x^{a_n} - \gamma_{n,1}x^{a_{n+1}} - \gamma_{n,0})$ for some $\gamma_{i,j} \in \mathbb{Q}_p^*$. We then call the rational function $g(u) := -1 + u^{b_{n+1}} \prod_{i=1}^n (\gamma_{i,1}u + \gamma_{i,0})^{b_i}$ a *Gale Dual Form* of F, and set $\gamma_{n+1,1} := 1$ and $\gamma_{n+1,0} := 0$ as well.

Setting $u = x^{a_{n+1}}$ it is not hard to show that the number of non-degenerate roots of g in $\mathbb{Q}_p^*$ is exactly the number of roots of F in $(\mathbb{Q}_p^*)^n$, provided all $n \times n$ sub-matrices of the coefficient matrix $[c_{i,j}]$ are invertible. This is true generically, but a slightly stronger assumption, and some additional algebraic work, ultimately yields our main theorem:

Theorem 1.5. *Suppose $p \in \mathbb{N}$ is a prime with $p \geq n+1$ and F is an $n \times n$ circuit system F over $\mathbb{Q}_p$ with Gale Dual Form $g(u) := -1 + u^{b_{n+1}} \prod_{i=1}^{n} (\gamma_{i,1} u + \gamma_{i,0})^{b_i}$ such that*
(a) $\gamma_{i,j} \neq 0$ for all $(i,j) \in \{1,\ldots,n\} \times \{0,1\}$ and
(b) $\{-\gamma_{i,0}/\gamma_{i,1} \mid b_i > 0 \text{ and } i \in \{1,\ldots,n+1\}\} \cap \{-\gamma_{i,0}/\gamma_{i,1} \mid b_i < 0 \text{ and } i \in \{1,\ldots,n+1\}\}$ mod p is empty. Then F has no more than $2n+2$ non-degenerate roots in $\mathbb{Q}_{p,+}^n$. In particular, Hypothesis (a) holds generically and, for fixed F, Hypothesis (b) holds for all p sufficiently large.

Example 1.6. *Consider the (disjoint) sets of rational numbers $\left\{\frac{95}{46}, \frac{234}{397}\right\}$ and $\left\{\frac{339}{512}, \frac{94}{244}, \frac{282}{1952}\right\}$. Then for $p \leq 397$ prime, we can have one of the preceding fractions cease to be well-defined and/or have the sets intersect mod p. For instance, the mod 3 reductions of these sets are respectively $\{2,0\}$ and $\{0,1\}$, which intersect. However, for prime $p > 397$, the mod p reductions of our two first sets remain disjoint.* $\diamond$

The proof of Theorem 1.5 is based on the p-adic root counting techniques from [13, Lemma 2.18], which in turn use a tree-like data structure from [7] to encode roots of polynomials in $\mathbb{Z}/(p^k)$. In future work, we hope to remove Hypotheses (a) and (b) and at last give an explicit upper bound for $N_p^{n+2,n}$, at least for $p \geq n+1$.

There are in fact simple examples violating Condition (b), already for $n=1$:

Example 1.7. *Consider $g(u) := u^{10}(10u - 738)^{-1} - 1$ and $p = 3$. Then the mod 3 reductions of the sets from Condition (b) reduce to $\{0\}$ and $\{0\}$. It also happens to be the case that g is the Gale Dual Form for $x^{10} - 10x + 738$, which has exactly 4 roots in $\mathbb{Q}_{3,+}$ (easily verifiable via, say, `Maple`).* $\diamond$

1.3 Proof Overview

Let $\mathbb{F}_p$ denote the finite field with p elements.

Definition 1.8. *A root $\zeta \in \mathbb{F}_p$ of a polynomial $f \in \mathbb{F}_p[x_1]$ is said to have* multiplicity *m if and only if $(x_1 - \zeta)^m$ divides f but $(x_1 - \zeta)^{m+1}$ does not.* $\diamond$

The following lemma is the key to our proof.

Lemma 1.9. *In the notation of Theorem 1.5, if Conditions (a) and (b) hold for the Gale Dual g, and $p \geq n+1$, then the multiplicity of any root $\zeta \in \mathbb{F}_p$ of g is at most $n+1$.*

Succinctly, the techniques from [7, 13] imply that we can bound from above the number of roots of g in $\mathbb{Q}_{p,+}$ by the sums of the multiplicities of the roots 0 and 1 of the mod p reduction of g. So our main theorem then follows easily from Lemma 1.9.

To prove Lemma 1.9 we need a technical lemma concerning the derivatives of slight variants of our Gale Dual Forms.

Lemma 1.10. *Let $f(x) = \prod_{i=1}^{n+1} (x + \alpha_i)^{b_i}$ where $\alpha_i \in \mathbb{Q}$ and $b_i \in \mathbb{Z}$ for each i. Then for each integer $k \geq 1$ we have that*

$$f^{(k)} = \sum_{i=0}^{k-1} (-1)^{k-i-1} (k-i-1)! \binom{k-1}{k-i-1} \Omega_{k-i} f^{(i)}$$

where

$$\Omega_k = \sum_{i=1}^{n+1} \frac{b_i}{(x+\alpha_i)^k}.$$

In the full version of this paper (currently in progress), we will provide all missing proofs, and further elaborate the tree-like data structure that helps us encode roots in $\mathbb{Z}_p$.

References

[1] B. Bertrand, F. Bihan, and F. Sottile. Polynomial systems with few real zeroes. *Mathematische Zeitschrift*, 253(2):361–385, 2006. doi: 10.1007/s00209-005-0912-8. URL `https://doi.org/10.1007/s00209-005-0912-8`.

[2] F. Bihan and F. Sottile. New fewnomial upper bounds from gale dual polynomial system. *Moscow Mathematical Journal*, 7:387–407, 2007. doi: https://doi.org/10.17323/1609-4514-2007-7-3-387-407. URL `http://mi.mathnet.ru/mmj287`.

[3] J. Denef and L. van den Dries. p-adic and real subanalytic sets. *Annals of Mathematics*, 128(1): 79–138, 1988. ISSN 0003486X, 19398980. URL `http://www.jstor.org/stable/1971463`.

[4] J. Goldstein. *New Explicit Bounds in p-adic Fewnomial Theory*. doctoral dissertation, Texas A&M University, College Station, in progress, 2026.

[5] A. G. Khovanskiĭ. A class of systems of transcendental equations. *Soviet Mathematics Doklady*, 22 (3):762–765, 1980.

[6] A. G. Khovanskiĭ. *Fewnomials*, volume 88 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, Rhode Island, 1991.

[7] L. Kopp, N. Randall, J. M. Rojas, and Y. Zhu. Randomized polynomial-time root counting in prime power rings. *Mathematics of Computation*, 89(321):373–385, 2020.

[8] H. W. Lenstra, Jr. On the factorization of lacunary polynomials. In *Proceedings of the International Conference on Number Theory organized by the Stefan Banach International Mathematical Center in Honor of the 60th Birthday of Andrzej Schinzel (June 30–July 9, 1997, Zakopane-Kościelisko, Poland)*, volume 1 of *Number Theory in Progress*, pages 277–291, Berlin, 1999. De Gruyter. doi: https://doi.org/10.1515/9783110285581.277.

[9] K. Phillipson and J. M. Rojas. Fewnomial systems with many roots, and an adelic tau conjecture. In O. Amini, M. Baker, and X. Faber, editors, *Proceedings of Bellairs workshop on Tropical and Non-Archimedean Geometry (May 6–13, 2011, Barbados)*, volume 605 of *Contemporary Mathematics*, pages 45–71, Providence, Rhode Island and Montreal, Quebec, Canada, 2013. American Mathematical Society and Centre de Recherches Mathématiques. doi: https://doi.org/10.1090/conm/605.

[10] A. M. Robert. *A Course in p-adic Analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, New York, 2000.

[11] J. M. Rojas. Arithmetic multivariate descartes rule. *American Journal of Mathematics*, 126(1):1–30, 2004.

[12] J. M. Rojas. Counting real roots in polynomial-time via diophantine approximation. *Foundations of Computational Mathematics*, 24(2):639–681, 2024.

[13] J. M. Rojas and Y. Zhu. Root repulsion and faster solving for very sparse polynomials over p-adic fields. *J. Number Theory*, 241:655–699, 2022. ISSN 0022-314X,1096-1658. doi: 10.1016/j.jnt.2022.01.013. URL `https://doi.org/10.1016/j.jnt.2022.01.013`.