Appendix to "An Introduction to Algorithmic Fewnomial Theorem over $\mathbb{R}$"

J. Maurice Rojas[1]

March 12, 2025

Abstract

These are some additional notes and references for my brief survey "An Introduction to Algorithmic Fewnomial Theorem over $\mathbb{R}$," which should be appearing in the AMS Notices by July 2025.

We now go over some finer points and proof sketches that needed to be skipped in [Roj25] due to the length restrictions of the AMS Notices: In what follows, all sections refer to [Roj25]. We also point out that [Mun00], [Pra04], and [SW05] are excellent references respectively on basic topology, linear algebra, and numerical polynomial system solving.

Notes on Section 1.1

The notion of "simplicity" for equations, or algebraic varieties, is primordial and can naturally be approached from many points of view. Another exposition, focussing more on geometry (and *rational connectedness*) than computational complexity, can be found in the beautiful paper [Kol01].

Notes on Section 1.2

The exposition here mentions roots in $(\mathbb{R}_+ \cup \{0\})^n$ while the rest of the paper focusses entirely on roots in $\mathbb{R}^n_+$. This is for technical simplicity and, in some applications, it is perfectly reasonable to assume that only a fixed subset of coordinates of the roots will be set to 0. However, algorithmically, counting affine roots (*without* prior knowledge of which coordinates might vanish) is significantly harder than counting roots with all coordinates nonzero.

A concrete example comes from counting *complex* roots for binomial ideals:

Theorem 5.1 *Let $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$ be binomials. Let v_i denote the difference of the exponent vectors of f_i (the order of subtraction will not matter in what follows), and A the $n \times m$ matrix whose ith column is v_i. Finally, let N be $|\det A|$ or 0, according as $m=n$ or not. Then the number of roots of $F := (f_1, \ldots, f_m)$ in $(\mathbb{C}^*)^n$ is either N or ∞, and we can decide which (and compute the value of N) in polynomial-time. However, computing the number of roots of F in $\mathbb{C}^n$ is $\#\mathbf{P}$-hard.* ■

The first part of Theorem 5.1 follows easily from framework of Section 1.5. The second part is due to Cattani and Dickenstein [CD07]. A real analogue of this theorem should hold and follow straightforwardly from these methods.

[1]Department of Mathematics, Texas A&M University TAMU 3368, College Station, Texas 77843-3368, USA. e-mail: rojas@math.tamu.edu , Web Page: people.tamu.edu/~rojas .

Notes on Section 1.3

Theorem 1.6 is an amalgam of earlier results. One key geometric idea underlying Theorem 1.6 is the path connectivity of $\mathrm{GL}_n^+(\mathbb{R})$ (the group of real $n \times n$ matrices with positive determinant). This fact is standard in differential geometry courses and can be proved, say, via the QR-decomposition algorithm from linear algebra.

To prove Theorem 1.6, let

$$g(y) := c_1 e^{a_1 \cdot y} + \cdots + c_{n+1} e^{a_{n+1} \cdot y}.$$

It is a simple exercise to show that the real zero set of g is ambiently isotopic in $\mathbb{R}^n$ to the positive zero set of $f(x) = c_1 x^{a_1} + \cdots + c_{n+1} x^{a_{n+1}}$ when the a_i all lie in $\mathbb{Z}^n$.

By working with g instead of f, and then allowing the a_i to lie in $\mathbb{R}^n$, we will in fact have enough flexibility to enable a short proof of Theorem 1.6. In particular, dividing by $e^{a_1 \cdot y}$, we may assume $a_1 = \mathbf{O}$. The path connectivity of $\mathrm{GL}_n^+(\mathbb{R})$ then easily implies an isotopy between $Z_{\mathbb{R}}(g)$ and

$$Z_{\mathbb{R}}(c_1 + c_2 e^{y_1} + \cdots + c_{n+1} e^{y_n}).$$

If one then translates the variables y_i then one can clearly rescale all the c_i to absolute value 1, i.e., one then obtains an isotopy to $Z_{\mathbb{R}}(\pm 1 \pm e^{y_1} \pm \cdots \pm e^{y_n})$ for some suitable choice of signs. Clearly then, the only way this real zero set is empty is when all the signs are the same. This proves Assertion (1). Assertion (0) then follows easily since our preceding isotopy also induces an isotopy of $\{x \in \mathbb{R}_+^n \mid f(x) > 0\}$ to one of the pieces of the complement of a hyperplane in $\mathbb{R}_+^n$.

Assertion (2) is immediate after taking coordinatewise logarithms of the equation $c_1 x^{a_1} = c_2 x^{a_2}$.

As for Assertion (3), the first part is just a special case of [AKNR18, Assertion (1)(a)]. The second part is [AKNR18, Lemma 3.2, Assertion (2)].

Notes on Section 1.4

[BCS97] is an outstanding reference on algebraic complexity, as well as the subtleties of arithmetic complexity and computational models for algebraic computation.

Lemma 1.11 is due to Yinyu Ye [Ye94] and his methods extend to a broader class of analytic functions satisfying certain convexity conditions. The fast approximation of radicals goes back centuries and even the computation of square roots (for power series rings) still admits further improvements: See, e.g., [Har11].

A detailed account on efficiently numerically approximating complex (and real) roots of arbitrary univariate polynomials is [Sag10], and an important older reference on complexity lower bounds for approximating roots is [Ren87]. Also, an outstanding reference with a wealth of classical results on the distribution of the roots of univariate polynomials is [RS02].

Notes on Section 1.5

A recent paper on the bound mentioned for the matrix multiplication exponent is [ADVWXXZ24].

The complexity estimates on Smith Factorization were derived from [Sto00]. [Sch86] also provides a nice account of Hermite Factorization.

Notes on Section 1.6

That the positive solutions of a degenerate binomial system are ambiently isotopic to a subspace follows routinely from our framework: Again, one can simplify matters via an exponential change of variables (which can also be turned into an isotopy to the original positive zero set) to instead work with a system of the following form:

$$(e^{a_1\cdot y},\ldots,e^{a_n\cdot y}) = (c_1,\ldots,c_n).$$

One can then simply apply the change of variables $y \mapsto A^{-1}y$ to reduce to a system of the form $(e^{y_1},\ldots,e^{y_r},e^0,\ldots,e^0) = (c_1,\ldots,c_r,c_{r+1},\ldots,c_n)$. where r is the rank of the matrix A. This last system clearly has a real solution if and only if $c_{r+1} = \cdots = c_n = 1$, in which case, taking logs, we clearly obtain an isotopy to a real subspace.

The notion of approximate root goes back to [Sma81].

A randomized version of Theorem 1.23, counting arithmetic complexity instead, appears in [PPR19].

Notes on Section 2.2

The key new ingredient to the proof of Corollary 2.11 is the use of *anti-concentration* of certain random variables: The main probabilistic tools used in [DEPR24] come from [RV15].

Notes on Section 2.3

That an $n\times n$ circuit system never has more than $n+1$ isolated roots in $\mathbb{R}^n_+$ was first proved in [BBS05].

Some relevant references on condition numbers for random sparse polynomial systems are [EPR19, EPR21, T-CT20].

Notes on Section 3

The cryptic final sentence on there being p-adic analogues of the main results can be elaborated as follows. (See [AIRR12, RZ22] for further background.)

First, while some of the natural questions on solving ((S1), (S2), and (S5) — on detecting, counting, and approximating roots) still make sense over $\mathbb{Q}_p$, Questions (S3) and (S4) (on connected components and isotopy type) no longer make sense over $\mathbb{Q}_p$ since $\mathbb{Q}_p$ is totally disconnected! Nevertheless, the notion of p-adic analytic manifold goes back to 1964 work of Serre [Ser64]. So it would be valuable to explore whether one could still prove that n-variate $(n+k)$-nomial hypersurfaces over $\mathbb{Q}_p$ (or their restriction to $(1+p\mathbb{Z}_p)^n$) can always be partitioned into a "small" number (depending only on n and k) of p-adic manifolds of suitably restricted type. An analogous statement for isolated roots of *systems* of equations over $\mathbb{Q}_p$ was proved in [DvdD88] but with no explicit upper bounds for $n\geq 2$. Explicit bounds for the special case $n=1$ can be found in [Len99, AK11] and, under the assumption of *tropical genericity*, explicit bounds in the cases $n\geq 2$ were derived in [Roj04].

Another important detail is the notion of (generalized) phase: Just as a positive real number x can be thought of as a complex number with *phase* $\frac{x}{|x|}=1$ (or *argument* $\mathrm{Imag}(\mathrm{Log}x)=0$),

the analogous notion over $\mathbb{Q}_p$ is *most significant digit*. In particular, any $x \in \mathbb{Q}_p$ can be written in the form $\sum_{k=v}^{\infty} x_k p^k$ with $x_k \in \{0, \ldots, p-1\}$ for all $k \geq v$, $v = \mathrm{ord}_p x$, and $x_v \neq 0$ (where ord_p denotes the standard p-adic valuation on $\mathbb{Q}_p$ [Rob00]). We then call x_v the *most significant digit* of x. The natural p-adic analogue of $\mathbb{R}_+$ is then the union $\bigcup_{k\in\mathbb{Z}} p^k(1+p\mathbb{Z}_p)$, i.e, the set of all p-adic rational numbers with most significant digit 1.

Finally, it is important to note that the notion of *p-adic tropical variety*

$$\mathrm{Trop}_p(f) := \{\mathrm{ord}_p x \mid f(x) = 0 \ , \ x \in (\mathbb{C}_p^*)^n\},$$

where $\mathrm{ord}_p(x_1, \ldots, x_n) := (\mathrm{ord}_p x_1, \ldots, \mathrm{ord}_p x_n)$, has been known at least since work of Kapranov around 2000 [Kap00], and the case $n = 1$ dates back to early 20th century work of Hensel (see, e.g., [Wei63, Ch. 3] and [RZ22, Thm. 2.3]). In fact, the use of a polytope (or rather, the slopes of its edges, or coordinates of its inner face normals) to exactly determine the norms of roots goes back to 17th century work of Newton on Puiseux series solutions to polynomial equations [New76, pp. 126–127].

Let $Z_{p,+}(f)$ denote the zero set of f in $(\bigcup_{k\in\mathbb{Z}} p^k(1+p\mathbb{Z}_p))^n$: This will be our p-adic rational analogue of $Z_+(f)$, assuming $f \in \mathbb{Z}\left[x_1^{\pm 1}, \ldots, x_n^{\pm 1}\right]$. Similary, the coordinate-wise valuation map $\mathrm{ord}_p(\cdot)$ will be the p-adic analogue of Log. We can then state the following analogues, over $\mathbb{Q}_p$, of our main results over $\mathbb{R}$:

Definition 1.2 While $\mathrm{Trop}_+(f)$ and $Z_+(f)$ are always ambiently isotopic to each other in $\mathbb{R}^n$ in the simplex case, $Z_{p,+}(f)$ can be uncountable and totally disconnected in the simplex case when $n \geq 2$. The more natural correspondence is then to consider $\mathrm{ord}_p Z_{p,+}(f)$ instead, just as we considered $\mathrm{Log} Z_+(f)$ to get a nice metric guarantee. However, while $\mathrm{Trop}_p(f)$ is still a polyhedral complex, $\mathrm{ord}_p Z_{p,+}(f)$ winds up instead being a subset of the integral points in $\mathrm{Trop}_p(f)$.

Theorem 1.6 As noted above, there is not yet a natural analogue of isotopy type for $Z_{p,+}(f)$. However, there is an interesting complexity wrinkle: While deciding the emptiness of $Z_+(f)$ can be done in linear time (simply by checking coefficient signs), deciding the emptiness of $Z_{p,+}(f)$ is **NP**-complete! This is contained in [AIRR12, Prop. 3 and Thm. 4, Ass. 3(a)] and, as observed by B. Poonen around 2005, **NP**-hardness persists even for *fixed* p (if n is allowed to vary). If $n = 1$ then we can in fact count the roots of binomials over $\mathbb{Q}_p$ in polynomial-time: A precise statement is in [RZ22, Cor. 2.8].

Lemma 1.11 & Corollary 1.14 A p-adic analogue is [RZ22, Thm. 2.21]. In particular, the notion of approximate root extends naturally to $\mathbb{Q}_p$, and polynomial bit-complexity persists... provided p is fixed. The technical reason for why the complexity is (unfortunately) linear in p is that computing dth roots in prime fields $\mathbb{F}_p$ is still not known to be doable in time polynomial in $\log p$ for $d \geq 3$, even if randomization is allowed. That square roots can be computed in randomized polynomial-time goes all the way back to work of A. Tonelli in the 19th century: See, e.g., [BS96, Ch. 7].

Theorem 1.13 The RBSP has a p-adic analogue: One instead asks for the most significant digit of $\prod_{i=1}^m (\alpha_i^{b_i}) - 1$. In particular, this can be accomplished once an explicit upper bound on $\mathrm{ord}_p(\prod_{i=1}^m (\alpha_i^{b_i}) - 1)$ is known, and such a bound is given by *Yu's Theorem on Linear Forms in p-adic Logarithms* [Yu94, Yu07]. The resulting bounds are sufficiently good

that the resulting p-adic analogue of RBSP can actually be solved within time similar to that stated in Theorem 1.13. This is pursued further in the Texas A&M Ph.D. thesis of Joshua Goldstein [Gol25].

Corollary 1.19 Using the notion of most significant digit, the corollary remains true if we simply replace $\mathbb{R}_+$, $\mathbb{R}^*$, and $\mathbb{C}^*$ respectively by $\bigcup_{k\in\mathbb{Z}} p^k(1+p\mathbb{Z}_p)$, $\mathbb{Q}_p^*$, and $\mathbb{C}_p^*$ [Gol25].

Theorem 1.23 Using the notion of most significant digit, there is a natural analogue on quickly finding approximate roots (in the sense of Smale) for $n \times n$ binomial systems over $\mathbb{Q}_p$ [Gol25].

Theorem 2.5 As stated above, classification up to isotopy breaks down. However, there is still the possibility of proving that $Z_{p,+}(f)$ can be partitioned into "few" p-adic manifolds of a restricted type.

Lemma 2.6 A p-adic analogue for this particular case is unknown.

Theorem 2.8 Here, one can at least assert that $\mathrm{ord}_p Z_{p,+}(f)$ is always a subset of the integral points of $\mathrm{Trop}_p(f)$.

Corollary 2.9 The p-adic analogue of the special case $n = 1$ was only recently proved: See [RZ22, Thm. 1.1]. As for $n \geq 2$, even the complexity of deciding $Z_{p,+}(f) \stackrel{?}{=} \emptyset$ remains unknown.

Theorem 2.10 & Corollary 2.11 p-adic analogues for these results are unknown.

Theorem 2.12 A p-adic analogue, giving a new upper bound on the number of isolated roots for circuit systems over $\mathbb{Q}_p$ is developed in [GRSV25, Gol25].

Problem 3.1 A p-adic analogue of Smale's 17th Problem appears in a 2011 NSF proposal by Rojas [Roj11]. Another p-adic analogue was stated independently by Tonelli-Cueto [T-C22].

References

[ADVWXXZ24] Josh Alman; Ran Duan; Virginia Vassilevska Williams; Yinzhan Xu; Zixuan Xu; and Renfei Zhou, *"More Asymmetry Yields Faster Matrix Multiplication,"* Math ArXiV preprint `2404.16349`

[AIRR12] Martíin Avendaño, Ashraf Ibrahim, J. Maurice Rojas, and Korben Rusek, *"Faster p-adic Feasibility for Certain Multivariate Sparse Polynomials,"* Journal of Symbolic Computation, special issue in honor of 60th birthday of Joachim von zur Gathen, vol. 47, no. 4, pp. 454–479 (April 2012).

[AKNR18] Martín Avendaño; Roman Kogan; Mounir Nisse; and J. Maurice Rojas, *"Metric Estimates and Membership Complexity for Archimedean Amoebae and Tropical Hypersurfaces,"* presented at MEGA 2013. Published in Journal of Complexity, Vol. 46, June 2018, pp. 45–65.

[AK11] Martín Avendaño and Teresa Krick, *"Sharp Bounds for the Number of Roots of Univariate Fewnomials,"* Journal of Number Theory, vol. 131 (1), pp. 1209–1228, 2011.

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

[BBS05] Benoit Bertrand, Frederic Bihan, and Frank Sottile, *"Polynomial Systems with Few Real Zeroes,"* Mathematisches Zeitschrift, 253 (2006), no. 2, pp. 361–385.

[BCS97] Peter Bürgisser; Michael Clausen; and M. Amin Shokrollahi, *Algebraic complexity theory,* with the collaboration of Thomas Lickteig, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 315, Springer-Verlag, Berlin, 1997.

[CD07] Eduardo Cattani and Alicia Dickenstein, *"Counting solutions to binomial complete intersections,"* J. Complexity 23 (2007), no. 1, pp. 82–107.

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

[DEPR24] Weixun Deng, Alperen Ali Ergür, Grigoris Paouris, and J. Maurice Rojas, *"Feasibility of Circuit Polynomials without Purple Swans,"* in Proceedings of ISSAC 2024, ACM Press, pp. 429–436.

[EPR19] Alperen Ali Ergür, Grigoris Paouris, and J. Maurice Rojas, *"Probabilistic Condition Number Estimates for Real Polynomial Systems I: A Broader Family of Distributions,"* Foundations of Computational Mathematics, Feb. 2019, Vol. 19, No. 1, pp. 131–157.

[EPR21] Alperen Ali Ergür, Grigoris Paouris, and J. Maurice Rojas, *"Smoothed analysis for the condition number of structured real polynomial systems,"* Math. of Comput., 90 (Sep. 2021), pp. 2161–2184.

[Gol25] Joshua Goldstein, *"Tropical Algorithms for p-adic Circuit Systems,"* doctoral dissertation, mathematics department, Texas A&M University, 2025.

[GRSV25] Joshua Goldstein, J. Maurice Rojas, Henry Stone, Arnaldo Vera, *"Solving p-adic Circuit Systems Faster,"* in preparation, 2025.

[Har11] David Harvey, *"Faster Algorithms for the Square Root and Reciprocal of Power Series,"* Math. of Comput. Vol. 80, No. 273, Jan. 2011.

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

[Kol01] János Kollár, *"Which are the simplest algebraic varieties,"* Bulletin of the American Mathematical Society, Vol. 38, No. 4, pp. 409–433, S 0273-0979(01)00917-X.

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

[Mun00] James R. Munkres, *Topology*, 2nd edition, Pearson, 2000.

[New76] Issac Newton, *letter to Oldenburg dated 1676 Oct 24,* in: The Correspondence of Isaac Newton, Vol II (1676-1687), H. W. Turnbull (ed.), pp. 126–127, Cambridge University Press, 1960.

[PPR19] Grigoris Paouris, Kaitlyn Phillipson, and J. Maurice Rojas, *"A Faster Solution to Smale's 17th Problem I: Real Binomial Systems,"* in proceedings of ISSAC 2019 (July 15-18, 2019, Beihang University, Beijing, China), ACM Press, 2019.

[Pra04] Victor V. Prasolov, *Problems and Theorems in Linear Algebra,* translations of mathematical monographs, vol. 134, AMS Press, 2004.

[RS02] Qazi Ibadur Rahman and Gerhard Schmeisser, *Analytic Theory of Polynomials,* London Mathematical Society Monographs 26, Oxford Science Publications, 2002.

[Ren87] James Renegar, *"On the Worst-Case Arithmetic Complexity of Approximating Zeros of Polynomials,"* Journal of Complexity 3, pp. 90–113 (1987).

[Rob00] Alain M. Robert, *A course in p-adic analysis,* Graduate Texts in Mathematics, 198, Springer-Verlag, New York, 2000.

[Roj04] J. Maurice Rojas, *Arithmetic Multivariate Descartes' Rule,* American Journal of Mathematics, vol. 126, no. 1, February 2004, pp. 1–30.

[Roj11] J. Maurice Rojas, *"Tropical Geometry of Smale's 17th Problem over Local Fields,"* grant proposal DMS-1201559, National Science Foundation, submitted October 4, 2011.

[Roj25] J. Maurice Rojas, *"An Introduction to Algorithmic Fewnomial Theory Over $\mathbb{R}$,"* Notices of the American Mathematical Society, in press, to appear June 2025.

[RZ22] J. Maurice Rojas and Yuyu Zhu, *"Root Repulsion and Faster Solving for Very Sparse Polynomials Over p-adic Fields,"* J. Number Theory, Vol. 241, Dec. 2022, pp. 655–699.

[RV15] Mark Rudelson and Roman Vershynin, *"Small Ball Probabilities for Linear Images of High-Dimensional Distributions,"* International Mathematics Research Notices, Vol. 2015, Issue 19, 2015, pp. 9594–9617, `https://doi.org/10.1093/imrn/rnu243`

[Sag10] Michael Sagraloff, *"A General Approach to Isolating Roots of a Bit-stream Polynomial,"* Mathematics in Computer Science **4**, 481 (2010), Springer-Verlag.

[Sch86] Alexander Schrijver, *Theory of Linear and Integer Programming,* John Wiley & Sons, 1986.

[Ser64] Jean-Pierre Serre, *Lie Algebras and Lie Groups,* 1964 Lectures given at Harvard University, Lecture Notes in Mathematics 1500, corrected 5th printing, Springer-Verlag, 2006.

[Sma81] Steve Smale, *"The fundamental theorem of algebra and complexity theory,"* Bull. Amer. Math. Soc. (N.S.) Volume 4, Number 1 (1981), pp. 1–36.

[SW05] Andrew J. Sommese and Charles W. Wampler, *"The Numerical Solution to Systems of Polynomials Arising in Engineering and Science,"* World Scientific, Singapore, 2005.

[Sto00] Arne Storjohann, *"Algorithms for matrix canonical forms,"* doctoral dissertation, Swiss Federal Institute of Technology, Zurich, 2000.

[T-CT20] Josué Tonelli-Cueto and Elias Tsigaridas, *"Condition numbers for the cube. I: Univariate polynomials and hypersurfaces,"* in Proceedings of ISSAC 2020 (International Symposium on Symbolic and Algebraic Computation), pp. 434–441. https://doi.org/10.1145/3373207.3404054

[T-C22] Josué Tonelli-Cueto, *"A p-adic Descartes solver: the Strassman solver,"* Math ArXiV preprint 2203.07016 .

[Wei63] Edwin Weiss, *Algebraic Number Theory*, McGraw-Hill, 1963.

[Ye94] Yinyu Ye, *"Combining Binary Search and Newton's Method to Compute Real Roots for a Class of Real Functions,"* J. Complexity 10 (1994), no. 3, 271–280.

[Yu94] Kunrui Yu, *"Linear forms in p-adic logarithms III,"* Compositio Mathematica, 3 (241–276), 1994.

[Yu07] Kunrui Yu, *"p-adic logarithmic forms and group varieties III,"* Forum Math., 19(2):187–280, 2007.