Trinomials and Deterministic Complexity Limits for Real Solving

Erick Boniface[*]
embonifa@ncsu.edu
North Carolina State University
Raleigh, North Carolina, USA

Weixun Deng[†]
J. Maurice Rojas[†]
deng15521037237@tamu.edu
rojas@tamu.edu
Texas A&M University
College Station, Texas, USA

ABSTRACT

We detail an algorithm that — for all but a $\frac{1}{\Omega(\log(dH))}$ fraction of $f \in \mathbb{Z}[x]$ with exactly 3 monomial terms, degree d, and all coefficients in $\{-H,\ldots,H\}$ — produces an approximate root (in the sense of Smale) for each real root of f in deterministic time $\log^{4+o(1)}(dH)$ in the classical Turing model. (Each approximate root is a rational with logarithmic height $O(\log(dH))$.) The best previous deterministic bit complexity bounds were exponential in $\log d$. We then relate this to Koiran's Trinomial Sign Problem (2017): Decide the sign of a degree d trinomial $f \in \mathbb{Z}[x]$ with coefficients in $\{-H,\ldots,H\}$, at a point $r \in \mathbb{Q}$ of logarithmic height $\log H$, in (deterministic) time $\log^{O(1)}(dH)$. We show that Koiran's Trinomial Sign Problem admits a positive solution, at least for a fraction $1-\frac{1}{\Omega(\log(dH))}$ of the inputs (f,r).

ACM Reference Format:
Erick Boniface, Weixun Deng, and J. Maurice Rojas. 2022. Trinomials and Deterministic Complexity Limits for Real Solving. In *ISSAC 2022: International Symposium on Symbolic & Algebraic Computation.* ACM, New York, NY, USA, 8 pages. https://doi.org/???/???

1 INTRODUCTION

The applications of solving systems of real polynomial equations permeate all of non-linear optimization, as well as numerous problems in engineering. As such, it is important to find the best possible speed-ups for real-solving. Furthermore, *structured* systems — such as those with a fixed number of monomial terms or invariance with respect to a group action — arise naturally in many computational geometric applications, and their computational complexity is closely related to a deeper understanding of circuit complexity (see, e.g., [15]). So if we are to fully understand the complexity of solving sparse polynomial systems over the real numbers, then we should at least be able to settle the univariate case, e.g., classify when it is possible to separate and approximate roots in deterministic time polynomial in the input size. Independent of a complete classification, the underlying analytic estimates should give us a more fine-grained understanding of how randomization helps speed up real-solving for more general sparse polynomial equations.

Recall that for any function g analytic on $\mathbb{R}$, the corresponding *Newton endomorphism* is $N_g(z) := z - \frac{g(z)}{g'(z)}$, and the corresponding sequence of *Newton iterates* of a $z_0 \in \mathbb{R}$ is the sequence $(z_i)_{i=0}^{\infty}$ where $z_{i+1} := N_g(z_i)$ for all $i \geq 0$. Given a trinomial $f(x) := c_1 + c_2x^{a_2} + c_3x^{a_3} \in \mathbb{Z}[x]$ with $a_2 < a_3 =: d$ and all $c_i \in \{-H,\ldots,-1,1,\ldots,H\}$, we call f *ill-conditioned* if and only if

$$\left|\left|\frac{c_2}{a_3}\right|\left|\frac{a_3-a_2}{c_1}\right|^{(a_3-a_2)/a_3}\left|\frac{a_2}{c_3}\right|^{a_2/a_3} - 1\right| < \frac{1}{\log(dH)} \qquad (1)$$

and f has no degenerate real roots.

We will see soon that Inequality (1) is the same as forcing the discriminant of f to be near 0 in an explicit way. Also, we'll see how we can check in time $\log^{2+o(1)}(dH)$ whether f is ill-conditioned in the sense above. A peculiarity to observe that is that approximating real degenerate roots *is* also doable efficiently in our framework: Being "near" degeneracy — not degeneracy itself — is the remaining problem.

We use $\#S$ for the cardinality of a set S.

Theorem 1.1. *Following the notation above, assume f is* not *ill-conditioned. Then we can find, in deterministic time* $\log^{4+o(1)}(dH)$, *a set* $\left\{\frac{r_1}{s_1},\ldots,\frac{r_m}{s_m}\right\} \subset \mathbb{Q}$ *of cardinality $m = m(f)$ such that:*

1. *For all j we have $r_j \neq 0 \implies \log|r_j|, \log|s_j| = O(\log(dH))$.*
2. *$z_0 := r_j/s_j \implies f$ has a root $\zeta_j \in \mathbb{R}$ with sequence of Newton iterates ($z_{i+1} := N_{f'}(z_i)$ or $z_{i+1} := N_f(z_i)$, according as ζ is degenerate or not) satisfying $|z_i - \zeta_j| \leq (1/2)^{-2^{i-1}}|z_0 - \zeta_j|$ for all $i \geq 1$.*
3. *$m = \#\{\zeta_1,\ldots,\zeta_m\}$.*

In particular, if the exponents a_2 and a_3 are fixed (and distinct), then at most a fraction of $\frac{1}{\log(dH)} + \frac{1}{H}$ of the $(c_1,c_2,c_3) \in \{-H,\ldots,H\}^3$ yield $f(x) = c_1 + c_2x^{a_2} + c_3x^{a_3}$ that are ill-conditioned.

We prove Theorem 1.1 in Section 3, via Algorithm 3.1 there. We will call the convergence condition on z_0 above *being an approximate root (in the sense of Smale) with associated true root ζ_j*. This type of convergence provides an efficient encoding of an approximation that can be quickly tuned to any desired accuracy. It is known (e.g., already for the special case of solving $x^2 = c$) that one can not do much better, with respect to asymptotic arithmetic complexity, than Newton iteration [9].

Our complexity bound from Theorem 1.1 appears to be new, and complements earlier work on the arithmetic complexity of approximating [27, 29] and counting [5, 14] real roots of trinomials.

[*]Partially supported by NSF REU grant DMS-1757872 and the Texas A&M Mathematics Department.
[†]Partially supported by NSF grant CCF-1900881.

ISSAC 2022, 4–7 July, 2022, Lille, France

ACM ISBN ???…$15.00
https://doi.org/???/???

In particular, Theorem 1.1 nearly settles a question of Koiran from [14] on the bit complexity of solving trinomial equations over the reals. One should also observe that the best general bit complexity bounds for solving real univariate polynomials are super-linear in d and work in terms of ε-approximation, thus requiring an extra parameter depending on root separation (which is not known a priori): see, e.g., [18, 22].

Remark 1.2. *Defining the* input size *of a univariate polynomial* $f(x) := \sum_{i=1}^{t} c_i x^{a_i} \in \mathbb{Z}[x]$ *as* $\sum_{i=1}^{t} \log((|c_i|+2)(|a_i|+2))$ *we see that Theorem 1.1 implies that one can solve "most" real univariate trinomial equations in deterministic time polynomial in the input size.* ⋄

Remark 1.3. *Efficiently solving univariate t-nomial equations over $\mathbb{R}$ in the sense of Theorem 1.1 is easier for $t \le 2$: The case $t=1$ is clearly trivial (with 0 the only possible root) while the case $t=2$ is implicit in work on computer arithmetic from the 1970s (see, e.g., [7]). We review this case in Theorem 2.3 of Section 2.1 below.* ⋄

Efficiently counting real roots for trinomials turns out to be equivalent to a special case of Baker's classic theorem on linear forms in logarithms [2, 21], and we review this equivalence in Lemma 2.6 below. Our approach to *approximating* roots (in the sense of Smale) is to apply *$\mathcal{A}$-hypergeometric functions* [24] (briefly reviewed in Section 2.3) and a combination of earlier analytic estimates of Ye [33], Rojas and Ye [27], and Koiran [14] (see Sections 2.2 and 1.1).

An important question Koiran posed near the end of his paper [14] is whether one can determine the sign of a trinomial evaluated at a rational number in (deterministic) time polynomial in the input size. (Determining the sign of a t-nomial at an *integer* turns out to be doable in deterministic polynomial-time for all t [10].) We obtain a partial positive answer to Koiran's question, thanks to an equivalence between solving and sign determination that holds for trinomials:

Corollary 1.4. *Following the notation above, suppose $u, v \in \mathbb{Z}$ with $|u|, |v| \le H$, and f is not ill-conditioned. Then we can determine the sign of $f(u/v)$ in time $O(\log^{O(1)}(dH))$.*

Lemma 1.5. *Koiran's Sign Problem has a positive solution if and only if finding approximate roots (in the sense of Smale) for trinomials is doable in deterministic time* $\log^{O(1)}(dH)$.

We prove Corollary 1.4 and Lemma 1.5 in Section 4. Our use of $\mathcal{A}$-hypergeometric series thus provides an alternative to how bisection is used to start higher-order numerical methods. In particular, our approach complements another approach to computing signs of trinomials at rational points of "small" height due to Gorav Jindal (write-up available at his blog).

1.1 The Root Separation Chasm at Four Terms

Unfortunately, there are obstructions to solving univariate polynomial equations over $\mathbb{R}$ in polynomial-time when there are too many monomial terms. Indeed, the underlying root spacing changes dramatically already at 4 terms.

Theorem 1.6. [20, 28, 29] *Consider the family of tetranomials*

$$f_d(x) := x^d - 4^h x^2 + 2^{h+2} x - 4$$

with $h \in \mathbb{N}$, $h \ge 3$, and $d \in \left\{4, \ldots, \left\lfloor e^h \right\rfloor\right\}$ even. Let $H := 4^h$. Then f_d has distinct roots $\zeta_1, \zeta_2 \in \mathbb{R}$ with $\log|\zeta_1 - \zeta_2| = -\Omega(d \log H)$. In particular, the coefficients of f_d all lie in $\mathbb{Z}$ and have bit-length $O(\log H)$.

While this result goes back to work of Mignotte [20], we point out that in [28] a more general family of polynomials was derived, revealing that the same phenomenon of tightly-spaced roots for tetranomials occurs over *all* characteristic zero local fields, e.g., the roots of tetranomials in $\mathbb{Q}_p$ (for p *any* prime) can be exponentially close as a function of the degree. One may conjecture that the basin of attraction, for Newton's Method applied to a real root of a tetranomial, can also be exponentially small, but so far only the analogous statement over $\mathbb{Q}_p$ is proved [28, Rem. 4.1].

Tight spacing of real roots is thus partial evidence against being able to find approximate roots in the sense of Smale — with "small" height, as in our main theorem for trinomials — for tetranomials. Fortunately, for our setting, binomials and trinomials have well-spaced roots as a function of d and H:

Theorem 1.7. *(See [28, Prop. 2.4] and [14].) If $f \in \mathbb{Z}[x]$ is a degree d univariate t-nomial, with coefficients in $\{-H, \ldots, H\}$, then any two distinct roots $\zeta_1, \zeta_2 \in \mathbb{C}$ satisfy*
$\log|\zeta_1 - \zeta_2| > -[\log(d) + \frac{1}{d}\log H]$ *or* $\log|\zeta_1 - \zeta_2| = -O(\log^3(dH))$, *according as t is 2 or 3.* ■

One should also recall the following refined bound on the norms of nonzero roots of trinomials:

Lemma 1.8. Suppose $f(x) = c_1 + c_2 x^{a_2} + c_3 x^{a_3} \in \mathbb{C}[x] \setminus \{0\}$ and $c_1 c_2 c_3 \neq 0$. Then any root $\zeta \in \mathbb{C}$ of f must also satisfy
$\frac{1}{2}\min\left\{\left|\frac{c_1}{c_2}\right|^{\frac{1}{a_2}}, \left|\frac{c_1}{c_3}\right|^{\frac{1}{a_3}}\right\} < |\zeta| < 2\max\left\{\left|\frac{c_2}{c_3}\right|^{\frac{1}{a_3 - a_2}}, \left|\frac{c_1}{c_3}\right|^{\frac{1}{a_3}}\right\}$. ■

Such bounds had their genesis in work of Cauchy and Hadamard in the $19^{\underline{\text{th}}}$ century, and have since been extended to several variables via tropical geometry: See, e.g., [1, 11].

1.2 Going Beyond Univariate Trinomials

It is curious that the sign of an arbitrary t-nomial $f \in \mathbb{Z}[x]$ with degree d and coefficients in $\{-H, \ldots, H\}$, at an *integer* $r \in \{-H, \ldots, H\}$, can be computed in polynomial-time [10], while the extension to rational r is still an open question. It is conceivable that (but still unknown if) computing such sign evaluations at rational points can exhibit a leap in complexity for some family of tetranomials, akin to Theorem 1.6.

Let us call a polynomial in $\mathbb{Z}[x_1, \ldots, x_n]$ having exactly t terms in its monomial term expansion an *n-variate t-nomial*. It is worth recalling that merely deciding the existence of roots over $\mathbb{R}$ for n-variate $(n + n^{\varepsilon})$-nomials (with $n \in \mathbb{N}$ and $\varepsilon > 0$ *arbitrary*) is **NP**-hard [5].

However, there is a different way to generalize univariate trinomial equations: They are the $n=1$ case of *$n \times n$ circuit systems*: Consider a system of equations $F := (f_1, \ldots, f_n) \in \mathbb{Z}\left[x_1^{\pm 1}, \ldots, x_n^{\pm 1}\right]$ where the exponent vectors of all the f_i are contained in a set $A \subset \mathbb{Z}^n$ of cardinality $n+2$, with A *not* lying in any affine hyperplane. Such an A is called a *circuit* (the terminology coming from combinatorics, instead of complexity theory), and such systems have been studied from the point of view of real solving and fewnomial theory since 2003 (if not earlier): See, e.g., [4, 5, 17, 26]. In particular, it has been known at least since [4] that solving such systems over $\mathbb{R}$ reduces mainly to finding the real roots of univariate rational functions of the form

$$g(u) := \prod_{i=1}^{n+1} \left(\gamma_{i,1}u + \gamma_{i,0}\right)^{b_i} - 1 \tag{2}$$

where $\gamma_{i,j} \in \mathbb{Q}$ and $b_i \in \mathbb{Z}$ for all i, j. Given any $u, v \in \mathbb{Z}$ with $\gcd(u, v) = 1$, we define the *logarithmic height of* u/v to be $h(u/v) := \max\{|u|, |v|\}$. (We also set $h(0) := 0$.) We pose the following conjecture:

Conjecture 1.9. *Following the preceding notation, we can find approximate roots (in the sense of Smale) for all the real roots of (2), in time polynomial in* $\log^n(BH)$*, where* $B := \max_i |b_i|$ *and* $\log H := \max_{i,j} h(\gamma_{i,j})$.

Recently, it was shown that one can count the real roots of circuit systems in deterministic polynomial-time, for any fixed n [26]: The proof reduced to proving the simplification of Conjecture 1.9 where one only asks for *the number* of real roots of g. This provides some slight evidence for Conjecture 1.9. More to the point, the framework from [26] reveals that proving Conjecture 1.9 would be the next step toward polynomial-time real-solving for circuit systems for $n > 1$. Such speed-ups are currently known only for binomial systems so far [23], since real-solving for arbitrary $n \times n$ systems still has exponential-time worst-case complexity when n is fixed (see, e.g., [25]).

2 BACKGROUND

2.1 Approximating Logarithms and Roots of Binomials

Counting real roots for the binomial $c_1 + c_2x^d$ (with $c_1, c_2 \in \mathbb{Z}$ and $d \in \mathbb{N}$) depends only on the signs of the c_i and the parity of d: From the Intermediate Value Theorem, it easily follows that the preceding binomial has real roots if and only if [$c_1 = 0 \neq c_2$, $c_1c_2 < 0$, or [d is odd and $c_2 \neq 0$]]. Also, two nonzero real roots are possible if and only if [$c_1c_2 < 0$ and d is even]. So we now quickly review the bit complexity of finding a positive rational approximate root (in the sense of Smale) for $f(x) := c_2x^d - c_1$, with $c_1, c_2, d \in \mathbb{N}$. (The case of negative roots obviously reduces to the case of positive roots by considering $f(-x)$.)

First note that f must have a root in the open interval $\left(0, \max\left\{\frac{c_1}{c_2}, 1\right\}\right)$. So we can check the sign of f at the midpoint of this interval and then reduce to either the left interval $\left(0, \frac{1}{2}\max\left\{\frac{c_1}{c_2}, 1\right\}\right)$, or the right interval $\left(\frac{1}{2}\max\left\{\frac{c_1}{c_2}, 1\right\}, \max\left\{\frac{c_1}{c_2}, 1\right\}\right)$, and proceed recursively, i.e., via the ancient technique of bisection. The signs can be computed efficiently by rapidly approximating $d \log x + \log(c_2/c_1)$, and other expressions of this form, to sufficiently many bits of accuracy.

To see how to do this, we should first observe that logarithms of rational numbers can be approximated efficiently in the following sense: Recall that the binary expansion of $\left\lfloor 2^{\ell-1-\lfloor \log_2 x \rfloor} x \right\rfloor$ forms the ℓ *most significant bits* of an $x \in \mathbb{R}_+$. (So knowing the ℓ most significant bits of x means that one knows x up to a multiple in the closed interval $\left[(1 + 2^{-\ell})^{-1}, 1 + 2^{-\ell}\right]$.)

Theorem 2.1. *[3, Sec. 5] Given any positive* $x \in \mathbb{Q}$ *of logarithmic height* h*, and* $\ell \in \mathbb{N}$ *with* $\ell \geq h$*, we can compute* $\lfloor \log_2 \max\{1, \log|x|\} \rfloor$*, and the* ℓ *most significant bits of* $\log x$*, in time* $O(\ell \log^2 \ell)$. ■

The underlying technique (*AGM Iteration*) dates back to Gauss and was refined for computer use in the 1970s by many researchers (see, e.g., [7, 8, 30]). We note that in the complexity bound above, we are applying the recent $O(n \log n)$ algorithm of Harvey and van der Hoeven for multiplying two n-bit integers [13]. Should we use a more practical (but asymptotically slower) integer multiplication algorithm then the time can still be kept at $O(\ell^{1.585})$ or lower.

The next fact we need is that only a moderate amount of accuracy is needed for Newton Iteration to converge quickly to a $d^{\underline{\text{th}}}$ root.

Lemma 2.2. *[33] Suppose* $\zeta^d = c$ *with* $c \in \mathbb{R}_+$ *and* $d \in \mathbb{N}$*. Then any* $z \in \mathbb{R}_+$ *satisfying* $|z - \zeta| \leq \frac{2c^{1/d}}{d-1}$ *is an approximate root of* $x^d - c$ *with associated true root* ζ. ■

The key to using fast logarithm computation to efficiently extract approximate $d^{\underline{\text{th}}}$ roots of rational numbers will then be knowing how roughly one can approximate the logarithms. An explicit estimate follows from a famous result of Baker, more recently refined by Matveev:

Baker's Theorem (over $\mathbb{Q}$). *(See [2] and [19, Cor. 2.3].) Suppose* $\alpha_i \in \mathbb{Q} \setminus \{0\}$ *and* $b_i \in \mathbb{Z} \setminus \{0\}$ *for all* $i \in \{1, \ldots, m\}$*. Let* $B = \max_i\{|b_1|, \ldots, |b_m|\}$, $\log \mathscr{A}_i := \max\{h(\alpha_i), |\log \alpha_i|, 0.16\}$*, and* $\Lambda := \sum_{i=1}^m b_i \log \alpha_i$*, where we fix any suitable branch of* $\log$ *a priori. Then* $\Lambda \neq 0 \Longrightarrow \log|\Lambda| > -1.4 \cdot m^{4.5} 30^{m+3}(1 + \log B) \prod_{i=1}^m \log \mathscr{A}_i$. ■

Combining Theorem 2.1, Lemma 2.2, and Baker's Theorem, we easily obtain the following result:

Theorem 2.3. *Suppose* $f \in \mathbb{Z}[x]$ *is a univariate binomial of degree* d *with coefficients in* $\{-H, \ldots, -1, 1, \ldots, H\}$*. Then, in time* $\log^{2+o(1)}(dH)$*, we can count exactly how many real roots* f *has and, for any nonzero real root* ζ *of* f*, find a* $z_0 \in \mathbb{Q}$*, with* $\zeta z_0 > 0$ *and bit-length* $O(\log(dH))$*, that is an approximate root of* f *in the sense of Smale.* ■

Theorem 2.3 is most likely known to experts. In particular, an analogue for the arithmetic complexity of random binomial systems appears in [23].

We now set the groundwork for extending the preceding theorem to the trinomial case.

2.2 Discriminants and α-Theory for Trinomials

There are three obstructions to extending the simple approach to binomials from last section to trinomials: (1) computing signs of trinomials at rational points is not known to be doable in polynomial-time, (2) counting roots requires the computation of the sign of a discriminant, (3) we need explicit estimates on how close a rational z must be to a real root ζ before z can be used as an approximate root in the sense of Smale.

Circumventing Obstruction (1) is covered in the next section, so let us now review how to deal with Obstructions (2) and (3).

First recall the special case of the $\mathcal{A}$*-discriminant* [12] for trinomials:

Definition 2.4. *Given any* $a_2, a_3 \in \mathbb{N}$ *with* $\gcd(a_2, a_3) = 1$ *and* $a_2 < a_3$*, we define*

$\Delta_{\{0,a_2,a_3\}}(c_1,c_2,c_3) := a_2^{a_2}(a_3-a_2)^{a_3-a_2}(-c_2)^{a_3} - a_3^{a_3}c_1^{a_3-a_2}c_3^{a_2}$, *and abbreviate with* $\Delta(f) := \Delta_{(0,a_2,a_3)}(c_1,c_2,c_3)$ *when* $f(x) = c_1 + c_2x^{a_2} + c_3x^{a_3}$. ⋄

Remark 2.5. *By dividing out by a suitable monomial, the vanishing of* $\Delta(f)$ *is clearly equivalent to a monomial (with integer exponents) being* 1*. Taking logarithms, we then see that we can decide the sign of any trinomial discriminant as above in time* $\log^{2+o(1)}(dH)$*, by combining Baker's Theorem with the fast logarithm approximation from Theorem 2.1. Similarly,* f *being ill-conditioned is equivalent to* $\Delta(f) = O\left((1+\frac{1}{\log(dH)})^d\right)$*, which can also be checked in time* $\log^{2+o(1)}(dH)$ *by approximating logarithms.* ⋄

Lemma 2.6. *Following the notation above, suppose*
$f(x) = c_1 + c_2x^{a_2} + c_3x^{a_3} \in \mathbb{R}[x]$ *with* $c_1c_2c_3 \neq 0$,
and set $\mathrm{sign}(f) := (\mathrm{sign}(c_1), \mathrm{sign}(c_2), \mathrm{sign}(c_3)) \in \{\pm\}^3$*. Then* f *has...*

1. *no positive roots if and only if [*$\mathrm{sign}(f) \in \{(+,+,+),(-,-,-)\}$ *or [*$\mathrm{sign}(f) \in \{(+,-,+),(-,+,-)\}$ *and* $\mathrm{sign}(\Delta(f)) = \mathrm{sign}(c_2)$*]].*
2. *a unique positive root if and only if [*$\mathrm{sign}(f) \in \{(-,+,+),(-,-,+),(+,-,-),(+,+,-)\}$*] or [*$\Delta(f) = 0$ *and* $\mathrm{sign}(f) \in \{(+,-,+),(-,+,-)\}$*]].*
3. *exactly two positive roots if and only if [*$\mathrm{sign}(f) \in \{(+,-,+),(-,+,-)\}$ *and* $\mathrm{sign}(\Delta(f)) = -\mathrm{sign}(c_2)$*].*
4. $\left(-\frac{a_2c_2}{a_3c_3}\right)^{1/(a_3-a_2)}$ *as a positive degenerate root (with no other positive root for* f*) if and only if [*$\Delta(f) = 0$ *and* $\mathrm{sign}(f) \in \{(+,-,+),(-,+,-)\}$*].* ■

Lemma 2.6 follows easily from Descartes' Rule of Signs (see, e.g., [31]) and Assertion (4) (see, e.g., [5]). Since deciding the sign of $\Delta(f)$ is clearly reducible to deciding the sign of a linear combination of logarithms, Lemma 2.6 combined with Baker's Theorem thus enables us to efficiently count the positive roots of trinomials (as already observed in [5]).

So now we deal with the convergence of Newton's Method in the trinomial case.

Definition 2.7. *For any analytic function* $f : \mathbb{R} \longrightarrow \mathbb{R}$*, let* $\gamma(f,x) := \sup\limits_{k\geq 2}\left|\frac{f^{(k)}(x)}{k!f'(x)}\right|^{\frac{1}{k-1}}$. ⋄

Remark 2.8. *It is worth noting that* $1/\gamma(f,x_0)$ *is a lower bound for the radius of convergence of the Taylor series of* f *about* x_0*, so* $\gamma(f,x_0)$ *is finite whenever* $f'(x_0) \neq 0$ *[6, Prop. 6, Pg. 167].* ⋄

A globalized variant, Γ_f, of $\gamma(f,x)$ will help us quantify how near $z \in \mathbb{R}_+$ must be to a positive root ζ of a trinomial for z to be an approximate root in the sense of Smale with associated true root ζ:

Definition 2.9. *Consider* $f(x) = c_1 + c_2x^{a_2} + c_3x^{a_3} \in \mathbb{R}[x]$ *with* $0 < a_2 < a_3$, $c_3 > 0 > c_2$*, and* $c_1 \neq 0$*. Let* x_1 *be the unique positive root of the derivative* f'*.*

1. *If* f *has two positive roots then let* x_2 *be the unique positive root of* f'' *(or set* $x_2 := 0$ *should* f'' *not have a positive root). Then set* $\Gamma_f := \max\left\{\sup\limits_{x\in(0,x_2)} x\gamma(f,x), \sup\limits_{x\in(x_2,\infty)} (x-x_1)\gamma(f,x)\right\}$.
2. *If* $c_1 < 0$ *then we set* $\Gamma_f := \sup\limits_{x\in(0,x_2)} x\gamma(f,x)$. ⋄

Lemma 2.6 tells us that Cases (1) and (2) in our definition above are indeed disjoint, and Baker's Theorem (combined with Theorem 2.1) tells us that we can efficiently distinguish Cases (1) and (2). Later, we will see some simple reductions implying that Cases (1) and (2) above are really the only cases we need to prove our main results.

Theorem 2.10. *(See [33, Thm. 2] and [27, Thm. 5].) Following the notation and assumptions of Definition 2.9, set* $d := a_3$ *and suppose* $z, \zeta \in \mathbb{R}_+$ *with* $f(\zeta) = 0$ *and* $d \geq 3$*. Also let* x_2 *be the unique positive root of* f'' *(or set* $x_2 := 0$ *should* f'' *not have a positive root). Then:*

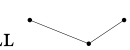
(0) $-f$ *is convex on* $(0,x_2)$ *and* f *is convex on* (x_2,∞)*.*
(1) *If* f *is monotonically decreasing in* $[z,\zeta]$, $x_2 \notin [z,\zeta]$*, and* $\zeta \in \left[z, \left(1+\frac{1}{8\Gamma_f}\right)z\right]$*, then* z *is an approximate root of* f*.*
(2) *If* f *is monotonically increasing in* $[\zeta,z]$, $x_2 \notin [x,\zeta]$*, and* $\zeta \in \left[\left(1-\frac{1}{8\Gamma_f}\right)z, z\right]$*, then* z *is an approximate root of* f*.*
(3) $\frac{d-1}{2} \leq \Gamma_f \leq \frac{(d-1)(d-2)}{2}$.

In particular, Assertions (1) and (2), combined with Assertion (3), imply $|z-\zeta| \leq \frac{\zeta}{4(d-1)(d-2)}$. ■

2.3 $\mathcal{A}$-Hypergeometric Functions

Let us now consider the positive roots of $1 - cx^m + x^n$ and $-1 - cx^m + x^n$ as a function of $c \in \mathbb{R}$, when $0 < m < n$ and $\gcd(m,n) = 1$, from the point of view of $\mathcal{A}$-hypergeometric series [12]. These series date back to 1757 work of Johann Lambert for the special case $m = 1$. Many authors have since extended these series in various directions. Passare and Tsikh's paper [24] is the most relevant for our development here. The union of the domains of convergence of these series will turn out to be $\mathbb{C} \setminus \{r_{m,n}\}$ where $r_{m,n} := \frac{n}{m^{\frac{m}{n}}(n-m)^{\frac{n-m}{n}}}$: This quantity, easily checked to be strictly greater than 1, is closely related to the trinomial discriminant via $\Delta(\pm 1 - cx^m + x^n) = 0 \Longrightarrow |c| = r_{m,n}$.

There will be two series for $|c| > r_{m,n}$, and one more series for $|c| < r_{m,n}$, that we will focus on. These two convergence domains are in fact related to triangulations of the point set $\{0,m,n\}$ via the *Archimedean Newton polygon* [1, 12], but we will not elaborate further here on this combinatorial aspect. The reader should be aware that these series in fact yield all complex roots, upon inserting suitable roots of unity in the series formulae. So our choices of sign are targeted toward numerical bounds for positive roots.

$|c| > r_{m,n} \Longrightarrow$ FINEST LOWER HULL 

The first series is:

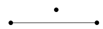
$$x_{\mathrm{low}}(c) = \frac{1}{c^{1/m}}\left[1 + \sum_{k=1}^{\infty}\left(\frac{1}{km^k}\cdot\prod_{j=1}^{k-1}\frac{1+kn-jm}{j}\right)\left(\frac{1}{c^{n/m}}\right)^k\right]$$

(yielding a positive root of $1 - cx^m + x^n$ with norm within a factor of 2 of $c^{-1/m}$, thanks to Lemma 1.8), while the second is:

$$x_{\mathrm{hi}}(c) = c^{\frac{1}{n-m}}\left[1 - \sum_{k=1}^{\infty}\left(\frac{1}{k(n-m)^k}\cdot\prod_{j=1}^{k-1}\frac{km+j(n-m)-1}{j}\right)\left(\frac{1}{c^{n/(n-m)}}\right)^k\right]$$

(yielding a positive root of $1 - cx^m + x^n$ with norm within a factor of

2 of $c^{1/(n-m)}$, thanks to Lemma 1.8, and distinct from the previous root).

$|c|<r_{m,n} \Longrightarrow$ COARSEST LOWER HULL 

Our final series yields a root of $-1-cx^m+x^n$ in the interval $\left(\frac{1}{2},2\right)$, via Descartes' Rule of Signs and Lemma 1.8:

$$\boxed{x_{\text{mid}}(c)=1+\sum_{k=1}^{\infty}\left(\frac{1}{kn^k}\cdot\prod_{j=1}^{k-1}\frac{1+km-jn}{j}\right)c^k.}$$

A key fact about these $\mathcal{A}$-hypergeometric series is that their tails decay quickly enough for us to use their truncations (sometimes efficiently) as start points for Newton iteration.

Lemma 2.11. *Suppose $f(x)=c_1+c_2x^{a_2}+c_3x^{a_3}\in\mathbb{Z}[x]$, with $\sigma(f)\in\{(-,-,+),(+,-,+)\}$ and all coefficients in $\{-H,\dots,-1,1,\dots,H\}$, is not ill-conditioned. Set $c:=\left|\frac{c_2}{c_1^{(n-m)/n}c_3^{m/n}}\right|$. Also let $x^{(\ell)}_{\text{low}}$, $x^{(\ell)}_{\text{hi}}$, and $x^{(\ell)}_{\text{mid}}$ denote the truncation of the corresponding series to its $\ell^{\underline{th}}$ term. Then $|c_1/c_3|^{1/a_3}x^{(\ell)}_{\text{low}}(c)$ (resp. $|c_1/c_3|^{1/a_3}x^{(\ell)}_{\text{hi}}(c)$, $|c_1/c_3|^{1/a_3}x^{(\ell)}_{\text{mid}}(c)$) is an approximate root of f with associated true root $|c_1/c_3|^{1/a_3}x_{\text{low}}(c)$ (resp. $|c_1/c_3|^{1/a_3}x_{\text{hi}}(c)$, $|c_1/c_3|^{1/a_3}x^{(\ell)}_{\text{mid}}(c)$) if $\ell=O(\log^2(dH))$.*

Proof: Let $m:=a_2$ and $n:=a_3$. Observe that if we set $\alpha:=|1/c_1|$, $\beta:=|c_1/c_3|^{1/n}$, and $g(x):=\alpha f(\beta x)$, then $g(x)=\pm1-cx^m+x^n$, with the sign being exactly $\text{sign}(c_1)$. So we'll work with g henceforth. Now note that

$$\prod_{j=1}^{k-1}\frac{1+kn-jm}{j}=\exp\left(\sum_{j=1}^{k-1}\log(1+kn-jm)-\log(j)\right)$$

$$\leq\exp\left(\log(1+kn-1\cdot m)+\int_1^{k-1}\log(1+kn-jm)-\log(j)\,dj\right)$$

$$=\left(\frac{1-m+kn}{1+m-km+kn}\right)^{\frac{1+kn}{m}}\left(\frac{1+m-km+kn}{k-1}\right)^{k-1}$$

$$\leq\left(\frac{n}{n-m}\right)^{\frac{1+kn}{m}}(n-m)^{k-1}=\frac{1}{n-m}\left(\frac{n}{n-m}\right)^{\frac{1}{m}}\left(m\,r_{m,n}^{\frac{n}{m}}\right)^k$$

$$\leq k\left(m\,r_{m,n}^{\frac{n}{m}}\right)^k.$$

So $\left|x_{\text{low}}(c)-x^{(\ell)}_{\text{low}}(c)\right|$

$$=\left|\frac{-1}{c^{1/m}}\sum_{k=\ell+1}^{\infty}\left(\frac{(-1)^{nk}}{km^k}\cdot\prod_{j=1}^{k-1}\frac{1+kn-jm}{j}\right)\left(\frac{1}{c^{n/m}}\right)^k\right|$$

$$\leq\frac{1}{|c|^{1/m}}\sum_{k=\ell+1}^{\infty}\left(\frac{r_{m,n}^{n/m}}{|c|^{n/m}}\right)^k$$

$$=\frac{1}{|c|^{1/m}}\cdot\frac{1}{1-\left(r_{m,n}/|c|\right)^{\frac{n}{m}}}\cdot\left(\frac{r_{m,n}}{|c|}\right)^{\frac{n}{m}(\ell+1)}.$$

Assume $c>r_{m,n}$ (and recall $r_{m,n}>1$). By Theorem 2.10, when $n\geq3$, it suffices to find ℓ such that $\left|x_{\text{low}}(c)-x^{(\ell)}_{\text{low}}(c)\right|\leq\frac{x_{\text{low}}(c)}{4(n-1)(n-2)}$. When $n=2$, we can in fact complete the square, reduce to the binomial case, and then Lemma 2.2 tells us that it suffices to find ℓ such that $\left|x_{\text{low}}(c)-x^{(\ell)}_{\text{low}}(c)\right|\leq 2x_{\text{low}}(c)$. Also, Lemma 1.8 tells us that $x_{\text{low}}(c)\in\left(\frac{1}{2c^{1/m}},\frac{2}{c^{1/m}}\right)$. In other words, it suffices to enforce $\left|x_{\text{low}}(c)-x^{(\ell)}_{\text{low}}(c)\right|\leq\frac{1}{8(n-1)^2c^{1/m}}$, which (thanks to our last tail bound involving $r_{m,n}/|c|$) is implied by:

$(\ell+1)\log\frac{|c|}{r_{m,n}}\geq\frac{m}{n}\log(8(n-1)^2)-\frac{m}{n}\log\left(1-\left(\frac{r_{m,n}}{|c|}\right)^{\frac{n}{m}}\right).$

Since f is not ill-conditioned we have $\frac{|c|}{r_{m,n}}\geq1+\frac{1}{\log(nH)}$ and thus

$$-\frac{m}{n}\log\left(1-\left(\frac{r_{m,n}}{|c|}\right)^{\frac{n}{m}}\right)\leq-\frac{m}{n}\log\left(1-\left(\frac{1}{1+\frac{1}{\log(nH)}}\right)^{\frac{n}{m}}\right)$$

$$\leq\log\left(1+\frac{1}{\log(nH)}\right)-\frac{m}{n}\log\frac{1}{\log(nH)}$$

$$\leq\log(nH)$$

Also, $\log\frac{|c|}{r_{m,n}}\geq\log\left(1+\frac{1}{\log(nH)}\right)\geq\frac{\log 2}{\log(nH)}$ by the inequality $\log(x)\geq(\log 2)(x-1)$ if $1\leq x\leq2$. Therefore, if

$$\ell\geq\frac{\log(nH)[\log(8(n-1)^2)+\log(nH)]}{\log 2},$$

we then have $(\ell+1)\log\frac{|c|}{r_{m,n}}>\log(8(n-1)^2)+\log(nH)$

$$\geq\frac{m}{n}\log(8(n-1)^2)-\frac{m}{n}\log\left(1-\left(\frac{r_{m,n}}{|c|}\right)^{\frac{n}{m}}\right).$$

The proof for $x^{(\ell)}_{\text{hi}}(c)$ is similar, just using

$$\prod_{j=1}^{k-1}\frac{1+kn-jm}{j}\leq k\left((n-m)\,r_{m,n}^{\frac{n}{n-m}}\right)^k$$

and $\left|x_{\text{hi}}(c)-x^{(\ell)}_{\text{hi}}(c)\right|\leq\frac{c^{\frac{1}{n-m}}}{1-(r_{m,n}/|c|)^{\frac{n-m}{n}}}\cdot\left(\frac{r_{m,n}}{|c|}\right)^{\left(\frac{n-m}{n}\right)(\ell+1)}$ instead.

The proof for $x^{(\ell)}_{\text{mid}}(c)$ also follows similarly, assuming $0<|c|<r_{m,n}$ instead, and using

$$\prod_{j=1}^{k-1}\frac{1+km-jn}{j}\leq k\left(\frac{n}{r_{m,n}}\right)^k$$

and $|x_{\text{mid}}(c)-x_{\text{mid}}|\leq\frac{1}{1-(c/r_{m,n})}\left(\frac{c}{r_{m,n}}\right)^{\ell+1}$ instead. ■

3 SOLVING TRINOMIAL EQUATIONS OVER $\mathbb{R}$

Algorithm 3.1. (Solving Trinomial Equations Over $\mathbb{R}_+$)
Input. $c_1, c_2, c_3, a_2, a_3 \in \mathbb{Z}\setminus\{0\}$ *with* $|c_i| \leq H$ *for all* i *and* $1 \leq a_2 < a_3 =: d$.
Output. $z_1, \ldots, z_m \in \mathbb{Q}_+$ *with logarithmic height* $O(\log(dH))$ *such that* m (≤ 2) *is the number of roots of* $f(x) := c_1 + c_2x^{a_2} + c_3x^{a_3}$ *in* $\mathbb{R}_+$, z_j *is an approximate root of* f *with associated true root* $\zeta_j \in \mathbb{R}_+$ *for all* j, *and the* ζ_j *are pair-wise distinct.*
Description.

(0) *Let* `xflip:= 1`, $c := \left|\frac{c_2}{c_1^{(a_3-a_2)/a_3} c_3^{a_2/a_3}}\right|$, $\beta := |c_1/c_3|^{1/a_3}$, *and let* $c' \in \mathbb{Q}_+$ *(resp.* β'*) an approximation to* c *(resp.* β*) within distance* $\frac{c}{96(n-1)^2}$ *computed via Theorem 2.3, and* $\ell := \frac{\log(a_3H)[\log(24(a_3-1)^2)+\log(a_3H)]}{\log 2}$.
(1) *If* $\sigma(f) \in \{(+,+,+),(-,-,-)\}$ *then* `output` `“Your f has no positive roots.”` *and* `STOP`.
(2) *Replacing* $f(x)$ *by* $\pm f(x)$ *or* $\pm x^{a_3} f(1/x)$ *(and setting* `xflip:= −1`*) as necessary, reduce to the special case* $c_3 > 0 > c_2$.
(3) *If* $\Delta(f) = 0$ *then, using Theorem 2.3, let* $z_1^{\texttt{xflip}}$ *be a rational approximation to* $\left(-\frac{a_2c_2}{a_3c_3}\right)^{1/(a_3-a_2)}$ *of logarithmic height* $O(\log(dH))$, `output` `“`z_1 `is your only positive approximate root.”` *and* `STOP`.
(4) *If* $\Delta(f) < 0$ *then* `output` `“Your trinomial has no positive roots.”` *and* `STOP`.
(5) *If* $c_1 < 0$ *then let* $z_1^{\texttt{xflip}} := \beta' x_{\text{mid}}^{(\ell)}(c')$ *and* `output` `“`z_1 `is your only positive approximate root.”` *and* `STOP`.
(6) *Let* $z_1^{\texttt{xflip}} := \beta' x_{\text{low}}^{(\ell)}(c')$, $z_2^{\texttt{xflip}} := \beta' x_{\text{hi}}^{(\ell)}(c')$, *and* `output` `“`$z_1$ `and` z_2 `are your only positive approximate roots.”` *and* `STOP`.

Proof of Theorem 1.1: We make one arithmetic reduction first: By computing $\delta := \gcd(a_2, a_3)$ first, replacing (a_2, a_3) with $(a_2, a_3)/\delta$, and solving the resulting trinomial $\bar{f}$, we can solve f over $\mathbb{R}$ by taking the $\delta^{\underline{\text{th}}}$ root of all the real roots of $\bar{f}$ if δ is odd. (If δ is even, then we only take $\delta^{\underline{\text{th}}}$ roots of the positive roots of $\bar{f}$.) The underlying computation of $\delta^{\underline{\text{th}}}$ roots is done via rational approximations with precision $\frac{1}{96H(a_3-1)^2}$ via Theorem 2.3, possibly at the expense of a few extra Newton Iterations of neglible cost. The precision guarantees that the resulting approximations are indeed approximate roots in the sense of Smale for f. The computation of $\gcd(a_2, a_3)$ takes time $O(\log(d)(\log(\log d))^2)$ via the *Half-GCD Method* [32], so this reduction to the case $\gcd(a_2, a_3) = 1$ has negligible complexity.

Assuming Algorithm 3.1 is correct and runs within the stated time bound, our theorem then follows directly by applying Algorithm 3.1 to $f(x)$ and $f(-x)$. So it suffices to prove correctness, and analyze the complexity, of Algorithm 3.1.

Correctness: This follows directly from Lemma 2.6, Theorem 2.10, and Lemma 2.11. In particular, the constants in our algorithm are chosen so that multiplicative error in the underlying radicals and evaluations of our series combine so that $\beta' x_{\text{mid}}^{(\ell)}(c')$, $\beta' x_{\text{low}}^{(\ell)}(c')$, and $\beta' x_{\text{hi}}^{(\ell)}(c')$ are indeed approximate roots in the sense of Smale.

Complexity Analysis: The logarithmic height bounds on our approximate roots follow directly from construction, and our time bound follows easily upon observing that the truncated series we evaluate involve only $O(\log^2(dH))$ many terms, and each term is an easily computable rational multiple of the previous one. In particular, to get $O(\log(dH))$ bits of accuracy it suffices to compute the leading $O(\log(dH))$ bits of each term (with a suitable increase of the second O-constant).

Our final assertion on the fraction of trinomials that are ill-conditioned can be obtained as follows: We want to find the cardinality of the set:

$$\left\{(c_1, c_2, c_3) \in \{-H, \ldots, H\}^3 \;\middle|\; 0 < \frac{|c_2|}{|c_1|^{\frac{n-m}{n}} |c_3|^{\frac{m}{n}} r_{m,n}} - 1 < \frac{1}{\log(dH)}\right\}.$$

Fix $(c_1, c_3) \in \{-H, \ldots, H\}^2$. Then c_2 satisfies

$$r_{m,n} |c_1|^{\frac{n-m}{n}} |c_3|^{\frac{m}{n}} < |c_2| < \left(1 + \frac{1}{\log(dH)}\right) r_{m,n} |c_1|^{\frac{n-m}{n}} |c_3|^{\frac{m}{n}}$$

Since $|c_2|$ is an integer, the number of c_2 satisfying the last inequality is no more than

$$\sum_{\substack{(c_1,c_3)\in\{-H,\ldots,H\}^2\\ r_{m,n}|c_1|^{\frac{n-m}{n}}|c_3|^{\frac{m}{n}} \leq H}} 2\left\lceil \frac{1}{\log(dH)} r_{m,n} |c_1|^{\frac{n-m}{n}} |c_3|^{\frac{m}{n}} \right\rceil$$
$$\leq \sum_{\substack{(c_1,c_3)\in\{-H,\ldots,H\}^2\\ r_{m,n}|c_1|^{\frac{n-m}{n}}|c_3|^{\frac{m}{n}} \leq H}} 2\left\lceil \frac{H}{\log(dH)} \right\rceil \leq 8H^3\left(\frac{1}{\log(dH)} + \frac{1}{H}\right)$$

where $\lceil x \rceil$ is the smallest integer no less than x. Therefore, the fraction of trinomials that are ill-conditioned is at most $\frac{1}{\log(dH)} + \frac{1}{H}$.

4 SIGNS AND SOLVING ARE ROUGHLY EQUIVALENT FOR TRINOMIALS

In what follows, it clearly suffices to focus on sign evaluation on $\mathbb{R}_+$ and approximation of roots in $\mathbb{R}_+$, since we can simply work with $f(\pm x)$.

Proof of Lemma 1.5: ($\Longrightarrow$) If Koiran's Trinomial Sign Problem can be solved in polynomial-time then we simply apply bisection to solve for all the positive roots of any input trinomial $f \in \mathbb{Z}[x]$ with degree d and all coefficients having logarithmic height $\log H$.

In particular, Lemma 1.8 tells us that the positive roots of f lie in the interval $(1/(2H), 2H)$, and Lemma 2.6 (combined with Baker's Theorem and Theorem 2.1) tells us that we can count exactly how many positive roots there are in time $\log^{2+o(1)}(dH)$.

If there are no positive roots then we are done.

If there is only one positive root then we start with the interval $[0, 2H]$ and then apply bisection (employing the assumed solution to Koiran's Trinomial Sign Problem) until we reach an interval of width $\frac{1}{2H\cdot 4(d-1)^2}$. Theorem 2.10 (combined with a simpler argument for the case $d=2$ involving completing the square and Theorem 2.3) then tells us that this is sufficient accuracy to obtain an approximate root in the sense of Smale. The number of bisection steps is clearly $O(\log(dH))$, so the overall final complexity is $\log^{O(1)}(dH)$ since we've assumed trinomial sign evaluation takes time $\log^{O(1)}(dH)$.

If there are two positive roots then we first approximate the unique positive critical point w of f via Theorem 2.3 (since it is the unique root of a binomial with coefficients of logarithmic height $O(\log(dH))$), to accuracy $\frac{1}{3\cdot 2H\cdot 4(d-1)^2}$. This ensures that the intervals $(0, w)$ and $(w, 2H)$ each contain a positive root of f, thanks to Theorem 2.10. We then apply bisection (in each interval) as in the case of just one positive root, clearly ending in time $\log^{O(1)}(dH)$. ■

(⟸): Our argument is almost identical to the converse case, except that we re-organize our work slightly differently. First, we count the number of positive roots of f in time $\log^{2+o(1)}(dH)$, as outlined in the converse case. Then, we additionally compute the signs of $f(0)$ and $f(+\infty)$ essentially for free by simply evaluation $\text{sign}(c_1)$ and $\text{sign}(c_3)$,

This data will partition $\mathbb{R}_+$ into at most 3 open intervals upon which f has constant (nonzero) sign. So to evaluate $\text{sign}(f(r))$ at an $r \in \mathbb{Q}$ with logarithmic height $\log H'$, we simply need to check which interval contains r *or* if r is itself a rational root of f.

Doing the latter is already known algorithmically, thanks to earlier work of Lenstra: [16] in fact details a polynomial time algorithm for finding all rational roots of any sparse polynomial (and even extends to finding all bounded degree factors, over number fields of bounded degree). In particular, [16] also proves that the logarithmic heights of the rational roots of f are $\log^{O(1)}(dH)$. So we can simply compare r to the rational roots of f (in time $\log^{O(1)}(dH)$) and output $\text{sign}(f(r))=0$ if r matches any such root.

So let us now assume that r is not a root of f. If we compute the positive roots of f to accuracy $\frac{1}{3H'}$, then we can easily decide which interval contains r and immediately compute $\text{sign}(f(r))$. By assumption, finding a set of positive approximate roots respectively converging to each true positive root of f is doable in time $\log^{O(1)}(dH)$. So, to potentially upgrade our approximate roots to accuracy $\frac{1}{3H'}$, we merely apply Newton Iteration: This involves $O(\log\log(dHH'))$ further iterations, and each such iteration involves $\log(dH)$ arithmetic operations. Since we only need accuracy $\frac{1}{3H'}$, we can in fact work with just the $O(\log(dHH'))$ most significant digits of our approximate roots. So we are done. ■

Proof of Corollary 1.4: Our corollary follows easily from the proof of Lemma 1.5: Just as in the proof of the (⟸) direction of our last proof, we first apply [16] to check whether u/v is a root of f in time $\log^{O(1)}(dH)$. If so, then we are done (with $\text{sign}(f(u/v))=0$), so let us assume u/v is *not* a root of f.

From Theorem 1.1, if f is *not* ill-conditioned, then we can find a set of positive approximate roots respectively converging to each true positive root of f. Furthermore, by construction (by Algorithm 3.1 in particular), each approximate root is within distance $\frac{\zeta}{4(d-1)^2}$ of a (unique) true positive root ζ. So, as before, we merely need to refine slightly via Newton iteration until we attain accuracy $\frac{1}{3H}$, to find which interval (on which f has constant sign) r lies in. This additional work takes time $\log^{4+o(1)}(dH)$, so we are done. ■

REFERENCES

[1] Martín Avendano, Roman Kogan, Mounir Nisse, and J. Maurice Rojas. 2018. Metric estimates and membership complexity for Archimedean amoebae and tropical hypersurfaces. *Journal of Complexity* 46 (2018), 45–65.

[2] Alan Baker. 1966. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika* 13 (1966), 204–216; ibid. 14 (1967), 102–107; ibid. 14 (1967), 220–228. https://doi.org/10.1112/s0025579300003843

[3] Daniel J. Bernstein. 2003. Computing Logarithm Intervals with the Arithmetic-Geometric Mean Iterations. http://cr.yp.to/papers.html.

[4] Benoît Bertrand, Frédéric Bihan, and Frank Sottile. 2006. Polynomial systems with few real zeroes. *Math. Z.* 253, 2 (2006), 361–385. https://doi.org/10.1007/s00209-005-0912-8

[5] Frédéric Bihan, J. Maurice Rojas, and Casey E. Stella. 2009. Faster Real feasibility via circuit discriminants. In *Proceedings of ISSAC 2009*.

[6] Lenore Blum, Felipe Cucker, Michael Shub, and Steve Smale. 1998. *Complexity and real computation*. Springer-Verlag, New York. xvi+453 pages. With a foreword by Richard M. Karp.

[7] J. M. Borwein and P. B. Borwein. 1988. On the complexity of familiar functions and numbers. *SIAM Rev.* 30, 4 (1988), 589–601. https://doi.org/10.1137/1030134

[8] Richard P. Brent. 1976. Fast multiple-precision evaluation of elementary functions. *J. Assoc. Comput. Mach.* 23, 2 (1976), 242–251. https://doi.org/10.1145/321941.321944

[9] Nader H. Bshouty, Yishay Mansour, Baruch Schieber, and Prasoon Tiwari. 1997. A tight bound for approximating the square root. *Inform. Process. Lett.* 63, 4 (1997), 211–213. https://doi.org/10.1016/S0020-0190(97)00126-9

[10] Felipe Cucker, Pascal Koiran, and Steve Smale. 1999. A polynomial time algorithm for Diophantine equations in one variable. *J. Symbolic Comput.* 27, 1 (1999), 21–29. https://doi.org/10.1006/jsco.1998.0242

[11] Alperen A. Ergür, Grigoris Paouris, and J. Maurice Rojas. 2021. Correction to: Tropical varieties for exponential sums. *Math. Ann.* 380, 3-4 (2021), 2073–2077. https://doi.org/10.1007/s00208-021-02198-3

[12] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. 1994. *Discriminants, Resultants and Multidimensional Determinants*. Birkhauser.

[13] David Harvey and Joris van der Hoeven. 2021. Integer multiplication in time $O(n\log n)$. *Ann. of Math. (2)* 193, 2 (2021), 563–617. https://doi.org/10.4007/annals.2021.193.2.4

[14] Pascal Koiran. 2019. Root separation for trinomials. *J. Symbolic Comput.* 95 (2019), 151–161. https://doi.org/10.1016/j.jsc.2019.02.004

[15] Pascal Koiran, Natacha Portier, and Sébastien Tavenas. 2015. A Wronskian approach to the real τ-conjecture. *J. Symbolic Comput.* 68, part 2 (2015), 195–214. https://doi.org/10.1016/j.jsc.2014.09.036

[16] H. W. Lenstra, Jr. 1999. Finding small degree factors of lacunary polynomials. In *Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997)*. de Gruyter, Berlin, 267–276.

[17] Tien-Yien Li, J. Maurice Rojas, and Xiaoshen Wang. 2003. Counting real connected components of trinomial curve intersections and m-nomial hypersurfaces. *Discrete Comput. Geom.* 30, 3 (2003), 379–414. https://doi.org/10.1007/s00454-003-2834-8

[18] Thomas Lickteig and Marie-Françoise Roy. 2001. Sylvester-Habicht sequences and fast Cauchy index computation. *J. Symbolic Comput.* 31, 3 (2001), 315–341. https://doi.org/10.1006/jsco.2000.0427

[19] E. M. Matveev. 2000. An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II. *Izv. Ross. Akad. Nauk Ser. Mat.* 64, 6 (2000), 125–180. https://doi.org/10.1070/IM2000v064n06ABEH000314

[20] Maurice Mignotte. 1995. On the Distance Between the Roots of a Polynomial. *Appl. Algebra Eng. Commun. Comput.* 6 (11 1995), 327–332. https://doi.org/10.1007/BF01198012

[21] Yuri Nesterenko. 2003. Linear forms in logarithms of rational numbers. In *Diophantine approximation (Cetraro, 2000)*. Lecture Notes in Math., Vol. 1819. Springer, Berlin, 53–106. https://doi.org/10.1007/3-540-44979-5_2

[22] Victor Y. Pan and Elias P. Tsigaridas. 2013. On the Boolean complexity of real root refinement. In *ISSAC 2013—Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*. ACM, New York, 299–306. https://doi.org/10.1145/2465506.2465938

[23] Grigoris Paouris, Kaitlyn Phillipson, and J. Maurice Rojas. 2019. A faster solution to Smale's 17th problem I: real binomial systems. In *ISSAC'19—Proceedings of the 2019 ACM International Symposium on Symbolic and Algebraic Computation*. ACM, New York, [323–330].

[24] Mikael Passare and August Tsikh. 2004. Algebraic equations and hypergeometric series. In *The legacy of Niels Henrik Abel*. Springer, Berlin, 653–672.

[25] P. Pedersen, M.-F. Roy, and A. Szpirglas. 1993. Counting real zeros in the multivariate case. In *Computational algebraic geometry (Nice, 1992)*. Progr. Math., Vol. 109. Birkhäuser Boston, Boston, MA, 203–224. https://doi.org/10.1007/978-1-4612-2752-6_15

[26] J. Maurice Rojas. 2022. Counting Real Roots in Polynomial-Time for Systems Supported on Circuits. *arXiv e-prints*, Article arXiv:2012.04868 (2022), arXiv:2012.04868 pages. arXiv:2012.04868 [math.AG]

[27] J. Maurice Rojas and Yinyu Ye. 2005. On solving univariate sparse polynomials in logarithmic time. *J. Complexity* 21, 1 (2005), 87–110. https://doi.org/10.1016/j.jco.2004.03.004

[28] J. Maurice Rojas and Yuyu Zhu. 2020. A Complexity Chasm for Solving Sparse Polynomial Equations Over p-adic Fields. *ArXiv* arXiv:2003.00314 (2020).

[29] Michael Sagraloff. 2014. A near-optimal algorithm for computing real roots of sparse polynomials. In *ISSAC 2014 (39th International Symposium on Symbolic and Algebraic Computation)*. 359–366.

[30] Eugene Salamin. 1976. Computation of π using arithmetic-geometric mean. *Math. Comp.* 30, 135 (1976), 565–570. https://doi.org/10.2307/2005327

[31] David Eugene Smith and Marcia L. Latham. 1954. *The Geometry of Renè Descartes*. Dover Publications Inc. https://books.google.com/books?id=G7BJAwAAQBAJ

[32] Joachim von zur Gathen and Jürgen Gerhard. 2013. *Modern Computer Algebra* (3rd ed.). Cambridge University Press.

[33] Yinyu Ye. 1994. Combining binary search and Newton's method to compute real roots for a class of real functions. *J. Complexity* 10, 3 (1994), 271–280. https://doi.org/10.1006/jcom.1994.1014