hexagon:2611.01119v2

Breaking the Linear-Ansatz Barrier for the Sum-of-Square-Roots Problem: $r(n,k) = O(n^{-2k+1/2})$ via Quadratic Radicals, Explicit Families ($k = 2, 3, 4, 5$), Sharp $k = 2$ Separation Bounds, and Lean 4 Formalization

Ivan Besevic
ESIEE-IT, France
ivan.besevic@edu.esiee-it.fr
ORCID: 0009-0004-4124-1465

November 2026

Abstract

For integers $n \geq 1$ and $k \geq 2$, let

$$r(n,k) := \min\left\{ \left| \sum_{i=1}^{k} \sqrt{a_i} - \sum_{j=1}^{k} \sqrt{b_j} \right| > 0 \ : \ a_i, b_j \in \{1, \ldots, n\} \right\}$$

denote the minimal non-zero separation between two sums of k square roots of integers bounded by n. Bounding $r(n,k)$ is the central bottleneck of the *Sum-of-Square-Roots Problem* (Open Problems Project, Problem 33), which asks whether deciding $\sum_{i=1}^{k} \sqrt{a_i} \leq \sum_{j=1}^{k} \sqrt{b_j}$ lies in P or even in NP. For two decades, the sharpest general-k constructive upper bound has been $r(n,k) = O(n^{-2k+3/2})$, established by Qian and Wang (*Inform. Process. Lett.*, 2006) using linear radicands $A_i^2 N + u_i$ (while for $k = 2$, Qian and Wang noted separately that $r(n,2) = \Theta(n^{-7/2})$).

We explain why linear radicands hit an insurmountable Vandermonde wall at $O(n^{-2k+3/2})$, and bypass it via an even-symmetric quadratic radical ansatz combining $2k-2$ pure terms $A_i^2 m^2 + q_i$ with a single conjugate pair $B^2 m^2 \pm rm + s$. To separate elementary machine-checked theorems cleanly from arithmetic-geometric arguments proved on paper, we organize our contributions into two distinct tiers:

1. **Tier 1 — Explicit, elementary, and machine-checked results ($k = 2, 3, 4, 5$):**
   - *Sharp $k = 2$ lower and upper bounds:* we prove $r(n,2) \geq \frac{1}{4} n^{-7/2}$ for *every* $n \geq 1$ (4096× sharper than Burnikel–Fleischer–Mehlhorn–Schirra's $4^{-7} n^{-7/2}$), the asymptotic floor $\left(\frac{8}{27} - O(n^{-4})\right) n^{-7/2}$, and a constant-norm ($M \equiv 82944$) family with $\Delta_2(m) = -\frac{3}{2} m^{-7} + O(m^{-9})$.
   - *Explicit $k = 3$ bound ($O(n^{-11/2})$):* a tiny-integer family at $u = 5$ with $\Delta_3(m) = -\frac{730468750000}{7} m^{-11} + O(m^{-13})$, giving $r(n,3) \leq 10^{70}/(n^5\sqrt{n})$ for all $n \geq 3.13811 \times 10^{16}$.
   - *Compact explicit $k = 4$ bound ($O(n^{-15/2})$):* a compact rational family at $u = 5$ whose six rational nodes all have ≤ 32 bits (weights ≤ 177 bits, $c = 10$), giving $r(n,4) \leq 10^{1780}/(n^7\sqrt{n})$ for all $n \geq 10^{232}$.
   - *Explicit rational $k = 5$ family ($O(n^{-19/2})$):* an exact rational family at $u = 5$ (eight nodes ≤ 1359 bits, verified in exact SymPy rational arithmetic) giving $r(n,5) = O(n^{-19/2})$.

- *Machine-checked Lean 4.36.0 formalization:* all explicit global theorems for $k = 2, 3, 4$ together with the universal algebraic core of the general-k theory (the Vandermonde wall, the quartic leading-coefficient identity, the automatic rational square, the universal U_1 limit, and the unconditional non-torsion of $z = \frac{23+7i\sqrt{3}}{26}$) are completely formalized and kernel-verified in Lean 4.36.0 + Mathlib with zero `sorry`, zero `native_decide`, and strictly the three standard axioms `[propext, Classical.choice, Quot.sound]`.

2. **Tier 2 — All-k constructive upper bound (proved on paper):** we prove that for *every* integer $k \geq 2$,
$$r(n,k) = O\Big(n^{-2k+1/2}\Big),$$
improving the Qian–Wang general-k construction by a full factor of n, strictly improving the best previously known asymptotic exponent for every $k \geq 3$, and matching the birthday-paradox heuristic exponent $-2k + \frac{1}{2}$. The proof uses an inductive dipole perturbation on genus-1 quartic curves, universal $R \to \infty$ nodal quartic limits, Mazur's Torsion Theorem, and Kronecker density on $E(\mathbb{R})^\circ \cong S^1$. These arithmetic-geometric and analytic steps are proved on paper and are *not* formalized in Lean.

Finally, we report exhaustive search records up to $N = 4000$ ($k = 2$) and $N = 350$ ($k = 3$), and analyze the 7-*moment Diophantine surface* for $k = 3$ ($O(n^{-13/2})$): we prove symbolically its exact affine collapse, its Hankel window $v \in (\frac{97}{420}, \frac{1}{4})$, its p-adic constraint $42 \mid \mathrm{lcm}(\mathrm{denom}(y_i))$, and genus-2 slices, and report the empirical observation that modular sieving over 8.5×10^7 rational candidates finds zero non-trivial rational points.

1 Introduction

Given positive integers $a_1, \ldots, a_k, b_1, \ldots, b_k \in \{1, \ldots, n\}$, the *Sum-of-Square-Roots Problem* asks to decide the sign of
$$\sum_{i=1}^{k} \sqrt{a_i} - \sum_{j=1}^{k} \sqrt{b_j}.$$
Introduced in computational geometry by Garey, Graham, and Johnson [1] in connection with Euclidean shortest paths and minimum spanning trees, and listed as Problem 33 in the Open Problems Project [9], this decision problem remains famously open as of 2026: it is not even known to lie in NP, the best known complexity upper bound being the counting-hierarchy class $\mathrm{P}^{\mathrm{PP}^{\mathrm{PP}^{\mathrm{PP}}}}$ (Allender, Bürgisser, Kjeldgaard-Pedersen, and Miltersen [6]).

Because the sum of square roots can be evaluated to b bits of precision in time polynomial in k, $\log n$, and b, deciding its sign reduces to bounding the minimal non-zero separation
$$r(n,k) := \min\left\{ \left| \sum_{i=1}^{k} \sqrt{a_i} - \sum_{j=1}^{k} \sqrt{b_j} \right| > 0 \ : \ 1 \leq a_i, b_j \leq n \right\}. \tag{1}$$
A polynomial-bit lower bound $-\log_2 r(n,k) = \mathrm{poly}(k, \log n)$ would immediately place the Sum-of-Square-Roots Problem in P. However, the gap between proved lower bounds and constructive upper bounds remains vast:

- **Effective lower bounds:** Using degree bounds and root separation in the multiquadratic extension $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{b_k})$, Burnikel, Fleischer, Mehlhorn, and Schirra [3] established the doubly exponential lower bound
$$r(n,k) \geq (2k)^{-(2^{2k}-1)} n^{-(2^{2k-1}-1/2)},$$
later refined in the exponent via algebraic-degree reductions by Cheng, Meng, Sun, and Chen [7] and Cheng and Li [8]. Recently, Eisenbrand, Haeberle, and Singer [10] applied Schmidt's Subspace Theorem to obtain a polynomial-degree bound $|\sum_{i=1}^{m} x_i \sqrt{a_i}| \geq$

$\gamma(a_1, \ldots, a_m)(m \max_i |x_i|)^{-2m}$, but only for *fixed* radicands a_i and with a non-effective constant γ.

- **Heuristic and conjectured separation:** A pigeonhole / birthday-paradox count over the $\binom{n+k-1}{k} = \Theta(n^k)$ sums of k square roots inside $[0, k\sqrt{n}]$ predicts typical minimal gaps of order

$$r(n,k) \approx \frac{k\sqrt{n}}{\binom{n+k-1}{k}^2} = \Theta\Big(n^{-2k+1/2}\Big),$$

and the prevailing conjecture (see [9, 4, 8]) asserts that $r(n,k) = \Omega(n^{-2k})$, or at least $r(n,k) \geq n^{-O(k)}$.

- **Constructive upper bounds:** Using an explicit family of linear radicands $a_i(N) = A_i^2 N + u_i$ with rational weights canceling the first $2k-1$ Taylor moments, Qian and Wang [4, 5] proved the general-k bound

$$r(n,k) = O\Big(n^{-2k+3/2}\Big) \qquad (\forall k \geq 2),$$

yielding $r(n,2) = O(n^{-5/2})$ from their general construction, $r(n,3) = O(n^{-9/2})$, $r(n,4) = O(n^{-13/2})$, and $r(n,5) = O(n^{-17/2})$. For the special case $k=2$, Qian and Wang [4, 5] already noted separately that $r(n,2) = \Theta(n^{-7/2})$; for every $k \geq 3$, however, the exponent $-2k + \frac{3}{2}$ has remained the sharpest known constructive upper bound.

1.1 Why Linear Radicands Hit a Wall at $O(n^{-2k+3/2})$

Before presenting our construction, we observe why the exponent $-2k + \frac{3}{2}$ of Qian and Wang [4] is an absolute barrier for linear radicands.

Proposition 1.1 (Vandermonde Wall for Linear Radicands)**.** *Let $A_1, \ldots, A_k, B_1, \ldots, B_k > 0$ and $u_1, \ldots, u_k, v_1, \ldots, v_k \in \mathbb{R}$. Define*

$$\Delta_{\text{lin}}(N) := \sum_{i=1}^{k} \sqrt{A_i^2 N + u_i} - \sum_{j=1}^{k} \sqrt{B_j^2 N + v_j}.$$

If $\Delta_{\text{lin}}(N) = o\big(N^{-2k+3/2}\big)$ as $N \to \infty$, then $\Delta_{\text{lin}}(N) \equiv 0$ identically.

Proof. Set $t_i := u_i/A_i^2$ $(1 \leq i \leq k)$, $t_{k+j} := v_j/B_j^2$ $(1 \leq j \leq k)$, $w_i := A_i$, and $w_{k+j} := -B_j$. Expanding in $x = 1/N$ yields

$$\Delta_{\text{lin}}(N) = \sqrt{N} \sum_{m=0}^{\infty} \binom{1/2}{m} \left(\sum_{r=1}^{2k} w_r t_r^m \right) N^{-m}.$$

The condition $\Delta_{\text{lin}}(N) = o(N^{-2k+3/2})$ forces the $2k$ moments $m = 0, 1, \ldots, 2k-1$ to vanish identically:

$$\sum_{r=1}^{2k} w_r t_r^m = 0 \qquad (m = 0, 1, \ldots, 2k-1).$$

Grouping identical nodes t_r into $s \leq 2k$ distinct values $\tau_1, \ldots, \tau_s$ with combined weights $W_1, \ldots, W_s$, the first s equations form an invertible $s \times s$ Vandermonde system $\sum_{\ell=1}^{s} W_\ell \tau_\ell^m = 0$ $(0 \leq m < s)$, forcing $W_1 = \cdots = W_s = 0$ (formalized in Lean 4 as `vandermonde_wall_moments`). Hence all terms cancel pairwise and $\Delta_{\text{lin}}(N) \equiv 0$. □

1.2 Main Results and Two-Tier Verification Architecture

We break the linear-ansatz wall by switching to *even-symmetric quadratic radicands* in an integer parameter m (so $n = \Theta(m^2)$): $2k-2$ pure terms $A_i^2 m^2 + q_i$ balanced against a *single* conjugate pair $B^2 m^2 \pm rm + s$. All odd powers of m^{-1} vanish by symmetry, and the even moments of the conjugate pair have *infinite Hankel rank*, avoiding the Vandermonde collapse of Proposition 1.1.

To make the verification status of every claim completely transparent, we separate our results into **Tier 1** (elementary, explicit, and formally verified in Lean 4.36.0 for $k = 2, 3, 4$, plus exact SymPy rational arithmetic for $k = 5$) and **Tier 2** (the all-k induction proved on paper via elliptic curves and Mazur's Torsion Theorem).

Tier 1: Explicit, Elementary, and Machine-Checked Theorems ($k = 2, 3, 4, 5$)

Theorem 1.2 (Explicit $k = 3$ Family and Global Bound — Lean 4 Verified)**.** *For every integer $m \geq 8$, the six strictly positive integers*

$$\begin{aligned} a_1(m) &= 28968^2(m^2 - 55), & b_1(m) &= 13720^2(49m^2 - 1295), \\ a_2(m) &= 53125^2(m^2 - 35), & b_2(m) &= 81600^2(m^2 + 10m + 20), \\ a_3(m) &= 59049^2(9m^2 + 5), & b_3(m) &= 81600^2(m^2 - 10m + 20) \end{aligned}$$

satisfy $\max(a_i, b_j) = a_3(m) = \Theta(m^2)$ *and*

$$\sum_{i=1}^{3} \sqrt{a_i(m)} - \sum_{j=1}^{3} \sqrt{b_j(m)} = -\frac{730468750000}{7}\, m^{-11} + O\big(m^{-13}\big)\,.$$

Consequently, for every integer $n \geq 31\,381\,100\,000\,000\,000$,

$$r(n, 3) \leq \frac{10^{70}}{n^5\sqrt{n}},$$

improving Qian and Wang's $r(n, 3) = O(n^{-9/2})$ by a full factor of n.

Theorem 1.3 (Compact Explicit $k = 4$ Family and Global Bound — Lean 4 Verified)**.** *At $u = 5$, the six distinct rational nodes (each of bit-length at most 32)*

$$t = \left(-\frac{11}{4},\ -\frac{7}{4},\ \frac{1}{8},\ -\frac{1950401}{4041576},\ -\frac{2304476651}{923949684},\ -\frac{182532769}{1258501356}\right)$$

and their unique exact rational weights $w_1, \ldots, w_6$ of signature $(+4, -2)$ (bit-length ≤ 177, common denominator W of 362 bits, scaling $c = 10$; see Section 4.3) yield eight explicit quadratic integer polynomials $a_1(m), \ldots, a_4(m), b_1(m), \ldots, b_4(m) = \Theta(m^2)$ satisfying

$$\sum_{i=1}^{4} \sqrt{a_i(m)} - \sum_{j=1}^{4} \sqrt{b_j(m)} = -\frac{161866452303987151320657971}{898296045741140423812495441920000}\, W \cdot 10^{16} m^{-15} + O\big(m^{-17}\big)\,.$$

Consequently, for every integer $n \geq 10^{232}$,

$$r(n, 4) \leq \frac{10^{1780}}{n^7\sqrt{n}},$$

improving Qian and Wang's $r(n, 4) = O(n^{-13/2})$ by a full factor of n.

Theorem 1.4 (Sharp Effective Lower and Upper Bounds for $k = 2$ — Lean 4 Verified)**.** *(a) For every integer $n \geq 1$ and all $a_1, a_2, b_1, b_2 \in \{1, \ldots, n\}$ with $\sqrt{a_1} + \sqrt{a_2} \neq \sqrt{b_1} + \sqrt{b_2}$,*

$$\left|\sqrt{a_1} + \sqrt{a_2} - \sqrt{b_1} - \sqrt{b_2}\right| \geq \frac{1}{4\, n^3 \sqrt{n}},$$

improving the Burnikel–Fleischer–Mehlhorn–Schirra bound $4^{-7} n^{-7/2}$ by a factor of 4096. Moreover, as $n \to \infty$,

$$r(n, 2) \geq \left(\frac{8}{27} - O\big(n^{-4}\big)\right) n^{-7/2},$$

where $\frac{8}{27} \approx 0.296296$ is the exact maximum of the continuous normalized conjugate product.

(b) For every integer $m \geq 3$, the explicit constant-norm ($M \equiv 82944$) family

$$a_1(m) = 16m^2, \quad a_2(m) = 4m^2 - 24, \quad b_1(m) = 9m^2 + 18m - 9, \quad b_2(m) = 9m^2 - 18m - 9$$

satisfies $\sqrt{a_1} + \sqrt{a_2} - \sqrt{b_1} - \sqrt{b_2} = -\frac{3}{2} m^{-7} - 15m^{-9} + O(m^{-11})$, yielding $r(n, 2) \leq \frac{2^{22}}{n^3 \sqrt{n}}$ for every $n \geq 144$.

Note that while $r(n, 2) = \Theta(n^{-7/2})$ was already noted separately by Qian and Wang [4, 5], Theorem 1.4 supplies the first explicit constant-norm family and sharp effective lower bounds, whereas Theorems 1.2, 1.3, Proposition 4.2 ($k = 5$, verified in exact SymPy rational arithmetic), and Theorem 1.5 strictly improve the best previously known asymptotic exponent for every $k \geq 3$.

Tier 2: All-k Constructive Upper Bound (Proved on Paper)

Theorem 1.5 (All-k Constructive Upper Bound)**.** *For every integer $k \geq 2$, there exist constants $C_k > 0$ and $N_k \geq 1$ such that for all integers $n \geq N_k$,*

$$r(n, k) \leq C_k\, n^{-2k+1/2}.$$

In particular, $r(n, k) = O\big(n^{-2k+1/2}\big)$ for every $k \geq 2$, improving Qian and Wang's general-k linear-radicand construction [4] by a factor of n for all $k \geq 2$ and strictly improving the best previously known asymptotic exponent for every $k \geq 3$.

As detailed in Section 7, the universal algebraic lemmas underlying Theorem 1.5 are formalized in Lean 4 (`UniversalLemmas.lean`) and verified in exact SymPy rational arithmetic, while the arithmetic-geometric and analytic steps of Theorem 1.5 (Mazur's Torsion Theorem, Kronecker density on $E(\mathbb{R})^\circ \cong S^1$, convergence of elliptic logarithms, and the inductive dipole perturbation) are proved on paper in Sections 2–3 and are not formalized in Lean.

2 Even-Symmetric Quadratic Radicals and Prony Reformulation

Fix a non-zero rational parameter $u \in \mathbb{Q} \setminus \{0, 4\}$ (in our general-k proof we set $u = -4$; in our explicit $k = 3, 4, 5$ families we use $u = 5$). Consider the even-symmetric conjugate pair

$$f_u(x) := \sqrt{1 + \sqrt{u}\, x + x^2} + \sqrt{1 - \sqrt{u}\, x + x^2}. \tag{2}$$

Since $f_u(-x) = f_u(x)$, all odd powers of x vanish identically in its Taylor expansion at $x = 0$. Expanding via the binomial series gives

$$f_u(x) = \sum_{j=0}^{\infty} \binom{1/2}{j} \mu_j(u)\, x^{2j},$$

where the *normalized moment sequence* $\mu_j(u) \in \mathbb{Q}[u]$ has the explicit closed form

$$\mu_j(u) := \frac{2}{\binom{1/2}{j}} \sum_{r=0}^{j} \binom{1/2}{j+r} \binom{j+r}{2r} u^r \in \mathbb{Q}[u] \qquad (j \geq 0). \tag{3}$$

For $u = -4$, setting $y = 2x$ gives $f_{-4}(y/2) = \sqrt{1 + y - y^2/4} + \sqrt{1 - y - y^2/4}$ with $\mu_j(-4) \in \mathbb{Q}$:

$$\mu_0(-4) = 2, \;\; \mu_1(-4) = 4, \;\; \mu_2(-4) = 24, \;\; \mu_3(-4) = 144, \;\; \mu_4(-4) = \frac{4256}{5}, \;\; \mu_5(-4) = \frac{35008}{7}, \ldots$$

Note that the linear combination of $L = 2k - 2$ pure quadratic radicals with rational nodes $t_1, \ldots, t_L \in \mathbb{Q}$ and weights $w_1, \ldots, w_L \in \mathbb{Q}$ expands as

$$\sum_{i=1}^{L} w_i \sqrt{1 + t_i x^2} = \sum_{j=0}^{\infty} \binom{1/2}{j} \left(\sum_{i=1}^{L} w_i t_i^j \right) x^{2j}.$$

(For $u = -4$ with $y = 2x$, to keep all signs completely uniform across the general-k proof and our verification script, we adopt the exact convention of (3) with $x^2 = -y^2/4$ at $u = -4$, i.e., $\sqrt{1 + y - y^2/4} + \sqrt{1 - y - y^2/4} = \sum_{j \geq 0} \binom{1/2}{j} \mu_j(-4)(-y^2/4)^j$ and pure terms $\sqrt{1 - (t_i/4)y^2}$.)

Lemma 2.1 (Reduction to Rational Signed-Measure Moments)**.** *Fix $u \in \mathbb{Q} \setminus \{0, 4\}$ and an integer $k \geq 2$, and set $L := 2k - 2$. Suppose there exist L distinct rational nodes $t_1, \ldots, t_L \in \mathbb{Q}$ and rational weights $w_1, \ldots, w_L \in \mathbb{Q}$ satisfying:*

(1) ***Moment matching:*** *$\sum_{i=1}^{L} w_i t_i^j = \mu_j(u)$ for all $j = 0, 1, \ldots, 2k - 1$;*

(2) ***Non-degeneracy:*** *$\sum_{i=1}^{L} w_i t_i^{2k} \neq \mu_{2k}(u)$;*

(3) ***Signature:*** *exactly k of the weights w_i are strictly positive and $k - 2$ are strictly negative.*

Then $r(n, k) = O\big(n^{-2k+1/2}\big)$.

Proof. Substitute $y = \sqrt{u}\, x = c/m$ with $x^2 = y^2/u = c^2/(um^2)$, so that the conjugate pair becomes $\sqrt{1 + c/m + c^2/(um^2)} + \sqrt{1 - c/m + c^2/(um^2)}$ and each pure term becomes $\sqrt{1 + (t_i/u)c^2/m^2}$, yielding rational quadratic radicands in m for every $u \in \mathbb{Q} \setminus \{0\}$. Clear the denominators of $w_1, \ldots, w_L$ by multiplying by $W := \operatorname{lcm}_i(\operatorname{denom}(w_i)) \in \mathbb{Z}_{>0}$. By condition (3), this yields k strictly positive integers $A_1, \ldots, A_k$ (from $w_i > 0$), $k - 2$ strictly positive integers $B_1, \ldots, B_{k-2}$ (from $w_i < 0$), and $B := W \in \mathbb{Z}_{>0}$. Choose $c \in \mathbb{Z}_{>0}$ divisible by $\operatorname{lcm}(\operatorname{num}(u), \operatorname{denom}(t_1), \ldots, \operatorname{denom}(t_L))$ and large enough that $q_i := A_i^2 t_i c^2/u$, $s_j := B_j^2 t_j c^2/u$, $r_{\text{pair}} := B^2 c$, and $s_{\text{pair}} := B^2 c^2/u$ are all integers.

For all integers $m \geq m_0$, all $2k$ quadratic polynomials

$$\begin{aligned} a_i(m) &:= A_i^2 m^2 + q_i \quad (1 \leq i \leq k), & b_j(m) &:= B_j^2 m^2 + s_j \quad (1 \leq j \leq k-2), \\ b_{k-1}(m) &:= B^2 m^2 + r_{\text{pair}} m + s_{\text{pair}}, & b_k(m) &:= B^2 m^2 - r_{\text{pair}} m + s_{\text{pair}} \end{aligned}$$

are strictly positive integers bounded above by $M_k m^2$ for a constant $M_k > 0$. By conditions (1) and (2),

$$\begin{aligned} \Delta(m) &:= \sum_{i=1}^{k} \sqrt{a_i(m)} - \sum_{j=1}^{k} \sqrt{b_j(m)} \\ &= \binom{1/2}{2k} \frac{W c^{4k}}{u^{2k}} \left(\sum_{i=1}^{L} w_i t_i^{2k} - \mu_{2k}(u) \right) m^{-(4k-1)} + O\Big(m^{-(4k+1)}\Big). \end{aligned}$$

Since $\binom{1/2}{2k} \neq 0$ and $\sum_{i=1}^{L} w_i t_i^{2k} \neq \mu_{2k}(u)$, there exist $m_1 \geq m_0$ and $c_k > 0$ such that $0 < |\Delta(m)| \leq c_k m^{-(4k-1)}$ for all $m \geq m_1$. Finally, for any integer $n \geq M_k(m_1 + 1)^2$, setting $m := \lfloor \sqrt{n/M_k} \rfloor \geq m_1$ guarantees $1 \leq a_i(m), b_j(m) \leq M_k m^2 \leq n$ and $m \geq \frac{1}{2}\sqrt{n/M_k}$, whence

$$0 < |\Delta(m)| \leq c_k \left(2\sqrt{M_k}\right)^{4k-1} n^{-(4k-1)/2} = C_k\, n^{-2k+1/2}. \qquad \square$$

2.1 Prony Reformulation and the Two-Quartic Step

Fix $u \in \mathbb{Q} \setminus \{0, 4\}$ and let $\langle\cdot\rangle_\mu : \mathbb{Q}[t] \to \mathbb{Q}$ denote the linear functional $\langle t^j\rangle_\mu := \mu_j(u)$. Given L distinct nodes $t_1, \dots, t_L \in \mathbb{Q}$ with monic nodal polynomial $Q(t) := \prod_{i=1}^{L}(t - t_i)$, the unique Vandermonde weights $w_1, \dots, w_L \in \mathbb{Q}$ matching $\mu_0, \dots, \mu_{L-1}$ automatically match μ_L and μ_{L+1} *if and only if*

$$\langle Q(t)\rangle_\mu = 0 \qquad \text{and} \qquad \langle t\,Q(t)\rangle_\mu = 0. \tag{4}$$

Indeed, expanding $t^L = Q(t) + \text{lower terms}$ and $t^{L+1} = tQ(t) + \text{lower terms}$ shows that $\sum w_i t_i^m = \mu_m$ for $m = L, L+1$ is equivalent to $\langle Q\rangle_\mu = \langle tQ\rangle_\mu = 0$, while condition (2) of Lemma 2.1 is equivalent to $\langle t^2 Q(t)\rangle_\mu \neq 0$.

Now factor $Q(t) = A(t)(t^2 + st + p)$, where $A(t) = \prod_{i=1}^{L-2}(t - t_i)$, and define the shifted moments $\nu_m := \langle t^m A(t)\rangle_\mu$. Then (4) becomes the 2×2 linear system

$$\nu_2 + s\nu_1 + p\nu_0 = 0, \qquad \nu_3 + s\nu_2 + p\nu_1 = 0,$$

with determinant $\Delta(A) := \nu_1^2 - \nu_0\nu_2$, solution $s = s_{\text{num}}/\Delta(A)$, $p = p_{\text{num}}/\Delta(A)$ where

$$s_{\text{num}} := -\nu_2\nu_1 + \nu_3\nu_0, \qquad p_{\text{num}} := -\nu_1\nu_3 + \nu_2^2,$$

and quadratic discriminant numerator

$$D(A) := s_{\text{num}}^2 - 4p_{\text{num}}\Delta(A). \tag{5}$$

Whenever $\Delta(A) \neq 0$ and $D(A) > 0$ is a *rational square*, the final two nodes

$$t_{L-1}, t_L = \frac{-s \pm \sqrt{D(A)}/|\Delta(A)|}{2}$$

are distinct rational numbers.

Lemma 2.2 (Leading-Coefficient Identity and Automatic Rational Point — Lean 4 Verified)**.** *Let $B(t) = \prod_{i=1}^{L-3}(t - t_i)$ be a monic polynomial of degree $L - 3$ with distinct rational roots, and set $A_x(t) := B(t)(t - x)$.*

(1) The discriminant numerator $D(A_x)$ is a polynomial of degree at most 4 in x, whose coefficient of x^4 is identically $D(B)$ (`leading_coeff_identity`).

(2) If $(t_1, \dots, t_{L-2})$ is already a valid $(k-1)$-solution (so $A(t) = B(t)(t - t_{L-2})$ satisfies $\langle A\rangle_\mu = \langle tA\rangle_\mu = 0$ and $\delta := \langle t^2 A\rangle_\mu \neq 0$), then setting $c_0 := w_{L-2}B(t_{L-2}) \neq 0$ we have

$$D(B) = (c_0\delta)^2 > 0$$

(`automatic_rational_square`), which is automatically a non-zero rational square.

Proof. (1) Letting $\sigma_m := \langle t^m B(t)\rangle_\mu$, we have $\nu_m(x) = \langle t^m B(t)(t - x)\rangle_\mu = \sigma_{m+1} - x\sigma_m$. Since D is homogeneous of degree 4 in $(\nu_0, \nu_1, \nu_2, \nu_3)$, the coefficient of x^4 in $D(A_x)$ equals

$$D(-\sigma_0, -\sigma_1, -\sigma_2, -\sigma_3) = D(\sigma_0, \sigma_1, \sigma_2, \sigma_3) = D(B).$$

(2) Because the $(k-1)$-solution $(t_1, \dots, t_{L-2})$ with weights $(w_1, \dots, w_{L-2})$ matches moments $0, \dots, L-1$ and $\deg B = L - 3$, we have $B(t_i) = 0$ for $1 \le i \le L - 3$, hence

$$\sigma_m = \sum_{i=1}^{L-2} w_i t_i^m B(t_i) = c_0 t_{L-2}^m \qquad (m = 0, 1, 2).$$

For $m = 3$, using $t^3 B(t) = t^2 A(t) + t_{L-2}t^2 B(t)$ gives $\sigma_3 = \langle t^2 A\rangle_\mu + t_{L-2}\sigma_2 = c_0 t_{L-2}^3 + \delta$. Direct substitution into (5) yields $\Delta(B) = \sigma_1^2 - \sigma_0\sigma_2 = 0$ and $s_{\text{num}}(B) = -\sigma_2\sigma_1 + \sigma_3\sigma_0 = c_0\delta$, so $D(B) = (c_0\delta)^2 > 0$. □

Lemma 2.3 (Universal 3-Torsion, Non-Vanishing $\psi_3'(0)$, and Dipole Opening)**.** *Let $(t_1, \dots, t_L)$ be any valid m-solution ($m \geq 2$, $L = 2m-2$) with non-zero weights $(w_1, \dots, w_L)$ and nodal polynomial $Q(t) = A_{\mathrm{prev}}(t)(t - t_{L-1})(t - t_L)$, where $A_{\mathrm{prev}}(t) = \prod_{i=1}^{L-2}(t - t_i)$ and $\delta_Q := \langle t^2 Q(t)\rangle_\mu \neq 0$. Translate coordinates by $t \mapsto t + t_L$ (so $t_L = 0$ and $t_{L-1} = -a$ with $a := t_L - t_{L-1} \neq 0$), and set*

$$n_1 := \langle t A_{\mathrm{prev}}(t)\rangle_\mu = -a w_{L-1} A_{\mathrm{prev}}(t_{L-1}) \neq 0, \qquad c_0 := \langle (t+a) A_{\mathrm{prev}}(t)\rangle_\mu = a w_L A_{\mathrm{prev}}(t_L) \neq 0.$$

Consider the 1-parameter family of quartic curves

$$E_2(\varepsilon) \ : \ Z^2 = D_2(\varepsilon, y) := D\Big(A_{\mathrm{prev}}(t)(t + a - \varepsilon)(t - y)\Big)$$

for small $\varepsilon \in \mathbb{Q}$ with $D_1(-a + \varepsilon) = \square$ (supplying rational points at infinity $Q_\infty^\pm \in E_2(\varepsilon)(\mathbb{Q})$ by Lemma 2.2(1)). Then:

(1) ***Unbounded component and exact universal 3-torsion at $\varepsilon = 0$:*** *Writing $s_4 := \langle t^3 Q(t)\rangle_\mu / \delta_Q$,*

$$D_2(0, y) = c_0^2 \delta_Q^2 \, y \left(y(y - s_4)^2 - \frac{4\delta_Q}{c_0} \right)$$

(formalized in Lean 4 as `universal_D2_zero`*). In particular, $D_2(0, y) > 0$ on the entire half-line $\{y : \mathrm{sgn}(y) = -\mathrm{sgn}(\delta_Q / c_0)\}$, so $y = 0$ always lies on the unbounded real component containing $Q_\infty^\pm$. Moreover, on $E_2(0)$,*

$$\mathrm{div}\left(\frac{\big(Z - c_0 \delta_Q y(y - s_4)\big)^2}{y} \right) = 3\big(Q_\infty^+ - Q_\infty^-\big),$$

so $[Q_\infty^- - Q_\infty^+]$ has exact order 3 at $\varepsilon = 0$ (and its real elliptic logarithm $\alpha(\varepsilon) \in \mathbb{R}/\mathbb{Z}$ on the unbounded component converges continuously to $\pm\frac{1}{3}$ as $\varepsilon \to 0$, whether $E_2(0)$ is smooth or has a real node at $y = s_4/3$ outside the unbounded component).

(2) ***Universal non-vanishing derivative of the 3-division polynomial:*** *Transforming $E_2(\varepsilon)$ to Weierstrass form with Q_∞^+ at infinity, the 3-division polynomial of $[Q_\infty^- - Q_\infty^+]$ satisfies identically*

$$\psi_3(0) = 0, \qquad \psi_3'(0) = 196608 \, a \, \delta_Q^{10} \, n_1 \, c_0^5 \neq 0.$$

Consequently, for every sufficiently small rational $\varepsilon \neq 0$ with $D_1(-a + \varepsilon) = \square$, either $E_2(\varepsilon)$ is a smooth elliptic curve on which $[Q_\infty^- - Q_\infty^+]$ has order > 12 (hence infinite order *by Mazur's Torsion Theorem [2]), or $E_2(\varepsilon)$ is a singular genus-0 conic with the rational point Q_∞^+. In either case, $E_2(\varepsilon)(\mathbb{Q})$ is topologically dense in the unbounded real component of $E_2(\varepsilon)(\mathbb{R})$.*

(3) ***Dipole opening, unbounded scale $R' \to +\infty$, and universal opposite signs:*** *For $\varepsilon \to 0$ with $\mathrm{sgn}(\varepsilon) = \mathrm{sgn}\big(\delta_Q/(a n_1)\big)$, the open dipole interval $I_{\mathrm{dip}}(\varepsilon)$ between the root $y_{\mathrm{root}}(\varepsilon)$ of $D_2(\varepsilon, \cdot)$ and the adjacent root $y_{\mathrm{pole}}(\varepsilon)$ of $\Delta_2(\varepsilon, \cdot)$ satisfies*

$$y_{\mathrm{pole}}(\varepsilon) - y_{\mathrm{root}}(\varepsilon) = -\frac{a^2 n_1^2}{4\delta_Q c_0} \, \varepsilon^2 + O(\varepsilon^3),$$

so $I_{\mathrm{dip}}(\varepsilon)$ lies strictly inside the unbounded real component of $E_2(\varepsilon)(\mathbb{R})$. As y sweeps $I_{\mathrm{dip}}(\varepsilon)$, the shifted moments $\tau_j = \langle t^j A_{\mathrm{prev}}(t)(t + a - \varepsilon)(t - y)\rangle_\mu$ satisfy $\tau_2 = \delta_Q + O(\varepsilon)$, $\tau_1 = a n_1 \varepsilon + O(\varepsilon^2)$, and $\tau_0 = \lambda' \tau_1^2 / \tau_2$ with λ' sweeping continuously across $(\frac{3}{4}, 1)$, giving scale $R' := \tau_2/\tau_1 = \frac{\delta_Q}{a n_1 \varepsilon} + O(1) \to +\infty$. For every $\lambda' \in (\frac{3}{4}, 1)$, the two new nodes $t_{L+1} = r_1 R' + O(1)$, $t_{L+2} = r_2 R' + O(1)$ (roots of $(1 - \lambda')r^2 - r + 1 = 0$) carry strictly opposite-signed weights $(+1, -1)$ while all L old weights vary by $O(\varepsilon)$, preserving all L original signs.

Proof. (1) Since $\langle Q\rangle_\mu = \langle tQ\rangle_\mu = 0$ and $Q(t) = (t+a)tA_{\mathrm{prev}}(t)$, the moments $\sigma_j := \langle t^j(t+a)A_{\mathrm{prev}}(t)\rangle_\mu$ satisfy $\sigma_0 = c_0$, $\sigma_1 = \sigma_2 = 0$, $\sigma_3 = \delta_Q$, and $\sigma_4 = s_4\delta_Q$. Substituting $\tau_j = \sigma_{j+1} - y\sigma_j$ into (5) directly gives $D_2(0,y) = c_0^2\delta_Q^2 y^2(y-s_4)^2 - 4c_0\delta_Q^3 y$. For y of sign $-\operatorname{sgn}(\delta_Q/c_0)$, $y(y-s_4)^2$ and $-4\delta_Q/c_0$ have the same sign, so $D_2(0,y) > 0$ on the entire half-line; moreover, if $E_2(0)$ is singular, its double root $y_0 = s_4/3$ satisfies $y_0(y_0 - \frac{4}{3}s_4) = -\frac{1}{3}s_4^2 < 0$ and is strictly separated from the unbounded component $\{y : y(y-\frac{4}{3}s_4) \geq 0\}$, where the inversion $w = 1/(y-y_0)$ gives continuous convergence of the real elliptic logarithm to the circle angle $\frac{1}{2} \pm \frac{1}{\pi}\arcsin(\frac{1}{2}) = \pm\frac{1}{3} \pmod 1$. The principal divisor identity follows from $(Z - c_0\delta_Q y(y-s_4))(Z + c_0\delta_Q y(y-s_4)) = -4c_0\delta_Q^3 y$, noting that $\operatorname{div}(y) = 2(0,0) - Q_\infty^+ - Q_\infty^-$ and $\operatorname{div}(Z - c_0\delta_Q y(y-s_4)) = (0,0) + Q_\infty^+ - 2Q_\infty^-$.

(2) Exact symbolic expansion in dual numbers $\bmod \varepsilon^2$ (verified in `scripts/verify_general_k.py`) yields $\psi_3(0) = 0$ and $\psi_3'(0) = 196608\, a\, \delta_Q^{10}\, n_1\, c_0^5 \neq 0$. Note that Q_∞^+ and Q_∞^- lie on the same unbounded real component $E_2(\varepsilon)(\mathbb{R})^\circ$, and when $E_2(\varepsilon)$ is smooth the real elliptic logarithm $\alpha(\varepsilon) : E_2(\varepsilon)(\mathbb{R})^\circ \xrightarrow{\sim} \mathbb{R}/\mathbb{Z}$ is an *injective* group isomorphism. Hence a torsion point of exact order $q \in \{1,\dots,10,12\}$ maps to a reduced fraction $p/q \in \mathbb{R}/\mathbb{Z}$ with $\gcd(p,q) = 1$, which can equal $\pm\frac{1}{3} \pmod 1$ *only* when $q = 3$ (ruling out $q = 6, 9, 12$ from landing on $\pm\frac{1}{3}$). Since $\lim_{\varepsilon\to 0}\alpha(\varepsilon) = \pm\frac{1}{3} \pmod 1$ and $\min\{|p/q - 1/3| : 1 \leq q \leq 12,\ \gcd(p,q) = 1,\ q \neq 3\} = \frac{1}{33}$, every sufficiently small $\varepsilon \neq 0$ satisfies $0 < |\alpha(\varepsilon) - (\pm\frac{1}{3})| < \frac{1}{33}$ (with $q = 3$ excluded by $\psi_3(\varepsilon) = \psi_3'(0)\varepsilon + O(\varepsilon^2) \neq 0$). If $E_2(\varepsilon)$ is smooth, Mazur's Torsion Theorem [2] implies $[Q_\infty^- - Q_\infty^+]$ has infinite order and Kronecker density on $E_2(\varepsilon)(\mathbb{R})^\circ$ gives density of $E_2(\varepsilon)(\mathbb{Q})$ on the unbounded component. If $E_2(\varepsilon)$ is singular for small ε, note that at $\varepsilon = 0$, $y = 0$ is a simple root ($D_2'(0,0) = -4c_0\delta_Q^3 \neq 0$) and the other finite endpoint of the unbounded component is also simple (since any double root $y_0 = s_4/3$ of $D_2(0,y)$ lies strictly outside the unbounded component); thus for small ε, $D_2(\varepsilon, y)$ has at least two simple real roots and hence at most one double root y_*. Being unique, y_* is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant and therefore rational, so stereographic projection from Q_∞^+ parameterizes $E_2(\varepsilon)$ over $\mathbb{Q}$, again giving density on the entire real locus.

(3) Setting $y = -\frac{n_1}{c_0}\varepsilon + y_2\varepsilon^2$, direct expansion gives $\tau_1 = an_1\varepsilon + O(\varepsilon^2)$, $\tau_2 = \delta_Q + O(\varepsilon)$, $D_2(\varepsilon, y) = a^2\delta_Q^2 n_1^2(4\lambda' - 3)\varepsilon^2 + O(\varepsilon^3)$, $\Delta_2(\varepsilon, y) = a^2 n_1^2(1-\lambda')\varepsilon^2 + O(\varepsilon^3)$, and $y_{\mathrm{pole}}(\varepsilon) - y_{\mathrm{root}}(\varepsilon) = -\frac{a^2 n_1^2}{4\delta_Q c_0}\varepsilon^2 + O(\varepsilon^3)$, whose sign matches $-\operatorname{sgn}(\delta_Q/c_0)$, placing $I_{\mathrm{dip}}(\varepsilon)$ inside the unbounded component. For every $\lambda' \in (\frac{3}{4}, 1)$, the rescaled new nodes $r_1 < r_2$ are the positive roots of $(1-\lambda')r^2 - r + 1 = 0$. Evaluating at $r = 1/\lambda'$ gives $(1-\lambda')^2/(\lambda')^2 > 0$, while the midpoint $\frac{1}{2(1-\lambda')} > \frac{1}{\lambda'}$ (since $\lambda' > \frac{2}{3}$); hence $1/\lambda' < r_1 < r_2$ and $1 - r_2\lambda' < 1 - r_1\lambda' < 0$. By Lagrange interpolation, the two new weights are

$$w_{L+1} \sim \frac{\delta_Q(1 - r_2\lambda')/R'}{-(r_1R')^L(r_2 - r_1)R'}, \qquad w_{L+2} \sim \frac{\delta_Q(1 - r_1\lambda')/R'}{+(r_2R')^L(r_2 - r_1)R'},$$

whose numerators share the same sign ($-\operatorname{sgn}(\delta_Q)$) while their denominators have strictly opposite signs, giving exact signature $(+1, -1)$. Meanwhile, for $1 \leq i \leq L$, the old weights satisfy $w_i' = w_i + O(\varepsilon)$, preserving all L original signs for small ε. To check non-degeneracy explicitly, let $A_{\mathrm{new}}(t) = A_{\mathrm{prev}}(t)(t + a - \varepsilon)(t - y)$ and $Q_{\mathrm{new}}(t) = A_{\mathrm{new}}(t)(t - t_{L+1})(t - t_{L+2})$. Then

$$\langle t^2 Q_{\mathrm{new}}\rangle_\mu = \tau_4 - (t_{L+1} + t_{L+2})\tau_3 + t_{L+1}t_{L+2}\tau_2 \sim r_1 r_2 (R')^2\delta_Q \neq 0$$

for sufficiently small ε, with λ' in a compact subinterval of $(3/4, 1)$.

Finally, the dipole calculation used translated coordinates. Returning to the original coordinate by adding the fixed translation $h = t_L$ gives $\widehat{\tau}_0 = \tau_0$, $\widehat{\tau}_1 = \tau_1 + h\tau_0$, and $\widehat{\tau}_2 = \tau_2 + 2h\tau_1 + h^2\tau_0$. Thus $\widehat{R} = \widehat{\tau}_2/\widehat{\tau}_1 = R' + O(1)$ and $\widehat{\lambda} = \widehat{\tau}_0\widehat{\tau}_2/\widehat{\tau}_1^2 = \lambda' + O(1/R')$. In the base and induction steps choose the translated λ' in a smaller open interval whose closure lies inside J, and choose ε small enough that $\widehat{\lambda} \in J$ and $\widehat{R}$ exceeds the required threshold. All moment-ratio bounds in the induction hypothesis are taken in the original coordinates; their limits are the corresponding ratios for the fixed polynomial Q. □

3 Proof of Theorem 1.5: $r(n,k) = O(n^{-2k+1/2})$ for All $k \geq 2$

We now fix $u = -4$ throughout this section. For $k = 2$, $(t_1, t_2) = (0, 6)$ with weights $(w_1, w_2) = (\frac{4}{3}, \frac{2}{3})$ satisfies conditions (1)–(3) of Lemma 2.1 (matching $\mu_0 = 2, \mu_1 = 4, \mu_2 = 24, \mu_3 = 144$, with $\sum w_i t_i^4 = 864 \neq \frac{4256}{5} = \mu_4$; verified in Lean 4 as `base_k2_moments`). To establish Theorem 1.5 for all $k \geq 3$, we prove by induction on $m \geq 3$ the following quantitative statement.

Definition 3.1 (Induction Hypothesis $\mathcal{H}(m)$, $m \geq 3$)**.** Fix an open interval J centered at $\lambda_0 = 21/25$, with closure contained in $(3/4, 1)$, sufficiently small as specified in Step 3 below. There exists a constant $B_m > 0$ such that for every threshold $M > 0$, there exist $L = 2m - 2$ distinct rational numbers $t_1, \ldots, t_L \in \mathbb{Q}$ satisfying conditions (1)–(3) of Lemma 2.1 for $k = m$ and $u = -4$, such that letting $A_{\text{prev}}(t) := \prod_{i=1}^{L-2}(t - t_i)$ and $\nu_j := \langle t^j A_{\text{prev}}(t) \rangle_\mu$:

(a) $\delta := \nu_2 \neq 0$ and $|\nu_j/\delta| \leq B_m$ for $j = 3, 4, 5$;

(b) $\nu_1 = \delta/R$ and $\nu_0 = \lambda\delta/R^2$ with $R > M$ and $\lambda \in J$.

Note that at the center $\lambda_0 = \frac{21}{25} = 0.84$, the final two nodes satisfy $t_{L-1} = r_1 R + O(1)$ and $t_L = r_2 R + O(1)$ with $r_1 = \frac{5}{4}$, $r_2 = 5$.

3.1 Base Case $\mathcal{H}(3)$

Start from the fixed $k = 2$ solution $(t_1, t_2) = (0, 6)$ with $w_1 = \frac{4}{3}, w_2 = \frac{2}{3}$ and $\delta_Q = \mu_4 - 6\mu_3 = -\frac{64}{5} \neq 0$. Perturbing $t_1 = 0 \to \varepsilon$ defines the smooth genus-1 quartic curve

$$E_1^{(3)} \ : \ Y^2 = D_1(\varepsilon) = \frac{4096}{25}\left(225\varepsilon^4 - 2680\varepsilon^3 + 8104\varepsilon^2 - 736\varepsilon + 16\right).$$

By Lemma 2.2(2), $P_0^{\pm} = (0, \pm\frac{256}{5}) \in E_1^{(3)}(\mathbb{Q})$ lie on the unbounded real component $(-\infty, 0.03530\ldots] \cup [5.92472\ldots, +\infty)$. Transforming $E_1^{(3)}$ birationally to Weierstrass form with P_0^+ at infinity, exact rational arithmetic (`scripts/verify_general_k.py`) verifies $j \cdot [P_0^+ - P_0^-] \neq \mathcal{O}$ for all $1 \leq j \leq 12$. By Mazur's Torsion Theorem [2], $[P_0^+ - P_0^-]$ has infinite order in $E_1^{(3)}(\mathbb{Q})$, so by Kronecker's theorem rational points $\varepsilon \in E_1^{(3)}(\mathbb{Q})$ are dense near $\varepsilon = 0$.

Now let $M > 0$ be given. Since $(t_1, t_2) = (0, 6)$ is fixed, Lemma 2.3(2)–(3) applies directly: pick a sufficiently small rational $\varepsilon > 0$ with $D_1(\varepsilon) = \square$ so that $E_2^{(3)}(\varepsilon)(\mathbb{Q})$ is dense in $I_{\text{dip}}(\varepsilon)$, $R' = \frac{4}{15\varepsilon} + O(1) > M$, and the perturbed old weights stay positive ($w_1' = \frac{4}{3} + O(\varepsilon) > 0$, $w_2' = \frac{2}{3} + O(\varepsilon) > 0$). Choosing a rational $y \in E_2^{(3)}(\varepsilon)(\mathbb{Q}) \cap I_{\text{dip}}(\varepsilon)$ where $\lambda' \in J$ yields four distinct rational nodes $(\varepsilon, y, t_3, t_4)$ with signature $(+3, -1)$, $R' > M$, and $|\tau_j/\tau_2| \leq B_3$ uniformly as $\varepsilon \to 0^+$ (since $\tau_j \to \langle t^j t(t-6) \rangle_\mu$ and $\tau_2 \to -\frac{64}{5}$). This proves $\mathcal{H}(3)$.

3.2 Inductive Step $\mathcal{H}(m) \implies \mathcal{H}(m+1)$ $(m \geq 3)$

Assume $\mathcal{H}(m)$ holds with constant $B_m > 0$. We first show that for a *single* sufficiently large scale $R > M_1(B_m)$, the first quartic curve E_1 has dense rational points near t_{L-1}, and then hold that m-solution *completely fixed* while applying Lemma 2.3 to achieve any desired threshold $M' > 0$.

Step 1: Universal $R \to \infty$ scaling limit for E_1. For any m-solution from $\mathcal{H}(m)$, set $e := 1/R$ and rescale $x = \xi R$. Substituting $\nu_0 = \lambda\delta e^2$, $\nu_1 = \delta e$, $\nu_2 = \delta$, and $|\nu_j/\delta| \leq B_m$ $(j = 3, 4, 5)$ into $D_1(x) = D(A_{\text{prev}}(t)(t - x))$ yields an exact m-independent, B_m-independent leading asymptotic as $e \to 0$ (formalized in Lean 4 as `universal_U1_limit`):

$$\frac{e^2 D_1(\xi R)}{\delta^4} = \xi^2\Big((4\lambda - 3)\xi^2 + 2\xi - 3\Big) + e\, g_e(\xi), \tag{6}$$

where $g_e(\xi)$ is a polynomial of degree at most 4 in ξ whose coefficients are bounded uniformly in terms of B_m and $\overline{J}$. The unperturbed nodes t_{L-1}, t_L are the roots of $(1-\lambda)(et)^2 - (1+O(e))(et) + (1+O(e)) = 0$, whose discriminant $(4\lambda-3)+O(e)$ is bounded strictly away from 0 uniformly on $\overline{J}$; hence $et_{L-1} = r_1(\lambda) + O(e)$ uniformly on $\overline{J}$ as $e \to 0^+$. At $\xi = r_1(\lambda)$, $(4\lambda-3)r_1^2 + 2r_1 - 3 = (r_1-1)^2 > 0$, so $P_0^{\pm} = (t_{L-1}, \pm c_0\delta_Q) \in E_1(\mathbb{Q})$ (guaranteed rational by Lemma 2.2(2)) lie strictly inside the unbounded real component $(-\infty, r_-] \cup [r_+, +\infty)$ of $E_1(\mathbb{R})$.

Step 2: Convergence of elliptic logarithms to S^1 nodal angles. For any real quartic family $f_e(\xi) = \xi^2(a\xi^2 + b\xi - s^2) + e\, g_e(\xi)$ with $a > 0$, $s > 0$, and $g_e(\xi)$ a polynomial of degree at most 4 with uniformly bounded coefficients, the inversion $w = 1/\xi$ maps the unbounded real component onto a compact interval $[w_-(e), w_+(e)]$ strictly bounded away from the two merging roots $w = O(1/e)$ near $\xi = 0$, transforming the holomorphic differential into

$$\frac{d\xi}{\sqrt{f_e(\xi)}} = -\frac{dw}{\sqrt{a + bw - s^2w^2 + e\, w^4 g_e(1/w)}},$$

where $w^4 g_e(1/w)$ is again a polynomial of degree at most 4 in w with uniformly bounded coefficients on $[w_-(e), w_+(e)]$ (including across $w = 0$). The two endpoints in the w-coordinate are simple roots converging uniformly to those of $a + bw - s^2w^2$. Factoring the transformed polynomial as $(w - w_-(e))(w_+(e) - w)h_e(w)$ on this interval gives $h_e \to s^2$ uniformly (by uniform convergence of the polynomial coefficients and the simple roots). Substituting $w = w_-(e) + (w_+(e) - w_-(e))\sin^2\theta$ removes the endpoint singularities. By dominated convergence in this fixed integration coordinate, as $e \to 0^+$, the real period $\Omega_e \to \frac{2\pi}{s}$ and the real elliptic logarithm $\alpha_e(P) \in \mathbb{R}/\mathbb{Z}$ of any point P bounded away from $\xi = 0$ converges uniformly to the exact circle angle

$$\alpha_0(P) = \frac{1}{2\pi}\left[\arcsin\left(\frac{2s^2w(P) - b}{\sqrt{b^2 + 4as^2}}\right) - \arcsin\left(\frac{2s^2w(O) - b}{\sqrt{b^2 + 4as^2}}\right)\right] \pmod 1. \tag{7}$$

Step 3: Density of rational points on E_1 for one fixed large R. Apply Step 2 to (6) ($a = 4\lambda - 3 > 0$, $b = 2$, $s = \sqrt{3}$). At $\lambda_0 = \frac{21}{25}$ ($r_1 = \frac{5}{4}$, $w(P_0^{\pm}) = \frac{4}{5}$), the exact limiting angle of $[P_0^+ - P_0^-]$ corresponds to the unit complex number

$$z(P_0^+ - P_0^-) = \frac{23 + 7i\sqrt{3}}{26}, \qquad \min_{1 \le j \le 12} |z^j - 1| = 0.457564\cdots > 0.45.$$

We have an exact, unconditional non-torsion certificate at the center (formalized in Lean 4 as `z_center_norm_sq` and `z_center_not_root_of_unity`): $|z|^2 = 1$ and $z + z^{-1} = 23/13$ is rational but not integral, so $z^n \neq 1$ for every integer $n \geq 1$. In particular $d_0 := \min_{1 \le j \le 12} |z^j - 1| > 0$, without relying on any decimal approximation. For nearby λ, the limiting unit complex number of the difference of the two sheets is, up to conjugation,

$$z(\lambda) = 2v(\lambda)^2 - 1 + 2iv(\lambda)\sqrt{1 - v(\lambda)^2}, \qquad v(\lambda) = \frac{1 + 3\sqrt{4\lambda - 3}}{\sqrt{48\lambda - 32}}.$$

This follows by integrating on both sheets of the limiting conic, using $w(P_0^{\pm}) = 1/r_1(\lambda) = (1 + \sqrt{4\lambda - 3})/2$. By continuity, choose the fixed open interval J in $\mathcal{H}(m)$ so small that $|z(\lambda)^j - 1| \geq d_0/2$ for every $\lambda \in \overline{J}$ and $1 \leq j \leq 12$. The same J works at every induction level; the dipole lemma permits choosing λ' in any smaller open subinterval of J. Because $et_{L-1} = r_1(\lambda) + O(e)$, the normalized quartic convergence, and the simple-root integration argument are all uniform on $\overline{J}$, there exists a threshold $M_1 = M_1(B_m) > 0$ such that for any m-solution from $\mathcal{H}(m)$ with $R > M_1$, either:

- E_1 is a smooth elliptic curve, in which case $[P_0^+ - P_0^-]$ has order > 12 and therefore *infinite order* by Mazur's Torsion Theorem [2], so $E_1(\mathbb{Q})$ is dense in the unbounded component containing $P_0^{\pm}$ by Kronecker's theorem; or

- E_1 has a double root near $\xi = 0$ (necessarily rational, since the other two roots $r_\pm$ are simple), in which case E_1 is a rational conic with the rational point P_0^+, so stereographic projection makes $E_1(\mathbb{Q})$ dense in the entire real locus.

Step 4: Closing the induction with a fixed m-solution. Invoke $\mathcal{H}(m)$ *once* with threshold $M_1(B_m)$ to fix a single valid m-solution $(t_1, \ldots, t_L)$ with non-zero weights $(w_1, \ldots, w_L)$, nodal polynomial $Q(t)$, and $\delta_Q = \langle t^2 Q(t) \rangle_\mu \neq 0$. Define the constant

$$B_{m+1} := 1 + \max_{j \in \{3,4,5\}} \left| \frac{\langle t^j Q(t) \rangle_\mu}{\delta_Q} \right|,$$

which depends only on this fixed m-solution (and is completely independent of any future threshold M').

Now let an arbitrary threshold $M' > 0$ be given. By Step 3, rational points $x = t_{L-1} + \varepsilon \in E_1(\mathbb{Q})$ are dense on both sides of t_{L-1}. Applying Lemma 2.3(2)–(3) to the fixed m-solution $(t_1, \ldots, t_L)$, choose a sufficiently small rational ε of sign $\operatorname{sgn}(\delta_Q/(an_1))$ with $D_1(t_{L-1} + \varepsilon) = \square$ such that:

- $E_2(\varepsilon)(\mathbb{Q})$ is dense in $I_{\text{dip}}(\varepsilon)$;
- $R' = \frac{\delta_Q}{an_1\varepsilon} + O(1) > M'$;
- all L perturbed old weights satisfy $|w_i' - w_i| < \frac{1}{2}|w_i|$ (preserving all L signs);
- for every $y \in I_{\text{dip}}(\varepsilon)$ (note $y = t_L + O(\varepsilon)$), the shifted moments τ_j satisfy $|\tau_j/\tau_2| = |\langle t^j Q(t) \rangle_\mu / \delta_Q| + O(\varepsilon) \leq B_{m+1}$ for $j = 3, 4, 5$;
- all $L+2$ nodes $(t_1, \ldots, t_{L-2}, t_{L-1} + \varepsilon, y, t_{L+1}, t_{L+2})$ remain pairwise distinct (since $t_1, \ldots, t_L$ are pairwise distinct, $t_{L-1} + \varepsilon \to t_{L-1}$, $y \to t_L$, and $|t_{L+1}|, |t_{L+2}| = \Theta(R') \to \infty$ with $t_{L+2}/t_{L+1} \to r_2/r_1 > 1$).

Finally, pick a rational $y \in E_2(\varepsilon)(\mathbb{Q}) \cap I_{\text{dip}}(\varepsilon)$ in the non-empty open sub-interval where $\lambda' \in J$. By Lemma 2.3(3), the resulting $L+2 = 2m$ distinct rational nodes $(t_1, \ldots, t_{L-2}, t_{L-1} + \varepsilon, y, t_{L+1}, t_{L+2})$ satisfy conditions (1)–(3) of Lemma 2.1 with signature $(+(m+1), -(m-1))$, scale $R' > M'$, and $|\tau_j/\tau_2| \leq B_{m+1}$. This establishes $\mathcal{H}(m+1)$.

By induction, $\mathcal{H}(k)$ holds for every $k \geq 3$. Combined with $k = 2$ and Lemma 2.1, this completes the proof of Theorem 1.5. $\square$

3.3 Symbolic Verification and 250-Digit Real-Geometry Test

Our companion script `scripts/verify_general_k.py` performs two distinct checks:

1. **Exact symbolic verification (Part 1):** verifies in exact SymPy rational arithmetic the non-torsion check $j \cdot [P_0^+ - P_0^-] \neq \mathcal{O}$ $(1 \leq j \leq 12)$ on $E_1^{(3)}$, the universal dual-number identity $\psi_3(0) = 0$ and $\psi_3'(0) = 196608\, a\, \delta_Q^{10}\, n_1\, c_0^5$ of Lemma 2.3(2), the universal limits $U_1(\xi)$ and $U_2(r_1, \eta)$, and $\min_{1 \leq j \leq 12} |z^j - 1| = 0.457564\ldots$.
2. **250-digit real-geometry test (Part 2):** executes the *real* inductive dipole chain at 250-digit precision from $k = 2$ through $k = 8$ (Table 1). We emphasize that Table 1 tests only the *real* dipole-opening geometry, scaling ratios (R, λ), and signature preservation $(+k, -(k-2))$; it does *not* test rational realizability over $\mathbb{Q}$. Rational realizability is proved theoretically in Theorem 1.5 (via Mazur's Torsion Theorem and Kronecker density) and verified explicitly over $\mathbb{Q}$ for $k = 2, 3, 4$ (in Lean 4) and $k = 5$ (in exact SymPy rational arithmetic) in Section 4.

Table 1: 250-digit *real-geometry* test of the inductive dipole chain from $k = 2$ to $k = 8$ at $u = -4$ (`scripts/verify_general_k.py`, Part 2). This tests real dipole opening, scaling ratios, and signature preservation $(+k, -(k-2))$ (not rationality over $\mathbb{Q}$).

k	Target Bound	Signature	Scale R	λ	$\max_{0\le j<2k} \lvert\mathrm{err}_j\rvert$
3	$O(n^{-5.5})$	$(+3,-1)$	2.67×10^{3}	0.8403	1.76×10^{-238}
4	$O(n^{-7.5})$	$(+4,-2)$	2.03×10^{5}	0.8400	4.30×10^{-225}
5	$O(n^{-9.5})$	$(+5,-3)$	2.67×10^{7}	0.8400	1.13×10^{-207}
6	$O(n^{-11.5})$	$(+6,-4)$	5.38×10^{9}	0.8400	7.64×10^{-185}
7	$O(n^{-13.5})$	$(+7,-5)$	2.20×10^{12}	0.8400	3.97×10^{-157}
8	$O(n^{-15.5})$	$(+8,-6)$	9.03×10^{14}	0.8400	2.16×10^{-123}

4 Explicit Polynomial Families for $k = 2, 3, 4, 5$

4.1 Constant-Norm Family for $k = 2$ $(u = -4)$

Taking $(t_1, t_2) = (0, 6)$ and $(w_1, w_2) = (\frac{4}{3}, \frac{2}{3})$ at $u = -4$ with $W = 3, c = 2$ yields

$$a_1(m) = 16m^2, \qquad a_2(m) = 4m^2 - 24, \qquad b_{1,2}(m) = 9m^2 \pm 18m - 9.$$

Remarkably, the degree-4 algebraic norm

$$M(a_1, a_2, b_1, b_2) := \Big((a_1 + a_2 - b_1 - b_2)^2 - 4a_1a_2 - 4b_1b_2\Big)^2 - 64a_1a_2b_1b_2$$

evaluates identically to the *constant* $M(a_1(m), a_2(m), b_1(m), b_2(m)) \equiv 82944 = 2^{10} \cdot 3^4$ for every $m \in \mathbb{Z}$. Because all four conjugate factors in M satisfy clean elementary bounds for $m \ge 3$ (Section 7), this yields an immediate non-zero lower bound and the explicit upper bound $\Delta_2(m) \le 27m^{-7}$ without any Taylor series at all, while its exact asymptotic expansion is $\Delta_2(m) = -\frac{3}{2}m^{-7} - 15m^{-9} + O(m^{-11})$.

4.2 Compact Explicit Family for $k = 3$ $(u = 5)$: Proof of Theorem 1.2

Scanning small rational parameters u and t_1 followed by a single Fermat quartic step reveals a remarkably small-integer realization at $u = 5$, with nodes and weights

$$t = \left(-\frac{11}{4}, -\frac{7}{4}, -\frac{37}{28}, \frac{1}{36}\right), \qquad w = \left(\frac{71}{200}, \frac{125}{192}, -\frac{2401}{2040}, \frac{59049}{27200}\right)$$

(signature $(+3, -1)$). Clearing denominators with $W = 81600$ and $c = 10$ gives the six quadratic polynomials of Theorem 1.2.

To make the proof completely elementary and directly formalizable in Lean 4 without analytic Taylor remainder theory, we use pure polynomial squaring. Define the degree-6 polynomials

$$T_6(t) := 1 + \frac{1}{2}t - \frac{1}{8}t^2 + \frac{1}{16}t^3 - \frac{5}{128}t^4 + \frac{7}{256}t^5 - \frac{21}{1024}t^6,$$
$$Q_{\mathrm{pair}}(w) := 2 - \frac{1}{20}w - \frac{21}{1600}w^2 - \frac{261}{64000}w^3 - \frac{2921}{2048000}w^4 - \frac{221407}{409600000}w^5 - \frac{7096321}{32768000000}w^6.$$

Since $T_6(t)^2 - (1+t) = \frac{t^7}{1048576}(441t^5 - 1176t^4 + 2464t^3 - 4928t^2 + 10560t - 33792)$ and $\sqrt{1+t} + T_6(t) \ge \frac{3}{2}$ for $|t| \le \frac{1}{4}$, we obtain the purely algebraic enclosure

$$\left|\sqrt{1+t} - T_6(t)\right| \le \frac{1}{10}|t|^7 \qquad \left(|t| \le \frac{1}{4}\right),$$

and squaring $P(z) = \sqrt{1+z+z^2/5}+\sqrt{1-z+z^2/5}$ (using $P(z)^2 = 2+\frac{2}{5}z^2+2\sqrt{1-\frac{3}{5}z^2+\frac{1}{25}z^4}$) similarly yields $|P(z) - Q_{\text{pair}}(z^2)| \le \frac{1}{400}z^{14}$ for $0 \le z \le \frac{1}{10}$. Setting $z = 10/m$ and $w = z^2 = 100/m^2$, the exact polynomial identity

$$28968\,T_6\big(-\tfrac{11}{20}w\big) + 53125\,T_6\big(-\tfrac{7}{20}w\big) + 177147\,T_6\big(\tfrac{1}{180}w\big) - 96040\,T_6\big(-\tfrac{37}{140}w\big) - 81600\,Q_{\text{pair}}(w) = -\frac{187}{1792}\,w^6$$

annihilates all powers $w^0, \dots, w^5$ identically. For every $m \ge 1000$ ($w \le 10^{-4}$), the weighted $O(w^7)$ remainders sum to at most $300w^7 \le 0.03w^6 < \frac{1}{2}\cdot\frac{187}{1792}w^6$, proving $0 < |\Delta_3(m)| \le 1.6 \times 10^{11} m^{-11}$. Choosing $m = \lfloor\sqrt{n/31381100000}\rfloor$ for $n \ge 31\,381\,100\,000\,000\,000$ gives $r(n,3) \le 10^{70}/(n^5\sqrt{n})$.

4.3 Compact Explicit Family for $k = 4$ ($u = 5$): Proof of Theorem 1.3

Starting from the tiny 3-node prefix $(t_1, t_2, t_3) = (-\frac{11}{4}, -\frac{7}{4}, \frac{1}{8})$ at $u = 5$ (where t_1, t_2 are inherited from our $k = 3$ family and $t_3 = \frac{1}{8}$ makes $D_1(t_3)$ a rational square), a *single* Fermat quartic step on $E_2(t_3)$ yields six remarkably compact rational nodes (all ≤ 32 bits, Table 2) with exact signature $(+4, -2)$, weight denominators of at most 177 bits, common denominator W of 362 bits (109 decimal digits), and minimal integer scaling $c = 10$ (the same $c = 10$ as for $k = 3$).

Table 2: Compact exact rational $k = 4$ solution at $u = 5$, verified in exact rational arithmetic (`scripts/verify_k4_family.py`) and completely formalized in Lean 4.36.0 (`K4UpperBound.lean`). Moments $0 \dots 7$ vanish identically; the normalized w^8 residual is $-\frac{161866452303987151320657971}{898296045741140423812495441920000} \approx -1.8019 \times 10^{-8}$.

i	Exact node t_i	bits(t_i)	w_i (approx.)	Sign	bits(w_i)
1	$-11/4$	4/3	+0.179867	+	81/83
2	$-7/4$	3/3	−0.294622	−	81/83
3	$1/8$	1/4	+0.669416	+	88/88
4	$-1950401/4041576$	21/22	−1.596018	−	154/154
5	$-2304476651/923949684$	32/30	+0.397480	+	174/175
6	$-182532769/1258501356$	28/31	+2.643877	+	177/176

Just as for $k = 3$, the entire proof of Theorem 1.3 reduces to elementary degree-8 polynomial squaring and exact rational arithmetic, with zero calculus. Using the degree-8 Maclaurin polynomial $T_8(t) = T_6(t) + \frac{33}{2048}t^7 - \frac{429}{32768}t^8$ and the degree-8 conjugate-pair polynomial $Q_{\text{pair},8}(w) = Q_{\text{pair}}(w) - \frac{118346893}{1310720000000}w^7 - \frac{16266193469}{419430400000000}w^8$, squaring yields the purely algebraic enclosures

$$\big|\sqrt{1+t} - T_8(t)\big| \le \frac{1}{50}|t|^9 \quad \left(|t| \le \frac{1}{4}\right), \qquad \big|P(z) - Q_{\text{pair},8}(z^2)\big| \le \frac{1}{3000}z^{18} \quad \left(0 \le z \le \frac{1}{10}\right)$$

(`sqrt_one_add_approx8` and `k4_pair_approx` in Lean 4). Setting $z = 10/m$ and $w = 100/m^2$, the exact polynomial identity (`k4_exact_moment_cancellation`)

$$\sum_{i=1}^{6} w_i T_8\left(\frac{t_i}{5}w\right) - Q_{\text{pair},8}(w) = -\frac{161866452303987151320657971}{898296045741140423812495441920000}\,w^8$$

annihilates all powers $w^0, \dots, w^7$ identically. For every $m \ge 10^6$ ($w \le 10^{-10}$), the $O(w^9)$ remainder is bounded by $\frac{1}{2}w^9 \le 10^{-10}w^8 \ll 1.8 \times 10^{-8}w^8$, proving $0 < |\Delta_4(m)| \le 10^{120}m^{-15}$ (`k4_upper_bound_family`) and $r(n,4) \le 10^{1780}/(n^7\sqrt{n})$ for all $n \ge 10^{232}$ (`k4_upper_bound`).

Remark 4.1. An earlier draft of this paper constructed a $k = 4$ family at $u = 1600/379$ via four iterated Fermat steps, yielding weights of 33,428 bits. The $u = 5$ witness in Table 2 reduces weight bit-length by 188× (and node bit-length from 4991 to 32 bits), making direct machine-checked verification in Lean 4.36.0 feasible in seconds.

4.4 Explicit Rational Family for $k = 5$ $(u = 5)$

Proposition 4.2 (Explicit $k = 5$ Rational Family Achieving $O(n^{-19/2})$)**.** *At $u = 5$, starting from the four compact $k = 4$ nodes $(-\frac{11}{4}, -\frac{7}{4}, \frac{1}{8}, -\frac{2304476651}{923949684})$, one Fermat tangent step on E_1 from the known rational point $t_4 = -\frac{1950401}{4041576}$ (whose evaluation $D_1(t_4)$ is an exact rational square by Lemma 2.2(2)) followed by one Fermat tangent step on $E_2(t_5)$ from infinity produces eight distinct rational nodes $t_1, \dots, t_8 \in \mathbb{Q}$ ($\leq$ 1359 bits) and exact rational weights $w_1, \dots, w_8 \in \mathbb{Q}$ ($\leq$ 11792 bits) of signature $(+5, -3)$ satisfying $\sum_{i=1}^{8} w_i t_i^j = \mu_j(5)$ for $j = 0, \dots, 9$ and $\sum_{i=1}^{8} w_i t_i^{10} - \mu_{10}(5) \approx 0.351783 \neq 0$ (Table 3; verified in exact SymPy rational arithmetic in `scripts/verify_k5_family.py`). By Lemma 2.1, this gives an explicit polynomial family proving $r(n, 5) = O(n^{-19/2})$, improving Qian and Wang's $r(n, 5) = O(n^{-17/2})$ by a full factor of n.*

Table 3: Exact rational $k = 5$ solution at $u = 5$ verified in exact SymPy rational arithmetic (`scripts/verify_k5_family.py`). Moments $0 \dots 9$ vanish identically; moment 10 residual $\approx 3.5178 \times 10^{-1} \neq 0$.

i	t_i (approx.)	bits(t_i) (num/den)	w_i (approx.)	Sign	bits(w_i) (num/den)
1	−2.750000	4/3	+0.1262	+	4069/4072
2	−1.750000	3/3	+0.5701	+	4066/4066
3	+0.125000	1/4	+0.2787	+	4071/4073
4	−2.494158	32/30	+0.6243	+	4162/4163
5	−1.402947	160/160	−0.6092	−	4827/4828
6	−0.050996	1163/1167	+2.4558	+	10821/10820
7	−2.118670	1359/1358	−0.5704	−	11776/11777
8	−0.490044	1358/1359	−0.8755	−	11791/11792

5 Sharp Effective Lower Bounds and Exhaustive Search Records

5.1 Proof of Theorem 1.4(a): Sharp $k = 2$ Lower Bound

Let $1 \leq a_1, a_2, b_1, b_2 \leq n$ with $\Delta := |\sqrt{a_1} + \sqrt{a_2} - \sqrt{b_1} - \sqrt{b_2}| > 0$. Setting $x_i = \sqrt{a_i}$, $y_i = \sqrt{b_i}$, the integer norm

$$M := \Big((a_1 + a_2 - b_1 - b_2)^2 - 4a_1a_2 - 4b_1b_2\Big)^2 - 64a_1a_2b_1b_2 \in \mathbb{Z}$$

satisfies the exact algebraic factorization

$$M = \Big((x_1{+}x_2)^2{-}(y_1{+}y_2)^2\Big)\Big((x_1{+}x_2)^2{-}(y_1{-}y_2)^2\Big)\Big((x_1{-}x_2)^2{-}(y_1{+}y_2)^2\Big)\Big((x_1{-}x_2)^2{-}(y_1{-}y_2)^2\Big). \tag{8}$$

If $M = 0$, one of the last three factors vanishes; in each case, an elementary check shows $|(x_1 + x_2)^2 - (y_1 + y_2)^2| \geq 2$, giving $\Delta \geq \frac{2}{4\sqrt{n}} = \frac{1}{2\sqrt{n}} \geq \frac{1}{4n^3\sqrt{n}}$.

If $M \neq 0$, then $|M| \geq 1$. Suppose for contradiction that $\Delta < \frac{1}{4n^3\sqrt{n}}$ (note $n \geq 2$ since $\Delta > 0$). Rescaling to $u_i = x_i/\sqrt{n}, v_i = y_i/\sqrt{n} \in (0, 1]$ with $S_1 = u_1 + u_2$, $S_2 = v_1 + v_2$, $S = \max(S_1, S_2) \leq 2$, $d_a = |u_1 - u_2|$, $d_b = |v_1 - v_2|$, we have $|S_1 - S_2| = \Delta/\sqrt{n} < \frac{1}{4n^4} \leq \frac{1}{64}$, and (8) gives

$$1 \leq |M| = \Delta \cdot n^{7/2} \cdot \underbrace{(S_1 + S_2)\left|S_1^2 - d_b^2\right|\left|d_a^2 - S_2^2\right|\left|d_a^2 - d_b^2\right|}_{=:\,\Phi(u_1,u_2,v_1,v_2)}.$$

When $S_1 = S_2 = S \in [1, 2]$, using $d_a, d_b \leq 2 - S$ and $D := \max(d_a^2, d_b^2) \leq (2 - S)^2$, we obtain the exact sharp bound

$$\Phi \leq 2S^3(S^2 - D)D \leq 2S^3\big(S^2 - (2 - S)^2\big)(2 - S)^2 = 8S^3(S - 1)(2 - S)^2 \leq \frac{27}{8},$$

since $\frac{27}{8} - 8S^3(S-1)(2-S)^2 = \frac{1}{8}(2S-3)^2\big(16S^3(2-S) + 4S^2 + 4S + 3\big) \geq 0$, with equality uniquely at $S = \frac{3}{2}$ ($u = (1, \frac{1}{2})$, $v = (\frac{3}{4}, \frac{3}{4})$). Including the perturbation $|S_1 - S_2| \leq \frac{1}{64}$ (valid for all $n \geq 2$) replaces $(2-S)$ by $(2 - S + \frac{1}{64})$, and splitting into $S \leq \frac{21}{20}$, $\frac{21}{20} < S \leq \frac{5}{4}$ (AM–GM: $(S^2 - D)D \leq S^4/4$), and $\frac{5}{4} < S \leq 2$ (monotonicity in $D \leq (2 - S + \frac{1}{64})^2 \leq S^2/2$) yields $\Phi \leq 4$ unconditionally for every $n \geq 2$, contradicting $1 \leq \Delta n^{7/2}\Phi < \frac{1}{4} \cdot 4 = 1$. For large n, $|S_1 - S_2| = O(n^{-4})$ gives $\Phi \leq \frac{27}{8} + O(n^{-4})$ and hence $r(n,2) \geq (\frac{8}{27} - O(n^{-4}))n^{-7/2}$. □

Remark 5.1 (Numerical Lower-Bound Constant for $k = 3$). For $k = 3$, the norm of $A^2 - B^2$ (where $A = \sqrt{a_1} + \sqrt{a_2} + \sqrt{a_3}$ and $B = \sqrt{b_1} + \sqrt{b_2} + \sqrt{b_3}$) is an integer equal to the product of 16 sign conjugates of $(A^2 - B^2)$. Numerical global optimization over the normalized simplex $[0,1]^6$ with $S_1 = S_2$ indicates that the product of the remaining 15 conjugate factors (times $A + B$) is maximized at the symmetric configuration $u = (s, s, s)$, $v = (3s - 2, 1, 1)$ with value $\approx 5979.6\, n^{31/2}$. Assuming this numerical maximum is global, it yields an empirical separation floor $\approx 1.67 \times 10^{-4} n^{-31/2}$—a factor of 2.2×10^{20} sharper than the Burnikel–Fleischer–Mehlhorn–Schirra constant $6^{-31} n^{-31/2}$. Unlike Theorem 1.4(a), this $k = 3$ constant is computed numerically and is not yet formally proved.

5.2 Exhaustive Search Records

Using an exact Rust hunter (combining Besicovitch's linear-independence criterion for zero testing with 256-bit arithmetic), we computed exact values of $r(n,2)$ up to $N = 4000$ (0.40 s) and $r(n,3)$ up to $N = 350$ (7.2×10^6 triples in 0.27 s). Table 4 highlights the tightest observed instances. Notice that for $k = 2$, the tightest instance $(446, 1152)$ vs. $(514, 1049)$ has $\Delta \cdot n^{3.5} = 0.799351$ (already within 2.7× of our exact asymptotic floor $\frac{8}{27} \approx 0.2963$), and for $k = 3$ the tightest instance at $n = 222$ already reaches $-\log(\Delta)/\log(n) = 5.2498$.

Table 4: Selected exact minimal separations from exhaustive Rust search ($k = 2$ up to $N = 4000$; $k = 3$ up to $N = 350$).

k	n	$(a_1, \ldots, a_k)$ vs. $(b_1, \ldots, b_k)$	Δ	$-\frac{\log \Delta}{\log n}$	$\Delta \cdot n^{2k-1/2}$
2	100	$(28, 82)$ vs. $(33, 74)$	1.5331×10^{-7}	3.407	1.533
2	990	$(86, 990)$ vs. $(165, 778)$	2.7585×10^{-11}	3.524	0.842
2	1152	$(446, 1152)$ vs. $(514, 1049)$	1.5405×10^{-11}	3.532	0.799
3	30	$(14, 15, 16)$ vs. $(6, 21, 21)$	3.9971×10^{-7}	4.332	53.201
3	120	$(36, 39, 115)$ vs. $(38, 43, 105)$	6.8569×10^{-11}	4.888	18.691
3	222	$(85, 110, 214)$ vs. $(90, 99, 222)$	4.810×10^{-13}	5.250	3.865

6 The 7-Moment Diophantine Surface for $k = 3$ ($O(n^{-13/2})$)

It is natural to ask whether our quadratic ansatz can push one moment further at $k = 3$—annihilating *seven* moments ($m = 0, \ldots, 6$) with $L = 4$ pure terms plus one conjugate pair, which would give $r(n,3) = O(n^{-13/2})$ and refute the conjecture $r(n,3) = \Omega(n^{-6})$. Below we carefully distinguish between (i) the *proved algebraic properties* of this 7-moment surface (verified symbolically in `scripts/verify_seven_moment_barrier.py`), and (ii) our *empirical observation* from bounded-height modular sieving (which is not a non-existence theorem).

6.1 Proved Algebraic Collapse, Hankel Window, and p-Adic Constraint

Introducing the shifted coordinates $v := 1/u$ and $y_i := (t_i - 1)/u$ halves all degrees in u and eliminates all denominators from the 7-moment system. Writing the monic quartic $Q(y) = \prod_{i=1}^{4}(y - y_i) = y^4 + e_1 y^3 + e_2 y^2 + e_3 y + e_4$, the three Prony equations $\langle Q \rangle_{\tilde{\mu}} = \langle yQ \rangle_{\tilde{\mu}} = \langle y^2 Q \rangle_{\tilde{\mu}} = 0$

on the unique non-degenerate branch $v \neq \frac{1}{4}$ (verified symbolically in the companion script `verify_seven_moment_barrier.py`) collapse to the exact affine relations

$$v = \frac{168e_2 - 222e_1 + 247}{192},$$
$$E_3 : \ 7770e_1^2 - 5880e_1e_2 - 17381e_1 + 5040e_2 + 6720e_3 + 10426 = 0,$$
$$E_4 : \ 233100e_1^2 + 10080e_1e_2 - 671580e_1 - 141120e_2^2 + 111888e_2 + 1290240e_4 + 453947 = 0.$$

Exact symbolic algebra on this 2-dimensional surface S establishes:

1. **Exact hyperbolic $(+3,-1)$ window via the 4×4 Hankel determinant:** The 4×4 Hankel matrix $H_4(v) = (\tilde{\mu}_{i+j}(v))_{0\le i,j\le 3}$ satisfies $\det(H_4(v)) = w_1w_2w_3w_4\prod_{i<j}(y_i - y_j)^2$ on any 4-node realization, and evaluates identically to

$$\det(H_4(v)) = \frac{(4v-1)^3(420v-97)}{4704000}.$$

   Because signature $(+3,-1)$ requires $w_1w_2w_3w_4 < 0$, real 4-root solutions of signature $(+3,-1)$ exist *only* inside the open window $v \in \left(\frac{97}{420}, \frac{1}{4}\right)$, i.e., $u \in \left(4, \frac{420}{97}\right)$ (and real $(+3,-1)$ points do exist throughout this window).

2. **Exact p-adic denominator constraint ($42 \mid \mathrm{lcm}(\mathrm{denom}(y_i))$):** Every non-constant integer coefficient of E_4 is divisible by $42 = 2\cdot 3\cdot 7$, whereas its constant term satisfies $453947 \equiv 1 \pmod 2$, $2 \pmod 3$, and $4 \pmod 7$. Hence no rational point can be p-adically integral at $p \in \{2,3,7\}$, forcing $42 \mid \mathrm{lcm}(\mathrm{denom}(y_1),\dots,\mathrm{denom}(y_4))$. (Hensel lifting does succeed at $p = 2,3,5,7$ with p-adic denominators and over $\mathbb{F}_{11},\dots,\mathbb{F}_{23}$, so there is no local obstruction.)

3. **Genus-2 slices:** Natural 1-dimensional slices—such as the line $e_2 = \frac{90e_1-37}{120}$ (where $(y+\frac{1}{4})$ factors out of $Q(y)$ identically, leaving a cubic with squarefree degree-5 discriminant in e_1, hence a genus-2 hyperelliptic curve) and the biquadratic locus $Q(y) = (y^2+ay+b)(y^2+ay+d)$ (whose splitting condition is a sextic in a of genus 2)—have genus 2 and therefore admit only finitely many rational points by Faltings' Theorem. More generally, the Galois closure of the splitting cover $Q(y) = 0$ over (e_1, e_2) is fibered over $\mathbb{P}^1_u$ by curves of genus 13.

6.2 Empirical Observation: Modular Sieving Over 8.5×10^7 Candidates

We implemented four multi-prime modular sieves in Rust covering the hyperbolic window $v \in (\frac{97}{420}, \frac{1}{4})$, the two genus-2 slices, and the resultant elimination $\Phi(y_1,y_2,y_3) = 0$ (where $y_4 \in \mathbb{Q}$ is determined linearly/quadratically). Across 85 425 298 rational candidates of bounded height (Table 5), *zero* non-trivial rational points were found.

We stress that this zero-hit sieve is an *empirical observation*, not a theorem: it does not rule out high-height rational points on the 2-dimensional 7-moment surface S. Nevertheless, the sharp geometric transition between 6 moments (elliptic Fermat fibrations with Zariski-dense rational points, yielding Theorems 1.2–1.3 and 1.5) and 7 moments (a surface of general type, where the Bombieri–Lang conjecture predicts non-density) is heuristically consistent with the conjectured barrier $r(n,3) = \Omega(n^{-6})$.

7 Lean 4.36.0 Formalization, Verification Scope, and Axiom Audit

The Lean 4.36.0 + Mathlib library `SumOfSquareRoots` (Table 6) formally verifies our entire Tier 1 theory for $k = 2,3,4$ together with the universal algebraic building blocks of the general-k theory. All Lean proofs rely exclusively on elementary algebra, polynomial squaring, and exact rational arithmetic—with zero calculus, zero external numerical certificates, zero `sorry`, zero `admit`, and

Table 5: Empirical Rust modular sieves on the 7-moment $k = 3$ surface ($O(n^{-13/2})$): bounded-height search yielding zero non-trivial hits (not a non-existence proof).

Search Space	Parameters	Candidates	Non-trivial Hits
(u, t_1) in $(4, \frac{420}{97})$ (10-prime sieve)	$q_u \le 250,\ s_{t_1} \le 40$	18 469 480	0
Magic line $y_1 = -\frac{1}{4}$ + 2D (e_1, e_2) band	$q \le 8000;\ D \le 1200$	19 583 037	0
Biquadratic genus-2 slice $D_1(a) = \square$	$q \le 12000$	7 937 293	0
Resultant $\Phi(y_1, y_2, y_3) = 0$ (y_4 free)	$42 \mid D \le 504$; mixed $q \le 45$	39 435 488	0
Total		**85 425 298**	**0**

zero `native_decide`. Running `lake env lean check_axioms.lean` confirms that all 21 audited declarations depend *strictly* on the three standard axioms of classical Lean mathematics: `propext`, `Classical.choice`, and `Quot.sound`.

Formalization scope boundary. To keep the boundary between machine-checked and paper proofs unambiguous:

- **Machine-checked in Lean 4.36.0 + Mathlib:** Theorem 1.4(a)–(b) ($k = 2$ lower and upper bounds), Theorem 1.2 ($r(n, 3) = O(n^{-11/2})$), Theorem 1.3 ($r(n, 4) = O(n^{-15/2})$), and the algebraic core of Proposition 1.1, Lemma 2.2(1)–(2), Lemma 2.3(1), the universal $U_1(\xi)$ limit (6), the unconditional non-torsion of $z = (23 + 7i\sqrt{3})/26$, and the base $k = 2$ moment realization at $u = -4$.
- **Verified in exact SymPy rational arithmetic (outside Lean):** Proposition 4.2 ($k = 5$ explicit rational family, `scripts/verify_k5_family.py`), the non-torsion check $1 \le j \le 12$ on $E_1^{(3)}$ and universal $\psi_3'(0)$ formula (`scripts/verify_general_k.py`, Part 1), and the 7-moment $k = 3$ algebraic collapse, Hankel determinant $\det(H_4(v))$, mod-42 constraint, and magic-line genus-2 slice (`scripts/verify_seven_moment_barrier.py`).
- **Proved on paper (not formalized in Lean):** the arithmetic-geometric and analytic steps of Theorem 1.5 for arbitrary $k \ge 6$—specifically, Mazur's Torsion Theorem, Kronecker density on $E(\mathbb{R})^\circ \cong S^1$, convergence of real elliptic logarithms to nodal circle angles, and the inductive dipole-opening perturbation in Sections 2–3.

References

[1] M. R. Garey, R. L. Graham, and D. S. Johnson, *Some NP-complete geometric problems*, in Proc. 8th Annual ACM Symposium on Theory of Computing (STOC), 1976, pp. 10–22.

[2] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. Inst. Hautes Études Sci. **47** (1977), 33–186.

[3] C. Burnikel, R. Fleischer, K. Mehlhorn, and S. Schirra, *A strong and easily computable separation bound for arithmetic expressions involving radicals*, Algorithmica **27** (2000), no. 1, 87–99.

[4] J. Qian and C. A. Wang, *How much precision is needed to compare two sums of square roots of integers?*, Inform. Process. Lett. **100** (2006), no. 5, 194–198.

[5] J. Qian and C. A. Wang, *An optimal bound for sum of square roots of special type of integers*, in Proc. 6th International Symposium on Operations Research and Its Applications (ISORA '06), Lecture Notes in Operations Research **6** (2006), 131–138.

Table 6: Module map of the Lean 4.36.0 library `SumOfSquareRoots` (all 21 audited declarations depend strictly on `[propext, Classical.choice, Quot.sound]`).

Module	Lines	Key Verified Declarations
`Basic.lean`	192	`diff2`, `diff3`, `diff4`, `T6`, `T8`, `sqrt_one_add_approx` ($\leq \frac{1}{10}\|t\|^7$), `sqrt_one_add_approx8` ($\leq \frac{1}{50}\|t\|^9$)
`K2Bounds.lean`	722	`k2_norm_identity`, `k2_exact_constant_bound` (sharp $\frac{27}{8}$), `k2_lower_bound` (Theorem 1.4a), `k2_upper_bound_family`, `k2_upper_bound` (Theorem 1.4b)
`K3UpperBound.lean`	408	`Qpair`, `k3_exact_moment_cancellation` ($-\frac{187}{1792}w^6$), `k3_pair_approx`, `k3_upper_bound_family`, `k3_upper_bound` (Theorem 1.2)
`K4UpperBound.lean`	654	`Qpair8`, `k4_exact_moment_cancellation`, `k4_pair_approx`, `k4_upper_bound_family`, `k4_upper_bound` (Theorem 1.3: $r(n,4) \leq 10^{1780}/(n^7\sqrt{n})$)
`UniversalLemmas.lean`	250	`vandermonde_wall_moments`, `leading_coeff_identity`, `automatic_rational_square`, `universal_D2_zero`, `universal_U1_limit`, `z_center_norm_sq`, `z_center_not_root_of_unity`, `base_k2_moments`
`SumOfSquareRoots.lean`	5	Root aggregator module
Total library	**2,231**	21 audited declarations (plus 23 lines in `check_axioms.lean`)

[6] E. Allender, P. Bürgisser, J. Kjeldgaard-Pedersen, and P. B. Miltersen, *On the complexity of numerical analysis*, SIAM J. Comput. **38** (2009), no. 5, 1987–2006.

[7] Q. Cheng, X. Meng, C. Sun, and J. Chen, *Bounding the sum of square roots via lattice reduction*, Math. Comp. **79** (2010), no. 270, 1109–1122.

[8] Q. Cheng and Y.-H. Li, *On the minimum gap between sums of square roots of small integers*, Theoret. Comput. Sci. **412** (2011), no. 39, 5458–5465.

[9] E. D. Demaine, J. S. B. Mitchell, and J. O'Rourke, *The Open Problems Project, Problem 33: Sum of Square Roots*, `https://topp.openproblem.net/p33`.

[10] F. Eisenbrand, M. Haeberle, and N. Singer, *An improved bound for the sum-of-square-roots problem via the Subspace Theorem*, in Proc. 40th International Symposium on Computational Geometry (SoCG 2024), LIPIcs **293**, 2024.