SHARP LOWER BOUNDS, UNIVERSAL PARSEVAL SEPARATION, AND STRUCTURAL EXPONENT-BREAKING FOR THE SUM-OF-SQUARE-ROOTS PROBLEM ($k = 3$ AND GENERAL k)

IVAN BESEVIC

hexagon:2611.01275v1

Date: November 28, 2026.

2020 *Mathematics Subject Classification.* Primary 11J25, 11Y16; Secondary 68Q25, 68V20.

Key words and phrases. Sum-of-Square-Roots problem, separation bounds, conjugate product optimization, Parseval identity, 2-adic norm divisibility, Galois subfield collapse, Lean 4 formalization.

ORCID: 0009-0004-4124-1465. All theorems in this paper are machine-checked in Lean 4.36.0 with zero `sorry`, zero `admit`, and zero `native_decide` (relying strictly on the standard axioms `propext`, `Classical.choice`, and `Quot.sound`).

ABSTRACT. Let $r(n,k)$ denote the minimum positive value of $\left|\sum_{i=1}^{k}\sqrt{a_i}-\sum_{j=1}^{k}\sqrt{b_j}\right|$ over integers $1\le a_i,b_j\le n$. We establish four lower-bound theorems (together with their universal even-parity 2-adic refinements) for $r(n,3)$ and general $r(n,k)$, all completely formalized in Lean 4.36.0 with zero axioms beyond the standard kernel foundations:

(1) **Exact $k=3$ Global Extremum, All-n Floor, and Even-Parity Boost.** We resolve the exact global maximum of the normalized 31-conjugate product $\Phi_3(u,v)$ on the equal-sum cube $\{u,v\in[0,1]^3:\sum u_i=\sum v_j\}$, proving $\Phi_3(u,v)\le\Phi_3(s^*)\in(5979.83,5980)$ (attained uniquely at $u=(s^*,s^*,s^*)$, $v=(3s^*-2,1,1)$, where $s^*\in(0.7809236,0.7809237)$ is the unique root in $(2/3,1)$ of $504s^5-1920s^4+2491s^3-1409s^2+344s-28=0$). Combining this with a perturbation transfer and complete Hamming-distance degeneracy elimination yields the unconditional all-n lower bound $r(n,3)\ge\frac{1}{5981}n^{-31/2}$ for every $n\ge1$ (more than 2.21×10^{20} times sharper than the classical half-norm / BFMS bound $6^{-31}n^{-31/2}$) together with the sharp asymptotic floor $r(n,3)\ge(\Phi_3(s^*)+2.2\times10^7n^{-16})^{-1}n^{-31/2}$ for all $n\ge3$. Moreover, whenever $a_1+a_2+a_3\equiv b_1+b_2+b_3 \pmod 2$, we prove that $2^{16}=65\,536$ divides the degree-16 algebraic norm M_3, boosting the floor to $|\Delta|\ge\frac{65536}{5981}n^{-31/2}>10.95\,n^{-31/2}$ ($1.45\times10^{25}\times$ sharper than $6^{-31}n^{-31/2}$).

(2) **Universal All-k Parseval–AM–GM Bound and $2^{2^{2k-2}}$-Parity Boost.** Using the exact Walsh–Parseval identity over all 2^{2k-1} conjugates, pure-polynomial half-norm integrality, and strong-induction Hamming halving for degenerate instances, we prove that for every $k\ge2$ and every $n\ge1$,

$$r(n,k)\ \ge\ \frac{1}{\sqrt{e}}\,(2kn)^{-(2^{2k-2}-1/2)}\ =\ \frac{1}{\sqrt{e}}\,(2k)^{-(2^{2k-2}-1/2)}\,n^{-(2^{2k-2}-1/2)},$$

which halves the exponent of $2k$ in the classical half-norm / BFMS bound $(2k)^{-(2^{2k-1}-1)}n^{-(2^{2k-2}-1/2)}$, yielding a doubly-exponential improvement factor of $(2k)^{2^{2k-2}-1/2}/\sqrt{e}$ ($\approx 6.99\times10^{11}\times$ at $k=3$ and $1.35\times10^{57}\times$ at $k=4$). Furthermore, via a universal 2-adic integrality theorem, whenever $\sum_{i=1}^{k}a_i\equiv\sum_{j=1}^{k}b_j \pmod 2$, the integer $2^{2^{2k-2}}$ divides the half-norm, cancelling the factor of 2 inside $2k$ to give

$$|\Delta|\ \ge\ \sqrt{\frac{2}{e}}\,(kn)^{-(2^{2k-2}-1/2)},$$

beating the classical half-norm constant by $\sqrt{2/e}\,(4k)^{2^{2k-2}-1/2}$.

(3) **Clustered / Spread-L Exponent-Breaking Theorem.** When all six integers lie in a window $[m,m+L]$ ($m\ge1$, $L\ge1$, $n=m+L$), we prove that every one of the 9 inner conjugate factors satisfies $|A_i^2-B_j^2|\le6L$ unconditionally, yielding $|\Delta|\ge3^{-12}\cdot6^{-10}\cdot n^{-13/2}L^{-9}$ (and $|\Delta|\ge64\cdot3^{-22}\cdot n^{-13/2}L^{-9}$ under even parity). This breaks the generic $-31/2$ exponent by 9 full powers of n at bounded spread $L=O(1)$ ($\Omega(n^{-13/2})$) and by 4.5 powers at $L=O(\sqrt{n})$ ($\Omega(n^{-11})$). For general $k\ge2$, we prove the exact Vandermonde count of collapsed inner factors, $N_{\text{small}}(k)=\frac12\binom{2k}{k}-\mathbf{1}_{2|k}\frac14\binom{k}{k/2}^2-1$.

(4) **Universal All-k Galois Exponent-Halving Theorem.** For every $k\ge2$, whenever any non-empty even-cardinality subset S of the $2k$ integers has square product $\prod_{x\in S}c_x=d^2$, we prove via elementary $\mathbb{Z}[X]$ polynomial splitting (zero Galois theory) that the half-norm factors into two integer quarter-norms of degree 2^{2k-2}, halving the algebraic degree and reducing the separation exponent of n from $-(2^{2k-2}-\frac12)$ to $-(2^{2k-3}-\frac12)$ (for $k=3$: from $-31/2$ to $-15/2$). Under even parity, $2^{2^{2k-3}}$ divides the quarter-norm ($256\times$ boost at $k=3$), sharpening the base constant from $(2k,2k+2)$ to $(k,k+1)$ with prefactor $\sqrt{2/e}$.

1. INTRODUCTION

The *Sum-of-Square-Roots* (SSR) problem asks to determine the sign of

$$\Delta\ =\ \sum_{i=1}^{k}\sqrt{a_i}-\sum_{j=1}^{k}\sqrt{b_j},\qquad a_i,b_j\in\{1,2,\dots,n\}.$$

Despite its elementary statement, deciding the sign of Δ in polynomial time remains one of the most celebrated open problems in computational geometry and numerical complexity, standing at the core of Euclidean shortest paths, Delaunay triangulations, and the complexity class

PosSLP [4, 1, 3, 5]. A central quantitative measure of the precision required to resolve the sign of Δ is the *separation function*

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

On the upper-bound side, Qian and Wang [5] constructed instances showing $r(n,k) = O(n^{-2k+3/2})$, which was recently improved to $r(n,k) = O(n^{-2k+1/2})$ for every $k \ge 2$ in [2] (where also the sharp $k=2$ lower bounds $r(n,2) \ge \frac{1}{4}n^{-7/2}$ and $r(n,2) \ge \frac{8}{27}n^{-7/2}$ for $n \ge 15$ were formalized in Lean 4). On the lower-bound side, applying the root-separation framework of Burnikel, Fleischer, Mehlhorn, and Schirra (BFMS [3]) to the degree-2^{2k-1} half-norm of Δ (exploiting the $\pm\Delta$ sign symmetry, which already halves the raw 2^{2k} DAG degree) and bounding each of the $2^{2k-1}-1$ companion conjugates pointwise by $2k\sqrt{n}$ gives the classical half-norm / BFMS bound

$$r(n,k) \;\ge\; (2k\sqrt{n})^{-(2^{2k-1}-1)} \;=\; (2k)^{-(2^{2k-1}-1)}\, n^{-(2^{2k-2}-1/2)}, \tag{1}$$

which evaluates to $4^{-7}n^{-7/2}$ at $k=2$,

$$r(n,3) \;\ge\; 6^{-31}\, n^{-31/2} \;\approx\; 7.54\times 10^{-25}\, n^{-31/2}$$

at $k=3$, and $8^{-127}n^{-127/2}$ at $k=4$. In Remark 5.1 of [2], a numerical exploration of the 31-conjugate product Φ_3 suggested that the true $k=3$ root-separation constant should be on the order of $1.67\times 10^{-4}n^{-31/2}$, an improvement of twenty orders of magnitude over (1), but left both the global optimization of Φ_3 and the handling of degenerate ($M_3=0$) and near-equal-sum perturbations completely open.

Contributions. In this paper we completely settle the $k=3$ conjugate-product optimization problem and establish three general-k structural theorems (with universal even-parity 2-adic boosts) that systematically sharpen both the leading constant and, in structured regimes, the separation exponent of $r(n,k)$:

- **Theorem 3.2 & Theorem 3.3 (Exact $k=3$ Extremum, All-n Floor, and Parity Boost):** We determine the exact global maximum of the 31-conjugate functional $\Phi_3(u,v)$ on the equal-sum cube $[0,1]^6$ via an algebraic $t_i = u_i(S-u_i)$ collapse, a pure Lean-kernel 1,047-leaf exact-integer interval tree for $S \in [396/256, 2]$, and pure AM–GM run-collapse reducing $S \in [2,3]$ to an explicit 1D quintic critical point $s^* \in (0.7809236, 0.7809237)$ with $\Phi_3(s^*) \approx 5979.85945798 < 5980$. This yields $r(n,3) \ge \frac{1}{5981}n^{-31/2}$ for *all* $n \ge 1$ ($> 2.21\times 10^{20}\times$ over (1)), the exact asymptotic floor $(\Phi_3(s^*) + 2.2\times 10^7 n^{-16})^{-1}n^{-31/2}$ for $n \ge 3$, and a $2^{16} = 65\,536$-fold divisibility boost whenever $a_1+a_2+a_3 \equiv b_1+b_2+b_3 \pmod 2$ ($> 10.95\, n^{-31/2}$, i.e., $1.45\times 10^{25}\times$ over (1)).
- **Theorem 4.2 & Theorem 4.4 (Universal All-k Parseval–AM–GM Bound and $2^{2^{2k-2}}$-Parity Boost):** Replacing the crude pointwise conjugate bound $|\Delta_\sigma| \le 2k\sqrt{n}$ by the exact Parseval identity $\sum_\sigma \Delta_\sigma^2 = 2^{2k-1}\sum(a_i+b_j)$ and AM–GM cuts the constant exponent of $2k$ in (1) in half (from $2^{2k-1}-1$ to $2^{2k-2}-\frac{1}{2}$) for *every* $k \ge 2$, beating (1) by $(2k)^{2^{2k-2}-1/2}/\sqrt{e}$ ($\approx 6.99\times 10^{11}\times$ at $k=3$ and $1.35\times 10^{57}\times$ at $k=4$). Moreover, whenever $\sum a_i \equiv \sum b_j \pmod 2$, our universal 2-adic divisibility theorem shows $2^{2^{2k-2}} \mid N_{\text{half}}$, sharpening the bound to $|\Delta| \ge \sqrt{2/e}\,(kn)^{-(2^{2k-2}-1/2)}$ and boosting the improvement over (1) to $\sqrt{2/e}\,(4k)^{2^{2k-2}-1/2}$ ($4.58\times 10^{16}\times$ at $k=3$, $2.48\times 10^{76}\times$ at $k=4$).
- **Theorem 5.1, Corollary 5.2, & Proposition 5.3 (Spread-L Exponent-Breaking):** When $a_i, b_j \in [m, m+L]$ with $n = m+L$, all 9 inner factors of M_3 collapse from $O(n)$ to $|A_i^2 - B_j^2| \le 6L$ unconditionally for all $m, L \ge 1$, breaking the $-31/2$ exponent to $\Omega(n^{-13/2}L^{-9})$ (saving 9 full powers of n at $L = O(1)$, with an additional 2^{16}-fold

boost under even parity). We also prove the exact general-k collapsed-factor count $N_{\text{small}}(k) = \frac{1}{2}\binom{2k}{k} - \mathbf{1}_{2|k}\frac{1}{4}\binom{k}{k/2}^2 - 1$.

- **Theorem 6.2 & Corollary 6.3 (Universal All-k Galois Exponent-Halving and Parity Boost):** Whenever any non-empty *even-cardinality* subset S of the $2k$ integers has a square product $\prod_{x\in S} c_x = d^2$, the half-norm splits into two integer quarter-norms of degree 2^{2k-2}, halving the algebraic degree and reducing the worst-case separation exponent of n from $-(2^{2k-2}-\frac{1}{2})$ to $-(2^{2k-3}-\frac{1}{2})$ for every $k \geq 2$ (for $k = 3$: from $-31/2$ to $-15/2$). Under even parity, $2^{2^{2k-3}}$ divides the quarter-norm, boosting the constant by an additional $2^{2^{2k-3}}$ ($256\times$ at $k = 3$). We also note why odd-size square subsets do not halve the exponent (because $-I$ no longer lies in the Galois group).

Remark 1.1 (Scope and Comparison with Upper Bounds)**.** The unconditional bounds of Theorems 3.3 and 4.2 retain the classical half-norm exponent $-(2^{2k-2}-\frac{1}{2})$ ($-31/2$ at $k = 3$): their gain over (1) lies in sharp (and at $k = 3$, asymptotically exact for the norm method) leading constants rather than an unconditional exponent improvement. A wide gap remains between the generic norm exponent $-(2^{2k-2}-\frac{1}{2})$ and the constructive upper bound $r(n,k) = O(n^{-2k+1/2})$ ($O(n^{-11/2})$ at $k = 3$) of [2]. Theorems 5.1 and 6.2 strictly break the generic exponent in structured regimes (clustered inputs and multiplicative square relations), though neither structured exponent is known to be optimal.

Every theorem, lemma, and numerical bound in this paper has been formally verified in Lean 4.36.0 (`SSRK3`) with zero `sorry`, zero `admit`, and zero `native_decide`; Table 2 in Section 7 maps every result to its verified Lean identifier.

2. Degree-16 Algebraic Norm, Even-Parity Boost, and Degeneracy Elimination

For integers $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{N}$, define the four signed triples

$$A_0 = \sqrt{a_1} + \sqrt{a_2} + \sqrt{a_3}, \qquad A_1 = \sqrt{a_1} + \sqrt{a_2} - \sqrt{a_3},$$
$$A_2 = \sqrt{a_1} - \sqrt{a_2} + \sqrt{a_3}, \qquad A_3 = -\sqrt{a_1} + \sqrt{a_2} + \sqrt{a_3},$$

and analogously B_0, B_1, B_2, B_3 for (b_1, b_2, b_3), with $\Delta = A_0 - B_0$. The degree-16 algebraic half-norm is

$$M_3(a,b) := \prod_{i=0}^{3}\prod_{j=0}^{3}(A_i^2 - B_j^2). \tag{2}$$

Lemma 2.1 (Integrality and Even-Parity 2^{16}-Divisibility)**.** *For all $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{N}$:*

(1) $M_3(a,b) \in \mathbb{Z}$.
(2) *If $a_1 + a_2 + a_3 \equiv b_1 + b_2 + b_3 \pmod 2$, then $2^{16} = 65\,536$ divides $M_3(a,b)$.*

Proof. Set $s_a = a_1+a_2+a_3$, $q_a = a_1a_2+a_2a_3+a_3a_1$, $p_a = a_1a_2a_3$, and similarly (s_b, q_b, p_b). Direct algebraic expansion shows that A_0, A_1, A_2, A_3 are the four roots of the biquadratic polynomial

$$P_a(X) \;=\; \left(X^2 - s_a\right)^2 - 4q_a - 8\sqrt{p_a}\,X,$$

and hence

$$\prod_{i=0}^{3}(X - A_i^2) \;=\; \left((X - s_a)^2 - 4q_a\right)^2 - 64p_aX.$$

Setting $Y = X - s_a$ shifts the inner polynomial to $G_a(Y) = (Y^2 - 4q_a)^2 - 64p_a(Y + s_a) \in \mathbb{Z}[Y]$. Letting $d = s_b - s_a$, $t_j = B_j^2 - s_b$ satisfies the identical quartic equation $(t_j^2 - 4q_b)^2 = 64p_b(t_j + s_b)$ for $j = 0, 1, 2, 3$. Therefore

$$M_3(a,b) \;=\; \prod_{j=0}^{3} G_a(t_j + d),$$

which is a symmetric polynomial with integer coefficients in the roots t_0, t_1, t_2, t_3 of the monic integer quartic $(T^2 - 4q_b)^2 - 64p_b(T + s_b) = 0$. Expanding $G_a(t_j + d)$ in powers of t_j and reducing

via the elementary symmetric polynomials $e_1 = 0$, $e_2 = -8q_b$, $e_3 = 64p_b$, $e_4 = 16q_b^2 - 64p_b s_b$ produces an explicit integer formula for $M_3(a, b)$.

For part (2), observe that $e_1 = 0$, $2^2 \mid e_2$, $2^3 \mid e_3$, and $2^4 \mid e_4$, so each root t_j behaves with 2-adic valuation at least 1: substituting $t_j = 2w_j$ yields the monic integer quartic

$$w^4 - 2q_b w^2 - 8p_b w + (q_b^2 - 4p_b s_b) \;=\; 0,$$

whose roots w_0, w_1, w_2, w_3 are algebraic integers! When $s_a \equiv s_b \pmod 2$, write $d = s_b - s_a = 2k$ ($k \in \mathbb{Z}$). Then $t_j + d = 2(w_j + k)$, so every factor pulls out $2^4 = 16$:

$$\begin{aligned} G_a(t_j + d) \;&=\; \big(4(w_j + k)^2 - 4q_a\big)^2 - 64p_a\big(2(w_j + k) + s_a\big) \\ &=\; 16\Big[\big((w_j + k)^2 - q_a\big)^2 - 4p_a\big(2(w_j + k) + s_a\big)\Big]. \end{aligned}$$

Multiplying over $j = 0, 1, 2, 3$ yields $M_3(a, b) = 16^4 \prod_{j=0}^{3} H(w_j) = 65\,536 \cdot N$, where $N = \prod_{j=0}^{3} H(w_j) \in \mathbb{Z}$ since $H \in \mathbb{Z}[w]$ and $w_0, \ldots, w_3$ are the roots of a monic polynomial in $\mathbb{Z}[w]$. □

Remark 2.2. The 2^{16}-divisibility of Lemma 2.1(2) is sharp: for $(a_1, a_2, a_3) = (1, 2, 3)$ and $(b_1, b_2, b_3) = (1, 1, 2)$ (sums $6 \equiv 4 \pmod 2$), $M_3/65\,536$ is an odd integer.

Lemma 2.3 (Complete Degeneracy Elimination via Hamming-Distance Halving)**.** *Let* $1 \le a_i, b_j \le n$ *with* $\Delta = A_0 - B_0 \neq 0$. *If* $M_3(a, b) = 0$, *then*

$$|\Delta| \;\ge\; \frac{1}{2n\sqrt{n}}.$$

Proof. If $M_3(a, b) = 0$, then some factor $A_i^2 - B_j^2 = 0$, hence there exists a sign vector $\sigma \in \{\pm 1\}^6$ with $\sum_{r=1}^{6} \sigma_r \sqrt{c_r} = 0$, where $c = (a_1, a_2, a_3, b_1, b_2, b_3)$. Let $v = (+1, +1, +1, -1, -1, -1)$ so $\Delta = \sum_{r=1}^{6} v_r \sqrt{c_r} \neq 0$. Comparing v and σ on $\{1, \ldots, 6\}$, set $S_1 = \{r : v_r \neq \sigma_r\}$ and $S_2 = \{r : v_r = \sigma_r\}$. Then $|S_1| + |S_2| = 6$, and

$$\Delta \;=\; \Delta - 0 \;=\; 2\sum_{r \in S_1} v_r \sqrt{c_r}, \qquad \Delta \;=\; \Delta + 0 \;=\; 2\sum_{r \in S_2} v_r \sqrt{c_r}.$$

Choosing the smaller of S_1, S_2 yields a non-empty subset S of size $1 \le |S| \le 3$ with $|\Delta| = 2\big|\sum_{r \in S} v_r \sqrt{c_r}\big|$.

- If $|S| = 1$, $|\Delta| = 2\sqrt{c_r} \ge 2 \ge \frac{1}{2n\sqrt{n}}$.
- If $|S| = 2$, $|\Delta| = 2|\sqrt{x} \pm \sqrt{y}| \ge \frac{2|x-y|}{\sqrt{x}+\sqrt{y}} \ge \frac{1}{\sqrt{n}}$.
- If $|S| = 3$, multiplying $|\sqrt{x} + \sqrt{y} - \sqrt{z}|$ by the three other signed conjugates gives $|(x + y - z)^2 - 4xy| \ge 1$ (since $x, y, z \in \mathbb{N}$ and the expression is non-zero), while each of the three companion factors is bounded by $3\sqrt{n}$ (actually their product is $\le 4n\sqrt{n}$ since $|\sqrt{x} + \sqrt{y} + \sqrt{z}| \le 3\sqrt{n}$ and $|(\sqrt{x} - \sqrt{y})^2 - z| \le n$):

  $$|\sqrt{x} + \sqrt{y} - \sqrt{z}| \;=\; \frac{|(x + y - z)^2 - 4xy|}{(\sqrt{x} + \sqrt{y} + \sqrt{z})\,|z - (\sqrt{x} - \sqrt{y})^2|} \;\ge\; \frac{1}{3\sqrt{n} \cdot n},$$

  and since $|\Delta| = 2|\sqrt{x} + \sqrt{y} - \sqrt{z}|$ we obtain $|\Delta| \ge \frac{2}{3n\sqrt{n}} > \frac{1}{2n\sqrt{n}}$. □

3. Exact Global Maximum of Φ_3 and Sharp $k = 3$ Lower Bounds

On the equal-sum unit cube $\Omega = \{(u, v) \in [0, 1]^3 \times [0, 1]^3 : u_1 + u_2 + u_3 = v_1 + v_2 + v_3\}$, where $u_i = \sqrt{a_i/n}$ and $v_j = \sqrt{b_j/n}$, the product of all 31 remaining conjugate factors (together with $A_0 + B_0 = 2S$, where $S = u_1 + u_2 + u_3 = v_1 + v_2 + v_3$) is

$$\Phi_3(u, v) \;:=\; 2S \prod_{\substack{0 \le i,j \le 3 \\ (i,j) \neq (0,0)}} \big|A_i(u)^2 - B_j(v)^2\big|.$$

Here $A_0(u) = u_1 + u_2 + u_3$, $A_1(u) = u_1 + u_2 - u_3$, etc. Our key structural observation is that Φ_3 collapses identically into the quadratic coordinates $t_i = u_i(S - u_i)$ and $r_j = v_j(S - v_j)$.

Lemma 3.1 (Exact t_i–r_j Collapse)**.** *For all $(u,v) \in \Omega$ with $S = u_1+u_2+u_3$,*

$$\Phi_3(u,v) \;=\; 2^{31} S \left(\prod_{i=1}^{3} t_i\right)\left(\prod_{j=1}^{3} r_j\right)\prod_{i=1}^{3}\prod_{j=1}^{3}|t_i - r_j|, \tag{3}$$

where $t_i = u_i(S-u_i)$, $r_j = v_j(S-v_j)$, and $t_i - r_j = (u_i - v_j)(S-u_i-v_j)$.

Proof. Since $A_0 = B_0 = S$ and $A_i = S - 2u_{4-i}$ (reindexing so $A_i = S-2u_i$ for $i=1,2,3$), we have $A_0^2 - B_j^2 = S^2 - (S-2v_j)^2 = 4v_j(S-v_j) = 4r_j$, $A_i^2 - B_0^2 = -4t_i$, and $A_i^2 - B_j^2 = 4(r_j - t_i)$. Multiplying all 15 factors produces $2S\cdot 4^{15}\prod t_i \prod r_j \prod|t_i-r_j| = 2^{31} S\prod t_i\prod r_j\prod|t_i-r_j|$. □

Theorem 3.2 (Exact Global Maximum of Φ_3)**.** *Let*

$$\Phi_{3,1\mathrm{D}}(s) \;:=\; 3\cdot 2^{38} s^7 (3s-2)(3s-1)^2(2s-1)^6(2-s)^3(1-s)^9,$$

and let $Q(s) = 504s^5 - 1920s^4 + 2491s^3 - 1409s^2 + 344s - 28$. There exists a unique root $s^* \in (7809236/10^7,\, 7809237/10^7)$ of $Q(s)=0$ such that

$$5979.83 \;<\; \Phi_{3,1\mathrm{D}}(s^*) \;<\; 5980 \qquad (\Phi_{3,1\mathrm{D}}(s^*) \approx 5979.85945798),$$

and for all $(u,v)\in\Omega$,

$$\Phi_3(u,v) \;\le\; \Phi_{3,1\mathrm{D}}(s^*) \;=\; \Phi_3(s^*,s^*,s^*;\, 3s^*-2,1,1).$$

Proof Overview. By permutation symmetry and degree-31 homogeneity, we have $\Phi_3(\lambda u,\lambda v) = \lambda^{31}\Phi_3(u,v)$, so we may assume $0\le u_1\le u_2\le u_3\le 1$, $0\le v_1\le v_2\le v_3\le 1$, and $\max(u_3,v_3) = 1$. We split $S = u_1+u_2+u_3 \in [0,3]$ into three regimes:

Case 1: $S \le 396/256 = 1.546875$. Each t_i, r_j lies in $[0,M]$ where $M = S^2/4$. By the elementary sum-of-squares identity

$$\frac{27}{256}M^5 - aM(M-a)^3 \;=\; \frac{1}{256}M(4a-M)^2\big((4a-5M)^2 + 2M^2\big) \;\ge\; 0,$$

every pair satisfies $t_i r_j |t_i - r_j|^3 \le \frac{27}{256}M^5$. Taking the cube of the product in (3) pairs each t_i and r_j three times, giving $\Phi_3(u,v) \le 2^{31} S (27/256)^3 (S^2/4)^{15} < 2000 < 5800$.

Case 2: $S \in [396/256, 2]$ (with $v_3 = 1$ by $u\leftrightarrow v$ symmetry). We verify $\Phi_3(u,v)\le 5800$ on the 4-dimensional domain $(v_1,v_2,u_1,u_2) \in [0,1/2]\times[1/4,1]\times[0,176/256]\times[0,1]$ (scaled by 256) using an exact-integer interval bisection tree of 1,047 leaves implemented in pure Lean `Init` (`SSRK3.PureCertS2`) and checked directly by the Lean kernel via `by decide +kernel` in under one second, with soundness proved analytically against (3).

Case 3: $S \in [2,3]$. Here every mirror pole $S - v_j \ge 1$ lies outside $[0,1]$, so for any two coordinates x, y on the same side of every v_j, $|x-c||y-c| \le |\frac{x+y}{2} - c|^2$ holds simultaneously for all poles $c \in \{0, S, v_j, S-v_j\}$ (and similarly for any run of three coordinates by 3-term AM–GM). Assuming $v_1 \le u_1$ by $u\leftrightarrow v$ symmetry, the 10 interleaving orderings of sorted (u,v) split into:

- 5 coordinate-dominated orderings ($v_i \le u_i$ for all i), where equal sums force $u = v$ and $\Phi_3 = 0$;
- *Pattern 2* ($v_1\le v_2\le u_1\le u_2\le u_3\le v_3$): run-collapse gives $(s,s,s;\, a,a,v_3)$, bounded by $\frac{2^{37}}{3^{21}}\cdot\frac{8}{6^9}S^{22}(3-S)^9 < 50 < 5800$;
- *Pattern 3* ($v_1\le u_1\le u_2\le v_2\le v_3\le u_3$): run-collapse and scaling $u_3\to 1$ yield $y+z = (3-S)/2$ and $\max_{q\in[0,1/2]}(1-q)^5(1-2q)^2q^2 = (5/6)^5(2/3)^2(1/6)^2$, giving $\Phi_3 < 1220 < 5800$;
- *Patterns 4 & 5* ($v_1\le u_1\le u_2\le v_2\le u_3\le v_3$ and $v_1\le u_1\le v_2\le u_2\le u_3\le v_3$): run-collapse on the adjacent u-pair combined with the variance-adjusted bound $r_1r_2r_3 \le \big(\frac{2S^2}{9} - \frac{(v_3-v_1)^2}{6}\big)^3$ and $\frac{4}{27}A^5(1-2A)(1-A)^2 \le \frac{1}{8900}$ gives $\Phi_3 < 4950 < 5800$;
- *Pattern 1* ($v_1\le u_1\le u_2\le u_3\le v_2\le v_3$): 3-term collapse on u and 2-term collapse on (v_2,v_3) followed by scaling $b = (v_2+v_3)/2\to 1$ yields $\Phi_3(u,v)\le \Phi_3(s,s,s;\, 3s-2,1,1) = \Phi_{3,1\mathrm{D}}(s)$ for $s\in[2/3,1]$.

Finally, $\Phi'_{3,1\mathrm{D}}(s) = 3 \cdot 2^{38} s^6 (2-s)^2 (1-s)^8 (2s-1)^5 (3s-1) Q(s)$. Bernstein expansions on $[2/3, 0.72]$ and $[0.72, 1]$ show $Q > 0$ on $[2/3, 0.72]$ and $Q' < 0$ on $[0.72, 1]$, so Q has a unique zero $s^* \in (0.7809236, 0.7809237)$, giving the unique global maximum of $\Phi_{3,1\mathrm{D}}$ in $(5979.83, 5980)$. □

To pass from the equal-sum surface Ω to actual integer instances with $\Delta = A_0 - B_0 \neq 0$, we perturb the largest coordinate u_3 to $\tilde{u}_3 = u_3 - \Delta/\sqrt{n}$ (assuming WLOG $\Delta > 0$ and $u_3 \geq u_1, u_2$) so that $\tilde{u}_1 + \tilde{u}_2 + \tilde{u}_3 = v_1 + v_2 + v_3$. Since $|\Delta| \leq 1/(5981\, n^{31/2})$ otherwise we are done, the perturbation $\delta = |\Delta|/\sqrt{n} \leq 1/(5981\, n^{16})$ moves each of the 31 conjugate factors by at most δ (or 2δ), giving an explicit Lipschitz error of at most $2.2 \times 10^7/n^{16}$ (which is < 1 for every $n \geq 3$!). Checking $n = 1$ (empty) and $n = 2$ (where $a_i, b_j \in \{1, 2\}$ reduces to $|p + q\sqrt{2}| \geq \frac{1}{3+3\sqrt{2}}$) yields our first main theorem.

Theorem 3.3 (Sharp $k = 3$ Separation Bounds and Even-Parity Boost)**.** *Let $n \geq 1$ and $1 \leq a_1, a_2, a_3, b_1, b_2, b_3 \leq n$ with $\Delta = (\sqrt{a_1} + \sqrt{a_2} + \sqrt{a_3}) - (\sqrt{b_1} + \sqrt{b_2} + \sqrt{b_3}) \neq 0$. Then:*

(1) ***Unconditional All-n Bound:***

$$|\Delta| \;\geq\; \frac{1}{5981\, n^{31/2}}.$$

(2) ***Exact Asymptotic Floor ($n \geq 3$):***

$$|\Delta| \;\geq\; \frac{1}{\big(\Phi_{3,1\mathrm{D}}(s^*) + 2.2 \times 10^7/n^{16}\big) n^{31/2}}, \qquad \Phi_{3,1\mathrm{D}}(s^*) \approx 5979.85945798.$$

(3) ***Even-Parity $65\,536$-Fold Boost:*** *If $a_1 + a_2 + a_3 \equiv b_1 + b_2 + b_3 \pmod 2$, then*

$$|\Delta| \;\geq\; \frac{65\,536}{5981\, n^{31/2}} \;>\; 10.95\, n^{-31/2}.$$

For $n \geq 6$ in part (3), the perturbation is at most $65\,536/(5981\, n^{16}) < 10^{-11}$, while the small cases $n \in \{3, 4\}$ and $n = 5$ are handled directly via the degree-4 norm in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ($|\Delta| \geq 1/16^3$) and the degree-8 norm in $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ ($|\Delta| \geq 1/23^7$, with irrationality proved by elementary 2-, 3-, and 5-adic descent in `N8_eq_zero_iff`).

4. Universal All-k Parseval–AM–GM Bound and $2^{2^{2k-2}}$-Parity Boost

For general $k \geq 2$, the classical half-norm / BFMS bound (1) bounds every one of the $2^{2k-1} - 1$ companion conjugates pointwise by $2k\sqrt{n}$. In fact, the quadratic mean of all conjugates is vastly smaller—only $\sqrt{2k\, n}$—by exact orthogonality of Walsh characters.

Lemma 4.1 (Parseval Identity and Pure-Polynomial Half-Norm Integrality)**.** *For every $m \geq 1$ and $c_0, c_1, \ldots, c_m \in \mathbb{N}$:*

(1) (Half-Parseval Identity)

$$\sum_{\tau \in \{\pm 1\}^m} \left(\sqrt{c_0} + \sum_{i=1}^{m} \tau_i \sqrt{c_i} \right)^2 \;=\; 2^m \sum_{i=0}^{m} c_i.$$

(2) (Half-Norm Integrality) $N_{\mathrm{half}}(c) := \prod_{\tau \in \{\pm 1\}^m} \big(\sqrt{c_0} + \sum_{i=1}^{m} \tau_i \sqrt{c_i} \big) \in \mathbb{Z}$.

Proof. Part (1) follows immediately by induction on m using the parallelogram identity $(u+v)^2 + (u-v)^2 = 2(u^2 + v^2)$ and sign-flip symmetry. For part (2), we prove by induction on m that for every $P \in \mathbb{Z}[X]$ there exists $Q \in \mathbb{Z}[X]$ such that $\prod_{\sigma \in \{\pm 1\}^m} P\big(x + \sum_{i=1}^{m} \sigma_i \sqrt{c_i}\big) = Q(x)$ for all $x \in \mathbb{R}$: at each step, $F(Y) = P(X+Y)P(X-Y) \in (\mathbb{Z}[X])[Y]$ is an even polynomial in Y, so substituting $Y = \sqrt{c_i}$ leaves a polynomial in $\mathbb{Z}[X]$. Taking $P(X) = X$ gives $Q \in \mathbb{Z}[X]$ with $Q(-x) = (-1)^{2^m} Q(x) = Q(x)$ for $m \geq 1$, so $Q(X) = Q_2(X^2)$ for some $Q_2 \in \mathbb{Z}[X]$, and $N_{\mathrm{half}}(c) = Q_2(c_0) \in \mathbb{Z}$. □

Theorem 4.2 (Universal All-k Parseval–AM–GM Separation Bound)**.** *For every $k \geq 2$, every $n \geq 1$, and all integers $1 \leq a_i, b_j \leq n$ with $\Delta = \sum_{i=1}^{k} \sqrt{a_i} - \sum_{j=1}^{k} \sqrt{b_j} \neq 0$,*

$$|\Delta| \;\geq\; \frac{1}{\sqrt{e}}\,(2kn)^{-(2^{2k-2}-1/2)} \;=\; \frac{1}{\sqrt{e}}\,(2k)^{-(2^{2k-2}-1/2)}\,n^{-(2^{2k-2}-1/2)}. \tag{4}$$

Proof. More generally, we prove by strong induction on $m \geq 1$ that for any $c_1, \ldots, c_m \in \{1, \ldots, n\}$ and $v \in \{\pm 1\}^m$ with $\Delta = \sum_{i=1}^{m} v_i \sqrt{c_i} \neq 0$,

$$|\Delta| \;\geq\; \frac{1}{\sqrt{e}\,(mn)^{(2^{m-1}-1)/2}}.$$

The case $m = 1$ gives $|\Delta| = \sqrt{c_1} \geq 1 \geq 1/\sqrt{e}$. For $m \geq 2$:

- If $N_{\mathrm{half}}(c) = 0$, some conjugate $\sum \sigma_i \sqrt{c_i} = 0$. By Hamming halving (choosing the smaller of $\{i : v_i \neq \sigma_i\}$ and $\{i : v_i = \sigma_i\}$), $|\Delta| = 2\bigl|\sum_{i \in S} v_i \sqrt{c_i}\bigr|$ with $1 \leq |S| < m$, and the inductive hypothesis immediately yields a strictly stronger bound.
- If $N_{\mathrm{half}}(c) \neq 0$, Lemma 4.1(2) gives $|N_{\mathrm{half}}(c)| \geq 1$. Write $M = 2^{m-1} - 1$ and let $\mathcal{S}$ be the set of the M companion conjugates distinct from $\pm\Delta$. By Lemma 4.1(1), $\sum_{\tau \in \mathcal{S}} g(\tau)^2 \leq 2^{m-1} mn$. Applying AM–GM to $\{g(\tau)^2\}_{\tau \in \mathcal{S}}$ gives

$$\prod_{\tau \in \mathcal{S}} g(\tau)^2 \;\leq\; \left(\frac{2^{m-1}}{M}\,mn\right)^{M} \;=\; \left(1 + \frac{1}{M}\right)^{M} (mn)^M \;\leq\; e\,(mn)^M.$$

  Taking square roots and using $1 \leq |\Delta| \prod_{\tau \in \mathcal{S}} |g(\tau)|$ gives $|\Delta| \geq e^{-1/2}(mn)^{-M/2}$.

Setting $m = 2k$ gives $(2^{2k-1} - 1)/2 = 2^{2k-2} - \frac{1}{2}$, proving (4). □

Comparing (4) against the classical half-norm / BFMS bound (1), both share the n-exponent $-(2^{2k-2} - \frac{1}{2})$, while the constant ratio is

$$\frac{(2k)^{-(2^{2k-2}-1/2)}/\sqrt{e}}{(2k)^{-(2^{2k-1}-1)}} \;=\; \frac{1}{\sqrt{e}}\,(2k)^{2^{2k-2}-1/2},$$

which cuts the constant exponent of $2k$ in half and still grows doubly exponentially in k ($\approx 77.6\times$ at $k = 2$, $6.99 \times 10^{11}\times$ at $k = 3$, $1.35 \times 10^{57}\times$ at $k = 4$, and $1.92 \times 10^{255}\times$ at $k = 5$).

Next, we generalize the 2^{16}-divisibility of Lemma 2.1(2) to arbitrary conjugate products and arbitrary $k \geq 2$.

Lemma 4.3 (Universal Even-Parity 2-Adic Norm Divisibility)**.** *Let $\mathcal{F}$ be a finite family of $2D$ sign vectors $\sigma \in \{\pm 1\}^N$, and let $c_1, \ldots, c_N \in \mathbb{N}$ have even sum $\sum_{i=1}^{N} c_i = 2s$ ($s \in \mathbb{N}$). If the product $Z := \prod_{\sigma \in \mathcal{F}} \bigl(\sum_{i=1}^{N} \sigma_i \sqrt{c_i}\bigr)$ lies in $\mathbb{Z}$, then $2^D \mid Z$. In particular, for every $m \geq 1$ and $c_0, \ldots, c_m \in \mathbb{N}$ with even sum, $2^{2^{m-1}} \mid N_{\mathrm{half}}(c)$ (for $m = 2k - 1$: $2^{2^{2k-2}} \mid N_{\mathrm{half}}$).*

Proof. For each $\sigma \in \mathcal{F}$, expanding the square gives

$$\left(\sum_{i=1}^{N} \sigma_i \sqrt{c_i}\right)^2 \;=\; \sum_{i=1}^{N} c_i + 2 \sum_{1 \leq i < j \leq N} \sigma_i \sigma_j \sqrt{c_i c_j} \;=\; 2\bigl(s + \alpha_\sigma\bigr),$$

where each $\alpha_\sigma = \sum_{i<j} \sigma_i \sigma_j \sqrt{c_i c_j}$ is integral over $\mathbb{Z}$ (since each $\sqrt{c_i}$ satisfies the monic polynomial $X^2 - c_i = 0$ and the integral closure is a ring). Multiplying over all $2D$ vectors $\sigma \in \mathcal{F}$ yields $Z^2 = 2^{2D} W$, where $W := \prod_{\sigma \in \mathcal{F}} (s + \alpha_\sigma)$ is integral over $\mathbb{Z}$. By induction on r (for $2^r W = u \in \mathbb{Z}$, clearing denominators in a monic annihilating polynomial $p(W) = 0$ of degree $d \geq 1$ gives $u^d \equiv 0 \pmod 2$, hence $2 \mid u$ and $2^{r-1} W = u/2$), we obtain $2^{2D} \mid Z^2$, and therefore $2^D \mid Z$. □

Theorem 4.4 (Universal All-k Even-Parity Parseval–AM–GM Boost)**.** *For every $k \geq 2$, every $n \geq 1$, and all $1 \leq a_i, b_j \leq n$ with $\sum_{i=1}^{k} a_i \equiv \sum_{j=1}^{k} b_j \pmod 2$ and $\Delta \neq 0$,*

$$|\Delta| \;\geq\; \frac{2^{2^{2k-2}}}{\sqrt{e}\,(2kn)^{2^{2k-2}-1/2}} \;=\; \sqrt{\frac{2}{e}}\,(kn)^{-(2^{2k-2}-1/2)}, \tag{5}$$

improving upon (1) by $\sqrt{2/e}\,(4k)^{2^{2k-2}-1/2}$.

Proof. If $N_{\text{half}}(c) = 0$, Hamming halving reduces $|\Delta| = 2\left|\sum_{i\in S} v_i\sqrt{c_i}\right|$ to a subset S of size $1 \le |S| \le k$; applying Theorem 4.2 on $|S|$ terms gives

$$|\Delta| \;\ge\; \frac{2}{\sqrt{e}}\,(|S|\,n)^{-(2^{|S|-1}-1)/2} \;\ge\; \sqrt{\frac{2}{e}}\,(kn)^{-(2^{2k-2}-1/2)}.$$

If $N_{\text{half}}(c) \neq 0$, Lemma 4.3 gives $|N_{\text{half}}(c)| \ge 2^{2^{2k-2}}$, and the Parseval–AM–GM companion bound from Theorem 4.2 yields

$$|\Delta| \;\ge\; \frac{2^{2^{2k-2}}}{\sqrt{e}\,(2kn)^{2^{2k-2}-1/2}} \;=\; \sqrt{\frac{2}{e}}\,(kn)^{-(2^{2k-2}-1/2)}. \qquad \square$$

Table 1 summarizes the exact exponents and constant improvement factors across $k = 2, 3, 4, 5$ alongside the constructive upper bound $O(n^{-2k+1/2})$ of [2].

TABLE 1. Quantitative comparison of separation bounds for $r(n,k)$ across $k = 2, 3, 4, 5$.

k	Generic n-exp.	Thm. 4.2 / (1)	Thm. 4.4 / (1)	Thm. 6.2 n-exp.	Upper bound [2]
2	$-7/2$	$7.76 \times 10^{1}\times$	$1.24 \times 10^{3}\times$	$-3/2$	$O(n^{-7/2})$
3	$-31/2$	$6.99 \times 10^{11}\times$	$4.58 \times 10^{16}\times$	$-15/2$	$O(n^{-11/2})$
4	$-127/2$	$1.35 \times 10^{57}\times$	$2.48 \times 10^{76}\times$	$-63/2$	$O(n^{-15/2})$
5	$-511/2$	$1.92 \times 10^{255}\times$	$2.22 \times 10^{332}\times$	$-255/2$	$O(n^{-19/2})$

5. Clustered / Spread-L Exponent-Breaking

Many geometric and number-theoretic constructions of small SSR differences—including the Qian–Wang [5] and optimal $O(n^{-2k+1/2})$ constructions of [2]—choose all integers a_i, b_j inside a narrow cluster $[m, m+L]$ of spread $L \ll n$. We prove that clustering forces a massive algebraic collapse of the inner conjugate factors, breaking the generic separation exponent by 9 full powers of n for $k = 3$.

Theorem 5.1 (Clustered / Spread-L Exponent-Breaking for $k = 3$)**.** *Let $m \ge 1$, $L \ge 1$, $n = m + L$, and let $a_1, a_2, a_3, b_1, b_2, b_3 \in [m, m+L]$ satisfy $\Delta = (\sqrt{a_1} + \sqrt{a_2} + \sqrt{a_3}) - (\sqrt{b_1} + \sqrt{b_2} + \sqrt{b_3}) \neq 0$. Then*

$$|\Delta| \;\ge\; \frac{1}{3^{12}\cdot 6^{10}\cdot n^{13/2}\cdot L^{9}}. \tag{6}$$

In particular, $|\Delta| = \Omega(n^{-13/2})$ whenever $L = O(1)$ (saving 9 full powers of n over $n^{-31/2}$), and $|\Delta| = \Omega(n^{-11})$ whenever $L = O(\sqrt{n})$.

Proof. If $M_3(a,b) = 0$, Lemma 2.3 gives $|\Delta| \ge \frac{1}{2n\sqrt{n}}$, which is much stronger than (6). Otherwise $|M_3(a,b)| \ge 1$ by Lemma 2.1(1). In the product (2):

- The main factor satisfies $|A_0^2 - B_0^2| = (A_0 + B_0)|\Delta| \le 6\sqrt{n}\,|\Delta|$.
- Each of the 6 mixed-weight factors ($i = 0, j \ge 1$ or $i \ge 1, j = 0$) satisfies $|A_i^2 - B_j^2| \le \max(A_i^2, B_j^2) \le 9n$.
- Each of the 9 inner factors ($i, j \in \{1, 2, 3\}$) satisfies

$$|A_i^2 - B_j^2| \;\le\; 6L \tag{7}$$

unconditionally for *all* $m \ge 1$ and $L \ge 1$. Indeed, every A_i, B_j lies in $[2\sqrt{m} - \sqrt{n},\, 2\sqrt{n} - \sqrt{m}]$.

(1) If $L \le 3m$, then $n = m + L \le 4m$, so $\sqrt{n} \le 2\sqrt{m}$. Hence $A_i, B_j \ge 0$, $|A_i - B_j| \le 3(\sqrt{n} - \sqrt{m})$, and $A_i + B_j \le 4\sqrt{n} - 2\sqrt{m} \le 2(\sqrt{n} + \sqrt{m})$. Multiplying gives $|A_i^2 - B_j^2| \le 6(\sqrt{n} - \sqrt{m})(\sqrt{n} + \sqrt{m}) = 6(n - m) = 6L$.

(2) If $L > 3m$, then $n = m + L < \frac{4}{3}L$, while $A_i, B_j \in [-\sqrt{n}, 2\sqrt{n}]$ implies $0 \le A_i^2, B_j^2 \le 4n$, so $|A_i^2 - B_j^2| \le 4n < \frac{16}{3}L < 6L$.

Multiplying all 16 factor bounds gives $1 \le |M_3| \le (6\sqrt{n}|\Delta|)\cdot(9n)^6\cdot(6L)^9 = 3^{12}\cdot 6^{10}\cdot n^{13/2}L^9|\Delta|$. □

Corollary 5.2 (Even-Parity Spread-L Boost)**.** *Under the hypotheses of Theorem 5.1, if additionally* $a_1+a_2+a_3 \equiv b_1+b_2+b_3 \pmod 2$*, then* $|M_3| \ge 2^{16}$ *(for* $M_3 \ne 0$*) yields*

$$|\Delta| \;\ge\; \frac{65\,536}{3^{12}\cdot 6^{10}\cdot n^{13/2}\cdot L^9} \;=\; \frac{64}{3^{22}\cdot n^{13/2}\cdot L^9}.$$

More generally, for any $k \ge 2$, the degree-2^{2k-2} half-norm $\prod_{\varepsilon,\delta}(A_\varepsilon^2 - B_\delta^2)$ (fixing $\varepsilon_1 = \delta_1 = +1$) has a collapsed factor $A_\varepsilon^2 - B_\delta^2 = O(L)$ whenever the signed weights $w(\varepsilon) = \sum_{i=1}^k \varepsilon_i$ and $w(\delta) = \sum_{j=1}^k \delta_j$ satisfy $|w(\varepsilon)| = |w(\delta)|$ (excluding the main factor $\varepsilon = \delta = (+1,\dots,+1)$).

Proposition 5.3 (Exact General-k Spread-Collapsed Factor Count)**.** *For every* $k \ge 2$*, the number of non-main sign pairs* $(\varepsilon,\delta) \in \{\pm1\}^{k-1}\times\{\pm1\}^{k-1}$ *with* $|w(\varepsilon)| = |w(\delta)|$ *is*

$$N_{\text{small}}(k) \;=\; \frac{1}{2}\binom{2k}{k} - \mathbf{1}_{2|k}\cdot\frac{1}{4}\binom{k}{k/2}^2 - 1.$$

Proof. Write $m = k-1$ and let r be the number of -1 signs in ε, so $w(\varepsilon) = k - 2r$. By Vandermonde's identity, the number of pairs with $w(\varepsilon) = w(\delta)$ is $\sum_{r=0}^m \binom{m}{r}^2 = \binom{2m}{m}$, and the number with $w(\varepsilon) = -w(\delta)$ is $\sum_{r=0}^m \binom{m}{r}\binom{m}{m+1-r} = \binom{2m}{m+1}$. Their sum is $\binom{2m+1}{m+1} = \frac{1}{2}\binom{2k}{k}$. The intersection $\{w(\varepsilon) = w(\delta) = 0\}$ is empty for odd k and has size $\binom{k-1}{k/2}^2 = \frac{1}{4}\binom{k}{k/2}^2$ for even k. Subtracting 1 for the main pair yields the result (giving $N_{\text{small}}(k) = 1, 9, 25, 125, \dots$ for $k = 2,3,4,5,\dots$). □

6. Universal All-k Galois Exponent-Halving Theorem

When the $2k$ integers satisfy a multiplicative square relation $\prod_{x\in S} c_x = d^2$ for a non-empty subset $S \subseteq \{1,\dots,2k\}$, the radical extension $K = \mathbb{Q}(\sqrt{c_1},\dots,\sqrt{c_{2k}})$ drops in degree by at least a factor of 2. Crucially, however, the separation exponent halves *if and only if* $|S|$ *is even*: an automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ must satisfy $\prod_{x\in S}\sigma_x = +1$, so $-I = (-1,\dots,-1)$ remains in the Galois group if and only if $(-1)^{|S|} = +1$. When $|S|$ is even, the half-norm splits into two integer quarter-norms of degree 2^{2k-2}, halving the algebraic degree and reducing the worst-case n-exponent from $-(2^{2k-2} - \frac{1}{2})$ to $-(2^{2k-3} - \frac{1}{2})$ for every $k \ge 2$. We prove this with zero Galois theory via pure $\mathbb{Z}[X]$ parity-split polynomial algebra.

Lemma 6.1 (Quarter-Norm Integrality)**.** *Let* $r \ge 1$ *be odd,* $t \ge 0$ *with* $r + t \ge 2$*, and* $c_0, s_1, \dots, s_r, y_1, \dots, y_t \in \mathbb{N}$*. Suppose* $c_0\prod_{i=1}^r s_i = d^2$ *for some* $d \in \mathbb{N}$*. Then for each sign parity* $\pi \in \{\pm1\}$*,*

$$Q_\pi \;:=\; \prod_{\substack{\tau\in\{\pm1\}^r \\ \prod\tau_i=\pi}} \prod_{\rho\in\{\pm1\}^t} \left(\sqrt{c_0} + \sum_{i=1}^r \tau_i\sqrt{s_i} + \sum_{j=1}^t \rho_j\sqrt{y_j}\right) \;\in\; \mathbb{Z}.$$

Proof. We first prove by induction on $r \ge 1$ that there exist $A, B \in \mathbb{Z}[X]$ such that

$$\prod_{\substack{\tau\in\{\pm1\}^r \\ \prod\tau_i=\pm1}} \left(x + \sum_{i=1}^r \tau_i\sqrt{s_i}\right) \;=\; A(x) \pm B(x)\prod_{i=1}^r \sqrt{s_i}$$

for all $x \in \mathbb{R}$, with exact parities: (A odd, B even) for $r = 1$, (A even, B even) for even $r \ge 2$, and (A even, B odd) for odd $r \ge 3$. At each inductive step ($r \to r+1$), write $A(x \pm \sqrt{s_0}) = E_A(x) \pm O_A(x)\sqrt{s_0}$ and $B(x \pm \sqrt{s_0}) = E_B(x) \pm O_B(x)\sqrt{s_0}$ with $E_A, O_A, E_B, O_B \in \mathbb{Z}[X]$ preserving parity. Letting $\Pi = \prod_{i=1}^r \sqrt{s_i}$ (so $\Pi^2 \in \mathbb{Z}$), the product for parity $+1$ splits as a difference of squares:

$$\begin{aligned}&\big(A(x+\sqrt{s_0}) + B(x+\sqrt{s_0})\Pi\big)\big(A(x-\sqrt{s_0}) - B(x-\sqrt{s_0})\Pi\big)\\ &\quad= \big(E_A^2 + s_0\Pi^2 O_B^2 - s_0 O_A^2 - \Pi^2 E_B^2\big) + 2(E_A O_B - O_A E_B)\cdot(\sqrt{s_0}\,\Pi),\end{aligned}$$

and parity -1 flips the sign of $\sqrt{s_0}\,\Pi$, advancing the exact parity pattern.

Next, induction on $t \geq 0$ multiplies over $\rho_j = \pm 1$ via the second difference-of-squares identity

$$\begin{aligned}&\big(A(x+\sqrt{y_0}) \pm B(x+\sqrt{y_0})\Pi\big)\big(A(x-\sqrt{y_0}) \pm B(x-\sqrt{y_0})\Pi\big)\\ &\quad= \big(E_A^2 + \Pi^2 E_B^2 - y_0 O_A^2 - y_0 \Pi^2 O_B^2\big) \pm 2(E_A E_B - y_0 O_A O_B)\cdot \Pi.\end{aligned}$$

Whenever r is odd and $r + t \geq 2$, this unconditionally produces $A(-X) = A(X)$ (even) and $B(-X) = -B(X)$ (odd), hence $A(X) = A_2(X^2)$ and $B(X) = XB_2(X^2)$ for $A_2, B_2 \in \mathbb{Z}[X]$. Substituting $x = \sqrt{c_0}$ yields

$$Q_\pi \;=\; A_2(c_0) + \pi\, B_2(c_0)\,\sqrt{c_0}\prod_{i=1}^{r}\sqrt{s_i} \;=\; A_2(c_0) + \pi\, d\, B_2(c_0) \;\in\; \mathbb{Z}. \qquad \square$$

Theorem 6.2 (Universal All-k Galois Exponent-Halving Theorem)**.** *Let $k \geq 2$, $n \geq 1$, and $1 \leq a_i, b_j \leq n$ with $\Delta = \sum_{i=1}^{k}\sqrt{a_i} - \sum_{j=1}^{k}\sqrt{b_j} \neq 0$. Suppose there exists a non-empty even-cardinality subset $S \subseteq \{1,\ldots,2k\}$ such that $\prod_{x\in S} c_x = d^2$ for some $d \in \mathbb{N}$, where $(c_1,\ldots,c_{2k}) = (a_1,\ldots,a_k,b_1,\ldots,b_k)$. Then*

$$|\Delta| \;\geq\; \frac{1}{\sqrt{e}\,(C_S\cdot n)^{(2^{2k-2}-1)/2}}, \qquad C_S = \begin{cases} 2k & \text{if } |S| \geq 4,\\ 2k+2 & \text{if } |S| = 2.\end{cases} \tag{8}$$

In particular, for $k = 3$, whenever any pair (a_ia_j, b_ib_j, a_ib_j), any quadruple ($a_ia_jb_pb_q$, $a_1a_2a_3b_p$, $a_ib_1b_2b_3$), or the full 6-term product $a_1a_2a_3b_1b_2b_3$ is a perfect square,

$$|\Delta| \;\geq\; \frac{1}{\sqrt{e}\,(C_S\cdot n)^{15/2}}, \qquad C_S \in \{6, 8\}, \tag{9}$$

halving the algebraic degree ($32 \to 16$) and reducing the separation exponent from $-31/2$ to $-15/2$.

Proof. Pick $i_0 \in S$, set $S' = S \setminus \{i_0\}$ (size $r = |S| - 1$, odd), and $T = \{1,\ldots,2k\} \setminus S$ (size $t = 2k - |S|$, with $r + t = 2k - 1 \geq 3$). Normalize the sign of $\sqrt{c_{i_0}}$ to $+1$, and let π be the sign product on S'. If the quarter-norm $Q_\pi = 0$, some conjugate vanishes; Hamming-distance halving reduces Δ to at most k square roots, where Theorem 4.2 (on $r \leq k$ terms, with $2^{r-1} - 1 \leq 2^{2k-2} - 1$) yields an even stronger lower bound. If $Q_\pi \neq 0$, Lemma 6.1 gives $|Q_\pi| \geq 1$. For $|S| \geq 4$ (so $r \geq 3$), flipping any two indices in S' preserves $\prod \tau_i = \pi$, so all degree-1 and degree-2 Walsh characters vanish on the parity-restricted subgroup; hence the exact Parseval sum is $2^{2k-2}\sum_{i=1}^{2k} c_i \leq 2^{2k-2}(2k)n$. For $|S| = 2$ ($r = 1$), the single sign in S' is fixed and $(x_0 \pm x_1)^2 \leq 2x_0^2 + 2x_1^2$, giving Parseval sum $\leq 2^{2k-2}(2k+2)n$. Applying AM–GM over the $M = 2^{2k-2} - 1$ companion conjugates in Q_π gives $\prod_{\text{comp}} g^2 \leq (1 + 1/M)^M (C_S n)^M \leq e(C_S n)^M$, proving (8) (whose n-exponent is $-M/2 = -(2^{2k-3} - \frac{1}{2})$). $\square$

Corollary 6.3 (Even-Parity Quarter-Norm $2^{2^{2k-3}}$-Divisibility and Boost)**.** *Under the hypotheses of Theorem 6.2, if additionally $\sum_{i=1}^{k} a_i \equiv \sum_{j=1}^{k} b_j \pmod 2$, then Lemma 4.3 implies $2^{2^{2k-3}} \mid Q_\pi$ (a 256-fold boost at $k = 3$ and 2^{32}-fold boost at $k = 4$), yielding*

$$|\Delta| \;\geq\; \sqrt{\frac{2}{e}}\,(C'_S\cdot n)^{-(2^{2k-3}-1/2)}, \qquad C'_S = \begin{cases} k & \text{if } |S| \geq 4,\\ k+1 & \text{if } |S| = 2.\end{cases}$$

In particular, for $k = 3$, $|\Delta| \geq \sqrt{2/e}\,(3n)^{-15/2}$ whenever $|S| \in \{4, 6\}$ and $|\Delta| \geq \sqrt{2/e}\,(4n)^{-15/2}$ whenever $|S| = 2$.

7. Pure Lean 4 Formalization and Axiom Audit

All results in this paper have been machine-checked in Lean 4.36.0 with Mathlib across six modular files in the `SSRK3` library. Table 2 lists each major theorem alongside its Lean identifier and its verified axiom footprint from `check_axioms.lean`.

Notably, the Case 2 certificate `SSRK3.PureCertS2` imports *no* Mathlib modules and is verified by pure kernel reduction (`by decide +kernel`), avoiding `native_decide` (`Lean.ofReduceBool`)

TABLE 2. Summary of formally verified theorems in Lean 4.36.0 (`SSRK3`).

Paper Result	Lean Identifier	Axioms
Case 2 cert (1,047 leaves)	`PureCertS2.s2_cert_ok`	*none* (`decide +kernel`)
Lemma 2.1(1)	`SSRK3.M3_is_int`	`propext, choice, Quot.sound`
Lemma 2.1(2)	`SSRK3.M3_even_parity_div_65536`	`propext, choice, Quot.sound`
Lemma 2.3	`SSRK3.k3_degenerate_lower_bound`	`propext, choice, Quot.sound`
Theorem 3.2	`SSRK3.Phi3_global_max_exact`	`propext, choice, Quot.sound`
Theorem 3.3(1)	`SSRK3.k3_lower_bound_all_n`	`propext, choice, Quot.sound`
Theorem 3.3(2)	`SSRK3.k3_asymptotic_sharp_floor`	`propext, choice, Quot.sound`
Theorem 3.3(3)	`SSRK3.k3_lower_bound_even_parity`	`propext, choice, Quot.sound`
Lemma 4.1(2)	`SSRK3.all_m_half_norm_is_int`	`propext, choice, Quot.sound`
Theorem 4.2	`SSRK3.all_k_parseval_lower_bound`	`propext, choice, Quot.sound`
Lemma 4.3	`SSRK3.prod_signed_sqrt_even_sum_div`	`propext, choice, Quot.sound`
Lemma 4.3 (half)	`SSRK3.all_m_even_parity_half_norm_div`	`propext, choice, Quot.sound`
Theorem 4.4	`SSRK3.all_k_parseval_even_parity_lower_bound`	`propext, choice, Quot.sound`
Theorem 5.1	`SSRK3.k3_spread_lower_bound`	`propext, choice, Quot.sound`
Corollary 5.2	`SSRK3.k3_spread_even_parity_lower_bound`	`propext, choice, Quot.sound`
Proposition 5.3	`SSRK3.all_k_spread_collapsed_count`	`propext, choice, Quot.sound`
Lemma 6.1	`SSRK3.quarter_norm_is_int`	`propext, choice, Quot.sound`
Corollary 6.3 (div)	`SSRK3.quarter_norm_even_parity_div`	`propext, choice, Quot.sound`
Theorem 6.2	`SSRK3.all_k_subfield_collapse_lower_bound`	`propext, choice, Quot.sound`
Equation (9)	`SSRK3.k3_subfield_collapse_lower_bound`	`propext, choice, Quot.sound`
Corollary 6.3 (all-k)	`SSRK3.all_k_subfield_even_parity_lower_bound`	`propext, choice, Quot.sound`
Corollary 6.3 ($k = 3$)	`SSRK3.k3_subfield_even_parity_lower_bound`	`propext, choice, Quot.sound`

and `Lean.trustCompiler`. Automated checks confirm zero occurrences of `sorry`, `admit`, or `native_decide` across the entire repository.

REFERENCES

[1] 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.
[2] I. Besevic, *Breaking the Linear-Ansatz Barrier for the Sum-of-Square-Roots Problem*, Preprint (2026).
[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] M. R. Garey, R. L. Graham, and D. S. Johnson, *Some NP-complete geometric problems*, Proc. 8th Annual ACM Symposium on Theory of Computing (STOC), 1976, pp. 10–22.
[5] 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.

ESIEE-IT, FRANCE
Email address: `ivan.besevic@edu.esiee-it.fr`