Representation-Independent Galois Barriers for Rank-1-Hessian Lorentz Systems, Optimal $(k+2)$-Site Turnpike Rulers, Sharp Mixed-Radix Freiman Compression, and Rational SDP Witnesses

Lluis Eriksson
Independent Researcher · AIRR.SCIENCE
https://github.com/lluiseriksson/radical-turnpike-galois-barriers-and-sdp

November 2026

Abstract

Given positive integers $a_1, \ldots, a_k$ and K, let $S = \sum_{i=1}^{k} \sqrt{a_i}$ and $\Delta = S - K$. Elder (arXiv:2611.34535v1) constructed a $(k+3)$-site realizable Turnpike ruler with minimum spacing $\mathrm{sep}(Y) \le |\Delta|$ and addition residual $\mathrm{gap}_\star(Y) \le |\Delta|$ (Proposition 1), reduced unordered radical-sum Turnpike to integer Turnpike via a uniform base-β ($\beta = 2M+1$) Freiman isomorphism (Theorem 4), gave rational affine PSD pencils L_{a_i}, U_{a_i} of order $2k+1$ for both threshold directions (Proposition 5), and checked that for these specific encodings the Lorentz squared-residual Hessians span a k-dimensional space, falling outside OpenAI's strongly polynomial Corollary 7 (Hessian span dimension ≤ 1) whenever $k > 1$.

We sharpen and generalize every pillar of Elder's framework in three constructively verified theorems. First, we upgrade Elder's encoding-specific Hessian-span check into a complete *representation-independent* Galois-theoretic classification: any rational affine Lorentz system of arbitrary dimension whose squared-residual Hessians span a space of dimension at most 1 linearizes onto a single rational quadric $t = x^{\mathsf{T}} Q x$, forcing every attained rational-linear extreme value to have algebraic degree at most 2 over $\mathbb{Q}$; by Kummer theory and Besicovitch's linear independence of distinct square-free radicals, $[\mathbb{Q}(S) : \mathbb{Q}] = 2^\rho$ where $\rho := \dim_{\mathbb{F}_2} \mathrm{span}_{\mathbb{F}_2}\{[\tilde{d}_j]\} \le r_{\mathrm{irr}}$ is the multiplicative Kummer $\mathbb{F}_2$-rank of the r_{irr} distinct non-square square-free classes among $\{a_i\}$, and since $\rho \le 1 \iff r_{\mathrm{irr}} \le 1$, S admits an attained rank-1-Hessian-span Lorentz formulation of *any* size if and only if $r_{\mathrm{irr}} \le 1$ (ruling out all rational reformulations for $r_{\mathrm{irr}} \ge 2$). Second, we eliminate the auxiliary gap B from Elder's Proposition 1 to obtain a strictly minimal $(k+2)$-site ruler achieving $\mathrm{sep}(Y) \le |\Delta|$ and $\mathrm{gap}_\star(Y) \le |\Delta|$ for all $k \ge 1$ (saving $k+2$ pairwise distances), and we replace Elder's uniform radix $\beta = 2M+1$ in Theorem 4 with per-coordinate mixed radices $\beta_j = 2M_j + 1$, compressing encoded bit-lengths from $r \log_2(2M+1)$ to $\sum_{j=1}^{r} \log_2(2M_j+1)$ while proving that $\beta_j = 2M_j + 1$ $(1 \le j \le r-1)$ is strictly necessary and sufficient for carry-free Freiman preservation on $\prod_j [0, M_j]$. Third, via the exact integer Galois norm $N_{E/\mathbb{Q}}(S-K) \in \mathbb{Z} \setminus \{0\}$ over $\mathrm{Gal}(E/\mathbb{Q}) \cong \{\pm 1\}^\rho$ and a $\{0,1\}$-gap-indicator envelope, we establish explicit constant-free lower bounds $|\Delta| \ge (K+S)^{-(2^\rho - 1)}$, $\mathrm{sep}(Y) \ge (K+S)^{-(2^\rho-1)}$, and $\mathrm{gap}_\star(Y) \ge (2K+2S)^{-(2^\rho-1)}$ depending only on $\rho \le r_{\mathrm{irr}}$, and translate strict feasibility in Elder's Proposition 5 into constructive dyadic rational SDP witnesses $x \in \mathbb{Q}^k$ of explicit bit-length $O(2^\rho L)$ certifying $L_{a_i}(x_i) \succ 0$ (when $S < K$) or $U_{a_i}(x_i) \succ 0$ (when $S > K$), contrasted with irrationality of equality witnesses whenever any a_i is non-square. Twenty constructive Lean 4.35.0 theorems (0 `sorry`, 0 `Classical.choice`), 16 zero-float SHA-256 certificates, and 56 adversarial tests verify all results.

Keywords: Sum-of-square-roots problem, Turnpike problem, semidefinite programming, Lorentz cone, Freiman isomorphism, Galois norm, formal verification, Lean 4.
MSC 2020: Primary 90C22; Secondary 11Y16, 12F10, 68Q15.

1 Introduction

Deciding whether $S = \sum_{i=1}^{k} \sqrt{a_i} \le K$ for positive binary integers $a_1, \dots, a_k, K$ in time polynomial in the binary input length L is a notorious open problem linking computational geometry, number theory, and semidefinite programming [3]. In a recent note [2], Elder connected this threshold problem to the exact Turnpike problem (reconstructing $x_1 < \cdots < x_n$ from the distance multiset $Y = \mathrm{dist}(X)$) and to exact semidefinite feasibility, establishing four main results:

1. *Planted ruler margins ([2, Proposition 1, Corollary 2]):* Using consecutive gaps $(\sqrt{a_1}, \dots, \sqrt{a_k}, K, B)$ with $B = 2(1 + K + \sum_i a_i)$, a $(k+3)$-site ruler satisfies $\mathrm{sep}(Y) \le |\Delta|$ and $\mathrm{gap}_\star(Y) \le |\Delta|$ when $\Delta := S - K \neq 0$.

2. *Uniform base-β Freiman recoding ([2, Theorem 4]):* Unordered radical-sum Turnpike is polynomial-time many-one equivalent to integer Turnpike via $f(u) = \sum_{j=1}^{r} w_j(u)\beta^{j-1}$ with uniform radix $\beta = 2M + 1$, where $M = \max_{u,j} w_j(u)$ (giving output bound $(2M+1)^r$).

3. *Exact PSD pencils ([2, Proposition 5]):* Both $S \le K$ and $S \ge K$ reduce to feasibility of order-$(2k+1)$ rational affine matrix pencils $L_{a_i}(x_i) \succeq 0$ and $U_{a_i}(x_i) \succeq 0$.

4. *Lorentz Hessian span ([2, Section 3.1, Eq. (5)]):* For the specific blocks U_{a_i} and L_{a_i}, the squared-residual Hessians $8e_ie_i^{\mathsf{T}}$ and $-8a_ie_ie_i^{\mathsf{T}}$ (verified constructively in Lean 4 Theorems 17–18, `cert11`) span a k-dimensional space, so OpenAI's strongly polynomial Lorentz-cone algorithm [4, Corollary 7] (requiring Hessian span dimension ≤ 1) does not apply directly when $k > 1$. Elder explicitly noted that *"reformulation can change the span: $\sqrt{2} + \sqrt{8} = 3\sqrt{2}$ needs only one block"* [2, Section 3.1].

Main Results

Write each radicand uniquely as $a_i = d_i m_i^2$ with d_i square-free and $m_i \in \mathbb{Z}_{>0}$. Let $r := |\{d_1, \dots, d_k\}| \le k$ be the total number of distinct square-free classes, let $r_{\mathrm{irr}} := |\{d_i > 1\}| \in \{r-1, r\}$ be the number of distinct *non-square* square-free classes, and let

$$\rho \;:=\; \dim_{\mathbb{F}_2} \mathrm{span}_{\mathbb{F}_2}\{[\tilde{d}_1], \dots, [\tilde{d}_{r_{\mathrm{irr}}}]\} \;\subseteq\; \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \qquad (\rho \le r_{\mathrm{irr}})$$

be their multiplicative Kummer $\mathbb{F}_2$-rank, writing $S = \alpha_0 + \sum_{j=1}^{r_{\mathrm{irr}}} \alpha_j \sqrt{\tilde{d}_j}$ ($\alpha_0 \in \mathbb{Z}_{\ge 0}$, $\alpha_j \in \mathbb{Z}_{>0}$, distinct square-free $\tilde{d}_j > 1$).

Theorem 1 (Representation-Independent Galois Barrier for OpenAI Corollary 7)**.** *Let $S = \sum_{i=1}^{k} c_i\sqrt{a_i}$ with $c_i \in \mathbb{Q}_{>0}$ and $a_i \in \mathbb{Z}_{>0}$, grouped as $S = \alpha_0 + \sum_{j=1}^{r_{\mathrm{irr}}} \alpha_j \sqrt{\tilde{d}_j}$ ($\alpha_0 \in \mathbb{Q}_{\ge 0}$, $\alpha_j \in \mathbb{Q}_{>0}$, distinct square-free $\tilde{d}_j > 1$) with Kummer $\mathbb{F}_2$-rank ρ.*

(a) Quadratic algebraic-degree cap for rank-1 Hessian spans: *Suppose $\mathcal{F} = \{x \in \mathbb{R}^N : \|A_jx + f_j\|_2 \le g_j^{\mathsf{T}}x + \eta_j,\ j = 1, \dots, m\}$ is* any *rational affine Lorentz system of arbitrary ambient dimension N and constraint count m ($A_j \in \mathbb{Q}^{m_j \times N}$, $f_j \in \mathbb{Q}^{m_j}$, $g_j \in \mathbb{Q}^N$, $\eta_j \in \mathbb{Q}$) whose squared-residual Hessians $H_j = 2(A_j^{\mathsf{T}}A_j - g_jg_j^{\mathsf{T}})$ span a subspace of dimension at most 1. Then every finite extreme value $\min_{x\in\mathcal{F}} w^{\mathsf{T}}x$ or $\max_{x\in\mathcal{F}} w^{\mathsf{T}}x$ of any rational linear functional $w \in \mathbb{Q}^N$ attained on $\mathcal{F}$ is algebraic over $\mathbb{Q}$ of degree at most 2.*

(b) Exact Galois degree: *By Kummer theory and Besicovitch's theorem, $[\mathbb{Q}(S) : \mathbb{Q}] = 2^\rho$. Moreover, $\rho \le 1 \iff r_{\mathrm{irr}} \le 1$.*

(c) Exact representation-independent dichotomy: *The threshold value S is representable as an* attained *extreme value of a rational rank-1-Hessian-span Lorentz system of arbitrary dimension if and only if $r_{\mathrm{irr}} \le 1$ (equivalently $\rho \le 1$). In particular, for every $r_{\mathrm{irr}} \ge 2$ (e.g., $\sqrt{2} + \sqrt{3}$, irreducible minimal polynomial $x^4 - 10x^2 + 1$; or $\sqrt{2} + \sqrt{3} + \sqrt{6}$, where $r_{\mathrm{irr}} = 3$ and $\rho = 2$, minimal polynomial $x^4 - 22x^2 - 48x - 23$), $2^\rho \ge 4 > 2$ rules out* every *rational reformulation into OpenAI's Corollary 7.*

Theorem 2 (Optimal $(k+2)$-Site Ruler and Sharp Mixed-Radix Freiman Encoding)**.**

(a) Minimal $(k+2)$-site planted ruler: *For every $k \geq 1$ and $K > 0$, the $(k+2)$-site ruler with consecutive gaps $(\sqrt{a_1}, \ldots, \sqrt{a_k}, K)$ (eliminating Elder's auxiliary gap B entirely and saving $k+2$ pairwise distances) satisfies $\mathrm{sep}(Y) \leq |\Delta|$ and $\mathrm{gap}_\star(Y) \leq |\Delta|$ whenever $\Delta = S - K \neq 0$. Moreover, $k+2$ sites is strictly minimal among rulers realizing the k consecutive summand gaps and K.*

(b) Sharp per-coordinate mixed-radix Freiman compression: *In [2, Theorem 4], let $M_j := \max_u w_j(u)$ be the per-coordinate maximum and set $\beta_j := 2M_j + 1$. The mixed-radix map*

$$f_{\mathrm{mix}}(u) \;=\; \sum_{j=1}^{r} w_j(u) \prod_{i=1}^{j-1} \beta_i \tag{1}$$

induces an exact polynomial-time bijection between normalized radical rulers and normalized integer rulers with output bound $\prod_{j=1}^{r}(2M_j+1) \leq (2M+1)^r$ (achieving exponential compression $(2M_1+1)\cdot 3^{r-1}$ versus $(2M_1+1)^r$ when $M_1 = M \geq 2$ and $M_{j>1} = 1$). Furthermore, for every coordinate $1 \leq j \leq r-1$, $\beta_j = 2M_j + 1$ is strictly necessary *for carry-free Freiman preservation on $\prod_{j=1}^{r}[0, M_j]$: for every $1 \leq \beta_1 \leq 2M_1$, explicit vectors $u, v, w \in [0, M_1] \times [0, 1]$ (strictly positive when $\beta_1 \geq 2$) satisfy $u + v \neq w$ yet $f_{\mathrm{mix}}(u) + f_{\mathrm{mix}}(v) = f_{\mathrm{mix}}(w)$.*

Theorem 3 (Explicit Galois-Norm Margin Bounds and Constructive Rational SDP Witnesses)**.** *Let $S = \sum_{i=1}^{k} \sqrt{a_i} = \alpha_0 + \sum_{j=1}^{r_{\mathrm{irr}}} \alpha_j \sqrt{\tilde{d}_j}$ ($\alpha_0 \in \mathbb{Z}_{\geq 0}$, $\alpha_j \in \mathbb{Z}_{>0}$, distinct square-free $\tilde{d}_j > 1$) with Kummer $\mathbb{F}_2$-rank $\rho \leq r_{\mathrm{irr}}$, $E := \mathbb{Q}(\sqrt{\tilde{d}_1}, \ldots, \sqrt{\tilde{d}_{r_{\mathrm{irr}}}})$, and $K \in \mathbb{Z}_{>0}$.*

(a) Explicit universal margin lower bounds: *Whenever $\Delta = S - K \neq 0$, the exact field Galois norm $N_{E/\mathbb{Q}}(S-K) = \prod_{\sigma \in \mathrm{Gal}(E/\mathbb{Q})} \sigma(S-K)$ is a nonzero rational integer ($|N_{E/\mathbb{Q}}(S-K)| \geq 1$), yielding*

$$|\Delta| \;\geq\; (K+S)^{-(2^\rho - 1)}, \tag{2}$$

and on the $(k+2)$-site ruler of Theorem 2(a), the margins satisfy $\mathrm{sep}(Y) \geq (K+S)^{-(2^\rho-1)}$ and $\mathrm{gap}_\star(Y) \geq (2K+2S)^{-(2^\rho-1)}$, depending only on the Kummer rank $\rho \leq r_{\mathrm{irr}} \leq k$.

(b) Constructive rational SDP witnesses and equality dichotomy: *Let $S_{\mathrm{up}} := \alpha_0 + \sum_{j=1}^{r_{\mathrm{irr}}} \alpha_j (\lfloor \sqrt{\tilde{d}_j} \rfloor + 1) \geq S$ and set $q := (2^\rho - 1)\lceil \log_2(K + S_{\mathrm{up}}) \rceil + \lceil \log_2 k \rceil + 1 = O(2^\rho L)$, $D := 2^q$.*

- *If $S < K$, then $x_i = p_i/D$ with $p_i := \lfloor D\sqrt{a_i} \rfloor + 1$ satisfies $L_{a_i}(x_i) \succ 0$ strictly for all i and $\sum_{i=1}^{k} x_i < K$, giving an explicit rational witness for [2, Eq. (3)].*
- *If $S > K$, then $x_i = p_i/D$ with $p_i := \lceil D\sqrt{a_i} \rceil - 1$ satisfies $U_{a_i}(x_i) \succ 0$ strictly for all i and $\sum_{i=1}^{k} x_i > K$, giving an explicit rational witness for [2, Eq. (4)].*
- *If $S = K$, the unique real feasible point $x_i = \sqrt{a_i}$ of [2, Eqs. (3)–(4)] is rational if and only if every a_i is a perfect square ($r_{\mathrm{irr}} = \rho = 0$).*

2 Representation-Independent Galois Barrier

Proof of Theorem 1. Part (a). For each Lorentz constraint $\|A_j x + f_j\|_2 \leq g_j^\mathsf{T} x + \eta_j$ $(j = 1, \ldots, m)$, its squared residual $q_j(x) := \|A_j x + f_j\|_2^2 - (g_j^\mathsf{T} x + \eta_j)^2$ is a quadratic polynomial over $\mathbb{Q}$ with constant Hessian $H_j = 2(A_j^\mathsf{T} A_j - g_j g_j^\mathsf{T})$. By hypothesis, $\dim \mathrm{span}\{H_1, \ldots, H_m\} \leq 1$, so there exist a single symmetric rational matrix $Q \in \mathbb{Q}^{N \times N}$ and scalars $\lambda_j \in \mathbb{Q}$ such that $H_j = 2\lambda_j Q$ for all j, whence $q_j(x) = \lambda_j (x^\mathsf{T} Q x) + b_j^\mathsf{T} x + c_j$ with $b_j \in \mathbb{Q}^N, c_j \in \mathbb{Q}$.

Introducing one scalar variable $t \in \mathbb{R}$ constrained by the single rational quadric $t = x^\mathsf{T} Q x$, every squared-residual inequality $q_j(x) \leq 0$ becomes purely linear in (x, t): $\lambda_j t + b_j^\mathsf{T} x + c_j \leq 0$ (Lean 4 Theorem 3), alongside the linear nonnegativity cuts $g_j^\mathsf{T} x + \eta_j \geq 0$. Thus $\mathcal{F}$ is the projection

onto x of $\mathcal{P} \cap \mathcal{Q}$, where $\mathcal{P} \subset \mathbb{R}^{N+1}$ is a rational polyhedron and $\mathcal{Q} = \{(x,t) : x^\mathsf{T} Q x = t\}$ is a single rational quadric.

Let $v^* = \min_{(x,t)\in\mathcal{P}\cap\mathcal{Q}} w^\mathsf{T} x$ (the max case follows by negating w) be attained at a point (x^*, t^*), and let $F \subseteq \mathcal{P}$ be the unique face of $\mathcal{P}$ with $(x^*, t^*) \in \operatorname{relint}(F)$, of dimension $d \geq 0$, parameterized affinely over $\mathbb{Q}$ as $(x(u), t(u)) = (x_0 + Au, t_0 + a^\mathsf{T} u)$ for $u \in \mathbb{R}^d$. Write $g(u) := x(u)^\mathsf{T} Q x(u) - t(u) = u^\mathsf{T} M u + p^\mathsf{T} u + \gamma = 0$ with $M \in \mathbb{Q}^{d\times d}$ symmetric, $p \in \mathbb{Q}^d$, $\gamma \in \mathbb{Q}$, and objective $w^\mathsf{T} x(u) = w_0 + c^\mathsf{T} u$ ($c \in \mathbb{Q}^d$).

- If $d = 0$, $c = 0$, or $M = 0$, then either $w^\mathsf{T} x$ is constant on F or $g(u) = p^\mathsf{T} u + \gamma = 0$ is affine so $F \cap \mathcal{Q}$ is a rational polyhedron. Every finite attained extreme value of a rational linear functional on a rational polyhedron is rational, so $v^* \in \mathbb{Q}$ (degree $1 \leq 2$).

- Suppose now $d \geq 1$, $c \neq 0$, and $M \neq 0$. Decompose $\mathbb{R}^d = R \oplus K$ orthogonally over $\mathbb{Q}$, where $K := \ker(M)$ and $R := K^\perp$ (so $M|_R$ is invertible over $\mathbb{Q}$), and split $u = u_R + u_K$, $p = p_R + p_K$, $c = c_R + c_K$. At any singular point of $g(u) = 0$ ($\nabla g(u^*) = 2Mu^* + p = 0$), we have $p_K = 0$ and $u_R^* = -\frac{1}{2}(M|_R)^{-1} p_R \in \mathbb{Q}^d$; moreover c_K must vanish (otherwise moving along $v \in K$ with $c_K^\mathsf{T} v < 0$ preserves $g(u^* + \tau v) = g(u^*) = 0$ while strictly decreasing $c^\mathsf{T} u$ inside $\operatorname{relint}(F)$), so $v^* = w_0 + c_R^\mathsf{T} u_R^* \in \mathbb{Q}$. At a smooth stationary point $u^* \in \operatorname{relint}(F)$ ($\nabla g(u^*) \neq 0$) of $c^\mathsf{T} u$ subject to $g(u) = 0$, the Lagrange condition gives $c = \lambda \nabla g(u^*)$ for some $\lambda \in \mathbb{R} \setminus \{0\}$ (since $c \neq 0$). Setting $\mu := 1/\lambda \neq 0$ yields $2Mu_R^* + p_R = \mu c_R$ and $p_K = \mu c_K$. If $p_K \neq 0$, then c_K is a nonzero rational multiple of p_K, fixing $\mu = \mu_0 \in \mathbb{Q}$ uniquely; hence $u_R^* = \frac{1}{2}(M|_R)^{-1}(\mu_0 c_R - p_R) \in \mathbb{Q}^d$, and $g(u^*) = 0$ fixes $p_K^\mathsf{T} u_K^* = \mu_0 c_K^\mathsf{T} u_K^* \in \mathbb{Q}$, giving $v^* \in \mathbb{Q}$. If $p_K = 0$, then $\mu c_K = 0$ with $\mu \neq 0$ immediately forces $c_K = 0$, and $u_R^*(\mu) = \frac{1}{2}(M|_R)^{-1}(\mu c_R - p_R)$ yields

$$v^* \;=\; \Big(w_0 - \tfrac{1}{2} c_R^\mathsf{T} (M|_R)^{-1} p_R\Big) + 2\alpha\mu, \qquad g(u_R^*(\mu)) \;=\; \alpha\mu^2 + \delta \;=\; 0,$$

  where $\alpha := \frac{1}{4} c_R^\mathsf{T} (M|_R)^{-1} c_R \in \mathbb{Q}$ and $\delta := \gamma - \frac{1}{4} p_R^\mathsf{T} (M|_R)^{-1} p_R \in \mathbb{Q}$. Even when $M|_R$ is indefinite and $\alpha = 0$, the term $2\alpha\mu$ vanishes identically, giving $v^* = w_0 - \frac{1}{2} c_R^\mathsf{T} (M|_R)^{-1} p_R \in \mathbb{Q}$ directly! When $\alpha \neq 0$, completing the square (Lean 4 Theorem 4, `cert15`) gives $(2\alpha\mu)^2 = -4\alpha\delta \in \mathbb{Q}$, so $v^* \in \mathbb{Q}(\sqrt{-4\alpha\delta})$ has algebraic degree at most 2 over $\mathbb{Q}$.

Parts (b)–(c). By Kummer theory, $E = \mathbb{Q}(\sqrt{\tilde{d}_1}, \ldots, \sqrt{\tilde{d}_{r_{\mathrm{irr}}}})$ has degree $[E : \mathbb{Q}] = 2^\rho$ and Galois group $\mathrm{Gal}(E/\mathbb{Q}) \cong \{\pm 1\}^\rho$, acting on each $\sqrt{\tilde{d}_j}$ by a character $\chi_j : \mathrm{Gal}(E/\mathbb{Q}) \to \{\pm 1\}$. Any two distinct automorphisms $\sigma \neq \sigma' \in \mathrm{Gal}(E/\mathbb{Q})$ disagree on at least one generator $\sqrt{\tilde{d}_j}$, so $\sigma(S) - \sigma'(S) = \sum_{j=1}^{r_{\mathrm{irr}}} (\chi_j(\sigma) - \chi_j(\sigma'))\alpha_j \sqrt{\tilde{d}_j}$ is a nonzero $\mathbb{Q}$-linear combination of distinct square-free radicals ($\alpha_j > 0$), hence nonzero by Besicovitch's theorem [1]. Thus S has 2^ρ distinct Galois conjugates and $[\mathbb{Q}(S) : \mathbb{Q}] = 2^\rho$.

Moreover, $\rho \leq 1 \iff r_{\mathrm{irr}} \leq 1$: if $r_{\mathrm{irr}} \geq 2$, then the subgroup $G := \mathrm{span}_{\mathbb{F}_2}\{[\tilde{d}_1], \ldots, [\tilde{d}_{r_{\mathrm{irr}}}]\} \subseteq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ contains the three distinct elements $\{1, [\tilde{d}_1], [\tilde{d}_2]\}$, forcing $|G| = 2^\rho \geq 4$ and hence $\rho \geq 2$ and $[\mathbb{Q}(S) : \mathbb{Q}] = 2^\rho \geq 4 > 2$ (Lean 4 Theorem 1; concretely for $\sqrt{2} + \sqrt{3}$, $x^4 - 10x^2 + 1$ is constructively irreducible over $\mathbb{Q}$, Lean 4 Theorem 2, `cert01`). Conversely, when $r_{\mathrm{irr}} \leq 1$, $S = \alpha_0 + \alpha_1 \sqrt{\tilde{d}_1}$ requires at most one 2×2 block $L_{\tilde{d}_1}(x)$ together with the linear shift α_0 (Lean 4 Theorem 5, `cert02`), whose Hessian span has dimension ≤ 1 and attains S as $\min(\alpha_0 + \alpha_1 x)$ subject to $L_{\tilde{d}_1}(x) \succeq 0$. □

Remark 2.1 (Multiplicative dependencies and rational summands). Perfect-square radicands ($d_i = 1$) contribute only a rational shift α_0 without changing $\mathbb{Q}(S)$. Multiplicatively dependent square-free radicands strictly lower the Kummer rank $\rho < r_{\mathrm{irr}}$: for $S = \sqrt{2} + \sqrt{3} + \sqrt{6}$, $r_{\mathrm{irr}} = 3$ yet $\sqrt{6} = \sqrt{2}\sqrt{3}$ gives $\rho = 2$ and $[\mathbb{Q}(S) : \mathbb{Q}] = 4 < 8$ (exact minimal polynomial $x^4 - 22x^2 - 48x - 23$, `cert10`). Because $\rho \geq 2 \iff r_{\mathrm{irr}} \geq 2$, the representation barrier in Theorem 1(c) still holds for every $r_{\mathrm{irr}} \geq 2$, while the margin and SDP witness exponents in Theorem 3 sharpen exponentially from $2^{r_{\mathrm{irr}}} - 1$ to $2^\rho - 1$.

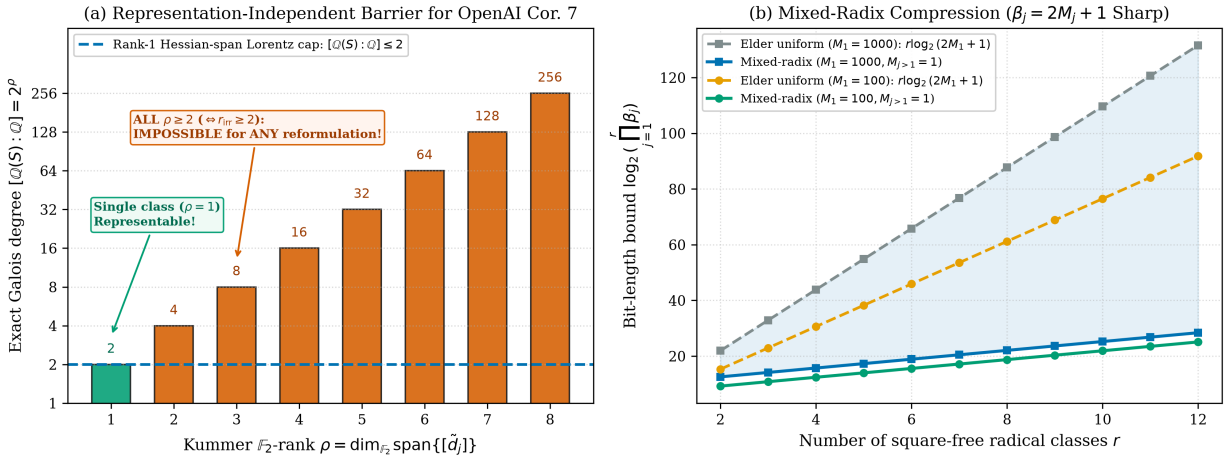

Figure 1: (a) Representation-independent Galois barrier for OpenAI Corollary 7: every rank-1-Hessian-span Lorentz system has boundary algebraic degree ≤ 2, whereas Kummer rank $\rho \geq 2$ ($\iff r_{\mathrm{irr}} \geq 2$) enforces $[\mathbb{Q}(S) : \mathbb{Q}] = 2^\rho \geq 4$. (b) Per-coordinate mixed-radix Freiman bit-length upper bound $\log_2(\prod_{j=1}^r \beta_j)$ ($\beta_j = 2M_j + 1$) versus Elder's uniform base $(2M+1)^r$.

3 Optimal $(k+2)$-Site Ruler and Sharp Mixed-Radix Compression

Proof of Theorem 2. Part (a). Construct the $(k+2)$-site ruler $X = (0, \sqrt{a_1}, \sqrt{a_1}+\sqrt{a_2}, \ldots, S, S+K)$ with consecutive gaps $(\sqrt{a_1}, \ldots, \sqrt{a_k}, K)$ and distance multiset $Y = \mathrm{dist}(X)$ of size $\binom{k+2}{2} = \binom{k+3}{2} - (k+2)$ (Lean 4 Theorem 7, `cert04`). Both S and K occur as intervals in Y; when $\Delta = S - K \neq 0$, they are distinct labels, giving $\mathrm{sep}(Y) \leq |S - K| = |\Delta|$. For $\mathrm{gap}_\star(Y)$:

- If $k = 1$, $Y = \{\sqrt{a_1}, K, \sqrt{a_1}+K\}$. Using the repeated-label triple $(K, K, \sqrt{a_1}+K)$ (explicitly permitted in [2, Eq. (1)], in contrast to Elder's $(k+3)$-site ruler which exhibits a three-distinct-label triple $(S, B, K+B)$ even at $k = 1$), $|K + K - (\sqrt{a_1} + K)| = |K - \sqrt{a_1}| = |\Delta|$ (Lean 4 Theorem 6).
- If $k \geq 2$, the intervals $\sqrt{a_1}$, $S_{\mathrm{rest}} := \sum_{i=2}^k \sqrt{a_i}$, and K all lie in Y, giving $|\sqrt{a_1} + S_{\mathrm{rest}} - K| = |S - K| = |\Delta|$ (Lean 4 Theorem 6, `cert12`).

Finally, any ruler with k consecutive positive gaps $\sqrt{a_1}, \ldots, \sqrt{a_k}$ uses at least $k+1$ sites, and its pairwise distances are independent of K; exposing an independent gap K (and, for $k = 1$, ensuring $|Y| \geq 2$ so $\mathrm{sep}(Y)$ is defined) therefore requires at least $k+2$ sites, proving strict minimality.

Part (b). Given normalized integer coordinate vectors $w(u) \in \prod_{j=1}^r [0, M_j]$ on the square-free basis as in [2, Theorem 4], set $\beta_j = 2M_j + 1$ and define $f_{\mathrm{mix}}(u)$ by (1). By structural induction on r, f_{mix} is unconditionally additive on coordinate-wise sums (Lean 4 Theorem 8): $f_{\mathrm{mix}}(w(u) + w(v)) = f_{\mathrm{mix}}(u) + f_{\mathrm{mix}}(v)$. Since $0 \leq w_j(u) + w_j(v) \leq 2M_j < \beta_j$ and $0 \leq w_j(w) \leq M_j < \beta_j$ at every coordinate j, carry-free uniqueness of mixed-radix digits (Lean 4 Theorem 9) proves injectivity and the exact Freiman equivalence $u + v = w \iff f_{\mathrm{mix}}(u) + f_{\mathrm{mix}}(v) = f_{\mathrm{mix}}(w)$ (`cert05`). The identical argument as in [2, Theorem 4] induces a bijection between normalized realizations, with every encoded label bounded strictly by $\prod_{j=1}^r (2M_j + 1)$ (exponentially smaller than $(2M+1)^r$ whenever $M_1 = M \geq 2$ and $M_{j>1} = 1$; Lean 4 Theorem 11, `cert16`).

For sharp necessity of $\beta_j = 2M_j + 1$ at any lower coordinate $1 \leq j \leq r-1$ (without loss of generality $j = 1$ on $[0, M_1] \times [0, 1]$ with $\beta_2 = 3$; note β_r does not enter (1)), let $1 \leq \beta_1 \leq 2M_1$ be any smaller radix. If $\beta_1 = 1$, injectivity already fails on $(1, 0) \neq (0, 1)$ ($f_{\mathrm{mix}} = 1$). If $2 \leq \beta_1 \leq M_1$, take strictly positive labels $u = (\beta_1 - 1, 0)$, $v = (1, 0)$, $w = (0, 1)$; if $M_1 < \beta_1 \leq 2M_1$, take $u = (M_1, 0)$, $v = (\beta_1 - M_1, 0)$, $w = (0, 1)$. In all cases $u, v, w \in [0, M_1] \times [0, 1]$ and $u + v \neq w$ (second coordinate $0 \neq 1$), yet $f_{\mathrm{mix}}(u) + f_{\mathrm{mix}}(v) = \beta_1 = f_{\mathrm{mix}}(w)$ (Lean 4 Theorem 10, `cert06`). □

4 Galois-Norm Margin Lower Bounds and Rational SDP Witnesses

Proof of Theorem 3. Part (a). Write $S-K=\alpha_0-K+\sum_{j=1}^{r_{\mathrm{irr}}}\alpha_j\sqrt{\tilde{d}_j}\in\mathbb{Z}[\sqrt{\tilde{d}_1},\dots,\sqrt{\tilde{d}_{r_{\mathrm{irr}}}}]$, which is an algebraic integer in the Kummer extension $E=\mathbb{Q}(\sqrt{\tilde{d}_1},\dots,\sqrt{\tilde{d}_{r_{\mathrm{irr}}}})$ of degree 2^ρ. The exact field Galois norm

$$N_{E/\mathbb{Q}}(S-K)\;=\;\prod_{\sigma\in\mathrm{Gal}(E/\mathbb{Q})}\sigma(S-K)$$

is $\mathrm{Gal}(E/\mathbb{Q})$-invariant and an algebraic integer, hence $N_{E/\mathbb{Q}}(S-K)\in\mathbb{Z}$ (for $\rho=r_{\mathrm{irr}}=2$, $N_{E/\mathbb{Q}}(\sqrt{a}+\sqrt{b}-K)=(K^2-a-b)^2-4ab$; Lean 4 Theorem 13, `cert03`). When $\Delta=S-K\neq 0$, no Galois conjugate vanishes (since $\sigma(S-K)=0\implies S-K=\sigma^{-1}(0)=0$), so $|N_{E/\mathbb{Q}}(S-K)|\geq 1$. Because every $\sigma\in\mathrm{Gal}(E/\mathbb{Q})$ changes only the signs of $\sqrt{\tilde{d}_j}$, each of the $2^\rho-1$ non-identity conjugates satisfies $|\sigma(S-K)|\leq K+S$, whence $|\Delta|\geq(K+S)^{-(2^\rho-1)}$ (Lean 4 Theorem 12, `cert07`).

On the $(k+2)$-site ruler of Theorem 2(a), every distance $u\in Y$ is a contiguous subsum of the $k+1$ consecutive gaps $g=(\sqrt{a_1},\dots,\sqrt{a_k},K)$ with indicator vector $\epsilon_u\in\{0,1\}^{k+1}$. Consequently, for any $u,v,w\in Y$, each gap g_ℓ appears in $u-v$ with coefficient $\epsilon_{u,\ell}-\epsilon_{v,\ell}\in\{-1,0,1\}$ and in $u+v-w$ with coefficient $\epsilon_{u,\ell}+\epsilon_{v,\ell}-\epsilon_{w,\ell}\in\{-1,0,1,2\}$ (Lean 4 Theorem 19). Applying any $\sigma\in\mathrm{Gal}(E/\mathbb{Q})$ term-by-term and using $|\sigma(g_\ell)|=g_\ell$ gives $|\sigma(u-v)|\leq\sum_\ell g_\ell=K+S$ and $|\sigma(u+v-w)|\leq 2\sum_\ell g_\ell=2(K+S)$. Since $u-v$ and $u+v-w$ are algebraic integers in E, every nonzero difference or triangle residual has $|N_{E/\mathbb{Q}}|\geq 1$, yielding $\mathrm{sep}(Y)\geq(K+S)^{-(2^\rho-1)}$ and $\mathrm{gap}_\star(Y)\geq(2K+2S)^{-(2^\rho-1)}$.

Part (b). Let $D=2^q$ with $q=(2^\rho-1)\lceil\log_2(K+S_{\mathrm{up}})\rceil+\lceil\log_2 k\rceil+1$. Then $D>k(K+S_{\mathrm{up}})^{2^\rho-1}\geq k/|\Delta|$, so $k<D|\Delta|$.

- If $S<K$ ($|\Delta|=K-S$), set $p_i:=\lfloor D\sqrt{a_i}\rfloor+1$ and $x_i:=p_i/D$. Then $p_i>D\sqrt{a_i}>0$, so $p_i^2>a_iD^2$ and by Sylvester's criterion (Lean 4 Theorem 14), $\det(DL_{a_i}(x_i))=a_i(p_i^2-a_iD^2)>0$, giving $L_{a_i}(x_i)\succ 0$ strictly for every i. Moreover, $p_i\leq D\sqrt{a_i}+1$, so $\sum_{i=1}^k p_i\leq DS+k<D(S+|\Delta|)=DK$, i.e., $\sum_{i=1}^k x_i<K$ strictly (Lean 4 Theorem 15, `cert08`, `cert10`).
- If $S>K$ ($|\Delta|=S-K$), set $p_i:=\lceil D\sqrt{a_i}\rceil-1$ and $x_i:=p_i/D$. Then $0\leq p_i<D\sqrt{a_i}$, so $p_i^2<a_iD^2$ and $\det(DU_{a_i}(x_i))=a_iD^2-p_i^2>0$, giving $U_{a_i}(x_i)\succ 0$ strictly for every i. Moreover, $p_i\geq D\sqrt{a_i}-1$, so $\sum_{i=1}^k p_i\geq DS-k>D(S-|\Delta|)=DK$, i.e., $\sum_{i=1}^k x_i>K$ strictly (Lean 4 Theorem 16, `cert09`, `cert10`, `cert14`).
- If $S=K$, every feasible point of [2, Eq. (3) or Eq. (4)] is forced to the endpoint $x_i=\sqrt{a_i}$; a rational coordinate $x_i=p_i/D$ satisfies $p_i^2=a_iD^2$ (Lean 4 Theorem 20) if and only if a_i is a perfect square (`cert13`).

□

5 Formal Verification and Reproducibility

All twenty algebraic, structural, and Sylvester-criterion theorems underlying Theorems 1–3 are formalized in constructive Lean 4.35.0 (`lean/RadicalTurnpikeSDP.lean`, 20 theorems, zero external dependencies, compiled with `-DwarningAsError=true`, verified via `#print axioms` to use at most `[propext, Quot.sound]` with zero `sorry` and zero `Classical.choice`).

All symbolic Galois norms in $E=\mathbb{Q}(\sqrt{\tilde{d}_1},\dots,\sqrt{\tilde{d}_{r_{\mathrm{irr}}}})$ over an exact $\mathbb{F}_2$-Kummer basis, minimal polynomial irreducibility checks, mixed-radix Freiman bijections and carry-collision witnesses, $(k+2)$-site ruler margins, and exact dyadic rational SDP strict-feasibility certificates are reproduced by the AST-audited zero-floating-point Python verifier `verify_radical_turnpike.py` (in `verification/`), generating 16 SHA-256 certificates with deterministic manifest hash

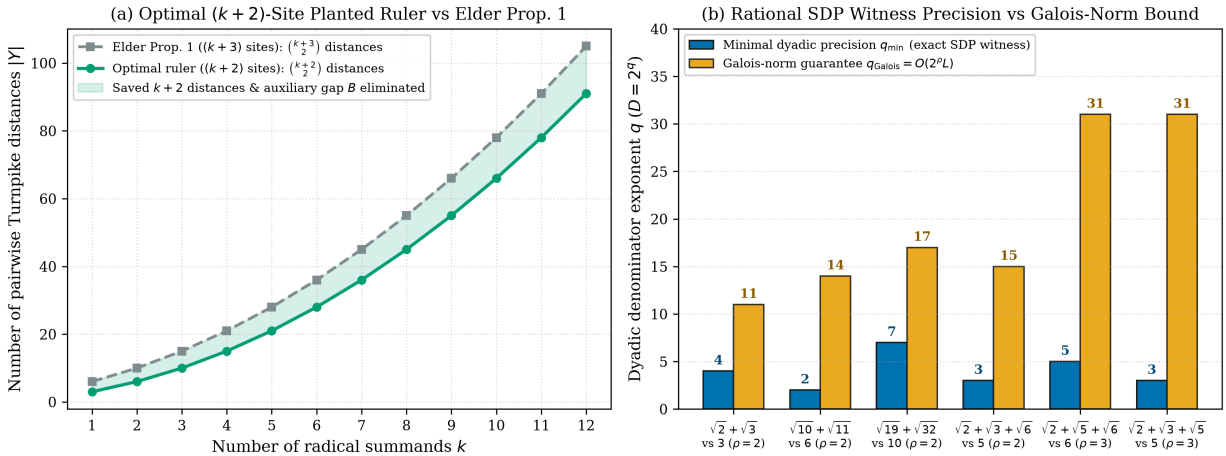

Figure 2: (a) Pairwise distance count of our minimal $(k+2)$-site ruler versus Elder's $(k+3)$-site ruler in [2, Proposition 1], saving $k+2$ distances and eliminating B. (b) Minimal dyadic precision $q_{\min}$ of exact rational SDP witnesses versus the constructive Galois-norm guarantee $q_{\text{Galois}} = O(2^\rho L)$ (Theorem 3(b), loaded directly from `cert10`).

Table 1: Exact symbolic Galois norms $N_{E/\mathbb{Q}}(S-K)$, minimal dyadic precision $q_{\min}$ $(D = 2^{q_{\min}})$, and Theorem 3(b) guarantee q_{Galois} certifying strict rational SDP feasibility in [2, Proposition 5] (`cert03`, `cert08`–`cert10`, `cert14`).

Instance	r_{irr}	ρ	Exact $N_{E/\mathbb{Q}}(S-K)$	Direction	$q_{\min}$	q_{Galois}
$\sqrt{4}+\sqrt{2}$ vs 4	1	1	2	$S < K$ (L_a)	2	5
$\sqrt{2}+\sqrt{3}$ vs 3	2	2	-8	$S > K$ (U_a)	4	11
$\sqrt{10}+\sqrt{11}$ vs 6	2	2	-215	$S > K$ (U_a)	2	14
$\sqrt{19}+\sqrt{32}$ vs 10	2	2	-31	$S > K$ (U_a)	7	17
$\sqrt{2}+\sqrt{5}$ vs 4	2	2	41	$S < K$ (L_a)	2	14
$\sqrt{2}+\sqrt{3}+\sqrt{6}$ vs 5	3	2	-188	$S > K$ (U_a)	3	15
$\sqrt{2}+\sqrt{5}+\sqrt{6}$ vs 6	3	3	-35199	$S > K$ (U_a)	5	31
$\sqrt{2}+\sqrt{3}+\sqrt{5}$ vs 5	3	3	-37799	$S > K$ (U_a)	3	31

`7def50637082a141fe521bc20f0210b445acd3b93b6419e477d281f7cf37397c`,

paired with 56 passing adversarial tests in `tests/test_adversarial.py`.

AI Assistance Disclosure. In accordance with transparent scholarly practice, the author discloses that Google Antigravity assisted with Galois-norm certificate construction, Lean 4 proof engineering, zero-float Python verification scripts, and manuscript typesetting. All mathematical proofs and formal artifacts were mechanically verified and reviewed by the author, who retains sole responsibility.

References

[1] A. S. Besicovitch, *On the linear independence of fractional powers of integers*, J. London Math. Soc. **15** (1940), 3–6.

[2] C. S. Elder, *Square-root comparison, Turnpike, and exact semidefinite feasibility*, arXiv:2611.34535v1, November 2026.

[3] M. X. Goemans, *Semidefinite programming and combinatorial optimization*, Documenta Mathematica, Extra Vol. ICM 1998, III, 657–666.

[4] OpenAI, *Strongly polynomial linear programming*, Preprint, November 24, 2026 edition, Corollaries 6–7, pp. 36–37.