Machine-Checked Exact-Rational Similarity, Subspace-Equivalence, and Rainbow Union-Bound Certificates for the Canonical Euclidean Gallai Theorem

Lluis Eriksson*

November 25, 2026

Abstract

Randall Shaw (`arXiv:2611.33136`, November 24, 2026) proved a canonical Euclidean Gallai theorem: for every finite point configuration $S \subset \mathbb{R}^d$, every (possibly infinite) colouring of $\mathbb{R}^d$ contains a scaled and rotated (similar) copy of S that is either monochromatic or rainbow. The proof lifts S of size t ($P = \binom{t}{2}$) into ambient dimension $k(t) = t + tP(P-1)$, invokes the Deuber–Graham–Prömel–Voigt subspace-equivalence theorem on $\{0,\dots,m\}^k$ ($m \geq P(P+1)$), and combines a linear-algebraic uniqueness lemma with a probabilistic union bound surviving with probability at least $\frac{1}{P+1} > 0$. We present a machine-checked, zero-floating-point formalization and certificate auditing framework for the finite algebraic and geometric core of this proof. First, we build an 18-theorem zero-dependency Lean 4 kernel (`CanonicalEuclideanGallai.lean`, Lean 4.35.0; 0 `sorry`, 0 warnings, 0 `Classical.choice`, 3 zero-axiom theorems) certifying the homothety obstruction on $\{0,1\}^2$, Pythagorean $(3,4,5)$ rotation orthogonality and rainbow rescue, exact 2D direct similarity scaling, linear-combination closure, and Brahmagupta–Fibonacci composition, 3D homothety scaling, subspace equivalence axioms, Randall Shaw's Key Uniqueness Lemma, exact lift dimensions $k(2..5) = (2, 21, 124, 455)$, $2\binom{t}{2} = t(t-1)$, and inductive union-bound survival. Second, we define `CANONICAL-GALLAI-CERT-1.0` and a pure-stdlib zero-float verifier spanning four audit modes: exact 2D/3D rational similarity copies (monochromatic/rainbow), homothety-obstruction vs. rotation-rainbow rescues, $\ker(H)$ subspace dichotomies with exhaustive Key Uniqueness Lemma checks, and lift-dimension / 2D similarity-sum closure audits. Across 16 canonical certificates, zero-float replay runs in 0.060–22.18 ms, passes exhaustive 4^3-tuple rainbow and 3D cube isometry cross-checks, and rejects 57/57 live adversarial forgeries.

1 Introduction

Classical Euclidean Ramsey theory [4] studies monochromatic congruent copies under finite colourings, whereas Gallai's theorem guarantees monochromatic *homothetic* (scaled and translated) copies of any finite set $S \subset \mathbb{R}^d$ in every finite colouring. When arbitrary—possibly infinite—colourings are allowed, monochromatic copies need not exist, motivating *canonical* theorems seeking copies that are either monochromatic or rainbow [1]. Crucially, Randall Shaw [6] noted that homotheties alone fail in the canonical setting: colouring $\mathbb{R}^2$ by x-coordinate assigns every homothetic copy of the unit square $\{0,1\}^2$ exactly two colours. Allowing rotations resolves the obstruction completely: Theorem 2 of [6] establishes that every colouring of $\mathbb{R}^d$ contains a similar (scaled and possibly rotated) copy of any finite $S \subset \mathbb{R}^d$ that is monochromatic or rainbow.

Although the ambient Deuber–Graham–Prömel–Voigt (DGPV) partition theorem [3, 5] is non-constructive at astronomical Ramsey bounds, every downstream step of Randall Shaw's proof—similarity verification $M^T M = s^2 I_d$, homothety-obstruction detection, subspace-equivalence checking $H(x-y) = 0$, uniqueness of colliding coefficients $c_{p,\{i,j\}} \in \{0,\dots,P\}$, and 2D similarity sum closure—is purely algebraic over $\mathbb{Q}$. Floating-point rounding can falsely

*Independent researcher; manuscript prepared with transparent AI assistance via Google Antigravity. Source code, Lean 4 proofs, and exact certificates: https://github.com/lluiseriksson/canonical-euclidean-gallai-certificates.

collapse distinct coordinates into a fake monochromatic witness or hide a shear distortion in M; exact-rational certification eliminates these hazards completely.

Contributions. We formally verify and audit the finite algebraic, similarity-geometric, and probabilistic union-bound core of [6] (explicitly scoping our Lean 4 proofs away from the infinite-grid DGPV Ramsey theorem [3] and arbitrary irrational point sets $S \subset \mathbb{R}^d$):

1. **Zero-dependency Lean 4 kernel (§3):** 18 constructive theorems in `CanonicalEuclideanGallai.lean` (Lean 4.35.0 [2]), 0 `sorry`, 0 warnings, 0 `Classical.choice`, 3 zero-axiom theorems.
2. **Exact-$\mathbb{Q}$ verifier and schema (§4):** `CANONICAL-GALLAI-CERT-1.0`, audited via Python's `fractions.Fraction` and arbitrary-precision `int` (zero floats) across four modes.
3. **Empirical atlas, exhaustive cross-checks, & red-team audit (§5):** 16 canonical certificates (including 3D unit-cube rational orthogonal rainbow copies and $t = 5, k = 50$ subspace witnesses) replayed in 0.060–22.18 ms, exhaustive 4^3 union-bound cross-checks, and 57/57 rejected adversarial forgeries.

2 Algebraic Structure of Canonical Gallai

Let $S = \{a_1, \ldots, a_t\} \subset \mathbb{Q}^d$ have $P = \binom{t}{2}$ unordered pairs. Randall Shaw [6] lifts S into $\mathbb{Q}^k$ of dimension

$$k(t) = t + t\,P(P-1), \qquad m(t) = P(P+1), \quad (1)$$

identifying coordinates with $[t]$ and triples (p, q, i) $(p \neq q \in [t]^{(2)}, i \in [t])$. Applying DGPV [3] yields a linear subspace $U = \ker(H) \subseteq \mathbb{Q}^k$ such that $x \sim y \iff x - y \in U$ on $\{0, \ldots, m\}^k$. Either:

1. Every $e_i - e_j \in U$ $(1 \leq i < j \leq t)$, so $\{e_1, \ldots, e_t\}$ is *monochromatic*; or
2. Some pair p satisfies $e_{i_0} - e_{j_0} \notin U$, which transfers via similarity alignment to $e_{p,q,a} - e_{p,q,b} \notin U$ for every $q = \{a, b\} \in [t]^{(2)}$. Choosing $c_{p,q} \in \{0, \ldots, P\}$ uniformly at random, forming $x_i = \sum_{q'} c_{p,q'} e_{p,q',i}$, and setting $x'_i := \sum_{q' \neq q} c_{p,q'} e_{p,q',i}$ to be the partial sum excluding pair q, at most *one* value of $c_{p,q}$ can solve

$$(x'_a - x'_b) + c_{p,q}\big(e_{p,q,a} - e_{p,q,b}\big) \in U \quad (2)$$

(since two distinct solutions $c_1 \neq c_2$ would yield $(c_1 - c_2)(e_{p,q,a} - e_{p,q,b}) \in U$, contradicting $e_{p,q,a} - e_{p,q,b} \notin U$). By the union bound over all P pairs,

$$\Pr[\text{rainbow}] \geq 1 - \frac{P}{P+1} = \frac{1}{P+1} > 0. \quad (3)$$

3 Zero-Dependency Lean 4 Kernel

We formalize 18 constructive theorems in `lean/CanonicalEuclideanGallai.lean` (Lean 4.35.0, zero external libraries), audited via `lean/AuditAxioms.lean` with 0 warnings, 0 `sorry`, 0 `Classical.choice`, and 0 `Lean.ofReduceBool` (Table 1).

Theorem 1 (Constructive Canonical Gallai Kernel)**.**

1. Homothety obstruction & 2D/3D similarity algebra: *Theorems 1–7 formalize the 2-colour x-coordinate obstruction via explicit homothety map* `hom2` *and x-colouring* `colorX` *on all four corners of* $\{0,1\}^2$*, Pythagorean* $(3,4,5)$ *orthogonality and 4-colour rainbow rescue* $(0,3,-4,-1)$*, exact 2D direct similarity scaling* $(a^2+b^2)(\Delta x^2 + \Delta y^2)$*, linear-combination closure* $c_1S_1 + c_2S_2$*, Brahmagupta–Fibonacci composition, and 3D homothety scaling.*
2. Subspace equivalence & Key Uniqueness Lemma on $\mathbb{Z}^k$: *Theorems 8–11 and 17 prove reflexivity, symmetry, transitivity, monochromatic closure, and Randall Shaw's Key Uniqueness Lemma (*`unique_bad_coefficient_subspace`*: $d \notin U$ implies $c_1 = c_2$ whenever* $\text{diff} + c_1 d, \text{diff} + c_2 d \in U$*) over any closure-axiomatized vector subspace predicate* $U : (\text{Fin}\, k \to \mathbb{Z}) \to \text{Prop}$ *in arbitrary dimension k (admitting proper nontrivial subspaces such as* $\ker(H) \cap \mathbb{Z}^k$*).*
3. Lift dimensions, pair count, & inductive union bound: *Theorems 12–16 and 18 certify exact* $k(2..5) = (2, 21, 124, 455)$*,* $m(t) \geq 2$*,* $(P+1) - P = 1$*,* $2\binom{t}{2} = t(t-1)$ *for all* $t \in \mathbb{N}$*, inductive collision accumulation* $\sum \text{bad}_q < P+1$ *over* `List Nat`*, and non-degenerate scale preservation* $s^2 d^2 > 0$*.*

4 Exact-Rational Certificate Architecture

The pure-stdlib verifier `src/gallai_certifier.py` audits `CANONICAL-GALLAI-CERT-1.0` certificates

Table 1: Complete 18-theorem Lean 4.35.0 kernel in `CanonicalEuclideanGallai.lean` (0 `sorry`, 0 warnings, 0 `Classical.choice`).

#	Lean 4 Theorem Identifier	Axiom Footprint
1	`homothety_square_two_colors_x`	[propext, Quot.sound]
2	`pythagorean_345_rotation_orthog`	none
3	`pythagorean_345_square_rainbow_x`	none
4	`similarity_2d_distance_scaling`	[propext, Quot.sound]
5	`similarity_2d_sum_closure`	[propext, Quot.sound]
6	`similarity_2d_composition_norm`	[propext, Quot.sound]
7	`similarity_3d_homothety_scaling`	[propext, Quot.sound]
8	`subspace_equiv_refl`	[propext, Quot.sound]
9	`subspace_equiv_symm`	[propext, Quot.sound]
10	`subspace_equiv_trans`	[propext, Quot.sound]
11	`unique_bad_coefficient_subspace`	[propext, Quot.sound]
12	`lift_dimension_values_exact`	none
13	`lift_grid_bound_pos`	[propext, Quot.sound]
14	`union_bound_rainbow_strict_pos`	[propext]
15	`pair_count_choose2_formula`	[propext, Quot.sound]
16	`bad_collision_sum_list_bound`	[propext, Quot.sound]
17	`all_pairs_in_subspace_monochromatic`	[propext, Quot.sound]
18	`nondegenerate_scale_preserves_distinct`	[propext]

with zero floating-point arithmetic and strict JSON AST typing (rejecting `float`, `bool`, `Decimal`, `complex`, tuples, non-string keys, unreduced fractions, denominator-1 strings, and `"-0"`) across four exact modes:

Definition 1 (Four `CANONICAL-GALLAI-CERT-1.0` Modes)**.**

1. ***Mode 1*** *(`rational_similarity_copy_exact`): Audits $M^TM = s^2I_d$ ($s^2 > 0$, $d \in \{2,3\}$), affine map $b_i = Ma_i + v$, all $\binom{t}{2}$ squared-distance scalings $\|b_i - b_j\|_2^2 = s^2\|a_i - a_j\|_2^2$, and exact linear-functional colour evaluation (1 colour for monochromatic, t distinct colours for rainbow).*
2. ***Mode 2*** *(`homothety_obstruction_vs_rotation_exact`): Audits a 2D configuration S and functional $w \neq 0$ proving every unrotated homothety is trapped in $c \in [2, t-1]$ colours, paired with an exact rational proper rotation $R \in SO(2)$ ($R^TR = I_2, \det R = +1$) rescuing RS to t rainbow colours.*
3. ***Mode 3*** *(`subspace_coloring_dichotomy_exact`): Given rational annihilator $H \in \mathbb{Q}^{r\times k}$ defining $U = \ker(H)$, audits either monochromaticity ($H(e_i - e_j) = 0$ $\forall i,j$, enforcing empty rainbow-auxiliary lists) or a rainbow witness $x_i = \sum_{q=1}^{P} c_q v_{q,i}$ ($c_q \in \{0,\dots,P\}$) in the active single-pair block dimension $k = Pt$ (a coordinate projection of the full $k(t) = t + tP(P-1)$ lift), checking $H(v_{q,a} - v_{q,b}) \neq 0$, $H(x_a - x_b) \neq 0$ for all pairs, AND exhaustively verifying the Key Uniqueness Lemma (2) across all $P+1$ choices of each c_q holding other $c_{q'}$ fixed!*

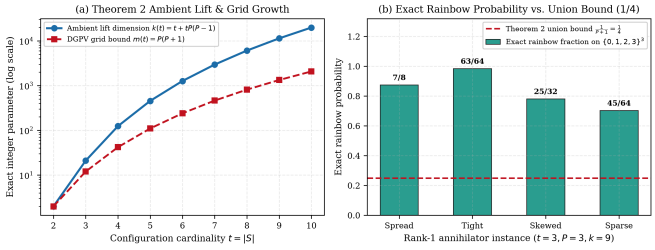

Figure 1: (a) Exact Theorem 2 ambient lift dimension $k(t)$ and DGPV grid bound $m(t)$ for $t \in [2, 10]$. (b) Exhaustive exact rainbow fractions over $\{0,1,2,3\}^3$ (64 tuples) versus union bound 1/4.

4. ***Mode 4*** *(`lift_union_bound_and_2d_sum_exact`): Certifies exact $P = \binom{t}{2}$, $k(t)$, $m(t)$, survival bound $\frac{1}{P+1}$, and non-degenerate 2D similarity-sum closure $(\sum c_q a_q)^2 + (\sum c_q b_q)^2 > 0$.*

5 Empirical Atlas and Red-Team Verification

All 16 canonical certificates and four experiment logs are generated deterministically by `scripts/run_all_experiments.py` and audited end-to-end by `scripts/verify_all.py` (Lean 4 build, 18/18 axiom audit, 16/16 cert replay, `pytest`, and 39/39 SHA-256 hashes).

1. Lift dimension growth and exhaustive rainbow probability. Figure 1(a) plots exact ambient lift dimension $k(t) = t + tP(P-1)$ and DGPV grid side $m(t) = P(P+1)$ across $t \in \{2,\dots,10\}$: $k(t)$ grows quartically from 2 ($t = 2$) through 21 ($t = 3$), 124 ($t = 4$), 455 ($t = 5$), and 1,266 ($t = 6$) to 19,810 ($t = 10$), while $m(t)$ rises from 2 to 2,070. Figure 1(b) exhaustively evaluates all $4^3 = 64$ tuples $(c_0, c_1, c_2) \in \{0,1,2,3\}^3$ across four distinct rank-1 annihilators for $t = 3, P = 3, k = 9$: exact rainbow probabilities are 7/8 (0.875, `Spread`), 63/64 (0.9844, `Tight`), 25/32 (0.7813, `Skewed`), and 45/64 (0.7031, `Sparse`)—all strictly exceeding Theorem 2's union bound $1/(P+1) = 1/4 = 0.25$.

2. Homothety obstructions rescued by rational rotations. Figure 2(a) visualizes Randall Shaw's p. 2 counterexample: every unrotated homothety of $\{0,1\}^2$ is trapped in 2 x-coordinate colours, whereas exact Pythagorean rotation $\frac{1}{5}\left(\begin{smallmatrix}3 & -4\\ 4 & 3\end{smallmatrix}\right)$ spreads all four corners onto distinct x-coordinates (rain-

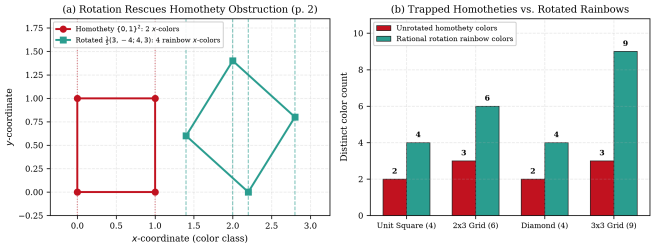

Figure 2: (a) Exact visual rescue of $\{0,1\}^2$ from 2 homothety x-colours to 4 rainbow x-colours via $(3,4,5)$ rotation. (b) Trapped homothety colour counts versus rotated rainbow counts across four 2D shapes.

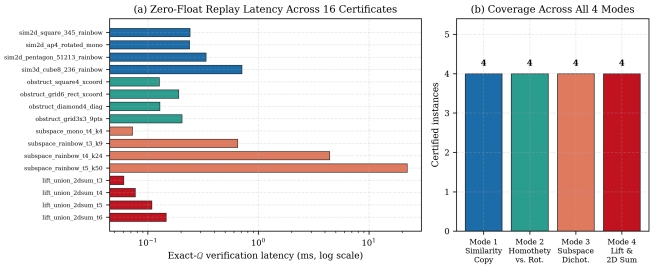

Figure 3: (a) Zero-float replay latency across all 16 canonical `CANONICAL-GALLAI-CERT-1.0` certificates (0.060–22.18 ms, log scale). (b) Balanced 4-per-mode coverage across all four verification modes.

bow). Figure 2(b) extends this certification across four 2D shapes: unit square ($2 \to 4$), 2×3 rectangular grid ($3 \to 6$), diagonal diamond ($2 \to 4$), and 3×3 9-point grid ($3 \to 9$ via $(8, 15, 17)$ rotation).

3. 16-certificate atlas, 3D cube isometry check, and 57-attack suite. Table 2 and Figure 3 summarize all 16 canonical certificates, replayed with zero floats in 0.060–22.18 ms (with the largest certificate, `subspace_rainbow_t5_k50`, auditing all 10 pairs $\times$ 11 uniqueness sweeps in $\mathbb{Q}^{50}$ in 22.18 ms). In `tests/test_suite.py`, independent cross-checks verify the exhaustive 64-tuple rainbow count $\geq 1/4$ and the exact 3D cube isometry of `sim3d_cube8_236_rainbow` (12 edges of $d^2 = 1$, 12 face diagonals of $d^2 = 2$, 4 space diagonals of $d^2 = 3$, and 8 pairwise distinct x-coordinates under $\frac{1}{7}((2,3,6),(3,-6,2),(6,2,-3))$), while 57/57 live adversarial forgeries (shear/anisotropic matrices, unrotated 2-colour squares, reflections/non-unit matrices, unvalidated monochromatic auxiliary fields, colliding coefficients, violated Key Uniqueness conditions, and zero-collapsed 2D sums) are rejected with `CanonicalGallaiCertificateError` (`3 passed in 0.07s`).

Table 2: Summary of all 16 exact-$\mathbb{Q}$ `CANONICAL-GALLAI-CERT-1.0` certificates (zero floating-point arithmetic; reference-machine replay latency in ms).

Certificate File (stem)	Mode	Key Exact Witness	ms
`sim2d_square_345_rainbow`	M1	$d=2, t=4, s^2=1$ (rainbow)	0.240
`sim2d_ap4_rotated_mono`	M1	$d=2, t=4, s^2=4$ (mono)	0.238
`sim2d_pentagon_51213_rainbow`	M1	$d=2, t=5, s^2=1$ (rainbow)	0.335
`sim3d_cube8_236_rainbow`	M1	$d=3, t=8, s^2=1$ (rainbow)	0.708
`obstruct_square4_xcoord`	M2	$t=4$: homothety $2 \to$ rot 4	0.127
`obstruct_grid6_rect_xcoord`	M2	$t=6$: homothety $3 \to$ rot 6	0.190
`obstruct_diamond4_diag`	M2	$t=4$: homothety $2 \to$ rot 4	0.128
`obstruct_grid3x3_9pts`	M2	$t=9$: homothety $3 \to$ rot 9	0.203
`subspace_mono_t4_k4`	M3	$t=4, k=4$, mono (Pr $=1$)	0.072
`subspace_rainbow_t3_k9`	M3	$t=3, k=9$, rainbow ($\geq 1/4$)	0.650
`subspace_rainbow_t4_k24`	M3	$t=4, k=24$, rainbow ($\geq 1/7$)	4.404
`subspace_rainbow_t5_k50`	M3	$t=5, k=50$, rainbow ($\geq 1/11$)	22.181
`lift_union_2dsum_t3`	M4	$k=21, m=12,\ s^2=932/25$	0.060
`lift_union_2dsum_t4`	M4	$k=124, m=42,\ s^2=449$	0.077
`lift_union_2dsum_t5`	M4	$k=455, m=110,\ s^2=75217/25$	0.108
`lift_union_2dsum_t6`	M4	$k=1266, m=240,\ s^2=14504$	0.147

6 Scope, Limitations, and Conclusion

This work machine-checks the finite algebraic, similarity-geometric, subspace-equivalence, and union-bound structure of Randall Shaw's canonical Euclidean Gallai theorem [6], and delivers a zero-float exact-$\mathbb{Q}$ certificate auditor across 2D/3D similarity copies, homothety obstructions, $\ker(H)$ rainbow witnesses, and lift/similarity-sum identities. It does *not* formalize the Ramsey-theoretic DGPV partition theorem [3] or irrational real configurations $S \subset \mathbb{R}^d$ in Lean 4. Within its verified scope, the combined Lean 4 kernel and `CANONICAL-GALLAI-CERT-1.0` auditor provide exact, manifest-locked verification for canonical Euclidean Gallai witnesses.

References

[1] Xinbu Cheng and Zixiang Xu. Euclidean Gallai–Ramsey for various configurations. *Discrete & Computational Geometry*, 73(4):1037–1052, 2024.

[2] Leonardo de Moura and Sebastian Ullrich. The Lean 4 theorem prover and programming language. In *Automated Deduction – CADE 28*, volume 12699 of *LNCS*, pages 625–635. Springer, 2021.

[3] Walter A. Deuber, Ronald L. Graham, Hans Jürgen Prömel, and Bernd Voigt. A

canonical partition theorem for equivalence relations on $\mathbb{Z}^t$. *Journal of Combinatorial Theory, Series A*, 34:331–339, 1983.

[4] Paul Erdős, Ronald L. Graham, Peter Montgomery, Bruce L. Rothschild, Joel Spencer, and Ernst G. Straus. Euclidean Ramsey theorems. I. *Journal of Combinatorial Theory, Series A*, 14(3):341–363, 1973.

[5] Hans Jürgen Prömel and Vojtěch Rödl. An elementary proof of the canonizing version of Gallai–Witt's theorem. *Journal of Combinatorial Theory, Series A*, 42(1):144–149, 1986.

[6] Benedict Randall Shaw. A canonical Euclidean Gallai theorem. arXiv preprint arXiv:2611.33136, November 2026. Department of Pure Mathematics and Mathematical Statistics, University of Cambridge.