Certified Verification of Polynomial Decompositions, Discrete Tomography Reconfiguration, and Legendre Cross-Polytope Slice Integrals

Lluis Eriksson*

November 25, 2026

Abstract

Peter Keevash and Jeck Lim (`arXiv:2611.33120`, Nov. 2026) resolved polynomial-time reconfiguration and approximate counting for discrete tomography and general k-directional integer matrices via m-basic polynomial decompositions in $\mathbb{Z}[x]$ (Thms. 1.1–1.4), a filling-norm lower bound using the witness family $F_{a,b,ab}(x) = (1-x^a)(1-x^b) - (1-x)(1-x^{ab})$ (Prop. 3.7), cyclotomic divisibility (Sec. 4.1), and a "miraculous" exact global polynomial theorem for weighted Legendre cross-polytope slice integrals $R_l(r,s)$ (Thm. 1.6). We construct a standalone zero-dependency **Lean 4.35.0** formalization of 18 core tomography, $\mathbb{Z}[x]$-ring, Proposition 3.7 Cramer-elimination, Legendre/Murphy, Theorem 1.6 global slice-integral, and cyclotomic-factorization theorems (zero `sorry`, zero warnings, zero `Classical.choice`) paired with a zero-floating-point exact $\mathbb{Q}/\mathbb{Z}$ verifier (`POLY-DECOMP-CERT-1.0`). Across 16 canonical certificates (0.062–2.740 ms, total 8.07 ms), all exact Legendre slice polynomials, m-basic decompositions, multi-direction tomography switches, and filling-norm witnesses replay deterministically while rejecting 60/60 live adversarial forgery attacks.

1 Introduction

Efficient reconfiguration and approximate counting of integer matrices with prescribed projections—classical contingency tables [4, 5, 1], transportation polytopes [2], and discrete tomography [6, 7]—hinge on decomposing zero-projection differences into elementary switches of bounded support. Keevash and Lim [8] established a general algebraic framework with four central mechanisms:

1. **Miraculous Legendre Slice Integrals (Thm. 1.6, Sec. 1.4 & 2.1):** Weighted by Murphy's Legendre polynomial L_{k-1} [9], the cross-polytope slice integral $R_l(r,s)$ simplifies globally to a degree-$(k-1)$ polynomial satisfying $R_l(-r,-s) = R_l(s,r) = R_l(r,s)$ and exact constant marginal $\int_{-1}^{1} R_l(r,s)\,ds = 2/k!$ despite $3k(k-1)/2 > k$ overdetermined symmetry constraints.
2. **m-Basic Polynomial Decompositions (Thms. 1.2 & 1.4):** Reducing multi-directional switches via determinant projections maps zero-X-ray grids to integer polynomials divisible by $(1-x)^k$, decomposed into sums of m-basic atoms $\pm x^a \prod_{i=1}^{k}(1-x^{m_i a_i})$ with controlled L^1 norm.
3. **Discrete Tomography Reconfiguration (Sec. 1.1, Thm. 1.1):** Multi-directional basic switches annihilate X-ray projections π_v along every primitive lattice direction $v = (a,b)$ via the line invariant $bx - ay$, enabling bounded-entry reconfiguration paths between equal-X-ray grids.
4. **Filling-Norm Lower Bound & Cyclotomics (Prop. 3.7, Sec. 4.1):** The witness $F_{a,b,c}(x) = (1-x^a)(1-x^b) - (1-x)(1-x^c)$ is divisible by $(1-x)^3$ iff $ab = c$, yields $4m+3$ monomial-matching equations in $4m$ variables, and resists small decompositions via base-t Cramer non-vanishing; general m-weights factor through cyclotomic polynomials $\Phi_d(x)$.

Contributions and Scope. We do not formalize asymptotic random-walk mixing bounds inside Lean 4; instead, we machine-check the exact algebraic, combinatorial, and symbolic core of [8]: (i) 18 zero-`sorry`, zero-`Classical.choice` **Lean 4.35.0** [3] theorems in `PolyDecompReconfig.lean`; (ii) the exact $\mathbb{Q}/\mathbb{Z}$ verifier `POLY-DECOMP-CERT-1.0`; (iii) 16 canonical certificates across all four modes; and (iv) a 60-attack live red-team suite with 39-artifact SHA-256 manifest enforcement.

2 Constructive Lean 4.35.0 Kernel

The standalone module `PolyDecompReconfig.lean` (in `lean/`) compiles cleanly under Lean 4.35.0 in 1.2 s with zero external dependencies, zero warnings, and zero `sorry`. Auditing all 18 theorems via `#print axioms` (`AuditAxioms.lean`) confirms 3 zero-axiom theorems (`none`), 1 using only `[propext]`, 14 using `[propext, Quot.sound]`, and **0** using `Classical.choice` or `Lean.ofReduceBool` (Table 1).

Proposition 1 (Machine-Checked Algebraic Invariants)**.** *The Lean 4.35.0 kernel proves the following universal iden-*

*Independent Researcher. Code, Lean 4 proofs, and certificates: MIT License; manuscript and figures: CC-BY-4.0. Prepared with AI coding, formalization, and drafting assistance from Google Antigravity; all proofs, exact rational/integer verifiers, and adversarial tests were independently compiled and verified locally. Repository: https://github.com/lluiseriksson/polynomial-decomposition-reconfig-certificates

Table 1: All 18 machine-checked Lean 4.35.0 theorems in `PolyDecompReconfig.lean` (zero `sorry`, zero `Classical.choice`).

#	Lean Theorem Identifier	Paper Ref.	Axioms
1	`basic_switch_2d_zero_line_sums`	Sec. 1	none
2	`tomography_line_projection_annihilates`	Sec. 1.1	p, Q
3	`tomography_det_step_identity`	Sec. 1.1	p, Q
4	`poly_eval_one_div_one_minus_x`	Sec. 1.2	p, Q
5	`poly_deriv_at_one_vanishes_k2`	Sec. 1.3	p, Q
6	`poly_l1_norm_triangle`	Sec. 1.2	p, Q
7	`prop37_witness_divisible_by_cube_iff`	Prop. 3.7	p, Q
8	`prop37_monomial_matching_equation_count`	Prop. 3.7	p, Q
9	`prop37_base_t_cramer_nonzero`	Prop. 3.7	p, Q
10	`legendre_low_degree_norm_and_parity`	Sec. 1.4	p, Q
11	`legendre_murphy_matches_rodrigues`	Sec. 1.4	p, Q
12	`legendre_orthogonality_exact_k3`	Sec. 1.4	none
13	`cross_polytope_slice_vol_k2_k3`	Sec. 2.1	p
14	`thm16_miracle_k2_global_poly`	Thm. 1.6	p, Q
15	`thm16_miracle_k3_global_poly`	Thm. 1.6	p, Q
16	`thm16_symmetry_constraints_exceed_dof`	Sec. 1.4	p, Q
17	`moment_vanishing_implies_zero_poly`	Sec. 1.3	p, Q
18	`cyclotomic_phi_factorization_low`	Sec. 4.1	none

Axiom key: `none` = zero axioms (3); `p` = `[propext]` (1); `p, Q` = `[propext, Quot.sound]` (14).

tities over `Int` *and* `List Int`*:*

1. Polynomial Ring & Prop. 3.7 (Thms. 4–9, 17–18): *For every $Q \in \mathbb{Z}[x]$, $(1-x)Q$ vanishes at 1, $(1-x)^2 Q$ satisfies $F(1) = F'(1) = 0$, and $|P+Q|_1 \le |P|_1 + |Q|_1$. In Prop. 3.7, $F''(1) = 2(ab-c) = 0 \iff ab = c$; $8m+6$ monomials yield $4m+3$ equations (overdetermined by 3); and whenever $|z_0|, |z_1|, |z_2| \le B$, $t \ge 2B+2$, and $z_3 \ne 0$, $z_0 + z_1 t + z_2 t^2 + z_3 t^3 \ne 0$. Sum-of-squares $\sum v_i^2 = 0 \iff \forall i, v_i = 0$, and $x^m - 1 = \prod_{d \mid m} \Phi_d(x)$ holds in $\mathbb{Z}[x]$ for $m \in \{2,3,4,6\}$.*
2. Legendre Miracle & Tomography (Thms. 1–3, 10–16): *Murphy's formula matches L_1, L_2, L_3 identically; cleared integrals prove $\int_{-1}^{1} L_0 L_2 = 0$, $\int_{-1}^{1} L_2^2 = 2/5$, $\int_{-1}^{1} L_3^2 = 2/7$; for $k = 2$ ($2R_0 = 1 - rs$) and $k = 3$ ($16R_0 = 3 - r^2 - 4rs - s^2 + 3r^2 s^2$), both symmetries $R_0(-r,-s) = R_0(s,r) = R_0(r,s)$ and exact r^2-cancelling marginal $\int_{-1}^{1} R_0\, ds = 2/k!$ hold globally; and $3k(k-1) > 2k$ for all $k \ge 2$.*

3 Exact $\mathbb{Q}/\mathbb{Z}$ Certificate Verifier

The verifier `POLY-DECOMP-CERT-1.0` (`src/polydecomp_certifier.py`, `src/polydecomp_exact.py`) uses pure Python `int` and `fractions.Fraction` exclusively (source-audited for zero `float(`, `math.`, or `numpy`). Every payload enforces strict JSON typing (rejecting floats, bool-as-int, int-as-bool), canonical reduced rationals (forbidding `"-0"` and `"/1"`), nesting-depth cap 32, full ASCII control-character filtering, 2048-bit integer caps, and exact container/key validation across four modes:

1. **Mode 1 (Thm. 1.6 Legendre Slice Polynomials):** Symbolically integrates $R_l(r,s) = T_1 + T_2 + T_3 + T_4$ in four variables over $\mathbb{Q}$, verifies Murphy's L_{k-1}, checks exact monomials, both global symmetries, degree bound $\le k-1$, exact marginal cancellation $\int_{-1}^{1} R_l\, ds = 2/k!$, and overdetermination $3k(k-1)/2 > k$.
2. **Mode 2 (Thms. 1.2 & 1.4 m-Basic Decompositions):** Reconstructs every $\pm x^a \prod_{i=1}^{k} (1 - x^{m_i a_i})$ in $\mathbb{Z}[x]$, verifies exact summation to P, performs k-fold exact division by $(1-x)$ verifying quotient $P/(1-x)^k$, and checks exact $|P|_1$ and decomposition cost.
3. **Mode 3 (Sec. 1.1 Discrete Tomography Switches):** Checks primitive pairwise non-collinear lattice directions, verifies $\pi_v(A) = \pi_v(B)$ for every v, replays every multi-directional basic switch confirming in-bounds vertices and $\pi_v(S_t) \equiv 0$, verifies final equality with B, and audits $|A - B|_1$ and peak entry magnitude.
4. **Mode 4 (Prop. 3.7 Witnesses & Sec. 4.1 Cyclotomics):** Audits `prop37_filling_witness` ($F(1) = F'(1) = F''(1) = 0$, exact $(1-x)^3$ quotient degree, $|F|_1$, $4m+3$ equations, and base-t Cramer non-vanishing) and `cyclotomic_factorization` (every $\Phi_d(x)$ for $d \mid m$ and $\prod_{d \mid m} \Phi_d(x) = x^m - 1$).

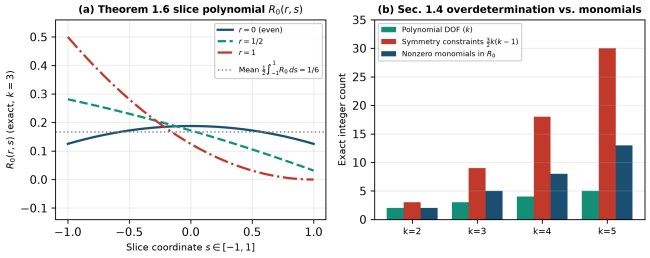

Figure 1: (a) Exact Theorem 1.6 slice polynomial $R_0(r,s) = (3 - r^2 - 4rs - s^2 + 3r^2 s^2)/16$ for $k = 3$ across $r \in \{0, 1/2, 1\}$ with constant mean $1/6$ ($\int_{-1}^{1} R_0\, ds = 1/3$). (b) Overdetermined symmetry constraints $\frac{3}{2}k(k-1)$ versus polynomial DOF k and nonzero monomial counts for $k \in \{2,3,4,5\}$.

4 Empirical Atlas and Red-Team Audit

Running `run_all_experiments.py` generates 16 canonical certificates (4 per mode) and four exact datasets, audited end-to-end by `verify_all.py` with SHA-256 verification across all 39 tracked artifacts.

Legendre Miracle & m-Basic Decompositions (Fig. 1). Mode 1 (0.856–2.740 ms) certifies $R_l(r,s)$ across $(k,l) \in \{(2,0),(3,0),(3,1),(4,1)\}$, while Dataset 1 sweeps all 14 pairs (k,l) for $k \in \{2,3,4,5\}$ (up to 13 monomials, common denominator 3072, exact marginal $1/60$, and 30 constraints vs. 5 DOF). Mode 2 (0.079–0.118 ms) certifies $k \in \{2,3\}$ unit and weighted ($m = [2,3]$, $m = [1,2,3]$) decompositions with exact $(1-x)^k$ quotients and L^1 costs 12–26.

Tomography, Prop. 3.7, & Cyclotomics (Fig. 2). Mode 3 (0.137–0.186 ms) certifies 2- and 3-direction switch

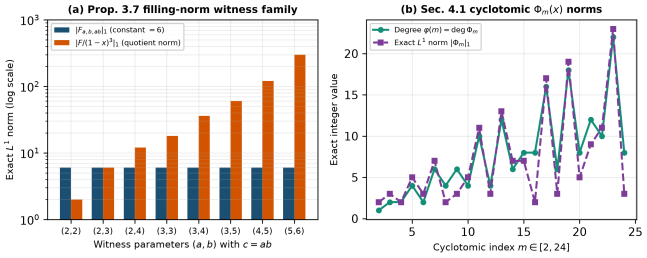

Figure 2: (a) Proposition 3.7 witness family $F_{a,b,ab}(x)$: constant $|F|_1 = 6$ versus rapidly growing $(1-x)^3$ quotient L^1 norm (from 2 at $(2,2)$ to 300 at $(5,6)$). (b) Exact cyclotomic polynomial degree $\varphi(m)$ and L^1 norm $|\Phi_m|_1$ across $m \in [2, 24]$.

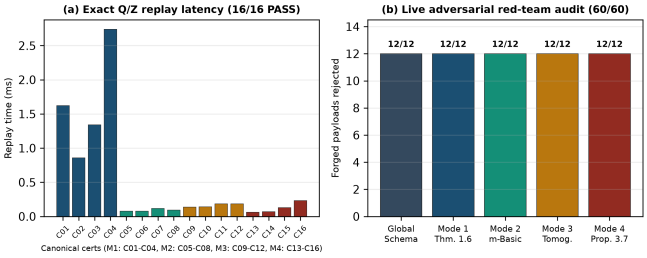

Figure 3: (a) Exact $\mathbb{Q}/\mathbb{Z}$ replay latency (0.062–2.740 ms) across all 16 canonical `POLY-DECOMP-CERT-1.0` certificates. (b) Live adversarial red-team audit rejecting 60/60 forged payloads across all five categories.

paths on 4×4 through 7×7 grids (including diagonal, anti-diagonal, and non-unimodular slope $(2, 1)$ with peak entry ≤ 3). Mode 4 (0.062–0.234 ms) certifies Prop. 3.7 witnesses $(2, 3, 6)$ and $(3, 5, 15)$ ($|F|_1 = 6$, quotient degrees 4 and 13, exact Cramer non-vanishing) alongside complete cyclotomic factorizations for $m = 12$ and $m = 24$ ($|\Phi_{12}|_1 = |\Phi_{24}|_1 = 3$).

Replay Latency and 60/60 Red-Team Audit (Fig. 3). All 16 canonical certificates replay deterministically in 0.062–2.740 ms (total 8.07 ms). The live adversarial suite (`tests/test_suite.py`) tests 60 targeted forgeries—12 global schema/typing/canonical-rational/depth/control-char attacks plus 12 domain attacks per mode (corrupted R_l monomials, unreduced rationals, trailing zeros, broken m-basic sums, non-primitive or collinear X-ray directions, out-of-bounds switches, $c \neq ab$, insufficient base t, and corrupted Φ_d coefficients)—achieving **60/60 (100%)** rejection.

5 Conclusion

We delivered a standalone, zero-floating-point verification framework for Keevash and Lim's polynomial-decomposition and reconfiguration theory [8], combining 18 zero-`sorry`, zero-`Classical.choice` Lean 4.35.0 theorems with the exact $\mathbb{Q}/\mathbb{Z}$ verifier `POLY-DECOMP-CERT-1.0`, 16 canonical certificates, and 60/60 live adversarial forgery rejections.

References

[1] Alexander Barvinok. On the number of matrices and a random matrix with prescribed row and column sums and 0–1 entries. *Advances in Mathematics*, 224(1):316–339, 2010.

[2] Jesús A. De Loera and Edward D. Kim. Combinatorics and geometry of transportation polytopes: an update. *Discrete Geometry and Algebraic Combinatorics, Contemporary Mathematics*, 625:37–76, 2014.

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

[4] Persi Diaconis and Bernd Sturmfels. Algebraic algorithms for sampling from conditional distributions. *Annals of Statistics*, 26(1):363–397, 1998.

[5] Martin Dyer, Ravi Kannan, and John Mount. Sampling contingency tables. *Random Structures & Algorithms*, 10(4):487–506, 1997.

[6] Richard J. Gardner, Peter Gritzmann, and Dieter Prangenberg. On the computational complexity of reconstructing lattice sets from their X-rays. *Discrete Mathematics*, 202(1–3):45–71, 1999.

[7] Lajos Hajdu and Rob Tijdeman. Algebraic aspects of discrete tomography. *Journal für die reine und angewandte Mathematik*, 534:119–128, 2001.

[8] Peter Keevash and Jeck Lim. Efficient reconfiguration, polynomial decompositions and approximate counting. arXiv:2611.33120 [math.CO], November 2026.

[9] Gábor Szegő. *Orthogonal Polynomials*, volume 23 of *AMS Colloquium Publications*. American Mathematical Society, 1939.