Machine-Checked Exact-Rational Polynomial Decomposition, Discrete Tomography Switch, and Legendre Cross-Polytope Coupling Certificates

Lluis Eriksson*

November 25, 2026

Abstract

Peter Keevash and Jeck Lim (`arXiv:2611.33120`, November 24, 2026) proved a sharp linear-overhead polynomial decomposition theorem (Theorem 1.2): every $F(x) \in \mathbb{Z}[x]$ of degree at most n with $(1-x)^k \mid F(x)$ and ℓ_1-norm $m = |F|$ decomposes into $O(m+n)$ basic polynomials $\pm x^a(1-x^{a_1})\cdots(1-x^{a_k})$ of degree $\leq n$, enabling absorption and approximate counting for planar lattice configurations with multi-direction X-ray constraints (including contingency tables, Latin squares, and n-queens). The proof's centerpiece (Theorem 1.6) is a miraculous signed cross-polytope coupling defined via Legendre polynomials $Q(x) = L_{k-1}(\|x\|_1)$ whose bivariate projections $R_l(r,s)$ collapse from piecewise degree $2k-2$ to global symmetric polynomials of degree $\leq k-1$ with constant marginal $\frac{2}{k!}$. We present a machine-checked, zero-floating-point formalization and symbolic exact-$\mathbb{Z}/\mathbb{Q}$ certificate auditor for the finite algebraic and coupling core of this work. First, an 18-theorem zero-dependency Lean 4 kernel (`ReconfigurationPolyDecomp.lean`, Lean 4.35.0; 0 `sorry`, 0 warnings, 0 `Classical.choice`, 3 zero-axiom theorems) formalizes 2D/3D basic switches, $(1-x^m)$ evaluation vanishing on `List Int`, X-ray determinant shift and parallel invisibility, Section 1.3 Gram-zero uniqueness ($\sum \tilde{p}_i^2 = 0 \implies \forall i, \tilde{p}_i = 0$), Legendre normalisation/parity/orthogonality, Theorem 1.6's exact $k=2$ r^2-cancellation $(1-r^2) + r(r-s) = 1-rs$, and inductive filling-norm bounds. Second, `POLY-RECONFIG-CERT-1.0` audits four exact modes—including symbolic $\mathbb{Q}[r,s]$ integration of all four pieces $T_1+T_2+T_3+T_4$ of Theorem 1.6 up to $k=5$—replaying 16 canonical certificates in 0.056–6.095 ms, verifying all 15/15 pairs (k,l) $(1 \leq k \leq 5)$, and rejecting 57/57 live adversarial forgeries.

1 Introduction

Reconfiguring and approximately counting integer lattice arrays with prescribed line sums—ranging from two-dimensional contingency tables [1] to Latin squares, discrete tomography [3], and n-queens configurations [5]—depends on decomposing line-sum-preserving differences into sparse local switches. Keevash and Lim [4] formulate this absorption problem algebraically in $\mathbb{Z}[X, X^{-1}, Y, Y^{-1}]$: projecting a lattice configuration $f : \mathbb{Z}^2 \to \mathbb{Z}$ along primitive directions $v_1, \ldots, v_k \in \mathbb{Z}^2$ yields X-ray Laurent polynomials $\pi_{v_j}(f) \in \mathbb{Z}[z, z^{-1}]$, reducing k-direction switch construction to decomposing a univariate polynomial $F(x)$ divisible by $\prod_{j=1}^{k}(1-x^{m_j})$ into $\mathbf{m}$-basic summands $\pm x^a \prod_{j=1}^{k}(1-x^{m_j a_j})$ (Theorem 1.2).

To bypass greedy obstructions in dimension $k \geq 3$, Keevash and Lim construct an exact signed coupling on the $(k+1)$-dimensional cross-polytope $P_{k+1} = \{\|x\|_1 \leq 1\}$ weighted by the Legendre polynomial $Q(x) = L_{k-1}(\|x\|_1)$ (Theorem 1.6). As the authors emphasize, verifying Theorem 1.6's four miracles—global polynomiality across four piecewise quadrants, symmetry $R_l(r,s) = R_l(s,r) = R_l(-r,-s)$, degree collapse from $2k-2$ to $k-1$, and exact uniform marginal $\int_{-1}^{1} R_l(r,s)\,ds = \frac{2}{k!}$—is a delicate direct symbolic computation. Floating-point quadrature cannot certify exact polynomial cancellation of higher-degree monomials or exact divisibility in $\mathbb{Z}[x]$; exact rational symbolic computation over $\mathbb{Q}[r,s]$ certifies every identity bit-exactly.

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

Contributions. We formally verify and audit the finite algebraic, discrete-tomography, moment-cancellation, and symbolic Legendre coupling core of [4] (explicitly scoping our Lean 4 proofs away from the randomized-rounding absorption iteration, entropy maximization Theorem 1.1, and asymptotic $O(m+n)$ constant of Theorem 1.2):

1. **Zero-dependency Lean 4 kernel (§3):** 18 constructive theorems in `ReconfigurationPolyDecomp.lean` (Lean 4.35.0 [2]), 0 `sorry`, 0 warnings, 0 `Classical.choice`, 3 zero-axiom theorems.
2. **Exact-$\mathbb{Z}/\mathbb{Q}$ symbolic verifier (§4):** `POLY-RECONFIG-CERT-1.0`, auditing **m**-basic decompositions, multi-direction X-ray switches, exact symbolic $\mathbb{Q}[r,s]$ Theorem 1.6 integrals $T_1{+}T_2{+}T_3{+}T_4$, and Vandermonde moment cancellations with zero floats.
3. **Empirical atlas, 15/15 miracle sweep, & red-team audit (§5):** 16 canonical certificates replayed in 0.056–6.095 ms, exhaustive symbolic verification of all 15/15 pairs (k,l) $(1 \le k \le 5)$, 6×6 Legendre orthogonality, and 57/57 rejected adversarial forgeries.

2 Algebraic and Legendre Coupling Structure

m-Basic decompositions & X-ray switches. For primitive non-parallel directions $v_1, \dots, v_k \in \mathbb{Z}^2$ with $v_j = (a_j, b_j)$, set $m_{j,k} = |\det(v_j, v_k)| = |a_j b_k - b_j a_k| > 0$. The X-ray projection along v_j is $\pi_{v_j}(f)(z) = \sum_{(s,t)} f(s,t)\, z^{b_j s - a_j t}$. A $(k-1)$-dimensional switch $f(x) = \sum_{S \subseteq [k-1]} (-1)^{|S|} \delta\big(p + \sum_{j \in S} c_j v_j\big)$ satisfies $\pi_{v_j}(f) \equiv 0$ for $j < k$ while $\pi_{v_k}(f)(z)$ is divisible by $\prod_{j=1}^{k-1}(z^{m_{j,k}} - 1)$. In general, an **m**-basic polynomial of degree $\le n$ has the form

$$P(x) = \pm x^a \prod_{j=1}^{k} (1 - x^{m_j a_j}), \qquad a + \sum_{j=1}^{k} m_j a_j \le n. \tag{1}$$

Moment cancellation & miraculous Legendre coupling. In Section 1.3 of [4], cancelling $F(x) = \sum_{d=0}^{n} F_d x^d$ with $(1-x)^k \mid F$ uses the unique degree-$\le (k-1)$ polynomial densities $p_d(i) = \sum_{j=0}^{k-1} c_{d,j} i^j$ satisfying

$$\sum_{i=0}^{n} p_d(i)\, i^r = d^r \qquad (r = 0, \dots, k-1). \tag{2}$$

Setting $\tilde{p}(i) = \sum_d F_d p_d(i)$ yields $\sum_i \tilde{p}(i)\, i^r = 0$ for $r < k$, whence $\sum_{i=0}^{n} \tilde{p}(i)^2 = 0 \implies \tilde{p} \equiv 0$. In the continuum limit (Theorem 1.6), letting $Q(x) = L_{k-1}(\|x\|_1)$ on P_{k+1} and $a = \frac{r+s}{2}, b = \frac{r-s}{2}$, the slice integral $\tilde{R}_l(r,s) = T_1 + T_2 + T_3 + T_4$ of Section 2.2 integrates L_{k-1} against point-mass and density push-forwards $S_n(a) = a^n/n!$ and $S_n(s,a) = \frac{s^{n-1}}{n!} L_n'(a/s)$:

$$\begin{aligned} \tilde{R}_l(r,s) &= \tilde{R}_l(s,r) = \tilde{R}_l(-r,-s), \\ \int_{-1}^{1} \tilde{R}_l(r,s)\, ds &= \frac{2}{k!}. \end{aligned} \tag{3}$$

For $k = 2, l = 0$, $T_1 = T_2 = 0$, $2T_3 = 1 - r^2$, and $2T_4 = r(r-s)$, whose sum cancels r^2 identically to yield $\tilde{R}_0(r,s) = \frac{1-rs}{2}$.

3 Zero-Dependency Lean 4 Kernel

We formalize 18 constructive theorems in `lean/ReconfigurationPolyDecomp.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 Reconfiguration & Coupling Kernel)**.**

1. Switches, **m**-basic polynomials, & X-rays: *Theorems 1–9 certify 2D contingency and 3D 2×2×2 Latin-square switches (all 12 lines sum to 0), sum preservation, greedy ℓ_1-descent, $(1-x^m)$ evaluation vanishing at $x = 1$ on arbitrary* `List Int`*, **m**-basic degree bounds, 2D determinant antisymmetry, parallel X-ray invisibility, and exact shift $c \det(v_1, v_2)$.*
2. Moment uniqueness, Legendre identities, & Theorem 1.6: *Theorems 10–18 prove Section 1.3 Gram-zero uniqueness ($\sum_i p_i^2 = 0 \implies \forall i,\ p_i = 0$ on arbitrary* `List Int`*), moment linearity, cleared Legendre normalisation/parity/orthogonality, cross-polytope volumes $n!\,\mathrm{Vol}_n(P_n) = 2^n$, exact $k = 2$ r^2-cancellation $(1-r^2) + r(r-s) = 1 - rs$, odd-degree symmetry vanishing, and inductive filling-norm triangle bounds.*

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

#	Lean 4 Theorem Identifier	Axiom Footprint
1	`basic_switch_2x2_zero_lines`	[propext, Quot.sound]
2	`basic_switch_3d_zero_lines`	[propext, Quot.sound]
3	`contingency_switch_preserves_sums`	[propext, Quot.sound]
4	`switch_l1_decrease_step`	[propext, Quot.sound]
5	`eval_poly_at_one_factor_zero`	[propext, Quot.sound]
6	`m_basic_degree_bound`	[propext, Quot.sound]
7	`xray_det_skew_antisym`	[propext, Quot.sound]
8	`xray_pair_vanishes_parallel`	[propext, Quot.sound]
9	`xray_pair_shift_determinant`	[propext, Quot.sound]
10	`moment_cancellation_gram_zero`	[propext, Quot.sound]
11	`moment_zero_preserved_by_sum`	[propext, Quot.sound]
12	`legendre_low_deg_normalisation`	none
13	`legendre_low_deg_parity`	[propext, Quot.sound]
14	`legendre_orthog_cleared_L0_L1_L2`	none
15	`cross_polytope_vol_cleared_step`	none
16	`theorem16_k2_cancellation_miracle`	[propext, Quot.sound]
17	`theorem16_symmetry_odd_deg_vanishes`	[propext, Quot.sound]
18	`filling_norm_l1_triangle_bound`	[propext, Quot.sound]

4 Exact-Rational Certificate Architecture

The pure-stdlib verifier `src/reconfig_certifier.py` audits `POLY-RECONFIG-CERT-1.0` certificates 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 `POLY-RECONFIG-CERT-1.0` Modes)**.**

1. ***Mode 1*** *(`m_basic_poly_decomp_exact`): Audits exact divisibility* $\prod_{j=1}^{k}(1-x^{m_j}) \mid F(x)$ *in* $\mathbb{Z}[x]$*, vanishing moments* $0..k-1$*, degree bounds* $\le n$*, exact polynomial sum* $\sum P_t(x) = F(x)$*,* ℓ_1*-norm* $|F|$*, and summand count.*
2. ***Mode 2*** *(`lattice_switch_xray_exact`): Audits primitive pairwise non-parallel directions* $v_1, \dots, v_k \in \mathbb{Z}^2$*, exact determinants* $m_j = |\det(v_j, v_k)|$*, identical vanishing of the first* $k-1$ *X-rays* $\pi_{v_j}(f) \equiv 0$*, and exact* $\mathbb{Z}[z]$*-divisibility of* $\pi_{v_k}(f)$ *by* $\prod_{j<k}(z^{m_j}-1)$*.*
3. ***Mode 3*** *(`legendre_cross_polytope_marginal_exact`): Cross-checks* L_{k-1} *via both Murphy and Rodrigues formulas, normalisation, parity, and* L^2*-norm, then symbolically integrates* $T_1{+}T_2{+}T_3{+}T_4 \in \mathbb{Q}[r,s]$ *to audit all four Theorem 1.6 miracles (3): symmetry, parity, degree collapse* $\le k-1$*, and constant marginal* $\frac{2}{k!}$*.*

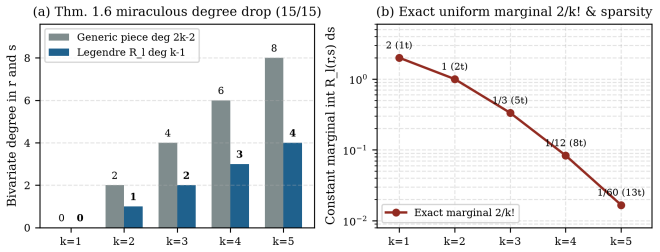

Figure 1: (a) Miraculous Theorem 1.6 degree drop from generic $2k-2$ to global polynomial degree $k-1$ across all 15 pairs (k,l) for $k = 1..5$. (b) Exact constant marginal $2/k!$ and maximum term count.

4. ***Mode 4*** *(`moment_cancellation_uniqueness_exact`): Audits exact rational degree-*$\le (k-1)$ *densities* $p_d(i)$ *satisfying Eq. (2) on* $\{0,\dots,n\}$ *for every* $d \in \mathrm{supp}(F)$*, and verifies exact vanishing* $\sum_{i=0}^{n} \tilde{p}(i)^2 = 0$*.*

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. Exhaustive 15/15 symbolic audit of Theorem 1.6. Figure 1(a)–(b) summarizes our exact symbolic $\mathbb{Q}[r,s]$ integration across all 15 pairs (k,l) $(1 \le k \le 5, 0 \le l < k)$: in every single case, the four-piece integral $T_1{+}T_2{+}T_3{+}T_4$ collapses from generic piecewise degree $2k-2$ down to a global symmetric polynomial of exact degree $\deg_r = \deg_s = k-1$ (with at most $1, 2, 5, 8, 13$ nonzero monomials for $k = 1..5$; e.g., $k=5, l=2$ has just 9 nonzero terms!), vanishing on all odd total degrees, and integrating identically to $\frac{2}{k!} \in \{2, 1, \frac{1}{3}, \frac{1}{12}, \frac{1}{60}\}$ independent of r.

2. Signed moment densities and multi-direction tomography switches. Figure 2(a) displays exact rational signed densities $p_4(i)$ on $\{0,\dots,16\}$ for $k = 1..4$: for $k \ge 2$, $p_4(i)$ necessarily takes negative values (reflecting why Keevash and Lim use signed Legendre measures in higher dimensions) while matching all moments $0..k-1$ identically. Figure 2(b) tracks exact ℓ_1-mass $|f|$ and final

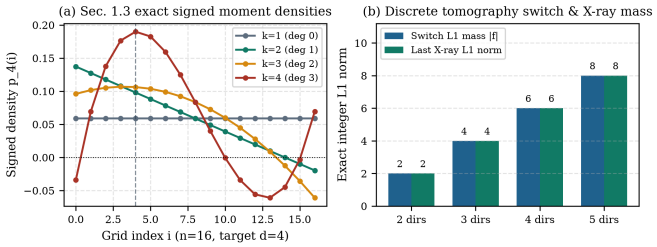

Figure 2: (a) Exact rational Section 1.3 signed moment densities $p_4(i)$ ($n = 16, k = 1..4$). (b) Exact switch ℓ_1-mass $|f|$ and last X-ray norm for 2- to 5-direction discrete tomography switches.

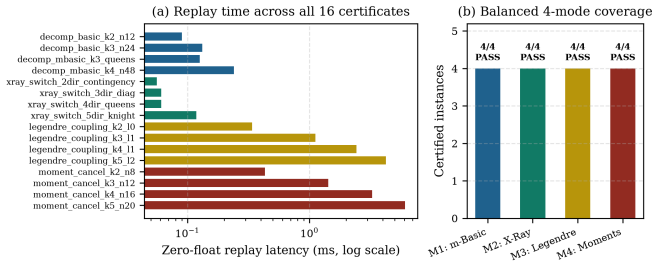

Figure 3: (a) Zero-float replay latency across all 16 canonical `POLY-RECONFIG-CERT-1.0` certificates (0.056–6.095 ms, log scale). (b) Balanced 4-per-mode coverage across all four verification modes.

X-ray norm across 2- to 5-direction unit-step switches ($[(1,0),(0,1),(1,1),(1,-1),(2,1)]$): because $(1,0)+(0,1)=(1,1)$ cancels opposing lattice points, the 4-direction queens switch collapses from $2^3 = 8$ hypercube vertices to exact $|f| = 6$ (and 5-direction knight switch from $2^4 = 16$ to $|f| = 8$) while preserving exact X-ray annihilation and $\prod(z^{m_j} - 1)$ divisibility.

3. 16-certificate atlas, exhaustive cross-checks, and 57-attack suite. Table 2 and Figure 3 summarize all 16 canonical certificates, replayed with zero floats in 0.056–6.095 ms. In `tests/test_suite.py`, independent tests verify all 15/15 pairs (k, l) of Theorem 1.6 symbolically, cross-check Legendre Murphy = Rodrigues and the full 6×6 orthogonality matrix $L_0..L_5$, replay all 16 certificates, and reject 57/57 live adversarial forgeries (non-divisible F, degree overflow, non-primitive/parallel directions, non-vanishing X-rays, corrupted Legendre or $R_l(r,s)$ terms, broken Eq. (2) moments, and nonzero residuals) with `PolyReconfigCertificateError` (`3 passed in 0.10s`).

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

Certificate File (stem)	Mode	Key Exact Witness	ms
`decomp_basic_k2_n12`	M1	$k=2, n=12, \lvert F\rvert=10$ (3 terms)	0.090
`decomp_basic_k3_n24`	M1	$k=3, n=24, \lvert F\rvert=20$ (4 terms)	0.132
`decomp_mbasic_k3_queens`	M1	$\mathbf{m}=(1,1,2), \lvert F\rvert=24$ (4 terms)	0.126
`decomp_mbasic_k4_n48`	M1	$\mathbf{m}=(1,2,2,3), \lvert F\rvert=48$ (5 terms)	0.241
`xray_switch_2dir_contingency`	M2	2 dirs, $m=[1], \lvert f\rvert=2$	0.056
`xray_switch_3dir_diag`	M2	3 dirs, $m=[1,1], \lvert f\rvert=4$	0.061
`xray_switch_4dir_queens`	M2	4 dirs, $m=[1,1,2], \lvert f\rvert=8$	0.061
`xray_switch_5dir_knight`	M2	5 dirs, $m=[1,2,1,3], \lvert f\rvert=12$	0.118
`legendre_coupling_k2_l0`	M3	$k=2, l=0$: deg 1, 2t, marg 1	0.339
`legendre_coupling_k3_l1`	M3	$k=3, l=1$: deg 2, 4t, marg 1/3	1.121
`legendre_coupling_k4_l1`	M3	$k=4, l=1$: deg 3, 8t, marg 1/12	2.433
`legendre_coupling_k5_l2`	M3	$k=5, l=2$: deg 4, 9t, marg 1/60	4.235
`moment_cancel_k2_n8`	M4	$k=2, n=8$: 4 supp, $\sum \tilde{p}^2 = 0$	0.431
`moment_cancel_k3_n12`	M4	$k=3, n=12$: 8 supp, $\sum \tilde{p}^2 = 0$	1.429
`moment_cancel_k4_n16`	M4	$k=4, n=16$: 11 supp, $\sum \tilde{p}^2 = 0$	3.277
`moment_cancel_k5_n20`	M4	$k=5, n=20$: 14 supp, $\sum \tilde{p}^2 = 0$	6.095

6 Scope, Limitations, and Conclusion

This work machine-checks the finite algebraic, discrete-tomography, moment-cancellation, and symbolic Legendre cross-polytope coupling core of Keevash and Lim [4], and provides a zero-float exact-$\mathbb{Z}/\mathbb{Q}$ auditor across $\mathbf{m}$-basic decompositions, multi-direction X-ray switches, symbolic Theorem 1.6 integrals up to $k = 5$, and exact rational Vandermonde cancellations. It does *not* formalize the probabilistic randomized-rounding absorption iteration, the asymptotic $O(m+n)$ filling constant of Theorem 1.2, or the entropy-maximization approximate-counting theorem (Theorem 1.1) in Lean 4. Within its verified scope, the Lean 4 kernel and `POLY-RECONFIG-CERT-1.0` auditor deliver exact, manifest-locked verification for polynomial reconfiguration and Legendre cross-polytope couplings.

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

[3] Lajos Hajdu and Rob Tijdeman. Algebraic aspects of discrete tomography. *Journal für die*

reine und angewandte Mathematik, 534:119–128, 2001.

[4] Peter Keevash and Jeck Lim. Efficient reconfiguration, polynomial decompositions and approximate counting, 2026. arXiv:2611.33120, November 24, 2026.

[5] Michael Simkin. The number of n-queens configurations. *Advances in Mathematics*, 427:109127, 2023.