Exact shell descent and finite-field norm gates in a prescribed-compression chart for Legendre pairs of length 333

Alec Kriebel
with heavy assistance from ChatGPT 5.6 Sol

Research draft prepared 25 July 2026
Not peer reviewed

Abstract

A binary Legendre pair of length 333 would give a Hadamard matrix of order 668. We study a deliberately restricted chart: both sequences are fixed by the order-three multiplier $\langle 10 \rangle$, and their length-37 compression is the prescribed quadratic-character compression proposed for the $p = 37, q = 3$ case of the q^2-uncompression conjecture. Compressing the nine rows modulo three turns each nonzero multiplier class into one of ten Eisenstein profile letters. We prove the resulting length-37 complementary-autocorrelation model is exact, stratify it by the number n_9 of norm-nine letters, and give exact finite classifications. The shells $n_9 = 6, 5, 4, 3$ are empty; the shell $n_9 = 2$ has exactly five orbits, of sizes $24, 12, 12, 12, 24$; and a separate released exhaustive dense-shell census has exactly eighteen compressed-profile orbits at $n_9 = 0$ in its stated characteristic-two/modulo-nine search scope. The complete production manifest, aggregate, and all 729 shard records are archived with this paper. The intermediate shell $n_9 = 1$ remains open.

For the five $n_9 = 2$ orbits, the first labelled placement digit has rank 18 and leaves an affine 36-space over $\mathbb{F}_3$. Exact physical row margins impose six further independent affine equations, after which a complete quadratic-retraction census finds maximum structured retraction dimensions $4, 3, 3, 3, 4$ and no five-form retraction. A parallel census on the eighteen dense profiles finds nine with maximum retraction dimension five and nine with maximum four. Reduction modulo 167 gives a six-factor primitive algebra. An exact meet-in-the-middle audit proves that every physical placement above every shell-two image is a unit in every primitive factor, permitting a ratio-torus normalization.

The resulting torus equations imply three separate pair-resultant norm equalities in $\mathbb{F}^*_{167^3}$. Their character factors have orders 2, 83, and 28057. Complete 3^9 physical slices show strong exact contraction, but a complete margin-conditioned join would still require 5,091,993,547,996 invariant evaluations and, at sixteen bytes per key, about 81.5 TB with target duplication. Thus the norm keys are a genuine exact reduction but not a feasible complete search on the current architecture. No Legendre pair of length 333 and no Hadamard matrix of order 668 is claimed.

Verification and authorship disclaimer. The human author is a complete amateur exploring the limits of AI-assisted mathematics and cannot independently validate the claims in this manuscript. This is an unreviewed research artifact for expert checking, not an established result. Passing the included programs establishes properties of their encoded finite models; it is not peer review and does not by itself establish priority. Large classification claims should be treated as computer-assisted claims whose hypotheses, implementations, certificates, and scope all require independent scrutiny.

1 Introduction and exact scope

A Hadamard matrix of order N is a matrix $H \in \{\pm 1\}^{N\times N}$ satisfying $HH^\top = NI_N$. A standard two-circulant-core construction turns a binary Legendre pair of odd length ℓ into a Hadamard matrix of order $2\ell+2$; see [5, 6, 1]. Thus a Legendre pair of length 333 would yield order 668, the smallest order currently open in the Hadamard existence problem. Eliahou's recent 64-modular construction at this order gives independent motivation for studying the case [4], but the present paper does not modify that matrix.

For a sign sequence $X = (x_j)_{j\in\mathbb{Z}/\ell\mathbb{Z}}$, write

$$\mathrm{PAF}_X(t) = \sum_{j\in\mathbb{Z}/\ell\mathbb{Z}} x_j x_{j+t}.$$

A normalized binary Legendre pair of length ℓ is a pair (A, B) of sign sequences satisfying

$$\sum_j A_j = \sum_j B_j = 1, \qquad \mathrm{PAF}_A(t) + \mathrm{PAF}_B(t) = -2 \quad (t \neq 0). \tag{1}$$

This paper studies only the following chart.

1. Identify
$$\mathbb{Z}/333\mathbb{Z} \simeq \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/37\mathbb{Z}.$$
Both sequences are fixed by the common multiplier subgroup
$$H_{333} = \langle 10\rangle \leq (\mathbb{Z}/333\mathbb{Z})^\times.$$
Its image is trivial modulo 9 and is
$$H = \{1, 10, 26\} \leq \mathbb{F}_{37}^*$$
modulo 37.

2. The compression along the nine-row fibers is prescribed:
$$\begin{aligned} &C(0) = D(0) = 1, \\ &\qquad C(j) = 3\left(\frac{j}{37}\right), \qquad\qquad D(j) = -3\left(\frac{j}{37}\right) \qquad (1 \leq j < 37). \end{aligned} \tag{2}$$
Here $(\frac{\cdot}{37})$ is the quadratic character.

Condition (2) is the $p = 37, q = 3$ instance proposed by Kotsireas, Gallardo-Cava, Gómez, and Gómez-Pérez [7]. It is an informed prescribed-compression conjecture, not a necessary condition for an arbitrary Legendre pair.

The recent paper of Ramos, Hulak, and de Queiroz proves that a common fixed multiplier subgroup for a length-333 Legendre pair must have order at most six [8]. Their table leaves the order-three subgroup $\langle 10\rangle$, labelled ID 3, open. Our chart is a strict subset of that public-open ID 3 family because it additionally imposes (2). Consequently:

$$\boxed{\text{No result here classifies ID 3, unrestricted LP(333), or Hadamard matrices of order 668.}}$$

The symmetry group used below is the restricted order-24 action preserving this normalized profile chart. It is not asserted to be the full Legendre pair equivalence group; for that formal problem see [2]. Generic 9×37 compression, multiplier-orbit search, and decompression also precede this work [3, 7].

Contributions. Within the scope just fixed, the paper records four connected results:

1. an exact Eisenstein profile model and a shell-by-shell finite descent;
2. exact classifications of five two-high and eighteen dense compressed profile orbits;
3. exact labelled lift algebra, physical-margin ranks, and quadratic retraction censuses;
4. a primitive-unit theorem and three separate pair-resultant norm keys, followed by an exact slice experiment and a complete cost gate.

2 The Eisenstein profile model

Let

$$C_j = 2^j H, \qquad 0 \le j < 12,$$

be the twelve nonzero cyclotomic classes in $\mathbb{F}_{37}$. Since 2 is a quadratic nonresidue modulo 37, the prescribed signs alternate with j. An H-invariant sign sequence is represented on each class by a binary word of length nine. After complementing the classes of sum $+3$, every such word is normalized to plus-weight three.

For a normalized word let

$$p = (p_0, p_1, p_2), \qquad p_0 + p_1 + p_2 = 3,$$

where p_s counts its plus signs in rows congruent to s modulo 3. There are ten profiles. Put

$$\omega^2 + \omega + 1 = 0, \qquad z(p) = p_0 + p_1\omega + p_2\omega^2.$$

The ten values are

$$\{0\} \;\cup\; 3\mu_3 \;\cup\; (1-\omega)\mu_6, \tag{3}$$

so one has Eisenstein norm 0, three have norm 9, and six have norm 3.

Let $\varepsilon_j = (-1)^j$. If $p_{A,j}$ and $p_{B,j}$ are the two profiles on C_j, define H-invariant Eisenstein sequences a, b on $\mathbb{F}_{37}$ by

$$\begin{aligned} a(0) &= -1, & a(c) &= -\varepsilon_j z(p_{A,j}) \quad (c \in C_j),\\ b(0) &= 2, & b(c) &= \varepsilon_j z(p_{B,j}) \quad (c \in C_j). \end{aligned} \tag{4}$$

The involution $*$ conjugates Eisenstein coefficients and reverses the group coordinate.

Proposition 1 (Exact profile equivalence)**.** *The three-row compression of the prescribed chart satisfies all compressed Legendre correlation equations if and only if*

$$aa^* + bb^* = 167\,\delta_0 \qquad \text{in } \mathbb{Z}[\omega][\mathbb{F}_{37}]. \tag{5}$$

This is an equivalence, not a relaxation.

Proof. For a compressed binary triple $v = (v_0, v_1, v_2)$ with even pairwise differences, put

$$F(v) = \frac{v_0 + v_1\omega + v_2\omega^2}{2}.$$

If

$$d_h(v,u) = \sum_{r\in\mathbb{Z}/3\mathbb{Z}} v_r u_{r+h},$$

then direct expansion in the basis $1, \omega$ gives

$$4F(v)\overline{F(u)} = (d_0 - d_1) + (d_2 - d_1)\omega. \tag{6}$$

Summing (6) over the 37 columns converts the nontrivial row-Fourier channel into the correlation of (4). The trivial row-Fourier channel is already fixed by (2); its three binary row correlations sum to 650 at zero and -18 away from zero. The resulting linear transformation is invertible over $\mathbb{Z}$. Its required targets are $(662, -6, -6)$ at zero and $(-6, -6, -6)$ away from zero, which are equivalent to (5). The distinguished zero-column triples give $a(0) = -1$ and $b(0) = 2$. □

Reversal leaves one real origin equation and six Eisenstein equations, or thirteen independent integer conditions. The exact row-sum catalog in the other direction contains 1,756 words. After compression to the three row residues it gives 22 aggregate states. At the trivial additive character their norm pairs are

$(\lvert a(1)\rvert^2, \lvert b(1)\rvert^2)$	$(19,148)$	$(28,139)$	$(64,103)$	$(91,76)$	$(100,67)$	$(163,4)$
multiplicity	4	4	2	8	2	2.

Every pair sums to 167.

2.1 Energy shells

Let n_d count the number of the 24 nonzero-class profile letters with Eisenstein norm d. The origin equation in (5) gives

$$n_0 + n_3 + n_9 = 24, \qquad 3n_3 + 9n_9 = 54.$$

Writing $h = n_9$ only inside this paper, the seven sectors are

$$(n_9, n_3, n_0) = (h, 18 - 3h, 6 + 2h), \qquad 0 \le h \le 6. \tag{7}$$

To avoid conflict with the multiplier-image notation in [8], we call these the n_9 shells rather than the "h-shells."

The local congruence modulo 3 on an opposite-class quartet is

$$\overline{z(p_{A,j})} + z(p_{A,j+6}) \equiv \overline{z(p_{B,j})} + z(p_{B,j+6}) \pmod 3. \tag{8}$$

Exactly 3,334 of the 10^4 ordered quartets satisfy (8). This is a useful exact sieve, but it leaves 3334^6 local assignments before global correlations.

3 Exact shell descent

Put $\lambda = 1 - \omega$. The alphabet (3) can be written uniquely as

$$0, \qquad \sigma\lambda\omega^u \ (\sigma \in \{\pm 1\},\, u \in \mathbb{F}_3), \qquad 3\omega^v \ (v \in \mathbb{F}_3).$$

We call the norm-three letters medium and the norm-nine letters high. After fixing a signed medium skeleton, each remaining medium-phase change and each high insertion is divisible by λ^2, which is associated to 3. If m is the base word and δ_i are the one-slot changes, bilinearity gives the lossless quotient identity

$$D\left(m + \sum_i \delta_i\right) \equiv D(m) + \sum_i \big(D(m+\delta_i) - D(m)\big) \pmod 9. \tag{9}$$

All omitted cross products are divisible by 9. One digit farther, writing $\delta_i = 3\eta_i$, the exact identity is

$$D\left(m + \sum_i \delta_i\right) \equiv D(m) + \sum_i \Delta_i + 9 \sum_{i<k} (\eta_i \eta_k^* + \eta_k \eta_i^*) \pmod{27}. \tag{10}$$

Thus the first descent is an additive signature join and the next is a quadratic correction, not a heuristic linearization.

Computer-assisted theorem 2 (Sparse shell descent)**.** *In the exact profile model* (5)*, subject to the* 22 *aggregate targets:*

1. *the shells* $n_9 = 6, 5, 4, 3$ *contain no solution;*

2. *the shell* $n_9 = 2$ *contains exactly five orbits under the restricted order-*24 *profile action; their orbit sizes are*
$$24,\ 12,\ 12,\ 12,\ 24.$$

Certificate and exhaustion proof. Each shell uses its complete legal local support partitions, the exact aggregate target, the lossless identities (9)–(10), and detached replay of all 37 Eisenstein correlations. The finite counters are:

n_9	outer objects	mod-9/aggregate	mod-27	exact
6	288 assignments	288	–	0
5	34,634,136 local/aggregate	552	–	0
4	27,468,720 oriented frames	345,984	–	0
3	908,800 signed skeletons	479,850	2	0
2	14,715,744 raw skeletons	10,201,038	61	5

For $n_9 = 3$, an independent characteristic-37 cubic moment rejects the two modulo-27 points; detached exact replay also rejects them. For $n_9 = 2$, the enumerator processes 617,788 canonical skeletons across the seven possible support partitions

$$222222,\ 332220,\ 333300,\ 422220,\ 433200,\ 442200,\ 444000.$$

The five exact hits lie on distinct canonical skeletons. Their stabilizers agree with their skeleton stabilizers, and orbit expansion gives 84 pairwise distinct images. The independent Python replay reconstructs all correlations, aggregate targets, shell counts, stabilizers, and orbits from the detached certificate. File and semantic hashes are recorded in Section 10. □

The five representatives are as follows. A target is written in the four-coordinate aggregate convention of the exact row-sum catalog.

label	partition	target	orbit	stabilizer
`h2-222222-0`	222222	$(2,-2,-2,2)$	24	1
`h2-422220-0`	422220	$(2,-2,-2,2)$	12	2
`h2-422220-1`	422220	$(2,-2,-4,-2)$	12	2
`h2-422220-2`	422220	$(4,2,-2,2)$	12	2
`h2-422220-3`	422220	$(-3,0,-3,-3)$	24	1

The complete profile vectors appear in Appendix A.

Remark 3. Theorem 2 is a profile-level theorem. Its five objects solve (5); they are not labelled sign sequences of length 333. Each representative still has 54 physical placement trits, hence a raw placement space of size 3^{54}.

4 The dense $n_9 = 0$ classification

The remaining dense sectors are $n_9 = 1$ and $n_9 = 0$. The former remains unclassified. The latter has 18 medium and 6 zero letters. A strict 729-shard production census was run in the `char2_mod9_intersection` scope, followed by exact correlation replay.

Computer-assisted theorem 4 (Released dense compressed-profile census)**.** *Inside the released exhaustive dense $n_9 = 0$ compressed-profile census scope, there are exactly eighteen canonical exact orbits under*

$$G = C_6 \times C_{2,A}^* \times C_{2,B}^*.$$

Twelve orbits have size 24 *and six have size* 12*, for* 360 *labelled profile images in total.*

The compact orbit ledger is:

orbit	digest	target	$\|Gx\|$	orbit	digest	target	$\|Gx\|$
01	$81065cf5$	$(2,-2,-4,-2)$	12	10	$e5d4ba0c$	$(1,-1,4,2)$	24
02	$64ef0d58$	$(4,-1,0,0)$	24	11	$533a4ccf$	$(2,-2,-2,2)$	24
03	$c90c2887$	$(-3,0,0,3)$	24	12	$5a8fa4d6$	$(-3,-3,-2,2)$	24
04	$3fcb4172$	$(2,1,2,-2)$	24	13	$e6860f05$	$(2,-2,-2,2)$	24
05	$7395e771$	$(-3,0,0,3)$	24	14	$5b160dfa$	$(4,2,-2,2)$	12
06	$6e45edfb$	$(0,3,-4,-2)$	24	15	$fdb6a5c8$	$(4,2,-2,2)$	12
07	$86b13a03$	$(4,2,-4,-2)$	12	16	$889b022b$	$(-3,0,-3,-3)$	24
08	$19d54815$	$(5,1,0,0)$	24	17	$63f0e12d$	$(-3,0,-3,-3)$	24
09	$aa1c4c14$	$(4,2,-4,-2)$	12	18	$ac3483a0$	$(4,2,-2,2)$	12

Certificate, released shards, and provenance proof. The production run completed all 729 prefix shards. The checkpoint release contains every shard record, the production manifest, the pinned helper, the strict aggregate, and the production and replay sources. A fresh-directory strict aggregation of the released records reproduces the aggregate byte for byte, with SHA-256

`3bccde87f456bfcd2f0c3da6ac8cf9cb3635538e831a95951003068ae87cae86`.

Its frozen counters are

raw decorations	47,730,304
canonical decorations processed	1,999,128
weighted primitive-flag leaves	25,368,365,895,696
characteristic-two/modulo-nine intersections	19,986
post-modulo-nine lambda hits	64
canonical exact hits	18
weighted exact hits	360

The strict aggregator validates completion and provenance on every shard and deterministically recovers the eighteen retained canonical orbits. The detached verifier reconstructs the twelve cyclotomic classes, expands all eighteen representatives to physical length-37 Eisenstein words, checks all 666 correlations, reconstructs and verifies the order-24 action, recomputes stabilizers and orbit sizes, and proves the eighteen orbits disjoint. It also pins the aggregate, manifest, source, binary, record, orbit, and physical-replay hashes. It does not rerun the enormous production enumeration. Thus exactness and inequivalence of the frozen representatives are independently replayed, while exhaustive coverage is supported by the complete released shard ledger and its strict aggregation. A fresh rerun or reimplementation of the expensive producer remains the strongest independent replication. □

Remark 5 (Dense scope). Theorem 4 classifies exact compressed profiles inside the stated dense census. It does not classify all labelled placements over those profiles, all uncompressions of (2), public ID 3, or arbitrary Legendre pairs. The missing $n_9 = 1$ shell prevents even a complete classification of the compressed profile model.

4.1 A six-dimensional quadratic algebra

The first genuinely quadratic λ-adic response in the two dense sectors has a useful closed form. For one channel let $x_0, \ldots, x_{11}$ be the medium phase corrections, and let $t_j \in C_j$ for $0 \le j < 6$. Define

$$q_j(x) = \sum_{c \in \mathbb{F}_{37}^*} x(c + t_j)x(c) \quad \text{over } \mathbb{F}_3,$$

and let M_j be its polar matrix on the twelve class coordinates.

Proposition 6 (Dense pencil algebra)**.** *The six symmetric matrices $M_0, \ldots, M_5$ are independent, commute, and are closed under multiplication. Their algebra is*

$$\mathrm{span}_{\mathbb{F}_3}\{M_0, \ldots, M_5\} \simeq \mathbb{F}_{27} \times \mathbb{F}_{27}.$$

Moreover

$$M_0 + \cdots + M_5 = 2I_{12}.$$

Among the 364 *projective nonzero pencils,* 338 *have rank* 12 *and* 26 *have rank* 6*.*

Proof. Exact cyclotomic transition counts show the matrices commute, are independent, and satisfy the displayed identity. The algebra has exactly four idempotents:

$$0, \quad (2,0,2,0,2,0), \quad (0,2,0,2,0,2), \quad (2,2,2,2,2,2).$$

The two nontrivial principal ideals are three-dimensional over $\mathbb{F}_3$, contain 27 elements, and have no zero divisors; each is therefore $\mathbb{F}_{27}$. A projective pencil supported in one component has rank six. There are $13+13=26$ such points. Every other nonzero pencil has both components nonzero and rank twelve, giving $364-26=338$. □

Exact Gauss-sum bounds show the all-ones pencil is not an obstruction after the actual affine local and aggregate rows: in the $n_9=1$ sector every right-hand side has at least 2,025 points on every nonempty fiber, and in the $n_9=0$ sector at least 54,675. Its value is therefore compression of the six-coordinate quadratic count, not exclusion.

5 Labelled phase lifting and quadratic retractions

For a profile $p=(p_0,p_1,p_2)$, each residue fiber of size one or two has one placement trit; fibers of size zero or three are fixed. The identity

$$\#\{\text{active fibers of } p\} = 3 - \frac{\mathrm{N}(z(p))}{3}$$

and total profile norm 54 show that every profile solution has exactly 54 active placement trits.

Writing a row coordinate as $r=s+3q$, define the sparse Eisenstein fiber sequence

$$U_s(c) = \sum_{q\in\mathbb{Z}/3\mathbb{Z}} X(s+3q,c)\omega^q.$$

Each $U_s(c)$ is zero or an Eisenstein unit. If $\alpha=\zeta_9$, the primitive-nine recombination is

$$W = U_0 + \alpha U_1 + \alpha^2 U_2. \tag{11}$$

Expansion in the basis $1,\alpha,\alpha^2$ shows that the full primitive-nine condition consists of a six-sequence diagonal equation and one directed cross-fiber equation; the formally third equation is the adjoint of the second. There are 39 independent integer equations, of which 36 are genuinely mixed-column conditions.

5.1 The first two placement digits

Computer-assisted proposition 7 (Shell-two first lift)**.** *For every one of the five $n_9=2$ profile representatives, the first placement digit is a consistent linear system with 54 variables, rank 18, and nullity 36. On the resulting affine $\mathbb{F}_3^{36}$ chart, the next digit consists of twenty quadratic equations: two vanish identically, the remaining eighteen have independent polar parts, and their common polar radical is zero.*

The eighteen individual polar ranks range from 34 to 36. A structured six-dimensional quotient, obtained by collapsing the three row fibers, has ranks between 15 and 21. Exact quadratic Gauss sums show that every one of the $3^6=729$ target fibers of this collapsed pencil is nonempty on every profile. This is a strong reduction but not an obstruction.

5.2 A general retraction criterion

The retraction calculations used in both the dense and two-high sectors are consequences of the following elementary lemma.

Lemma 8 (Radical-translation retraction)**.** *Let*

$$f_i(x) = c_i + \ell_i(x) + 2x^\top B_i x, \qquad 1 \le i \le k,$$

be quadratic polynomials on $\mathbb{F}_3^n$, with symmetric polar matrices B_i. Put

$$R = \bigcap_{i=1}^{k} \ker B_i.$$

There is a matrix $V = (v_1|\cdots|v_k)$ with columns in R for which

$$\Phi(x) = x - V(f_1(x), \ldots, f_k(x))^\top$$

satisfies $f_i(\Phi(x)) = 0$ for every x and every i if and only if

$$\operatorname{rank}\big((\ell_1, \ldots, \ell_k)|_R\big) = k.$$

Equivalently, one may require $B_i V = 0$ for all i and $\ell_i(v_j) = \delta_{ij}$.

Proof. If $v \in R$, all polar cross terms with v vanish and $v^\top B_i v = 0$, so

$$f_i(x+v) = f_i(x) + \ell_i(v).$$

The stated conditions therefore give

$$f_i(\Phi(x)) = f_i(x) - \sum_j \ell_i(v_j) f_j(x) = 0.$$

Conversely, evaluating the proposed identity in the translation directions forces the columns into the common radical and forces the restricted linear map to have the displayed right inverse. □

5.3 The eighteen dense profiles

Computer-assisted proposition 9 (Dense retraction census)**.** *For all eighteen dense profiles in Theorem 4:*

1. *the first placement layer has rank* 18 *and nullity* 36*;*
2. *the eighteen active next-digit quadrics have coefficient-span rank* 18*, with individual polar ranks between* 33 *and* 36*;*
3. *all* $18 \cdot 364 = 6{,}552$ *structured characters and all* 6,552 *five-dimensional hyperplanes in the structured six-form span have been audited;*
4. *nine profiles have maximum retraction dimension five and nine have maximum dimension four; none retract all six forms.*

The nine five-retractable profiles have eleven successful hyperplanes in total, with at most two for one profile.

Every profile was also intersected with all 1,756 exact row-margin words. The number of compatible catalog rows ranges from 45 to 96. These large transfer masses and the existence of isolated second-digit points do not constitute a higher-digit lift or a Legendre pair.

5.4 Physical margins on the five shell-two profiles

The exact row-margin catalog has respectively

$$72,\ 72,\ 72,\ 96,\ 93$$

compatible targets on the five profiles, for 405 targets in total. The first nonautomatic physical margin digit is affine on the 36-dimensional correlation chart.

Computer-assisted theorem 10 (Physical-margin retraction boundary)**.** *On every one of the* 405 *profile/target pairs:*

1. *the six first physical-margin equations have augmented rank* $6/6$*, leaving a parallel affine* 30*-space;*
2. *the next six margin equations are exact quadrics;*
3. *after the margin cut, the maximum structured retraction dimensions on the five profiles are*

$$4,\ 3,\ 3,\ 3,\ 4;$$

4. *no five-form retraction exists.*

The complete $\left[{6 \atop 4}\right]_3 = 11{,}011$ *four-subspace census finds six retracting four-spaces per target on* `h2-222222-0`*, eighty-six per target on* `h2-422220-3`*, and none on the other three profiles.*

Before the physical margin cut, the first and fifth profiles each have one five-form retraction. Exhaustion of all $\left[{6 \atop 5}\right]_3 = 364$ hyperplanes proves that the physical cut destroys both shortcuts. The six margin-quadric polar ranks are target-independent and range from 6 to 10; their joint polar radical is zero on every profile. No consecutive higher-digit physical lift is claimed.

6 Prime-167 phase algebra

The six sparse sequences have total support

$$3 \cdot 54 + 5 = 167,$$

where the fixed zero column contributes five active fibers. The exact phase equations can therefore be reduced modulo 167 without losing an integer equality.

Proposition 11 (Lossless prime reduction)**.** *On the support-*167 *phase shell, the diagonal group-ring equation and the directed cross-fiber equation hold over the cyclotomic integers if and only if their reductions hold modulo* 167*.*

Proof. Every coefficient is an inner product of two vectors of squared norm 167, so its complex modulus is at most 167. These group-ring coefficients are Eisenstein integers. Since 167 is inert in $\mathbb{Z}[\omega]$, a nonzero coefficient divisible by 167 must be 167 times an Eisenstein unit and must attain equality in Cauchy's inequality. For a nonzero column shift, equality would make the support a union of 37-cycles, impossible because $167 \not\equiv 0 \pmod{37}$. For the directed equation, the underlying twisted translation has orbit size 3 at column lag zero and 111 at nonzero lag; neither divides 167. Hence equality cannot occur, and divisibility by 167 forces exact zero. □

Let

$$K = \mathbb{F}_{167}(\alpha) = \mathbb{F}_{167^6}, \qquad E = \mathbb{F}_{167^{12}}.$$

Since $167^6 \equiv 11 \pmod{37}$ and $H = \langle 11^2 \rangle = \{1, 10, 26\}$, the primitive part of the H-invariant group algebra splits as

$$\mathcal{A}_{\mathrm{prim}} \simeq E^6.$$

For one recombined channel word W in (11), take coordinates

$$w_r = W(\zeta_{37}^{167^r}), \qquad 0 \le r < 6.$$

The involution pairs r with $r+3$, and the three primitive complementarity equations are

$$w_{A,r} w_{A,r+3}^{167^3} + w_{B,r} w_{B,r+3}^{167^3} = 0, \qquad r = 0, 1, 2. \tag{12}$$

The origin factor, inverse-CRT sparse-alphabet condition, and exact margins remain separate constraints.

7 Primitive units and the ratio torus

At the ambient finite-field level, (12) has degenerate branches where one or both channel coordinates vanish. The physical shell-two alphabets avoid every such branch.

Computer-assisted theorem 12 (Primitive-unit theorem)**.** *For every physical phase placement over every one of the* 84 *formal shell-two profile images, both channel words are nonzero in every primitive factor:*

$$w_{X,r} \neq 0 \quad (X \in \{A, B\},\ 0 \le r < 6).$$

Equivalently, $W_A, W_B \in \mathcal{A}_{\mathrm{prim}}^*$ *for every physical placement in this shell.*

Exact meet-in-the-middle certificate. The normalized labelled action partitions the 84 formal profile images into ten physical lift orbits, represented by the five canonical seeds and their five A-star images. Their sizes are

$$12, 6, 6, 6, 12,\ \ 12, 6, 6, 6, 12.$$

Five canonical A alphabets, five canonical B alphabets, and five new A-star A alphabets therefore cover all cases.

For a fixed seed, channel, and primitive factor, the complete twelve-class physical alphabet is divided into two halves. Exact sums are stored in all 36 prime-field coordinates of the ambient field representation. The largest case has 30 active trits and two lists of $3^{15} = 14{,}348{,}907$ entries. All ninety required channel/factor zero-sum counts are exactly zero. Each case checks direct polynomial evaluation against the period formula, a small-prefix Cartesian count, and a guaranteed-positive control. The maximal case has an independent 64-bit linear-hash replay: exact equality would imply hash equality, and the two hash sets are disjoint, so no collision assumption is used. Action closure then covers all 84 images. Peak resident memory was 1.86 GB. □

The theorem permits the global ratio

$$R = W_B / W_A \in \mathcal{A}_{\mathrm{prim}}^*.$$

Dividing (12) gives

$$RR^* = -1,$$

or in paired coordinates,

$$R_{r+3} = \left(-R_r^{-1}\right)^{167^9}, \qquad r = 0,1,2. \tag{13}$$

Thus three nonzero coordinates determine the other three. If $M = 167^{12}$, the ratio torus has $(M-1)^3$ points. This removes the degenerate case split; it does not make the inverse-CRT physical alphabet small.

An independent exact audit conditions all six phase sequences on their physical margins and imposes the first two nonconstant characteristic-37 diagonal coefficients, denoted T_1, T_2. Every one of the 405 targets survives:

margin-conditioned assignments	1,538,710,506,610,661,125,476
after T_1, T_2	1,123,966,766,238,638,605.

The contraction is approximately 37^2 and is exact, but it is not an exclusion.

8 Three pair-resultant norm keys

Put

$$F = \mathbb{F}_{167^3} \subset E = \mathbb{F}_{167^{12}}, \qquad N = N_{E/F}.$$

For $X \in \{A, B\}$ and $r = 0,1,2$, define

$$\nu_{X,r} = N(w_{X,r} w_{X,r+3}) \in F^*. \tag{14}$$

Theorem 13 (Pair-resultant norm identities)**.** *Every physical shell-two solution of the primitive equations* (12) *satisfies the three separate equalities*

$$\nu_{A,r} = \nu_{B,r}, \qquad r = 0,1,2. \tag{15}$$

Their product is the weaker total-resultant norm identity; keeping the three pair keys separately is strictly stronger.

Proof. By Theorem 12, $R_r = w_{B,r}/w_{A,r}$ is defined. Equation (12) becomes

$$1 + R_r R_{r+3}^{167^3} = 0.$$

Apply $N_{E/F}$. The extension degree is four, so $N(-1) = 1$, and the 167^3 Frobenius acts trivially on the norm value in F. Hence

$$N(R_r)N(R_{r+3}) = 1.$$

The left side is

$$\frac{N(w_{B,r} w_{B,r+3})}{N(w_{A,r} w_{A,r+3})} = \frac{\nu_{B,r}}{\nu_{A,r}},$$

which proves (15) separately for each r. □

The norm map $E^* \to F^*$ is surjective, and the three star pairs use disjoint coordinates. Thus the three keys are independent on the ambient unit cone. Their common cyclic order factors as

$$|F^*| = 167^3 - 1 = 4{,}657{,}462 = 2 \cdot 83 \cdot 28{,}057. \tag{16}$$

For $d \in \{2, 83, 28057\}$, equality in F^* is equivalent to equality of the character projections

$$\chi_d(x) = x^{(167^3-1)/d}.$$

Moreover

$$\chi_d(\nu_{X,r}) = (w_{X,r} w_{X,r+3})^{(167^{12}-1)/d},$$

so (15) is exactly nine cyclic character equalities. The abstract triple key space has

$$(167^3 - 1)^3 = 101{,}029{,}443{,}456{,}638{,}735{,}128$$

points and needs at least 67 bits. This is an exact join key, not a claim of a 10^{20} contraction on the sparse physical alphabet.

Exact witnesses over all fifteen seed/channel cases—five canonical A, five canonical B, and five A-star A alphabets—show that every individual character coordinate attains every value for all three orders, and that each triple image has affine rank three. In particular, no single-coordinate character obstruction eliminates a profile.

9 Exact slices and the complete-search cost gate

To measure the physical behavior of the keys rather than extrapolate from the ambient torus, a detached exact program varies the first three classes having three active fibers and fixes all other class options. Each channel slice has

$$3^9 = 19{,}683$$

physical placements. The fifteen alphabets are the five canonical A alphabets, five canonical B alphabets, and five A-star A alphabets. Ten ordered A/B joins are therefore complete Cartesian products of

$$19{,}683^2 = 387{,}420{,}489$$

pairs. These are exact finite subfamilies, not random samples.

Computer-assisted proposition 14 (Exact nine-trit slices)**.** *Across the fifteen channel slices, the single-channel character images are:*

character order	*marginal image of each ν_r*	*joint triple support*
2	2/2	8/8
83	83/83	18,969 *to* 19,387
28,057	13,880 *to* 14,231	19,332 *to* 19,683

On the ten exact pair joins, the equality counts and contractions are:

d	*one-pair count*	*factor*	*three-pair count*	*factor*
2	193,693,992–193,733,392	1.9998–2.0002	48,417,524–48,434,696	7.9988–8.0017
83	4,664,194–4,671,617	82.93–83.06	646–700	553,458–599,722
28,057	13,609–14,059	27,557–28,468	0	–

The simultaneous order-28,057 count is zero only on these deliberately small slices. Under a uniform independence model, its expected value in one slice join is about

$$387{,}420{,}489/28{,}057^3 \simeq 1.75 \cdot 10^{-5}.$$

Zero is therefore the ordinary expected slice outcome and is not used as a profile exclusion.

9.1 Why slicing does not complete the join

The complete margin-conditioned one-channel domain sizes over the 405 targets are:

domain	minimum	median	maximum
A	266,710,752	1,645,293,600	69,522,443,424
B	37,948,932	2,438,821,245	10,363,952,610
$A+B$	3,129,845,130	6,033,337,266	69,610,870,944

With target-wise duplication retained, a complete pass needs exactly

$$5{,}091{,}993{,}547{,}996 \tag{17}$$

invariant evaluations, or about 258.7 million nine-trit slice equivalents. The smallest target needs 159,014 slices and the largest 3,536,600.

The norm triple requires at least 67 bits. Including the exact T_1, T_2 residue requires at least 77 bits. At a practical sixteen bytes per stored key:

smallest target	50.1 GB
largest target	1.11 TB
all targets with duplication	81.5 TB

Even storing only the smaller channel is not an in-memory solution on a 16 GB workstation: the largest smaller side has 2,238,465,240 assignments, or about 35.8 GB at sixteen bytes per entry.

The frozen exact PARI/GP slice audit sustained about 1,570 assignments per second. At that implementation rate (17) would take about 103 years. Even sustained rates of 10^6 and 10^8 evaluations per second correspond to about 59 days and 14 hours, respectively, before external sorting, bucket input/output, and exact collision replay.

If the three F^* equalities behaved independently of the existing T_1, T_2 layer, the expected residual from the $1.123966766 \cdot 10^{18}$ survivors would be about 0.011. This is a heuristic, not a theorem. The exact conclusion is the cost gate: materializing the present complete join is outside the available memory and evaluation budget. A useful continuation requires an algebraic compression of the norm keys or an implicit character-sum method, not merely more nine-trit batching.

10 Reproducibility and artifact map

All paths below are relative to `hadamard_668_search/`. Exact verification commands and expected hashes are also recorded in the adjacent README files.

Claim	**Primary note or certificate**	**Independent replay entry point**
Profile equivalence, 22 targets, local sieve	`LP333_ORDER3_EISENSTEIN.md`	`verify_lp333_order3_mod3_sieve.py`
$n_9 = 6$ exclusion	`LP333_ORDER3_PROFILE_ENDPOINT_SHELL.md`	`verify_lp333_order3_profile_endpoint_shell.py`
$n_9 = 5$ exclusion	`LP333_ORDER3_PROFILE_PENULTIMATE_SHELL.md`	`verify_lp333_order3_profile_penultimate_shell.py`

Claim	Primary note or certificate	Independent replay entry point
$n_9 = 4$ exclusion	LP333_ORDER3_PROFILE_SHELL_FOUR.md	verify_lp333_order3_profile_shell_four.cpp
$n_9 = 3$ exclusion	shell_three_mod27/	shell_three_mod27/verify_lp333_order3_profile_shell_three_mod27.cpp
Five $n_9 = 2$ orbits	shell_two_exact/shell_two_exact_orbits_certificate.json	shell_two_exact/verify_shell_two_exact_orbits.py
Eighteen dense orbits	dense_shell_h0_complete_classification/certificate.json and output/releases/h668-dense-shell-production-v2-v1.0.0.tar.gz	dense_shell_classifier_pilot/aggregate_dense_shell_production.py, dense_shell_h0_complete_classification/verify_h0_complete_classification.py
Dense $\mathbb{F}_{27} \times \mathbb{F}_{27}$ algebra	LP333_ORDER3_DENSE_SHELL_QUADRATIC_ALGEBRA.md	verify_lp333_order3_dense_shell_quadratic_algebra.py
Dense retraction census	h0_new_orbits_lift_triage/FINAL_PRODUCTION_SCAN_18.json	h0_new_orbits_lift_triage/verify_new_orbits_lift_triage.py
Shell-two quadrics and margins	phase_second_digit/ and shell_two_physical_margin_lift/	phase_second_digit/verify_phase_second_digit_pencil.py, shell_two_physical_margin_lift/audit_row_margin_retraction.py, shell_two_physical_margin_lift/audit_four_subspaces.py
Prime-167 exactness	LP333_ORDER3_PHASE_PRIME167.md	verify_lp333_order3_phase_prime167.py
Primitive units and T_1, T_2	lp333_shell_two_primitive_units/	lp333_shell_two_primitive_units/REPRODUCE.md, lp333_shell_two_primitive_units/verify_action_closure.py
Pair-resultant theorem	lp333_shell_two_pair_resultant_norm/	lp333_shell_two_pair_resultant_norm/verify_ratio_resultant_norm.py, lp333_shell_two_pair_resultant_norm/verify_character_field_bridge.py
Exact slices and cost gate	lp333_shell_two_pair_resultant_slices/	lp333_shell_two_pair_resultant_slices/freeze_pair_norm_slices.py, lp333_shell_two_pair_resultant_slices/audit_pair_norm_slices.gp

Selected frozen identifiers are:

Five-orbit semantic certificate. `36099444b32f88869557a6f510f06cfa3b6eaa7a876b26cf62a0796ca4232565`

Dense aggregate. `3bccde87f456bfcd2f0c3da6ac8cf9cb3635538e831a95951003068ae87cae86`

Primitive action closure. `d89f8fce094dfc826749489a5dbff72f657ef07687a7f3e2eb1e25f5db0ed516`

Pair-resultant theorem. `4e4cdb32d2e54e8b402e71dc4e7adbdce4dec6fbe0c3a1e076fa98ed13 38cf9a`

Pair-slice semantic certificate. `3585ff30f2a2951bf071c03ea1a1c82c460c6ef46c729b12cd77 e53bd74f7010`

Because these strings are long, the repository `SHA256SUMS` files, not typesetting, are the authoritative hash source.

11 Data and code availability

The complete research checkpoint is distributed in the immutable release

`https://github.com/AlecKriebel/Math/releases/tag/h668-research-checkpoint-v1.0.0`.

The manuscript source is `hadamard_668_search/papers/lp333_fixed_compression/manuscript.tex`. Its exact verifiers and certificates are mapped in Section 10. The release asset `hadamard_668_search/output/releases/h668-dense-shell-production-v2-v1.0.0.tar.gz` contains the production manifest, strict aggregate, all 729 completed shard records, the pinned helper, and the relevant production and replay sources. Its SHA-256 is

`493f73884ff5b5454f179b7754c0207178eeb70c70c27750daa610f3bda6c2df`.

The adjacent release README gives a no-search aggregation replay and the authoritative file hashes. No external service or solver status is required for the lightweight certificate replays.

12 Limitations and conclusion

The finite profile classifications and the pair-resultant identities form a coherent exact reduction, but the boundary of the result is sharp.

- No binary Legendre pair of length 333 is constructed or excluded. No Hadamard matrix of order 668 is constructed.
- The prescribed compression (2) is an extra conjectural restriction. Even a complete failure of this chart would not settle public ID 3 or unrestricted LP(333).
- The $n_9 = 1$ compressed-profile shell remains open.
- Five $n_9 = 2$ orbits and eighteen $n_9 = 0$ compressed profiles are not labelled uncompressions. None has been lifted through all primitive-nine and physical-margin equations.
- The dense exhaustiveness claim relies on the released production census. Its manifest, aggregate, and all 729 completed shard records are available for strict reaggregation, while the detached verifier replays the retained mathematics. Neither replay reruns the expensive producer from scratch.
- Bounded searches, neutral independence estimates, and absence of a found higher-digit witness are not used as nonexistence evidence.

- The three pair-resultant norms are consequences of the primitive equations. Their large ambient key space does not automatically imply the same contraction on the sparse physical alphabet.

Within those limitations, the work supplies three durable outcomes. First, the exact shell descent turns a 10^{24} profile problem into explicit finite classifications, with five two-high and eighteen dense profile orbits preserved for independent checking. Second, the physical-margin and retraction censuses identify a precise algebraic boundary: the first favorable five-form shortcuts disappear after the physical cut. Third, the primitive-unit theorem converts the surviving shell-two problem into one ratio torus and yields three intrinsic norm keys. Exact slices confirm that the keys are highly nonconstant, while the complete cost calculation shows that direct materialization remains impractical. Any renewed construction attempt should therefore seek a theorem that compresses or implicitly sums these three keys, rather than enlarging the same explicit join.

A The five two-high representatives

Profile IDs index the lexicographically ordered compositions of three:

ID	0	1	2	3	4	5	6	7	8	9
p	$(0,0,3)$	$(0,1,2)$	$(0,2,1)$	$(0,3,0)$	$(1,0,2)$	$(1,1,1)$	$(1,2,0)$	$(2,0,1)$	$(2,1,0)$	$(3,0,0)$.

The twelve entries are in class order $C_0, \dots, C_{11}$:

`h2-222222-0`
$A = (2,5,8,1,7,9,5,8,5,5,5,7)$
$B = (2,5,3,6,5,5,5,4,7,5,4,7)$

`h2-422220-0`
$A = (2,5,7,8,6,5,2,5,7,8,6,5)$
$B = (5,8,5,0,1,5,5,8,5,0,1,5)$

`h2-422220-1`
$A = (2,8,8,5,5,5,2,8,8,5,5,5)$
$B = (2,5,5,4,1,3,2,5,5,4,1,3)$

`h2-422220-2`
$A = (4,9,8,5,5,5,4,9,8,5,5,5)$
$B = (2,7,5,1,5,6,2,7,5,1,5,6)$

`h2-422220-3`
$A = (8,5,4,5,9,1,6,8,5,5,2,6)$
$B = (2,3,5,5,1,5,1,4,7,5,5,5)$

AI-assistance statement

ChatGPT 5.6 Sol was used extensively to organize the research program, derive and test algebraic reductions, write and review verification code, audit scope against recent literature, and draft this manuscript. The human author directed the project and selected the claims for inclusion. No claim has been independently peer reviewed. The source artifacts and certificates are supplied so that domain experts can check the mathematical models, implementations, and claimed exhaustive coverage.

References

[1] S. Barrera Acevedo, P. Ó Catháin, and H. Dietrich, Cocyclic two-circulant core Hadamard matrices, *J. Algebraic Combin.* **55** (2022), 201–215, https://doi.org/10.1007/s10801-021-01033-x.

[2] D. Bulutoglu, D. Baczkowski, and J. Yauney, Determining the group that sends each Legendre pair to an equivalent Legendre pair, arXiv:2604.22423 (2026), https://doi.org/10.48550/arXiv.2604.22423.

[3] P. Chojecki, Computational search for a Hadamard matrix of order 668 via Legendre pairs of length 333: status report and roadmap, Ulam AI report, March 2026, https://www.ulam.ai/research/frontier-had.pdf.

[4] S. Eliahou, A 64-modular Hadamard matrix of order 668, *Australas. J. Combin.* **93** (2025), no. 2, 422–427, https://ajc.maths.uq.edu.au/pdf/93/ajc_v93_p422.pdf.

[5] R. J. Fletcher, M. Gysin, and J. Seberry, Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices, *Australas. J. Combin.* **23** (2001), 75–86.

[6] I. S. Kotsireas, C. Koukouvinos, and J. Seberry, Hadamard ideals and Hadamard matrices with two circulant cores, *European J. Combin.* **27** (2006), 658–668, https://doi.org/10.1016/j.ejc.2005.03.004.

[7] I. Kotsireas, R. Gallardo-Cava, A. I. Gómez, and D. Gómez-Pérez, On the search of binary Legendre pairs of length pq^2, *J. Symbolic Comput.* **138** (2027), article 102606, https://doi.org/10.1016/j.jsc.2026.102606.

[8] A. F. Ramos, D. B. Hulak, and R. J. G. B. de Queiroz, Multiplier obstructions for Legendre pairs of length 333, arXiv:2607.20765v1 (submitted 22 July 2026), https://doi.org/10.48550/arXiv.2607.20765.