Exact repair obstructions around a 64-modular Hadamard matrix of order 668

Alec Kriebel
with substantial assistance from ChatGPT 5.6 Sol

Research draft, 25 July 2026
Not peer reviewed

Abstract

Eliahou constructed a 64-modular Hadamard matrix of order 668 from a special binary quadruple of length 167. An exact repair within that special form is equivalent to a base sequence in BS(84, 83). We give several exact obstructions and reductions around the published seed.

First, if Eliahou's sequence $q = (+^{83}, -^{2}, +^{81}, -)$ is fixed, no choice of the other sign sequence gives an exact quadruple. A parity telescope and even–odd decimation would otherwise produce an element of TU(41); in addition to the known classification, we independently exhaust 461 normalized shards, comprising 57,543,021 deterministic search nodes and no solution.

Second, reduction of the four base rows modulo $z^{42} - 1$ proves that any exact repair changes at least 80 of the 334 base signs, and at least 41 signs in the natural (s, q) coordinates. At special distance 41, the only remaining form is 39 changes in s and one reciprocal pair of changes in q. Root filters leave 21 long and 18 short reciprocal pairs. Reduction modulo $z^{42} + 1$ removes endpoint orientation and collapses these to 30 canonical support problems. A checked DRAT proof excludes the boundary long case, and an exhaustive exact-integer census of 3,710,853,316,608 modular join rows excludes all nine short cases.

The remaining twenty long cases are not excluded. For them we prove an exact endpoint-orientation cascade: the positive fold modulo 8 is redundant on the full anti-fold characteristic-two code, the modulo-16 layer is a fixed binary linear system, exact root conditions are four cardinality equations, and the modulo-32 layer is quadratic. We also correct the scope of the two-fold method: the positive and negative 42-folds imply cyclic length-84 complementarity, not the original aperiodic equations. Forty-one causal equations restore exact equivalence. No BS(84, 83), Golay quadruple, or Hadamard matrix of order 668 is constructed or ruled out.

Verification and authorship disclaimer. This is an AI-assisted, unreviewed research artifact. The mathematical exploration, program development, certificate analysis, and manuscript drafting used substantial assistance from OpenAI language models operating through ChatGPT and Codex. The named human author directed the project and is responsible for any release, but describes himself as a non-specialist and cannot independently certify every derivation or implementation. The repository includes deterministic checkers and independently replayable certificates where stated. Those artifacts strengthen auditability; they do not replace expert review, establish priority, or constitute a proof-assistant formalization.

1 Introduction

A Hadamard matrix of order n is a matrix $H \in \{\pm 1\}^{n\times n}$ such that

$$HH^{\mathsf{T}} = nI_n.$$

The Hadamard conjecture predicts such a matrix whenever $4 \mid n$. Order 668 is a prominent unresolved instance in current construction tables [1, 9]. Eliahou constructed a 64-modular matrix at that order, satisfying

$$HH^{\mathsf{T}} \equiv 668 I_{668} \pmod{64},$$

from a structured length-167 quadruple and the Goethals–Seidel array [5]. Its failure of exact complementarity is concentrated at thirteen aperiodic lags. Eliahou's 2026 update is cited for bibliographic context only: its metadata and abstract, but not its full text, were inspected during this project [6]. No claim below depends on that article.

The most direct local question is whether signs in that structured seed can be changed to obtain exact complementarity. Ramos, Hulak, and de Queiroz have already recorded the basic translation of this question to BS$(84, 83)$ and a raw base-row distance lower bound of 64 in the artifact release accompanying their work on multiplier obstructions [7, 8]. The present paper starts from the same standard base-sequence translation. Its main additions are:

1. a fixed-q obstruction through TU(41), with an independent modern exhaustive certificate for the known endpoint;
2. an adjacent-42 fold giving the stronger base-row distance bound 80 and the exact special-coordinate boundary 41;
3. an orientation-free anti-fold, one checked DRAT exclusion, and a complete exact census of all nine short boundary cases; and
4. an exact 2-adic orientation cascade for the twenty open long cases, together with the necessary aperiodic scope correction.

These conclusions are deliberately local. The exact fixed-q family is closed, and ten of the thirty minimum-boundary anti-fold support cases are closed. Twenty long support cases remain open. Nothing here implies nonexistence of BS$(84, 83)$, of a nonspecial Golay quadruple of length 167, or of a Hadamard matrix of order 668.

2 Sequences and Eliahou's special form

2.1 Aperiodic norms and base sequences

For a real sequence $X = (x_0, \ldots, x_{r-1})$, put

$$N_X(k) = \sum_{i=0}^{r-k-1} x_i x_{i+k} \qquad (0 \le k < r),$$

and set $N_X(k) = 0$ when $k \ge r$. In polynomial notation, $X(z) = \sum_i x_i z^i$, the Laurent polynomial $X(z)X(z^{-1})$ has coefficient $N_X(|k|)$ at z^k.

A binary Golay quadruple of length r is a quadruple (X_1, X_2, X_3, X_4) of sign sequences satisfying

$$\sum_{j=1}^{4} N_{X_j}(k) = 0 \qquad (1 \le k < r).$$

A base sequence in $\mathrm{BS}(m,n)$ is a quadruple $(A;B;C;D)$ of binary sequences with

$$|A| = |B| = m, \qquad |C| = |D| = n,$$

and

$$R_k := N_A(k) + N_B(k) + N_C(k) + N_D(k) = 0 \qquad (1 \le k < m).$$

We use the standard base-sequence notation and equivalences of Đoković [3]. Its zero-lag energy is $R_0 = 2m + 2n$. We use coefficientwise products of sign sequences without a separate symbol.

2.2 The special quadruple and its base rows

Let $h \in \{\pm 1\}^{167}$ be $+1$ on coordinates $0, \dots, 83$ and -1 on coordinates $84, \dots, 166$. Eliahou's special quadruple has the form

$$\mathcal{G}(s,q) = (s, hs, sq, hsq). \tag{1}$$

The published sequence q has alternating run lengths

$$q = (+^{83}, -^{2}, +^{81}, -).$$

For a direct reconstruction of the seed, the run-length word of s is

$$((4)^5, (2,1,1)^5, 1, 5, (4)^4, (2,1,1)^6, (4)^4, 3,\\ (1,2,1)^5, 3, (4)^4, 3, (1,2,1)^5),$$

where the first run is positive and a parenthesized exponent denotes block repetition.

Split at the sign change of h:

$$A = s_{[0,84)}, \quad B = (sq)_{[0,84)}, \quad C = s_{[84,167)}, \quad D = (sq)_{[84,167)}. \tag{2}$$

Proposition 2.1 (Special-to-base-sequence translation)**.** *The quadruple $\mathcal{G}(s,q)$ is exactly Golay if and only if $(A;B;C;D) \in \mathrm{BS}(84,83)$. The correspondence is bijective, with inverse*

$$s = A \| C, \qquad q = (AB) \| (CD).$$

Proof. At lag k, the summed correlation in (1) is

$$\sum_i s_i s_{i+k}(1 + h_i h_{i+k})(1 + q_i q_{i+k}).$$

Terms crossing the $84 + 83$ split vanish. The remaining value is twice R_k for the four rows in (2), and it vanishes automatically for $k \ge 84$. The inverse follows coordinatewise. □

For the published base rows, the only nonzero positive-lag values of R_k are

k	4	8	12	16	26	30	34	38	42	46	50	54	58
R_k	−256	192	−128	64	−32	64	−96	128	−160	128	−96	64	−32.

(2.1)

The corresponding correlations of the four length-167 rows are twice these values. In particular, divisibility by 64 does not imply exact complementarity. In the associated Goethals–Seidel matrix, Eliahou records that every row is already orthogonal to 641 of the other 667 rows, with 26 nonzero off-diagonal Gram entries [5].

3 The fixed-q obstruction

This section keeps the published q fixed and permits arbitrary s. The proof reduces the exact equations to a Turyn sequence of parameter 41, then uses both the known classification and an independent enumeration.

3.1 A parity telescope

Write

$$X = (s_0, \dots, s_{82}), \quad u = s_{84}, \quad Y = (s_{85}, \dots, s_{165}), \quad v = s_{166}.$$

The coordinate s_{83} is isolated by the four runs of q. Writing $X = (x_0, \dots, x_{82})$ and $Y = (y_0, \dots, y_{80})$, exact complementarity is equivalent to

$$N_X(k) + N_Y(k) = 0 \qquad (1 \le k \le 80), \tag{3}$$

$$x_0x_{81} + x_1x_{82} = 0, \tag{4}$$

$$x_0x_{82} + uv = 0. \tag{5}$$

Lemma 3.1 (Parity telescope)**.** *Every solution of* (3)–(5) *satisfies*

$$x_{82-i} = (-1)^{i+1}x_i \qquad (0 \le i \le 82), \tag{6}$$

$$y_{80-i} = (-1)^i y_i \qquad (0 \le i \le 80), \tag{7}$$

$$u = v. \tag{8}$$

Proof. For $0 \le k \le 81$, let P_k be the product of all sign terms in $N_X(k) + N_Y(k)$, with the Y product empty at $k = 81$. At every positive lag the zero sum contains $2(82 - k)$ signs and exactly half are negative. Hence

$$P_k = (-1)^k, \qquad 0 \le k \le 81.$$

Cancellation in P_{i+1}/P_i gives

$$(x_ix_{82-i})(y_iy_{80-i}) = -1 \qquad (0 \le i \le 80).$$

Set $r_i = x_ix_{82-i}$ and $t_i = y_iy_{80-i}$. Reflection gives $r_i = r_{82-i}$ and $t_i = t_{80-i}$. Comparing the equations at i and $80 - i$ gives $r_i = r_{i+2}$. The central products are $r_{41} = t_{40} = 1$, and $r_{40}t_{40} = -1$. These values determine the two parity classes of every r_i and then every t_i, yielding (6) and (7). Finally $x_0x_{82} = -1$, so (5) gives $uv = 1$ and therefore $u = v$. □

3.2 Even–odd decimation

Define

$$\begin{aligned} E &= (x_0, x_2, \dots, x_{82}), & |E| &= 42, & \operatorname{rev}(E) &= -E, \\ O &= (x_1, x_3, \dots, x_{81}), & |O| &= 41, & \operatorname{rev}(O) &= O, \\ P &= (y_0, y_2, \dots, y_{80}), & |P| &= 41, & \operatorname{rev}(P) &= P, \\ Q &= (y_1, y_3, \dots, y_{79}), & |Q| &= 40, & \operatorname{rev}(Q) &= -Q, \end{aligned}$$

and let $\widehat{Q} = (u, Q, v)$, of length 42. Since Q is skew and $u = v$, the two endpoint contributions to $N_{\widehat{Q}}(k)$ cancel for $1 \le k \le 40$. The even-lag equations above, including the endpoint equation, become

$$N_E(k) + N_{\widehat{Q}}(k) + N_O(k) + N_P(k) = 0 \qquad (1 \le k \le 41).$$

Thus

$$(E;\widehat{Q};O;P)\in \mathrm{BS}(42,41),$$

with the first long row skew and the first short row symmetric. Under the standard definition this is an element of TU(41) [2, 4].

3.3 Independent exhaustion of TU(41)

The nonexistence of TU(41) is already contained in the exhaustive classification of Edmondson, Seberry, and Anderson [4]. For an independently reproducible endpoint, we also performed a fresh enumeration.

The standard normalized form at odd parameter $41 = 2\cdot 20+1$ is

$$\begin{aligned} A &= (1,1,a_2,\dots,a_{20},-a_{20},\dots,-a_2,-1,-1),\\ B &= (1,1,b_2,\dots,b_{20},-b_{20},\dots,-b_2,-1,1),\\ C &= (1,c_1,\dots,c_{19},c_{20},c_{19},\dots,c_1,1),\\ D &= (1,d_1,\dots,d_{19},d_{20},d_{19},\dots,d_1,1). \end{aligned} \tag{9}$$

This normalized search covers the object produced by the decimation above. Definition 7(i) of Edmondson–Seberry–Anderson states that every odd Turyn sequence—a base sequence whose first long row is skew and whose first short row is symmetric—has a representative of (9) under the standard sign, reversal, and equal-length interchange normalizations, all of which preserve the summed aperiodic norm [4]. The decimated quadruple $(E;\widehat{Q};O;P)$ has exactly those skew/symmetric types. Hence a hypothetical decimated solution would supply a normalized representative enumerated below. This bridge uses the cited normalization theorem; the certificate independently exhausts its normalized representatives rather than formalizing the equivalence theorem itself.

There are 78 free signs. The interchange symmetry of C, D is removed by lexicographic order. Evaluation at $z = 1$ gives

$$\sum(A)^2+\sum(B)^2+\sum(C)^2+\sum(D)^2 = 166.$$

Here $\sum(A) = 0$ and $\sum(B) = 2$, so

$$|\sum(C)| = |\sum(D)| = 9.$$

Computational Theorem 3.2 (Independent TU(41) certificate)**.** *No normalized quadruple in* (9) *satisfies all* 41 *positive-lag base-sequence equations. The deterministic outside-in enumeration has*

461 *complete shards*, 57,543,021 *search nodes*, 0 *solutions.*

Certificate method. After symbolic cancellation, the high-lag equations introduce the variables in small outside-in blocks. A branch is retained only if every newly complete high-lag equation is zero. For a lower lag with fixed contribution F and U unresolved product terms, a branch is rejected only if $|F| > U$ or $F+U$ is odd. These are necessary bounds even when the unresolved products are dependent. After five recursion steps, 19 signs have been assigned and exactly 461 prefixes survive. An independent Python program exhausts all 2^{19} prefix assignments and verifies this cover. Each shard then evaluates all 41 equations at every leaf. Small cases $n = 3, 7, 9$ reproduce the known pattern present, present, absent. The source, cube cover, shard index, and summary are joined by hashes in the certificate.

Theorem 3.3 (Fixed-q obstruction)**.** *Keep Eliahou's published sequence*

$$q = (+^{83}, -^{2}, +^{81}, -)$$

and the special form $\mathcal{G}(s, q)$. No binary sequence s makes $\mathcal{G}(s, q)$ exactly Golay.

Proof. A solution would yield an element of TU(41) by Lemma 3.1 and the even–odd decimation. This contradicts either the published classification [4] or the independent certificate in Theorem 3.2. □

Remark 3.4. The obstruction is not a two-squares argument. The relevant row-sum identity is

$$\sum(C)^2 + \sum(D)^2 = 162 = 9^2 + 9^2.$$

The final step is the exhaustive nonexistence of TU(41).

4 The adjacent-42 fold and exact distance

4.1 A cyclic image of BS(84, 83)

For a row X of length 84 or 83, fold modulo 42:

$$F_X(j) = X_j + X_{j+42}, \qquad 0 \le j < 42,$$

where the missing second endpoint in a short row contributes zero. Let P_k be the summed periodic correlation of the four folded rows. Ordinary reduction of the four-row norm modulo $z^{42} - 1$ gives

$$\begin{aligned} P_0 &= R_0 + 2R_{42}, \\ P_k &= R_k + R_{42-k} + R_{42+k} + R_{84-k} \qquad (1 \le k \le 20), \\ P_{21} &= 2(R_{21} + R_{63}). \end{aligned} \tag{10}$$

Consequently every BS(84, 83) has a periodically complementary length-42 integer image of energy 334.

For Eliahou's base rows the folds are

$$F_A = -2z^{41}, \qquad F_B = 0, \qquad F_C = 2 + z^{41}, \qquad F_D = -2z^{40} + z^{41}. \tag{11}$$

Their summed cyclic norm is the constant 14. In particular, all nonconstant fold correlations already vanish: the thirteen residual aperiodic lags cancel in four triples under (10).

4.2 The distance-80 theorem

Across the four base rows there are

$$42 + 42 + 41 + 41 = 166$$

disjoint separation-42 pairs and two unpaired short-row signs. If E of those pairs have equal endpoints, the folded energy is

$$2 + 4E. \tag{12}$$

An exact target has energy 334, so it has exactly 83 equal pairs. The seed in (11) has only three: row A at cell 41, row C at cell 0, and row D at cell 40.

Theorem 4.1 (Base and special distance bounds)**.** *Let $\mathcal{E}$ be Eliahou's labelled base quadruple.*

1. *Every $(A;B;C;D) \in \mathrm{BS}(84,83)$ differs from $\mathcal{E}$ in at least 80 of its 334 base signs.*
2. *Every exact special pair (s,q) differs from the published (s_0,q_0) in at least 41 of its 334 special-coordinate signs.*

Proof. Changing one base sign toggles the equality status of at most one separation-42 pair. Raising the number of equal pairs from 3 to 83 therefore takes at least 80 changes, proving the first assertion.

At one coordinate, changing s alone changes both associated base signs; changing q alone or changing both s and q changes one base sign. Thus special distance d produces base distance at most $2d$, and the first assertion gives $d \geq 40$. Equality $d = 40$ would require all 40 changes to be s-only, leaving $q = q_0$. This is impossible by Theorem 3.3, so $d \geq 41$. □

Equality in the first part is rigid. All three seed-equal pairs and the two short singletons remain fixed; exactly 80 of the 163 seed-opposite pairs become equal; and exactly one endpoint is changed in each selected pair. If F_0 denotes the four folds in (11), write $F = F_0 + 2G$. Then G is a four-row ternary word supported on exactly 80 seed-opposite cells and satisfies the exact group-ring equation

$$\sum_r \left(F_{0,r}G_r^* + G_r F_{0,r}^*\right) + 2\sum_r G_r G_r^* = 160 \quad \text{in } \mathbb{Z}[C_{42}]. \tag{13}$$

The sign of every nonzero coefficient of G identifies which endpoint was changed. Equation (13) is necessary and sufficient for the adjacent-42 cyclic image on the minimum shell, but not for the original aperiodic equations.

5 The special-distance-41 boundary

5.1 The reciprocal q skeleton

Write $q = g\|h$, with $|g| = 84$ and $|h| = 83$. Exact complementarity forces the number of active equal-q pairs at every lag to be even. Row reduction over $\mathbb{F}_2$ gives the following closed form.

Lemma 5.1 (Reciprocal skeleton)**.** *Every exact special quadruple has*

$$\begin{aligned} g &= (g_0, g_1, \ldots, g_{41}, g_{41}, \ldots, g_1, -g_0), \\ h &= (h_0, h_1, \ldots, h_{40}, h_{41}, h_{40}, \ldots, h_1, h_0). \end{aligned} \tag{14}$$

Conversely, every q of this form makes the active-pair count even at every lag.

Proof. Use bits for the signs of q. Modulo two, the indicator that two signs are equal is $1 + q_i + q_j$. If e_k is the parity equation at lag k, then elementary row operations give

$$\begin{aligned} &e_{83}: && g_0 + g_{83} = 1, \\ &e_j + e_{83-j}: && g_j + g_{83-j} = 0 \quad (1 \leq j \leq 41), \\ &e_{j+1} + e_{83-j}: && h_j + h_{82-j} = 0 \quad (0 \leq j \leq 40). \end{aligned}$$

These 83 independent equations are precisely (14). Reversing the row operations proves the converse. □

Relative to the published q_0, the skeleton has exactly one possible weight-one change, at the center of the short block (global coordinate 125). Every legal weight-two change is one reciprocal pair; there are 42 long and 41 short pairs.

5.2 Classification at equality

At one special coordinate let

$$a = \#(s\text{-only changes}), \quad b = \#(q\text{-only changes}), \quad c = \#(\text{changes in both } s \text{ and } q).$$

Then

$$d_{\text{special}} = a + b + 2c, \qquad d_{\text{base}} = 2a + b + c.$$

Theorem 5.2 (Complete special-distance-41 split)**.** *An exact repair at special distance* 41*, if one exists, has exactly*

$$39 \ s\text{-only changes} \quad + \quad 2 \ q\text{-only changes},$$

and the two q changes form one reciprocal pair.

Before root filtering there are 80 *shell-compatible reciprocal pairs. The evaluations at* $z = 1$ *and* $z = -1$ *leave exactly* 39 *pairs:* 21 *long and* 18 *short. Every surviving pair has exactly two compatible joined root profiles.*

Proof. Combining $d_{\text{special}} = 41$ with $d_{\text{base}} \geq 80$ in (5.2) leaves only

$$(a, b, c) = (41, 0, 0), \ (40, 1, 0), \ (39, 2, 0).$$

The first keeps q fixed and is impossible by Theorem 3.3. In the second, the unique q change is the short center. If λ and σ denote the ordinary signed sums of the common long and short fold changes, the root energy equation is

$$\lambda(\lambda + 1) + \sigma^2 = 41,$$

or

$$(2\lambda + 1)^2 + (2\sigma)^2 = 165.$$

This has no integer solution because both 3 and 11, primes congruent to 3 modulo 4, occur to odd exponent in 165. Hence only (5.2) remains, and Lemma 5.1 makes the two q changes reciprocal.

Three of the 83 reciprocal pairs are incompatible with equality in the base distance bound, leaving 80. For a reciprocal q pair, let $H(z)$ be its signed two-term contribution to the active product row after the adjacent fold, and define

$$h_+ = H(1), \qquad h_- = H(-1).$$

The exact $z = \pm 1$ calculation gives the following signed two-term fold distributions:

long (h_+, h_-)	$(-2, 0)$	$(0, 2)$	$(0, -2)$	$(2, 0)$
count	6	15	15	6
short (h_+, h_-)	$(2, -2)$	$(0, 0)$	$(-2, 2)$	
count	10	18	10	

Only the first two long types and the middle short type have compatible root energy and parity profiles. Their counts are $6 + 15 + 18 = 39$. Solving the two exact sum-of-squares systems gives two profiles per pair. □

Writing a profile as $((L(1), S(1)), (L(-1), S(-1)))$, the two profiles are

pair type	profile 0	profile 1
long $(-2, 0)$	$((-3, 4), (-5, -4))$	$((6, -5), (4, 5))$
long $(0, 2)$	$((-4, -5), (-6, 5))$	$((5, 4), (3, -4))$
short $(0, 0)$	$((-4, -5), (4, 5))$	$((5, 4), (-5, -4))$.

(15)

6 The orientation-free anti-fold

6.1 Reduction modulo $z^{42}+1$

For a base row define its anti-fold

$$D_X(j) = X_j - X_{j+42}, \qquad 0 \le j < 42,$$

again treating the missing short endpoint as zero. Let Q_k be the summed negacyclic correlation of the four anti-folds. Reduction modulo $z^{42}+1$ gives

$$\begin{aligned} Q_0 &= R_0 - 2R_{42}, \\ Q_k &= R_k - R_{42-k} - R_{42+k} + R_{84-k} \qquad (1 \le k \le 20), \\ Q_{21} &= 0, \qquad Q_{42-k} = -Q_k. \end{aligned} \tag{16}$$

Every BS$(84, 83)$ therefore satisfies

$$\sum_X D_X(z) D_X(z^{-1}) = 334 \quad \text{in } \mathbb{Z}[z]/(z^{42}+1).$$

For a seed-opposite pair $(x, -x)$, changing the lower endpoint gives $(-x) - (-x) = 0$, whereas changing the upper endpoint gives $x - x = 0$. Thus endpoint orientation disappears from the anti-fold. At the boundary in Theorem 5.2, the 39 changes in s select 39 cells; each selected long cell is zeroed in both long anti-fold rows, and each selected short cell is zeroed in both short anti-fold rows. The fixed reciprocal q pair zeroes two further entries in the active product row. The anti-fold energy drops by exactly

$$80 \cdot 4 = 320,$$

from the seed value 654 to the required 334. The remaining task is the set of 20 noncentral equations in (6.1).

The 21 long reciprocal pairs remain distinct. The 18 short pairs occur in nine mirrored pairs,

$$(2, 38), (4, 36), \ldots, (18, 22),$$

and each mirrored pair gives the same orientation-free support problem. There are therefore

$$21 \text{ long cases} + 9 \text{ short cases} = 30$$

canonical anti-fold instances. We label the long boundary instance $L0$ as case 0, the other long instances as cases $1, \ldots, 20$, and the short instances $S02, S04, \ldots, S18$ as cases $21, \ldots, 29$.

6.2 A checked DRAT exclusion

Case $0 = L0$ has 79 available support variables; all other cases have 78. In every case exactly 39 support cells must be selected.

Computational Theorem 6.1 (Case-0 anti-fold exclusion)**.** *The complete orientation-free anti-fold support problem for the long reciprocal pair $L0$ is unsatisfiable. This exclusion is independent of the two adjacent-fold root profiles.*

Encoding and certificate. The exact cardinality equation and the twenty integer anti-fold equations were translated to CNF. Every product of two retained-entry literals is linked to an auxiliary variable by the three-clause Boolean AND equivalence. Signed pseudo-Boolean sums are encoded exactly. Redundant modulo-two and modulo-four Hensel chains are consequences of the integer equations and therefore do not remove a genuine support. The resulting formula has

$$39{,}580 \text{ variables}, \qquad 127{,}589 \text{ clauses}.$$

Its SHA-256 digest is

`f3eb29b1ea9c386e53b03726349fe0c38577d7e187b56aa19f86412c8749755d`.

CaDiCaL 3.0.1 produced a binary DRAT proof in 200.17 seconds. The 90,490,737-byte compressed proof has digest

`efd8abd9d80d50365822754f36345f368d7cff8f2740ca33b9cab7d5866aa519`.

Independent `drat-trim` replay returned `VERIFIED`, using 73,135,509 resolution steps, 0 RAT lemmas, 75.00 seconds, and 471.1 MB peak resident memory.

The formal proof trace certifies the generated CNF. The mathematical interpretation additionally relies on the auditable encoder and on the reduction to the support equations; neither is formalized in a proof assistant.

6.3 Complete census of the nine short cases

The short cases have a common exact quotient structure. Modulo two, the 78 support variables form 39 pairs of equal syndrome columns. The affine quotient has rank 21, leaving 2^{18} parity states. For every state, a phase-adjusted parity splits the characteristic-three interaction graph into four cliques:

$$L_0,\ L_1,\ S_0,\ S_1.$$

After conditioning the common central pair, sums from these four components can be joined by exact packed modulo-six signatures. Any survivor is reconstructed as all 78 support bits, checked against the exact twenty-coordinate integer polynomial, and independently replayed in the four physical anti-fold rows.

Spatial reflection acts freely because every quotient state has an odd noncentral reflected pair. The canonical gauge fixes the lowest-index odd long-pair orientation. Two exceptional quotient states, one in $S08$ and one in $S14$, instead use the lowest odd short pair. The reflected mate of every retained representative is reconstructed, so the gauge loses no support.

Computational Theorem 6.2 (All nine short cases)**.** *The complete exact anti-fold support problems for cases* 21 *through* 29*, namely*

$$S02, S04, S06, S08, S10, S12, S14, S16, S18,$$

have no solution.

The frozen census is summarized below.

case	label	join rows	mod-6 survivors	best residual	
				$\# \neq 0$	ℓ_1
21	$S02$	412,316,860,416	9,564,254	4	72
22	$S04$	412,316,860,416	9,796,880	4	78
23	$S06$	412,316,860,416	9,807,738	3	54
24	$S08$	412,317,646,848	9,561,296	4	66
25	$S10$	412,316,860,416	9,789,738	3	72
26	$S12$	412,316,860,416	10,533,216	4	66
27	$S14$	412,317,646,848	10,285,492	3	66
28	$S16$	412,316,860,416	9,789,970	4	66
29	$S18$	412,316,860,416	9,799,156	4	66
	total	3,710,853,316,608	88,927,740		

(6.3)

All 88,927,740 modular survivors received both an exact integer-polynomial check and an independent bit-packed physical replay. The number of exact supports was zero. The production was partitioned into 2,304 atomic ranges. The completion certificate freezes every case total, best witness, source and binary hash, the original survivor-stream digest, and a timing-independent semantic range digest. Without the underlying range manifests, those stream digests are cryptographic commitments rather than independently inspectable survivor lists. The immutable companion release includes the production-manifest archive, so the live verifier can check all 2,304 records; an independent full production replay remains the strongest check.

Corollary 6.3 (Certified minimum-boundary frontier)**.** *Among the thirty canonical orientation-free anti-fold support problems at special distance* 41*, case* 0 *and all nine short cases are impossible. Only the twenty long cases* $1, \ldots, 20$ *remain.*

Remark 6.4. Corollary 6.3 is not a distance-41 nonexistence theorem. It closes ten support cases and leaves twenty. It also says nothing about repairs at larger special distance or about base sequences unrelated to Eliahou's seed.

7 Exact orientation cascade for the open long cases

The twenty open long instances all have 78 eligible support cells, split into 39 long and 39 short cells. Fix a support S of exact weight 39 that satisfies the characteristic-two anti-fold conditions and one of the two root profiles in (15). The remaining choice is which endpoint of each selected seed-opposite pair is changed.

For a selected cell i, let δ_i be the change in the four positive fold rows when the lower endpoint is chosen. The upper endpoint contributes $-\delta_i$. Encode the upper choice by $e_i \in \mathbb{F}_2$.

7.1 Modulo 8 is redundant

Let C_k be the summed periodic correlation at cyclic lag k of the positive folds. Exact expansion into constant, singleton, and pair coefficients proves the following.

Theorem 7.1 (Long-case orientation cascade)**.** *For each open long case* $1, \ldots, 20$*:*

1. *For every support in the full* 57*-dimensional affine anti-fold characteristic-two code, all positive-fold correlations vanish modulo* 8*, independently of endpoint orientation.*

2. *There is a support-independent binary matrix* $M_c \in \mathbb{F}_2^{23\times 78}$ *such that a support* S *selects its columns and the complete modulo-*16 *plus-fold and root-parity conditions are*

$$(M_c)_S e = b_{c,S,\rho}.$$

The first 21 *rows encode* $C_k/8 \bmod 2$ *and the final two rows encode the long- and short-block root-orientation parities.*

3. *On any consistent affine solution fiber of* (2)*, the four exact root values are equivalent, after a fixed sign gauge, to four disjoint Hamming-weight equations.*

4. *If a consistent fiber has free coordinates* $u_1, \dots, u_d$*, the next* 21 *plus-fold conditions modulo* 32 *are exact Boolean quadratics*

$$q_{c,S,\rho,k}(u) = 0, \qquad 1 \le k \le 21.$$

Proof outline and exact checks. For the first assertion, direct integer expansion proves that every positive-fold correlation is divisible by 4 for arbitrary support and that $C_k/4 \bmod 2$ is affine in the 78 support bits. Restricting these 21 affine functions to a basis and particular point of each complete 57-dimensional anti-fold affine code makes every coefficient and constant zero. All 20 cases and all 3,003 second differences per case were also reconstructed by an independent implementation.

Every orientation interaction coefficient

$$\langle \delta_i, T^k \delta_j \rangle + \langle \delta_j, T^k \delta_i \rangle$$

is divisible by 8. After division by 8 and reduction modulo 2, the orientation dependence is therefore affine, and the column belonging to cell i is independent of the other selected cells. This constructs M_c and proves (2).

For a block/parity bin G, let $a_j \in \{\pm 1\}$ be the signed root contribution in the lower orientation and put $n_j = e_j \,\mathsf{xor}\, [a_j = -1]$. A prescribed signed target t_G is equivalent to

$$\sum_{j\in G} a_j (-1)^{e_j} = |G| - 2\,\mathrm{wt}(n|_G) = t_G,$$

which is exactly one cardinality equation.

Finally, substitute an affine parameterization of the solution space of (2). An orientation flip changes a positive-fold coefficient by a multiple of 4. After division by 16 and reduction modulo 2, all terms of degree at least three vanish. Direct interpolation of every constant, linear, and quadratic coefficient, followed by physical replay at deterministic higher-weight points, proves (4). □

No universal lower bound on $\mathrm{rank}(M_c)_S$ is asserted. In the pinned audits, consistent supports usually had rank 22 and hence nullity 17, with a small number of nullity-18 fibers. Those counts are finite diagnostics, not a theorem about all supports.

Computational Proposition 7.2 (Sparse generation of the mod-2 support codes)**.** *For each of the twenty open long cases, the* 57*-dimensional homogeneous anti-fold characteristic-two code is generated by words of weight at most* 6*. In cases* 6 *and* 14*, weight at most* 4 *suffices. After adjoining the four block/parity profile checks, the homogeneous code has dimension* 55 *and is generated by words of weight at most* 6 *in every case.*

Exact rank certificate. The verifier `eliahou_long_orientation_cascade/audit_orientation_cascade.py` constructs the complete binary check matrix: the anti-fold linear rows and the all-ones weight-parity row, with the four block/parity rows adjoined in the profile-conditioned calculation. It encodes each coordinate column by its syndrome. Two unordered coordinate pairs with the same XOR syndrome have a symmetric difference in the kernel of weight at most 4. The verifier groups all pairs by syndrome, inserts these differences into an exact binary Gaussian basis, and records their rank. If that rank is not the full code dimension, it analogously groups all coordinate triples by syndrome; differences of equal-syndrome triples have weight at most 6. The resulting basis ranks are exactly 57 in every unconditioned case and 55 in every conditioned case. Pair differences already attain rank 57 in unconditioned cases 6 and 14, proving their stronger weight-4 statement. The ordered rank arrays and a semantic hash are frozen in `EXPECTED_SAMPLE5_SUMMARY.json`.

This provides an exact connected local-move system, but it does not bound the number of exact-weight-39 supports sharply enough for enumeration.

7.2 Certified finite controls

Two independent implementations used different deterministic sets of five supports per case and profile. Their exact finite results are:

	primary audit	red-team audit
supports tested	200	200
mod-16 inconsistent	5	5
points in consistent fibers	26,607,616	26,476,544
points satisfying exact roots	121,764	120,455
mod-32 survivors	22	24
mod-32 survivors satisfying exact roots	1	0

(17)

The one root-exact modulo-32 point in the primary audit was independently replayed and failed modulo 64. Thus all 400 pinned fixture evaluations were excluded at the recorded stage. Equation (17) is an exact statement about those fixed inputs only; it is not a sampling theorem, frequency estimate, or exclusion of any long case.

8 Why the two folds are not aperiodically complete

The positive and negative folds at the same 42 split do not reconstruct the original aperiodic norm. This point is essential to the scope of every computational claim above.

Proposition 8.1 (Two-fold scope correction)**.** *Let R_k be the summed aperiodic correlations of four rows of lengths $84, 84, 83, 83$. Exact positive-fold and anti-fold norm equations together are equivalent to the cyclic length-84 conditions*

$$R_{42} = 0, \qquad R_k + R_{84-k} = 0 \quad (1 \le k \le 41). \tag{18}$$

They do not imply $R_k = 0$ separately.

Adding the causal half

$$R_{43} = R_{44} = \cdots = R_{83} = 0 \tag{19}$$

to (18) *is equivalent to all* 83 *positive-lag aperiodic equations.*

Proof. Adding and subtracting the coefficient identities (10) and (16) yields exactly (18). The residual vector

$$R_1 = 2, \qquad R_{83} = -2, \qquad R_k = 0 \text{ otherwise}$$

is a nonzero integral kernel element, so the implication to aperiodic complementarity fails. If (19) is added, then (18) successively forces $R_1, \ldots, R_{41}$ to vanish as well, while $R_{42} = 0$ is already present. □

There is a compact exact ternary formulation of each long boundary case. For each eligible cell let

$$t_j \in \{-1, 0, 1\}, \qquad u_j = t_j^2,$$

where $t_j = 0$ means no change and the two nonzero signs choose the endpoint orientation. Then the exact physical problem is

$$\begin{aligned} \sum_j u_j &= 39, \\ 20 \text{ anti-fold equations} &\quad \text{in } u, \\ 21 \text{ positive-fold equations} &\quad \text{in } t, \\ 41 \text{ causal equations (19).} & \end{aligned} \tag{20}$$

Independent symbolic reconstruction verifies (20) against all original correlations in all twenty cases. The direct aperiodic model and the fold-plus-causal model each use exactly

$$5{,}928 = 1{,}482\,uu + 1{,}482\,ut + 1{,}482\,tu + 1{,}482\,tt$$

quadratic products. The causal equations touch all of them. Thus the folds expose strong modular structure, but they do not secretly eliminate the global aperiodic coupling.

9 Reproducibility and trust boundary

All paths below are relative to the public repository's `hadamard_668_search` directory. The accompanying paper README gives exact commands and separates quick verification from complete production replay.

Claim	**Primary artifact**	**Independent check**
Fixed-q reduction	`FIXED_Q_OBSTRUCTION.md`	`verify_fixed_q_obstruction.py`
Distance 80, boundary 41, root frontier	`ELIAHOU_ADJACENT42_REPAIR.md`	`verify_eliahou_adjacent42_repair.py`
Anti-fold reduction	`ELIAHOU_ANTIFOLD42.md`	`verify_eliahou_antifold42.py`
TU(41) exhaustion	`tu41_certificate/certificate.json`	`verify_manifest.py`, `verify_cube_cover.py`, `test_regressions.py`
Case-0 UNSAT	`output/antifold42_q0_proof/certificate.json`	`verify_eliahou_antifold_q0_proof.py`; full `drat-trim` replay
Nine short cases	`eliahou_short_block_census/NINE_CASE_COMPLETION_CERTIFICATE.json`	`verify_nine_case_completion.py`; independent model and physical replays
Long orientation cascade	`eliahou_long_orientation_cascade/`	separate `eliahou_long_orientation_redteam/` implementation

The trust levels are not identical.

- The algebraic reductions are short exact-integer identities with dependency-free reconstruction tests.
- The TU(41) result is an exhaustive C++ enumeration with an independently exhausted prefix cover. It trusts the displayed normalization, the small programs, and the compiler.
- The case-0 formula has an independently checked DRAT proof. It additionally trusts the formula generator's faithful encoding of the mathematical support problem.
- The nine-case certificate freezes the full production semantics, hashes, counts, and survivor streams. Bounded independent replays reconstruct quotient states and physical rows. Repeating all 3.71 trillion joins is possible with the resumable production driver but is not part of the quick verifier.
- The long-case statements labeled as theorems are complete symbolic audits over their stated affine spaces. The 200-support tables are explicitly bounded controls and have no extrapolated scope.

No solver timeout, interrupted search, or unproved solver `INFEASIBLE` status is used as a theorem in this manuscript. In particular, an older uncertified local-radius computation is intentionally omitted.

10 Discussion

The fixed-q theorem closes a natural but very narrow repair family. The adjacent fold then shows that "nearby" in the published special coordinates is already a global condition: an exact target cannot occur before distance 41, and equality forces the rigid $39 + 2$ form of Theorem 5.2. The anti-fold converts that boundary into a finite collection of orientation-free support equations. Ten of the thirty canonical instances are now exactly excluded.

The open part is not the endpoint-orientation layer by itself. Within the 400 bounded fixture evaluations in (17), Theorem 7.1 reduced a consistent fixed-support orientation problem from 2^{39} raw choices to a modulo-16 affine fiber usually of size about 2^{17} before the exact root and quadratic modulo-32 filters. No 2^{17} fiber-size claim is made for untested supports or for a complete long case. The bottleneck is the enormous collection of admissible supports and the aperiodic causal coupling in Proposition 8.1. A successful continuation appears to require a support-level theorem or a method that couples support and orientation algebraically; a literal support-first census remains out of reach on ordinary hardware.

The known empty status of TU(41) is not claimed as new. The independent enumeration is valuable as a modern, inspectable reproduction. The basic special-form/BS$(84, 83)$ equivalence and a weaker distance bound were already present in the companion release to Ramos–Hulak–de Queiroz [8]. We did not locate the distance-80 fold, special-distance-41 classification, anti-fold certificates, or long orientation cascade in the cited public sources. That literature search is not a guarantee of priority.

Code and data availability

The immutable companion release is

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

The paper package identifies the exact source paths and hashes used for this draft. The companion release includes the case-0 compressed DRAT artifact and a production-manifest archive for the nine short cases. Large artifacts are additionally identified by cryptographic digests. No external communication or independent peer validation occurred during preparation of this draft.

AI assistance and responsibility

The research program was conducted by Alec Kriebel with extensive assistance from ChatGPT 5.6 Sol, operating through ChatGPT and Codex. AI assistance included proposing reductions, deriving and checking algebra, writing and optimizing exact enumerators, constructing certificate verifiers, auditing scope, and drafting this manuscript. The human author selected the research directions and requested the explicit scope and verification disclosures. Language-model output can contain subtle mathematical or implementation errors. Readers should therefore treat every claim as provisional until the proofs, encodings, and computations receive independent expert review. The software and certificates are provided to make that review feasible, not to transfer responsibility to the tools.

References

[1] M. Cati and D. V. Pasechnik, *A database of constructions of Hadamard matrices*, arXiv:2411.18897 (2024); `https://arxiv.org/abs/2411.18897`.

[2] D. Ž. Đoković, Aperiodic complementary quadruples of binary sequences, *J. Combin. Math. Combin. Comput.* **27** (1998), 3–31; `https://combinatorialpress.com/article/jcmcc/Volume%20027/vol-27-paper%201.pdf`.

[3] D. Ž. Đoković, Classification of base sequences BS$(n+1, n)$, *Int. J. Combin.* (2010), Article ID 851857; `https://arxiv.org/abs/1002.1414`.

[4] G. M. Edmondson, J. Seberry, and M. R. Anderson, On the existence of Turyn sequences of length less than 43, *Math. Comp.* **62** (1994), 351–362; `https://doi.org/10.1090/S0025-5718-1994-1203733-8`.

[5] S. Eliahou, A 64-modular Hadamard matrix of order 668, *Australas. J. Combin.* **93**(2) (2025), 422–427; `https://ajc.maths.uq.edu.au/pdf/93/ajc_v93_p422.pdf`.

[6] S. Eliahou, An update on modular Hadamard matrices, *J. Algebraic Combin.* **64** (2026), Article 1; `https://doi.org/10.1007/s10801-026-01544-5`. Only its bibliographic metadata and abstract were inspected for this draft; the full text was not inspected.

[7] A. F. Ramos, D. B. Hulak, and R. J. G. B. de Queiroz, *Multiplier obstructions for Legendre pairs of length 333*, arXiv:2607.20765 (2026); `https://arxiv.org/abs/2607.20765`.

[8] A. F. Ramos, D. B. Hulak, and R. J. G. B. de Queiroz, *Hadamard-668 multiplier-obstruction proof artifacts*, companion repository and mod-64 report (2026); `https://github.com/Arthur742Ramos/hadamard-668-multiplier-obstructions`.

[9] SageMath, *Hadamard matrix constructions and current unknown orders*; `https://doc.sagemath.org/html/en/reference/combinat/sage/combinat/matrices/hadamard_matrix.html`.