Butson towers and high-rank Hadamard matrices

Alexander Kolpakov

28 November 2026

hexagon:2611.01070v3

Abstract

We construct real Hadamard matrices of forty-nine new orders and obtain seventeen new infinite families. The constructions are explicit: we prove the Gram identities and show that every final entry is 1 or -1.

1 Results and conventions

A *sign matrix* is a real matrix with entries in $\{1, -1\}$. A real Hadamard matrix of order n is an $n \times n$ sign matrix H satisfying $HH^{\mathsf{T}} = nI_n$, where I_n is the identity matrix. This identity implies $H^{-1} = H^{\mathsf{T}}/n$, so the rank of H is n. Throughout the paper, "new" means new to the best of the author's knowledge. Section 8 discusses known orders and matrix equivalence; Appendix G gives the full comparison data.

Theorem 1. *Real Hadamard matrices exist at each of the following forty-nine new orders:*

$$\begin{gathered}
7572,\quad 17668,\quad 22716,\quad 26168,\quad 26968,\quad 32812\\
42808,\quad 42908,\quad 44728,\quad 55288,\quad 58052,\quad 66328\\
73196,\quad 75128,\quad 78244,\quad 80728,\quad 82168,\quad 86168\\
91288,\quad 91768,\quad 93388,\quad 98436,\quad 108532,\quad 118628\\
128724,\quad 133772,\quad 148916,\quad 153964,\quad 169108,\quad 174156\\
184252,\quad 199396,\quad 229684,\quad 234732,\quad 244828,\quad 259972\\
275116,\quad 295308,\quad 320548,\quad 386172,\quad 2985892,\quad 4772884\\
13001124,\quad 15131380,\quad 31305172,\quad 38816596,\quad 47251804,\quad 68806764\\
291145924.
\end{gathered}$$

They also exist at every order in the following seventeen families:

$$\begin{gathered}
7572 \cdot 5^r,\qquad 17668 \cdot 13^r,\qquad 22716 \cdot 17^r\\
32812 \cdot 3^r,\qquad 78244 \cdot 61^r,\qquad 128724 \cdot 101^r\\
153964 \cdot 121^r,\qquad 174156 \cdot 137^r,\qquad 15131380 \cdot 109^r\\
32812 \cdot 25^r,\qquad 93388 \cdot 73^r,\qquad 199396 \cdot 157^r\\
229684 \cdot 181^r,\qquad 244828 \cdot 193^r,\qquad 295308 \cdot 233^r\\
13001124 \cdot 10301^r,\qquad 38816596 \cdot 30757^r\\
(r \in \mathbb{Z}_{\geq 0}).
\end{gathered}$$

A bar denotes complex conjugation, and $A^* = \overline{A}^{\mathsf{T}}$ is the conjugate transpose of a matrix. We call a square complex matrix of order n *flat* if every entry has absolute value 1. A Butson matrix $\mathrm{BH}(n, k)$ is a flat matrix B whose entries are kth roots of unity and for which $BB^* = nI_n$. For an arbitrary matrix satisfying $BB^* = wI_n$, we call w its *Gram scale*. When constructing a Hadamard matrix, we also prove $w = n$. Matrices and vectors are indexed starting at 0. The symbol $\delta_{x,y}$ is 1 if $x = y$ and 0 otherwise. For a prime p, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is represented by $0, \ldots, p-1$, with arithmetic reduced modulo p.

We use *Butson tower* as a descriptive name for a finite chain of restrictions of scalars applied to a matrix satisfying a Gram identity, starting with a Butson matrix or one of the explicitly defined weighted sources below.

At each step we keep track of the scalar action, involution and trace form. A tower may consist of a single restriction. We allow nonflat intermediate matrices, but prove flatness for the final matrix directly from its entries. Restriction of scalars and Butson morphisms are classical; our starting point was Egan and Ó Catháin's recent work [11], together with the earlier constructions [10, 12, 14].

The scalar restrictions start from a vector-valued function on $\mathbb{F}_{631}$ whose correlation identity is proved in Appendix A. It gives a sixth-root scalar action and four matrices into which we can substitute commuting sign matrices. The same construction on $\mathbb{F}_{127}$ gives periodic T-matrices of order 127. Sixteen of the listed families follow by combining this construction with Spence's classical recurrence for the source matrices. They are special cases of a uniform prime-power theorem. The remaining family uses classical tripling of a sixth-root source. The appendices contain the finite inputs, expanded calculations and verification programs.

2 The common coefficient construction

2.1 The finite T-matrix ingredient

Let e_0, e_1, e_2, e_3 be the standard basis of $\mathbb{Z}^4$. We use a function

$$b : \mathbb{F}_p \longrightarrow \{\pm e_0, \pm e_1, \pm e_2, \pm e_3\}, \qquad p \in \{631, 127\},$$

whose coordinates satisfy

$$\sum_{j=0}^{3} \sum_{x \in \mathbb{F}_p} b_j(x) b_j(x+s) = p\delta_{s,0}. \tag{1}$$

Appendix A specifies both functions by short orbit tables and proves this identity by integer calculation at every shift. The four coordinate functions have disjoint supports covering $\mathbb{F}_p$, so their circulants are periodic T-matrices. In particular this gives the new periodic T-matrices of order 127, as well as the length-631 input used for the Hadamard orders below.

We now derive the coefficient design from this correlation identity.

2.2 Circulants and reversal

Let G be a finite abelian group, written additively. For a function $f\colon G \to \mathbb{R}$, define its circulant matrix L_f by

$$(L_f)_{u,v} = f(v-u) \qquad (u, v \in G).$$

For $G = \mathbb{Z}/w\mathbb{Z}$ we also write $\mathrm{Circ}(f) = L_f$. Define $f^-(x) = f(-x)$ and the convolution $(f * g)(z) = \sum_{x \in G} f(x)g(z-x)$. Computing the entries of the matrix products gives

$$L_f^{\mathsf{T}} = L_{f^-}, \qquad L_f L_g = L_{f*g} = L_g L_f,$$

since $(L_f L_g)_{u,v} = \sum_x f(x)g(v-u-x)$, and substituting $x \mapsto v-u-x$ interchanges f, g. The row Gram has entries

$$(L_f L_f^{\mathsf{T}})_{u,v} = \sum_{x \in G} f(x) f(x+v-u). \tag{2}$$

In the matrix product, substitute $x = t - v$ and use commutativity of multiplication in $\mathbb{R}$.

Fix any $t \in G$. Let $\mathcal{J}$ be the permutation matrix $\mathcal{J}_{u,v} = \delta_{u+v,t}$. The permutation $u \mapsto t-u$ is its own inverse, so $\mathcal{J}^{\mathsf{T}} = \mathcal{J}$ and $\mathcal{J}^2 = I$. Moreover

$$(\mathcal{J} L_f \mathcal{J})_{u,v} = f((t-v)-(t-u)) = f(u-v), \qquad \mathcal{J} L_f \mathcal{J} = L_f^{\mathsf{T}}.$$

For the length-p constructions, take $G = \mathbb{F}_p$ additively and $t = -1$. Thus $\mathcal{J}_{u,v} = 1$ when $u + v = p - 1$.

For four functions f_0, f_1, f_2, f_3 on the same group, set $A = L_{f_0}, B = L_{f_1}, C = L_{f_2}, D = L_{f_3}$ and define

$$\mathrm{GS}(f) = \begin{pmatrix} A & B\mathcal{J} & C\mathcal{J} & D\mathcal{J} \\ -B\mathcal{J} & A & -D^{\mathsf{T}}\mathcal{J} & C^{\mathsf{T}}\mathcal{J} \\ -C\mathcal{J} & D^{\mathsf{T}}\mathcal{J} & A & -B^{\mathsf{T}}\mathcal{J} \\ -D\mathcal{J} & -C^{\mathsf{T}}\mathcal{J} & B^{\mathsf{T}}\mathcal{J} & A \end{pmatrix}. \tag{3}$$

Every block has order $|G|$. The transpose of a circulant is again a circulant, so all of $A, B, C, D, A^\mathsf{T}, B^\mathsf{T}, C^\mathsf{T}, D^\mathsf{T}$ commute. Using this and $\mathcal{J}X\mathcal{J} = X^\mathsf{T}$, each diagonal block of $\mathrm{GS}(f)\,\mathrm{GS}(f)^\mathsf{T}$ is $N = AA^\mathsf{T} + BB^\mathsf{T} + CC^\mathsf{T} + DD^\mathsf{T}$. The off-diagonal blocks vanish by the same commutation identities; Appendix A.2 lists all six expressions. Thus

$$\mathrm{GS}(f)\,\mathrm{GS}(f)^\mathsf{T} = I_4 \otimes \sum_{j=0}^{3} L_{f_j} L_{f_j}^\mathsf{T}. \tag{4}$$

Here $A \otimes B$ is the Kronecker product, with entry $A_{i,j}B_{u,v}$ at row (i,u) and column (j,v). The product rule $(A \otimes B)(C \otimes D) = AC \otimes BD$ follows by summing independently over the two middle indices.

Taking $f = b$ from Section 2.1, equations (2) and (1) imply $\sum_j L_{b_j} L_{b_j}^\mathsf{T} = pI_p$. The four matrices L_{b_j} have pairwise disjoint supports, and exactly one of them is 1 or -1 at each position: their entries there are the four coordinates of the same $b(v-u)$. These are the defining properties of *periodic T-matrices*, so the construction gives such matrices for both $p = 631$ and $p = 127$.

2.3 Four coefficient matrices with disjoint supports

For $x = (x_0, x_1, x_2, x_3)^\mathsf{T} \in \mathbb{R}^4$ define

$$M(x) = \begin{pmatrix} x_0 & -x_1 & -x_2 & -x_3 \\ x_1 & x_0 & x_3 & -x_2 \\ x_2 & -x_3 & x_0 & x_1 \\ x_3 & x_2 & -x_1 & x_0 \end{pmatrix}.$$

Direct multiplication gives $M(x)^\mathsf{T}M(x) = (\sum_j x_j^2)I_4$; the individual products are listed in Appendix A.2. Set $f^x(u) = M(x)b(u)$, a vector of four functions on $\mathbb{F}_p$. Then for every shift s,

$$\sum_u f^x(u)^\mathsf{T} f^x(u+s) = \sum_u b(u)^\mathsf{T} M(x)^\mathsf{T} M(x) b(u+s) = p\Big(\sum_j x_j^2\Big)\delta_{s,0}.$$

By (4), the matrix $\mathrm{GS}(f^x)$ therefore has Gram $p(\sum_j x_j^2)I_{4p}$. It is linear in x, so define its four coefficient matrices by

$$X_j = \mathrm{GS}(f^{e_j}), \qquad \mathrm{GS}(f^x) = \sum_{j=0}^{3} x_j X_j.$$

Putting $x = e_j$ proves $X_j X_j^\mathsf{T} = pI_{4p}$. Putting $x = e_i + e_j$ for $i \neq j$ and subtracting the two individual identities proves

$$X_j X_j^\mathsf{T} = pI_{4p}, \qquad X_i X_j^\mathsf{T} + X_j X_i^\mathsf{T} = 0 \quad (i \neq j). \tag{5}$$

We must check the supports separately from the Gram identities. Since $b(u)$ is a signed standard basis vector, $f^x(u)$ is a signed column of $M(x)$. Every entry of every such column is exactly one of $x_0, -x_0, \ldots, x_3, -x_3$. Every entry of $\mathrm{GS}(f^x)$ is, by (3), a signed entry of one of these vectors. Consequently, at every position exactly one X_j is nonzero, and that entry is 1 or -1. Their supports are therefore disjoint and cover all matrix positions.

The Gram identities control inner products; the support partition ensures that each final entry is a single signed entry from an input matrix. The next proposition combines these two facts, reducing the Hadamard condition to relations among the four inputs.

Proposition 2. *Suppose A_0, A_1, A_2, A_3 are sign matrices of order w satisfying*

$$\sum_{j=0}^{3} A_j A_j^\mathsf{T} = 4wI_w, \qquad A_i A_j^\mathsf{T} = A_j A_i^\mathsf{T} \quad (i \neq j).$$

Then $H = \sum_{j=0}^{3} X_j \otimes A_j$ is a real Hadamard matrix of order $4pw$, for either of the two values of p above.

Proof. At each position of H there is exactly one nonzero summand, the product of a sign in an X_j and a sign in A_j. Thus H is a sign matrix. In its Gram product, the two terms belonging to $i < j$ have sum

$$X_i X_j^\mathsf{T} \otimes A_i A_j^\mathsf{T} + X_j X_i^\mathsf{T} \otimes A_j A_i^\mathsf{T} = (X_i X_j^\mathsf{T} + X_j X_i^\mathsf{T}) \otimes A_i A_j^\mathsf{T} = 0.$$

The diagonal terms sum to $pI_{4p} \otimes \sum_j A_j A_j^\mathsf{T} = 4pwI_{4pw}$. This is the required Hadamard identity. □

2.4 The same construction as restriction of scalars

The Williamson and Spence source matrices used below are circulants on finite abelian groups. We now express their construction as restriction of scalars. For a finite abelian group G of order w, let $\mathbb{Q}[G]$ be the vector space with basis symbols c_g for $g \in G$, with multiplication $c_g c_h = c_{g+h}$ and identity c_0. Extend this multiplication bilinearly. It is a commutative algebra. Define the involution $c_g^* = c_{-g}$, extended $\mathbb{Q}$-linearly, and $\tau(\sum_g a_g c_g) = a_0$.

Use the ordered basis $\beta_g = c_{-g}$, where an ordering of G is fixed. For $a = \sum_g a_g c_g$, let $\rho(a)$ be the matrix of multiplication by a in this basis. The coefficient of $\beta_u = c_{-u}$ in $a\beta_v = \sum_g a_g c_{g-v}$ is a_{v-u}. Therefore

$$\rho(a)_{u,v} = a_{v-u}, \quad \rho(ab) = \rho(a)\rho(b), \quad \rho(a^*) = \rho(a)^{\mathsf{T}}. \tag{6}$$

The first identity proves the third; the second follows because the composition of multiplication by b and by a is multiplication by ab. The action is faithful, since multiplication by a applied to c_0 recovers a. Its trace is $\mathrm{Tr}(\rho(a)) = wa_0$, so τ is the normalized regular trace. Moreover

$$\tau(\beta_u^* \beta_v) = \delta_{u,v}.$$

Thus the trace metric in the chosen basis is I_w, with no change of basis or rescaling.

Suppose $f_j = \sum_{g \in G} a_j(g) c_g$ satisfy

$$f_i f_j^* = f_j f_i^*, \qquad \sum_{j=0}^{3} f_j f_j^* = 4w c_0, \qquad a_j(g) \in \{1, -1\}.$$

The matrix $S = \sum_j X_j f_j$ has order $4p$ over $\mathbb{Q}[G]$. By (5), the cancellation in Proposition 2 gives $SS^* = 4pwI_{4p}$, where the matrix involution transposes entries and applies $*$ to each entry. Its entries are signed copies of the four explicit elements f_j, by the support property of X_j. Applying ρ entrywise replaces them with the sign circulants $\rho(f_j)$ and gives a rational matrix of order $4pw$ with Gram $4pwI_{4pw}$. This is restriction of scalars from $\mathbb{Q}[G]$ to $\mathbb{Q}$. The source has order $4p$ and Gram scale $4pw$. The algebra has rational dimension w and trace metric I_w. The source entries are the signed group-algebra elements defined above. For symmetric commuting sign circulants $A_j = L_{a_j}$ satisfying $\sum_j A_j A_j^{\mathsf{T}} = 4wI_w$, the multiplication and transpose identities, together with faithfulness of ρ, give all three hypotheses on f_j.

2.5 Two sign matrices for sixth-root scalars

For this subsection take $p = 631$, although the argument also works for 127. Define the integer matrix

$$\Delta = \begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & 1 & -1 \\ -1 & -1 & 0 & 1 \\ -1 & 1 & -1 & 0 \end{pmatrix}, \qquad a(u) = \Delta b(u).$$

Its transpose is $-\Delta$. Its columns have squared length 3, and their six pairwise dot products are 0, giving $\Delta^{\mathsf{T}}\Delta = 3I_4$. It follows from (1) that

$$\sum_u a(u)^{\mathsf{T}} a(u+s) = 3p\delta_{s,0}.$$

Also, for every s,

$$\sum_u \big(a(u)^{\mathsf{T}} b(u+s) + b(u)^{\mathsf{T}} a(u+s)\big) = \sum_u b(u)^{\mathsf{T}} (\Delta^{\mathsf{T}} + \Delta) b(u+s) = 0.$$

Consequently the summed correlation of $a + tb$, for any real number t, is $(3 + t^2)p\delta_{s,0}$. Put

$$U = \mathrm{GS}(a), \qquad V = \mathrm{GS}(b), \qquad d = 4p = 2524.$$

Linearity of (3) gives $\mathrm{GS}(a + tb) = U + tV$. Equation (4), first with a, then with b, and then with $a + b$, proves respectively

$$UU^{\mathsf{T}} = 3pI_d, \qquad VV^{\mathsf{T}} = pI_d, \qquad UV^{\mathsf{T}} + VU^{\mathsf{T}} = 0.$$

At each residue u, the vector $b(u)$ is a signed column of I_4, and $a(u)$ is the same signed column of Δ. That column of Δ is zero in precisely the coordinate occupied by $b(u)$ and is a sign in its other three coordinates. Thus $a_i(u)$ and $b_i(u)$ have complementary supports, and each nonzero entry is a sign. Since the block layout of GS acts on a and b in exactly the same positions, the same assertion holds entrywise for U, V. Therefore

$$P = U - V, \qquad Q = U + V$$

are both sign matrices. Expanding their products yields

$$\begin{aligned} PP^{\mathsf{T}} = QQ^{\mathsf{T}} = UU^{\mathsf{T}} + VV^{\mathsf{T}} = 4pI_d = dI_d, \\ PQ^{\mathsf{T}} + QP^{\mathsf{T}} = 2(UU^{\mathsf{T}} - VV^{\mathsf{T}}) = 4pI_d = dI_d. \end{aligned} \tag{7}$$

We will use these three identities for P, Q in the scalar action. The matrices themselves are given explicitly above.

3 Restriction of scalars and a sixth-root example

Restriction of scalars preserves a Gram identity with its trace metric. Let K be a finite-dimensional commutative $\mathbb{Q}$-algebra with an involution, and choose a $\mathbb{Q}$-linear functional τ satisfying $\tau(\bar{z}) = \tau(z)$. In a basis $\beta_0, \ldots, \beta_{m-1}$, let $\rho(z)$ represent multiplication by z and put $G_{ab} = \tau(\bar{\beta}_a \beta_b)$. If G is invertible, then

$$\rho(\bar{z}) = G^{-1}\rho(z)^{\mathsf{T}}G.$$

Consequently, a matrix N with $NN^* = wI_n$ for $w \in \mathbb{Q}$ gives a rational matrix $X = (\rho(N_{ij}))$ of order mn satisfying

$$X(I_n \otimes G^{-1})X^{\mathsf{T}} = w(I_n \otimes G^{-1}).$$

The dimension has increased, while the Gram scale remains w. The trace metric must therefore be carried through the construction. Lemma 6 in Appendix B proves these identities and explains their compatibility with successive restrictions, including products of fields and nonidentity incoming forms.

To obtain a Hadamard matrix, we need a compatible representation and a separate condition on the final entries.

Proposition 3. *Let n, d be positive integers and let $\rho : K \longrightarrow M_d(\mathbb{Q})$ be a unital $\mathbb{Q}$-algebra homomorphism with $\rho(\bar{z}) = \rho(z)^{\mathsf{T}}$. Suppose that $N \in K^{n\times n}$ and $F \in \mathbb{Q}^{d\times d}$ satisfy $NN^* = wI_n$ and $FF^{\mathsf{T}} = cI_d$ for $w, c \in \mathbb{Q}$. Form the block matrix $H_{ij} = \rho(N_{ij})F$. Then*

$$HH^{\mathsf{T}} = cwI_{dn}.$$

If every entry of these blocks is a sign and $cw = dn$, then H is a real Hadamard matrix of order dn.

Proof. The (i, j) block of the Gram matrix is

$$\sum_k \rho(N_{ik})FF^{\mathsf{T}}\rho(N_{jk})^{\mathsf{T}} = c\rho\left(\sum_k N_{ik}\overline{N_{jk}}\right) = cw\delta_{ij}I_d.$$

The other two hypotheses give the sign entries and the required scale. □

The matrices P, Q above give a concrete example. Put $d = 2524$ and

$$\xi = \sqrt{-3} = \mathrm{i}\sqrt{3}, \qquad \zeta = \frac{1+\xi}{2}, \qquad K = \mathbb{Q}(\zeta), \qquad R = \frac{1}{d}QP^{\mathsf{T}}.$$

The frame identities (7) imply

$$RR^{\mathsf{T}} = I_d, \qquad R + R^{\mathsf{T}} = I_d, \qquad R^2 - R + I_d = 0, \qquad RP = Q.$$

Since $t^2 - t + 1$ is irreducible over $\mathbb{Q}$, these relations define the faithful representation

$$\rho(a + b\zeta) = aI_d + bR, \qquad \rho(\bar{z}) = \rho(z)^{\mathsf{T}}.$$

Here $[K:\mathbb{Q}]=2$, whereas $\mathbb{Q}^d$ has dimension 1262 over K. The identity metric in these coordinates comes from a Hermitian form: with $S=2R-I_d$, set

$$h(u,v)=\frac{u^{\mathsf{T}}v}{2}-\frac{u^{\mathsf{T}}Sv}{6}\,\xi,\qquad \operatorname{Tr}_{K/\mathbb{Q}}h(u,v)=u^{\mathsf{T}}v.$$

Appendix B proves the representation and form identities, and compares this realization with the regular representation in the basis $(1,\zeta)$.

The four scalars $1,\zeta,-1,-\zeta$ give sign blocks $P,Q,-P,-Q$ when their representations are multiplied by P. In particular, take

$$M=\begin{pmatrix}-1&\zeta&\zeta\\ \zeta&-1&\zeta\\ \zeta&\zeta&-1\end{pmatrix},\qquad H=\begin{pmatrix}-P&Q&Q\\ Q&-P&Q\\ Q&Q&-P\end{pmatrix}.$$

The relation $\zeta+\bar{\zeta}=1$ gives $MM^*=3I_3$. Proposition 3, with $F=P$ and $c=d$, therefore gives $HH^{\mathsf{T}}=7572I_{7572}$. More generally, any order-n source with entries in $\{1,\zeta,-1,-\zeta\}$ and Gram nI_n gives a Hadamard matrix of order $2524n$. The restriction to this four-element alphabet matters: $\rho(\zeta^2)P=Q-P$ has zeros and entries of absolute value 2, as shown in Appendix B.

The next three sections apply the length-631 construction to finite commuting quadruples, Spence's recurrence and sixth-root tripling. These give the individual orders and the two family constructions. We then turn to the paired construction, which uses a different coefficient design and also requires a conference matrix.

4 Finite commuting sources

Set $p=631$ in Proposition 2. For symmetric, pairwise commuting sign matrices of order w, its hypotheses reduce to

$$\sum_{j=0}^{3}A_j^2=4wI_w.$$

The classical Williamson inputs in the Sage table [4] give the thirteen widths

$$w\in\{3,7,9,13,17,23,29,31,37,39,43,51,61\}.$$

The published near-Williamson inputs [5], together with the Williamson quadruple of order 69 [6], give twelve more:

$$w\in\{47,53,59,67,69,73,79,93,97,103,109,127\}.$$

For these inputs the first matrix may be a symmetric back-circulant, obtained by multiplying a circulant by the reversal matrix; the other three are symmetric circulants. Their symmetry and commutation, and the summed cyclic correlations, are checked in Appendix C. Substitution gives the twenty-five distinct new orders $2524w$ in Theorem 1. The first of these, 7572, also has the sixth-root construction above.

The scalar interpretation keeps the full algebra $\mathcal{A}=\mathbb{Q}[A_0,A_1,A_2,A_3]$ and its action on $\mathbb{Q}^w$. In the noncyclic cases it is a product of totally real fields, acting with the module multiplicities recorded in Appendix C. All field factors and multiplicities enter the normalized trace. If the columns of B form the chosen rational basis adapted to the field decomposition, the transported Euclidean metric is $B^{\mathsf{T}}B$. Returning to the original basis recovers the sign matrices used in the substitution. The appendix includes the field degrees, multiplicities and rational reconstruction.

5 Infinite families from Spence's recurrence

The length-631 construction combines with classical Turyn starters and Spence's recurrence to give a uniform existence theorem. This accounts for sixteen of the seventeen families in Theorem 1.

Theorem 4. *For every prime power $q\equiv 1 \pmod 4$ and every integer $r\geq 0$, there is a real Hadamard matrix of order*

$$1262(q+1)q^r.$$

Proof. Put $w_0 = (q+1)/2$. Turyn's construction [18] gives symmetric commuting circulants $R+I, R-I, S, S$ of order w_0, with sign entries and $R^2+S^2 = qI$; see [8, Theorem 2 and Lemma 1, p. 352]. Starting with

$$D_0 = E_0 = S, \qquad F_0 = R+I, \qquad G_0 = R-I,$$

we have

$$(D_0-E_0)^2 + (F_0-G_0)^2 = 4I, \qquad (D_0+E_0)^2 + (F_0+G_0)^2 = 4qI.$$

Let χ_q be the quadratic character on $\mathbb{F}_q$, extended by zero at zero, and put $(K_q)_{x,y} = \chi_q(y-x)$. Let J_q be the all-one matrix. Since $q \equiv 1 \pmod 4$, the Paley identities are

$$K_q^{\mathsf{T}} = K_q, \quad K_q^2 = qI_q - J_q, \quad K_qJ_q = J_qK_q = 0, \quad J_q^2 = qJ_q.$$

The diagonal of K_q is zero and its other entries are signs. The character-sum proof and explicit finite-field conventions are in Appendix D.

Spence's recurrence [7, Theorem 4, p. 254] replaces each ordered pair (U, V) by

$$\begin{aligned} U' &= \tfrac{1}{2}(U-V)\otimes J_q + \tfrac{1}{2}(U+V)\otimes (K_q+I_q), \\ V' &= \tfrac{1}{2}(U-V)\otimes J_q + \tfrac{1}{2}(U+V)\otimes (K_q-I_q). \end{aligned} \tag{8}$$

Apply this to (D_r, E_r) and (F_r, G_r) at each step. The half-sum and half-difference have disjoint entry supports. Both K_q+I_q and K_q-I_q have sign entries, so the new entries are signs. Symmetry and commutativity are preserved because the old matrices commute and the second factors lie in the commutative algebra generated by I_q, J_q, K_q.

To track the norm, write

$$M_r = (D_r-E_r)^2 + (F_r-G_r)^2, \qquad N_r = (D_r+E_r)^2 + (F_r+G_r)^2.$$

Adding and subtracting the two lines of (8) gives

$$U'-V' = (U+V)\otimes I_q, \qquad U'+V' = (U-V)\otimes J_q + (U+V)\otimes K_q.$$

The mixed terms in the square of the second expression vanish. Hence

$$M_{r+1} = N_r \otimes I_q, \qquad N_{r+1} = qN_r \otimes I_q + (qM_r - N_r)\otimes J_q.$$

The term involving the all-one matrix explains why the summed Williamson norm alone does not suffice. We need separate identities for the sums and differences in each pair: their initial scales make that term vanish, and the recurrence preserves the relation. Consequently the component width and the summed Gram scale grow by the same factor at every step.

From $M_0 = 4I$ and $N_0 = 4qI$, induction gives $M_r = 4q^rI$ and $N_r = 4q^{r+1}I$. Thus, with $w_r = w_0q^r$,

$$D_rD_r^{\mathsf{T}} + E_rE_r^{\mathsf{T}} + F_rF_r^{\mathsf{T}} + G_rG_r^{\mathsf{T}} = \tfrac{1}{2}(M_r+N_r) = 4w_rI.$$

The four matrices therefore satisfy the hypotheses of Proposition 2, which gives order $2524w_r = 1262(q+1)q^r$. □

The sixteen Spence families in Theorem 1 use

$$q \in \{5, 13, 17, 25, 61, 73, 101, 109, 121, 137, 157, 181, 193, 233, 10301, 30757\}.$$

Except at $q = 109$, we start each sequence at its new initial order. The order 138820 at $q = 109, r = 0$ is known, so that family starts at $138820 \cdot 109^{r+1} = 15131380 \cdot 109^r$. These sixteen specializations and the cubic family are the seventeen sequences counted in the main theorem; the uniform theorem is not counted separately.

For example, $q = 13$ starts with source width 7 and Hadamard order 17668. One recurrence step gives width 91 and order 229684; the same length-631 coefficient design is used at both stages.

Each sequence contains infinitely many orders outside the other sixteen. For sequences ap^{er} and $b\ell^{fs}$ with distinct primes p, ℓ, comparison of their p- and ℓ-valuations fixes r, s, so they have at most one common term. The only repeated growth prime is 5, in the multipliers 5 and 25. Their initial terms have quotient $32812/7572 =$

13/3, so those two sequences are disjoint. Some families nevertheless share an initial order; for example, $295308 = 32812 \cdot 3^2$.

Appendix D gives the explicit starters, finite-field arithmetic and full recurrence calculations. Its listed starters may be used in place of Turyn's source, since they satisfy the same strong norm identities. The source group is $C_{w_0} \times (\mathbb{F}_q, +)^r$; for $q = p^e$, each additive field factor is $(C_p)^e$. In particular the field-of-order-25 construction uses two coordinates modulo 5, not one coordinate modulo 25. The group-algebra interpretation and normalized trace are those of Section 2.4.

Computing the first recurrence step at $q = 157, 193, 233$ gives the new orders 31305172, 47251804 and 68806764. The same computation at $q = 25, 73, 181$ gives the known orders 820300, 6817324 and 41572804. The first-step coefficient rows at $q = 10301, 30757$ were not computed, so we omit those first-step orders from the finite inventory. Existence at every step follows from the theorem. Appendix D.2 contains the independent integer checks. Section 9 describes which results also have Lean proofs.

6 The cubic family

The remaining family comes from classical sixth-root tripling [14]. We start with sign matrices A_0, B_0 of order 13 such that

$$A_0 B_0^{\mathsf{T}} = B_0 A_0^{\mathsf{T}}, \qquad A_0 A_0^{\mathsf{T}} + 3B_0 B_0^{\mathsf{T}} = 52 I_{13}.$$

The explicit rows and their finite verification are given in Appendix E.

More generally, suppose A, B are sign matrices of order n satisfying $AB^{\mathsf{T}} = BA^{\mathsf{T}}$ and $AA^{\mathsf{T}} + 3BB^{\mathsf{T}} = 4nI_n$. Let J_3 be the all-one matrix of order 3 and put

$$C = \begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}, \qquad A' = B \otimes J_3, \qquad B' = A \otimes I_3 + B \otimes C.$$

The diagonal and off-diagonal supports in B' are disjoint, so both new matrices are sign matrices. The identities $C^{\mathsf{T}} = -C$, $CC^{\mathsf{T}} = 3I_3 - J_3$ and $CJ_3 = J_3 C = 0$ give

$$A'B'^{\mathsf{T}} = B'A'^{\mathsf{T}}, \qquad A'A'^{\mathsf{T}} + 3B'B'^{\mathsf{T}} = 3(AA^{\mathsf{T}} + 3BB^{\mathsf{T}}) \otimes I_3 = 12nI_{3n}.$$

Thus iteration gives sign pairs A_r, B_r of order $n_r = 13 \cdot 3^r$ with the same two identities. The quadruple (A_r, B_r, B_r, B_r) therefore satisfies Proposition 2, giving Hadamard matrices of order

$$2524 n_r = 32812 \cdot 3^r, \qquad r \geq 0.$$

There is also a sixth-root realization, which will matter for the matrix comparison below. With ξ, ζ, ρ, P as in Section 3, define

$$N_r = \zeta^{-1} \frac{A_r + \xi B_r}{2}, \qquad H^{(r)} = \rho(N_r)(I_{n_r} \otimes P). \tag{9}$$

The two pair identities give $N_r N_r^* = n_r I_{n_r}$, and its entries lie in $\{1, \zeta, -1, -\zeta\}$, so the scalar-frame proposition gives the same orders. Appendix E proves these assertions and the tripling identities in full. The sixth-root and real quadruple constructions need not give identical labelled matrices.

7 The paired-design construction

A different coefficient design gives twelve further new orders. Call a real Hadamard matrix *paired* if its rows and columns can be partitioned into pairs so that every resulting 2×2 block is Hadamard. The row and column partitions may differ, and the blocks may have either determinant sign. Kline's paired-transfer theorem [24, Theorem 1] constructs a Hadamard matrix of order $8m$ from a paired Hadamard matrix of order $2(m-1)$ and a symmetric or skew conference matrix of order $m+1$, for odd $m \geq 3$. The quaternary-input case is Miyamoto's earlier construction; this extension allows both determinant signs.

We use an order-20 coefficient design E_0, E_1, E_2, E_3 whose disjoint signed supports cover all positions and satisfy

$$E_j E_j^{\mathsf{T}} = 5I_{20}, \qquad E_i E_j^{\mathsf{T}} + E_j E_i^{\mathsf{T}} = 0 \quad (i \neq j).$$

It is obtained from the length-five T-rows in Appendix F. The appendix gives row and column pairings with the following property: in every paired coefficient block the product of signs is -1, and, after identifying the first two variables, each variable occurs an even number of times.

Let A_0, A_1, A_2, A_3 be a Williamson-type quadruple of order w, meaning sign matrices satisfying the norm and pairwise relations of Proposition 2. If $A_0 = A_1$, then

$$F = \sum_{j=0}^{3} E_j \otimes A_j, \qquad FF^{\mathsf{T}} = 20wI_{20w}.$$

The Gram proof is the same cancellation as in Proposition 2. Pair rows and columns using the coefficient pairings, with the internal indices fixed. Each resulting sign block has four-entry product -1, because the substituted variables occur to even powers. Its rows are therefore orthogonal, so F is paired.

Turyn's repeated-member inputs have width $w = (p+1)/2$ for prime powers $p \equiv 1 \pmod 4$ [18]. Take $m = 10w + 1$. The fifteen choices in Table 1 have prime m congruent to 3 modulo 4, so Paley supplies a skew conference matrix of order $m + 1$. Since $20w = 2(m-1)$, the transfer theorem gives the listed orders. For example, $p = 653$ gives $w = 327$, $m = 3271$ and order 26168.

p	w	m	$8m$	Status
653	327	3271	26168	New
673	337	3371	26968	New
1069	535	5351	42808	New
1117	559	5591	44728	New
1373	687	6871	54968	Known
1381	691	6911	55288	New
1657	829	8291	66328	New
1877	939	9391	75128	New
2017	1009	10091	80728	New
2053	1027	10271	82168	New
2153	1077	10771	86168	New
2213	1107	11071	88568	Known
2281	1141	11411	91288	New
2293	1147	11471	91768	New
2297	1149	11491	91928	Known

Table 1: The fifteen paired-design constructions.

Appendix F gives the coefficient rows and pairings, all finite-field recipes, and the integer checks. The conference condition is a separate hypothesis: the repeated-member inputs alone do not give an unconditional infinite family of final orders.

8 Completion and comparison with known orders

Proof of Theorem 1. Section 4 gives twenty-five new orders. The cubic family gives one further order, 295308; its preceding member 98436 is already among those twenty-five. The Spence recurrences give eleven more new finite orders. Eight of these orders and their parameters are listed in Appendix G; the other three are 31305172, 47251804 and 68806764 from Section 5. The twelve new paired-design orders in Table 1 complete the list, since $25 + 1 + 11 + 12 = 49$ and these sets of orders are disjoint. The sixteen Spence specializations and the cubic recurrence give all seventeen families. □

The individually checked examples include thirty-seven known orders, bringing the finite total to eighty-six distinct orders. Appendix G lists the earlier construction at each known order and gives its parameters. The known orders include members of the infinite families: for example, the cubic family gives the Paley order 885924, and the $q = 121$ Spence family gives the Paley order 18629644 at its first expansion.

The paired method also constructs order 41368, which Pender had already claimed [26, p. 79; PDF p. 94]. We exclude it from the new-order list. We have not recovered Pender's matrix or its parameters, so equality or Hadamard equivalence with our matrix remains unresolved.

Order existence and matrix equivalence are separate questions. Two Hadamard matrices are equivalent if independent row and column permutations and sign changes transform one into the other. At order 885924 we can prove a distinction for the sixth-root matrix $H^{(3)}$ in (9):

Proposition 5. *The matrix $H^{(3)}$ has rank* 246090 *over $\mathbb{F}_3$. Every skew Hadamard matrix of order* 885924 *has rank* 442962 *over $\mathbb{F}_3$. Thus $H^{(3)}$ is inequivalent to the standard Paley I matrix with prime parameter* 885923*.*

Proof outline. Hadamard equivalence preserves rank over $\mathbb{F}_3$. The scalar action reduces the rank of $H^{(3)}$ to 1262 times the rank of a 702×702 matrix, whose exact rank is 195. For a skew Hadamard matrix of order h divisible by 3, the identities $KK^{\mathsf{T}} = hI_h$ and $K + K^{\mathsf{T}} = 2I_h$ give matching upper and lower rank bounds of $h/2$. Appendix G gives the full proof and the finite rank calculation. □

At the other thirty-six known orders, equivalence with earlier matrices remains unsettled. The three paired-design comparisons in the appendix distinguish the normalized labelled matrices, without proving Hadamard inequivalence.

9 Verification and availability

The public repository [1] contains the finite inputs, reconstruction programs and independent integer checks. The appendices give the finite data, expanded calculations and verification programs. The source identities allow the largest matrices to be verified without storing them in full.

Lean proofs cover the original thirty-four finite existence statements and nine families. The fifteen paired-design orders and the eight added Spence families, including their six individually checked first expansions, have mathematical proofs supported by independent exact computations; they have not been formalized in Lean. The matrix-inequivalence proof is also outside the Lean development. Appendix H records the precise formalization scope, software versions and reproduction instructions.

Computational assistance. The author proposed the scalar-reduction viewpoint and projective-flatness formulation. The search implementation, computations, cross-checks and initial draft were developed with OpenAI Codex and its automated agents.

A Finite T-matrices and coefficient calculations

A.1 Two finite correlation identities

Let e_0, e_1, e_2, e_3 be the standard column vectors of $\mathbb{Z}^4$. Define the permutation matrix Π by

$$\Pi e_0 = e_0, \quad \Pi e_1 = e_2, \quad \Pi e_2 = e_3, \quad \Pi e_3 = e_1, \qquad \Pi = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Thus $\Pi^3 = I_4$ and $\Pi^{\mathsf{T}}\Pi = I_4$. We specify two functions

$$b\colon \mathbb{F}_p \longrightarrow \{e_0, -e_0, e_1, -e_1, e_2, -e_2, e_3, -e_3\}, \qquad p \in \{631, 127\}.$$

Write the four integer-valued coordinate functions of b as b_0, b_1, b_2, b_3, so that $b(x) = \sum_{j=0}^{3} b_j(x) e_j$.

For $p = 631$ put $\mu = 458$ and $m = 21$; for $p = 127$ put $\mu = 22$ and $m = 9$. To verify the order, we compute μ^m and $\mu^{m/\ell}$ for each prime divisor ℓ of m. The powers in the table are reduced modulo p; a dash marks $\ell \nmid m$.

p	m	μ^m	$\mu^{m/3}$	$\mu^{m/7}$
631	21	1	587	269
127	9	1	107	—

Indeed, a proper divisor of 21 divides 7 or 3, and a proper divisor of 9 divides 3. None of the displayed smaller powers is 1. Both 631 and 127 are prime, as trial division by the primes up to their square roots shows. The program below includes these divisions.

For $r \neq 0$, write $\mathcal{O}(r) = \{r, \mu r, \ldots, \mu^{m-1} r\}$. These sets partition $\mathbb{F}_p \setminus \{0\}$. Each has m elements: $\mu^k r = \mu^\ell r$ implies $\mu^{k-\ell} = 1$. The next two tables give one representative r from each orbit and its value $b(r)$; the row $r = 0$ specifies $b(0)$. The remaining values of b are defined by

$$b(\mu^k r) = \Pi^k b(r) \quad (0 \le k < m), \qquad b(0) = e_0. \tag{10}$$

This rule is well defined: the representative sets are disjoint, and $\Pi^m = I_4$ because $3 \mid m$.

$p = 631$

r	$b(r)$	r	$b(r)$	r	$b(r)$	r	$b(r)$
0	e_0	1	e_0	2	$-e_2$	3	e_2
4	e_2	5	e_0	6	$-e_3$	7	e_0
8	$-e_3$	9	e_1	10	$-e_1$	12	e_0
13	$-e_0$	14	e_1	17	e_3	18	$-e_0$
20	e_2	23	e_1	24	e_0	25	$-e_0$
26	$-e_0$	27	e_2	28	$-e_1$	35	e_2
36	$-e_3$	46	$-e_1$	50	$-e_1$	52	$-e_2$
56	e_3	70	e_1	140	$-e_3$		

$p = 127$

r	$b(r)$	r	$b(r)$	r	$b(r)$	r	$b(r)$
0	e_0	1	e_0	2	e_2	3	e_0
4	$-e_0$	5	e_3	8	e_1	10	$-e_1$
11	e_3	13	$-e_0$	16	e_0	20	$-e_1$
23	$-e_2$	33	e_2	39	$-e_1$		

For $s \in \mathbb{F}_p$, define the integer

$$c(s) = \sum_{x \in \mathbb{F}_p} b(x)^{\mathsf{T}} b(x+s) = \sum_{j=0}^{3} \sum_{x \in \mathbb{F}_p} b_j(x) b_j(x+s). \tag{11}$$

Substituting $x = \mu y$ and using (10) gives

$$c(\mu s) = \sum_{y} (\Pi b(y))^{\mathsf{T}} \Pi b(y+s) = c(s).$$

Also $c(-s) = c(s)$, by replacing x with $x + s$ and transposing a scalar. Since m is odd, $-1 \notin \langle \mu \rangle$. The subgroup $\langle \mu, -1 \rangle$ therefore has $2m$ elements, and its multiplication orbits on nonzero shifts have $2m$ elements each. It suffices to calculate $c(s)$ on the 15 or 7 representatives below.

For each such s, let P_s count the residues x for which $b(x) = b(x + s)$, and let N_s count those for which $b(x) = -b(x + s)$. The dot product of two signed standard basis vectors is 1 in the first case, -1 in the second case, and 0 in all other cases. Thus $c(s) = P_s - N_s$. The counts on the shift representatives are:

$p = 631:\ s$	1	2	3	5	6	7	9	13	14	17	18	25	26	27	35
P_s	76	78	87	85	78	73	85	83	86	79	73	88	73	81	69
N_s	76	78	87	85	78	73	85	83	86	79	73	88	73	81	69

$p = 127:\ s$	1	2	3	4	5	8	10
P_s	15	18	20	18	16	12	17
N_s	15	18	20	18	16	12	17

Every summand in $c(0)$ is 1, so $c(0) = p$. This proves

$$c(s) = p\delta_{s,0} \qquad (s \in \mathbb{F}_p). \tag{12}$$

The integer program below reconstructs both functions from the tables and checks every shift. It uses only the printed data, independently of the search that produced them.

A.2 Expanded coefficient calculations

Use the circulants and reversal from Section 2. The six upper off-diagonal blocks of the Goethals–Seidel Gram, in row order, are

$(0,1)$	$(BA - AB)\mathcal{J} + DC - CD$
$(0,2)$	$(CA - AC)\mathcal{J} + BD - DB$
$(0,3)$	$(DA - AD)\mathcal{J} + CB - BC$
$(1,2)$	$(AD^{\mathsf{T}} - D^{\mathsf{T}}A)\mathcal{J} + BC^{\mathsf{T}} - C^{\mathsf{T}}B$
$(1,3)$	$(C^{\mathsf{T}}A - AC^{\mathsf{T}})\mathcal{J} + BD^{\mathsf{T}} - D^{\mathsf{T}}B$
$(2,3)$	$(AB^{\mathsf{T}} - B^{\mathsf{T}}A)\mathcal{J} + CD^{\mathsf{T}} - D^{\mathsf{T}}C$

All six vanish; the lower blocks are their transposes. This proves (4).

For the matrix $M(x)$ in the same section, each column has squared length $\sum_j x_j^2$. The dot products of column 0 with columns $1, 2, 3$ are respectively

$$-x_0x_1 + x_1x_0 - x_2x_3 + x_3x_2, \quad -x_0x_2 + x_1x_3 + x_2x_0 - x_3x_1, \quad -x_0x_3 - x_1x_2 + x_2x_1 + x_3x_0.$$

Those of column pairs $(1,2), (1,3), (2,3)$ are

$$x_1x_2 + x_0x_3 - x_3x_0 - x_2x_1, \quad x_1x_3 - x_0x_2 - x_3x_1 + x_2x_0, \quad x_2x_3 - x_3x_2 + x_0x_1 - x_1x_0.$$

Thus $M(x)^{\mathsf{T}}M(x) = (\sum_j x_j^2)I_4$.

A.3 Integer check for the two finite functions

The following Python program checks (12) using only the standard library and the finite inputs below. In the input pairs (r, t), the nonzero integer t stands for $\mathrm{sign}(t)e_{|t|-1}$ at representative r. This encodes the two tables in Section A.1. In the program, `a` is a coordinate index in $\{0, 1, 2, 3\}$, and `b[u]` is the four-entry tuple representing $b(u)$. The inner loops in the final sum are exactly the two finite sums in (11).

```
T = {
    631: (458, 21, [
        (0, 1), (1, 1), (2, -3), (3, 3), (4, 3), (5, 1),
        (6, -4), (7, 1), (8, -4), (9, 2), (10, -2), (12, 1),
        (13, -1), (14, 2), (17, 4), (18, -1), (20, 3), (23, 2),
        (24, 1), (25, -1), (26, -1), (27, 3), (28, -2), (35, 3),
        (36, -4), (46, -2), (50, -2), (52, -3), (56, 4), (70, 2),
```

```
        (140, -4),
    ]),
    127: (22, 9, [
        (0, 1), (1, 1), (2, 3), (3, 1), (4, -1), (5, 4),
        (8, 2), (10, -2), (11, 4), (13, -1), (16, 1), (20, -2),
        (23, -3), (33, 3), (39, -2),
    ]),
}

for p, (mu, m, data) in T.items():
    assert pow(mu, m, p) == 1
    assert all(pow(mu, k, p) != 1 for k in range(1, m))
    b = [None] * p
    b[0] = (1, 0, 0, 0)
    assert data[0] == (0, 1)
    for r, t in data[1:]:
        assert 0 < r < p and 1 <= abs(t) <= 4
        j, sign = abs(t)-1, (1 if t > 0 else -1)
        for k in range(m):
            u = (r * pow(mu, k, p)) % p
            assert b[u] is None
            a = 0 if j == 0 else 1 + (j-1+k) % 3
            b[u] = tuple(sign if i == a else 0 for i in range(4))
    assert all(v is not None and sum(z*z for z in v) == 1 for v in b)
    for s in range(p):
        c = sum(b[x][j] * b[(x+s) % p][j]
                for x in range(p) for j in range(4))
        assert c == (p if s == 0 else 0)
```

The first assertions check the multiplier orders. In the orbit loop, the check for an unassigned value proves that the listed orbits are disjoint; the following assertion checks that they cover all residues. The tuple formula implements Π^k. The final loop checks the correlation at every shift, including zero, without reducing the shifts to orbits.

The following trial-division function checks the two primes defining the functions, the two primes identifying the known Paley orders in Section G.1, and every prime character parameter used in the recurrence:

```
def prime(n):
    if n < 2:
        return False
    d = 2
    while d*d <= n:
        if n % d == 0:
            return False
        d += 1
    return True
assert all(prime(n) for n in
           (5, 13, 17, 61, 101, 109, 127, 137, 631, 885923, 9314821))
```

If an integer $n \geq 2$ is composite, write $n = ab$ with $1 < a \leq b$; then $a^2 \leq n$. Thus checking all integers $2 \leq d \leq \sqrt{n}$ proves primality, which justifies the function. All operations above are integer additions, products, divisions with remainder, and finite loops. The repository file `scripts/verify_manuscript_data.py` combines these checks with the thirteen cyclic quadruple checks, the twelve additional quadruple checks, the eight strong starter checks and the order-13 pair check. It also checks the paired-design inputs printed in Appendix F.2, and the additional strong starters and six finite Spence sources in Appendix D.2. It reconstructs the three triplings from that pair and performs independent Gaussian elimination over $\mathbb{F}_3$ on (30), obtaining rank 195. This check uses only the Python standard library and the printed finite inputs.

B Trace metrics and the sixth-root action

B.1 Restriction of scalars and the final entry condition

For matrices over an algebra with an involution, write $N^* = \overline{N}^{\mathsf{T}}$, where the involution is denoted by $z \mapsto \bar{z}$. Here an involution is a $\mathbb{Q}$-linear map satisfying $\overline{xy} = \bar{x}\bar{y}$ and $\overline{\bar{x}} = x$. We write J_m for the matrix of order m all of whose entries are 1. The Kronecker product is indexed by pairs:

$$(X \otimes Y)_{(i,a),(j,b)} = X_{ij}Y_{ab}.$$

In particular, $I_n \otimes G$ is the block diagonal matrix with n copies of G.

Lemma 6 (The metric under restriction of scalars)**.** *Let K be a commutative $\mathbb{Q}$-algebra of finite dimension m, with an involution, and let $\tau : K \longrightarrow \mathbb{Q}$ be a $\mathbb{Q}$-linear map satisfying $\tau(\bar{z}) = \tau(z)$. Choose a basis $\beta_0, \ldots, \beta_{m-1}$ of K over $\mathbb{Q}$. Define*

$$G_{ab} = \tau(\overline{\beta_a}\beta_b), \qquad z\beta_b = \sum_{a=0}^{m-1} \rho(z)_{ab}\beta_a.$$

Suppose that G is invertible. Then

$$\rho(z)^{\mathsf{T}}G = G\rho(\bar{z}), \qquad \rho(\bar{z})G^{-1} = G^{-1}\rho(z)^{\mathsf{T}}. \tag{13}$$

If $N \in K^{n\times n}$ satisfies $NN^* = wI_n$ for $w \in \mathbb{Q}$, the rational block matrix $X = (\rho(N_{ij}))_{i,j=0}^{n-1}$, of order mn, satisfies

$$X(I_n \otimes G^{-1})X^{\mathsf{T}} = w(I_n \otimes G^{-1}). \tag{14}$$

Proof. For $u = \sum_a x_a\beta_a$ and $v = \sum_b y_b\beta_b$, with rational coordinate columns x, y, expansion of the two sums gives

$$x^{\mathsf{T}}Gy = \tau(\bar{u}v).$$

The form is symmetric because $\tau(\bar{v}u) = \tau(\overline{\bar{v}u}) = \tau(\bar{u}v)$. Multiplication by z sends x to $\rho(z)x$. Consequently

$$x^{\mathsf{T}}\rho(z)^{\mathsf{T}}Gy = \tau(\overline{z\bar{u}}\, v) = \tau(\bar{u}\bar{z}v) = x^{\mathsf{T}}G\rho(\bar{z})y.$$

Taking x and y to be coordinate basis vectors proves the first identity in (13). Multiplying it on the left and right by G^{-1} gives the second identity. This is why the inverse metric occurs in the row Gram identity (14).

Multiplication in coordinates gives $\rho(ab) = \rho(a)\rho(b)$, $\rho(a+b) = \rho(a) + \rho(b)$ and $\rho(q) = qI_m$ for $q \in \mathbb{Q}$. Indeed, each equality follows by applying both sides to the coordinates of each β_b. Thus the (i,j) block of the left side of (14) is

$$\begin{aligned}\sum_k \rho(N_{ik})G^{-1}\rho(N_{jk})^{\mathsf{T}} &= \sum_k \rho(N_{ik})\rho(\overline{N_{jk}})G^{-1} \\ &= \rho\left(\sum_k N_{ik}\overline{N_{jk}}\right)G^{-1} = w\delta_{ij}G^{-1}.\end{aligned}$$

Here δ_{ij} is 1 when $i = j$ and 0 otherwise. These are exactly the blocks of the right side. □

For a number field $K \subset \mathbb{C}$ stable under complex conjugation, one may take $\tau = \mathrm{Tr}_{K/\mathbb{Q}}$: the trace of the rational linear map $x \mapsto zx$ gives its value at z. The same lemma applies to products of number fields and to other explicitly specified trace normalizations, provided that the displayed G is invertible.

Successive restrictions agree with direct restriction in the product basis. More precisely, let $\mathbb{Q} \subset K \subset L$ be finite field extensions, all stable under complex conjugation, with bases (β_a) of $K/\mathbb{Q}$ and (γ_b) of L/K. Then $(\beta_a\gamma_b)_{b,a}$, ordered first by b and then by a, is a basis of $L/\mathbb{Q}$. If multiplication by $z \in L$ has matrix $(c_{bd}(z))$ in the K-basis (γ_b), its rational matrix in this product basis has (b,d) block $\rho_K(c_{bd}(z))$. This follows by expanding

$$z\beta_a\gamma_d = \sum_b \beta_a c_{bd}(z)\gamma_b$$

once more in the basis (β_a). Taking diagonal entries of the rational block matrix proves

$$\mathrm{Tr}_{L/\mathbb{Q}}(z) = \sum_b \mathrm{Tr}_{K/\mathbb{Q}}(c_{bb}(z)) = \mathrm{Tr}_{K/\mathbb{Q}}\big(\mathrm{Tr}_{L/K}(z)\big)\,.$$

Applying this identity to $\overline{\beta_a\gamma_b}\,\beta_c\gamma_d$ also identifies the trace metrics at the two stages. For a square matrix N with $NN^* = wI$ and $w \neq 0$, the right inverse N^*/w is also its inverse, so $N^*N = wI$. The column form lets us carry a Hermitian form through successive restrictions. If an intermediate form is not the identity, we transfer its full matrix. Given a Hermitian matrix $E = (E_{ij}) \in M_n(L)$, use the L/K basis (γ_b) above to define a matrix over K by

$$\widehat{E}_{(i,b),(j,d)} = \mathrm{Tr}_{L/K}(\bar{\gamma}_b E_{ij}\gamma_d).$$

For vectors $u_i = \sum_b x_{ib}\gamma_b$ and $v_j = \sum_d y_{jd}\gamma_d$, expansion of the sums gives

$$x^*\widehat{E}y = \mathrm{Tr}_{L/K}(u^*Ev).$$

Conjugation commutes with this trace: in the conjugate basis $(\bar{\gamma}_b)$, the multiplication matrix of $\bar{z}$ is the entrywise conjugate of that of z in (γ_b), and the matrix trace is independent of the chosen basis. It follows that $\widehat{E}^* = \widehat{E}$. If $T \in M_n(L)$ obeys $T^*ET = wE$ for $w \in K$, and $\widehat{T}$ is its multiplication matrix on the K-coordinate vectors, the same expansion proves

$$x^*\widehat{T}^*\widehat{E}\widehat{T}y = \mathrm{Tr}_{L/K}((Tu)^*E(Tv)) = w\,\mathrm{Tr}_{L/K}(u^*Ev) = wx^*\widehat{E}y.$$

This proves $\widehat{T}^*\widehat{E}\widehat{T} = w\widehat{E}$ by taking coordinate basis vectors for x, y. Restriction once more from K to $\mathbb{Q}$ gives entries

$$\begin{aligned}&\mathrm{Tr}_{K/\mathbb{Q}}\big(\bar{\beta}_a\beta_c\,\mathrm{Tr}_{L/K}(\bar{\gamma}_b E_{ij}\gamma_d)\big)\\ &\quad= \mathrm{Tr}_{L/\mathbb{Q}}\big(\overline{\beta_a\gamma_b}E_{ij}\beta_c\gamma_d\big)\,,\end{aligned}$$

by the trace transitivity just proved. These are exactly the entries of the form obtained by direct restriction in the product basis. For products of number fields, perform these calculations in each component and sum with the specified trace weights. The formulas are linear in the trace, so the same argument carries the full form through the Butson towers defined in the introduction.

To obtain a sign matrix, we also need an entry condition at the last step. The next lemma allows any rational representation, including a direct sum of copies of the regular representation above.

Lemma 7 (Obtaining a sign matrix)**.** *Let n, d be positive integers, let K be as above, and let $\rho : K \longrightarrow M_d(\mathbb{Q})$ be a unital $\mathbb{Q}$-algebra homomorphism such that $\rho(\bar{z}) = \rho(z)^{\mathsf{T}}$. Suppose that $N \in K^{n\times n}$ satisfies $NN^* = wI_n$ for $w \in \mathbb{Q}$, and that $F \in \mathbb{Q}^{d\times d}$ satisfies $FF^{\mathsf{T}} = cI_d$ for $c \in \mathbb{Q}$. Form the matrix H of order dn with blocks*

$$H_{ij} = \rho(N_{ij})F.$$

Then $HH^{\mathsf{T}} = cwI_{dn}$. If every entry of every block $\rho(N_{ij})F$ is a sign and $cw = dn$, then H is a real Hadamard matrix of order dn.

Proof. For each i, j, the (i, j) block of the row Gram matrix is

$$\begin{aligned}\sum_k H_{ik}H_{jk}^{\mathsf{T}} &= \sum_k \rho(N_{ik})FF^{\mathsf{T}}\rho(N_{jk})^{\mathsf{T}}\\ &= c\sum_k \rho(N_{ik})\rho(\overline{N_{jk}})\\ &= c\rho\left(\sum_k N_{ik}\overline{N_{jk}}\right) = cw\delta_{ij}I_d.\end{aligned}$$

The assumed entry condition gives $H_{ab} \in \{-1, 1\}$ for every position (a, b), and $cw = dn$ gives the required Gram scale. □

For each scalar z occurring in N, the entry condition is the finite system of polynomial equations

$$\big(\rho(z)F\big)_{ab}^2 = 1 \qquad (0 \le a, b < d).$$

Over $\mathbb{Q}$ each of these equations is equivalent to the corresponding entry being 1 or -1, since $t^2-1 = (t-1)(t+1)$.

B.2 The sixth-root action from the length-631 construction

Keep the sign matrices P, Q of order $d = 2524$ obtained above. They satisfy (7). Put

$$\xi = \sqrt{-3} = \mathrm{i}\sqrt{3}, \qquad \zeta = \zeta_6 = \frac{1+\xi}{2}, \qquad K = \mathbb{Q}(\zeta) = \mathbb{Q}(\xi).$$

Thus $\bar{\zeta} = 1 - \zeta$, $\zeta^2 - \zeta + 1 = 0$ and $\zeta^3 = -1$. The polynomial $t^2 - t + 1$ is irreducible over $\mathbb{Q}$: a rational root r would satisfy $(2r-1)^2 = -3$, which is impossible in the ordered field $\mathbb{Q}$. Consequently every element of K has a unique expression $a + b\zeta$ with $a, b \in \mathbb{Q}$.

Define

$$R = \frac{1}{d} Q P^{\mathsf{T}}.$$

Its rational entries are given by

$$R_{ij} = \frac{1}{d} \sum_{k=0}^{d-1} Q_{ik} P_{jk}.$$

This determines the scalar action from the two sign matrices.

Lemma 8. *The formula $\rho(a + b\zeta) = aI_d + bR$ defines an injective unital $\mathbb{Q}$-algebra homomorphism $\rho : K \longrightarrow M_d(\mathbb{Q})$ satisfying*

$$\rho(\bar{z}) = \rho(z)^{\mathsf{T}}, \qquad \rho(\zeta) P = Q.$$

Proof. The identity $PP^{\mathsf{T}} = dI_d$ implies $P^{-1} = P^{\mathsf{T}}/d$, hence also $P^{\mathsf{T}} P = dI_d$. Using all three identities in (7), we obtain

$$\begin{aligned} RR^{\mathsf{T}} &= d^{-2} Q P^{\mathsf{T}} P Q^{\mathsf{T}} = d^{-1} Q Q^{\mathsf{T}} = I_d, \\ R + R^{\mathsf{T}} &= d^{-1}(QP^{\mathsf{T}} + PQ^{\mathsf{T}}) = I_d, \\ RP &= d^{-1} Q P^{\mathsf{T}} P = Q. \end{aligned}$$

Substituting $R^{\mathsf{T}} = I_d - R$ into $RR^{\mathsf{T}} = I_d$ gives $R^2 - R + I_d = 0$.

The relation $\zeta^2 = \zeta - 1$ gives

$$(a + b\zeta)(c + e\zeta) = (ac - be) + (ae + bc + be)\zeta.$$

Expansion using $R^2 = R - I_d$ gives exactly the same coefficients for $(aI_d + bR)(cI_d + eR)$. Thus ρ preserves multiplication; its additivity, rational linearity and value $\rho(1) = I_d$ follow directly from the definition. To check injectivity, suppose $aI_d + bR = 0$. If $b \neq 0$, then $R = -(a/b) I_d$, so $-a/b$ would be a rational root of $t^2 - t + 1$, which was excluded above. Hence $b = 0$, and then $a = 0$. Finally,

$$\rho(\overline{a + b\zeta}) = (a + b) I_d - bR = aI_d + bR^{\mathsf{T}} = \rho(a + b\zeta)^{\mathsf{T}}.$$

□

Although the field extension has degree 2, the representation has rational dimension 2524. It makes $\mathbb{Q}^d$ into a vector space over K by $z \cdot v = \rho(z) v$. The dimension formula $\dim_{\mathbb{Q}} \mathbb{Q}^d = [K : \mathbb{Q}] \dim_K \mathbb{Q}^d$ gives $\dim_K \mathbb{Q}^d = 1262$.

We now compute the trace metric in the 2524 rational coordinates of this representation. Put $S = 2R - I_d$. The identities above give

$$S^{\mathsf{T}} = -S, \qquad S^2 = 4R^2 - 4R + I_d = -3I_d,$$

so multiplication by $\xi = 2\zeta - 1$ is represented by S. For $u, v \in \mathbb{Q}^d$ define

$$h(u, v) = \frac{u^{\mathsf{T}} v}{2} - \frac{u^{\mathsf{T}} S v}{6}\, \xi. \tag{15}$$

This is a Hermitian form over K, conjugate linear in the first argument and linear in the second. Indeed, skew symmetry of S gives $h(v, u) = \overline{h(u, v)}$. If $s = u^{\mathsf{T}} v$ and $t = u^{\mathsf{T}} S v$, then

$$h(u, Sv) = \frac{t}{2} + \frac{s}{2}\xi = \xi \left(\frac{s}{2} - \frac{t}{6}\xi \right) = \xi h(u, v).$$

Together with rational bilinearity and $K = \mathbb{Q} + \mathbb{Q}\xi$, this proves K-linearity in the second argument. Conjugate symmetry then proves conjugate linearity in the first. Since $\mathrm{Tr}_{K/\mathbb{Q}}(a + b\xi) = 2a$ and $u^{\mathsf{T}} S u = 0$, we obtain

$$\mathrm{Tr}_{K/\mathbb{Q}}\, h(u, v) = u^{\mathsf{T}} v, \qquad h(u, u) = \frac{1}{2} u^{\mathsf{T}} u > 0 \quad (u \neq 0).$$

Thus this trace form is exactly the ordinary Euclidean form in the coordinates used to construct P, Q. For comparison, on K itself the basis $(1, \zeta)$ gives

$$G = \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\zeta) \\ \mathrm{Tr}(\bar{\zeta}) & \mathrm{Tr}(\bar{\zeta}\zeta) \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \qquad \rho_{\mathrm{reg}}(\zeta) = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

Here ρ_{reg} is the multiplication matrix in the specified two-element basis, rather than the representation ρ of order 2524.

Now take

$$M = \begin{pmatrix} -1 & \zeta & \zeta \\ \zeta & -1 & \zeta \\ \zeta & \zeta & -1 \end{pmatrix}.$$

Each row has squared norm 3. The Hermitian product of two different rows is $1 - \zeta - \bar{\zeta} = 0$. Hence $MM^* = 3I_3$. The two scalars occurring in it give the sign matrices

$$\rho(-1)P = -P, \qquad \rho(\zeta)P = Q.$$

Lemma 7, with $F = P$ and $c = d$, therefore gives

$$H = \begin{pmatrix} -P & Q & Q \\ Q & -P & Q \\ Q & Q & -P \end{pmatrix}, \qquad HH^{\mathsf{T}} = 3dI_{3d} = 7572 I_{7572}.$$

The Gram identity can also be checked directly: a diagonal block is $PP^{\mathsf{T}} + 2QQ^{\mathsf{T}} = 3dI_d$, and an off-diagonal block is $-PQ^{\mathsf{T}} - QP^{\mathsf{T}} + QQ^{\mathsf{T}} = 0$.

More generally, each of the four scalars

$$1, \quad \zeta, \quad -1, \quad -\zeta \tag{16}$$

has a sign matrix image after multiplication by P, namely $P, Q, -P, -Q$, respectively. Any matrix N of order n with entries in (16) and $NN^* = nI_n$ therefore gives a real Hadamard matrix of order $2524n$ by the block formula $H_{ij} = \rho(N_{ij})P$. The entry condition fails for the sixth root ζ^2, which gives

$$\rho(\zeta^2)P = (R - I_d)P = Q - P = 2V,$$

where $P = U - V$ and $Q = U + V$ as above. The entries of V lie in $\{0, 1, -1\}$, and $VV^{\mathsf{T}} = pI_d$ gives exactly p nonzero entries in each row of length $4p$. Thus $2V$ has both zero entries and entries of absolute value 2.

C Finite commuting inputs and their scalar algebras

C.1 Thirteen finite commuting quadruples

We now take $p = 631$. By a Williamson quadruple of order w we mean four symmetric, pairwise commuting sign matrices A_0, A_1, A_2, A_3 satisfying $\sum_j A_j^2 = 4wI_w$. Symmetry and commutation imply $A_i A_j^{\mathsf{T}} = A_i A_j = A_j A_i = A_j A_i^{\mathsf{T}}$, so Proposition 2 applies. The thirteen quadruples below come from the small-order Sage table [4]. Combining these known sources with the length-631 construction gives the new orders.

For each order w, the table gives the first rows of the four circulants, in the order A_0, A_1, A_2, A_3. Each word is read from left to right at indices $0, \ldots, w - 1$; + means 1 and − means −1.

w	four first rows, in order

3	`+++`
	`+-`
	`+-`
	`+-`

7	`+-++-`
	`+-+-+-`
	`++--+`
	`+---`

9	`+--++--`
	`+-+-+-`
	`+-+--+-`
	`++---+`

13	`++++-+-+-+++`
	`+--+-++-+--`
	`++--+-+--+`
	`++--+-+--+`

17	`+--+++--+++--`
	`++-+--+-+--+-+`
	`+-+-+++++++-+-`
	`+-++-+++-+++-++-`

23	`++--+--+-++-+--+--+`
	`+-++-++-++++++-++-++-`
	`+++--++-+-++-+-++--++`
	`+++-+++-+---+-+++-++`

29	`+++--++-+-+--+-+-++--++`
	`+-+--++-+-++++++-+-++--+-`
	`++++-++-+--++++++--+-++-+++`
	`++-+-+-+++-++++-+++-+-+-+`

31	`++++++-+-+--++++--+-+-+++++`
	`+-++--+-+-++--++-+-+--++-`
	`+-++--+-+-++--++-+-+--++-`
	`+---+-++-+++--+++-++-+---`

37	`+-+-+-+-++--+-++++-+--++-+-+-+-`
	`+--++-++-+-+-++--++-+-+-++-++--`
	`+++++-+---++--++--++---+-++++`
	`+-+++-+---+--++--+---+-+++-`

39	`+++-+-+---+-++--++-+---+-+-++`
	`+++-++-+--+-+--+-+--+-++-++`
	`++++--+-++--+-+-+-+--++-+--+++`
	`+--++-+-+---+++-++-+++---+-+-++--`

43	`++--++++-+-+-++----++-+-+-++++--+`
	`+++-+-++-+-+-++++-+--+-++++-+-+-++-+-++`
	`++-++++++--+-+-++-++-++-+-+--+++++++-+`
	`+--++-++++-+-+++-++-++-+++-+-++++-++--`

51	`+--+++-++-+-+++-+++++-++-+++++-+++-+-++-+++--`
	`--+++-++-+-+++-+++++-++-+++++-+++-+-++-+++--`
	`-+-+--+-+++-+-+++++-+-+-+++++-+-+++-+--+-+`
	`-+-+--+-+++-+-+++++-+-+-+++++-+-+++-+--+-+`

61	`++-+-++-+-+-++++-+---+---+---+-++++-+-+-++-+-+`
	`++-+-++-+-+-++++-+---+---+---+-++++-+-+-++-+-+`
	`+--+-+-++++--++-+-++-+--++++++--+-++-+-++--++++-+-+--`
	`++++-+-+--+++-++-+-+-+++---+++-+-+-++-+++--+-+-+++`

For every word h in the table, $h(-x) = h(x)$, with arguments reduced modulo its order w. Hence its circulant is symmetric. Commutativity was proved in Section 2. If h_0, h_1, h_2, h_3 are the four integer rows, the remaining condition is precisely

$$\sum_{j=0}^{3} \sum_{x=0}^{w-1} h_j(x) h_j(x+s) = \begin{cases} 4w & s = 0, \\ 0 & 1 \le s < w. \end{cases}$$

Indeed these are the entries of the sum of the four row Grams by (2). The zero-shift value follows by counting the $4w$ squared signs. For each of the thirteen orders, all nonzero-shift sums are 0. The following loop checks these sums, with `W[w]` denoting the four printed words of order `w`:

```
for w, words in W.items():
    assert len(words) == 4
    assert all(len(h) == w and set(h) <= {'+', '-'} for h in words)
    rows = [[1 if z == '+' else -1 for z in h] for h in words]
    assert all(h[x] == h[-x % w] for h in rows for x in range(w))
    for s in range(w):
        c = sum(h[x] * h[(x+s) % w] for h in rows for x in range(w))
        assert c == (4*w if s == 0 else 0)
```

The standalone checker in the public repository includes all the table entries. The thirteen quadruples therefore give the following Hadamard orders:

w	$2524w$	w	$2524w$	w	$2524w$
3	7572	7	17668	9	22716
13	32812	17	42908	23	58052
29	73196	31	78244	37	93388
39	98436	43	108532	51	128724
61	153964				

The two constructions of order 7572 prove the same existence statement, although their matrices may be inequivalent.

C.2 Twelve further compatible quadruples

The preceding subsection uses symmetric circulants. The substitution theorem also applies when the first matrix is a symmetric back-circulant. We use published near-Williamson data [5] and a Williamson quadruple of order 69 [6] as twelve further inputs. All twelve quadruples were previously known.

For each row a below, put $C(a)_{i,j} = a(j-i)$, reducing arguments modulo its displayed width w. Let R_w be the reversal matrix, defined by $(R_w)_{i,j} = 1$ when $i + j = w - 1$ and 0 otherwise. Thus $R_w^2 = I_w$. For $w \neq 69$, the four matrices used here are

$$A_0 = C(a_0)R_w, \qquad A_j = C(a_j) \quad (1 \le j \le 3).$$

For $w = 69$ use $A_j = C(a_j)$ for all four indices. Each group of four words in the table is (a_0, a_1, a_2, a_3), in that order; the signs and residue indexing have the same meaning as in the preceding subsection.

w	four rows, in order
47	++-+-+++--+-+-+++-+-+--+-++-++-+-+-++---
	+-+--+++-++++----------++++-+++--+-
	-+++-+--+++-++-+-+-++-+-+-++-+++--+-+++-
	-+++-+-++-++--+-+-++-+-+--++-++-+-+++-
53	++--++-++--+-+-+-+-++++++++-+-+-+-+--++-++--
	+--++-+-+-++-+-++++++-++++-++++++-+-++-+-+-++--
	+-+++++-+--+---++++-++--++-++++---+--+-++++-
	+--+-++--+-++--+--++-++-++--+--++-+--++-+--
59	++--++++--++-+--+-++-+++-+++-++-+--+-++--++++---
	+--++-++++-+-+++-+-++-+++-+-+-+++-++-+-+++-+-++++-++--
	+-+--++++-+-+-+-+-+--++-++--+-+-+-+-+-++++--+-
	+---+--+-+-++++++-+--++++++--+-++++++-+-+--+---
67	+-++-+-++-+--+-+++--+-++-+-++-+-+--+-+-+-+++++-++-+-+--
	+-+-+++-++++++-++---+--+----+--+---++-++++++-+++-+-
	++-++--+-+++--++-+-+-+-+--++--+-+-+-+-++--+++-+--++-+
	+-+-++---+++++--+--+-+-++-++-++-+-+--+++++---++-+-
69	+---+-+-++-++-++++--+-++-+-+-++-+-+-++-+--++++-++-++-+-+---
	++++++-+-++-+-+---+++-++-+-+-+-+-+-+-++-+++--+-+-++-+-+++++
	+++-++---++++-+--++--+--+-+-+-+-+--+--++--+-++++---++-++
	+++-++---++++-+--++--+--+-+-+-+-+--+--++--+-++++---++-++
73	+-+-+++--+--+++++----++--++-+-+-+-++++-++++++-+-+-++-+-+-+-++-
	+---++-+-+++-+-+++++-+--+++-++-++-+++--+-+++++-+-++++-+-++---
	+-+-++----+-+-+++++-+-+-+-++--++-+-+-+-++++-+-+----++-+-
	+--++-+-++-+++-+-+++--+-++++++-++-++++++-+--+++-+-+++-++-+-++--
79	+--+++--+-++---+--+---+-++-+++-----+--+-+-+++++-+--+++++-+++
	+-++-+++-+-+-+---++++++-+-+-+++-++-+++-+-+-++++++---+-+-+-+++-++-
	++--+-++-+++-+++-++-++-+-+-+-++-+-----+-++-+-+-+-++-++-+++-+++-++-+--+
	++-+-+--++-+-+-+-+-++++--++++-+-+-++++--++++-+-+-+-++--++--+-+
93	++-++-+-+-++-++++-+-+++-++-++++-++--+-+-+-+-++--++-+--++++++-+--+--++-++-+-++-+-
	++---++++-+-++++-+-++-+-+----++-+-+---+-+---+-+-++----+-+-++-+-++++-+-++++---+
	+--+--++-+-+--+++-++-+++-+-++---+--++++++--+----++-+-+++-++-+++--+-+-++--+--
	++-+-+-++++-++----++-+-++--+--+++-+-+-+-+-+++--+--++-+-++----++-++++-+-+-+
97	+++-+---+--+----++-++-++--++++++-++++-+-+-++--++-+-+-++--+-++-+-++-+-++--++-+-+-+
	+-++-+-++-+++-++-++++-----++-+-+-+--++--++--+-+-+-++-----++++-++-+++-++-+-++-
	++----+--+--++++--+-++++-+--+--+-++++-++++-+--+--+-++++-+--++++-++---+--+---+
	+--++++--+-+--++-++-+-++-+-+-+-++-+-+--++--+-+-++-+-+-+-++-+-++-++---+--+--++++--
103	-+-+-+-++-++++++-++-+-+++-++-+++-+--++-+-++-++-+++-++-+++---+-++++++-+++-++++--+-++-++++-+
	+-+-++++++-+-+--++-+-++++-++++-++-+--++-+----++---+-++--+-++-++++-++++-+-++--+-+-++++++-+-
	+-++-++-+-+-++-+-++-+-++++-+-++++-+-+++----++++----+++-+-++++-+-++++-+-++-+-++-+-+-++-++-
	--++++++-+-++--+++-+++-++++--++-+--+--++-+-++++-+-++--+--+-++--++++-+++-+++---++-+-++++++--
109	-+-+-+-+-+-++++-++++--++++---+--+-+++-+-+--++++-++-+-++-+-++-+-+++-++-+-++++-+--+++-++--+++-++-
	+-+++-+-++-+-+-+-+-+-++++++++-++-++-+--++-+++--++--++++-++--+-++-++-++++++++-+-+-+-+-+-++-+-+++-
	-+-+-+-+++-++++-++++-++-++-+-+++-++--+--++++--++++++--+--++-+++-+-++-++-++++-++++-+++-+-+-+-
	-+-++++++++++-+-++-+-+-+-+-++-++-+++-+++---+++--+++---+++-+++-++-++-+-+-+-+-++-+-++++++++-+-
127	+-+---++++++++-++-+--+++-+-+-+-+++-++-++-+++-++-+--++++++--++++++++--++-+-+-+-+-++-+-+-++-+++-++-++-+++-+++++-+
	+-+-+---+--+++++-+++---+-+-+-++++++++-++++++++--++-++-+--+-++-++--+++++++-++++++++-+-+-+---+++-++++--+---+-+-
	+-+++-++-+-++++-+-+-+-+-++++--+-+++-++-++--++++-+-+-+-+-+-+-+-+-++--++-+++-++-+--++++-+-+-+-+-++++-+-++-+++-
	++-+++-+++--++-++++-+-+-+--+++---+--+-+++-++-++-++-++-++-++-++-++-++-+++-+--+---+++--+-+-+-++++-++--+++-+++-+

To apply the substitution theorem, first observe that for $j = 1, 2, 3$ each printed row satisfies $a_j(-x) = a_j(x)$, so $C(a_j)$ is symmetric. At $w = 69$ this holds for a_0 as well. In every other case,

$$(C(a_0)R_w)_{i,j} = a_0(w - 1 - i - j),$$

which is symmetric in i, j without any assumption on a_0. A direct entry calculation gives $R_w C(a_j) = C(a_j) R_w$ for each symmetric circulant $C(a_j)$: both entries at (i, j) are $a_j(w - 1 - i - j)$. All circulants commute, as already proved. Hence $C(a_0)R_w$ commutes with the other three matrices. Finally

$$(C(a_0)R_w)(C(a_0)R_w)^{\mathsf{T}} = C(a_0)C(a_0)^{\mathsf{T}}.$$

It remains to sum the four periodic autocorrelations. The following loop checks every shift, with `NW[w]` denoting the four words printed at width `w`:

```
for w, words in NW.items():
    assert len(words) == 4
    assert all(len(h) == w and set(h) <= {'+', '-'} for h in words)
    a = [[1 if c == '+' else -1 for c in h] for h in words]
    symmetric = range(4) if w == 69 else range(1, 4)
    assert all(a[j][x] == a[j][-x % w]
               for j in symmetric for x in range(w))
    for t in range(w):
        c = sum(h[x]*h[(x+t) % w] for h in a for x in range(w))
        assert c == (4*w if t == 0 else 0)
```

The repository checker includes all four words at each width. These sums prove $\sum_j A_j A_j^{\mathsf{T}} = 4wI_w$. Symmetry and commutation were proved above, so Proposition 2 gives the twelve additional Hadamard orders

w	$2524w$	w	$2524w$	w	$2524w$
47	118628	53	133772	59	148916
67	169108	69	174156	73	184252
79	199396	93	234732	97	244828
103	259972	109	275116	127	320548

We can also describe these sources by restriction of scalars. Let $\mathcal{A} = \mathbb{Q}[A_0, A_1, A_2, A_3] \subseteq M_w(\mathbb{Q})$ and let $V = \mathbb{Q}^w$ with its standard inner product. The scalar action is the given inclusion on V. The algebra is commutative, and its involution is the identity, because its generators commute and are symmetric. Commuting real symmetric matrices are simultaneously diagonalizable, so $\mathcal{A}$ has no nonzero nilpotent elements. The structure theorem for finite-dimensional commutative reduced rational algebras gives

$$\mathcal{A} \cong \prod_\nu K_\nu, \qquad V \cong \bigoplus_\nu K_\nu^{m_\nu}, \qquad \sum_\nu m_\nu [K_\nu : \mathbb{Q}] = w.$$

Here K_ν are totally real number fields, and the positive integers m_ν record their module multiplicities, which may exceed one. The normalized trace of the actual representation is

$$\tau(a) = \frac{1}{w} \operatorname{tr}_V(a) = \frac{1}{w} \sum_\nu m_\nu \operatorname{Tr}_{K_\nu/\mathbb{Q}}(a_\nu).$$

Put $T = A_0 + 3A_1 + 5A_2 + 7A_3$. Exact matrix calculations give $A_j = p_j(T)$ for four rational polynomials. Since $T \in \mathcal{A}$, this proves $\mathcal{A} = \mathbb{Q}[T]$. The fields K_ν are therefore $\mathbb{Q}[t]/(f_\nu)$ for the distinct monic irreducible factors f_ν of $\det(tI_w - T)$. The table gives their degrees and module multiplicities. Each pair is $([K_\nu : \mathbb{Q}], m_\nu)$; a repeated pair denotes a separate factor, not a further power of one factor.

w	$\dim_{\mathbb{Q}} \mathcal{A}$	$([K_\nu : \mathbb{Q}], m_\nu)$
47	47	$(1,1)$, $(46,1)$
53	53	$(1,1)$, $(52,1)$
59	59	$(1,1)$, $(58,1)$
67	67	$(1,1)$, $(66,1)$
69	35	$(1,2)$, $(1,1)$, $(11,2)$, $(22,2)$
73	25	$(1,1)$, $(24,3)$
79	79	$(1,1)$, $(78,1)$
93	93	$(1,1)$, $(1,1)$, $(1,1)$, $(30,1)$, $(60,1)$
97	97	$(1,1)$, $(96,1)$
103	35	$(1,1)$, $(34,3)$
109	37	$(1,1)$, $(36,3)$
127	43	$(1,1)$, $(42,3)$

The matrix T is symmetric, hence diagonalizable over $\mathbb{R}$. Its minimal polynomial is therefore $M = \prod_\nu f_\nu$, with each factor occurring once, and $M(T) = 0$. Put $g_\nu = M/f_\nu$. The projector onto the νth field component is $e_\nu(T)$, where

$$e_\nu(t) = g_\nu(t)\big(g_\nu(t)^{-1} \bmod f_\nu(t)\big) \bmod M(t).$$

The inverse exists because the factors are distinct. Modulo f_μ, e_ν is 1 if $\mu = \nu$ and 0 otherwise. Thus the sum minus 1 and every product with distinct indices vanish modulo M; evaluating at T proves that the projectors sum to the identity and their pairwise products vanish. Applying them to standard basis columns of V, and retaining linearly independent strings $v, Tv, \dots, T^{\deg f_\nu - 1}v$, supplies every copy of K_ν. The accompanying program carries out this rational reconstruction. In the resulting basis B of V, the transported metric is $B^{\mathsf{T}}B$, and the scalar action is $B^{-1}A_jB$. The program checks both the intertwining and metric identities over the rationals. In the original standard basis the metric is I_w and the scalar images are the sign matrices specified above. Applying this action to the weighted source $\sum_j X_jA_j$ gives $\sum_j X_j \otimes A_j$, of order and Gram scale $2524w$. The individual field components may therefore be nonflat before rational reconstruction. The construction does not require these noncyclic inputs to belong to $\mathbb{Q}[C_w]$.

D Spence starters, character fields and finite checks

This appendix gives the starter rows, their finite checks and the field models for the explicit matrices. The uniform proof in Section 5 may start from Turyn's classical source; the rows below specify particular representatives. For $q = p^e$ and $w_0 = (q+1)/2$, the full scalar algebra at stage r is $\mathbb{Q}[C_{w_0} \times (C_p)^{er}]$. Since p is coprime to w_0, it decomposes as

$$\prod_{d \mid w_0} \mathbb{Q}(\zeta_d) \;\times\; \prod_{d \mid w_0} \mathbb{Q}(\zeta_{dp})^{(q^r-1)/(p-1)}.$$

Factors of multiplicity zero are omitted. All factors enter the normalized trace, which is the identity coefficient and gives the identity metric in the inverse-group basis of Section 2.4.

D.1 Sixteen infinite families from Spence's recurrence

Spence's classical recurrence [7, Theorem 4], applied to the eight initial quadruples below and combined with the length-631 construction, gives eight of our families. We verify its hypotheses here. Section D.1.5 gives a uniform prime-power theorem and eight further specializations.

A *sign matrix* is a real matrix whose entries belong to $\{1, -1\}$. A matrix A is symmetric if $A^{\mathsf{T}} = A$, and two square matrices commute if $AB = BA$. Fix

$$q \in \{5, 13, 17, 61, 101, 109, 121, 137\}, \qquad w_0 = (q+1)/2.$$

We need four symmetric, pairwise commuting sign matrices D_0, E_0, F_0, G_0 of order w_0 satisfying

$$(D_0 - E_0)^2 + (F_0 - G_0)^2 = 4I_{w_0}, \qquad (D_0 + E_0)^2 + (F_0 + G_0)^2 = 4qI_{w_0}. \tag{17}$$

The induction uses both identities; the weaker condition that the sum of the four squares is $4w_0I_{w_0}$ does not suffice.

D.1.1 The initial matrices

For a row $h\colon \mathbb{Z}/w\mathbb{Z} \to \mathbb{Z}$, define its circulant matrix by

$$\mathrm{Circ}(h)_{i,j} = h(j-i) \qquad (i, j \in \mathbb{Z}/w\mathbb{Z}).$$

In the table below, row arguments are reduced modulo w. The table gives the first rows d, e, f, g of D_0, E_0, F_0, G_0. A + means 1, a − means −1, and each word lists the entries at $0, 1, \dots, w_0 - 1$, in that order.

q	row	entries
5	d	+++
5	e	-++
5	f	+-
5	g	+-
13	d	+-++++-
13	e	+-++++-
13	f	+-++-
13	g	--++-
17	d	+-++++-
17	e	+-++++-
17	f	+-+--+-
17	g	-+--+-
61	d	++++++-+-+--++++--+-+-+++++
61	e	-+++++-+-+--++++--+-+-+++++
61	f	+-++--+-+-++--++-+-+--++-
61	g	+-++--+-+-++--++-+-+--++-
101	d	+--+++-++-+-+++-+++++-++-+++++-+++-+-++-+++--
101	e	--+++-++-+-+++-+++++-++-+++++-+++-+-++-+++--
101	f	-+-+--+-+++-+-+++++-+-+-+++++-+-+++-+--+-+
101	g	-+-+--+-+++-+-+++++-+-+-+++++-+-+++-+--+-+
109	d	+-+-+-+-++-+-+++++-+++-++++-+++-+++++-+-++-+-+-+-
109	e	-+-+-+-++-+-+++++-+++-++++-+++-+++++-+-++-+-+-+-
109	f	+++--++-++-++--+-+-+++++++++-+-+--++-++-++--++
109	g	+++--++-++-++--+-+-+++++++++-+-+--++-++-++--++
121	d	++-+-++-+-+-++++-+---+---+---+-++++-+-+-++-+-+
121	e	++-+-++-+-+-++++-+---+---+---+-++++-+-+-++-+-+
121	f	+--+-+-++++--++-+-++-+--++++++--+-++-+-++--++++-+-+--
121	g	--+-+-++++--++-+-++-+--++++++--+-++-+-++--++++-+-+--
137	d	+---+-+-++-++-++++--+-++-+-+-++-+-+-++-+--++++-++-++-+-+---
137	e	---+-+-++-++-++++--+-++-+-+-++-+-+-++-+--++++-++-++-+-+---
137	f	+++-++---++++-+--++--+--+-+-+-+--+--++--+-++++---++-++
137	g	+++-++---++++-+--++--+--+-+-+-+--+--++--+-++++---++-++

Each row consists of signs and satisfies $h(-x) = h(x)$, so every initial matrix is symmetric. For arbitrary rows h, k, multiplication gives

$$\big(\mathrm{Circ}(h)\,\mathrm{Circ}(k)\big)_{i,j} = \sum_{t \in \mathbb{Z}/w\mathbb{Z}} h(t)k(j-i-t).$$

Replacing t by $j-i-t$ interchanges h and k. Thus any two circulants of the same order commute.

In each of the eight cases, one of $d-e, f-g$ is zero and the other is $2\delta_0$, where $\delta_0(0) = 1$ and $\delta_0(x) = 0$ for $x \neq 0$. Since $\mathrm{Circ}(\delta_0) = I$, this proves the first identity in (17). For the second, put

$$u = (d+e)/2, \qquad v = (f+g)/2, \qquad c(s) = \sum_{x=0}^{w_0-1} \big(u(x)u(x+s) + v(x)v(x+s)\big).$$

The displayed rows give the following sums:

q	w_0	$c(0)$	$(c(1), \ldots, c(w_0-1))$
5	3	5	$(0, \ldots, 0)$
13	7	13	$(0, \ldots, 0)$
17	9	17	$(0, \ldots, 0)$
61	31	61	$(0, \ldots, 0)$
101	51	101	$(0, \ldots, 0)$
109	55	109	$(0, \ldots, 0)$
121	61	121	$(0, \ldots, 0)$
137	69	137	$(0, \ldots, 0)$

The rightmost vector has $w_0 - 1$ entries. The following integer calculation checks these equalities, together with the signs, symmetry and difference rows. The eight quadruples are included in the code, so the check requires no external data file.

```
starters = {
    13: (
        '+-++++-',
        '+-++++-',
        '+--++--',
```

```
        '---++--',
    ),
    17: (
        '+--++++--',
        '+--++++--',
        '+-+----+-',
        '--+----+-',
    ),
    61: (
        '++++++-+--+---++++---+--+-+++++',
        '-+++++-+--+---++++---+--+-+++++',
        '+--++---+-+-++----++-+-+---++--',
        '+--++---+-+-++----++-+-+---++--',
    ),
    101: (
        '+---+++-++-+-+++--++++--++--++++--+++-+-++-+++---',
        '----+++-++-+-+++--++++--++--++++--+++-+-++-+++---',
        '-+--+----+-+++-+-++++--+--+--++++-+-+++-+----+--+',
        '-+--+----+-+++-+-++++--+--+--++++-+-+++-+----+--+',
    ),
    121: (
        '++--+--++--+-+-++++--+-----+-----+-----+--++++-+-+--++--+--+',
        '++--+--++--+-+-++++--+-----+-----+-----+--++++-+-+--++--+--+',
        '+---+-+++++---++--+-++-+---++++++---+-++-+--++---++++-+-+---',
        '----+-+++++---++--+-++-+---++++++---+-++-+--++---++++-+-+---',
    ),
    5: (
        '+++',
        '-++',
        '+--',
        '+--',
    ),
    109: (
        '+-+--+-+-++--+-+++++-+++--++++--+++-+++++-+--++-+-+--+-',
        '--+--+-+-++--+-+++++-+++--++++--+++-+++++-+--++-+-+--+-',
        '+++----++-++--++----+-+-++++++++-+-+----++--++-++----++',
        '+++----++-++--++----+-+-++++++++-+-+----++--++-++----++',
    ),
    137: (
        '+-----+-+--++-++-++++---+--++-+-+-++-+-+-++--+---++++-++-++--+-+-----',
        '------+-+--++-++-++++---+--++-+-+-++-+-+-++--+---++++-++-++--+-+-----',
        '+++--++-----++++-+----++---+---+-+--+-+---+---++----+-++++-----++--++',
        '+++--++-----++++-+----++---+---+-+--+-+---+---++----+-++++-----++--++',
    ),

}
for q, words in starters.items():
    w = (q + 1) // 2
    assert len(words) == 4
    assert all(len(h) == w and set(h) <= {'+', '-'} for h in words)
    a = [[1 if z == '+' else -1 for z in h] for h in words]
    assert all(h[x] == h[-x % w] for h in a for x in range(w))
    minus = [[a[0][x] - a[1][x] for x in range(w)],
             [a[2][x] - a[3][x] for x in range(w)]]
    plus = [[a[0][x] + a[1][x] for x in range(w)],
```

```
        [a[2][x] + a[3][x] for x in range(w)]]
for s in range(w):
    def corr(rows):
        return sum(h[x] * h[(x+s) % w]
                   for h in rows for x in range(w))
    assert corr(minus) == (4 if s == 0 else 0)
    assert corr(plus) == (4*q if s == 0 else 0)
```

All sums are computed with integers. For any row h,

$$\big(\mathrm{Circ}(h)\,\mathrm{Circ}(h)^{\mathsf{T}}\big)_{i,j} = \sum_{x=0}^{w-1} h(x)h(x+j-i).$$

The rows $d \pm e$ and $f \pm g$ are symmetric, so their circulants equal their transposes. The two correlation vectors therefore prove (17) entry by entry. The Lean kernel independently checks the same rows and integer equalities in `Data/StrongStarters.lean` and `Data/AdditionalSpence/`.

D.1.2 The character matrices used in the recurrence

For each of the eight values of q, define the field $\mathbb{F}_q$ and its character matrix K_q as follows.

For $q = 5, 13, 17, 61, 101, 109, 137$, take $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$. For $q = 121$, take

$$\mathbb{F}_{121} = \mathbb{F}_{11}[u]/(u^2 - 2).$$

The nonzero squares modulo 11 are $1, 3, 4, 5, 9$. Thus 2 is not a square modulo 11, $u^2 - 2$ is irreducible, and this quotient is a field. Its elements are uniquely $a + bu$ with $0 \le a, b < 11$, and its arithmetic is

$$(a + bu)(c + du) = (ac + 2bd) + (ad + bc)u,$$

with coefficients reduced modulo 11. For numerical indexing, label $a+bu$ by the integer $a+11b$. Field subtraction acts componentwise modulo 11; subtraction modulo 121 would give a different operation.

For any of these fields, define its quadratic character $\chi_q \colon \mathbb{F}_q \to \{0, 1, -1\}$ by $\chi_q(0) = 0$, with $\chi_q(z) = 1$ if z is a nonzero square, and $\chi_q(z) = -1$ otherwise. Set

$$(K_q)_{x,y} = \chi_q(y - x) \qquad (x, y \in \mathbb{F}_q), \qquad (J_q)_{x,y} = 1.$$

The following are the first rows of K_q in the residue order $0, 1, \ldots, q-1$ for the seven prime values. The meaning of the signs is as above, and 0 denotes the zero entry.

q	$(\chi_q(0), \ldots, \chi_q(q-1))$
13	0+-++--++-+
17	0++-+--++--+-++
61	0+-+++--+-+++++-++-+-+-+---+-+-+-++-+++++-+--+++-+
101	0+-+++-+--++-++-++++++++--++-+-++---+-+-+-+-+-+-+-+---++-+-++--++++++-++-++--+-+++-+
5	0+-+
109	0+-+++-+-+-+-++--+++-+++++-+-+++-+--+-++-++-----++-++-+--+-+++-+-+++++-+++--++-+-+-+-+++-+
137	0++-+-+++-+-++++++-+-+-+-+-+-+++++--+--++---+-+++-+++-++-+++-+++-+---++--+--+++++-+-+-+-+-+-++++++-+-+++-+-++

For $q = 121$, the next table gives the eleven consecutive blocks in the first row; each block lists $\chi_{121}(a + bu)$ as a runs from 0 to 10.

b	values	b	values
0	0++++++++++	6	+-++--++-
1	+--++++--	7	+-+-++-+-
2	++-+--+-+	8	++-+-+-+
3	++-+-+-+	9	++-+--+-+
4	+-+-++-+-	10	+--++++--
5	+-++--++-		

These blocks can also be obtained directly from the formula

$$\chi_{121}(a + bu) = \chi_{11}(a^2 - 2b^2), \tag{18}$$

where χ_{11} is given by the square list $1, 3, 4, 5, 9$. The binomial theorem in characteristic 11 gives $(a + bu)^{11} = a - bu$, because $u^{11} = 2^5 u = -u$. Hence

$$(a + bu)^{12} = a^2 - 2b^2.$$

For a nonzero element z of $\mathbb{F}_{121}$, the square subgroup has 60 elements: the map $t \mapsto t^2$ has precisely the two preimages $t, -t$ at each nonzero square. All these squares satisfy $z^{60} = 1$ by Lagrange's theorem. Since a nonzero polynomial of degree 60 over a field has at most 60 roots, these are exactly the roots of $z^{60} = 1$. Also $z^{120} = 1$, so z^{60} is 1 or -1. It follows that $\chi_{121}(z) = z^{60}$, interpreting these two field elements as the integer signs. The identical argument in $\mathbb{F}_{11}$ gives $\chi_{11}(t) = t^5$ for $t \neq 0$. The displayed twelfth-power identity now proves (18); both sides also vanish at zero.

The recurrence uses the identities

$$K_q^{\mathsf{T}} = K_q, \qquad K_q^2 = qI_q - J_q, \qquad K_q J_q = J_q K_q = 0, \qquad J_q^2 = qJ_q. \tag{19}$$

The diagonal entries of K_q are zero, and all its off-diagonal entries are signs by the definition of χ_q.

First, the nonzero squares form a subgroup of index two in $\mathbb{F}_q^\times$, because the squaring map has two preimages at each nonzero square. Its two cosets show that $\chi_q(xy) = \chi_q(x)\chi_q(y)$, including the case in which one factor is zero. There are equally many nonzero squares and nonsquares, whence

$$\sum_{x \in \mathbb{F}_q} \chi_q(x) = 0.$$

Also -1 is a square in each field. Explicit square roots are $2, 5, 4, 11, 10, 33, 37$ for $q = 5, 13, 17, 61, 101, 109, 137$, respectively, and $4u$ for $q = 121$. Thus $\chi_q(-x) = \chi_q(x)$, proving the symmetry of K_q. The character sum proves that all row and column sums of K_q vanish, which gives $K_q J_q = J_q K_q = 0$. Multiplication of the all-one matrix gives $J_q^2 = qJ_q$.

For the remaining square identity, define

$$T(a) = \sum_{t \in \mathbb{F}_q} \chi_q(t)\chi_q(t + a).$$

If $a = 0$, all $q - 1$ nonzero terms are 1, so $T(0) = q - 1$. If $a \neq 0$, substituting $t = av$ and using multiplicativity gives

$$T(a) = \sum_{v \in \mathbb{F}_q} \chi_q(v(v + 1)).$$

For a fixed v, the number of $z \in \mathbb{F}_q$ satisfying $z^2 = v(v + 1)$ is $1 + \chi_q(v(v + 1))$. Therefore the total number of such pairs (v, z) is $q + T(a)$. The invertible change of variables

$$x = 2v + 1, \qquad y = 2z$$

changes the equation into $(x - y)(x + y) = 1$. Choosing any $c \in \mathbb{F}_q^\times$ gives exactly one solution by setting $x - y = c$, $x + y = c^{-1}$; division by 2 is possible because the field has odd characteristic. There are $q - 1$ choices, so $q + T(a) = q - 1$ and $T(a) = -1$. Finally,

$$(K_q K_q^{\mathsf{T}})_{x,y} = T(y - x) = \begin{cases} q - 1 & x = y, \\ -1 & x \neq y. \end{cases}$$

This is $qI_q - J_q$. Symmetry of K_q completes the proof of (19).

D.1.3 The recursion and its proof

Keep q fixed. Starting from the four initial matrices, construct D_r, E_r, F_r, G_r recursively. Given a pair (U, V) of matrices of order w_r, define two matrices of order $w_r q$ by

$$\begin{aligned} U' &= \tfrac{1}{2}(U - V) \otimes J_q + \tfrac{1}{2}(U + V) \otimes (K_q + I_q), \\ V' &= \tfrac{1}{2}(U - V) \otimes J_q + \tfrac{1}{2}(U + V) \otimes (K_q - I_q). \end{aligned} \tag{20}$$

Here $\otimes$ denotes the Kronecker product: the entry of $A \otimes B$ at row (i,x) and column (j,y) is $A_{i,j}B_{x,y}$. Apply (20) to (D_r, E_r) to obtain (D_{r+1}, E_{r+1}), and to (F_r, G_r) to obtain (F_{r+1}, G_{r+1}). The index sets are

$$\Omega_0 = \mathbb{Z}/w_0\mathbb{Z}, \qquad \Omega_{r+1} = \Omega_r \times \mathbb{F}_q, \qquad w_r = |\Omega_r| = w_0 q^r.$$

The cardinality formula follows by induction: $|\Omega_0| = w_0$, and each step multiplies the cardinality by q.

We prove by induction that the four matrices remain symmetric, pairwise commuting sign matrices and that

$$\begin{aligned} M_r &:= (D_r - E_r)^2 + (F_r - G_r)^2 = 4q^r I_{w_r}, \\ N_r &:= (D_r + E_r)^2 + (F_r + G_r)^2 = 4q^{r+1} I_{w_r}. \end{aligned} \tag{21}$$

The initial case was proved above. For the induction step, consider first the entries.

Let $u, v \in \{1, -1\}$ be corresponding entries of U, V. If $u = -v$, then $(u+v)/2 = 0$ and $(u-v)/2 = u$, so both new entries are u because every entry of J_q is 1. If $u = v$, then $(u-v)/2 = 0$ and $(u+v)/2 = u$. Each entry of $K_q + I_q$ and of $K_q - I_q$ is a sign: off the diagonal it is the corresponding nonzero entry of K_q, and on the diagonal it is 1 or -1, respectively. Thus both new entries are signs in either case, and all four new matrices are sign matrices.

The transpose of a Kronecker product is the Kronecker product of the transposes of its factors. All factors in (20) are symmetric, so the new matrices are symmetric. For commutativity, use

$$(A \otimes B)(C \otimes D) = AC \otimes BD.$$

The first factors are linear combinations of the old four matrices and commute by the induction hypothesis. The second factors are linear combinations of I_q, J_q, K_q, which commute by (19). Hence all Kronecker summands commute, and so do the four new matrices.

For the norms, adding and subtracting the two equations in (20) gives

$$U' - V' = (U+V) \otimes I_q, \qquad U' + V' = (U-V) \otimes J_q + (U+V) \otimes K_q.$$

In the square of the last expression, both mixed terms vanish because $J_q K_q = K_q J_q = 0$. Thus, using (19),

$$\begin{aligned} (U'+V')^2 &= (U-V)^2 \otimes qJ_q + (U+V)^2 \otimes (qI_q - J_q) \\ &= q(U+V)^2 \otimes I_q + \big(q(U-V)^2 - (U+V)^2\big) \otimes J_q. \end{aligned}$$

Applying these formulas to both pairs gives

$$M_{r+1} = N_r \otimes I_q, \qquad N_{r+1} = qN_r \otimes I_q + (qM_r - N_r) \otimes J_q.$$

By the induction hypothesis $qM_r - N_r = 0$. Therefore

$$M_{r+1} = 4q^{r+1} I_{w_{r+1}}, \qquad N_{r+1} = 4q^{r+2} I_{w_{r+1}},$$

which proves (21) and completes the induction.

Expanding the two squares for each pair gives $(U-V)^2 + (U+V)^2 = 2U^2 + 2V^2$. Consequently

$$\begin{aligned} D_r D_r^{\mathsf{T}} + E_r E_r^{\mathsf{T}} + F_r F_r^{\mathsf{T}} + G_r G_r^{\mathsf{T}} &= \tfrac{1}{2}(M_r + N_r) \\ &= 2(q+1)q^r I_{w_r} = 4w_r I_{w_r}. \end{aligned} \tag{22}$$

Moreover, any two of these matrices, say A, B, satisfy $AB^{\mathsf{T}} = AB = BA = BA^{\mathsf{T}}$, by symmetry and commutativity. Thus the four matrices satisfy the norm and pairwise relations in the substitution theorem.

The index set is the finite abelian group

$$\Omega_r = \mathbb{Z}/w_0\mathbb{Z} \times (\mathbb{F}_q, +)^r.$$

All four matrices have the form $A_{x,y} = a(y-x)$ on this group. Indeed this is true for the initial circulants, and I_q, J_q, K_q also have entries depending only on $y - x$; the Kronecker products and sums in the recursion preserve this property. In the case $q = 121$, the additive factor is $(\mathbb{Z}/11\mathbb{Z})^2$ at each step.

D.1.4 The resulting real Hadamard orders

Let X_0, X_1, X_2, X_3 be the four matrices of order $4p = 2524$ from the length-$p = 631$ construction. They satisfy

$$X_i X_i^{\mathsf{T}} = pI_{4p}, \qquad X_i X_j^{\mathsf{T}} + X_j X_i^{\mathsf{T}} = 0 \quad (i \neq j),$$

and at each matrix position exactly one X_i is nonzero, with value 1 or -1.

Put $(A_0, A_1, A_2, A_3) = (D_r, E_r, F_r, G_r)$ and define

$$H_{q,r} = \sum_{i=0}^{3} X_i \otimes A_i.$$

At a given position there is precisely one nonzero summand, equal to a product of two signs. Thus every entry of $H_{q,r}$ is a sign. For each pair $i \neq j$, symmetry and commutativity give $A_i A_j^{\mathsf{T}} = A_j A_i^{\mathsf{T}}$, so the two corresponding terms in the Gram product cancel. The remaining terms, by (22), are

$$\begin{aligned} H_{q,r} H_{q,r}^{\mathsf{T}} &= pI_{4p} \otimes \sum_{i=0}^{3} A_i A_i^{\mathsf{T}} \\ &= 4pw_r I_{4pw_r}. \end{aligned}$$

This is the defining identity for a real Hadamard matrix of order $4pw_r = 1262(q+1)q^r$. In particular the eight formulas are

q	w_0	$4pw_r$
5	3	$7572 \cdot 5^r$
13	7	$17668 \cdot 13^r$
17	9	$22716 \cdot 17^r$
61	31	$78244 \cdot 61^r$
101	51	$128724 \cdot 101^r$
109	55	$138820 \cdot 109^r$
121	61	$153964 \cdot 121^r$
137	69	$174156 \cdot 137^r$

$(r \geq 0)$.

Each matrix is nonsingular because its Gram matrix is a positive multiple of the identity, so its rank equals the displayed order. The induction proves the result for every nonnegative integer r, without constructing the full matrices.

For $q = 109$ the order at $r = 0$ is known. We start the family in Theorem 1 at $r = 1$, replacing its parameter by $r + 1$: $138820 \cdot 109^{r+1} = 15131380 \cdot 109^r$.

D.1.5 A uniform prime-power source and eight further families

Turyn's construction supplies a strong starter for every prime power in the required congruence class. Combining it with Spence's recurrence and the T-matrices of order 631 gives the following theorem.

Theorem 9. *For every prime power $q \equiv 1 \pmod 4$ and every integer $r \geq 0$, there is a real Hadamard matrix of order*

$$1262(q+1)q^r.$$

Proof. Turyn's construction [18] supplies symmetric commuting circulants $R + I, R - I, S, S$ of order $w_0 = (q+1)/2$, with sign entries and $R^2 + S^2 = qI$; see [8, Theorem 2 and Lemma 1, p. 352]. Order the four initial matrices as

$$D_0 = E_0 = S, \qquad F_0 = R + I, \qquad G_0 = R - I.$$

Their difference norm is $4I$ and their sum norm is $4(S^2 + R^2) = 4qI$, proving (17). For any such prime power the finite field $\mathbb{F}_q$ exists, and -1 is a square because its multiplicative group is cyclic and $4 \mid q - 1$. The quadratic-character proof above therefore gives (19) on $\mathbb{F}_q$ without change. Apply Spence's recurrence [7, Theorem 4, p. 254] in (20). The induction above gives symmetric, commuting sign matrices with (21) for every $r \geq 0$. Proposition 2, equivalently the Cooper–Wallis substitution [3, Theorem 3, p. 274], then gives order $2524w_0q^r = 1262(q+1)q^r$. □

The following eight choices give the remaining Spence families in Theorem 1. Its seventeen families comprise sixteen specializations of the uniform construction and the cubic family. The uniform statement is not counted separately.

q	w_0	$1262(q+1)q^r$
25	13	$32812 \cdot 25^r$
73	37	$93388 \cdot 73^r$
157	79	$199396 \cdot 157^r$
181	91	$229684 \cdot 181^r$
193	97	$244828 \cdot 193^r$
233	117	$295308 \cdot 233^r$
10301	5151	$13001124 \cdot 10301^r$
30757	15379	$38816596 \cdot 30757^r$

$(r \geq 0)$.

Each of these sequences contains infinitely many orders outside the preceding nine families. Indeed, for sequences ap^{er} and $b\ell^{fs}$ with distinct primes p, ℓ, their p- and ℓ-valuations determine r, s, so the sequences have at most one common term. The eight added multipliers are powers of distinct primes. The only prime shared with a preceding multiplier is 5, in the multipliers 25 and 5; the quotient of the two initial terms is $32812/7572 = 13/3$, so those sequences are disjoint. Thus each added family contains infinitely many orders outside the other sixteen. Some initial orders coincide: for example, $295308 = 32812 \cdot 3^2$. Equality of orders alone gives no conclusion about equivalence of the corresponding matrices.

Finite recipes and the field of order 25. For $q = 25$, use the following four first rows of length 13:

d	`--+-++-+--`
e	`+--+-++-+--`
f	`-+++-++-+++-`
g	`-+++-++-+++-`

These rows are obtained by changing signs in the width-13 input above. Their cyclic correlations satisfy both strong identities at $q = 25$. For its character core use

$$\mathbb{F}_{25} = \mathbb{F}_5[u]/(u^2 - 2), \qquad (a + bu)(c + du) = (ac + 2bd) + (ad + bc)u.$$

The nonzero squares modulo 5 are $1, 4$, so 2 is a nonsquare and this is a field. Index $a + bu$ by $a + 5b$, with $0 \leq a, b < 5$. Field subtraction is componentwise modulo 5. Its quadratic character is $\chi_{25}(0) = 0$ and $\chi_{25}(z) = z^{12}$ at nonzero z, with the values $1, 4$ interpreted as integer signs $1, -1$. The same square-subgroup and polynomial-root argument used for (18) proves this exponent formula. The recurrence group is $\mathbb{Z}/13\mathbb{Z} \times (\mathbb{F}_{25}, +)^r$, with each additive field factor represented by two coordinates modulo 5.

For each prime q in the next table, take $\mathbb{F}_q[\alpha]/(\alpha^2 - d)$, $g = c + \alpha$ and $g^{(q+1)/2} = \delta\alpha$. The Turyn formulas (29), with the field parameter renamed from r to q, specify the starter $(s, s, h + e, h - e)$.

q	d	c	δ	w_0
73	5	4	22	37
157	2	6	86	79
181	2	2	180	91
193	5	7	146	97
233	3	3	85	117
10301	2	6	2885	5151
30757	2	6	27180	15379

The program in Appendix D.2 checks the nonsquares, generator orders and denominators in this table. It reconstructs the eight starters and verifies both strong norm identities at every group coefficient. It also checks every cyclic Gram coefficient of the prime-field character cores, and the full order-25 core using the field arithmetic above.

For the first six parameters, the same program constructs the first recurrence step and checks every group

correlation. The resulting Hadamard orders are

q	w_1	$2524w_1$	order status
25	325	820300	Known
73	2701	6817324	Known
157	12403	31305172	New
181	16471	41572804	Known
193	18721	47251804	New
233	27261	68806764	New

Here "New" follows the convention in Section 1. On 28 November 2026 we checked classical construction criteria, thirteen Hexagon source archives, the announcement concerning Alpöge's constructions and the survey [9, 15], and searched for the individual orders. We found no earlier construction for the three orders marked New. The known orders follow from the constructions in Table 3. The source norms and T631 substitution prove the Gram and sign conditions without forming the final matrices. For $q = 10301, 30757$, we checked the finite starters independently but did not compute their first-step coefficient rows. Those first steps are therefore omitted from the finite list above, although Theorem 9 proves existence at every step. These eight families and six finite examples have not been formalized in Lean.

D.2 Integer check for the additional Spence sources

The following standard-library program uses the function `prime` from Appendix A.3 and the parameter table and four order-13 words printed in Section D.1.5. It checks every cyclic shift of each prime core and starter and constructs the six smaller first recurrence sources in full.

The bitset calculation recovers every Gram entry from the following autocorrelations. For a ternary row, let P, N be the bitsets of its positive and negative supports. For a group shift, let P_s, N_s be the corresponding shifted bitsets. Its autocorrelation is

$$|P \cap P_s| + |N \cap N_s| - |P \cap N_s| - |N \cap P_s|.$$

Python's `bit_count` computes each cardinality exactly. For a coordinate of size d and stride t, each block has dt bits; a shift of b positions moves the first bt bits to the end of its own block. The masks in `group_operations` repeat these block boundaries, so no bits cross into another coordinate block. Recursing through the coordinate sizes enumerates each group shift once. The half-difference norms must equal $q^r\delta_{s,0}$ and the half-sum norms $q^{r+1}\delta_{s,0}$, which are precisely the two strong matrix norms after multiplication by 4. Group development and the separately checked symmetry identify these autocorrelations with all Gram entries. These integer support operations avoid quadratic Python loops for the large cyclic fields. The calculation uses neither floating-point arithmetic nor an external matrix package.

```
# BEGIN_EXTENDED_SPENCE
# Independent finite recipes for the eight additional all-parameter families.
EXTENDED_TURYN_PARAMETERS = [
    (73, 5, 4, 22), (157, 2, 6, 86), (181, 2, 2, 180),
    (193, 5, 7, 146), (233, 3, 3, 85),
    (10301, 2, 6, 2885), (30757, 2, 6, 27180),
]
EXTENDED_25_WORDS = ('----+-++-+---', '+---+-++-+---',
                     '--+++-++-+++-', '--+++-++-+++-')
EXTENDED_SMALL = (25, 73, 157, 181, 193, 233)

def prime_divisors(n):
    result = []
    d = 2
    while d*d <= n:
        if n % d == 0:
            result.append(d)
            while n % d == 0:
                n //= d
        d += 1
    if n > 1:
        result.append(n)
```

```
    return result

def extended_turyn(q, d, c, delta):
    assert prime(q) and q % 4 == 1
    assert pow(d, (q-1)//2, q) == q-1
    def mul(x, y):
        return ((x[0]*y[0]+d*x[1]*y[1]) % q,
                (x[0]*y[1]+x[1]*y[0]) % q)
    def power(x, n):
        z = (1, 0)
        while n:
            if n & 1:
                z = mul(z, x)
            x = mul(x, x)
            n //= 2
        return z
    g, order, w = (c, 1), q*q-1, (q+1)//2
    assert power(g, order) == (1, 0)
    assert all(power(g, order//p) != (1, 0)
               for p in prime_divisors(order))
    assert power(g, w) == (0, delta) and delta
    inverse, z, b = pow(delta, -1, q), (1, 0), []
    for j in range(q+1):
        x = -2*z[1]*inverse % q
        value = pow(x, (q-1)//2, q) if x else 0
        b.append(-1 if value == q-1 else value)
        z = mul(z, g)
    h = [(-1)**k*b[2*k] for k in range(w)]
    o = [(-1)**k*b[2*k+1] for k in range(w)]
    s = [o[(k+(w-1)//2) % w] for k in range(w)]
    return [s, s, [h[k]+(k == 0) for k in range(w)],
                  [h[k]-(k == 0) for k in range(w)]]

def support_mask(row, value):
    data = bytearray((len(row)+7)//8)
    for i, x in enumerate(row):
        if x == value:
            data[i >> 3] |= 1 << (i & 7)
    return int.from_bytes(data, 'little')

def group_operations(dims):
    n = 1
    for d in dims:
        n *= d
    mask, stride, operations = (1 << n)-1, n, []
    for d in dims:
        stride //= d
        block = d*stride
        repeat = mask//((1 << block)-1)
        operations.append([(b*stride, block-b*stride,
            ((1 << (block-b*stride))-1)*repeat,
            ((1 << (b*stride))-1)*repeat) for b in range(d)])
    return n, operations

def all_group_correlations(rows, dims, expected):
    """Exact ternary dot products for every direct-product group shift."""
    n, operations = group_operations(dims)
    assert all(len(row) == n and set(row) <= {-1, 0, 1} for row in rows)
    planes = tuple(support_mask(row, value)
                   for value in (1, -1) for row in rows)
    count, channels = 0, len(rows)
    def visit(axis, shifted, origin):
        nonlocal count
        if axis == len(dims):
            correlations = []
            for j in range(channels):
                p, m = planes[j], planes[j+channels]
                sp, sm = shifted[j], shifted[j+channels]
                correlations.append((p & sp).bit_count()+(m & sm).bit_count()
```

```
                    -(p & sm).bit_count()-(m & sp).bit_count())
            assert correlations == expected(origin, correlations)
            count += 1
            return
        for shift, left, low, wrap in operations[axis]:
            moved = shifted if shift == 0 else tuple(
                ((x >> shift) & low) | ((x & wrap) << left) for x in shifted)
            visit(axis+1, moved, origin and shift == 0)
    visit(0, planes, True)
    assert count == n
    return count

def extended_strong_check(rows, dims, q, r):
    n = len(rows[0])
    assert len(rows) == 4 and all(len(row) == n and set(row) <= {-1, 1}
                                  for row in rows)
    # Group inversion is performed digit by digit in the declared dimensions.
    for i in range(n):
        remaining, inverse, stride = i, 0, n
        for d in dims:
            stride //= d
            digit, remaining = divmod(remaining, stride)
            inverse += (-digit % d)*stride
        assert all(row[i] == row[inverse] for row in rows)
    parts = [[(rows[0][i]-rows[1][i])//2 for i in range(n)],
             [(rows[2][i]-rows[3][i])//2 for i in range(n)],
             [(rows[0][i]+rows[1][i])//2 for i in range(n)],
             [(rows[2][i]+rows[3][i])//2 for i in range(n)]]
    def expected(origin, values):
        assert values[0]+values[1] == (q**r if origin else 0)
        assert values[2]+values[3] == (q**(r+1) if origin else 0)
        return values
    return all_group_correlations(parts, dims, expected)

def extended_character(q):
    if q != 25:
        assert prime(q) and q % 4 == 1
        squares = {a*a % q for a in range(1, q)}
        row = [0]+[1 if a in squares else -1 for a in range(1, q)]
        assert all(row[i] == row[-i % q] for i in range(q))
        all_group_correlations([row], (q,),
            lambda origin, values: [q-1 if origin else -1])
    else:
        # GF25=GF5[u]/(u^2-2), indexed by a+5b. Exponent12 is independent
        # of the norm shortcut used by the construction repository.
        assert pow(2, 2, 5) == 4
        def mul(x, y):
            return ((x[0]*y[0]+2*x[1]*y[1]) % 5,
                    (x[0]*y[1]+x[1]*y[0]) % 5)
        row = []
        for i in range(25):
            z, x, exponent = (1, 0), (i % 5, i//5), 12
            while exponent:
                if exponent & 1:
                    z = mul(z, x)
                x = mul(x, x)
                exponent //= 2
            assert z in ((0, 0), (1, 0), (4, 0))
            row.append(0 if z == (0, 0) else 1 if z == (1, 0) else -1)
        sub = lambda a, b: (a % 5-b % 5) % 5+5*((a//5-b//5) % 5)
        core = [[row[sub(j, i)] for j in range(25)] for i in range(25)]
        assert all(core[i][j] == core[j][i]
                   for i in range(25) for j in range(25))
        assert all(sum(a) == 0 for a in core)
        assert all(sum(core[i][k]*core[j][k] for k in range(25))
                   == 25*(i == j)-1 for i in range(25) for j in range(25))
    assert row[0] == 0 and sum(row) == 0 and set(row[1:]) == {-1, 1}
    return row
```

```
extended_starters = {25: [[1 if c == '+' else -1 for c in word]
                          for word in EXTENDED_25_WORDS]}
extended_starters.update({q: extended_turyn(q, d, c, delta)
                         for q, d, c, delta in EXTENDED_TURYN_PARAMETERS})
extended_finite_checks = []
for q, rows in extended_starters.items():
    w = (q+1)//2
    assert all(len(row) == w for row in rows)
    extended_strong_check(rows, (w,), q, 0)
    chi = extended_character(q)
    if q in EXTENDED_SMALL:
        expanded = []
        for a, b in ((rows[0], rows[1]), (rows[2], rows[3])):
            for sign in (1, -1):
                expanded.append([(a[k]-b[k])//2
                    +(a[k]+b[k])//2*(chi[x]+sign*(x == 0))
                    for k in range(w) for x in range(q)])
        dims = (w, 5, 5) if q == 25 else (w, q)
        extended_strong_check(expanded, dims, q, 1)
        extended_finite_checks.append((q, w*q, 2524*w*q))
assert extended_finite_checks == [(25, 325, 820300), (73, 2701, 6817324),
    (157, 12403, 31305172), (181, 16471, 41572804),
    (193, 18721, 47251804), (233, 27261, 68806764)]

# Positive prior recipes for the three recovered known first members.
assert prime(410149) and 410149 % 4 == 1 and 2*(410149+1) == 820300
assert prime(3408661) and 3408661 % 4 == 1 and 2*(3408661+1) == 6817324
assert prime(1598953) and 1598953 % 4 == 1
assert (1598953+1)//2 == 799477 and 4*13*799477 == 41572804

# Different growth primes give at most one intersection, by prime valuations.
# The sole common growth prime is new25 versus old5; their bases have
# different 13-valuations, so those two families have no intersection.
OLD_FAMILIES = [(7572,5), (17668,13), (22716,17), (32812,3), (78244,61),
    (128724,101), (153964,121), (174156,137), (15131380,109)]
EXTENDED_FAMILIES = [(1262*(q+1), q) for q in extended_starters]
assert len(OLD_FAMILIES+EXTENDED_FAMILIES) == 17
for i, (base, ratio) in enumerate(EXTENDED_FAMILIES):
    assert ratio % 4 == 1 and len(prime_divisors(ratio)) == 1
    for other_base, other_ratio in OLD_FAMILIES+EXTENDED_FAMILIES[:i]:
        if prime_divisors(ratio) == prime_divisors(other_ratio):
            assert (base, ratio, other_base, other_ratio) == (32812,25,7572,5)
            assert base % 13 == 0 and other_base % 13 != 0
# END_EXTENDED_SPENCE
```

E The cubic seed and tripling identities

E.1 An explicit cubic family

We obtain matrices of every order $32812 \cdot 3^r$, for all integers $r \geq 0$, by iterating the classical sixth-root tripling construction [14]. We first specify the starting pair and then prove the tripling step.

Lemma 10 (The starting pair of order 13)**.** *There are sign matrices A_0, B_0 of order 13 satisfying*

$$A_0 B_0^{\mathsf{T}} = B_0 A_0^{\mathsf{T}}, \qquad A_0 A_0^{\mathsf{T}} + 3 B_0 B_0^{\mathsf{T}} = 52 I_{13}. \tag{23}$$

Proof. Table 2 specifies their rows in order $0, \ldots, 12$: each $+$ means the integer 1 and each $-$ means the integer -1. The corresponding sixth-root source is the known order-13 example $M_{13A}^{(0)}$ up to multiplication of rows and columns by sixth roots of unity [13]. We check the two identities directly from these integer entries. In the last column, L denotes the symmetric matrix with zero diagonal whose entries above the diagonal are 1 at the listed indices and 0 at the unlisted indices.

To write the products compactly, let E be the symmetric 13×13 matrix whose entry E_{ij} is 1 precisely when $i \neq j$ and i, j belong to the same one of the three sets

$$\{1, 2, 3, 4\}, \qquad \{5, 7, 9, 11\}, \qquad \{6, 8, 10, 12\},$$

i	row i of A_0	row i of B_0	$\{j > i : L_{ij} = 1\}$
0	`+------`	`++++++++++++`	$\varnothing$
1	`--+++++++--`	`+++++++---`	$2, 3, 5, 6, 9, 10$
2	`--+++++++-+`	`+++--+++-+`	$4, 5, 8, 9, 12$
3	`--+++-+++-+`	`+--++-+-+++`	$4, 6, 7, 10, 11$
4	`--++++-++-+`	`+-+-+-++++-`	$7, 8, 11, 12$
5	`-++-++-+++`	`+-+++--+-+-+`	$9, 10, 11, 12$
6	`-++-+--++++-`	`+-+-+-+-+-++`	$7, 8, 9, 10$
7	`-+++-++-+-+`	`+-+-+++-++-`	$8, 9, 11$
8	`-++-++-+-++-`	`+-++-+-++-+-`	$9, 12$
9	`-+-+-++-+++`	`++-+-+--+-++`	$\varnothing$
10	`-++-+-++++-`	`++--++-+-+-+`	$11, 12$
11	`-+++-++--++`	`++-+-+++-+-`	12
12	`-++-++--+++-`	`++-++-+-++-`	$\varnothing$

Table 2: The order-13 sign pair and the upper triangular entries of the auxiliary symmetric matrix L.

and is 0 otherwise. Finally, let $e_0 = (1, 0, \ldots, 0)^{\mathsf{T}} \in \mathbb{Q}^{13}$. Taking the dot products of the displayed rows gives

$$A_0 A_0^{\mathsf{T}} = 16 I_{13} - 3 J_{13} + 12 E, \tag{24}$$

$$B_0 B_0^{\mathsf{T}} = 12 I_{13} + J_{13} - 4 E, \tag{25}$$

$$A_0 B_0^{\mathsf{T}} = J_{13} - 12 e_0 e_0^{\mathsf{T}} - 4 L. \tag{26}$$

Each identity is a finite calculation from the table, using

$$(X Y^{\mathsf{T}})_{ij} = \sum_{k=0}^{12} X_{ik} Y_{jk}, \qquad X, Y \in \{A_0, B_0\}.$$

For example, the $(0,0)$ entries in the three products are $13, 13, -11$, since row 0 of A_0 has one plus sign and twelve minus signs, whereas row 0 of B_0 consists entirely of plus signs. For distinct indices, the first two right sides give respectively $(9, -3)$ when $E_{ij} = 1$ and $(-3, 1)$ when $E_{ij} = 0$. The last matrix has off-diagonal entry -3 at the pairs listed in the table's last column, and 1 at the other pairs. These cases cover all row products. In particular (26) is symmetric. Adding (24) and three times (25) cancels both E and J_{13} and leaves $(16 + 36) I_{13} = 52 I_{13}$. This proves (23).

The following integer loop checks the same calculation. Let `A` and `B` be the arrays of rows in the table; the loop checks all 169 entries of both identities:

```
def dot(x, y):
    return sum(a*b for a, b in zip(x, y))
for i in range(13):
    for j in range(13):
        assert dot(A[i], B[j]) == dot(B[i], A[j])
        assert dot(A[i], A[j]) + 3*dot(B[i], B[j]) == 52*(i == j)
```

□

Lemma 11 (The tripling step)**.** *Suppose that A, B are sign matrices of order n satisfying*

$$A B^{\mathsf{T}} = B A^{\mathsf{T}}, \qquad A A^{\mathsf{T}} + 3 B B^{\mathsf{T}} = 4 n I_n. \tag{27}$$

Define

$$C = \begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}, \qquad A' = B \otimes J_3, \qquad B' = A \otimes I_3 + B \otimes C.$$

Then A', B' are sign matrices of order $3n$ and satisfy

$$A' B'^{\mathsf{T}} = B' A'^{\mathsf{T}}, \qquad A' A'^{\mathsf{T}} + 3 B' B'^{\mathsf{T}} = 4(3n) I_{3n}.$$

Proof. Both matrices are indexed by $\{0,\dots,n-1\}\times\{0,1,2\}$. Their entries are

$$A'_{(i,a),(j,b)} = B_{ij}, \qquad B'_{(i,a),(j,b)} = A_{ij}\delta_{ab} + B_{ij}C_{ab}.$$

The first entry is a sign. In the second formula, if $a = b$ the entry is A_{ij}, and if $a \neq b$ it is $C_{ab}B_{ij}$ with $C_{ab} \in \{-1, 1\}$. Thus every entry of B' is also a sign.

Direct multiplication of the displayed 3×3 matrices gives

$$C^{\mathsf{T}} = -C, \quad CC^{\mathsf{T}} = \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix} = 3I_3 - J_3, \quad CJ_3 = J_3C = 0, \quad J_3^2 = 3J_3.$$

The vanishing products with J_3 also follow from the zero row sums and zero column sums of C. We use the identities $(X \otimes Y)^{\mathsf{T}} = X^{\mathsf{T}} \otimes Y^{\mathsf{T}}$ and $(X \otimes Y)(Z \otimes W) = XZ \otimes YW$; both follow by expanding a matrix entry and separating the two finite summation indices. Consequently

$$\begin{aligned} A'B'^{\mathsf{T}} &= BA^{\mathsf{T}} \otimes J_3 + BB^{\mathsf{T}} \otimes J_3C^{\mathsf{T}} = BA^{\mathsf{T}} \otimes J_3, \\ B'A'^{\mathsf{T}} &= AB^{\mathsf{T}} \otimes J_3 + BB^{\mathsf{T}} \otimes CJ_3 = AB^{\mathsf{T}} \otimes J_3. \end{aligned}$$

They are equal by (27). The two norm expansions are

$$\begin{aligned} A'A'^{\mathsf{T}} &= 3BB^{\mathsf{T}} \otimes J_3, \\ B'B'^{\mathsf{T}} &= AA^{\mathsf{T}} \otimes I_3 + AB^{\mathsf{T}} \otimes C^{\mathsf{T}} + BA^{\mathsf{T}} \otimes C + BB^{\mathsf{T}} \otimes CC^{\mathsf{T}} \\ &= AA^{\mathsf{T}} \otimes I_3 + BB^{\mathsf{T}} \otimes (3I_3 - J_3). \end{aligned}$$

In the last equality, the two mixed terms cancel because $C^{\mathsf{T}} = -C$ and $AB^{\mathsf{T}} = BA^{\mathsf{T}}$. It follows that

$$\begin{aligned} A'A'^{\mathsf{T}} + 3B'B'^{\mathsf{T}} &= 3(AA^{\mathsf{T}} + 3BB^{\mathsf{T}}) \otimes I_3 \\ &= 12n(I_n \otimes I_3) = 4(3n)I_{3n}. \end{aligned}$$

□

Starting with the pair A_0, B_0 in Table 2, apply Lemma 11 r times, and call the result A_r, B_r. Induction gives sign matrices of order $n_r = 13 \cdot 3^r$ with

$$A_rB_r^{\mathsf{T}} = B_rA_r^{\mathsf{T}}, \qquad A_rA_r^{\mathsf{T}} + 3B_rB_r^{\mathsf{T}} = 4n_rI_{n_r} \qquad (r \geq 0).$$

These identities give real Hadamard matrices directly. The quadruple (A_r, B_r, B_r, B_r) satisfies the hypotheses of Proposition 2: its summed norm is the weighted norm above, and the mixed-product relations reduce to $A_rB_r^{\mathsf{T}} = B_rA_r^{\mathsf{T}}$ or have both sides equal to $B_rB_r^{\mathsf{T}}$. Hence

$$\widetilde{H}_r = X_0 \otimes A_r + (X_1 + X_2 + X_3) \otimes B_r$$

is a real Hadamard matrix of order $2524n_r = 32812 \cdot 3^r$. The Lean existence proof formalizes this construction. We can obtain matrices of the same orders from sixth-root sources, although the two constructions need not give the same matrices.

For the scalar interpretation of A_r, B_r, put

$$W_r = \frac{A_r + \xi B_r}{2}, \qquad N_r = \zeta^{-1}W_r.$$

Since A_r, B_r are real matrices and $\bar{\xi} = -\xi$, multiplication gives

$$\begin{aligned} W_rW_r^* &= \frac{1}{4}\left(A_rA_r^{\mathsf{T}} + 3B_rB_r^{\mathsf{T}} + \xi(B_rA_r^{\mathsf{T}} - A_rB_r^{\mathsf{T}})\right) \\ &= n_rI_{n_r}. \end{aligned}$$

Each entry of W_r is one of $\zeta, \bar{\zeta}, -\zeta, -\bar{\zeta}$, because its real and imaginary parts are respectively $\pm 1/2$ and $\pm\sqrt{3}/2$. Also $\bar{\zeta}/\zeta = -\zeta$, as follows from $\zeta^3 = -1$ and $\bar{\zeta} = \zeta^{-1}$. It follows that every entry of N_r belongs to the four scalars (16). Multiplication by ζ^{-1} has absolute value 1, so $N_r N_r^* = n_r I_{n_r}$ as well. The blocks

$$H_{ij}^{(r)} = \rho\big((N_r)_{ij}\big)P$$

are all $P, Q, -P$ or $-Q$ and form a real Hadamard matrix of order

$$dn_r = 2524 \cdot 13 \cdot 3^r = 32812 \cdot 3^r.$$

Thus the cubic family exists for every $r \geq 0$, with orders 32812, 98436 and 295308 at $r = 0, 1, 2$.

F Paired-design data and finite-field recipes

F.1 A conditional paired-design construction

A coefficient design of order 20 gives the fifteen Hadamard orders in the table below. Twelve are new and three are known. We call a real Hadamard matrix *paired* if its rows and columns have partitions into pairs for which every resulting 2×2 block is Hadamard. The partitions for rows and columns may differ, and block determinants may have either sign. We use Kline's paired-transfer theorem [24, Theorem 1]: for odd $m \geq 3$, a paired real Hadamard matrix of order $2(m-1)$ and a symmetric or skew-symmetric conference matrix of order $m+1$ give a real Hadamard matrix of order $8m$. The quaternary-input case is Miyamoto's earlier construction; the cited extension permits both signs of the paired-block determinants.

F.1.1 The order-20 coefficient design and its pairing

On $\mathbb{Z}/5\mathbb{Z}$, take the four rows

$$a_0 = (1,0,0,0,0), \quad a_1 = (0,1,1,0,0), \quad a_2 = (0,0,0,1,-1), \quad a_3 = (0,0,0,0,0).$$

Their supports partition the five coordinates and their summed periodic correlation is $5\delta_{s,0}$. In the notation of (3), with back-diagonal reversal $u + v = 4$, put

$$\begin{aligned} E_0 &= \mathrm{GS}(a_0, a_1, a_2, a_3), & E_1 &= \mathrm{GS}(a_1, -a_0, a_3, -a_2), \\ E_2 &= \mathrm{GS}(a_2, -a_3, -a_0, a_1), & E_3 &= \mathrm{GS}(a_3, a_2, -a_1, -a_0). \end{aligned}$$

These are order-20 matrices with disjoint signed supports covering all positions. The Cooper–Wallis coefficient identities are

$$E_j E_j^{\mathsf{T}} = 5I_{20}, \qquad E_i E_j^{\mathsf{T}} + E_j E_i^{\mathsf{T}} = 0 \quad (i \neq j). \tag{28}$$

They can also be checked directly from the five-entry rows, as in Appendix F.2 below. Encode their signed partition by $L_{a,b} = \sum_{j=0}^{3} (j+1)(E_j)_{a,b}$; thus an entry $\pm(j+1)$ means $\pm x_j$ in the coefficient design.

Use the following ordered row and column pair partitions of $\{0, \ldots, 19\}$:

$$\begin{aligned} \mathcal{R} = ((0,12),&(1,11),(2,10),(3,14),(4,13),\\ &(5,15),(6,19),(7,18),(8,17),(9,16)),\\ \mathcal{C} = ((19,7),&(6,15),(1,12),(5,16),(0,13),\\ &(2,11),(8,18),(17,9),(3,10),(4,14)). \end{aligned}$$

For each of the 100 resulting 2×2 coefficient blocks, the product of its four coefficient signs is -1. After identifying $x_0 = x_1$, each remaining variable occurs an even number of times in that block. Appendix F.2 checks these assertions for every block of L and verifies both partitions.

Let A_0, A_1, A_2, A_3 be a Williamson-type quadruple of order w with $A_0 = A_1$. Thus its entries are signs, its summed row Gram is $4wI_w$, and $A_i A_j^{\mathsf{T}} = A_j A_i^{\mathsf{T}}$. The cancellation in Proposition 2, now using (28), gives

$$H = \sum_{j=0}^{3} E_j \otimes A_j, \qquad HH^{\mathsf{T}} = 20wI_{20w}.$$

Pair rows $(\mathcal{R}_i(0), u), (\mathcal{R}_i(1), u)$ for every internal index u, and pair columns $(\mathcal{C}_j(0), v), (\mathcal{C}_j(1), v)$ for every v. In each sign block, equal variable labels have the same internal indices. Each substituted variable therefore occurs to an even power and contributes 1 to the product. The product of all four entries is then -1. A 2×2 sign matrix with product -1 has orthogonal rows, proving that H is paired.

F.1.2 Explicit repeated-member inputs

We use classical repeated-member Williamson quadruples [18]. The following finite-field formulas, also used in [25, Appendix A], specify the fifteen inputs. For each row of the table, work in $K = \mathbb{F}_r[\alpha]/(\alpha^2 - d)$, let $w = (r+1)/2$, and put $g = c + \alpha$. The listed d is a nonsquare, g has order $r^2 - 1$, and $g^w = \delta\alpha$:

r	d	c	δ	w	$m = 10w + 1$	$8m$	*Status*
653	2	2	1	327	3271	26168	New
673	5	4	230	337	3371	26968	New
1069	2	3	730	535	5351	42808	New
1117	2	2	1	559	5591	44728	New
1373	2	12	1335	687	6871	54968	Known
1381	2	2	1380	691	6911	55288	New
1657	5	4	365	829	8291	66328	New
1877	2	2	1876	939	9391	75128	New
2017	5	5	2	1009	10091	80728	New
2053	2	2	2052	1027	10271	82168	New
2153	3	5	1906	1077	10771	86168	New
2213	2	2	2212	1107	11071	88568	Known
2281	7	9	434	1141	11411	91288	New
2293	2	2	2292	1147	11471	91768	New
2297	3	7	416	1149	11491	91928	Known

Let $\chi_r(0) = 0$ and let χ_r be the quadratic character on $\mathbb{F}_r^*$. For $0 \le j \le r$ define

$$b_j = \chi_r\left(\frac{g^{jr} - g^j}{g^w}\right).$$

The argument is in $\mathbb{F}_r$: both numerator and denominator change sign under Frobenius. With indices modulo w, set

$$h_k = (-1)^k b_{2k}, \quad o_k = (-1)^k b_{2k+1}, \quad s_k = o_{k+(w-1)/2}, \quad e_k = \delta_{k,0}.$$

The required quadruple consists of the circulants with first rows

$$(s, s, h + e, h - e). \tag{29}$$

For each row of the table, the program below checks that these are symmetric sign rows and that all w coefficients of their summed cyclic Gram equal $4w\delta_{s,0}$. Symmetric circulants commute, so the amicability relations follow. The program in Appendix F.2 also checks every generator order and nonsquare, and proves primality for every r and m.

In each case the paired input has order $20w = 2(m-1)$. The primes m are 3 modulo 4, so Paley's construction gives a skew conference matrix of order $m + 1$. Kline's theorem now gives all fifteen real Hadamard orders $8m$ in the table. The twelve entries marked New contribute to Theorem 1; the other three also follow from the earlier constructions in Section G.2. The Gram and sign identities prove the result without forming the final matrices. Independent programs in the repository check every cyclic Gram coefficient of the inputs, the finite Paley identities and the transfer identities. These fifteen cases have not been formalized in Lean.

F.2 Integer check for the paired-design inputs

The following code uses the standard library and the trial-division function `prime` printed above. It constructs the four order-20 coefficient matrices in the stated GS convention, checks every coefficient Gram entry and every paired block after $x_0 = x_1$, and reconstructs all fifteen finite-field inputs. It checks each primitive order at every

prime divisor of r^2-1 and sums the cyclic correlations at every shift, including zero. The sign, symmetry, pairing and norm arguments in Section F.1 then prove the input Grams. Paley's conference matrices and the cited paired-transfer theorem give all fifteen Hadamard matrices. The code uses no stored matrix or search transcript.

```
# BEGIN_PAIRED_INPUTS
PAIR_PARAMETERS = [
    (653, 2, 2, 3271),
    (673, 5, 4, 3371),
    (1069, 2, 3, 5351),
    (1117, 2, 2, 5591),
    (1373, 2, 12, 6871),
    (1381, 2, 2, 6911),
    (1657, 5, 4, 8291),
    (1877, 2, 2, 9391),
    (2017, 5, 5, 10091),
    (2053, 2, 2, 10271),
    (2153, 3, 5, 10771),
    (2213, 2, 2, 11071),
    (2281, 7, 9, 11411),
    (2293, 2, 2, 11471),
    (2297, 3, 7, 11491),
]
T5 = [[1,0,0,0,0], [0,1,1,0,0],
      [0,0,0,1,-1], [0,0,0,0,0]]
PAIR_ROWS = [(0,12),(1,11),(2,10),(3,14),(4,13),
             (5,15),(6,19),(7,18),(8,17),(9,16)]
PAIR_COLS = [(19,7),(6,15),(1,12),(5,16),(0,13),
             (2,11),(8,18),(17,9),(3,10),(4,14)]
IX = [[0,1,2,3],[1,0,3,2],[2,3,0,1],[3,2,1,0]]
SG = [[1,1,1,1],[1,-1,1,-1],
      [1,-1,-1,1],[1,1,-1,-1]]
# GS slots: input, transpose, reversal, sign.
SL = [[(0,0,0,1),(1,0,1,1),(2,0,1,1),(3,0,1,1)],
      [(1,0,1,-1),(0,0,0,1),(3,1,1,-1),(2,1,1,1)],
      [(2,0,1,-1),(3,1,1,1),(0,0,0,1),(1,1,1,-1)],
      [(3,0,1,-1),(2,1,1,-1),(1,1,1,1),(0,0,0,1)]]
E = [[[0]*20 for i in range(20)] for v in range(4)]
for a in range(20):
    for b in range(20):
        k,tr,rev,sg = SL[a//5][b//5]
        i,j = a%5,b%5
        if rev: j=4-j
        if tr: i,j=j,i
        for v in range(4):
            E[v][a][b]=sg*SG[v][k]*T5[IX[v][k]][(j-i)%5]
        assert sum(abs(E[v][a][b]) for v in range(4))==1
for u in range(4):
    for v in range(u+1):
        for a in range(20):
            for b in range(20):
                c=sum(E[u][a][k]*E[v][b][k] for k in range(20))
                if u==v: assert c==5*(a==b)
                else:
                    c+=sum(E[v][a][k]*E[u][b][k] for k in range(20))
                    assert c==0
L=[[sum((v+1)*E[v][a][b] for v in range(4))
    for b in range(20)] for a in range(20)]
assert sorted(x for p in PAIR_ROWS for x in p)==list(range(20))
assert sorted(x for p in PAIR_COLS for x in p)==list(range(20))
for rp in PAIR_ROWS:
    for cp in PAIR_COLS:
        block=[L[a][b] for a in rp for b in cp]
        assert sum(x<0 for x in block)%2==1
        classes=[0 if abs(x)<=2 else abs(x)-1 for x in block]
        assert all(classes.count(c)%2==0 for c in (0,2,3))
paired_checked=[]
for r,d,g0,m in PAIR_PARAMETERS:
    assert prime(r) and r%4==1 and prime(m) and m%4==3
    assert pow(d,(r-1)//2,r)==r-1
    def fm(x,y):
        return ((x[0]*y[0]+d*x[1]*y[1])%r,
                (x[0]*y[1]+x[1]*y[0])%r)
    def fp(x,n):
        z=(1,0)
        while n:
            if n%2: z=fm(z,x)
            x=fm(x,x);n//=2
        return z
    N=r*r-1;left=N;factors=[];p=2
    while p*p<=left:
```

```
        if left%p==0:
            factors.append(p)
            while left%p==0: left//=p
        p+=1
    if left>1: factors.append(left)
    g=(g0,1);w=(r+1)//2
    assert fp(g,N)==(1,0)
    assert all(fp(g,N//p)!=(1,0) for p in factors)
    den=fp(g,w);assert den[0]==0 and den[1]
    inv=pow(den[1],-1,r);z=(1,0);b=[]
    for j in range(r+1):
        x=(-2*z[1]*inv)%r
        h=pow(x,(r-1)//2,r) if x else 0
        b.append(-1 if h==r-1 else h);z=fm(z,g)
    h=[(-1)**k*b[2*k] for k in range(w)]
    o=[(-1)**k*b[2*k+1] for k in range(w)]
    s=[o[(k+(w-1)//2)%w] for k in range(w)]
    rows=[s,s,[h[k]+(k==0) for k in range(w)],
              [h[k]-(k==0) for k in range(w)]]
    assert all(abs(x)==1 for row in rows for x in row)
    assert all(row[k]==row[-k%w] for row in rows for k in range(w))
    for shift in range(w):
        c=sum(row[k]*row[(k+shift)%w] for row in rows for k in range(w))
        assert c==4*w*(shift==0)
    assert m==10*w+1 and 20*w==2*(m-1)
    paired_checked.append((20*w,8*m))
PAIRED_EXPECTED = [
    (6540, 26168),
    (6740, 26968),
    (10700, 42808),
    (11180, 44728),
    (13740, 54968),
    (13820, 55288),
    (16580, 66328),
    (18780, 75128),
    (20180, 80728),
    (20540, 82168),
    (21540, 86168),
    (22140, 88568),
    (22820, 91288),
    (22940, 91768),
    (22980, 91928),
]
assert paired_checked==PAIRED_EXPECTED

KNOWN_PAIRED_SY = [(54968,6871,3435,6869),
                   (88568,11071,5535,11069),
                   (91928,11491,5745,11489)]
for n,q,w,p in KNOWN_PAIRED_SY:
    assert prime(q) and q%4==3 and prime(p) and p%4==1
    assert p==q-2 and w==(p+1)//2==(q-1)//2 and n==8*q
# END_PAIRED_INPUTS
```

G Earlier constructions and matrix comparisons

G.1 Completion of the theorem and known members

Proof of Theorem 1. Section C.1 gives thirteen orders and Section C.2 gives twelve more. The cubic family adds $295308 = 32812 \cdot 3^2$. Eight further orders follow from the Spence recurrences:

(q, r)	w_r	$2524 w_r$
$(13, 1)$	91	229684
$(17, 1)$	153	386172
$(61, 1)$	1891	4772884
$(101, 1)$	5151	13001124
$(13, 2)$	1183	2985892
$(13, 3)$	15379	38816596
$(61, 2)$	115351	291145924
$(109, 1)$	5995	15131380

This gives thirty-four distinct orders. Section F.1 contributes the twelve new orders in its table, and Section D.1.5 contributes 31305172, 47251804 and 68806764. These fifteen orders are distinct from the preceding thirty-four and from each other, proving the forty-nine finite claims of Theorem 1. The sixteen Spence specializations and

the cubic recurrence give the seventeen families. In every case we have proved sign entries and a Gram identity whose scale equals the order. Nonsingularity follows as in Section 1. □

Each of the seventeen families starts at a new order, although some later members have known orders. For example, $32812 \cdot 3^3 = 885924$ is known by Paley's first construction, with prime parameter 885923, and $153964 \cdot 121 = 18629644$ is known by Paley's second construction, with prime parameter 9314821. We recall both constructions below; the integer checker verifies their prime parameters.

For an odd prime t, let $K_{x,y} = \chi_t(y - x)$ on $\mathbb{F}_t$, and let J_t be the all-one matrix. The character-sum proof in Section D.1 applies without change to give $KK^\mathsf{T} = tI_t - J_t$ and $KJ_t = J_tK = 0$. It does not use $\chi_t(-1) = 1$ until symmetry is asserted. The squaring map has $(t-1)/2$ nonzero values. By Lagrange's theorem all are roots of $X^{(t-1)/2} - 1$, and the degree bound for polynomial roots shows that these are precisely its roots. Therefore $\chi_t(a) = a^{(t-1)/2}$ for $a \neq 0$, with the two values interpreted as the integer signs. In particular, $\chi_t(-1) = (-1)^{(t-1)/2}$.

If $t \equiv 3 \pmod 4$, then $K^\mathsf{T} = -K$. Let $\mathbf{1}$ denote the column of t ones. The sign matrix

$$B = \begin{pmatrix} 1 & \mathbf{1}^\mathsf{T} \\ \mathbf{1} & K - I_t \end{pmatrix}$$

has order $t + 1$. Its upper-left Gram entry is $t + 1$, its off-diagonal Gram blocks vanish because the rows of $K - I_t$ sum to -1, and its lower-right Gram block is

$$J_t + (K - I_t)(K^\mathsf{T} - I_t) = J_t + KK^\mathsf{T} + I_t = (t + 1)I_t.$$

This is Paley's first construction [2]. Taking $t = 885923$ gives order 885924.

If $t \equiv 1 \pmod 4$, then $K^\mathsf{T} = K$ and the matrix

$$C = \begin{pmatrix} 0 & \mathbf{1}^\mathsf{T} \\ \mathbf{1} & K \end{pmatrix}$$

is symmetric, has zero diagonal and sign off-diagonal entries, and satisfies $C^2 = tI_{t+1}$. Indeed the off-diagonal blocks vanish by $K\mathbf{1} = 0$, and the lower-right block is $J_t + K^2 = tI_t$. With $I = I_{t+1}$, form

$$B = \begin{pmatrix} C + I & C - I \\ C - I & -C - I \end{pmatrix}.$$

Both $C + I$ and $C - I$ are sign matrices. A diagonal Gram block of B is $(C + I)^2 + (C - I)^2 = 2(t + 1)I$, and an off-diagonal block is $(C + I)(C - I) - (C - I)(C + I) = 0$. This proves Paley's second construction [2]. The value $t = 9314821$ gives order $2(t + 1) = 18629644$. The trial-division code proves that both parameters are prime.

The length-127 construction gives a separate T-matrix result, not a new Hadamard order. For example, the order-3 quadruple in Section C.1 and Proposition 2 give a Hadamard matrix of the known order $4 \cdot 127 \cdot 3 = 1524$. The dated survey [15], Table 3, lists 127 as its smallest open *periodic* T-matrix order. Its Table 5 lists 631 in the unresolved $4 \cdot 3p$ row; the other records consulted on 24 November 2026 also list order 7572 as unresolved [16, 17]. The next subsection lists the earlier constructions we found for the known orders. The repository contains the dated literature checks for all finite orders considered here.

G.2 Recovered known orders and matrix equivalence

G.2.1 The thirty-seven known orders

The same constructions also give real Hadamard matrices at the thirty-seven known orders in Table 3. Together with the forty-nine new orders in Theorem 1, these give eighty-six distinct orders. We count repeated orders once and count only the finite examples checked individually, rather than all members of the infinite families.

In the table, Paley I has order $q + 1$ for a prime $q \equiv 3 \pmod 4$, and Paley II has order $2(q + 1)$ for a prime $q \equiv 1 \pmod 4$; their Gram calculations were given above. The Paley-block product uses $q \equiv 3 \pmod 8$ and a classical T-matrix input of length t to give order $(q + 1)t$; see Seberry–Yamada, Theorem 4 [20], and the Paley-block formulation in [15]. The Cooper–Wallis construction combines T-matrices of length t with a Williamson-type quadruple of order w to give order $4tw$ [3]. In the rows marked "CW/TW", the latter quadruple

is supplied by the Turyn–Whiteman construction, with $w = (q+1)/2$ for the indicated prime $q \equiv 1 \pmod 4$ [18, 19]. The rows marked "SY/TW" use Seberry–Yamada's construction [27, Lemma 8.12], which gives order $8q$ from a Williamson-type quadruple of order $(q-1)/2$ and the conference input; see also the Seberry–Yamada row of [15, Table 4]. Here q is prime and $q \equiv 3 \pmod 4$, so Paley supplies that input. Turyn supplies the quadruple of order $w = (p+1)/2 = (q-1)/2$ because $p = q-2$ is prime and $p \equiv 1 \pmod 4$. The three pairs (q, p) are $(6871, 6869)$, $(11071, 11069)$ and $(11491, 11489)$. The integer verifier checks all six primes and all three order formulas.

All T-matrix lengths $t \le 19$ used in the table are classical [3]. For $t = 113$, Best et al., Corollary 5.1 [23], construct the required T-sequences from base sequences of lengths $75, 75, 38, 38$. Aperiodic T-sequences also satisfy the periodic correlation identity used here: at a nonzero shift s, the periodic sum is the sum of the two aperiodic correlations at shifts s and $t - s$, both of which vanish.

The order-8636 row uses a previously known Williamson-type quadruple of order 127 [22], not the new T-matrices of length 127 proved in this paper. The order-2524 row refers to the cyclic supplementary difference sets and Goethals–Seidel construction of Đoković, Golubitsky and Kotsireas [21], Section 3.3. Their cyclic group has order $v = 631$, and their block sizes are $315, 330, 330, 330$ in $\mathbb{Z}/v\mathbb{Z}$; the common difference multiplicity is 674.

Table 3: Recovered known orders and positive prior constructions. "CW" denotes Cooper–Wallis; "TW" denotes Turyn–Whiteman. The parameters have the meanings specified above.

Order	Prior construction	Parameters
1524	Paley I	$q = 1523$
2524	Cyclic difference sets	$v = 631$
3252	Paley I	$q = 3251$
6564	Paley I	$q = 6563$
8636	CW	$t = 17,\ w = 127$
12620	Paley I	$q = 12619$
27764	Paley I	$q = 27763$
37860	Paley-block product	$q = 12619,\ t = 3$
47956	Paley II	$q = 23977$
53004	Paley I	$q = 53003$
54968	SY/TW	$q = 6871,\ w = 3435,\ p = 6869$
63100	Paley-block product	$q = 12619,\ t = 5$
68148	Paley I	$q = 68147$
83292	Paley-block product	$q = 27763,\ t = 3$
88340	Paley I	$q = 88339$
88568	SY/TW	$q = 11071,\ w = 5535,\ p = 11069$
91928	SY/TW	$q = 11491,\ w = 5745,\ p = 11489$
103484	Paley I	$q = 103483$
113580	Paley-block product	$q = 12619,\ t = 9$
123676	Paley II	$q = 61837$
138820	Paley-block product	$q = 27763,\ t = 5$
143868	Paley II	$q = 71933$
159012	Paley-block product	$q = 53003,\ t = 3$
164060	Paley-block product	$q = 12619,\ t = 13$
239780	Paley I	$q = 239779$
335692	CW/TW	$t = 7,\ w = 11989,\ q = 23977$
456844	Paley II	$q = 228421$
820300	Paley II	$q = 410149$
885924	Paley I	$q = 885923$
3611844	CW/TW	$t = 9,\ w = 100329,\ q = 200657$
6564924	CW/TW	$t = 9,\ w = 182359,\ q = 364717$
6817324	Paley II	$q = 3408661$
11996572	CW/TW	$t = 7,\ w = 428449,\ q = 856897$

Order	Prior construction	Parameters
16257084	CW/TW	$t = 113,\ w = 35967,\ q = 71933$
18629644	Paley II	$q = 9314821$
23859372	Paley I	$q = 23859371$
41572804	CW/TW	$t = 13,\ w = 799477,\ q = 1598953$

The verification programs in the repository check the integer order formulas, prime parameters and congruences in this table, and link each order to its construction certificate. The dated verification records cover the original thirty-one orders, the three paired-design examples and the three added Spence members. These earlier constructions establish existence at the same orders; whether their matrices are equivalent to ours is a separate question.

G.2.2 Comparing the three paired-design examples

For the three SY/TW rows, we reconstruct the classical quaternary-input representatives using the universal quaternion coefficient design of order 4 and the Turyn inputs above. Direct integer calculations verify their cyclic Grams and the required transfer identities. To compare the labelled matrices, normalize a sign matrix by $\widehat{H}_{ij} = H_{00}H_{i0}H_{0j}H_{ij}$, making its first row and column positive. Exact entry evaluation gives

Order	i	j	$\widehat{H}_{ij}$ (classical)	$\widehat{H}_{ij}$ (paired design)
54968	53471	42200	-1	1
88568	56989	814	1	-1
91928	59151	845	-1	1

The normalized labelled matrices therefore differ at the displayed entries. They may still be Hadamard equivalent, since independent row and column permutations and sign changes are allowed. The public repository contains the classical construction data and the exact entry comparisons alongside the paired-design constructions.

G.2.3 A separate historical claim at order 41368

The same coefficient pairing and repeated-member construction gives a Hadamard matrix of order 41368, using $r = 1033$, $d = 5$, $g = 4 + \alpha$, $w = 517$ and Paley prime $m = 5171$. Pender's university-hosted *Balanced Group Matrices: Theory and Applications* [26, p. 79; PDF p. 94] explicitly lists 5171(3) under its convention $n(t) = 2^t n$ for real Hadamard orders. We therefore exclude 41368 from the new orders above. We have not recovered the parameters or matrix underlying Pender's claim, so we cannot yet compare the two matrices for equality or Hadamard equivalence. We discuss this case separately from the thirty-seven orders with explicit prior constructions in Table 3.

G.2.4 An inequivalence at order 885924

Two real Hadamard matrices H, K of the same order are *Hadamard equivalent* if $K = UHV$ for signed permutation matrices U, V. A signed permutation matrix has exactly one nonzero entry in every row and column, and that entry is 1 or -1; multiplication by such matrices permutes and changes signs of rows and columns. Their reductions modulo 3 are invertible, so equivalent matrices have the same rank over $\mathbb{F}_3$. For the order-885924 member, this invariant distinguishes the sixth-root representative $H^{(3)}$ of Section E.1 from the standard Paley matrix.

Proposition 12. *The matrix $H^{(3)}$ of order 885924 has rank 246090 over $\mathbb{F}_3$. Every skew Hadamard matrix of that order has rank 442962 over $\mathbb{F}_3$. In particular, $H^{(3)}$ is not Hadamard equivalent to the Paley I matrix with prime parameter 885923.*

Proof. Keep the integral sign matrices P, Q and $d = 2524$ from (7). Rational matrices whose denominators are not divisible by 3 can be reduced modulo 3. The identity $PP^{\mathsf{T}} = dI$ implies that P is invertible over $\mathbb{F}_3$, since 3 does not divide d. Put $M = P + Q$. Equation (7) gives

$$MM^{\mathsf{T}} = 3dI_d.$$

The row space of M modulo 3 is therefore totally isotropic for the nondegenerate standard bilinear form on $\mathbb{F}_3^d$: every two of its vectors have dot product zero. Its dimension r is at most $d/2$, since that space is contained in its orthogonal complement, of dimension $d-r$.

For the reverse inequality, taking determinants gives $(\det M)^2 = (3d)^d$. If $v_3(a)$ denotes the exponent of 3 in a nonzero integer a, this implies $v_3(\det M) = d/2$. An integral $d \times d$ matrix of rank r modulo 3 satisfies $3^{d-r} \mid \det M$. Indeed, perform Gaussian row elimination modulo 3 and lift its operations to integer row operations. The operations are row swaps, multiplication of a row by -1, and addition of an integer multiple of one row to another. Their determinants are 1 or -1, and the final $d-r$ rows have all entries divisible by 3. Factoring 3 from those rows proves the divisibility. Thus $d - r \le v_3(\det M) = d/2$, and $r = d/2 = 1262$.

Recall $R = QP^{-1}$, so $R^2 - R + I = 0$. Over $\mathbb{F}_3$ put $E = R + I = MP^{-1}$. Then $E^2 = 0$ and $\operatorname{rank} E = 1262$. Its image and kernel both have dimension 1262, and its image is contained in its kernel, so they are equal. Choose a basis u_i of this space and choose v_i with $Ev_i = u_i$. The vectors u_i, v_i are a basis of $\mathbb{F}_3^d$: applying E to a linear relation first kills all coefficients of the v_i, and independence of the u_i kills the rest. In this basis E is a direct sum of 1262 copies of $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$. Consequently the action of ζ is a direct sum of copies of $-I_2 + \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$.

Let $A = A_3, B = B_3$ be obtained by three applications of Lemma 11 to Table 2; their order is 351. The sixth-root source is $N_3 = \zeta^{-1}(A + \xi B)/2$, where $\xi = 2\zeta - 1$. On each two-dimensional summand write $\zeta = -1 + \epsilon$, where $\epsilon^2 = 0$. Then $\xi = 2\epsilon$ over $\mathbb{F}_3$. Multiplication by $\zeta^{-1}/2$ is invertible, so the regular action of N_3 has the same rank as $A + 2\epsilon B$. In the ordered basis $(\epsilon, 1)$, the latter has block matrix

$$\begin{pmatrix} A & 2B \\ 0 & A \end{pmatrix}.$$

Conjugating by $\operatorname{diag}(2I_{351}, I_{351})$ replaces $2B$ by B over $\mathbb{F}_3$. Therefore it has the same rank as

$$T = \begin{pmatrix} A & B \\ 0 & A \end{pmatrix} \in M_{702}(\mathbb{F}_3). \tag{30}$$

Direct calculation gives $\operatorname{rank} T = 195$. The repository's rank checker reproduces this calculation from the printed sign rows and the tripling formula. It takes 195 selected columns U of T, constructs a matrix V and a left inverse L, and verifies $T = UV$ and $LU = I_{195}$ over $\mathbb{F}_3$, proving both rank bounds. The certificate records the selected column indices and factor hashes; the specified elimination algorithm regenerates the factors. The largest matrix in this calculation has order 702.

The resulting real matrix is $H^{(3)} = \rho(N_3)(I_{351} \otimes P)$. Its right factor is invertible modulo 3, and the preceding decomposition of the scalar action therefore gives

$$\operatorname{rank}_{\mathbb{F}_3} H^{(3)} = 1262 \operatorname{rank}_{\mathbb{F}_3} T = 1262 \cdot 195 = 246090.$$

A *skew Hadamard matrix* K of order h satisfies $K + K^{\mathsf{T}} = 2I_h$ as well as $KK^{\mathsf{T}} = hI_h$. When $3 \mid h$, the latter identity implies $\operatorname{rank}_{\mathbb{F}_3} K \le h/2$ by the same isotropic-space argument used above. The first identity gives the reverse bound:

$$h = \operatorname{rank}_{\mathbb{F}_3}(2I_h) = \operatorname{rank}_{\mathbb{F}_3}(K + K^{\mathsf{T}}) \le 2 \operatorname{rank}_{\mathbb{F}_3} K.$$

Thus its rank is $h/2$. The Paley I matrix displayed above becomes skew after changing the signs of all rows other than the first. Indeed its first off-diagonal row and column then cancel in the sum with its transpose, and its lower-right block has diagonal 1 and skew off-diagonal part. With $h = 885924$ this gives rank 442962. The two ranks differ, proving the assertion. □

Thus our matrix is inequivalent to every skew Hadamard matrix of this order, including the standard Paley matrix. Other previously known equivalence classes may exist. At the other thirty-six known orders, equivalence with earlier matrices remains unsettled.

H Formal verification and reproducibility

H.1 Running the verification programs

The repository [1] contains the current construction programs and a frozen portable Lean package. The following commands use the source snapshot tagged `hexagon-2611.01070-v4-code`. Obtain that snapshot with

```
git clone --branch hexagon-2611.01070-v4-code \
  https://github.com/sashakolpakov/butson_towers.git
cd butson_towers
```

Then use Python 3.11 or later for the repository programs.

Finite inputs and current constructions. The quickest check uses only Python's standard library:

```
python3 scripts/verify_manuscript_data.py
```

It reconstructs the printed finite inputs and reports `"all_checks_passed": true`. Its checks include the source correlations, the strong starter identities, the paired-design inputs and the six smaller first Spence expansions. It needs no external data or network connection once the source file has been obtained.

For the reconstruction programs, create an environment and install the repository's runtime dependencies, NumPy and SymPy:

```
python3 -m venv .venv
. .venv/bin/activate
python -m pip install -e .
python -m experiments.scalar_lift.extended_family_inventory
python -m experiments.scalar_lift.paired_completed_orders
python -m experiments.scalar_lift.extended_spence_families \
  --output /tmp/extended-spence.json
```

The inventory check reports 86 distinct orders, comprising 49 new and 37 known orders, and 17 listed families. The paired-design command checks all fifteen inputs and transfers. The Spence command reconstructs the eight added starters, verifies their core identities and six first expansions, and writes a new certificate. For the two larger parameters, the first-step coefficient rows are not computed. The source and block identities checked here prove the high-order Gram identities without forming the dense final Hadamard matrices. Installing dependencies may require network access; the checks themselves use local data.

The portable Lean package. The archive is in `release/additional_source_verification/`, with filename `butson-towers-additional-sources.zip`. Its SHA256 is

`6ff9f98c20fa577dcb9c756e0c904d85b4c57c23f62238450cd3fe7e0f69f1e5`.

For the full proof build, Git and elan must also be installed. From the repository root, extract the archive into a fresh directory and run:

```
cd release/additional_source_verification
python3 -m zipfile -e butson-towers-additional-sources.zip \
  /tmp/butson-lean
cd /tmp/butson-lean/butson-towers-additional-sources
python3 verify.py --check-only
elan toolchain install leanprover/lean4:v4.32.0
python3 verify.py --report /tmp/butson-lean-report.json
```

The extracted package also works without the rest of the repository. The first check requires only Python 3.10 or later: it verifies the payload hashes, import closure and agreement of the public data with the Lean literals. It reports `success: true` and `kernel_checked: false`; this is not a proof compilation.

Full verification requires Git and elan/Lake with `leanprover/lean4:v4.32.0`. It builds the project proofs and runs the three axiom audits, reporting 143 checked statements, including 48 additional-source statements. The pinned dependencies and their compiled caches are downloaded on the first run. Matching local dependency checkouts can instead be supplied with `-cache-dir /path/to/.lake/packages`; the verifier checks their revisions before using them. The package's own proof modules are built from source even when dependency caches are reused. From an initialized repository checkout, `./scripts/check_formal.sh` performs the corresponding build and audits directly.

This frozen package proves the original 34 finite existence statements and nine families. The current repository supplies exact source and construction checks for the later paired constructions and eight added Spence families. Their existence proofs are given in the main text; these extensions are outside the frozen Lean package's scope. The next subsection lists the formal statements and their assumptions.

H.2 Verification and availability

The proofs use the printed finite inputs, the matrix identities proved above and the cited paired-transfer theorem. The programs printed here or supplied in the public repository repeat the finite integer calculations. Even at order 291145924, the recurrence and block Gram calculation prove orthogonality and sign entries without storing the full matrix or checking its rows one by one.

The public repository [1] contains the integer checker `scripts/verify_manuscript_data.py`, reconstruction programs, finite data, literature comparisons and independent verification programs. All paths in this subsection are relative to the repository root. For the saved order-7572 matrix, a separate integer calculation checked all $\binom{7572}{2} = 28\,663\,806$ distinct row pairs and found zero inner products. The matrix and its hashes are in `artifacts/hadamard-7572/`. The existence proofs depend only on direct verification of the fixed functions, not on the search that found them.

The formal development uses Lean 4.32.0. Its pinned mathlib revision is

`81a5d257c8e410db227a6665ed08f64fea08e997`.

It proves the original thirty-four existence statements and nine families for every nonnegative integer parameter, from explicit finite witnesses. The finite inputs include T127 and T631, 27 Williamson quadruples, twelve additional symmetric amicable quadruples, eight strong starters and the order-13 pair. The proofs establish the Gram identities and sign entries.

The fifteen paired-design orders are proved in Section F.1 and independently checked by exact computation. The six later finite Spence examples and eight additional families follow from the finite calculations and induction in Section D.1.5. These extensions have not been formalized in Lean. The formal proofs establish existence, not novelty in the literature. Proposition 12 also lies outside the Lean development; it uses the separate finite-field rank certificate. The Lean existence proof does not identify its matrix with the particular saved matrix, which has the independent integer verification described above.

The Lean development uses the reversal $u + v = 0$. Its convention lemmas recover the reversal $u + v = -1$ used here by simultaneous row and column translation by 316 modulo 631, or 64 modulo 127. It verifies the character matrices from their explicit integer rows; the general character-sum argument is proved separately above. The repository also records the correspondence between the manuscript and the formal statements.

The directory `release/additional_source_verification/` contains the Lean sources, pinned dependency versions and a program for reproducing the verification. The audit covers 143 selected statements: 85 original statements, ten rational sixth-root matrix identities and 48 additional source and recurrence statements. The sources compiled successfully after extraction into a fresh directory. Each audited statement uses only Lean's standard axioms `propext`, `Classical.choice` and `Quot.sound`; the audit lists these dependencies for each statement. The ten rational matrix identities assume the proved P, Q identities and $d \neq 0$; they do not formalize the particular cyclotomic field or Hermitian form. The repository gives instructions for repeating the build and axiom check and preserves the earlier proof and construction records unchanged.

References

[1] A. Kolpakov, *Butson Towers: source code, finite data and verification*, source snapshot `hexagon-2611.01070-v4-code`, 2026. `https://github.com/sashakolpakov/butson_towers/tree/hexagon-2611.01070-v4-code`.

[2] R. E. A. C. Paley, *On Orthogonal Matrices*, J. Math. Phys. 12 (1933), 311–320. `https://doi.org/10.1002/sapm1933121311`.

[3] J. Cooper and J. Wallis, *A construction for Hadamard arrays*, Bull. Austral. Math. Soc. 7 (1972), 269–277. `https://doi.org/10.1017/S0004972700045019`.

[4] The SageMath Developers, *Williamson-type quadruples, small cases*, `hadamard_matrix.py`, commit `8de8dad7`, 14 November 2026. `https://github.com/sagemath/sage/blob/8de8dad7bcb38e1baa43508cbe944bf04a2d0401/src/sage/combinat/matrices/hadamard_matrix.py`.

[5] H. Kharaghani, A. Mohammadian, B. Tayfeh-Rezaie and V. Zaitsev, *A Search for Hadamard Matrices of Near-Williamson Type*, arXiv:2605.08661v2, 6 September 2026. `https://arxiv.org/abs/2605.08661v2`. Literal data: `https://www.cs.uleth.ca/~zaitsevv/nearwilliamson.html`.

[6] C. Bright, I. S. Kotsireas and V. Ganesh, *Enumeration of Williamson sequences divisible by 2 or 3*, version 2, Zenodo, 2018, file `williamson-69.txt`. `https://zenodo.org/records/1195693/files/williamson-69.txt`.

[7] E. Spence, *An infinite family of Williamson matrices*, J. Austral. Math. Soc. Ser. A 24 (1977), 252–256, Theorem 4. `https://doi.org/10.1017/S1446788700020255`.

[8] J. Seberry and N. A. Balonin, *Two infinite families of symmetric Hadamard matrices*, Australas. J. Combin. 69(3) (2017), 349–357, Theorem 2 and Lemma 1. `https://ajc.maths.uq.edu.au/pdf/69/ajc_v69_p349.pdf`.

[9] Claude, *Hadamard matrices of orders 668, 716, 892, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948 and 1964*, HexagonMath 2611.00637v1, November 2026; primary source consulted 28 November 2026. https://hexagonmath.org/2611.00637v1.

[10] R. Egan and P. Ó Catháin, *Morphisms of Butson classes*, Linear Algebra Appl. 577 (2019), 78–93. https://doi.org/10.1016/j.laa.2019.04.020. https://arxiv.org/abs/1707.08815v3.

[11] R. Egan and P. Ó Catháin, *On complete morphisms of Butson Hadamard matrices*, J. Combin. Des., Early View, 2 November 2026, 1–7. https://doi.org/10.1002/jcd.70047. Preprint arXiv:2610.28394v1, 20 October 2026. https://arxiv.org/abs/2610.28394v1.

[12] P. Ó Catháin and E. Swartz, *Homomorphisms of matrix algebras and constructions of Butson-Hadamard matrices*, Discrete Math. 342(12) (2019), article 111606. https://doi.org/10.1016/j.disc.2019.111606. https://arxiv.org/abs/1904.10771v3.

[13] W. Bruzda, W. Tadej and K. Życzkowski, *Complex Hadamard Matrices catalogue*, sources P_7 and $M^{(0)}_{13A}$. The latter is attributed to R. Nicoară, A. LaClair, N. Geist and A. Wintenberg, May 2016. https://matrix-toolbox.github.io/chm/catalogue/1306B.html.

[14] B. Compton, R. Craigen and W. de Launey, *Unreal $BH(n,6)$'s and Hadamard matrices*, Des. Codes Cryptogr. 79 (2016), 219–229. https://doi.org/10.1007/s10623-015-0045-y.

[15] R. Egan, I. S. Kotsireas, S. London and P. Ó Catháin, *Recent progress in the construction of Hadamard matrices*, arXiv:2610.27175v2, revised 3 November 2026, Tables 3 and 5. https://arxiv.org/abs/2610.27175v2.

[16] *Hadamard Matrix Explorer: Unknown Orders*, 7001–8000 row, consulted 24 November 2026. https://www.math74.com/Hadamard/unknown.html.

[17] vatskishan03/Hadamard, *Unresolved orders*, FRONTIER.md, commit d885022144ba6bf4efa8315e14871a3736947527, 6 November 2026, consulted 24 November 2026. https://github.com/vatskishan03/Hadamard/blob/d885022144ba6bf4efa8315e14871a3736947527/FRONTIER.md.

[18] R. J. Turyn, *An infinite class of Williamson matrices*, J. Combin. Theory Ser. A 12 (1972), 319–321. https://doi.org/10.1016/0097-3165(72)90095-7.

[19] A. L. Whiteman, *An infinite family of Hadamard matrices of Williamson type*, J. Combin. Theory Ser. A 14 (1973), 334–340. https://doi.org/10.1016/0097-3165(73)90010-1.

[20] J. Seberry and M. Yamada, *On the products of Hadamard matrices, Williamson matrices and other orthogonal matrices using M-structures*, J. Combin. Math. Combin. Comput. 7 (1990), 97–137, Theorem 4. https://documents.uow.edu.au/~jennie/WEBPDF/139_1990.pdf.

[21] D. Ž. Đoković, O. Golubitsky and I. S. Kotsireas, *Some new orders of Hadamard and skew-Hadamard matrices*, J. Combin. Designs 22 (2014), 270–277, Section 3.3. https://doi.org/10.1002/jcd.21358. https://arxiv.org/abs/1301.3671v2.

[22] D. Ž. Đoković, *Hadamard matrices of small order and Yang conjecture*, arXiv:0912.5091, Sections 2–3. https://arxiv.org/abs/0912.5091.

[23] D. Best, D. Ž. Đoković, H. Kharaghani and H. Ramp, *Turyn-type sequences: Classification, Enumeration and Construction*, J. Combin. Designs 21 (2013), 24–35. https://doi.org/10.1002/jcd.21318. https://arxiv.org/abs/1206.4107.

[24] J. Kline, *A Hadamard matrix of order 4792*, version 0.1.0, 27 November 2026, Theorem 1. https://github.com/jeff-kline/hadamard-order-4792/blob/v0.1.0/paper/main.tex.

[25] J. Kline, *An infinite family of paired Hadamard matrices from Williamson-type matrices*, 2026, Appendix A. https://github.com/jeff-kline/hadamard-order-15896/blob/v0.1.0/paper/main.tex.

[26] T. Pender, *Balanced Group Matrices: Theory and Applications*, university-hosted work, 2020 PDF, printed p. 79 (PDF p. 94). https://www.ulethbridge.ca/sites/default/files/2020/12/pender_thesis.pdf.

[27] J. Seberry and M. Yamada, *Hadamard matrices, sequences, and block designs*, in J. H. Dinitz and D. R. Stinson (eds.), *Contemporary Design Theory: A Collection of Surveys*, Wiley, 1992, 431–560, Lemma 8.12. https://documents.uow.edu.au/~jennie/WEBPDF/175_1992.pdf.