Butson towers and high-rank Hadamard matrices

Alexander Kolpakov

25 November 2026

Abstract

We construct eighteen new real Hadamard matrices of ranks 7572, 17668, 22716, 32812, 42908, 58052, 73196, 78244, 93388, 98436, 108532, 128724, 153964, 229684, 295308, 386172, 4772884 and 13001124, and six new infinite families. The constructions preserve orthogonality and ensure that every final entry is 1 or -1. Explicit recipes and reproducible formal proofs establish every listed rank and every member of the six families.

hexagon:2611.01070v1

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. We use rank and order accordingly. Throughout the paper, "new" means new to the best of the author's knowledge. Known individual orders in the infinite families are identified in Section 10.

Theorem 1. *Real Hadamard matrices exist at each of the eighteen ranks listed in the abstract, and at every rank in the following six families:*

$$17668 \cdot 13^r, \qquad 22716 \cdot 17^r, \qquad 32812 \cdot 3^r,$$
$$78244 \cdot 61^r, \qquad 128724 \cdot 101^r, \qquad 153964 \cdot 121^r \qquad (r \in \mathbb{Z}_{\geq 0}).$$

Here are the conventions used in the proof. A bar denotes complex conjugation, and $A^* = \overline{A}^{\mathsf{T}}$ is the conjugate transpose of a matrix. A square complex matrix of order n is *flat* in this paper 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*; the equality $w = n$ is a separate assertion. 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 with a proved Gram identity, starting with a Butson matrix or one of the explicitly defined weighted sources below. At each step the scalar action, involution and trace form are retained. A single restriction is allowed. Flatness is required only of the final matrix, and is proved from its entries. This terminology does not assert priority for restriction of scalars or Butson morphisms. Our immediate starting reference was Egan and Ó Catháin's recent work [6]; see also the earlier constructions [5, 7, 9].

The new finite ingredient is a vector-valued function on $\mathbb{F}_{631}$ with the correlation identity proved in Section 2. It gives both a sixth-root scalar action and four matrices that allow substitution of commuting sign matrices. The same construction on $\mathbb{F}_{127}$ gives periodic T-matrices of order 127. Five infinite families use Spence's classical recurrence for the *source* matrices; we call the resulting five real output families our Spence families. The sixth uses the classical tripling construction for an explicitly specified sixth-root source. All finite initial data and all recurrence identities needed here are given below.

2 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

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

The four integer-valued coordinate functions of b are denoted b_0, b_1, b_2, b_3: explicitly, $b(x) = \sum_{j=0}^{3} b_j(x) e_j$.

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; trial division by the primes at most their square roots proves this, and the integer check in the appendix 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 list one representative r from each set and the value $b(r)$; the separate row $r = 0$ specifies $b(0)$. They give every value of b through the rule

$$b(\mu^k r) = \Pi^k b(r) \quad (0 \le k < m), \qquad b(0) = e_0. \tag{1}$$

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

$$c(s) = \sum_{x \in \mathbb{F}_p} b(x)^{\mathsf{T}} b(x+s) = \sum_{j=0}^{3} \sum_{x \in \mathbb{F}_p} b_j(x) b_j(x+s). \tag{2}$$

Substituting $x = \mu y$ and using (1) 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 $c(s) = P_s - N_s$. Here is the complete calculation on shift orbits:

$p = 631:\ s$	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

$$c(s) = p\delta_{s,0} \qquad (s \in \mathbb{F}_p). \tag{3}$$

The appendix gives an integer program containing the complete input and checking every summand, every residue and every shift. In particular the finite arithmetic here does not depend on a saved matrix or an external search result.

3 Circulants and the four-matrix construction

3.1 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

$$(L_f L_f^{\mathsf{T}})_{u,v} = \sum_{x \in G} f(x)f(x+v-u). \tag{4}$$

To obtain this formula from the matrix product, one can substitute $x = t - v$ and then 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 saved length-p constructions we take $G = \mathbb{F}_p$ additively and $t = -1$, so the literal convention is $\mathcal{J}_{u,v} = 1$ 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

$$\mathrm{GS}(f) = \begin{pmatrix} A & B\mathcal{J} & C\mathcal{J} & D\mathcal{J} \\ -B\mathcal{J} & A & -D^{\mathsf{T}}\mathcal{J} & C^{\mathsf{T}}\mathcal{J} \\ -C\mathcal{J} & D^{\mathsf{T}}\mathcal{J} & A & -B^{\mathsf{T}}\mathcal{J} \\ -D\mathcal{J} & -C^{\mathsf{T}}\mathcal{J} & B^{\mathsf{T}}\mathcal{J} & A \end{pmatrix}. \tag{5}$$

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 $N = AA^{\mathsf{T}} + BB^{\mathsf{T}} + CC^{\mathsf{T}} + DD^{\mathsf{T}}$. For completeness its six upper off-diagonal blocks, in row order, are

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

All six vanish; the lower blocks are their transposes. We have proved

$$\mathrm{GS}(f)\,\mathrm{GS}(f)^{\mathsf{T}} = I_4 \otimes \sum_{j=0}^{3} L_{f_j} L_{f_j}^{\mathsf{T}}. \tag{6}$$

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, equations (4) and (3) 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 the *periodic T-matrices* used in this paper. In particular they prove the asserted T-matrix existence for both $p = 631$ and $p = 127$.

3.2 Four coefficient matrices with disjoint supports

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

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

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 $M(x)^{\mathsf{T}}M(x) = (\sum_j x_j^2)I_4$. 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 (6), 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

$$X_j X_j^{\mathsf{T}} = pI_{4p}, \qquad X_i X_j^{\mathsf{T}} + X_j X_i^{\mathsf{T}} = 0 \quad (i \neq j). \tag{7}$$

There is also an entrywise property that does not follow merely from these 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 (5), 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. This proves the required disjoint-support assertion as well as the fact that their supports cover all matrix positions.

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 $pI_{4p} \otimes \sum_j A_j A_j^{\mathsf{T}} = 4pwI_{4pw}$. The Gram scale equals the displayed order, as required. □

3.3 The same construction as restriction of scalars

The Williamson and Spence source matrices used below are circulants on finite abelian groups. Here is the exact algebra, basis, involution and trace in their scalar interpretation. 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

$$\rho(a)_{u,v} = a_{v-u}, \quad \rho(ab) = \rho(a)\rho(b), \quad \rho(a^*) = \rho(a)^{\mathsf{T}}. \tag{8}$$

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 this declared basis is exactly I_w. No unmentioned change of basis or rescaling is used.

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

$$f_i f_j^* = f_j f_i^*, \qquad \sum_{j=0}^{3} f_j f_j^* = 4wc_0, \qquad a_j(g) \in \{1, -1\}.$$

The matrix $S = \sum_j X_j f_j$ has order $4p$ over $\mathbb{Q}[G]$. By (7), precisely the same paired-term calculation as 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 order is $4p$, its Gram scale is $4pw$, the scalar dimension is w, the trace metric is I_w, and its actual entries have just been specified. These are distinct pieces of the construction. For symmetric commuting sign circulants $A_j = L_{a_j}$ satisfying $\sum_j A_j A_j^{\mathsf{T}} = 4wI_w$, their multiplication and transpose identities show, by faithfulness of ρ, exactly the three hypotheses on f_j above.

4 Two sign matrices for sixth-root scalars

For this section 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 (3) 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 (5) gives $\mathrm{GS}(a+tb) = U + tV$. Equation (6), 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

$$\begin{aligned} PP^{\mathsf{T}} = QQ^{\mathsf{T}} &= UU^{\mathsf{T}} + VV^{\mathsf{T}} = 4pI_d = dI_d, \\ PQ^{\mathsf{T}} + QP^{\mathsf{T}} &= 2(UU^{\mathsf{T}} - VV^{\mathsf{T}}) = 4pI_d = dI_d. \end{aligned} \tag{9}$$

These are the three precise properties of P, Q needed for the scalar action. Their construction specifies every entry as an integer sign.

5 Restriction of scalars and the final entry condition

We also use $N^* = \overline{N}^{\mathsf{T}}$ when the entries lie in an algebra equipped with an involution $z \mapsto \bar{z}$. 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 3 (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

$$\rho(z)^{\mathsf{T}} G = G\rho(\bar{z}), \qquad \rho(\bar{z})G^{-1} = G^{-1}\rho(z)^{\mathsf{T}}. \tag{10}$$

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

$$X(I_n \otimes G^{-1})X^{\mathsf{T}} = w(I_n \otimes G^{-1}). \tag{11}$$

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

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

Taking x and y to be coordinate basis vectors proves the first identity in (10). 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 (11).

The definition of multiplication 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 (11) 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 $x \mapsto zx$ when evaluated 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 $N^*N = wI$. This column form of the initial identity permits transfer of a Hermitian form at each step. If an intermediate step carries a nonidentity form, its entire matrix is transferred. 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. Every displayed formula for the transferred form is linear in the trace. These rules retain the full form through the Butson towers defined in the introduction.

The next lemma states the additional entry condition that we use at the last step. It permits an arbitrary rational representation, including a direct sum of several copies of the regular representation above.

Lemma 4 (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 $NN^* = wI_n$, 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. □

In particular, for every scalar z that actually occurs in N, the final entry condition is the finite collection of 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 $t^2-1 = (t-1)(t+1)$. This gives explicit polynomial conditions for final flatness after restriction of scalars.

6 The sixth-root action furnished by the length-631 construction

Keep the sign matrices P, Q of order $d = 2524$ obtained above. They satisfy (9). 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

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

Every entry is rational, explicitly

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

This formula is also an exact recipe for every entry of the scalar action; it requires only the two previously defined sign matrices.

Lemma 5. *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 (9), we obtain

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

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,

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

□

For clarity, the field extension here has degree 2, whereas 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 $\dim_K \mathbb{Q}^d = 1262$.

The trace metric can also be given directly in these actual 2524 rational coordinates. Put $S = 2R - I_d$. The proved identities 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

$$h(u, v) = \frac{u^{\mathsf{T}}v}{2} - \frac{u^{\mathsf{T}}Sv}{6}\,\xi. \tag{12}$$

This is a Hermitian form over K, conjugate linear in its first argument and linear in its second argument. Here are the required checks. The skew symmetry of S gives $h(v, u) = \overline{h(u, v)}$. If $s = u^{\mathsf{T}}v$ and $t = u^{\mathsf{T}}Sv$, 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 $u^{\mathsf{T}}Su = 0$, 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 $MM^* = 3I_3$. Its two entries have the sign matrix images

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

Lemma 4, with $F = P$ and $c = d$, therefore gives

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

One can check this last Gram directly as well: 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

$$1, \quad \zeta, \quad -1, \quad -\zeta \tag{13}$$

has a sign matrix image after multiplication by P, namely $P, Q, -P, -Q$, respectively. Any matrix N of order n with entries in (13) and $NN^* = nI_n$ therefore gives a real Hadamard matrix of order $2524n$ by the block formula $H_{ij} = \rho(N_{ij})P$. These statements concern exactly the four specified scalars. For example, the remaining sixth root ζ^2 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.

7 An explicit cubic family

We now prove the existence of matrices of every order $32812 \cdot 3^r$, for all integers $r \geq 0$. The source recurrence is the classical sixth-root tripling construction [9]. Both its finite starting point and its induction step are given here.

Lemma 6 (The starting pair of order 13)**.** *There are sign matrices A_0, B_0 of order 13 satisfying*

$$A_0B_0^{\mathsf{T}} = B_0A_0^{\mathsf{T}}, \qquad A_0A_0^{\mathsf{T}} + 3B_0B_0^{\mathsf{T}} = 52I_{13}. \tag{14}$$

Proof. Table 1 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 [8]. The existence proof here uses only the displayed integer entries. For the last column, let L be the symmetric matrix with zero diagonal whose entries above the diagonal are 1 at the listed indices and 0 at the unlisted indices.

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

To record the entire calculation 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

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

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

$$A_0 A_0^{\mathsf{T}} = 16 I_{13} - 3 J_{13} + 12 E, \tag{15}$$

$$B_0 B_0^{\mathsf{T}} = 12 I_{13} + J_{13} - 4 E, \tag{16}$$

$$A_0 B_0^{\mathsf{T}} = J_{13} - 12 e_0 e_0^{\mathsf{T}} - 4 L. \tag{17}$$

All entries in these identities are specified by the table. The exact rule for performing every check is

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

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 right side has off-diagonal entry -3 precisely at the pairs listed in the last column of the table, and 1 at all other pairs. These statements enumerate all row products. In particular (17) is symmetric. Adding (15) and three times (16) cancels both E and J_{13} and leaves $(16 + 36) I_{13} = 52 I_{13}$. This proves (14).

For a short independent way to repeat the finite calculation, let `A` and `B` be the two arrays of integer rows printed in the table. The following loop uses only integer addition and multiplication and checks all 169 entries of both required 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 7 (The tripling step)**.** *Suppose that A, B are sign matrices of order n satisfying*

$$A B^{\mathsf{T}} = B A^{\mathsf{T}}, \qquad A A^{\mathsf{T}} + 3 B B^{\mathsf{T}} = 4 n I_n. \tag{18}$$

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

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

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

$$A' B'^{\mathsf{T}} = B A^{\mathsf{T}} \otimes J_3 + B B^{\mathsf{T}} \otimes J_3 C^{\mathsf{T}} = B A^{\mathsf{T}} \otimes J_3,$$

$$B' A'^{\mathsf{T}} = A B^{\mathsf{T}} \otimes J_3 + B B^{\mathsf{T}} \otimes C J_3 = A B^{\mathsf{T}} \otimes J_3.$$

They are equal by (18). 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 literal pair A_0, B_0 in Table 1, apply Lemma 7 r times, and call the result A_r, B_r. Induction gives sign matrices of order $n_r = 13 \cdot 3^r$ with

$$A_r B_r^{\mathsf{T}} = B_r A_r^{\mathsf{T}}, \qquad A_r A_r^{\mathsf{T}} + 3B_r B_r^{\mathsf{T}} = 4n_r I_{n_r} \qquad (r \geq 0).$$

These equations also give an alternative, entirely real final step. The quadruple (A_r, B_r, B_r, B_r) satisfies the hypotheses of Proposition 2: its norm is the displayed weighted norm, its distinct mixed products are either the proved equality $A_r B_r^{\mathsf{T}} = B_r A_r^{\mathsf{T}}$ or an equality with both sides $B_r B_r^{\mathsf{T}}$. 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 $2524n_r = 32812 \cdot 3^r$. This is the recurrence-to-endpoint route used in the Lean existence proof. The following sixth-root description gives the scalar viewpoint directly; it proves the same existence statement without asserting that the two displayed representatives are equal.

The equations for A_r, B_r give the sixth-root source as follows. 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

$$\begin{aligned} W_r W_r^* &= \frac{1}{4}\left(A_r A_r^{\mathsf{T}} + 3B_r B_r^{\mathsf{T}} + \xi(B_r A_r^{\mathsf{T}} - A_r B_r^{\mathsf{T}})\right) \\ &= n_r I_{n_r}. \end{aligned}$$

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 (13). Multiplication by ζ^{-1} has absolute value 1, so $N_r N_r^* = n_r I_{n_r}$ as well. Finally the explicit 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

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

This proves the sixth infinite family for every $r \geq 0$, and gives the individual orders 32812, 98436 and 295308 at $r = 0, 1, 2$.

8 Thirteen finite commuting quadruples

We now take $p = 631$. A Williamson quadruple of order w means here 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 following thirteen quadruples are taken from the explicit small-order Sage table [3]. They are known sources; the new orders result from combining them with the length-631 construction.

For each order w, the following table gives the four first rows of the 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 3. 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 (4). The zero-shift value follows by counting the $4w$ squared signs. All nonzero-shift sums are 0 for every one of the thirteen rows of orders in the table. The complete finite arithmetic is the following loop, where `W[w]` is the tuple of 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)
```

Every loop index and every input in this check has been specified above. The complete standalone file in the ancillary material contains the literal assignment as well as the check. Thus the thirteen quadruples give the

following thirteen ranks:

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 rank 7572 given here prove the same existence statement; they need not produce equivalent matrices.

9 Five infinite families from Spence's recurrence

We use the classical recurrence in Spence's Theorem 4 [4]. We specify five initial quadruples explicitly, prove that they meet its hypotheses, and combine the resulting sources with the length-631 construction to obtain the five families below.

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

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

We first specify four symmetric, pairwise commuting sign matrices D_0, E_0, F_0, G_0 of order w_0 and prove the two identities

$$(D_0 - E_0)^2 + (F_0 - G_0)^2 = 4I_{w_0}, \qquad (D_0 + E_0)^2 + (F_0 + G_0)^2 = 4qI_{w_0}. \tag{19}$$

Both identities are required. The weaker condition that the sum of the four squares is $4w_0 I_{w_0}$ would not suffice for the induction.

9.1 The initial matrices

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

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

All row arguments in this subsection are reduced modulo w. The following 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 $0, 1, \ldots, w_0 - 1$, in that order.

q	row	entries
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	-+-+--+-+++-+-+++++-+-+-+++++-+-+++-+--+-+
121	d	++-+-++-+-+-++++-+---+---+---+---+-++++-+-+-++-+-+
121	e	++-+-++-+-+-++++-+---+---+---+---+-++++-+-+-++-+-+
121	f	+--+-+-++++--++-+-++-+--++++++--+-+-++-+-++--++++-+-+--
121	g	--+-+-++++--++-+-++-+--++++++--+-++-+-++--++++-+-+--

Every printed entry is a sign, and each row satisfies $h(-x) = h(x)$. Consequently every initial matrix is symmetric. To check commutativity without any spectral assumptions, for arbitrary rows h, k observe that

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

Replacing t by $j-i-t$ interchanges h and k. Thus any two circulant matrices of this order commute.

In each of the five 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 (19). 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 complete finite sums from the displayed rows are

q	w_0	$c(0)$	$(c(1),\dots,c(w_0-1))$
13	7	13	$(0,\dots,0)$
17	9	17	$(0,\dots,0)$
61	31	61	$(0,\dots,0)$
101	51	101	$(0,\dots,0)$
121	61	121	$(0,\dots,0)$

Here the rightmost vector has exactly w_0-1 entries. For completeness, the following complete integer check reproduces these finite equalities, and checks the signs, symmetry and the difference rows at the same time. Its input consists precisely of the five quadruples of sign words printed above; the literal assignment is included to make the check independent of any external data file.

```
starters = {
    13: (
        '+-++++-',
        '+-++++-',
        '+--++--',
        '---++--',
    ),
    17: (
        '+--++++--',
        '+--++++--',
        '+-+----+-',
        '--+----+-',
    ),
    61: (
        '++++++-+--+---++++---+--+-+++++',
        '-+++++-+--+---++++---+--+-+++++',
        '+--++---+-+-++----++-+-+---++--',
        '+--++---+-+-++----++-+-+---++--',
    ),
    101: (
        '+---+++-++-+-+++--+++++--++--+++++--+++-+-++-+++---',
        '----+++-++-+-+++--+++++--++--+++++--+++-+-++-+++---',
        '-+--+----+-+++-+-+++++--+--+--+++++-+-+++-+----+--+',
        '-+--+----+-+++-+-+++++--+--+--+++++-+-+++-+----+--+',
    ),
    121: (
        '++--+--++--+-+-++++--+-----+------+-----+--++++-+-+--++--+--+',
        '++--+--++--+-+-++++--+-----+------+-----+--++++-+-+--++--+--+',
        '+---+-+++++---++--+-++-+---++++++---+-++-+--++---++++-+-+---',
        '----+-+++++---++--+-++-+---++++++---+-++-+--++---++++-+-+---',
    ),
}
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)
```

There is no rounding in these sums. To see exactly why they prove the matrix identities, for any row h one has

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

The rows $d \pm e$ and $f \pm g$ are symmetric, so their circulants equal their transposes. The two checked correlation vectors therefore give (19), entry by entry. The same literal rows and finite integer equalities are checked independently by the Lean kernel in `Data/StrongStarters.lean`.

9.2 The character matrices used in the recurrence

We define a field $\mathbb{F}_q$ and a character matrix K_q for each of the five values of q. For $q = 13, 17, 61, 101$, 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. When numerical indices are needed, index $a + bu$ by the integer $a + 11b$. Subtraction of indices in the field means componentwise subtraction modulo 11, not subtraction modulo 121.

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 four 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+-+++-+--++-++-+++++++--++-+-++---+-+-+-+-+-+-+-+---++-+-++--+++++++-++-++--+-+++-+

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

$$\chi_{121}(a+bu) = \chi_{11}(a^2 - 2b^2), \tag{20}$$

where χ_{11} is given by the square list $1, 3, 4, 5, 9$. Here is a verification of that formula. 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 (20); both sides also vanish at zero.

We prove all the matrix identities needed in the recurrence:

$$K_q^{\mathsf{T}} = K_q, \qquad K_q^2 = qI_q - J_q, \qquad K_q J_q = J_q K_q = 0, \qquad J_q^2 = qJ_q. \tag{21}$$

The diagonal entries of K_q are zero, and all its off-diagonal entries are signs, directly 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 $5, 4, 11, 10$ for $q = 13, 17, 61, 101$, 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 $qI_q - J_q$. The already proved symmetry of K_q finishes (21).

9.3 The recursion and its proof

Keep q fixed. Starting with the four matrices already specified, 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

$$\begin{aligned} U' &= \tfrac{1}{2}(U - V) \otimes J_q + \tfrac{1}{2}(U + V) \otimes (K_q + I_q), \\ V' &= \tfrac{1}{2}(U - V) \otimes J_q + \tfrac{1}{2}(U + V) \otimes (K_q - I_q). \end{aligned} \tag{22}$$

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 (22) 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 next prove that all four matrices at every step are symmetric, pairwise commuting sign matrices and satisfy

$$\begin{aligned} M_r &:= (D_r - E_r)^2 + (F_r - G_r)^2 = 4q^r I_{w_r}, \\ N_r &:= (D_r + E_r)^2 + (F_r + G_r)^2 = 4q^{r+1} I_{w_r}. \end{aligned} \tag{23}$$

The initial case was proved above. We verify every assertion at the inductive step.

For 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 this case as well. This proves that all four new matrices are sign matrices.

The transpose of a Kronecker product is the product of the transposes of its two factors. All factors in (22) are symmetric, so the new matrices are symmetric. For commutativity, use

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

Every first factor occurring in the four new matrices is a linear combination of the old four matrices, so these first factors commute by the induction hypothesis. Every second factor is a linear combination of I_q, J_q, K_q, which commute by (21). Hence any two Kronecker summands commute with each other, and expanding the products shows that the four new matrices commute pairwise.

For the norms, adding and subtracting the two equations in (22) 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 (21),

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

Applying these formulas to both pairs proves the exact recurrences

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

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 (23) and completes the induction.

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

$$\begin{aligned} D_r D_r^{\mathsf{T}} + E_r E_r^{\mathsf{T}} + F_r F_r^{\mathsf{T}} + G_r G_r^{\mathsf{T}} &= \tfrac{1}{2}(M_r + N_r) \\ &= 2(q+1)q^r I_{w_r} = 4w_r I_{w_r}. \end{aligned} \tag{24}$$

Moreover, any two of these matrices, say A, B, satisfy $AB^{\mathsf{T}} = AB = BA = BA^{\mathsf{T}}$, by symmetry and commutativity. These are exactly the norm and pairwise relations required by the four-matrix substitution proved earlier.

For clarity, the index set can be regarded as 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.

9.4 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. Recall the proved properties

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

and that 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 (24), 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 five orders are

q	w_0	$4pw_r$
13	7	$17668 \cdot 13^r$
17	9	$22716 \cdot 17^r$
61	31	$78244 \cdot 61^r$
101	51	$128724 \cdot 101^r$
121	61	$153964 \cdot 121^r$

$(r \geq 0)$.

Each matrix is nonsingular, since its Gram matrix is a positive multiple of the identity, so its rank equals its displayed order. This proof applies to every nonnegative integer r; it does not require constructing a dense matrix or checking a finite initial segment of the family.

10 Completion of the theorem and known members

Proof of Theorem 1. Section 8 gives thirteen of the stated ranks, listed there as $2524w$. Section 7 gives every rank $32812 \cdot 3^r$, including the additional rank 295308 at $r = 2$. Section 9 gives the other five infinite families. Their first expanded members for $q = 13, 17, 61, 101$, respectively, are

$$17668 \cdot 13 = 229684, \qquad 22716 \cdot 17 = 386172,$$

$$78244 \cdot 61 = 4772884, \qquad 128724 \cdot 101 = 13001124.$$

These are the four remaining finite ranks. This accounts for all eighteen distinct integers in the abstract and all six families. Every construction proves both sign entries and the Gram identity with scale equal to the order. Nonsingularity, and hence the stated rank, follows from the inverse formula in Section 1. □

Each of the six families has a new initial rank. This assertion does not mean that every rank occurring in a family was previously unknown. 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 give the short verification of these positive identifications, so neither primality nor a database status is being used without an exact test.

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 9 applies without change to give $KK^{\mathsf{T}} = tI_t - J_t$ and $KJ_t = J_t K = 0$. 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 [1]. 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 [1]. The value $t = 9314821$ gives order $2(t+1) = 18629644$. The appendix includes the finite trial divisions proving the primality of both parameters.

The length-127 construction gives a separate T-matrix result, not a new Hadamard order. For example, the order-3 quadruple in Section 8 and Proposition 2 give a Hadamard matrix of the known order $4 \cdot 127 \cdot 3 = 1524$. The dated survey [10], 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 [11, 12]. The individual known/new labels for the other finite orders, together with the prior constructions located, are recorded in the repository's dated order ledgers. No nonexistence conclusion is inferred from a failed search or from the absence of a located construction.

11 Verification and availability

The proofs above require only the printed finite inputs and the proved matrix identities. The finite computations are integer sums; they can be repeated by the included programs. In particular, no dense matrix of order 13001124 needs to be stored or checked row by row: the source recurrence, sign-entry proof and block Gram calculation apply at that order as at every other parameter value.

The public repository is `https://github.com/sashakolpakov/butson_towers`. Its ancillary material provides the integer checker `manuscript_data.py`, reconstruction programs, complete finite data, order-status ledgers and independent exact audits. For the saved order-7572 representative, a separate integer audit checked all $\binom{7572}{2} = 28\,663\,806$ distinct row pairs; their inner products are all zero. The archived matrix and its hashes are preserved in `artifacts/hadamard-7572/`. The search that produced the finite functions is not a premise of any existence proof here; the fixed functions are verified directly.

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

`81a5d257c8e410db227a6665ed08f64fea08e997`.

It proves the eighteen existence statements and all six families for every nonnegative integer parameter, starting from literal finite witnesses. Its finite inputs include T127 and T631, 27 Williamson quadruples (thirteen suffice here), the five strong starters, and the order-13 pair. Its construction proofs establish the exact Gram identities and final sign entries. Literature novelty is not a formal claim. The formal existence proof also does not assert equality with a particular saved packed representative; that representative has the independent audit just described.

The core Lean reversal uses $u + v = 0$. The checked convention lemmas identify the reversal $u + v = -1$ used here by simultaneous row and column translation by 316 modulo 631, or 64 modulo 127. The five character

matrices are checked in Lean from their literal integer rows; their general character-sum derivation above is a separate proof. A manuscript-to-code correspondence audit is included in the repository.

The original source-only reproducibility package is retained under `release/lean_verification/`; the verified mathematical proof snapshot is commit `686acf9`. The package supplies its dependency lock and an audit of 85 selected statements. A fresh extracted build passed, and the selected statements use only Lean's standard axioms `propext`, `Classical.choice` and `Quot.sound`, as listed individually in the audit record. A separate source-only supplement under `release/lean_sixth_root_pair/` checks the ten rational matrix identities for R, S and the scalar coordinates. It assumes precisely the proved P, Q identities and $d \neq 0$; it does not formalize the particular cyclotomic field or Hermitian-form realization. Instructions in the packages reproduce the build and axiom check. The manuscript and executable reconstruction have their own versioned release, so improvements to exposition do not alter the frozen construction or proof archives.

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

A Integer check for the two finite functions

Here is a complete standard-library Python check of (3), with all its finite inputs. In the input pairs (r, t), the nonzero integer t stands for $\mathrm{sign}(t)e_{|t|-1}$ at representative r. This is merely a numerical encoding of the two tables in Section 2. The variable `a` in the program 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 (2).

```
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 prove the precise multiplier orders. In the orbit loop, the assertion that no value has already been assigned checks disjointness of the listed orbits; the assertion after it checks coverage of all residues. The tuple formula implements Π^k explicitly. The final loop proves the required correlation for every shift, including zero, without using the orbit reduction of shifts.

For completeness the following trial-division function checks the two primes used to define the functions and the two primes used to identify known Paley orders in Section 10:

```
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 (127, 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 ancillary file `anc/manuscript_data.py` combines these checks with the thirteen quadruple checks, the five strong starter checks and the order-13 pair check.

References

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

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

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

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