hexagon:2611.00637v1

HADAMARD MATRICES OF ORDERS 668, 716, 892, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948 AND 1964

CLAUDE

Abstract. We construct Hadamard matrices of orders 668, 716, 892, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948 and 1964, the twelve multiples of 4 below 2000 for which none was known, and a second, inequivalent matrix of order 668. Five come from the Goethals–Seidel array with circulant blocks invariant under a multiplier group, four from the width-4 bordered array of Wallis and Whiteman, and four from bordered Goethals–Seidel arrays of widths 12, 20 and 28 whose corner is itself a Hadamard matrix. To our knowledge borders wider than 4 with a Hadamard corner are new; the first two arrays are classical. The four matrices with a border of width 4, of orders 668, 716, 1676 and 1772, are instances of a theorem of Miyamoto on Hadamard matrices of order $8m + 4$, which Seberry and Yamada restated with their M-structures; the matrices to which the theorem applies were found here by computer search. The searches differ greatly in size. Those for the wider borders formed at most about 2^{44} pairs of candidate blocks. Those for orders 716 and 668 with a border of width 4, made with no multiplier group, formed about 2^{66} and 2^{59}, and these two matrices, that of order 716 above all, are results of large-scale computation more than of a new construction. With these matrices, a Hadamard matrix of order n is known for every $n \equiv 0 \pmod 4$ with $n \leq 2000$.

1. Introduction

1.1. **The result.** A *Hadamard matrix* of order n is an $n \times n$ matrix H with entries ± 1 and $HH^{\mathsf{T}} = nI_n$ [31]. The Hadamard conjecture, usually attributed to Paley [59], is that one exists for every n divisible by 4. By 2014 the multiples of 4 up to 2000 for which none was known were $4v$ for the twelve primes $v = 167$, 179, 223, 283, 311, 347, 359, 419, 443, 479, 487, 491 [7, 12, 20, 58, 65, 67].[1] The list has not changed since then [7, 19]. Its smallest member, 668, had been the least order in doubt since Kharaghani and Tayfeh-Rezaie constructed order 428 in 2004 [36]. It was the subject of recent partial results [24, 60] and of a conjecture that would give a matrix of this order through a Legendre pair of length 333 [38, Conj. 1] (§7). We give a Hadamard matrix of each of the twelve orders, and a second, inequivalent one of order 668, labelled $668'$ below (Table 1).

Theorem 1 (Twelve new orders)**.** *Hadamard matrices of orders* 668*,* 716*,* 892*,* 1132*,* 1244*,* 1388*,* 1436*,* 1676*,* 1772*,* 1916*,* 1948 *and* 1964 *exist.*

The proof is a finite verification: Tables A1–A2 determine one matrix of each order explicitly, through (1), Proposition 2 and Theorem 5, and [83] gives them in machine-readable form (§6). The printed matrices differ from the files released publicly earlier [1] only in the conventions stated in §6.2, except that $668'$ is not among those files. Consequently a Hadamard matrix of order n is known for every $n \equiv 0 \pmod 4$ with $n \leq 2000$. Egan, Kotsireas, London and Ó Catháin [23] have analysed the structure of the twelve released matrices, working from the matrices alone. Their paper is also a survey of how Hadamard matrices are constructed and of the orders each method reaches, a far broader landscape than the present one; it counts 95 orders up to 10 000 as still open when it appeared, the least being $2396 = 4 \cdot 599$. Readers who want the context in which the twelve orders sit should start there.

Date: November 2026.

2020 *Mathematics Subject Classification.* Primary 05B20; Secondary 05B10, 05-08, 05-11.

Key words and phrases. Hadamard matrix, supplementary difference sets, divisible difference family, Goethals–Seidel array, bordered array, multiplier group, compression of sequences, meet-in-the-middle search, Miyamoto's construction, M-structures, T-matrices.

Preprint; not yet peer-reviewed.

[1] See §7 on a construction method that may bear on orders 892, 1132 and 1948.

1.2. **The main idea.** Let G be a finite abelian group and let $a_1, \dots, a_4 \colon G \to \{\pm 1\}$ be four functions, the *blocks*. Write $\mathrm{PSD}(\chi) = \sum_f |\hat{a}_f(\chi)|^2$ for their total power spectrum, where $\hat{a}$ is the discrete Fourier transform on G and the characters χ are the frequencies (§1.5). The Goethals–Seidel array K of §2 is a ± 1 matrix of order $4|G|$ with $KK^{\mathsf{T}} = I_4 \otimes \sum_f A_f A_f^{\mathsf{T}}$, where $A_f = (a_f(y-x))_{x,y}$ is the group matrix of a_f, the G-circulant matrix it generates, and the eigenvalues of $\sum_f A_f A_f^{\mathsf{T}}$ are the numbers $\mathrm{PSD}(\chi)$. So K is a Hadamard matrix exactly when the spectrum is flat: $\mathrm{PSD}(\chi) = 4|G|$ for every character χ.

All twelve orders are $n = 4v$ with v prime, and the standard method takes $G = \mathbb{Z}_v$. A group of prime order has no proper non-trivial subgroup, hence no quotient to work through, and the structure the standard method imposes is invariance of each a_f under a group M of multipliers (maps $x \mapsto hx$ of $\mathbb{Z}_v$), of odd order $t > 1$ dividing $v - 1$. Invariance forces every row sum $r_f = \sum_x a_f(x)$ to be $\equiv \pm 1 \pmod{2t}$, because the non-zero elements fall into $(v-1)/t$ orbits of size t, an even number of them, and flatness at the trivial character forces $r_1^2 + \cdots + r_4^2 = 4v$. For five of the twelve primes the two demands are compatible for some t, and the known method succeeds (§5.1).

For the other seven primes no row sums suitable for that method exist, and we use bordered Goethals–Seidel arrays: a Goethals–Seidel array over an abelian group G of order slightly less than v, surrounded by a border of b rows and columns, its *width* (Figure 1). We call its four blocks the *core*. Unlike v, the order $|G| = v - b/4$ can have several small factors (§5).

	b	$4\lvert G\rvert$			
b	C	$E^{(1)}$	$E^{(2)}$	$E^{(3)}$	$E^{(4)}$
	$D^{(1)}$	A_1	A_2R	A_3R	A_4R
	$D^{(2)}$	$-A_2R$	A_1	$A_4^{\mathsf{T}}R$	$-A_3^{\mathsf{T}}R$
$4\lvert G\rvert$	$D^{(3)}$	$-A_3R$	$-A_4^{\mathsf{T}}R$	A_1	$A_2^{\mathsf{T}}R$
	$D^{(4)}$	$-A_4R$	$A_3^{\mathsf{T}}R$	$-A_2^{\mathsf{T}}R$	A_1

$$\big(+^k\,-^k\,+^k\,-^k \;\big|\; +^k\,-^k\,+^k\,-^k \;\big|\; -^k\,-^k\,+^k\,+^k \;\big|\; -^k\,+^k\,+^k\,-^k\big)$$

FIGURE 1. The bordered array H. Each row of E and each column of D has four segments, constant on the cosets of N and summing to zero. Below: the first row of E for $q = 4$ with the frame of Table 2; $\pm^k$ is k equal signs, $k = 41$ for order $668'$.

A border can repair a spectrum that is flat except at a few characters. Let N be a subgroup of G of even index q, take $b = 4(q-1)$, so that $|G| = v - (q-1)$, and ask that $\mathrm{PSD}(\chi) = n$ at every character except the $q-1$ non-trivial characters of the quotient $Q = G/N$. If PSD has a common value at those, Parseval's identity forces that value to be b. (Parseval gives $\sum_\chi \mathrm{PSD}(\chi) = 4|G|^2$; with the value $n = 4|G| + b$ at the other $|G| - q + 1$ characters, a common value c at these $q-1$ must satisfy $(q-1)(n-c) = |G|\,b = 4(q-1)|G|$, that is, $c = n - 4|G| = b$.) Then $nI - KK^{\mathsf{T}}$ is $4|G|$ times the orthogonal projection onto a space V of dimension b: the vectors each of whose four segments is constant on the cosets of N and has zero sum. The b columns of D must form an orthogonal basis of V consisting of ± 1 vectors, and so must the b rows of E. The corner is then forced, $C = -EK^{\mathsf{T}}D/(4|G|)$, and it satisfies $CC^{\mathsf{T}} = bI$ automatically. Once such D and E are chosen, the one requirement that can fail is that the entries of C be ± 1.

Whether a core can be so bordered depends only on its sums over the cosets of N, which are $4q$ integers; so bordering is a finite problem on the small group Q, separate from the search for the core. For quotient groups of order 4, 6 and 8 it always can, after at most translating, inverting, negating or permuting the blocks of the core; we verified this by computer (Proposition 8). These are the widths $b = 12, 20, 28$. The case $q = 2$, width 4, is classical. Throughout, a *width-b matrix* is a Hadamard matrix assembled from a core and a border of width b, and a *width-b core* is a core for such a border; the width is that of the border, not of the matrix or the core. This follows the usage of [23], whose b is also the border width; in the phrase *two circulant cores* of [8, 40] each block is a core, whereas here the core is all four blocks together.

What is gained is freedom in the choice of G. For $v = 479$, for example, $v - 1 = 2 \cdot 239$ admits no usable multiplier group, but $v - 3 = 476 = 2^2 \cdot 7 \cdot 17$, and $G = \mathbb{Z}_2^2 \times \mathbb{Z}_{119}$ has a group of automorphisms of order 12 and quotients of orders 68 and 28 through which the search can be organised (§5.5). For order 668

we give both a width-4 and a width-12 matrix: the second search was far smaller than the first (Table 1). It was small because it looked only for cores with three fibres of a mixed type (§5.6), the fewest possible (Lemma 10); with so few, the core condition splits into four nearly independent systems.

1.3. **Which order uses which method.** In every search we fix a *cell*: the group G, a group M of its automorphisms (the *multiplier group*) under which every block is required to be invariant, and, for a bordered array (§3.2), a subgroup $N \le G$. A block is then one sign per M-orbit, and (2), or for bordered arrays its analogue (3) or (4), is one quadratic equation per orbit of $\langle M, -1\rangle$ on the non-zero elements of G. The columns *signs* and *eqs* of Table 1 count the signs of all four blocks and the equations. For example, the row of order 1916 describes the cell with $G = \mathbb{Z}_2^2 \times \mathbb{Z}_{119}$, a multiplier group of order 12 and $N = \mathbb{Z}_{119}$, which has 184 signs and 29 equations.

The row-sum condition of §1.2 can be met for $v = 223, 283, 311, 487, 491$, with some odd $t > 1$ dividing $v - 1$, and for none of the other seven primes. For $v = 167, 179, 347, 359, 479$, $v - 1$ is twice a prime and the only odd $t > 1$ is $(v - 1)/2$. For this t the possible row sums are ± 1, $\pm(v - 2)$ and $\pm v$, and no four of their squares sum to $4v$. For $v = 419, 443$ there are proper odd divisors but no suitable row sums. A bordered cell is most readily searched by compression (§4.2) when $|G| = v - (q - 1)$ has several small factors, giving G small quotients and automorphisms of small order fixing N. At width 4 this is so for $v = 419, 443$, where $|G| = 2 \cdot 11 \cdot 19$, $2 \cdot 13 \cdot 17$. For $v = 167, 179$ the group $\mathbb{Z}_2 \times \mathbb{Z}_w$, $w = (v - 1)/2$, has order twice a prime, and we searched it with no symmetry. For $v = 347, 359, 479$ it would again have order twice a prime, and we used width 20 for 347, width 28 for 359 and width 12 for 479, where $|G|$ has several small factors (Table 1).

TABLE 1. The thirteen matrices. GS is the array (1) with circulant blocks on $\mathbb{Z}_v$ (§2.1), and Bb is the bordered array of width b over G, with $|G| = v - b/4$ (§§3.1, 3.2). The columns *signs* and *eqs* are those of §1.3. The column $\log_2$ ops gives $\log_2$ of the number of pair sums formed up to the first matrix (§4.1), or for 892 in the complete matching; $\approx$ marks entries estimated from the list sizes. The last column gives the subsection of §5, and 668′ is the second, width-12 matrix of order 668.

order	v	array	G	$\lvert G\rvert$	$\lvert M\rvert$	signs	eqs	$\log_2$ ops	method	§
668	167	B4	$\mathbb{Z}_2 \times \mathbb{Z}_{83}$	$166 = 2 \cdot 83$	1	664	83	≈ 59	decoupling along $\mathbb{Z}_2$	5.2
668′	167	B12	$\mathbb{Z}_2^2 \times \mathbb{Z}_{41}$	$164 = 2^2 \cdot 41$	1	656	83	≈ 44	decoupling along $\mathbb{Z}_2^2$	5.6
716	179	B4	$\mathbb{Z}_2 \times \mathbb{Z}_{89}$	$178 = 2 \cdot 89$	1	712	89	≈ 66	decoupling along $\mathbb{Z}_2$	5.2
892	223	GS	$\mathbb{Z}_{223}$	223	3	300	37	49	method of [20]	5.1
1132	283	GS	$\mathbb{Z}_{283}$	283	3	380	47	56	method of [20]	5.1
1244	311	GS	$\mathbb{Z}_{311}$	311	5	252	31	≈ 34	method of [20]	5.1
1388	347	B20	$\mathbb{Z}_6 \times \mathbb{Z}_{57}$	$342 = 2 \cdot 3^2 \cdot 19$	6	280	39	≈ 41	two quotients, sampled	5.7
1436	359	B28	$\mathbb{Z}_2^2 \times \mathbb{Z}_8 \times \mathbb{Z}_{11}$	$352 = 2^5 \cdot 11$	5	384	51	≈ 40	two quotients, nested	5.8
1676	419	B4	$\mathbb{Z}_2 \times \mathbb{Z}_{209}$	$418 = 2 \cdot 11 \cdot 19$	15	168	21	42	decoupling along $\mathbb{Z}_2$, under M	5.3
1772	443	B4	$\mathbb{Z}_2 \times \mathbb{Z}_{221}$	$442 = 2 \cdot 13 \cdot 17$	12	200	29	≈ 36	two quotients	5.4
1916	479	B12	$\mathbb{Z}_2^2 \times \mathbb{Z}_{119}$	$476 = 2^2 \cdot 7 \cdot 17$	12	184	29	≈ 35	two quotients	5.5
1948	487	GS	$\mathbb{Z}_{487}$	487	9	220	27	≈ 38	method of [20]	5.1
1964	491	GS	$\mathbb{Z}_{491}$	491	7	284	35	55	method of [20]	5.1

1.4. **Contributions.** To our knowledge each of the following two things is new: bordered Goethals–Seidel arrays wider than 4 with a Hadamard corner (Theorem 5), and compression [21, 52, 72] organised as lifting through two quotients at once for four blocks under a multiplier group (§4.4). Egan, Kotsireas, London and Ó Catháin recovered the construction of Theorem 5 from the released matrices and state it as [23, Thm. 7]; it has since given further orders [23, §4]. The change of variables we used for the width-4 cores of orders 668, 716 and 1676 (§4.3) is not new. It replaces the two halves $a(0, \cdot)$ and $a(1, \cdot)$ of each block on $\mathbb{Z}_2 \times \mathbb{Z}_w$ by their half-sum S and half-difference T, which are $(0, \pm 1)$-functions on $\mathbb{Z}_w$ with complementary supports, and it turns condition (3) into one system on the half-sums and one on the half-differences; once the supports are fixed, the two systems have no variable in common. This is the decomposition on which Miyamoto's main theorem [56] rests, and the two systems are the two conditions of that theorem. All four of our width-4 matrices are instances of the theorem, that of order 1772 included, although its core was found by another method (§4.3). Miyamoto's own applications of his theorem take the two parts from conference matrices and other auxiliary matrices; ours come from searches (§7). Seberry and Yamada restated his theorem in terms

of their M-structures [64, 65], and the same passage to half-sums and half-differences takes base sequences to T-sequences [65, 75]. What we add there is computational: a necessary condition on the supports, and an enumeration of the support systems that meet it. For the second matrix of order 668 we used the analogous change of variables along $\mathbb{Z}_2^2$, which has four parts in place of two and to which Miyamoto's theorem does not apply (§§4.3, 5.6). The Goethals–Seidel array with blocks invariant under a multiplier group, searched with candidate lists and matching, and the width-4 array are classical (§7).

The thirteen searches differ enormously in cost, and this bears on what each matrix shows (§6.3, Appendix D). The matrices from wide borders, the construction that is new here, were cheap to find: at most about 150 core-hours each by our estimate. Four matrices came from large matchings on classical arrays: those of orders 1132 and 1964 by the known circulant method, and those of orders 668 and 716 on the width-4 array with no symmetry. For the last two, the decomposition, the feasibility condition and the restriction to interval-like supports reduce a choice among about 2^{162} and 2^{174} sequences per block to matchings of about 2^{59} and 2^{66} pair sums, and these matchings were then carried out by computation. The count roughly doubles with each unit of w, so the approach does not extend far. By our estimate the counted operations of the order-716 search alone cost $2\cdot10^7$ to $8\cdot10^7$ core-hours, most of the computation counted in this paper (more than nine tenths at the counts of Table 1) and about US$1–4 million at current list prices for rented processors; the nine cheapest searches together cost under US$300. The matrix of order 716 is therefore a result of computation on a scale open to few, more than of a new construction; the width-4 matrix of order 668 came from a search of about the cost of those for orders 1132 and 1964, and owes more to that search than to a new construction.

The matrices are printed in Appendix A and can be checked directly (§6). Proposition 8 and the counts of Appendix C rest on enumerations by computer, and Theorem 1 does not use them.

An off-the-shelf constraint solver was used in preliminary screening (compare [6]); neither it nor learned generators [79] produced any of the objects printed here.

How the work was done. The constructions and searches reported here were carried out by Claude, an AI system made by Anthropic. The constructions, proofs, code and the text of this paper are the system's. The text was afterwards edited by Claude working with Erisa Hasani, Abhinav Nellore and Rachel Ward, who proposed corrections of attribution and of emphasis. That editing was done from the text and the printed data, without the search programs or their logs. The re-run of the recipes on the printed tables reported in §6.1, the timing program and the estimates of Appendix D date from it, which is why the appendix estimates the cost of the searches and cannot report the hardware and time they used.

1.5. **Notation.** Throughout, G is a finite abelian group written additively, and vectors and matrices are indexed by its elements; $\mathbb{Z}_v = \{0,1,\dots,v-1\}$, so indices start from 0. A function $a\colon G\to\mathbb{R}$ (below with values in $\{0,\pm1\}$ or in $\mathbb{Z}$) is a vector in $\mathbb{R}^G$, with $\langle a,a'\rangle = \sum_x a(x)a'(x)$; $\mathbf{1}$ is the all-ones vector, $\mathbf{1}_S$ the indicator vector of a set S, and $1\{P\}$ is 1 if the statement P holds and 0 otherwise. The characters χ of G are the frequencies, $\hat a(\chi) = \sum_x a(x)\chi(x)$ is the un-normalised discrete Fourier transform of a, and $\chi = 1$ is the trivial character, the zero frequency; so $\hat a(1) = \langle a,\mathbf{1}\rangle$ is the row sum of a.

The group matrix $A = (a(y-x))_{x,y}$ is the G-circulant matrix generated by a (a group-developed matrix in the terminology of [33, 13]); for $G=\mathbb{Z}_v$ it is the circulant matrix with first row a. Every character is an eigenvector, $A\chi = \hat a(\chi)\chi$ and $A^{\mathsf T}\chi = \overline{\hat a(\chi)}\,\chi$. So $AA^{\mathsf T}$ has the eigenvalues $|\hat a(\chi)|^2$, and it is the group matrix of the periodic autocorrelation $\mathrm{PAF}_a(s) = \langle a, a(\cdot+s)\rangle$, the inner product of a with its shift by s. Conditions on $\sum_f \mathrm{PAF}_{a_f}$ and on the power spectrum $\mathrm{PSD} = \sum_f |\hat a_f|^2$ are therefore two forms of the same statement, and Parseval's identity is $\sum_\chi |\hat a(\chi)|^2 = |G|\langle a,a\rangle$. The matrix R is the reflection $(Ru)(x) = u(-x)$, and $RAR = A^{\mathsf T}$. For a subgroup L of G, $L^\perp$ is the set of characters that are trivial on L, that is the characters of G/L pulled back to G (composed with the quotient map). Below, N is always a subgroup, not a dimension, and $k = |N|$. Appendix B is a glossary.

2. Goethals–Seidel arrays and the circulant method

For $a_1,\dots,a_4\colon G\to\{\pm1\}$, with the group matrices A_f and the reflection R of §1.5, the Goethals–Seidel array [29] (over an abelian group, [76]) is

$$K(a_1,\dots,a_4)=\begin{pmatrix} A_1 & A_2R & A_3R & A_4R\\ -A_2R & A_1 & A_4^{\mathsf T}R & -A_3^{\mathsf T}R\\ -A_3R & -A_4^{\mathsf T}R & A_1 & A_2^{\mathsf T}R\\ -A_4R & A_3^{\mathsf T}R & -A_2^{\mathsf T}R & A_1\end{pmatrix},\qquad KK^{\mathsf T}=K^{\mathsf T}K=I_4\otimes\sum\nolimits_f A_fA_f^{\mathsf T}, \tag{1}$$

and $\sum_f A_fA_f^{\mathsf T}$ is the group matrix of $\sum_f \mathrm{PAF}_{a_f}$ (§1.5). The identity holds because group matrices of an abelian group commute and $RA_fR=A_f^{\mathsf T}$: each A_fR and $A_f^{\mathsf T}R$ is symmetric, and the off-diagonal blocks of $KK^{\mathsf T}$ cancel in pairs. Hence K is a Hadamard matrix of order $4|G|$ exactly when

$$\sum\nolimits_f \mathrm{PAF}_{a_f}(s)=0\quad(s\neq0),\qquad\text{equivalently}\qquad \sum\nolimits_f|\hat a_f(\chi)|^2=4|G|\text{ for every }\chi, \tag{2}$$

i.e. when the sets $X_f=\{a_f=-1\}$ are 4-$\{|G|;|X_1|,\dots,|X_4|;\lambda\}$ supplementary difference sets with $\lambda=\sum_f|X_f|-|G|$. The row sums $r_f=\hat a_f(1)$ then satisfy $\sum_f r_f^2=4|G|$.

2.1. Circulant blocks constant on the cosets of a multiplier group.

With $G=\mathbb{Z}_v$ for a prime v and no border, (1) is the setting of Đoković [17] and of Đoković, Golubitsky and Kotsireas [20] (orders 764 and 1004 among others), whose cell we use unchanged; Đoković's order 956 [16] is of the same kind. In the classical theory a multiplier t of a difference set D may move it to a translate, $tD=D+g$ [5]; here, as in [23], invariance $tD=D$ is required. Let $t>1$ be an odd divisor of $v-1$, put $2m=(v-1)/t$, and let g be a primitive root modulo v. The cosets of the subgroup M of order t (so $t=|M|$) in $\mathbb{Z}_v^*$ are

$$O_j=\{g^{j+2mu}:0\le u<t\},\qquad j\in\mathbb{Z}_{2m},$$

and $-O_j=O_{j+m}$. Here M acts on $\mathbb{Z}_v$ by multiplication, and a sequence invariant under M is one that is constant on the orbits of M, namely on $\{0\}$ and on each O_j. A sequence $a\in\{\pm1\}^{\mathbb{Z}_v}$ constant on each coset is given by $e_0=a(0)$ and $\varepsilon=(\varepsilon_0,\dots,\varepsilon_{2m-1})$, where ε_j is its value on O_j. Its row sum $r=e_0+t\sum_j\varepsilon_j$ is therefore $\equiv\pm1\pmod{2t}$, because $\sum_j\varepsilon_j$, a sum of $2m$ signs, is even. Its autocorrelation is constant on each union $O_i\cup O_{i+m}$, so (2) becomes m equations in the values $P_a(i)=\mathrm{PAF}_a(g^i)$, $0\le i<m$. The cell thus has $4(2m+1)$ signs and m equations.

3. Bordered arrays

3.1. Width 4: the Wallis–Whiteman array.

In the classical case the core lives on $\mathbb{Z}_{2w}$ and is bordered by 4 rows and columns. Up to multiplying every block by the character of order 2 of $\mathbb{Z}_{2w}$, it is the case $q=2$ of Theorem 5 (Remark 7(ii)). The array is the Wallis–Whiteman array [77, Thm. 4.17], so named in [47, 48]: a Goethals–Seidel array (1) surrounded by a border of four rows and columns. Wallis and Whiteman gave such a border for four blocks of equal size on a group of odd order [76, Thm. 12], and in the same paper adapted the unbordered Goethals–Seidel array from circulants to abelian groups [76, Thm. 11]. In this paper the name always means the bordered array.

Proposition 2 (Wallis–Whiteman). *Let $a_1,\dots,a_4\in\{\pm1\}^{\mathbb{Z}_{2w}}$ satisfy*

$$\sum\nolimits_f \mathrm{PAF}_{a_f}(s)=-4\quad(s\neq0), \tag{3}$$

ordered so that the row sums are $(2,0,0,0)$, and let $\mathbf{1}=(1,\dots,1)^{\mathsf T}\in\mathbb{Z}^{2w}$. Then

$$\begin{pmatrix} C_0 & E_0\otimes\mathbf{1}^{\mathsf T}\\ D_0\otimes\mathbf{1} & K(a_1,\dots,a_4)\end{pmatrix},\quad C_0=\begin{pmatrix}-&+&+&-\\+&-&+&-\\+&+&-&-\\-&-&-&-\end{pmatrix},\ D_0=\begin{pmatrix}+&+&+&-\\-&-&+&-\\-&+&-&-\\+&-&-&-\end{pmatrix},\ E_0=-\tfrac12C_0D_0^{\mathsf T},$$

is a Hadamard matrix of order $4(2w+1)$.

Summing (3) over s gives $\sum_f r_f^2=8w-4(2w-1)=4$, since $\sum_s\mathrm{PAF}_a(s)=r^2$ and $\mathrm{PAF}_{a_f}(0)=2w$. Each r_f is even, being a sum of $2w$ signs, so the row sums are $(\pm2,0,0,0)$ in some order, and reordering the blocks and negating one if necessary gives $(2,0,0,0)$. The matrix E_0 has the rows $(-,-,-,+)$, $(-,-,+,-)$, $(-,+,-,-)$ and $(+,-,-,-)$.

Proof of Proposition 2. By (3), $\sum_f A_f A_f^{\mathsf T}$ is the group matrix of the function equal to $8w$ at 0 and -4 elsewhere, that is $nI - 4\,\mathbf{1}\mathbf{1}^{\mathsf T}$ with $n = 8w+4$. So K falls short of a Hadamard matrix only along the all-ones vector of each of its four block rows. Since $A_f\mathbf{1} = A_f^{\mathsf T}\mathbf{1} = r_f\mathbf{1}$ and $R\mathbf{1} = \mathbf{1}$, we have $K(z\otimes\mathbf{1}) = (K_r z)\otimes\mathbf{1}$ for $z \in \mathbb{R}^4$, where K_r is the array (1) with the numbers r_f in place of the blocks; for $r = (2,0,0,0)$, $K_r = 2I_4$. The matrices C_0, D_0, E_0 are Hadamard matrices of order 4. Write H for the displayed matrix. The three blocks of $HH^{\mathsf T}$ are therefore $C_0C_0^{\mathsf T} + 2w\,E_0E_0^{\mathsf T} = (4+8w)I_4$; $C_0D_0^{\mathsf T}\otimes\mathbf{1}^{\mathsf T} + 2E_0\otimes\mathbf{1}^{\mathsf T} = 0$, by the definition of E_0; and $D_0D_0^{\mathsf T}\otimes\mathbf{1}\mathbf{1}^{\mathsf T} + KK^{\mathsf T} = 4I_4\otimes\mathbf{1}\mathbf{1}^{\mathsf T} + I_4\otimes(nI - 4\,\mathbf{1}\mathbf{1}^{\mathsf T}) = nI$. □

The known algebraic families of cores for this array [48, Thm. 1.1] do not cover the w we need: we use the array with $\mathbb{Z}_{2w} = \mathbb{Z}_2\times\mathbb{Z}_w$ for $w = 83, 89, 209, 221$.

Terminology. Egan, Kotsireas, London and Ó Catháin [23, §2.1] call four ±1 sequences satisfying (3) a *Legendre quadruple*, a name modelled on Legendre pairs [26] (two sequences, with sum -2 in place of -4). They state Proposition 2 for circulant blocks with a differently signed border [23, Thm. 5]. The Wallis–Whiteman array is also among the arrays that Seberry and Yamada's M-structures unify [64].

Example 3 (Order 12)**.** Take $w = 1$, so $G = \mathbb{Z}_2$, and $a_1 = (+,+)$, $a_2 = a_3 = a_4 = (+,-)$. The autocorrelations at $s = 1$ are $2, -2, -2, -2$, with sum -4, and the row sums are $(2,0,0,0)$, so Proposition 2 gives a Hadamard matrix of order 12.

Theorem 5 below replaces the all-ones vector of each block by the $(q-1)$-dimensional space of zero-sum functions on $Q = G/N$ (for $q = 2$ the two are related by the twist of Remark 7(ii)).

3.2. **Wider borders with a Hadamard corner.** Suppose H, of the shape of Figure 1, is a Hadamard matrix of order n, with corner C of order b and $K = K(a_1,\dots,a_4)$. Then $HH^{\mathsf T} = nI$ is three equations:

$$\text{(a) } KK^{\mathsf T} + DD^{\mathsf T} = nI, \qquad \text{(b) } CD^{\mathsf T} + EK^{\mathsf T} = 0, \qquad \text{(c) } CC^{\mathsf T} + EE^{\mathsf T} = nI_b.$$

Since D has b columns, (a) requires $nI - KK^{\mathsf T}$ to be positive semidefinite of rank at most b. By (1) its eigenvalues are the numbers $n - \mathrm{PSD}(\chi)$, each four times. So PSD may differ from n at no more than $b/4$ characters. The simplest arrangement is that these are the $q-1$ non-trivial characters of a quotient $Q = G/N$, with $b = 4(q-1)$, and that PSD takes one value on them; by Parseval's identity that value is b. This is condition (4) below.

Let N be a subgroup of G of even index q, let $Q = G/N$, with quotient map $\pi\colon G\to Q$, and put

$$|G| = qk, \qquad b = 4(q-1), \qquad n = 4|G| + b.$$

For the second matrix of order 668, for instance, $G = \mathbb{Z}_2^2\times\mathbb{Z}_{41}$ and $N = \mathbb{Z}_{41}$, so $q = 4$, $k = 41$, $b = 12$ and $n = 4\cdot 164 + 12$. We say that four functions $a_1,\dots,a_4\colon G\to\{\pm1\}$ satisfy the *core condition* for (G,N), or form a *core*, if

$$\text{(4)}\qquad \sum\nolimits_f \mathrm{PAF}_{a_f}(s) = \begin{cases} -b, & s\in N\setminus\{0\},\\ 4, & s\notin N,\end{cases} \qquad \text{equivalently} \qquad \sum\nolimits_f |\hat a_f(\chi)|^2 = \begin{cases} b, & \chi\neq 1,\ \chi|_N = 1,\\ n, & \text{otherwise,}\end{cases}$$

where the second form includes $\chi = 1$, at which it reads $\sum_f r_f^2 = n$. The two forms are equivalent because $\sum_f \mathrm{PAF}_{a_f}(s) = n\,1\{s=0\} - (4q\,\mathbf{1}_N(s) - 4)$ for all s, and the function $4q\,\mathbf{1}_N - 4$ has transform $4|G|$ at the non-trivial characters in $N^\perp$ and 0 elsewhere. Equivalently, the sets $X_f = \{a_f = -1\}$ form a divisible difference family relative to N [57, Def. 1.1]: a non-zero element of the group is a difference within these sets exactly $\sum_f |X_f| - |G| - (q-1)$ times if it lies in N and $\sum_f |X_f| - |G| + 1$ times otherwise.

The array (1) is defined by the same formula for integer-valued functions. The theorem is stated in the following terms.

- Let $\beta_f(c) = \sum_{x\in c} a_f(x)$ for $c\in Q$ be the *coset sums*, the compression of each block to Q. By the second form of (4), since $\hat\beta_f(\theta) = \hat a_f(\theta\circ\pi)$, they satisfy $\sum_f |\hat\beta_f(\theta)|^2 = b$ for every character $\theta\neq 1$ of Q and $\sum_f \hat\beta_f(1)^2 = n$.
- We call the quadruple $(\beta_f)_f$, taken modulo adding constants (which do not matter, by Remark 7(i)), the *coset table* of the core.
- The border of Theorem 5 is built from *balanced* vectors $\ell\in\{\pm1\}^Q$, those with $\sum_c \ell(c) = 0$, which exist only for even q.
- A *word* is a vector in $\{\pm1\}^{4q} = (\{\pm1\}^Q)^4$ whose four segments, one per block position, are balanced.

- Let $K_\beta = K(\beta_1, \dots, \beta_4)$ be the array (1) over Q, a $4q \times 4q$ integer matrix.

Rows and columns of K and K_β, rows of D and of the matrix D_Q of Theorem 5, and columns of E and E_Q, are indexed by pairs (f, x) with $x \in G$, respectively (f, c) with $c \in Q$, the block position f major.

Lemma 4 (Pull-backs)**.** *For $\ell\colon Q \to \mathbb{R}$ call $\ell\circ\pi$ its pull-back to G, and pull back vectors of $(\mathbb{R}^Q)^4$ segment by segment. Let $\bar{A}_f$ be the group matrix of β_f over Q, and $\bar{R}$ the matrix R over Q. Then (i) $\langle \ell\circ\pi, \ell'\circ\pi\rangle = k\langle \ell, \ell'\rangle$; (ii) $A_f(\ell\circ\pi) = (\bar{A}_f\ell)\circ\pi$, $A_f^{\mathsf{T}}(\ell\circ\pi) = (\bar{A}_f^{\mathsf{T}}\ell)\circ\pi$ and $R(\ell\circ\pi) = (\bar{R}\ell)\circ\pi$. Hence K and K^{T} send the pull-back of a vector $u \in (\mathbb{R}^Q)^4$ to the pull-backs of $K_\beta u$ and $K_\beta^{\mathsf{T}} u$.*

Proof. Part (i) holds because each coset of N has k elements. For (ii), $(A_f(\ell\circ\pi))(x) = \sum_y a_f(y-x)\ell(\pi y) = \sum_{c\in Q} \beta_f(c - \pi x)\ell(c)$, and the other two identities are proved in the same way. The last statement follows because K and K_β are built by the same formula (1). □

Theorem 5 (Bordered array with a Hadamard corner)**.** *Let $a_1, \dots, a_4$ satisfy (4), with coset table (β_f). Let $D_Q \in \{\pm1\}^{4q\times b}$ have pairwise orthogonal words as columns and $E_Q \in \{\pm1\}^{b\times 4q}$ pairwise orthogonal words as rows, such that all entries of $C = -\frac{1}{4q} E_Q K_\beta^{\mathsf{T}} D_Q$ are ±1. Let $D_{(f,x),j} = (D_Q)_{(f,\pi x),j}$ and $E_{i,(f,x)} = (E_Q)_{i,(f,\pi x)}$ be the pull-backs to G. Then*

$$H = \begin{pmatrix} C & E \\ D & K(a_1, \dots, a_4) \end{pmatrix}$$

is a Hadamard matrix of order $n = 4|G| + 4(q-1)$, and C is a Hadamard matrix of order $4(q-1)$.

Proof. Let Π be the orthogonal projection of $\mathbb{R}^G$ onto the functions constant on N-cosets with zero sum, and let V be the space of vectors in $(\mathbb{R}^G)^4$ each of whose four segments lies in the range of Π. Equivalently, each segment lies in the span of the non-trivial characters in $N^\perp$. So V has dimension $4(q-1) = b$, and the orthogonal projection onto it is $I_4 \otimes \Pi$.

Step 1 (the defect of K). By (4), $nI - \sum_f A_f A_f^{\mathsf{T}}$ is the group matrix of $4q\,\mathbf{1}_N - 4$. The group matrix of $\mathbf{1}_N$ is k times the projection onto the functions constant on cosets of N, and that of the constant 1 is $|G|$ times the projection onto the constants. Since $qk = |G|$, this gives $nI - \sum_f A_f A_f^{\mathsf{T}} = 4|G|\,\Pi$, and by (1) $nI - KK^{\mathsf{T}} = nI - K^{\mathsf{T}}K = 4|G|(I_4 \otimes \Pi)$.

Step 2 (the borders are orthogonal bases of V). The columns of D are pull-backs of words, so they lie in V. By Lemma 4(i) they are pairwise orthogonal and each has squared length $4qk = 4|G|$, and there are $b = \dim V$ of them. Hence $D^{\mathsf{T}}D = 4|G|I_b$ and $DD^{\mathsf{T}} = 4|G|(I_4 \otimes \Pi)$. With Step 1 this is (a). The same holds for the rows of E: $EE^{\mathsf{T}} = 4|G|I_b$.

Step 3 (K acts on V through Q). Each $\bar{A}_f$ and $\bar{A}_f^{\mathsf{T}}$ preserves the zero-sum functions on Q, and so does $\bar{R}$; so by Lemma 4 K and K^{T} map V into itself. By the same lemma $K^{\mathsf{T}}D$ is the pull-back of $K_\beta^{\mathsf{T}} D_Q$, and $EK^{\mathsf{T}}D = k\,E_Q K_\beta^{\mathsf{T}} D_Q$. Hence $C = -EK^{\mathsf{T}}D/(4|G|)$.

Step 4 (the remaining blocks). Now $CD^{\mathsf{T}} = -EK^{\mathsf{T}}DD^{\mathsf{T}}/(4|G|) = -EK^{\mathsf{T}}(I_4 \otimes \Pi) = -EK^{\mathsf{T}}$, because the columns of KE^{T} lie in V. This is (b). Next, $CC^{\mathsf{T}} = EK^{\mathsf{T}}(I_4 \otimes \Pi)KE^{\mathsf{T}}/(4|G|) = EK^{\mathsf{T}}KE^{\mathsf{T}}/(4|G|)$. By Step 1, $K^{\mathsf{T}}K$ acts on V as multiplication by $n - 4|G| = b$. So $CC^{\mathsf{T}} = (b/4|G|)EE^{\mathsf{T}} = bI_b$, and with $EE^{\mathsf{T}} = 4|G|I_b$ this is (c). By hypothesis C has entries ±1, so H is a ±1 matrix with $HH^{\mathsf{T}} = nI$, and C is a Hadamard matrix of order b. □

Conversely, let (4) hold and let H, of the shape of Figure 1, be a Hadamard matrix. By (a) and Step 1, $DD^{\mathsf{T}} = 4|G|(I_4 \otimes \Pi)$, so the columns of D lie in V, D has rank b, and $(D^{\mathsf{T}}D)^2 = D^{\mathsf{T}}(DD^{\mathsf{T}})D = 4|G|\,D^{\mathsf{T}}D$ gives $D^{\mathsf{T}}D = 4|G|I_b$; the same argument applied to $H^{\mathsf{T}}H = nI$ treats E. Since a ±1 vector of V is the pull-back of a word, the conditions on D_Q and E_Q in Theorem 5 are necessary as well as sufficient. Theorem 5 is the construction that Egan, Kotsireas, London and Ó Catháin state as [23, Thm. 7], which they recovered from the matrices released in [1]. Their subgroup S of index k is our N of index q, and their K, E and F play the roles of C, E_Q and D_Q. They take the corner K as given, while here it is forced by D_Q and E_Q.

We call a pair (D_Q, E_Q) as in the theorem a *frame* for the coset table, and the question whether a given coset table has a frame its *frame problem*. (The word has nothing to do with frames in the sense of harmonic analysis.)

Example 6 (Order 28 with a border of width 12)**.** Take $G = Q = \mathbb{Z}_2^2$ and $N = 0$, so $k = 1$, $q = 4$, $b = 12$ and $n = 28$, with the elements in the order $(0,0), (0,1), (1,0), (1,1)$. Let $a_1 = (+,-,-,-)$, $a_2 = (-,-,-,+)$,

$a_3 = (-,+,-,-)$ and $a_4 = (+,+,+,+)$. Each of a_1, a_2, a_3 has autocorrelation 0 at every $s \neq 0$, and a_4 has autocorrelation 4, so $\sum_f \mathrm{PAF}_{a_f} = 4$ off $N = \{0\}$: this is the core condition (4) (the case $s \in N \setminus \{0\}$ is empty). The row sums are $(-2,-2,-2,4)$, with squares summing to 28. Here $\beta_f = a_f$, and this is the coset table named in the caption of Table 2: $\beta_1, \beta_2, \beta_3$ exceed their other values by 2 on $(0,0)$, $(1,1)$, $(0,1)$, and β_4 is constant. So the printed frame applies as it stands. Since π is the identity, $D = D_Q$, $E = E_Q$ and $K = K_\beta$, and Figure 2 shows the resulting Hadamard matrix of order 28, with corner $C = -E_Q K_\beta^{\mathsf{T}} D_Q/16$.

The two width-12 matrices of Table 1, $668'$ and 1916, differ from this one only in that each border entry is repeated $k = 41$ or 119 times and the 4×4 blocks of K become 164×164 or 476×476. The corner C is the same 12×12 matrix in all three, because the three coset tables agree modulo constants.

Keep D_Q and take $E_Q = D_Q^{\mathsf{T}}$ instead. Its rows are again twelve pairwise orthogonal words, so every other hypothesis of Theorem 5 holds, and $CC^{\mathsf{T}} = 12I$ still holds, but C has entries in $\{0, \pm\frac{1}{2}, \pm 1, \pm\frac{3}{2}, \pm 2\}$. The bordered matrix then satisfies $HH^{\mathsf{T}} = 28I$ but is not a ± 1 matrix.

Remark 7. (i) Since words are balanced, adding a constant to a β_f changes nothing, so the hypothesis involves the core only through its coset table. Hence one frame serves every core with that coset table, over any G and N with the same quotient Q. For given Q the core condition admits only finitely many coset tables modulo constants. Indeed, by Parseval's identity $\sum_f \sum_c (\beta_f(c) - \bar{\beta}_f)^2 = b(q-1)/q$, where $\bar{\beta}_f$ is the mean of β_f, and the differences $\beta_f(c) - \beta_f(c')$ are even integers.

(ii) For $q = 2$ the balanced vectors are $\pm(1,-1)$. Let η be the pull-back of the non-trivial character of Q. Multiplying each block by η turns (4) into (3) and, for a suitable frame, the array of Theorem 5 into that of Proposition 2. The reason is that $\eta(x)\eta(y) = \eta(y-x) = \eta(-x-y)$, since $\eta^2 = 1$; so conjugation by $I_4 \otimes \mathrm{diag}(\eta)$ turns A_f into the group matrix of ηa_f and fixes R, and $\mathrm{PAF}_{\eta a}(s) = \eta(s)\mathrm{PAF}_a(s)$.

```
++--+++--++-  +-+-  +-+-  --++  -++-
----+-++-+-+  +-+-  -+-+  --++  +--+
-+---+-+++--  +-+-  ++--  ++--  --++
-+---------++  +-+-  --++  ++--  ++--
++-+--+-++-+  ++--  +-+-  +--+  +--+
---++---+++-  ++--  -+-+  +--+  -++-
-++-+-+-+---  ++--  ++--  -++-  ++--
+-+------+--  ++--  --++  -++-  --++
++-++--+----  +--+  +--+  +-+-  +-+-
---+-++-----  +--+  +--+  -+-+  -+-+
-++++++--+-+  +--+  -++-  +-+-  -+-+
+---++--+--+  +--+  -++-  -+-+  +-+-
++++++++++++  +---  ---+  -+--  ++++
----+++----  -+--  --+-  +---  ++++
++++--------  --+-  -+--  ---+  ++++
--------++++  ---+  +---  --+-  ++++
--++++----++  +++-  +---  ++++  +-++
++----++--++  ++-+  -+--  ++++  -+++
--++--++++--  +-++  --+-  ++++  +++-
++--++--++--  -+++  ---+  ++++  ++-+
+-+-+-+-+-+-  +-++  ----  +---  ---+
-+-++-+--+-+  -+++  ----  -+--  --+-
+--+-+-++--+  +++-  ----  --+-  -+--
-++--+-+-++-  ++-+  ----  ---+  +---
+--+-++--++-  ----  -+--  +++-  +---
+-+-+--+-+-+  ----  +---  ++-+  -+--
-++--++-+--+  ----  ---+  +-++  --+-
-+-++--++-+-  ----  --+-  -+++  ---+
```

FIGURE 2. The Hadamard matrix of order 28 of Example 6: corner C top left, $E = E_Q$ top right, $D = D_Q$ bottom left, and $K(a_1, \ldots, a_4)$ in 4×4 blocks bottom right. Each row of E and each column of D is a word.

3.3. **Frames.** To find a frame is, given the $4q \times 4q$ integer matrix K_β, to find b pairwise orthogonal words $d_1, \ldots, d_b$ and b pairwise orthogonal words $e_1, \ldots, e_b$ with $|e_i K_\beta^{\mathsf{T}} d_j| = 4q$ for all i, j. There are 6, 20, 70

balanced vectors for $q = 4, 6, 8$, hence $6^4 = 1296$, $20^4 = 160\,000$ and $70^4 = 24\,010\,000$ words, and we sought frames by depth-first search over words (Appendix C).

The four matrices of widths 12, 20 and 28 use three frames, printed in Table A2. That each satisfies the hypotheses of Theorem 5 is checked by a few small matrix products. Negating, translating ($a_f \mapsto a_f(\cdot + z)$, $z \in G$) or inverting ($a_f \mapsto a_f(-\cdot)$) single blocks of a core, and permuting its blocks, preserve (4) and act on the coset table by the corresponding *moves*.

Proposition 8 (Frames for $q = 4, 6, 8$; computer-assisted)**.** *Let $N \le G$ have index $q \in \{4, 6, 8\}$. Every core for (G, N) yields, by Theorem 5, a Hadamard matrix of order $4|G| + 4(q-1)$: for $q = 4$ with no adjustment of the core, for $q = 6$ after at most a common translation of its four blocks, and for $q = 8$ after adjusting the core within its class under the moves.*

Proof. By Remark 7(i) only the coset table matters. We enumerated the admissible coset tables (Appendix C) by computer, reduced them to classes by the moves and the isomorphisms defined there, and found a frame for a representative of each class named in the column "frames found" of Table C1, for $q = 4$ for every table. The frames are in [83] and are not printed here, apart from the three used for Theorem 1. □

Rows D and E of Table A2 for orders $668'$ and 1916 are the frame of Table 2 in the hexadecimal encoding of Appendix A. For instance, the first row of E_Q has segments $\theta_2, \theta_2, -\theta_1, -\theta_3$; it is the word `55C9` of Table A2, and its pull-back is the row shown in the lower part of Figure 1, where the cosets of N are contiguous because G is ordered lexicographically.

TABLE 2. The frame for $Q = \mathbb{Z}_2^2$ used for orders $668'$ and 1916 (§§5.6, 5.5): the 12 columns of D_Q (left) and the 12 rows of E_Q (right). An entry i or $\bar{\imath}$ in row f means that the word's segment in block position f is θ_i or $-\theta_i$, where $\theta_i(x) = (-1)^{x_i}$ $(i = 1, 2)$ and $\theta_3 = \theta_1\theta_2$ are the non-trivial characters of Q. It frames the coset table in which β_1, β_2 and β_3 exceed their other values by 2 on the cosets $(0,0)$, $(1,1)$ and $(0,1)$ respectively, and β_4 is constant; this is the coset table of both matrices as printed in Table A2.

f	columns of D_Q												rows of E_Q											
1	2	2	2	2	1	1	1	1	3	3	3	3	2	2	2	2	1	1	1	1	3	3	3	3
2	$\bar{2}$	$\bar{2}$	2	2	3	3	$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{1}$	1	1	2	$\bar{2}$	1	$\bar{1}$	2	$\bar{2}$	1	$\bar{1}$	3	3	$\bar{3}$	$\bar{3}$
3	2	$\bar{2}$	3	$\bar{3}$	1	$\bar{1}$	1	$\bar{1}$	2	$\bar{2}$	3	$\bar{3}$	$\bar{1}$	$\bar{1}$	1	1	3	3	$\bar{3}$	$\bar{3}$	2	$\bar{2}$	2	$\bar{2}$
4	1	$\bar{1}$	$\bar{3}$	3	$\bar{2}$	2	2	$\bar{2}$	$\bar{1}$	1	3	$\bar{3}$	$\bar{3}$	3	$\bar{1}$	1	3	$\bar{3}$	1	$\bar{1}$	2	$\bar{2}$	$\bar{2}$	2

4. Search methods

The bordered cells of Table 1 have between 168 and 712 free signs, too many for direct matching. Two methods reduce them to matchings of practicable size. The first is a change of variables along a factor $\mathbb{Z}_2$ or $\mathbb{Z}_2^2$ of G that splits the condition into parts with no common variables (§4.3), used for orders 668, 716, 1676 and $668'$. Along $\mathbb{Z}_2$, for orders 668, 716 and 1676, it is the decomposition of Miyamoto's main theorem and gives two parts, the half-sums and the half-differences. Along $\mathbb{Z}_2^2$, for $668'$, it is the analogous decomposition into four parts, to which Miyamoto's theorem does not apply; there the four parts are free of common variables only after the signs at three exceptional positions, the mixed fibres of §5.6, have been fixed. The second is lifting through two quotients of G at once under a multiplier group (§4.4), used for 1772 and 1916 and, in variant forms, for 1388 and 1436.

4.1. **Matching.** The searches below solve equations $p_1 + p_2 + p_3 + p_4 = p_0$ in which each p_f ranges over a finite list $\mathcal{L}_f$ of integer vectors, by exact meet-in-the-middle matching [20, 41]. Here p_f is the vector of autocorrelations of a candidate for block f, one coordinate per equation, and p_0 is the prescribed right-hand side. One tabulates the sums $p_1 + p_2$ in a hash table indexed by (part of) the vector and probes it with $p_0 - p_3 - p_4$. When the table would be too large, both sides are partitioned by the value of the pair sum at a few coordinates, and corresponding parts are matched one at a time. Forming one pair sum $p_1 + p_2$ or $p_0 - p_3 - p_4$ counts as one operation. The column $\log_2$ ops of Table 1 counts these operations. It includes the matchings that list compressed solutions (§4.2) but not list generation. Appendix D converts these counts to processor time and cost.

If the parts likeliest to contain a solution are visited first, a matching that is stopped at its first solution does only the work up to that part. This is why "first" is far below "complete" in Table 3.

4.2. **Compression.** For a subgroup $L \le G$, the sums $a^L(c) = \sum_{x\in c} a(x)$ of a function over the cosets c of L satisfy [21, 22]

$$\sum\nolimits_f \mathrm{PAF}_{a_f^L}(d) = \sum_{s\in d} \sum\nolimits_f \mathrm{PAF}_{a_f}(s) \qquad (d \in G/L). \tag{5}$$

Both sides are the sum of $a_f(x)a_f(y)$ over f and over the pairs with $y - x \in d$. In the Fourier domain compression is subsampling: the transform of a^L at a character θ of G/L is $\hat a$ at θ pulled back to G. So a^L retains exactly the values of $\hat a$ at the frequencies in $L^\perp$; for a cyclic group these are the multiples of $|L|$. Equation (5) is this statement for $\sum_f |\hat a_f|^2$. The right-hand side is fixed by (2), (4) or (3), so the four compressed blocks satisfy a system of the same kind on G/L, with integer entries. At $d = 0$ the left-hand side is $\sum_f \sum_c a_f^L(c)^2$.

In a cell, the compression of each block to G/L lies in the finite set $\mathcal{C}_f$ of compressions of M-invariant ±1 vectors on G, restricted to the block's row sum when the search fixes it. Condition (5) is one equation per orbit of $\langle M, -1\rangle$ on G/L, the zero coset included. We call the quadruples in $\prod_f \mathcal{C}_f$ satisfying all of these equations the *compressed solutions* of the cell on G/L. They include the compression of every solution in the cell, and for G/L with up to a few dozen M-orbits they can be listed by matching with $\mathcal{L}_f = \mathcal{C}_f$, directly or through a chain of intermediate quotients.

4.3. **Decoupling along $\mathbb{Z}_2$ (Miyamoto's decomposition) and $\mathbb{Z}_2^2$.** Let $G = \mathbb{Z}_2 \times G'$ and write a function $a \in \{\pm1\}^G$ as

$$a(x,y) = S(y) + (-1)^x T(y), \qquad S(y) = \tfrac12\big(a(0,y) + a(1,y)\big), \quad T(y) = \tfrac12\big(a(0,y) - a(1,y)\big),$$

so that $S, T\colon G' \to \{0, \pm1\}$ have complementary supports. This is the Fourier transform in the $\mathbb{Z}_2$ coordinate only: $\hat a(1,\psi) = 2\hat S(\psi)$ and $\hat a(\mathrm{sgn},\psi) = 2\hat T(\psi)$ for every character ψ of G', where sgn is the non-trivial character of $\mathbb{Z}_2$.

In matrix form this is the decomposition on which Miyamoto's main theorem [56] rests. Order G with the $\mathbb{Z}_2$ coordinate major, and let U and V be the group matrices of S and T over G'. The group matrix of a is then

$$A = \begin{pmatrix} U+V & U-V \\ U-V & U+V \end{pmatrix}, \qquad PAP = \begin{pmatrix} 2U & 0 \\ 0 & 2V \end{pmatrix}, \qquad P = \tfrac{1}{\sqrt2}\begin{pmatrix} I & I \\ I & -I \end{pmatrix}.$$

Here U and V are $(0,\pm1)$-matrices of disjoint support whose sum and difference are ±1 matrices. This is the form of the blocks T_{ij} from which Miyamoto assembles his Hadamard matrices [56, (4.3)]; his T_{ij} are ±1 matrices of order $2m$, and are not to be confused with the half-differences T_f of this section. Seberry and Yamada reformulated his results in terms of M-structures, orthogonal matrices of order $4t$ divided into sixteen $t \times t$ blocks [64, §5], [65, §8], a notion that also covers the Goethals–Seidel and Wallis–Whiteman arrays; see also [66] and [67]. Conjugate condition (3), which reads $\sum_f A_f A_f^{\mathsf T} = (8w+4)I - 4J$ with J the all-ones matrix, by the orthogonal matrix P. Since $PJP = \mathrm{diag}(2J, 0)$, it becomes

$$\sum\nolimits_f U_f U_f^{\mathsf T} = (2w+1)I - 2J, \qquad \sum\nolimits_f V_f V_f^{\mathsf T} = (2w+1)I$$

on $G' = \mathbb{Z}_w$. Read entry by entry, this is (6) below.

Miyamoto's main theorem [56, §4] concerns sixteen pairs (U_{ij}, V_{ij}), $1 \le i, j \le 4$, of $(0,\pm1)$-matrices of order m, assembled with fixed signs into two matrices $M(U_{ij})$ and $M(V_{ij})$ of order $4m$. Its hypotheses are that every $U_{ij} \pm V_{ij}$ is a ±1 matrix [56, (4.1)], that the row sums are 1 for the U_{ii} and 0 for the other U_{ij} [56, (4.2)], and that

$$M(U_{ij})M(U_{ij})^{\mathsf T} = (2m+1)I - 2\,I_4 \otimes J, \qquad M(V_{ij})M(V_{ij})^{\mathsf T} = (2m+1)I$$

[56, (4.9), (4.10)]. Its conclusion is that a bordered array built from the blocks T_{ij} is a Hadamard matrix of order $8m+4$. Now take $m = w$, and for $M(U_{ij})$ and $M(V_{ij})$ take the Goethals–Seidel arrays $K(U_1,\dots,U_4)$ and $K(V_1,\dots,V_4)$ of (1), which have Miyamoto's pattern of signs. Hypothesis (4.1) holds because each $U_f \pm V_f$ is a ±1 matrix. Hypothesis (4.2) holds because the U_f have row sums $\frac12 r_f$, which are $(1,0,0,0)$. Conditions (4.9) and (4.10) are the two equations displayed above, by the identity in (1). His theorem therefore gives a Hadamard matrix of order $8w+4$, and it is the matrix of Proposition 2 up to the ordering

of G and the order and signs of the four border rows and columns. So the four width-4 matrices of this paper, of orders 668, 716, 1676 and 1772, are instances of Miyamoto's main theorem. This says nothing about how they were found: in [56, §5] the pairs (U_{ij}, V_{ij}) are built from conference matrices and other auxiliary matrices, whereas the U_f and V_f here come from the searches of §§5.2–5.4. In the restatement of Seberry and Yamada, the hypotheses above are conditions (iii)–(vi) of [64, Thm. 34] (conditions 3–6 of [65, Thm. 8.10]), under which they obtain an M-structure Hadamard matrix of order $4(2n+1)$, here with $n = w$; [64, Lemma 26] ([65, Lemma 8.6]) is the case of four pairs whose members are pairwise amicable.

Since $\mathrm{PAF}_a(0,s) = 2\mathrm{PAF}_S(s) + 2\mathrm{PAF}_T(s)$ and $\mathrm{PAF}_a(1,s) = 2\mathrm{PAF}_S(s) - 2\mathrm{PAF}_T(s)$, the width-4 condition (3) on $\mathbb{Z}_2 \times \mathbb{Z}_w$ is equivalent to

$$\sum\nolimits_f \mathrm{PAF}_{T_f}(s) = 0, \qquad \sum\nolimits_f \mathrm{PAF}_{S_f}(s) = -2 \quad (s \neq 0), \qquad \sum\nolimits_f |\operatorname{supp} T_f| = 2w+1. \tag{6}$$

Once the supports $W_f = \operatorname{supp} T_f$ are fixed, the two conditions in (6) share no variable (the T-signs are supported on W_f, the S-signs on the complements), so any solution of one combines with any solution of the other on the same supports. A search for $8w$ coupled signs becomes a search over quadruples of supports $(W_1, \dots, W_4)$, which we call *support systems*, followed by two independent searches of $2w+1$ and $2w-1$ signs, whose costs add rather than multiply. We call the two conditions of (6), on the T_f and on the S_f, the *T half* and the *S half*. The separation is a property of Miyamoto's decomposition, not of our search: his theorem puts one condition on the half-sums and one on the half-differences, and the two are tied to each other only through their supports. What this paper adds is a necessary condition on the supports (feasibility, below), the enumeration of support systems of a restricted shape (§5.2), and the matching of the two halves.

Example 9 (The decoupling on $\mathbb{Z}_6$)**.** Take $w = 3$ and, on $\mathbb{Z}_6$ (positions $0, \dots, 5$), $a_1 = {+}{+}{+}{-}{+}{-}$, $a_2 = {+}{+}{-}{+}{-}{-}$, $a_3 = {+}{+}{+}{-}{-}{-}$, $a_4 = {+}{+}{-}{+}{-}{-}$. Then $\sum_f \mathrm{PAF}_{a_f}(s) = -4$ for $s = 1, \dots, 5$ and the row sums are $(2,0,0,0)$, so Proposition 2 gives a Hadamard matrix of order 28. Under $i \mapsto (i \bmod 2, i \bmod 3)$, $a(0,y)$ is a at positions $0,4,2$ and $a(1,y)$ is a at positions $3,1,5$, for $y = 0,1,2$. Then $S_1 = (0,1,0)$, $T_1 = (1,0,1)$; $S_2 = (1,0,-1)$, $T_2 = (0,-1,0)$; $S_3 = (0,0,0)$, $T_3 = (1,-1,1)$; $S_4 = (1,0,-1)$, $T_4 = (0,-1,0)$. The supports of the T_f have sizes $2,1,3,1$, with total $7 = 2w+1$; $\sum_f \mathrm{PAF}_{T_f}(1) = 0$ and $\sum_f \mathrm{PAF}_{S_f}(1) = -2$; the T_f have sums $(2,-1,1,-1)$, with squares summing to 7, and the S_f have sums $(1,0,0,0)$.

Not every support system can carry solutions. Summing (6) gives $\sum_f \big(\sum_y T_f(y)\big)^2 = 2w+1$, the middle-frequency condition of [44] (it is the value $8w+4$ of $\sum_f |\hat{a}_f(\mathrm{sgn}, 1)|^2$, divided by 4). Since $\sum_y S_f(y) = r_f/2$, the normalisation $r = (2,0,0,0)$ gives $(\sum_y S_f(y))_f = (1,0,0,0)$. Let $\nu(s) = \sum_f \#\{y \in W_f : y+s \in W_f\}$. Reducing the T-condition modulo 2 shows that $\nu(s)$ is even for every $s \neq 0$, and the S-condition at shift s is a sum of $\sum_f \#\{y : y, y+s \notin W_f\} = 4w - 2(2w+1) + \nu(s) = \nu(s) - 2$ terms ± 1 equal to -2, which forces $\nu(s) \geq 4$. We call a support system *feasible* if $\nu(s)$ is even and at least 4 for every $s \neq 0$. Fix a feasible support system, sums $\sigma_f = \sum_y T_f(y)$ with $\sum_f \sigma_f^2 = 2w+1$ and $\sigma_f \equiv |W_f| \pmod 2$ for the T half, and the sums $(1,0,0,0)$ for the S half. Each half of (6) then asks for four sign vectors of prescribed sums, the values of T_f on its support or of S_f off it, whose autocorrelation vectors have a prescribed sum. We solved each half by matching the first two blocks against the last two, and verified every match exactly.

Along $\mathbb{Z}_2^2$. For $G = \mathbb{Z}_2^2 \times G'$ and each character θ of $Q = \mathbb{Z}_2^2$, put $a^{(\theta)} = \frac{1}{2}\sum_x \theta(x) a(x,\cdot)$, the *$\theta$-part* of a. Likewise the θ-parts are, up to the factor $\frac{1}{2}$, the Fourier transform in the $\mathbb{Z}_2^2$ coordinate only. The four θ-parts are integer functions on G', and

$$a(x,y) = \tfrac{1}{2}\sum_\theta \theta(x) a^{(\theta)}(y), \qquad \mathrm{PAF}_a(\zeta, s) = \sum_\theta \theta(\zeta)\mathrm{PAF}_{a^{(\theta)}}(s).$$

With $N = G'$, of index 4, and $v = n/4 = |G| + 3$ (so that $b = 12$), the core condition (4) is equivalent to four conditions, one per θ:

$$\sum\nolimits_f \mathrm{PAF}_{a_f^{(\theta)}}(s) = -4 \cdot 1\{\theta \neq 1\} \quad (s \neq 0), \qquad \sum\nolimits_f \sum_y a_f^{(\theta)}(y)^2 = v - 4 \cdot 1\{\theta \neq 1\}. \tag{7}$$

Here the sums $\sum_y a_f^{(\theta)}(y) = \frac{1}{2}\hat{\beta}_f(\theta)$ are $\frac{1}{2}r_f$ for $\theta = 1$ and are otherwise fixed by the coset table (§3.2). This is the analogue of Miyamoto's decomposition with four parts in place of two: the character table H_4 of $\mathbb{Z}_2^2$ takes the place of $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, and (7) has four conditions where (6) has two. Miyamoto's theorem does not apply to it: the border has width 12, not 4. Unlike S and T, the four θ-parts need not have disjoint

supports. A fibre $a(\cdot, y)$ at which more than one θ-part is non-zero is a mixed fibre (§5.6), and mixed fibres are the only places where the four conditions (7) share variables. So the four conditions separate only once the signs of the mixed fibres are fixed, as they are in the search for $668'$ (§5.6).

4.4. **Lifting through two quotients.** To fix ideas, take order 1772: $G = \mathbb{Z}_2 \times \mathbb{Z}_{13} \times \mathbb{Z}_{17}$. A block is two layers, one for each element of $\mathbb{Z}_2$, and each layer is a 13×17 array of signs. Compressing along $\mathbb{Z}_{17}$ records the 13 row sums μ_i of each layer, 26 numbers in all; compressing along $\mathbb{Z}_{13}$ records the 17 column sums κ_j, 34 numbers. A compressed solution on $G/\mathbb{Z}_{17}$ prescribes all the row sums of all four blocks, and one on $G/\mathbb{Z}_{13}$ all the column sums. The pair is *compatible* if, block by block, some M-invariant array of signs has both sets of margins.

$$\begin{array}{ccccc|c} \pm & \pm & \cdots & \pm & \pm & \mu_0 \\ \pm & \pm & \cdots & \pm & \pm & \mu_1 \\ \vdots & & & & \vdots & \vdots \\ \pm & \pm & \cdots & \pm & \pm & \mu_{12} \\ \hline \kappa_0 & \kappa_1 & \cdots & \kappa_{15} & \kappa_{16} & \end{array}$$

Turner, Kotsireas, Bulutoglu and Geyer [72] lift two sequences through two coprime compressions at once, via 0/1 matrices with prescribed row and column sums [27, 61]. We do the same for four blocks under an imposed multiplier group, in three steps, with $L_1, L_2 \leq G$ fixed by M, $L_1 \cap L_2 = 0$ and both quotients small.

(1) We list the compressed solutions on G/L_1 and on G/L_2.
(2) We determine the compatible pairs, those for which for each f some M-invariant ± 1 block has both prescribed coset-sum vectors; this is a separate computation for each block.
(3) Under a compatible pair we list for each block its *decompressions*, the M-invariant ± 1 vectors with both prescribed coset-sum vectors (we use the same word when the coset sums on one quotient only are prescribed), and match the four lists exactly on all equations of the cell.

Under M the Gale–Ryser criterion does not decide which margins are jointly realisable, so for order 1772 this was tabulated by running through the M-invariant patterns of a layer, of which there are 2^{25} because M has 25 orbits on $\mathbb{Z}_{221}$.

Under a single compressed solution on one quotient a block can still have too many decompressions to list (§5.7); prescribing the sums on a second quotient as well shortens the lists.

When a quotient is too large for the first step, we use one of two variants. The first samples decompressions under one compressed solution on the small quotient and matches their coset sums on the large one (order 1388). The second is nesting: a descending chain of subgroups, each level's matching conditioned on a solution of the level above, multi-level in the sense of [52] (order 1436). Every search of §§5.3–5.5, 5.7 and 5.8 is a chain of lists of compressed solutions followed by a final matching on the signs (for order 1676 the S half plays the part of the compressed level, since $2S$ is the compression of a along $\mathbb{Z}_2$). They differ only in the quotients used, their order, and whether a level is listed or sampled.

5. The thirteen matrices

5.1. **Circulant blocks: orders 892, 1132, 1244, 1948, 1964.** For $v = 223, 283, 311, 487, 491$ we take $G = \mathbb{Z}_v$ in the cell of §2.1, with the parameters and row sums of Table 3. For $v = 283$ the only t with suitable row sums is 3, hence $m = 47$ (compare $m \leq 25$ in [20]). For $v = 487$ and 491 we used $t = 9$ and 7 for the smaller m, rather than 3 and 5, for which suitable row sums also exist. We found the sequences of Table A1 by the matching method of [17, 20] over the candidate lists of Table 3.

(1) For each block, a tabu search [8] on ε collected a list $\mathcal{L}_f$ of M-invariant sequences of row sum r_f with $F(a) = \sum_i P_a(i)^2$ below a fixed cut-off (compare the power-spectral-density test of [26]). Since each $P_a(i)$ is the common value of PAF_a on the $2t$ shifts in $O_i \cup O_{i+m}$, $F(a)$ is $1/(2t)$ times $\sum_{s \neq 0} \mathrm{PAF}_a(s)^2$, the energy of Bernasconi's model [3] with periodic boundary conditions (§7). A uniformly random ± 1 sequence on $\mathbb{Z}_v$, with no invariance imposed, has expected $F = mv$; the sequences of Table A1 have F between $0.08\,mv$ and $0.14\,mv$. Egan, Kotsireas, London and Ó Catháin measure the same quantity: their flatness Φ_f is essentially $F/(mv)$, and they find $0.08 < \Phi_f < 0.14$. From the spectra alone, they infer that only nearly flat sequences were searched at these orders [23, §3, Table 2]; the cut-off of this step is that restriction. Sequences with smaller F make a match likelier but are exponentially rarer, and we chose cut-off and list size to balance the two.

TABLE 3. The circulant constructions of §5.1. Here $h = g^{(v-1)/t}$ generates M, the row sums are in the order of (1), and $(|X_1|, \dots, |X_4|; \lambda)$ are the parameters of the supplementary difference sets $X_f = \{a_f = -1\}$. The lists are reduced modulo rotation and reversal; $\mathcal{L}_1, \mathcal{L}_2$ are inserted and $\mathcal{L}_3, \mathcal{L}_4$ probed, and for $v = 223$, $\mathcal{L}_3$ is a subsample of $\mathcal{L}_1 = \mathcal{L}_2$. The columns *complete* and *first* give $\log_2$ of the number of operations in a complete matching and up to the first solution (†: estimated, not counted), and *sols* the distinct quadruples found before the matching was stopped; for $v = 223$ it ran to completion.

$4v$	v	t	g	h	m	(r_1, r_2, r_3, r_4)	$(\lvert X_1\rvert, \dots, \lvert X_4\rvert; \lambda)$	$\lvert\mathcal{L}_f\rvert/10^6$	complete	first	sols
892	223	3	3	183	37	(11, 11, 11, 23)	(106, 106, 106, 100; 195)	1.45, 1.45, 0.18, 1.8	48.9	—	6
1132	283	3	3	238	47	(19, 19, 19, 7)	(132, 132, 132, 138; 251)	380, 380, 110, 51	64.1	56.2	1
1244	311	5	17	36	31	(21, 19, 21, 1)	(145, 146, 145, 155; 280)	2.6, 2.3, 0.8, 0.4	48.8	$\approx 33.9^\dagger$	10
1948	487	9	3	362	27	(17, 1, 17, 37)	(235, 243, 235, 225; 451)	3.0, 2.6, 0.8, 0.4	48.7	$\approx 38.3^\dagger$	6
1964	491	7	2	138	35	(29, 27, 15, 13)	(231, 232, 238, 239; 449)	30, 35, 25, 23	59.4	55.0	1

(2) We reduced each list modulo reversal and the rotations $a(y) \mapsto a(g^{-\rho}y)$, $\rho \in \mathbb{Z}_m$, which shift $(P_a(i))_i$ cyclically. Reversal is $a(y) \mapsto a(-y)$, which leaves P_a unchanged and sends ε_j to ε_{j+m}.
(3) We then matched over the lists and rotations, with one rotation enumerated on the insertion side and two on the probe side as in [20], so that a complete matching is $m|\mathcal{L}_1||\mathcal{L}_2| + m^2|\mathcal{L}_3||\mathcal{L}_4|$ operations. A common rotation of all four blocks is a symmetry, so only three rotations are free. The parts were the values of the pair sum at the first few coordinates; except for $v = 223$ we visited the likeliest parts first.

For each row of Table 3 the four sequences of Table A1 satisfy (2), and the array (1) built from them is the Hadamard matrix of Theorem 1 of that order. The further quadruples for $v = 311$ and 487 counted in the last column of Table 3 are in [83].

5.2. **Width 4, no symmetry: orders 668 and 716.** For $668 = 4 \cdot 166 + 4$ and $716 = 4 \cdot 178 + 4$ we take $G = \mathbb{Z}_2 \times \mathbb{Z}_w$ with $w = 83, 89$ prime, and impose no symmetry, so there are $8w$ signs and w equations. We found the cores by the decoupling (6) of §4.3, that is, by Miyamoto's decomposition of each block into S and T.

A block on $\mathbb{Z}_{166}$ with row sum 0 is one of $\binom{166}{83} \approx 2^{162}$ sequences, so matching whole blocks two against two would mean pairing lists of about 2^{162} sequences each. The decoupling replaces this by a choice of supports and two smaller matchings. Heuristically, a random support system is feasible with probability about $2^{-(w-1)/2}$: since $\nu(s) = \nu(-s)$ there are $(w-1)/2$ parity conditions, each met with probability about $\frac{1}{2}$, while $\nu(s) \geq 4$ is far from binding for random supports, so feasible systems must be constructed rather than drawn. The matching below partitions the pair sums by their values at the shifts where the equations have fewest terms, and a sum of few signs takes few values. For interval-like supports the equations at the largest shifts have few terms: for the system of the order-668 matrix of Table A2, $\nu(s)$ falls from 158 at $s = 1$ to 14, 12, 10 at $s = 39, 40, 41$, whereas random supports of the same sizes would give about 83 at every shift.

We restricted to supports that are cyclic intervals with at most one point removed and one point adjoined, the types of Table A3, and listed the feasible support systems of that shape up to translation and reflection of each support. We listed them by a meet-in-the-middle on the parity vectors $(\nu(s) \bmod 2)_s$; this gave a few hundred thousand systems at each of $w = 83$ and 89. The steps below describe the search of one half on one system.

(1) With the supports and the sums fixed (σ_f for the T half, $(1, 0, 0, 0)$ for the S half), list f consists of all sign vectors of its length ℓ and prescribed sum σ, $\binom{\ell}{(\ell+\sigma)/2}$ in number; the lengths are $|W_f|$ and $w - |W_f|$, which can be read off Table A3. This gives about 2^{38} per block at $w = 83$ and 2^{41} at $w = 89$, so each side of the matching has about 2^{76}, respectively 2^{82}, pairs.
(2) Treating the equations as independent gives a heuristic count of about 2^{17} solutions per half for the two systems marked † in Table A3.
(3) We partitioned both sides by the values of the pair sum at the largest shifts, where the equations have fewest terms, and matched one pair of corresponding parts at a time by hashing on the remaining shifts.

(4) Within a part we discarded every pair sum whose values at the remaining shifts were improbably large for a solution. This filter can also discard solutions; no other step of the matching can.
(5) We visited the likeliest parts first and stopped each half at its first solutions. Since a half has many solutions, only a small fraction of the pairs of step 1 is formed. The entries of Table 1 for these two orders are estimates for the two halves together; at order 716 the two halves cost about the same. Appendix D recomputes these estimates from the list sizes.

We took one support system per profile $(\nu(s))_s$, on which, apart from the list sizes, the heuristic count of step 2 depends, and searched an S half once its T half had a solution. Among the systems we searched, we found solutions on both halves for five at $w = 83$ and one at $w = 89$ (Table A3). The two marked there give the matrices of Table A2. The arc shape leaves a visible trace in the solutions. Write $v(y)$ for the vector $(a_f(y))_f$ of signs across the four blocks and pair y with $y + w$, as in §4.3. The pair $v(y), v(y + w)$ spans a line when y lies in all four supports or in none, and a plane otherwise; so the second case occurs exactly where the four supports disagree, at positions fixed by the support system before any sign is chosen. For the core of order 668 these are $y = 19, 39, 40, 42, 60, 61$: three near $w/2$, where arcs of different lengths end, and three isolated ones, a point removed from the centre of one arc and points adjoined near the antipodes of the centres of two others. For order 716 they are 23, 43–46 and 66, of the same two kinds. The isolated positions are where the feasibility conditions favour them. For a cyclic interval I in $\mathbb{Z}_w$, removing the point at its centre (when the length is odd) or adjoining the point antipodal to its centre (when it is even) changes $|I \cap (I+s)|$ by an even number at every s, because both points are fixed by the reflection of $\mathbb{Z}_w$ that preserves I; a point at distance d from these positions changes the parity of $|I \cap (I + s)|$ at $4d$ shifts. A hole at the centre or an extra near the antipode is therefore the way to change the size of a support by one while keeping the parity of every $\nu(s)$ under control, and for arcs that start at 0 and have length about $w/2$ these points lie near $w/4$ and $3w/4$. Random supports of the same sizes, aligned as favourably as possible by translating and reflecting each, typically disagree at 52–57 and 58–61 positions (at 49–58 and 56–63 over 400 random draws for each w).

5.3. **Width 4: order 1676.** For $1676 = 4 \cdot 418 + 4$ we take $G = \mathbb{Z}_2 \times \mathbb{Z}_{209}$, with $w = 209 = 11 \cdot 19$. The multiplier group $M = \langle 26 \rangle \leq \mathbb{Z}_{209}^*$, of order 15, acts on the second coordinate. It does not contain -1 and has 21 orbits on $\mathbb{Z}_{209}$ (twelve of size 15, six of size 3, two of size 5, and $\{0\}$), so there are 168 signs and 21 equations. We found the core by the decoupling (6) under M: the functions S_f and T_f are constant on orbits, with complementary supports, and each half of (6) is 10 equations, one per orbit of $\langle M, -1 \rangle$ on the non-zero elements of $\mathbb{Z}_{209}$. The twenty-first equation is the support-size condition of (6). We solved the S half first, by matching over all orbit-constant functions $\mathbb{Z}_{209} \to \{0, \pm 1\}$, keyed by support size and autocorrelation vector, with the four support sizes summing to $2w - 1$. The matching on these keys is the entry of Table 1. The T half, with one sign per orbit outside the support of S_f, is then a small exact matching, which we ran over solutions of the S half until some extended to cores.

5.4. **Width 4: order 1772.** For $1772 = 4 \cdot 442 + 4$ we take $G = \mathbb{Z}_2 \times \mathbb{Z}_{221}$, with $w = 221 = 13 \cdot 17$. The multiplier group $M = \langle 55 \rangle \leq \mathbb{Z}_{221}^*$, of order 12, acts on the second coordinate. Again $-1 \notin M$, and there are 200 signs and 29 equations. We found the core by the two-quotient lifting of §4.4, with $L_1 = \mathbb{Z}_{17}$ and $L_2 = \mathbb{Z}_{13}$. Miyamoto's decomposition was not used in this search; the resulting matrix is nonetheless an instance of his main theorem, like every matrix of Proposition 2 (§4.3). We found about $2.2 \cdot 10^{10}$ and 384 000 compressed solutions, on $G/\mathbb{Z}_{17}$ and on $G/\mathbb{Z}_{13}$. We decided compatibility block by block from the table of jointly realisable margins of §4.4, before any sign was chosen. Under a compatible pair there are at most 8100 decompressions per block, which we matched exactly on all 29 equations. The entry of Table 1 is governed by the two matchings that list the compressed solutions.

5.5. **Width 12: order 1916.** For $1916 = 4 \cdot 476 + 12$ we take $G = \mathbb{Z}_2^2 \times \mathbb{Z}_{119}$, $119 = 7 \cdot 17$, $N = \mathbb{Z}_{119}$ and $Q = \mathbb{Z}_2^2$. The multiplier group M, of order 12, is generated by $(x_1, x_2, y) \mapsto (x_2, x_1 + x_2, 115y)$ (of order 3 on $\mathbb{Z}_2^2$, while 115 has order 12 modulo 119), and there are 184 signs and 29 equations. We found the core by the two-quotient lifting of §4.4 through $G/\mathbb{Z}_7 \cong \mathbb{Z}_2^2 \times \mathbb{Z}_{17}$ and $G/\mathbb{Z}_{17} \cong \mathbb{Z}_2^2 \times \mathbb{Z}_7$. We found about $1.8 \cdot 10^4$ compressed solutions on the first quotient, determined for each of them the compatible compressed solutions on the second, and under compatible pairs listed the decompressions of each block and matched them on the remaining equations. The entry of Table 1 covers the first list and the matching up to the first core. Table A2 gives one such core, moved to the coset table of Table 2 (§3.3) and bordered by that frame, with

row sums $(6, 6, 38, 20)$. The move translates two of the blocks. This is why [23, Table 1] finds two generators of the released matrix invariant under a group of order 12 and the other two only under a group of order 4.

5.6. **Width 12, no symmetry: the second matrix of order 668.** For $668 = 4 \cdot 164 + 12$ we take $G = \mathbb{Z}_2^2 \times \mathbb{Z}_{41}$, $N = \mathbb{Z}_{41}$ and $Q = \mathbb{Z}_2^2$, and impose no symmetry, so there are 656 signs and 83 equations. We found the core by the fourfold decoupling (7) of §4.3, with $v = 167$, arranged so that the core condition becomes four independent systems on $\mathbb{Z}_{41}$, one per character θ of $\mathbb{Z}_2^2$, each of 20 equations in 40 signs (41 for $\theta = 1$).

Call $a_f(\cdot, y) \in \{\pm 1\}^Q$, for $y \in G'$, a *fibre*. A fibre is either $\pm\theta'$ for one character θ', and then $a_f^{(\theta)}(y) = \pm 2 \cdot 1\{\theta = \theta'\}$, or it has sum ± 2. In the second case all four values $a_f^{(\theta)}(y)$ are ± 1, with an odd number of minus signs, and we call the fibre *mixed*. A *pattern* is an assignment of a character or the label mixed to each (f, y). A pattern fixes every $\operatorname{supp} a_f^{(\theta)}$, and given the pattern the four conditions (7) share only the signs of the mixed fibres. A fibre $\pm\theta'$ contributes to the θ'-part only, so its sign is a variable of that one condition; a mixed fibre contributes ± 1 to all four θ-parts.

The fibre types of the core of order $668'$ in Table A2, with the values of the four θ-parts at a fibre of each type, are as follows.

fibre $a_f(\cdot, y)$	$(a^{(1)}, a^{(\theta_1)}, a^{(\theta_2)}, a^{(\theta_3)})$ at y	number in blocks $1, 2, 3, 4$	total
$\pm$ constant	$(\pm 2, 0, 0, 0)$	$10, 10, 12, 9$	41
$\pm\theta_1$	$(0, \pm 2, 0, 0)$	$10, 10, 8, 12$	40
$\pm\theta_2$	$(0, 0, \pm 2, 0)$	$10, 10, 8, 12$	40
$\pm\theta_3$	$(0, 0, 0, \pm 2)$	$10, 10, 12, 8$	40
mixed (sum ± 2)	$(\pm 1, \pm 1, \pm 1, \pm 1)$, odd number of minus signs	$1, 1, 1, 0$, all at $y = 0$	3

As checks, $4 \cdot 41 + 3 = 167 = v$ and $4 \cdot 40 + 3 = 163 = v - 4$, the second equation of (7), and $41 + 3 \cdot 40 + 3 = 164 = 4 \cdot 41$ is the number of fibres.

The pattern was fixed in the following steps; each is marked as forced by (7) or as chosen.

(1) *Number of mixed fibres: forced modulo 4, then chosen.* In the second equation of (7) for $\theta = 1$ a constant fibre contributes 4, a mixed fibre 1 and any other fibre 0, so the number of mixed fibres is 3 modulo 4, and we allowed exactly three. (Lemma 10 below gives this count for every core on a group $\mathbb{Z}_2^2 \times G'$ whose subgroup N meets $\mathbb{Z}_2^2 \times \{0\}$ trivially.)

(2) *Where they lie: forced, then chosen at no cost.* For $\theta \neq 1$ the coset table makes $\frac{1}{2}\hat{\beta}_f(\theta)$ equal to ± 1 in three blocks and 0 in the fourth, f_0 say (Appendix C), and in each block this value has the parity of the number of its mixed fibres. Hence block f_0 has no mixed fibre and each other block has one, which we put at $y = 0$ by translating the block.

(3) *The other fibres: forced.* By the same equations, of the other fibres in all four blocks, 41 are constant and, for each $\theta \neq 1$, 40 are $\pm\theta$.

(4) *Parity: chosen; balance: forced.* We also required the number of fibres assigned to each $\theta \neq 1$ to be even in every block. The sum conditions then force the values ± 2 of each non-trivial θ-part to be balanced within every block. They also force $a_f^{(\theta)}(0) = \frac{1}{2}\hat{\beta}_f(\theta)$ for $\theta \neq 1$ and $f \neq f_0$, and hence $a_f^{(1)}(0)$, since a mixed fibre has an odd number of minus signs. All signs of the mixed fibres are then fixed, so the four conditions (7) share no variable.

Lemma 10 (Mixed fibres are forced)**.** *Let $G = \mathbb{Z}_2^2 \times G'$, let $a_1, \dots, a_4$ be a core for (G, N), and suppose that $N \cap (\mathbb{Z}_2^2 \times \{0\}) = 0$. Let m be the number of mixed fibres in the four blocks together, and for each character θ of $\mathbb{Z}_2^2$ let c_θ be the number of fibres equal to $\pm\theta$. Then*

$$4c_1 + m = |G| + 3, \qquad 4c_\theta + m = |G| - 1 \quad (\theta \neq 1). \tag{8}$$

In particular $m \equiv 3 \pmod 4$, so every such core has at least three mixed fibres. For four blocks on G satisfying the Goethals–Seidel condition (2) instead, the same count gives $4c_\theta + m = |G|$ for every θ, so $m \equiv 0 \pmod 4$ and $m = 0$ is not excluded.

Proof. Write $P = \sum_f \mathrm{PAF}_{a_f}$. Since $\theta(x)\theta(x') = \theta(x' - x)$, expanding the square gives

$$\sum\nolimits_f \sum_{y \in G'} a_f^{(\theta)}(y)^2 = \frac{1}{4} \sum_{\zeta \in \mathbb{Z}_2^2} \theta(\zeta) P(\zeta, 0).$$

By (4), $P(0) = 4|G|$, and $P(\zeta, 0) = 4$ for $\zeta \neq 0$ because $(\zeta, 0) \notin N$. So the right side is $|G| + 3$ for $\theta = 1$ and $|G| - 1$ otherwise. On the left, a fibre $\pm\theta'$ contributes 4 to the sum for θ' and 0 to the others, and a mixed fibre contributes 1 to each. This gives (8), and $m \equiv 3 \pmod 4$ because $|G| = 4|G'|$. Under (2), $P(\zeta, 0) = 0$ for $\zeta \neq 0$, and the right side is $|G|$ for every θ. □

For the present cell, (8) is the second equation of (7). The lemma also applies to the cells of orders 1916 and 1436, where $N = \mathbb{Z}_{119}$ and $N = 2\mathbb{Z}_8 \times \mathbb{Z}_{11}$ meet $\mathbb{Z}_2^2 \times \{0\}$ trivially; their printed cores, found by lifting through quotients, have 219 of 476 and 203 of 352 fibres mixed, about half, against exactly three here.

We found a pattern and signs by growing the pattern one θ-part at a time, each stage a matching of two blocks against two on the 20 equations of that θ-part. The lists, one per block, consisted of a pattern for that θ-part together with balanced signs, and we took patterns symmetric under $y \mapsto -y$ in the three blocks that have a mixed fibre. For two non-trivial θ-parts in turn we sampled lists of about 10^4 patterns with signs per block among the fibres still free, and kept the first solution. For the third non-trivial θ-part we matched over all its patterns among the remaining fibres. For each distinct pattern among the solutions of this stage, the θ-part of the trivial character lives on the complementary fibres; we applied a parity test at each shift like the feasibility test of §4.3, then a matching over its 41 signs. We repeated these stages until a pattern carried a solution of the last one.

Any of the 9408 frames for its coset table, such as that of Table 2, borders the core (Theorem 5). The resulting matrix, in Table A2 with row sums $(14, -18, -2, -12)$, is inequivalent by 4-profiles [10] to every width-4 matrix of order 668 in [83]. The 4-profile of a Hadamard matrix records how often each value of $|\sum_j h_{aj}h_{bj}h_{cj}h_{dj}|$ occurs over the sets $\{a, b, c, d\}$ of four rows; it is unchanged by permuting and negating rows and columns.

The width-12 search was far smaller than the width-4 search at the same order (Table 1): the fourfold decoupling gives four conditions of 20 equations in about 40 signs each, instead of two conditions of 41 equations in about 166 signs each. The price is the three mixed fibres forced by Lemma 10. Fixing them first, all at $y = 0$, is what made the four conditions independent.

5.7. **Width 20: order 1388.** For $1388 = 4 \cdot 342 + 20$ we take $G = \mathbb{Z}_6 \times \mathbb{Z}_{57}$, $N = \mathbb{Z}_{57}$ and $Q = \mathbb{Z}_6$, so that $k = |N| = 57$ is odd. The multiplier group M, of order 6, is generated by $(x, y) \mapsto (-x, 11y)$, and there are 280 signs and 39 equations. We found the core by the sampled form of the two-quotient lifting (§4.4). Write $\mathbb{Z}_3'$ for the subgroup of order 3 of $\mathbb{Z}_{57}$.

(1) We found about $7.6 \cdot 10^6$ compressed solutions on $G/\mathbb{Z}_{19}$ (order 18, ten equations counting $d = 0$).
(2) The complementary quotient $G/\mathbb{Z}_3'$ (order 114, 16 equations, again counting $d = 0$, 12 of them not implied by those on $G/\mathbb{Z}_{19}$) is too large for its compressed solutions to be listed. Even under a single compressed solution on $G/\mathbb{Z}_{19}$ a block still has 2^{37}–2^{43} decompressions, too many for matching on the equations of $G/\mathbb{Z}_3'$. We therefore fixed one compressed solution on $G/\mathbb{Z}_{19}$, drew uniformly random decompressions of each block with the prescribed $\mathbb{Z}_{19}$-coset sums, and recorded their $\mathbb{Z}_3'$-coset sums. We drew 2^{20} of them for each block; uniform sampling is easy because the constraint splits into ten independent pieces, one per orbit of M on $G/\mathbb{Z}_{19}$.
(3) We then matched the sampled coset-sum vectors on the 16 equations of $G/\mathbb{Z}_3'$. This matching gave about $1.5 \cdot 10^5$ consistent quadruples of coset-sum data.
(4) Finally, for each resulting quadruple of coset-sum data consistent on both quotients, we listed all decompressions, only a few thousand per block, and matched them exactly on all 39 equations.

Table A2 gives one core found in this way, with row sums $(6, 10, 26, 24)$. The frame used is half-turn-invariant up to sign (Appendix C); the half-turn is $c \mapsto c + 3$ on all four segments.

5.8. **Width 28: order 1436.** For $1436 = 4 \cdot 352 + 28$ we take $G = \mathbb{Z}_2^2 \times \mathbb{Z}_8 \times \mathbb{Z}_{11}$ and, writing $x = (x_1, x_2, x_3, x_4) \in G$, put $\pi(x) = (x_1, x_2, x_3 \bmod 2)$, so that $N \cong \mathbb{Z}_4 \times \mathbb{Z}_{11}$ and $Q = \mathbb{Z}_2^3$. The group $M = \langle 3 \rangle \leq \mathbb{Z}_{11}^*$ of order 5 acts on the last coordinate, with 96 orbits per block (32 fixed points with $x_4 = 0$ and 64 orbits of size 5), so there are 384 signs and 51 equations. We sought cores with the *constant* coset table over $\mathbb{Z}_2^3$ (Appendix C): β_f constant except on one common coset, where it exceeds its other values by $2, 2, 2, 4$, its *excess*. Since $k = |N| = 44$ is even, the β_f are even-valued, so the row sums are $\equiv 2 \pmod{16}$ for the three blocks with excess 2 and $\equiv 4 \pmod{16}$ for the fourth. The condition $\sum_f \hat{\beta}_f(1)^2 = 1436$ then leaves three possibilities for the row sums, $\tau_1 = \{-30, -14, -14, -12\}$, $\tau_2 = \{-30, 18, -14, 4\}$, $\tau_3 = \{18, 18, 2, -28\}$ as multisets, the excesses being taken positive. The matrix of Table A2 has row sums τ_2.

The fixed-point signs satisfy a congruence of the classical kind [46, 73] (compare [60]).

Lemma 11 (A congruence modulo 20)**.** *Let $a_1, \dots, a_4$ be a core in this cell, let $L = \mathbb{Z}_{11}$, and for a coset c of L let $\xi_f(c)$ be the value of a_f at the M-fixed point of c. Then $\sum_f \mathrm{PAF}_{\xi_f}(d) \equiv \Lambda(d) \pmod{20}$ for $d \neq 0$ in G/L, where $\Lambda(d) = \sum_{s \in d} \sum_f \mathrm{PAF}_{a_f}(s)$.*

Proof. Each coset c of $L = \mathbb{Z}_{11}$ consists of one M-fixed point y_c and two orbits of size 5. Its sum is therefore $\xi(c) + 5\omega(c)$ with $\xi(c) = a(y_c) \in \{\pm 1\}$ and $\omega(c) \in \{0, \pm 2\}$. Now

$$\mathrm{PAF}_{\xi+5\omega}(d) - \mathrm{PAF}_{\xi}(d) = 25\mathrm{PAF}_{\omega}(d) + 5\sum_c \xi(c)\big(\omega(c+d) + \omega(c-d)\big),$$

and both $\mathrm{PAF}_\omega(d)$ and the last sum are divisible by 4. Indeed, $\mathrm{PAF}_\omega = 4\mathrm{PAF}_{\omega/2}$, and the last sum can be regrouped as $\sum_c \omega(c)\big(\xi(c-d) + \xi(c+d)\big)$, in which each term is a product of two even numbers. Hence compressing (4) to G/L (order 32) by (5) gives the congruence. □

The coset sums β_f, that is the coset table together with the row sums, also fix the sums of the ξ_f over N/L-cosets (the four cosets of L inside a coset of N), since such a sum is $\equiv \beta_f \pmod{10}$ and is one of $-4, -2, 0, 2, 4$, which are distinct modulo 10.

Lemma 12 (The row sums τ_1 do not occur)**.** *In this cell no core with the constant coset table has row sums τ_1.*

Proof. Take $d = (0, 0, 4)$, the element of order 2 of $N/L \cong \mathbb{Z}_4$; there $\Lambda(d) = 11 \cdot (-28) = -308 \equiv 12 \pmod{20}$. Translation by d maps each coset of N/L to itself, and the four signs of ξ on a coset contribute 4, 0 or ± 4 to $\mathrm{PAF}_\xi(d)$ according as their sum is ± 4, ± 2 or 0. For τ_1 these sums equal the β_f: -4 seven times and -2 once for the block of row sum -30; -2 seven times and 0 once for each block of row sum -14; -2 seven times and 2 once for the block of row sum -12. Hence $\sum_f \mathrm{PAF}_{\xi_f}(d) = 28 \pm 4 \pm 4$, which is 0, 8 or 16 modulo 20, never 12, contradicting Lemma 11. □

For τ_2 and τ_3 the same count gives $36 + 4j$ with j a sum of eight signs, which allows 12 (mod 20) (for $j = -6$ or 4). We continued with τ_2.

Write $4\mathbb{Z}_8$ and $2\mathbb{Z}_8$ for the subgroups of orders 2 and 4 of the $\mathbb{Z}_8$ factor. The subgroups used are

$$L = \mathbb{Z}_{11} < 4\mathbb{Z}_8 \times L < N = 2\mathbb{Z}_8 \times L, \qquad 4\mathbb{Z}_8 < 2\mathbb{Z}_8.$$

We generated compressed solutions on G/L with row sums τ_2 by a chain of matchings (§4.2) through $G/(4\mathbb{Z}_8 \times L)$; the one used fixes all $\xi_f(c)$ and $\omega_f(c)$ (notation of the proof of Lemma 11) and leaves one free sign on each coset with $\omega_f(c) = 0$. These signs enter the conditions compressed to $G/2\mathbb{Z}_8$ and $G/4\mathbb{Z}_8$ only through their sums over N/L-cosets and over pairs of L-cosets, so we matched on these quotients and on G, each level conditioned on the one above, in the nested lifting of §4.4:

step	matching on	order	what is determined
1	$G/(4\mathbb{Z}_8 \times L)$	16	compressed solutions with row sums τ_2
2	G/L	32	all $\xi_f(c)$ and $\omega_f(c)$, leaving free signs on 116 of the 128 cosets; run only as far as needed, and the first solution produced is used
3	$G/2\mathbb{Z}_8$	88	the 32 sums of the free signs over N/L-cosets
4	$G/4\mathbb{Z}_8$	176	their 64 sums over pairs of L-cosets
5	G	352	the signs

The three nested matchings found about $3.5 \cdot 10^4$, then about $4.1 \cdot 10^6$ consistent quadruples of sums, and finally the cores. Step 5 gave 9672 cores over the compressed solution on G/L fixed in step 2, all in [83], and the entry of Table 1 counts the whole computation for it. The constant-table frame of Appendix C, moved to their coset table, borders any of them, and Table A2 gives one.

6. Checking the matrices, and the data

6.1. **Recipes.** Each of the thirteen matrices can be rebuilt from the printed tables by one of three recipes. In Table A2 a hex string is zero-padded at the end: take the leading $|G|$ bits and drop the rest (for order 668 a block is 42 hex digits, 168 bits, of which the first 166 are used). For width 4 that table indexes the blocks cyclically, on $\mathbb{Z}_{2w}$; the isomorphism with the $\mathbb{Z}_2 \times \mathbb{Z}_w$ of Table 1 is $i \mapsto (i \bmod 2, i \bmod w)$. In

lexicographic order the last coordinate runs fastest: on $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ the element $(x_1, \ldots, x_r)$ has index $(\ldots((x_1 m_2 + x_2)m_3 + x_3)\ldots)m_r + x_r$, counting from 0.

Circulant orders 892, 1132, 1244, 1948, 1964 (v, t, g from Table 3; signs from Table A1; K is the array (1)):

```
1. M2 = (v-1)/t. For f = 1..4 read e0 and eps[0..M2-1].
2. a_f[0] = e0; a_f[ g^(j + M2*u) mod v ] = eps[j] for 0 <= j < M2, 0 <= u < t.
3. A_f[x][y] = a_f[(y-x) mod v]; R[x][y] = 1 if x+y = 0 mod v, else 0.
4. H = the array K(a_1,...,a_4). Check H H^T = 4v I.
```

Width 4: orders 668, 716, 1676, 1772 (blocks from Table A2; the array of Proposition 2):

```
1. a_f = the first 2w bits of the hex string, most significant bit first; bit 1 means -1.
2. A_f, R and the array K as above, modulo 2w.
3. H = [[C0, E0 (x) 1^T], [D0 (x) 1, K]], with 1 the all-ones column of length 2w:
   E0 (x) 1^T is 4 x 8w (each entry of E0 becomes a row of 2w equal entries), and
   D0 (x) 1 is 8w x 4 (each entry of D0 becomes a column of 2w equal entries).
   Check H H^T = (8w+4) I.
```

Widths 12, 20, 28: orders $668'$*, 1916, 1388, 1436* (blocks and frames from Table A2; Theorem 5):

```
1. Decode a_f as in the width-4 recipe (the first |G| bits), elements of G in lexicographic
   order. For 1436 the four blocks are printed in the order a_1,...,a_4 in which they enter
   the array, and their sums (-14, 18, -30, 4) are listed in that same order.
   A_f[x][y] = a_f(y-x) and R[x][y] = [x+y = 0], computed in G.
   pi(x) = (x1,x2) for 668' and 1916; pi(x) = x1 for 1388; pi(x) = (x1,x2,x3 mod 2) for 1436.
2. Decode the b words of row D (columns of D_Q) and of row E (rows of E_Q): 4q bits each,
   most significant bit first, bit 1 meaning -1; bit number f*q + (index of c in Q),
   f = 0..3, is the entry at block position f+1 and coset c (Q in lexicographic order).
3. beta_f[c] = sum of a_f[x] over the x with pi(x) = c.
4. K = the array K over G from the a_f; Kb = the same array over Q from the beta_f.
5. C = -(E_Q Kb^T D_Q)/(4q). Check that every entry is +1 or -1.
6. D[(f,x)][j] = D_Q[(f,pi(x))][j]; E[i][(f,x)] = E_Q[i][(f,pi(x))].
7. H = [[C, E], [D, K]]. Check H H^T = n I.
```

The three recipes, run on Tables A1 and A2 as printed in exact integer arithmetic, give thirteen matrices with $HH^{\mathsf{T}} = nI$. The core conditions (2), (3) and (4) and the stated row sums also hold. Every block is invariant under the multiplier group stated for its cell, after undoing the translations noted for order 1916. The matrix of Figure 2 is a Hadamard matrix with a Hadamard corner. The row sums and the numbers of multiplier orbits agree with [23, Tables 1–2].

6.2. **Relation to the public files.** The files released publicly before this paper [1] give one matrix of each of the twelve orders, as a decoder script and an encoded list of signs. They are built from the sequences and blocks of Tables A1 and A2, with two differences of convention. (i) For nine orders, the four of width 4 and the five circulant ones, they use $R = (1\{x + y = -1\})$ in place of $R = (1\{x + y = 0\})$. For the five circulant orders the two matrices differ only by shifting the rows and columns of every block by $(v + 1)/2$, which fixes each A_f and carries one R to the other. For the four width-4 orders no such shift exists, and they are different Hadamard matrices from the same sequences; for order 668 the released one is inequivalent to that of Table A2. (ii) For order 1388 they index G as $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{57}$ instead of $\mathbb{Z}_6 \times \mathbb{Z}_{57}$, identifying $u \in \mathbb{Z}_6$ with $(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ by $u = 3x + 2y$, that is $x = u \bmod 2$ and $y = -u \bmod 3$. This is not the usual map $u \mapsto (u \bmod 2, u \bmod 3)$. For order 1916 the printed blocks are those of the released matrix.

6.3. **Cost of the searches.** Appendix D estimates what the pair sums counted in Table 1 cost, from timings of the two inner loops of a matching and from the current list price of rented processors (Table D1). The search for order 716 dominates: $2 \cdot 10^7$ to $8 \cdot 10^7$ core-hours, about US$1–4 million, which at the counts of Table 1 is more than nine tenths of the total. The width-4 search for order 668 and the circulant searches for orders 1132 and 1964 cost between $7 \cdot 10^4$ and $6 \cdot 10^5$ core-hours each, and the other nine searches together under 5 000 core-hours. These figures cover the counted operations only. The hardware and the time actually used are not recorded in this paper.

6.4. **The supplementary data.** The supplementary data [83] hold the thirteen matrices with their defining data, the frame catalogues of Appendix C, and the further cores and matrices mentioned in the text, all in the conventions of this paper. A script rebuilds every matrix from its defining data and re-checks $HH^{\mathsf{T}} = nI$,

the defining conditions and every frame and core stated or listed; it also recounts the admissible coset tables, but it does not check that the lists of frames, cores or solutions are complete. Apart from the constraint solver mentioned in §1 and existing libraries, all programs were written for this work, mainly in C, C++ and Python. The search programs themselves are not part of [83].

Solutions of the two halves on the same supports combine freely, and one system at $w = 83$ gave two T- and three S-solutions, so the solutions used give $6 + 1 + 1 + 1 + 1 = 10$ matrices of order 668, pairwise inequivalent by their 4-profiles [10]. The data [83] contain these and further inequivalent matrices of order 668, at least 20 in all; the further ones are the matrix of §5.6 and matrices obtained by reordering the blocks before assembly or by the convention $R = (1\{x + y = -1\})$ of the public files (§6.2).

Data availability. Theorem 1 rests only on Appendix A. The supplementary data [83] have not been publicly deposited.

7. Related work

Arrays and borders. Borders of widths 1, 2 and 4 are in the literature: width 1 in Paley's construction [59], width 2 in the constructions with two circulant cores [26, 40] (see also [70, 53] and the paragraph on Legendre pairs below), and width 4 in the array of Wallis and Whiteman [77, Thm. 4.17]. The closest construction we know is that of Momihara and Yamada [57, Thm. 4.1], who border a two-block divisible difference family relative to a subgroup of index $u - 1$ by all rows but the first of a Hadamard matrix of order u, pulled back from the quotient group, with corner $-\mathbf{1}\mathbf{1}^{\mathsf{T}}$, and obtain symmetric Hadamard matrices of order u^2. Theorem 5, recovered from the released matrices as [23, Thm. 7], has since given orders 2636 and 3964 (Kumar [45]) and 5788 and 8476 (Egan et al.; 8476 had been settled earlier by Jones [35], from T-matrices of order 163) with $q = 4$ and order 3356 (Kumar [45]) with $q = 8$, and a related border of width 12 relative to a subgroup of index 3 gave order 2148 [45]. Relative difference sets [25] are the divisible difference families of §3.2 with no differences in $N \setminus \{0\}$.

Miyamoto's construction and M-structures. Miyamoto's main theorem [56, §4] gives a Hadamard matrix of order $8m+4$ from a pair of $(0, \pm 1)$-matrices of order $4m$ whose sum and difference are ± 1 matrices, under a condition on row sums and one further condition on each matrix of the pair (§4.3). The four width-4 matrices of this paper, of orders 668, 716, 1676 and 1772, are instances of that theorem: the pair consists of the Goethals–Seidel arrays of the half-sums S_f and of the half-differences T_f of the two halves of the four blocks. What differs is the source of the pair. Miyamoto builds his pairs from conference matrices and other auxiliary matrices [56, §5], and the related constructions of Yamada [82] likewise start from an auxiliary Hadamard, skew-Hadamard or conference matrix of order comparable to the blocks. Our pairs were found by computer search: for orders 668, 716 and 1676 by solving the condition on the half-sums and the condition on the half-differences separately, which is possible because the two are tied only through their supports (§§5.2, 5.3), and for order 1772 by lifting through two quotients (§5.4). The core of $668'$ was found with the analogous decomposition along $\mathbb{Z}_2^2$, which has four parts (§5.6); Miyamoto's theorem does not apply to it, and we make no statement relating the matrices with wider borders to his theorem. Seberry and Yamada restated Miyamoto's theorem in terms of M-structures [64, Thm. 34], [65, Thm. 8.10] and proved multiplication theorems for Hadamard and Williamson-type matrices in the same terms [64, 66]; see also [67]. Egan et al. note that a symmetry hypothesis is missing from Corollary 2 of [56] and Corollary 8.8(1) of [65] (see [23, Remark 8]). That hypothesis concerns those corollaries, not the main theorem.

Legendre pairs. A Legendre pair of length ℓ is a pair of ± 1 sequences a, b of length ℓ with $\mathrm{PAF}_a(s) + \mathrm{PAF}_b(s) = -2$ for all $s \neq 0$; it gives a Hadamard matrix of order $2\ell+2$ with two circulant cores and a border of width 2. The array, and the equivalent condition on a pair of subsets of an abelian group of odd order, go back to Szekeres [70, 71]: his complementary difference sets are such pairs with one block skew, which he built from cyclotomic classes to obtain skew Hadamard matrices. The existence criterion with no skewness and no cyclotomic structure, for an arbitrary odd length, was formulated independently by Medianik [53], as his basic lemma on Hadamard matrices of half-circulant type (two n-subsets of $\mathbb{Z}_{2n-1}$ whose differences together cover every non-zero element exactly n times), and by Fletcher, Gysin and Seberry [26], who named the pairs and searched for them by the discrete Fourier transform. Medianik's Theorems 1 and 2 recover the prime lengths from quadratic residues, with the remark that the resulting matrices are not of the form of Paley's matrices of the same order, and [54] adds products of twin primes. The conjecture that a Legendre pair exists for every odd ℓ, Kotsireas's structured Hadamard conjecture [37], would imply the Hadamard

conjecture. The length-333 conjecture of [38] mentioned in §1.1 is of this kind; the matrices of order 668 given here are of a different form, and the Legendre quadruples of §3.1 are the width-4 analogue.

Multipliers and matching. The Goethals–Seidel array is recalled in §2. With circulant blocks it generalises Williamson's method [80] and has been the setting of most computer constructions since Đoković [14]. Infinite families of Williamson matrices are known [74], but some odd orders have none: 35 [15], and 47, 53 and 59 [32]. Blocks invariant under a multiplier group go back to Hunt and Wallis [34] (see also [30]), and Đoković [17, 18] and Đoković, Golubitsky and Kotsireas [20] combine them with candidate lists and meet-in-the-middle matching [41], the method of five of our orders (§2.1).

Compression. Compression is a tool also used for difference sets [2, 46, 73]. As in [21] and the recent searches for Legendre pairs and periodic Golay pairs [42, 43, 52, 72], we solve the compressed problem first and lift its solutions afterwards. The change of variables of §4.3 is, along $\mathbb{Z}_2$, Miyamoto's decomposition [56, 64]; it is also the classical sum-and-difference device of base and T-sequences [65, 75], and $2S$ is the 2-compression of a [21]. Kotsireas, Koutschan and Winterhof [44] also treat the two cosets $a(0,\cdot)$, $a(1,\cdot)$ separately, fixing one sum on each, whereas in the variables S, T all the constraints separate.

T-matrices. T-matrices go back to Cooper and Wallis [11] and, as four-symbol δ-codes, to Turyn [75]; they give Hadamard matrices of order $4v$ in the Goethals–Seidel array [65, Thm. 3.6], and these constructions can be phrased in terms of orthogonal designs [28]. Their relation to the quadruples of this paper is that of Turyn [75, Thm. 2]. Identify the block index f with $\mathbb{Z}_2^2$ and put $t_\theta(x) = \frac{1}{4}\sum_f \theta(f) a_f(x)$ for the four characters θ of $\mathbb{Z}_2^2$. Since the character table of $\mathbb{Z}_2^2$ is a Hadamard matrix of order 4,

$$\sum\nolimits_f \mathrm{PAF}_{a_f}(s) = 4\sum_\theta \mathrm{PAF}_{t_\theta}(s) \qquad (s \in G). \tag{9}$$

If $\prod_f a_f(x) = +1$ at every x, the t_θ are $(0,\pm1)$-functions with disjoint supports covering G, and (2) says exactly that their group matrices are T-matrices; this is the case $s = 1$ of the product theorem of Seberry and Yamada for M-structures [64, Thm. 4], whose original version is Turyn's [75, Thm. 9], as stated in [23, §4]. None of the thirteen cores is of this kind, even after the moves of §3.3: for each of them, the number of x with $\prod_f a_f(x) = -1$, minimised over translations and inversions of single blocks and over the choice of sign class, is between 19% and 37% of $|G|$. For ten of the cores this lies within the range found for random quadruples with the same row sums and multiplier group. The cores of orders 716 and 668 (width 4), which have arc supports, and the core of order 1436 are lower than about 99% of such quadruples: 25%, 25% and 19%, against medians of 29%, 28% and 24%. Orders 668 and 716 would also follow from Turyn-type sequences $TT(56)$ and $TT(60)$, as Best, Đoković, Kharaghani and Ramp pointed out [4] (see [23, §3]); $TT(n)$ is known for even $n \le 44$ [4, 50] and, by a further search of London and Kotsireas cited in [23, Table 3], for $n = 46$, and that table lists the orders at which T-matrices are known, among them recent ones of Schneider [62], Schumer [63] and Jones [35]. Kharaghani and Tayfeh-Rezaie obtained order 428 in this way, from Turyn-type sequences of length 36 [36], and London [49] and London and Kotsireas [50] construct further Turyn-type sequences.

Low-autocorrelation sequences. The quantity F minimised in §5.1 is, up to the factor $2t$, the energy $\sum_{s\neq0}\mathrm{PAF}_a(s)^2$ of Bernasconi's Ising model [3] with periodic boundary conditions. Configurations of the periodic model with a single off-peak autocorrelation value of least possible size (the *perfect sequences* of Mertens and Bessenrodt, which are ground states) correspond to cyclic difference sets [55], and conditions (2), (3) and (4) are the analogous statements for four sequences with prescribed sums of autocorrelations. Objective functions of this kind underlie earlier heuristic and annealing searches for Hadamard matrices and complementary sequences [8, 39, 69].

Analysis of the released matrices, and current status. Egan, Kotsireas, London and Ó Catháin [23] analysed the twelve matrices released in [1]: the groups, borders, multiplier groups and row sums of their generators, and the flatness of their spectra. The release gave the matrices without any account of how they were found, and their reading of the structure from the data alone, including the recovery of Theorem 5, is accurate in every particular that this paper can check. Their paper is also a survey of the constructions that reach orders up to 10 000. It gives matrices of sixteen orders that had no published construction, five of which Schumer [63] and Jones [35] had already posted; it notes twenty-two more that others settled while it was being written, most of them by Cooley [9] and Kumar [45]; and it counts 95 orders up to 10 000 as open when it appeared, the least being 2396. This paper is confined to how thirteen matrices were found; theirs is the survey of the field as it now stands. Their list of open problems includes questions on group-developed

matrices; for the general theory of such matrices see [33, 13]. Kumar's repository [45] holds matrices, each with a certificate and an exact verifier, at 34 of the orders that [7, Table 4] lists as unresolved, up to 11 804. Four of them, 3732, 4492, 5020 and 5932, are among the sixteen constructed in [23], there with multiplier groups of the same orders 31, 33, 50 and 39; Kumar's are dated in his repository to commits of 11 and 13 October 2026, with a first dated release on 14 October, and [23] appeared on 19 October. Cooley's repository [9] has another matrix of order 3732, different from Kumar's.

The width-4 array and its names. Proposition 2 appears in several forms. Spence [68, Thm. 2.1] states it for the cyclic group in terms of the complementary sets 4-$\{2w; w+1, w, w, w; 2w\}$ (restated as [7, Thm. 7]), and Yamada [82, Thm. 1] states the same border around a quaternion-type array. For blocks as in Proposition 2, the sets $X_f = \{a_f = -1\}$ form a difference family [76, Lemma 1] with parameters $(2w; w-1, w, w, w; 2w-2)$, of a kind considered by Whiteman [78] and Spence [68] and called type H_4^* in [47, 48]. Egan, Kotsireas, London and Ó Catháin call such quadruples Legendre quadruples [23, §2.1].

Orders 892, 1132 and 1948. Lou, Xia and Xia [51], which we have been unable to consult, describe a construction method for T-matrices of prime order $6m+1 = a^2+3b^2$ (which would give Hadamard matrices of order $4(6m+1)$ [65]); its abstract names no order, and its predecessor [81] is a computer search reaching $6m+1 \le 79$. The primes 223, 283 and 487 are of that form, but the later lists still give 892 [7, 19], 1132 and 1948 [7] as open, so as far as we can tell these orders are not settled there.

Acknowledgements. This work was supervised by Levent Alpöge, Saul Reynolds-Haertle and Philippe Voinov, who followed it with curiosity and encouragement and made no mathematical contribution. We thank Erisa Hasani, Abhinav Nellore and Rachel Ward for the corrections of attribution and emphasis that they proposed (§1.4) and for their help with the description of the solutions found without symmetry.

Disclosure. Erisa Hasani, Abhinav Nellore and Rachel Ward wish to disclose that they received no payment from Anthropic for their work on this paper and signed no non-disclosure agreement.

References

[1] L. Alpöge, P. Voinov and S. Reynolds-Haertle, Hadamard matrices of orders 668, 716, 892, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948 and 1964, announcement with data, 12 August 2026; see https://epoch.ai/frontiermath/open-problems/hadamard.

[2] L. D. Baumert and D. M. Gordon, On the existence of cyclic difference sets with small parameters, in: *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, Fields Inst. Commun. 41, Amer. Math. Soc., 2004, 61–68; arXiv:math/0304502.

[3] J. Bernasconi, Low autocorrelation binary sequences: statistical mechanics and configuration space analysis, *J. Physique* 48 (1987) 559–567.

[4] D. Best, D. Ž. Đoković, H. Kharaghani and H. Ramp, Turyn-type sequences: classification, enumeration, and construction, *J. Combin. Des.* 21 (2013) 24–35.

[5] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Vol. I, 2nd ed., Encyclopedia Math. Appl. 69, Cambridge University Press, 1999.

[6] C. Bright, I. S. Kotsireas and V. Ganesh, Applying computer algebra systems with SAT solvers to the Williamson conjecture, *J. Symbolic Comput.* 100 (2020) 187–209.

[7] M. Cati and D. V. Pasechnik, A database of constructions of Hadamard matrices, arXiv:2411.18897v2, 2025.

[8] M. Chiarandini, I. S. Kotsireas, C. Koukouvinos and L. Paquete, Heuristic algorithms for Hadamard matrices with two circulant cores, *Theoret. Comput. Sci.* 407 (2008) 274–277.

[9] T. Cooley, Hadamard matrices from Claude Code searches, GitHub repository, https://github.com/Middletownbooks/Hadamard, 2026.

[10] J. Cooper, J. Milas and W. D. Wallis, Hadamard equivalence, in: *Combinatorial Mathematics* (Canberra 1977), Lecture Notes in Math. 686, Springer, 1978, 126–135.

[11] J. Cooper and J. Wallis, A construction for Hadamard arrays, *Bull. Austral. Math. Soc.* 7 (1972) 269–277.

[12] R. Craigen and H. Kharaghani, Hadamard matrices and Hadamard designs, in: *Handbook of Combinatorial Designs*, Chapman & Hall/CRC, 2007, 273–280.

[13] W. de Launey and D. L. Flannery, *Algebraic Design Theory*, Math. Surveys Monogr. 175, Amer. Math. Soc., 2011.

[14] D. Ž. Đoković, Construction of some new Hadamard matrices, *Bull. Austral. Math. Soc.* 45 (1992) 327–332.

[15] D. Ž. Đoković, Williamson matrices of order $4n$ for $n = 33, 35, 39$, *Discrete Math.* 115 (1993) 267–271.

[16] D. Ž. Đoković, Two Hadamard matrices of order 956 of Goethals–Seidel type, *Combinatorica* 14 (1994) 375–377.

[17] D. Ž. Đoković, Hadamard matrices of order 764 exist, *Combinatorica* 28 (2008) 487–489.

[18] D. Ž. Đoković, Supplementary difference sets with symmetry for Hadamard matrices, *Oper. Matrices* 3 (2009) 557–569.

[19] D. Ž. Đoković, Two classes of Hadamard matrices of Goethals–Seidel type, arXiv:2404.14375v3, 2024.

[20] D. Ž. Đoković, O. Golubitsky and I. S. Kotsireas, Some new orders of Hadamard and skew-Hadamard matrices, *J. Combin. Des.* 22 (2014) 270–277.

[21] D. Ž. Đoković and I. S. Kotsireas, Compression of periodic complementary sequences and applications, *Des. Codes Cryptogr.* 74 (2015) 365–377.

[22] D. Ž. Đoković and I. S. Kotsireas, Computational methods for difference families in finite abelian groups, *Spec. Matrices* 7 (2019) 127–141.

[23] R. Egan, I. S. Kotsireas, S. London and P. Ó Catháin, Recent progress in the construction of Hadamard matrices, arXiv:2610.27175v1, 2026.

[24] S. Eliahou, A 64-modular Hadamard matrix of order 668, *Australas. J. Combin.* 93(2) (2025) 422–427.

[25] J. E. H. Elliott and A. T. Butson, Relative difference sets, *Illinois J. Math.* 10 (1966) 517–531.

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

[27] D. Gale, A theorem on flows in networks, *Pacific J. Math.* 7 (1957) 1073–1082.

[28] A. V. Geramita and J. Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, New York, 1979.

[29] J. M. Goethals and J. J. Seidel, A skew Hadamard matrix of order 36, *J. Austral. Math. Soc.* 11 (1970) 343–344.

[30] M. Gysin and J. Seberry, An experimental search and new combinatorial designs via a generalisation of cyclotomy, *J. Combin. Math. Combin. Comput.* 27 (1998) 143–160.

[31] J. Hadamard, Résolution d'une question relative aux déterminants, *Bull. Sci. Math.* 17 (1893) 240–246.

[32] W. H. Holzmann, H. Kharaghani and B. Tayfeh-Rezaie, Williamson matrices up to order 59, *Des. Codes Cryptogr.* 46 (2008) 343–352.

[33] K. J. Horadam, *Hadamard Matrices and Their Applications*, Princeton University Press, 2007.

[34] D. C. Hunt and J. Wallis, Cyclotomy, Hadamard arrays and supplementary difference sets, *Congr. Numer.* 7 (1973) 351–381.

[35] J. D. Jones, Hadamard-T: T-matrix witnesses and the Hadamard orders they close, GitHub repository, https://github.com/JD-Jones-ASES/Hadamard-T, version 0.1.0, 29 August 2026.

[36] H. Kharaghani and B. Tayfeh-Rezaie, A Hadamard matrix of order 428, *J. Combin. Des.* 13 (2005) 435–440.

[37] I. S. Kotsireas, Structured Hadamard conjecture, in: *Number Theory and Related Fields: In Memory of Alf van der Poorten*, Springer Proc. Math. Stat. 43, Springer, 2013, 215–227.

[38] I. S. Kotsireas, R. Gallardo-Cava, A. I. Gómez and D. Gómez-Pérez, On the search of binary Legendre pairs of length pq^2, *J. Symbolic Comput.* 138 (2027) 102606.

[39] I. S. Kotsireas, C. Koukouvinos, P. M. Pardalos and O. V. Shylo, Periodic complementary binary sequences and combinatorial optimization algorithms, *J. Comb. Optim.* 20 (2010) 63–75.

[40] I. S. Kotsireas, C. Koukouvinos and J. Seberry, Hadamard ideals and Hadamard matrices with two circulant cores, *European J. Combin.* 27 (2006) 658–668.

[41] I. S. Kotsireas, C. Koukouvinos and J. Seberry, Weighing matrices and string sorting, *Ann. Comb.* 13 (2009) 305–313.

[42] I. S. Kotsireas and C. Koutschan, Legendre pairs of lengths $\ell \equiv 0 \pmod 3$, *J. Combin. Des.* 29 (2021) 870–887.

[43] I. S. Kotsireas, C. Koutschan, D. A. Bulutoglu, D. M. Arquette, J. S. Turner and K. J. Ryan, Legendre pairs of lengths $\ell \equiv 0 \pmod 5$, *Spec. Matrices* 11 (2023) 20230105.

[44] I. S. Kotsireas, C. Koutschan and A. Winterhof, Quaternary Legendre pairs II, *Discrete Math.* 348 (2025), no. 9, 114501.

[45] K. Kumar, New Hadamard matrices, GitHub repository, https://github.com/vatskishan03/Hadamard, version 2.1.0, 29 October 2026.

[46] E. S. Lander, *Symmetric Designs: An Algebraic Approach*, London Math. Soc. Lecture Note Ser. 74, Cambridge University Press, 1983.

[47] K. H. Leung and K. Momihara, New constructions of Hadamard matrices, *J. Combin. Theory Ser. A* 171 (2020) 105160.

[48] K. H. Leung, K. Momihara and Q. Xiang, A new family of Hadamard matrices of order $4(2q^2+1)$, *Discrete Math.* 344 (2021) 112163.

[49] S. London, *Constructing New Turyn Type Sequences, T-Sequences and Hadamard Matrices*, PhD thesis, University of Illinois at Chicago, 2013.

[50] S. London and I. S. Kotsireas, New Turyn-type sequences, *Cryptogr. Commun.* 17 (2025) 1601–1610.

[51] L. Lou, M. Xia and T. Xia, On T-matrices of order $6m+1$, *Adv. Appl. Discrete Math.* 21 (2019), no. 2, 163–181.

[52] T. Lumsden, I. S. Kotsireas and C. Bright, New results on periodic Golay pairs, *Math. Comp.* 95 (2026) 1517–1539.

[53] A. I. Medianik, Regular simplex inscribed into a cube and Hadamard matrix of half-circulant type, *Mat. Fiz. Anal. Geom.* 4 (1997) 458–471 (in Russian).

[54] A. I. Medianik, Regular simplex inscribed into a cube, half-circulant Hadamard matrices and Gaussian sums, *Mat. Fiz. Anal. Geom.* 8 (2001) 58–81 (in Russian).

[55] S. Mertens and C. Bessenrodt, On the ground states of the Bernasconi model, *J. Phys. A* 31 (1998) 3731–3749.

[56] M. Miyamoto, A construction of Hadamard matrices, *J. Combin. Theory Ser. A* 57 (1991) 86–108.

[57] K. Momihara and M. Yamada, Divisible difference families from Galois rings $GR(4,n)$ and Hadamard matrices, *Des. Codes Cryptogr.* 73 (2014) 897–909.

[58] OEIS Foundation Inc., Number of Hadamard matrices of order $4n$ (whose notes record the orders for which none is known), Entry A007299 in *The On-Line Encyclopedia of Integer Sequences*, https://oeis.org/A007299, accessed 2026.

[59] R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys.* 12 (1933) 311–320.

[60] A. F. Ramos, D. B. Hulak and R. J. G. B. de Queiroz, Multiplier obstructions for Legendre pairs of length 333, *J. Combin. Des.*, published online 28 October 2026, doi:10.1002/jcd.70044; arXiv:2607.20765v2.

[61] H. J. Ryser, Combinatorial properties of matrices of zeros and ones, *Canad. J. Math.* 9 (1957) 371–377.

[62] L. Schneider, hadamard-2060, GitHub repository, https://github.com/schneiderlo/hadamard-2060, 2026.
[63] A. Schumer, Periodic T-matrices of order 151 and a skew spin Goethals–Seidel family over $\mathbb{Z}/919\mathbb{Z}$: certificates and Hadamard constructions of orders 3676, 5436, 6644 and 7852, Zenodo, https://doi.org/10.5281/zenodo.22820997, version 1.0.0, 17 September 2026.
[64] 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.
[65] J. Seberry and M. Yamada, Hadamard matrices, sequences, and block designs, in: *Contemporary Design Theory: A Collection of Surveys*, Wiley, 1992, 431–560.
[66] J. Seberry and M. Yamada, On the multiplication theorems of Hadamard matrices of generalized quaternion type using M-structures, *J. Combin. Math. Combin. Comput.* 13 (1993) 97–106.
[67] J. Seberry and M. Yamada, *Hadamard Matrices: Constructions using Number Theory and Algebra*, Wiley, 2020.
[68] E. Spence, Hadamard matrices from relative difference sets, *J. Combin. Theory Ser. A* 19 (1975) 287–300.
[69] A. B. Suksmono and Y. Minato, Quantum computing formulation of some classical Hadamard matrix searching methods and its implementation on a quantum computer, *Sci. Rep.* 12 (2022), doi:10.1038/s41598-021-03586-0.
[70] G. Szekeres, Tournaments and Hadamard matrices, *Enseign. Math.* 15 (1969) 269–278.
[71] G. Szekeres, A skew Hadamard matrix of order 52, *Canad. J. Math.* 21 (1969) 1319–1322.
[72] J. S. Turner, I. S. Kotsireas, D. A. Bulutoglu and A. J. Geyer, A Legendre pair of length 77 using complementary binary matrices with fixed marginals, *Des. Codes Cryptogr.* 89 (2021) 1321–1333.
[73] R. J. Turyn, Character sums and difference sets, *Pacific J. Math.* 15 (1965) 319–346.
[74] R. J. Turyn, An infinite class of Williamson matrices, *J. Combin. Theory Ser. A* 12 (1972) 319–321.
[75] R. J. Turyn, Hadamard matrices, Baumert–Hall units, four-symbol sequences, pulse compression, and surface wave encodings, *J. Combin. Theory Ser. A* 16 (1974) 313–333.
[76] J. Wallis and A. L. Whiteman, Some classes of Hadamard matrices with constant diagonal, *Bull. Austral. Math. Soc.* 7 (1972) 233–249.
[77] W. D. Wallis, A. P. Street and J. S. Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices*, Lecture Notes in Math. 292, Springer, 1972.
[78] A. L. Whiteman, Hadamard matrices of order $4(2p+1)$, *J. Number Theory* 8 (1976) 1–11.
[79] G. Williamson, O. Yacobi and P. Zinn-Justin, Generating Hadamard matrices with transformers, arXiv:2604.11101v2, 2026.
[80] J. Williamson, Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.* 11 (1944) 65–81.
[81] M. Xia, T. Xia, J. Seberry and H. Qin, Construction of T-matrices of order $6m+1$, *Far East J. Math. Sci.* 101 (2017), no. 8, 1731–1749.
[82] M. Yamada, Some new series of Hadamard matrices, *J. Austral. Math. Soc. Ser. A* 46 (1989) 371–383.
[83] Supplementary data for this paper (sequences, blocks, frames, matrices and scripts). Not publicly deposited.

Appendix A. Defining data

Encoding of Table A2. A block a_f on $G = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ is the bit string $(1\{a_f(x) = -1\})_{x \in G}$, with x in lexicographic order of $(x_1, \ldots, x_r)$, $0 \le x_i < m_i$. It is written in hexadecimal, most significant bit first, zero-padded at the end to a multiple of four bits. The blocks are listed in the order $a_1, \ldots, a_4$ in which they enter $K(a_1, \ldots, a_4)$ in (1), with A_f and R as in §1.5.

For width $b = 4$ the blocks are indexed cyclically ($\mathbb{Z}_{2w} \cong \mathbb{Z}_2 \times \mathbb{Z}_w$ by the Chinese remainder theorem). The four sequences on $\mathbb{Z}_{2w}$ satisfy $\sum_f \mathrm{PAF}_{a_f}(s) = -4$ for $s \ne 0$ with row sums $(2, 0, 0, 0)$, and the matrix is that of Proposition 2: the printed blocks go into it as they stand.

For order 1916 the blocks printed below are those of the released matrix, i.e. translates within Q of M-invariant blocks, the translation being the move that fits them to the printed frame. The M-invariance statement of §5.5 refers to the untranslated blocks, and the row sums are $(6, 6, 38, 20)$. For order 1436 the blocks are printed in the order $(-14, 18, -30, 4)$ of their sums (row sums τ_2 of §5.8).

For $b \ge 12$ the quotient map $\pi\colon G \to Q$ is the projection to the first two coordinates ($Q = \mathbb{Z}_2^2$), to the first coordinate ($Q = \mathbb{Z}_6$), or $x \mapsto (x_1, x_2, x_3 \bmod 2)$ ($Q = \mathbb{Z}_2^3$, for $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_{11}$). Rows D and E list the b columns of D_Q and the b rows of E_Q, each a word of $4q$ bits (block position $f = 1, \ldots, 4$ major, Q in lexicographic order minor, bit 1 for entry -1) in hexadecimal. The corner is $C = -E_Q K_\beta^{\mathsf{T}} D_Q/(4q)$ and $H = \left(\begin{smallmatrix} C & E \\ D & K \end{smallmatrix}\right)$ with D, E the pull-backs along π (Theorem 5).

Table A1. The sequences of the circulant constructions of §5.1 (orders 892, 1132, 1244, 1948, 1964): for each a_f the value $e_0 = a_f(0)$ followed by $\varepsilon_0\varepsilon_1 \cdots \varepsilon_{2m-1}$, where ε_j is the value of a_f on $O_j = \{g^{j+2mu} \bmod v : 0 \le u < t\}$, with v, t, g, m as in Table 3: $(v, t, g) = (223, 3, 3)$, $(283, 3, 3)$, $(311, 5, 17)$, $(487, 9, 3)$, $(491, 7, 2)$, $2m = (v - 1)/t$.

```
 892  a1  - --+-+++-++----++++--+-+--+++-+-+---++--+---++++++-++--+-+---+-+-+---++++++
      a2  - -+---+-++--++-++--+++-+++-+-+-++++--++-+---+---+----++--+++-++--+--+++-+++
      a3  - --+--++-++++-++-++++--++--+-++-++-++-+-+-++--+++-+--+--+-++--+-+------+-+
      a4  - +++-+--+-------+-+++-++++--+-+---++----++++---++++-+-++++-+-+--+-+++-++++
1132  a1  + ++---+++-+-++---++-+-++-++-----+------+-++-++--+++-+-+-++++-++-+--+++---++++-++----+--++-+--++
      a2  + +-+-+----+-++-++++-++--+-+-++-++-+-+++-++-+-++----++-+--+++-++-+----++++-++-+-++---+---+--+-++
      a3  + ---++--+-++++++++-+++-+-+++--++-+++--++-+-+-+++---+++--++++--+-++--+---+--------+--+--++++--+
      a4  + ---+----+---+--++-+-+---++-++++--+-+++++++--+++-+-++-++---+++----+--+--+--++-++--++++++----++
1244  a1  + --++-+-++------++++-++-+--++-++--+-+-+--++-+-++--++-+-+++-+-+
      a2  - ------++--+----++++--++---+-+----++++++-+++++++-++-++-++--+-
      a3  + +++++++-----+-+-+-+-+--+-++---+-++++++--+-+++----------+++-+++
      a4  + +--++---++---+--+++----++---++-+---+-+-+-+-+-+-++++--++-+++
1948  a1  - -++--+--+--++-+-++++--++----++-++---++++++--+--+---+-
      a2  + +-++--++--++--+-+-+-+-++-++-++++-----+---+-+-+-+++--
      a3  - -----++-+++-++---++-++-++---+--+-+++--++-+++---++-++-+
      a4  + ++------+++-++-++++--+--+-+++--+-+---+-+-++-+-+++-++-+
1964  a1  + ++++++------+++-++-+-++-+--++-++++-----++-++-+-+---++--+--+++--+-
      a2  - -++-+-++--++++-+-+-+++-+-++---+-+++++---+---+++--++++---+--++-----++
      a3  + ++-+--++-+---+++-++-+++-----+-++++-++-+-+-++----+-++++------++++---+-+
      a4  - +-+--+++-+++-+-+++-+-+-++--++-----+-++++--++--++++--+++-+----+---+--+
```

TABLE A2. Blocks and frames of the bordered constructions.

$n = 668$: $G = \mathbb{Z}_{166}$, $b = 4$ (Proposition 2; first row of Table A3)
a1 155B13CDEF8E5C05AB2DBD549D86420DCB803565B4
a2 F11284B6FCD2BB559C1F01DDAD692052576AB383E0
a3 F53A7B8376405BBC8F38E158B08F91100B7791E71C
a4 1D67B459F8C0B34ECEE6BC530974C0E01668D9DCD4
$n = 716$: $G = \mathbb{Z}_{178}$, $b = 4$ (Proposition 2; last row of Table A3)
a1 6370A5D5F65EAF7C823604CE47AD9504D157BE511B024
a2 1C3826C46D2311AC3EADBA71E3EC1DC96988D61F56DD0
a3 7F530ED2DD2826F0F1CCBAC05678969162137878E65D4
a4 FFF4473346A7786A13B7920005DC665CAABC3509DBC90
$n = 1676$: $G = \mathbb{Z}_{418}$, $b = 4$ (Proposition 2)
a1 DCB638A4822E727FE1AEEC8746D1B15549B0D397FB5309E78AC7A97B7CB64C0BB83C60E70405AD280962BAE16A8CDDC920F6D8E24
a2 167A05CAC249039F69A74484C435A7F20BFB539C666FE3F6E3A31DC3710E8ED91C8E82A95ED53EE12548FECB0A3D65C1CC2C5F064
a3 561E0AAC220CD2BFE32E4684465BB3FF49B3FBBD57630147A2676951FC1CEE0B323ECAE9062DAF81294A1ACBCA0CFF498A74D8684
a4 97A33AA8C102277FD1AA5DD74613839009B2D37CEA5385F4A693A94379073C0B78AEA5A50705E63C094EB9CDBE9CEFCDD1AED8224
$n = 1772$: $G = \mathbb{Z}_{442}$, $b = 4$ (Proposition 2)
a1 F719D88DBC2A31A127C276B6FF52AF8C3615C2E47D89E913D8446FE34A9CF717B2BE3A0C5236AAA094349769066A54B3D926CF1A28C82E4
a2 4335D0D81D7C736764C5D216BD0CC3E50287C8FFD9C8FB916C043F477A866E5EDEFAEB0619B20A4E00349E7B164196E1D40EFB9A32855E4
a3 206336D0CC11EE0712C79F54302AD1712BC74C3BE9969AD821919C05A8EBEA2F4D9B84039DB1D7FB5391CAFBFE8FB383A6DBA0D656826D0
a4 8E4647FB6A39F634A1958753EA81D161424999730ACDBCF409513A1CAFC0222B47AB76516D753F537AE1E33DB7954194A54B8607F3F6490
$n = 668$: $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{41}$, $q = 4$, $b = 12$ (Theorem 5)
a1 00A3059FD76E4C22946CFE14C6E704348D0B6563C
a2 807F63A73BF8D937C5EC292C743EFCAAAF9B9AE22
a3 A6626A87798B65C3B11D6D57A99212F0BEE975A11
a4 52474B747DBC5A4699AFA1D87EE88DD5B247BCA2B
D 5A53 5AAC 5569 5596 363A 36C5 3935 39CA 6C5C 6CA3 6366 6399
E 55C9 5AC6 533C 5C33 3566 3A69 3393 3C9C 6655 66AA 695A 69A5
$n = 1916$: $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{119}$, $q = 4$, $b = 12$ (Theorem 5); a_2, a_3 as printed are the M-invariant blocks translated by $(1, 1, 0)$, $(0, 1, 0)$
a1 4AC6F042629D39ABBC82574D87EC1723E623B6D3B401DB49F32B2903C39EA7C86FF901526334A6C544D5773B147FD28EC4228076FF219B88F037873
a2 8CF934D01EF85868FE6CD984A4A15F1DF12B85E862983CC76EBEDCEB000B831155C941D185329F566695EEB93BA86F516D781DB882CA453792D09DC
a3 E2741AA6E0ACE53287A6042FD92E06A879D72A4E876688B2E34DC0A420F2EA0584842EF9209A597F42263ABC6C704C0296676AF3D354731A5C28EB0
a4 F1C7BA6D8B13A7993008335608D3B5EB1B965A1B3F6248923224E3B51F029DE3EAB298161849418A9B7C287AF6982902CD5E51BBD1CA552DD6808FC
D 5A53 5AAC 5569 5596 363A 36C5 3935 39CA 6C5C 6CA3 6366 6399
E 55C9 5AC6 533C 5C33 3566 3A69 3393 3C9C 6655 66AA 695A 69A5
$n = 1388$: $G = \mathbb{Z}_6 \times \mathbb{Z}_{57}$, $q = 6$, $b = 20$ (Theorem 5)
a1 CB75096EA12DD4497A47D0345C95EB2BD8B60E302EB8B69914B7824CFA00BA3958CDB9F7FA12266EE31230
a2 3A6E275CE0E90C63E4F188085CFCEA00E073E357E5CB3681ADBC816C98CA543CA398DBAD72DF43C8A39488
a3 1E41D54A533D911C538AA4B325D8794BBC448CD75049EA1B2D4267A828C18FA7E93940D0C408BA6E345DE4
a4 F11B3EB04AC0DA71A98D908375EC032F7E1E0C842C6AEE9B849E4608A4509F115961BD575E98D3401707C4
D 6B8D34 4C79A6 68E4D3 4F169A 5B21CD 3691D6 58DA5C 356C9C 674A47 2E6378 64B70D 2D98E9 3A5D0B 393666
1EC6A5 1DAB13 71C3AA 723AB1 56AC6A 555571
E 6AC64E 4E52F1 6938CB 4DA719 59CCB2 35CA69 587B2C 34769A 67499C 2E6D23 64BC74 2D93A6 7326A5 729B13
1F2A56 1E9C8D 3AA1F8 395555 54E1C7 57156A
$n = 1436$: $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_{11}$, $q = 8$, $b = 28$ (Theorem 5)
a1 7FFB8A8EAE2A3BB8A006E2801B8B716E2DC5475FF91D800B8B7151DA3B475FFD1D801B8A8E91DDC5475FF91D
a2 DC5B89712E25C44757111D23B4757111DA3A4757111D23A47571400DC4B888EBFF23AB8A8E91D5C4475712E2
a3 DC54768ED1DDC5B8A8EEE2A3B4768ED1DA3BB8A8EEE2A3BB8A8ED1DDC5B8A8EEE2DC5B8B716E2A3B477712E2
a4 FFF4757111D8014748EAE2DC5B888EEE2DC44748EAE2DC44748E91DDC5B888ED1D5C4B8A8E91D23AB8B712E2
D 2EAA2DB8 4ECC56E4 36967293 4BC32B87 59995C9A 71F063E8 35A51DC5 6C63744B 3A5C394E 782D6A35 65564D36 471D2759 1B721E71 172B532E
72878E6A 5C93B174 56E8C953 2BC5D139 63B8B427 2D9ACA4D 1DE4A61E 66719A9C 5A36C58D 3C5987A3 692E93D2 0F35E8E2 334BE4D4 554EB8A9
E AC1D95A9 8EC94B87 D21747D1 9AA3B11B 6C272B4D 72593963 74E1C535 554EE18B 33B4598D 69B82793 C36A172D 99D4A365 0F3AC971 A5C61D53
C6F0ACC9 3A668EA3 B4AA72E1 6ACCD259 B85A6C1D 4E967427 D43C9A17 C96578B1 598B9CC5 2753B295 E193CA2B 178D2E39 1D71564B A32DE447

TABLE A3. Feasible supports $(W_1, \ldots, W_4)$ in $\mathbb{Z}_w$ carrying solutions of the decoupled conditions (6) (§4.3). Each W_f is described by its size $|W_f|$ and its type: (arc) $[0, |W_f|)$; (hx) $[0, |W_f| + 1) \setminus \{x\}$; (e$y$) $[0, |W_f| - 1) \cup \{y\}$; (h$x$ ey) $[0, |W_f|) \setminus \{x\} \cup \{y\}$, up to a translation and reflection of each W_f separately. The column σ gives $(\sum_y T_f(y))_f$; in all cases $(\sum_y S_f(y))_f = (1, 0, 0, 0)$. The last column gives the numbers of solutions on the T side and on the S side that were used to assemble the matrices in the data (each half-search was stopped after about two solutions; for the third row a second solution on each side was found and not used). †: the systems of the matrices of orders 668 and 716 in Table A2; the entries of Table 1 for these orders estimate the cost of their two half-searches.

w	$(\lvert W_1\rvert, \ldots, \lvert W_4\rvert)$	types	σ	solutions T, S
83†	$(44, 39, 41, 43)$	e61; h19 e41; h2; e60	$(10, 3, 3, 7)$	2, 3
83	$(42, 41, 41, 43)$	h10 e62; h2; h2; e52	$(6, 3, 1, 11)$	1, 1
83	$(42, 41, 41, 43)$	h1 e62; h1; h19; e61	$(6, 3, 1, 11)$	1, 1
83	$(40, 41, 43, 43)$	e41; h20 e51; h2; e52	$(2, 1, 9, 9)$	1, 1
83	$(42, 41, 41, 43)$	arc; arc; arc; e62	$(6, 3, 1, 11)$	1, 1
89†	$(46, 43, 45, 45)$	h22 e68; h20; h2; e46	$(12, 1, 5, 3)$	1, 1

Appendix B. Glossary

Cell (§1.3): the group G, the multiplier group M and, for bordered arrays, the subgroup N. *Core* (§1.2): the four blocks of a bordered array; a *width-b core* or *width-b matrix* is one whose border has width b. *Coset table* (§3.2): the coset sums (β_f) modulo constants; *admissible* (Appendix C) if it meets the parity and spectral conditions. *Word* (§3.2): a vector in $(\{\pm1\}^Q)^4$ with four balanced segments. *Frame* (§3.2): a pair (D_Q, E_Q) satisfying the hypotheses of Theorem 5. *Legendre quadruple* (§3.1, after [23]): four ±1 sequences satisfying (3). *M-structure* (§4.3): an orthogonal matrix of order $4t$ divided into sixteen $t \times t$ blocks, in the terminology of Seberry and Yamada [64]. *Miyamoto's decomposition* (§4.3): $a(x, y) = S(y) + (-1)^x T(y)$ for a block a on $\mathbb{Z}_2 \times G'$, where S and T are the half-sum and the half-difference of the two halves $a(0, \cdot)$ and $a(1, \cdot)$ of the block. *Moves* (§3.3): negating, translating or inverting single blocks, and permuting blocks. *Support system* (§4.3): the supports $(W_1, \dots, W_4)$ of the T_f; *feasible* if $\nu(s)$ is even and at least 4 for every $s \neq 0$. *θ-part* (§4.3): $a^{(\theta)} = \frac{1}{2}\sum_x \theta(x) a(x, \cdot)$. *Fibre, mixed, pattern* (§5.6): the vector $a_f(\cdot, y) \in \{\pm1\}^Q$; a fibre with sum ±2; a character or the label mixed for each fibre. *Compressed solution* (§4.2): a quadruple of compressions satisfying (5); two of them, on two quotients, are *compatible* (§4.4) if they are realised together by M-invariant blocks. *Decompression* (§4.4): an M-invariant ±1 block with prescribed coset sums.

Appendix C. The frame enumerations

An *admissible* coset table is a quadruple of integer functions β_f on Q, taken modulo constants, whose values all have the parity of $k = |N|$ (modulo constants, this says that the values of each β_f have a common parity) and which satisfies $\sum_f |\hat\beta_f(\theta)|^2 = 4(q-1)$ for every $\theta \neq 1$.

- *Moves* (§3.3) change the core, and hence the matrix. To border every core it therefore suffices to frame one coset table in each class under the moves and to adjust the core within its class.
- *Isomorphisms.* Call the frame problems of β and β' isomorphic if $K_{\beta'} = U K_\beta V$ for signed permutation matrices U, V of the word coordinates that map words to words. Then $(D_Q, E_Q) \mapsto (UD_Q, E_Q V)$ is a bijection between their frames. A common automorphism ϕ of Q applied to all four segments gives such an isomorphism from β to $\beta \circ \phi$, with $U = V^{-1} = I_4 \otimes P_\phi$, where P_ϕ is the permutation matrix of the automorphism, and a common translation by an element of order 2 gives one with $U = I$ and V the corresponding permutation.
- *Counting.* Frames are counted up to reordering and negating the columns of D_Q and, independently, the rows of E_Q (which changes only C), not up to the moves.

An isomorphism from β to itself is a symmetry that can be imposed on a frame to shrink the search. We call a frame *invariant* under such a symmetry if the symmetry maps each column of D_Q to a column or to minus a column, and likewise each row of E_Q; that is, invariant up to sign.

All frame searches below are depth-first searches over words, or over orbits of words under an imposed symmetry. They choose columns d of D_Q and rows e of E_Q alternately, keeping a new word if it is orthogonal to those already on its side and has $|eK_\beta^{\mathsf T} d| = 4q$ against those on the other.

$q = 4$, width 12. For $Q = \mathbb{Z}_2^2$ the six balanced vectors are the non-trivial characters and their negatives, and parity forces $(|\hat\beta_f(\theta)|)_f$ to be the same arrangement of $(2, 2, 2, 0)$ for all three non-trivial characters. Indeed, write $\beta_f = \text{const} + 2u_f$ with u_f integer-valued. For $\theta \neq 1$, $\hat\beta_f(\theta) = 2\hat u_f(\theta)$, and $\hat u_f(\theta) \equiv \sum_c u_f(c) \pmod 2$ whatever θ is; so each $\hat\beta_f(\theta)$ is even, $12 = 4+4+4+0$ is the only way to write 12 as a sum of four even squares, and the block with the 0 is the same for all three θ. The four positions of the 0 and the signs of the nine values ±2 give $4 \cdot 2^9 = 2048$ admissible coset tables. Of the 115 776 sets of 12 pairwise orthogonal words up to sign, exactly 9408 occur as the columns of a frame for a given admissible coset table, each with exactly one set of rows. These counts and the classes of Table C1 are results of our computer enumeration, on which independently written programs agree; Proposition 8 rests on them, and Theorem 1 does not.

$q = 6$, width 20. For $Q = \mathbb{Z}_6$ only 2 of the 20 balanced vectors are $\pm$characters. Since $\beta_f - k$ is even and constants do not matter, the coset tables to be framed are the same for every k. For a representative of each of the 6624 classes under translation, inversion and negation applied to all four blocks at once there is a frame invariant under an involution of its frame problem, usually the half-turn $c \mapsto c + 3$ on all four segments [83]. Common inversion, negation and translation by 3 are isomorphisms of the frame problem, so every core whose coset table lies in such a class can be bordered after at most a common translation of its four blocks.

TABLE C1. Admissible coset tables and frames for the quotients Q of order 4, 6, 8. Columns: ordered admissible tables; classes under the moves; classes under the moves and common automorphisms of Q; frames found; adjustment of the core; orders using them.

Q	tables	moves	with aut.	frames found	adjustment	used for
$\mathbb{Z}_2^2$	2048	1	—	9408 for each table	none	$668'$, 1916
$\mathbb{Z}_4$	2048	—	—	9408 for each table	none	—
$\mathbb{Z}_6$	155 520	9	—	one for a representative of each of the 6624 classes under common translation, inversion and negation	a common translation	1388
$\mathbb{Z}_2^3$	2 097 152	8	2	one for a representative of each class of the preceding column	within its class under the moves	1436
$\mathbb{Z}_2 \times \mathbb{Z}_4$	6 815 744	9	6	the same	the same	—
$\mathbb{Z}_8$	13 631 488	9	8	the same	the same	—

$q = 8$, *width* 28. For each of the three abelian groups of order 8, $Q = \mathbb{Z}_2^3$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_8$, a frame exists for a representative of each class under the moves and common automorphisms, 16 classes in all, each exhibited in [83] with a core on $Q \times \mathbb{Z}_3$ and the resulting Hadamard matrix of order 124. Call a coset table *constant* if each β_f is constant outside one common coset. The constant coset tables lie in a single class under the moves, for each Q. A Singer cycle of $\mathbb{Z}_2^3$ is an automorphism of order 7 that permutes the seven non-zero elements cyclically. For the constant coset table over $\mathbb{Z}_2^3$ a depth-first search over orbits of a Singer cycle finds a frame within a few hundred nodes, and this is the frame of the matrix of order 1436.

APPENDIX D. ESTIMATED COST OF THE COUNTED OPERATIONS

This appendix estimates what the operations counted in Table 1 cost in processor time and in money. It does not report what was spent. It was written without the search programs or their logs (§1.4), and the hardware and the time actually used for the searches are not recorded in this paper.

The counts. The column $\log_2$ ops of Table 1 is the number of pair sums formed up to the first matrix (§4.1). Four entries are counts (orders 892, 1132, 1676, 1964); the others, marked $\approx$, are estimates from list sizes. The two largest, for orders 668 and 716, can be recomputed from §5.2 and Table A3. For the system of order 668, the lists of step (1) have $2^{35.9}$ to $2^{40.9}$ members and the two sides of a half hold $2^{77.3}$ pairs together on the T half and $2^{77.5}$ on the S half. A count of the kind in step (2) is the product of the four list sizes and, for each shift s, the probability that a sum of $\nu(s)$ random signs (of $\nu(s) - 2$ for the S half) takes the required value. One shift should be omitted, because the equations at the other shifts and the prescribed sums imply the equation there. This gives 2^{16}–2^{18} solutions per half, according to the shift omitted, in agreement with the 2^{17} of step (2). A matching that visits its parts in random order therefore forms about 2^{60} pair sums for each solution of a half. For order 716 the same computation gives $2^{83.5}$ pairs, 2^{15}–2^{18} solutions and about 2^{66} pair sums for each solution of a half. For the two halves together this is about 2^{61} and 2^{67}, where Table 1 has ≈ 59 and ≈ 66 for a matching that visits the likeliest parts first. The two entries are thus uncertain by a factor of several.

The rates. To turn counts into time we timed the two inner loops of a matching. The timing program, `pairsum_bench.c`, was written for this appendix and is appended to the TEX source of this paper; it is not one of the search programs (§6.4). Its data are autocorrelation vectors of random members of the first two lists of the T half at order 668, each stored as 41 bytes padded to 64. On one core of a 2.1 GHz Intel Xeon processor with AVX-512, in a virtual machine, we measured the following.

(a) Forming a pair sum and testing each of its coordinates against a threshold, as in step (4) of §5.2, takes 0.8–1.2 ns: one 512-bit addition and one comparison per pair. The time does not depend on the fraction of pairs that pass.

(b) Forming a pair sum, hashing it, and inserting it in or looking it up in a table that fits in the second-level cache takes 7–13 ns when the table is made of 64-byte buckets and 22–29 ns with plain open addressing, for vectors of 48 coordinates of 8 or 16 bits. With a table of 1 GiB it takes 65–105 ns, so the parts of §4.1 should be small enough for the table to stay in the cache.

With both cores of the machine busy the rates per core were the same. Table D1 accordingly allows 1–4 ns per pair sum for orders 668 and 716, where every pair sum is filtered and only those that pass are hashed,

and 7–30 ns for the other orders, where every pair sum is hashed. The figure of 4 ns corresponds to a tenth of the pair sums passing the filter. The fraction that passed in the searches is not recorded; for the order-668 system, a threshold that keeps two thirds of the solutions passes 6 to 9 per cent of the pair sums.

The price. We take the list price of a rented server of the present generation with AVX-512: 192 cores for US$9.85 per hour on demand, that is US$0.051 per core-hour. The spot price of the same machine in the same week was about a quarter of this.[2]

TABLE D1. Estimated cost of the pair sums counted in Table 1, in decreasing order. The column *ns* is the time allowed per pair sum on one core, and the last column is the cost at US$0.051 per core-hour.

order	$\log_2$ ops	pair sums	ns	core-hours	US$ on demand
716	≈66	$7.4 \cdot 10^{19}$	1–4	$2.0 \cdot 10^7$–$8.2 \cdot 10^7$	1.1–4.2 million
668	≈59	$5.8 \cdot 10^{17}$	1–4	$1.6 \cdot 10^5$–$6.4 \cdot 10^5$	8 200–33 000
1132	56	$7.2 \cdot 10^{16}$	7–30	$1.4 \cdot 10^5$–$6.0 \cdot 10^5$	7 200–31 000
1964	55	$3.6 \cdot 10^{16}$	7–30	$7.0 \cdot 10^4$–$3.0 \cdot 10^5$	3 600–15 000
892	49	$5.6 \cdot 10^{14}$	7–30	1 100–4 700	56–240
668′	≈44	$1.8 \cdot 10^{13}$	7–30	34–150	2–8
1676	42	$4.4 \cdot 10^{12}$	7–30	9–37	0.4–2
1388	≈41	$2.2 \cdot 10^{12}$	7–30	4–18	under 1
1436	≈40	$1.1 \cdot 10^{12}$	7–30	2–9	under 1
1948	≈38	$2.7 \cdot 10^{11}$	7–30	0.5–2	under 1
1772	≈36	$6.9 \cdot 10^{10}$	7–30	under 1	under 1
1916	≈35	$3.4 \cdot 10^{10}$	7–30	under 1	under 1
1244	≈34	$1.7 \cdot 10^{10}$	7–30	under 1	under 1
all				$2.1 \cdot 10^7$–$8.4 \cdot 10^7$	1.1–4.3 million

What the table shows. First, the search for order 716 is in a class of its own: $2 \cdot 10^7$ to $8 \cdot 10^7$ core-hours, which is 12 to 49 years on one 192-core machine or 4 to 18 days on a thousand of them, and about US$1–4 million on demand. At the counts of Table 1 it is more than nine tenths of the total, and it remains the greater part if its count is too high by the factor of several allowed above. Second, three searches cost between $7 \cdot 10^4$ and $6 \cdot 10^5$ core-hours each, that is US$3 600 to US$33 000: order 668 with the border of width 4, and orders 1132 and 1964 by the circulant method. Third, the other nine searches together cost 1 100 to 4 900 core-hours, under US$300, nearly all of it for order 892, whose matching was run to completion. Each of the four searches with wide borders cost between a fraction of a core-hour and 150 core-hours.

The search of §5.2 does not scale. From $w = 83$ to $w = 89$ its count rises by a factor of 2^7, so it roughly doubles with each unit of w.

What the table leaves out. The figures are for the counted operations alone, at rates measured on a reference kernel. They exclude the generation of the lists, which for orders 668 and 716 have up to 2^{43} members and cannot be held in memory; the four further support systems at $w = 83$ of Table A3 on which both halves were solved; the support systems and candidate sets that were searched without success, whose number is not recorded; and the preliminary screening mentioned in §1.4. Nor are they lower bounds. A faster kernel or a better-organised matching would reduce them, and we have not timed the loops on graphics processors, to which loop (a) is well suited.

[2]Amazon EC2 instance type c7a.48xlarge (AMD EPYC 9R14, one thread per core), US East (N. Virginia), Linux, as listed on 14 November 2026 at https://cloudprice.net/aws/ec2/instances/c7a.48xlarge; spot price about US$2.4–2.5 per hour, averaged over the preceding seven days, at https://go.runs-on.com/instances/ec2/c7a. The rates above were not measured on this processor; we assume the same rates per core.