# On Fourier and Hadamard matrices of prime order

Teo B and Chat GPT

**Abstract**

We study how much of the Fourier matrix $F_p$ is needed to recognize it among complex Hadamard matrices of prime order $p$. For regular or Butson matrices, taking the $p$th power of each entry gives either a Hadamard matrix or a matrix of rank one. For every odd prime, the block of $F_p$ on the rows and columns indexed by the nonzero squares determines $F_p$ up to equivalence in both classes. At level $p$, a symmetry with cycle lengths $1, (p-1)/2, (p-1)/2$ on each side also characterizes $F_p$ at every odd prime through 109.

hexagon:2611.00221v1

## Contents

Introduction 1
1 Entrywise powers at prime order 3
2 Examples of the Hadamard case 4
3 Recognizing the Fourier matrix from its rows 7
4 Completing three rows at order 11 8
5 Cyclic symmetries and quadratic residues 13
6 Complementary blocks and their differences 14
7 Ordering the squares and nonsquares 19
8 An inverse ordering which cannot be completed 27
9 A Fourier corner determines the matrix 29
10 Recovering the border of a Fourier block 36
References 41

## Introduction

The Fourier matrix $F_N$ of the cyclic group $\mathbb{Z}_N$ has one row for each character and one column for each element of the group, and couples these. With $w = e^{2\pi i/N}$, the pairing is $(i, j) \mapsto w^{ij}$ for $i, j = 0, \ldots, N-1$. In matrix form we have

$$F_N = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & \cdots & w^{N-1} \\ 1 & w^2 & w^4 & \cdots & w^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w^{N-1} & w^{2(N-1)} & \cdots & w^{(N-1)^2} \end{pmatrix}.$$

The quotient of two distinct rows is a nontrivial character, whose values sum to zero. Thus $F_N F_N^* = N I_N$, and $F_N$ is the basic example of a complex Hadamard matrix, a square matrix with entries in the unit circle $\mathbb{T}$ and mutually orthogonal rows.

As explained in [1], associated to every complex Hadamard matrix $H$ is a quantum permutation group $G$, and $H$ can be thought of as being the Fourier matrix of $G$. The construction uses the projections onto the lines spanned by the row quotients of $H$. For $H = F_N$ we recover $G = \mathbb{Z}_N$. In prime order $p$, the group $G$ is classical exactly when $H$ is equivalent to $F_p$.

There is arithmetic even in the diagonal of $F_N$. Its trace is the quadratic Gauss sum $\sum_{j=0}^{N-1} w^{j^2}$. For an odd prime $p$, the value is $\sqrt{p}$ if $p \equiv 1 \pmod 4$ and $i\sqrt{p}$ if $p \equiv 3 \pmod 4$. The sign in these formulas occupied Gauss for more than four years. He conjectured it in May 1801 and found his proof in August 1805 [3]. One can also read the sign from the Fourier matrix. The square of $F_p/\sqrt{p}$ sends the coordinate indexed by $x$ to the one indexed by $-x$, so the eigenvalues are among $1, -1, i, -i$. The determinant of $F_p$ is a Vandermonde determinant. Its phase resolves the ambiguity in the trace, as in Schur's proof [3].

We ask how much of the character table one must see in a Hadamard matrix of prime order to recognize $F_p$. Three problems led us to this question.

**A.** *From orders* 7 *and* 8 *to order* 11. In [9] we studied regular Hadamard matrices at orders 7 and 8. Regularity means that each quotient of distinct rows splits into rotated copies of $\mu_q$, the group of $q$th roots of unity, for primes $q$. At order 11, if one such quotient visits each vertex of a regular 11-gon once, the whole matrix is equivalent to $F_{11}$. On the classification of regular matrices of order 11 we hope to report later.

**B.** *The circulant theorem of Hiranandani and Schlenker.* A circulant Hadamard matrix of prime order $p$ with entries in $\mu_p$ is equivalent to $F_p$ [11]. For odd $p$ the circulant matrix $(w^{(i-j)^2})$ gives $F_p$ after rescaling rows and columns and permuting columns. We ask about another symmetry of $F_p$. If $g$ generates the nonzero squares, $(a, x) \mapsto (ga, g^{-1}x)$ fixes the entry $w^{ax}$ and permutes the squares and nonsquares in two cycles on each side.

**C.** *Szöllősi's observation on complementary blocks.* Complementary square blocks of a unitary matrix have the same singular values, apart from extra copies of 1 in the larger block [2, 22]. This leads to formulas for the polar part of a complementary block [2]. For real Hadamard matrices, Koukouvinos, Mitrouli and Seberry used complementation to study minors [13, 14]. Here it relates the exponent differences in opposite blocks of a matrix with the two-orbit symmetry.

Write $H \sim H'$ for equivalence under permutations and unit scalings of rows and columns. Dephasing makes the first row and column all ones. A Butson matrix of level $k$ is a Hadamard matrix with entries in $\mu_k$. We write $B(N, k)$ for the set of such matrices of order $N$. Our first result explains how level $p$ arises.

**Theorem I.** *Let $H$ be a complex Hadamard matrix of prime order $p$, either regular or Butson. Its entrywise $p$th power is either Hadamard or of rank one. It has rank one exactly when $H$ is equivalent to a member of $B(p, p)$.*

A single $p$-cycle among the row quotients forces the entrywise power to have rank one. Thus $H \sim F_p$ for $p \leq 17$ by [12]. At level $p$ we can put any two rows in Fourier form. Each further Fourier row in that column ordering rules out a slope for the graph of the exponents of a missing row.

**Theorem II.** *For every odd prime $p$, a Hadamard matrix of order $p$, either regular or Butson, is equivalent to $F_p$ if it contains $(p-1)/2$ distinct Fourier rows in a common column ordering.*

Can a symmetry force the Fourier rows when none is prescribed? Let $Q$ be the nonzero squares in $\mathbb{F}_p$. A simultaneous symmetry is a pair of row and column permutations preserving every entry.

**Theorem III.** *Let $p = 2m + 1$ be prime, where $m$ is an odd prime power and 4 generates $Q$. If a matrix in $B(p, p)$ admits a simultaneous symmetry with one fixed point and two cycles of length $m$ on each side, then it is equivalent to $F_p$. In particular this holds whenever $m$ is an odd prime.*

Comparing the four circulant blocks gives recognition at every odd prime through 109 (Corollary 7.14). Without assuming any symmetry, we can also recognize $F_p$ from a single block.

**Theorem IV.** *Let $p$ be any odd prime. Write $Q$ for the nonzero squares in $\mathbb{F}_p$ and $w = e^{2\pi i/p}$. If a Hadamard matrix of order $p$, either regular or Butson, contains a submatrix equivalent to $(w^{ax})_{a,x\in Q}$, then the whole matrix is equivalent to $F_p$.*

The rows and columns of the block may be permuted and rescaled independently. Theorem 10.4 allows up to $\lfloor |Q|/32 \rfloor$ unspecified entries in each row and each column. For the dephased corner with one square row and one square column deleted, we prove recognition through 103 (Proposition 9.4). At every odd prime, agreement with the missing Fourier column on more than $2\sqrt{p}+6$ surviving rows suffices (Proposition 10.5).

The paper is organized as follows. Sections 1–2 prove the power dichotomy of Theorem I and illustrate it with sixth-root matrices. In Sections 3–4 we use directions in the affine plane to prove Theorem II, then determine which regular triples with an 11-cycle extend. Sections 5–7 study the four circulant blocks by complementation and polar decomposition. Their cyclic orderings give Theorem III and the recognition tests through 109. Sections 8–10 treat the inverse ordering, corner deletions and reconstruction from two strips. Theorem IV recovers the missing border.

# 1 Entrywise powers at prime order

Raising each entry of $F_p$ to its $p$th power gives the all-ones matrix. In a regular or Butson matrix of order $p$, two rows whose quotient is a $p$-cycle become proportional on taking $p$th powers. To see why this forces rank one, we begin with a lemma on flat matrices, whose entries have modulus one.

**Lemma 1.1.** *Let $K$ be a flat $n \times n$ matrix whose rows are pairwise orthogonal or proportional, and whose columns have the same property. All row proportionality classes and all column proportionality classes have the same cardinality $d$. In particular* $\operatorname{rank}(K) = n/d$ *divides $n$.*

*Proof.* The number of row classes and the number of column classes both equal the rank, say $k$. Remove the proportionality phases and retain one row and column from each class to obtain a flat invertible $k \times k$ matrix $B$. Let $R = \operatorname{diag}(r_i)$ and $C = \operatorname{diag}(c_j)$ record the row and column class sizes. Orthogonality of distinct classes gives

$$BCB^* = nI_k, \qquad B^*RB = nI_k.$$

Thus $CB^* = B^*R$, or $RB = BC$. Since all entries of $B$ are nonzero, $r_i = c_j$ for every $i, j$. Their common value is $d$, and $n = kd$. □

**Lemma 1.2.** *Let $p$ be prime and let $z_1, \dots, z_p$ be roots of unity with $\sum_{j=1}^{p} z_j = 0$. Then either $\sum_{j=1}^{p} z_j^p = 0$ or $z_1^p = \cdots = z_p^p$.*

*Proof.* Work in a cyclotomic field $K$ containing the $z_j$. In its ring of integers, reduction modulo $p$ gives

$$\sum_{j=1}^{p} z_j^p \equiv \left( \sum_{j=1}^{p} z_j \right)^p = 0 \pmod{p}.$$

Thus $a = (z_1^p + \cdots + z_p^p)/p$ is an algebraic integer. Every conjugate of $a$ is an average of roots of unity and has absolute value at most one. If $a \neq 0$, the product over all embeddings of $K$ is a nonzero integer. Its absolute value is therefore one, and so is $|a|$. Equality in the triangle inequality forces all $z_j^p$ to coincide. □

**Theorem 1.3.** *Let $H$ be a complex Hadamard matrix of prime order $p$, either regular or Butson. The matrix $K = (H_{ij}^p)$ is either Hadamard or of rank one. The latter occurs exactly when $H$ is equivalent to a member of $B(p,p)$.*

*Proof.* Suppose first that $H$ is Butson, of any level. Apply Lemma 1.2 to the entries of each quotient of distinct rows of $H$. The corresponding rows of $K$ are orthogonal in the first case and proportional in the second. Since $H$ is square, its columns are orthogonal as well, and the same argument applies to each pair of columns. Lemma 1.1 now gives $\operatorname{rank}(K) \mid p$. In rank $p$ the rows are pairwise orthogonal, so $K$ is Hadamard. The only other possibility is rank one.

For regular $H$, fix a cycle decomposition of each row quotient. Let $G \subset \mathbb{T}$ be generated by the entries of $H$ and the groups $\mu_q$ for the cycle lengths $q$ used. This finitely generated abelian group splits as its torsion subgroup times a free abelian group. Fix the torsion subgroup pointwise and send each free generator to roots of unity tending to that generator. The resulting homomorphisms send each $t\mu_q$ to a rotated $q$-cycle, so applying them entrywise gives Butson matrices converging to $H$. Taking entrywise powers is continuous. The Hadamard condition and the vanishing of all $2 \times 2$ minors are closed conditions. Thus $K$ is again either Hadamard or of rank one, since its entries have modulus one.

Finally, dephasing commutes with taking entrywise powers. A dephased matrix of rank one has all entries equal to one. Hence $K$ has rank one exactly when the entries of the dephased $H$ belong to $\mu_p$, as claimed. □

**Corollary 1.4.** *Let $H$ be a complex Hadamard matrix of prime order $p$, either regular or Butson. If a quotient of 2 rows or 2 columns is a $p$-cycle, then every quotient of distinct rows and every quotient of distinct columns is a $p$-cycle. The matrix $H$ dephases into $B(p,p)$. For $p \leq 17$ we have $H \sim F_p$.*

*Proof.* The given pair becomes proportional after taking entrywise $p$th powers. Theorem 1.3 therefore gives rank one and puts the dephased $H$ in $B(p,p)$. In this form, every quotient of distinct rows or columns is a vanishing sum of $p$ elements of $\mu_p$. Its multiplicities are the coefficients of a polynomial of degree at most $p-1$ vanishing at $e^{2\pi i/p}$. This polynomial is a multiple of $1 + x + \cdots + x^{p-1}$ and its coefficients sum to $p$, so each is one. Undoing the dephasing only rotates these cycles. The final assertion follows from Hirasaka, Kim and Mizoguchi [12, Theorem 1.1]. □

**Proposition 1.5.** *Let $H$ be a Hadamard matrix of prime order $p$, either regular or Butson. Suppose an $r \times s$ submatrix has all its cross ratios in $\mu_p$. If $rs > p$, then $H$ is equivalent to a member of $B(p,p)$.*

*Proof.* Choose any row $i_0$ and column $j_0$ of the rectangle. For every entry in it the cross ratio $H_{ij}H_{i_0j_0}\bar{H}_{ij_0}\bar{H}_{i_0j}$ has $p$th power one. Thus the same rectangle of $K = H^{\circ p}$ has rank one. Its sole nonzero singular value is its Frobenius norm $\sqrt{rs}$. As a compression of $K$ its operator norm is at most $\|K\|$. If $K$ were Hadamard, we would have $\|K\| = \sqrt{p}$, contrary to $rs > p$. Theorem 1.3 gives the conclusion. □

For example, a $4 \times 5$ rectangle already detects level 19. Recognizing $F_{19}$ from a specified Fourier pattern is a different question, answered for a $9 \times 10$ corner in Section 9.

## 2 Examples of the Hadamard case

At the same prime, both possibilities in Theorem 1.3 occur. For the Fourier matrix and Szöllősi's sixth-root matrix [23] we have

$$F_{19}^{\circ 19} = J, \qquad W_{19}^{\circ 19} = W_{19},$$

where $J$ is the all-ones matrix and the powers are entrywise. The second equality follows from $19 \equiv 1 \pmod 6$. The same calculation applies to the 436 monomial classes in $B(13, 6)$ catalogued in [15, 16]. All these examples are regular, as follows.

**Lemma 2.1.** *Every vanishing sum of sixth roots of unity is a union of 2- and 3-cycles. Consequently every member of $B(n, 6)$ is regular.*

*Proof.* Put $w = e^{\pi i/3}$ and let $n_j$ count the occurrences of $w^j$. Cancel opposite pairs and write $r_j = n_j - n_{j+3}$ for $j = 0, 1, 2$. The relation $w^2 = w - 1$ gives

$$0 = r_0 + r_1 w + r_2 w^2 = (r_0 - r_2) + (r_1 + r_2)w.$$

Thus $r_0 = r_2 = -r_1$. If their common value is nonnegative, the remaining terms are copies of $\{1, w^2, w^4\}$; if it is negative, they are copies of $\{w, w^3, w^5\}$. Restore the cancelled opposite pairs. Applying this to row quotients proves the last assertion. □

**Proposition 2.2.** *Every affine Hadamard deformation of a member of $B(n, 6)$ is regular.*

*Proof.* Write the entries as $H_{ij} \exp(i\langle r_{ij}, t\rangle)$. In the scalar product of rows $i, k$, group terms with equal frequency $r_{ij} - r_{kj}$. Independence of the distinct exponentials on an open set forces each group of sixth roots to sum to zero. Lemma 2.1 splits each group into cycles, which rotate together with their common phase. □

At order 7 this gives the regular Petrescu family. Szöllősi also obtains its seed from a dephased symmetric real Hadamard matrix of order $n = 8$ [24, Theorem 4.1]. In general his construction deletes the first row and column, replaces off-diagonal $-1$ by $b$ and diagonal 1 by $-b$, where $|b| = 1$ and $\operatorname{Re} b = (6 - n)/(n - 4)$.

**Proposition 2.3.** *Let $n > 8$ be the order of the dephased symmetric real Hadamard matrix in Szöllősi's construction above. The resulting matrix of order $n - 1$ is not regular.*

*Proof.* The rational number $b + b^{-1} = -2 + 4/(n - 4)$ lies strictly between $-2$ and $-1$, so it cannot be an algebraic integer. Hence $b$ has infinite order and the only roots of unity in $\langle -1, b\rangle$ are $1, -1$. Ratios between terms of a row quotient lie in this group, so only 2-cycles are possible. Their lengths cannot sum to $n - 1$, which is odd. □

The next obstruction is the prime-order case of Winterhof's criterion, stated in [22, Theorem 3.2.12]. At prime order it has a short determinant proof.

**Proposition 2.4.** *If $p \equiv 5 \pmod 6$ is prime, then $B(p, 6)$ is empty.*

*Proof.* The determinant $d$ of such a matrix would belong to the Eisenstein integers and satisfy $d\bar{d} = p^p$. A prime $p \equiv 2 \pmod 3$ remains prime in that ring: the polynomial $X^2 + X + 1$ has no root modulo $p$, since $\mathbb{F}_p^\times$ has no element of order 3. Its valuation in $d\bar{d}$ is therefore twice its valuation in $d$, hence even. Its valuation in $p^p$ is the odd integer $p$, a contradiction. □

This excludes level 6 at $11, 17, 23$. Petrescu's array of order $3s + 1$ has the form

$$H = \begin{pmatrix} X & Y & T \\ Y & X & T \\ T^* & T^* & D \end{pmatrix},$$

where $T$ consists of the $s$ noninitial rows of a dephased Hadamard matrix of order $s + 1$. At level 6 this particular array requires a seed in $B(5, 6)$ for order 13, and in $B(11, 6)$ for order 31. Both seeds are excluded above. The existence of a matrix in $B(31, 6)$ is listed as open in [5].

For $W_{19}$, the seed has order 7. Here are its blocks [23], with each digit $a$ denoting $w^a$ for $w = e^{\pi i/3}$. Szöllősi asked whether this matrix deforms as the order-7 example does [22].

| $X$ | $Y$ | $T$ | $D$ |
|---|---|---|---|
| 301100 | 543532 | 1135430 | 0000113 |
| 001331 | 424515 | 1433150 | 0013010 |
| 001424 | 243241 | 3314510 | 1300010 |
| 124212 | 442450 | 3511340 | 0101041 |
| 254320 | 420142 | 4153130 | 1041100 |
| 035450 | 453134 | 5341310 | 1010401 |
| | | | 4110100 |

**Proposition 2.5.** *The dephased defect of $W_{19}$ is zero. Its class is isolated among all complex Hadamard matrices of order* 19*.*

*Proof.* Write $H_{ij} = w^{E_{ij}}$ in the displayed representative. Fix its first row and column to remove the row and column phase freedoms, and vary the remaining phases by $tR_{ij}$, with $R_{1j} = R_{i1} = 0$. Differentiating the row scalar products gives

$$\sum_j w^{E_{ij}-E_{kj}}(R_{ij} - R_{kj}) = 0 \qquad (i < k).$$

In the real basis $1, w$, the coordinates of $w^0, \dots, w^5$ are $(1,0), (0,1), (-1,1), (-1,0), (0,-1), (1,-1)$. Form the $342 \times 324$ integer matrix with pairs $(i,k)$ in lexicographic order, the two coordinates in the displayed order, and variables in row order. Delete rows $33, 34, 35, 36, 288, 297, 331, \dots, 342$, numbered from 1. Gaussian elimination gives determinant 19 mod 101 for the remaining minor. Thus the real kernel is zero, and the inverse function theorem isolates the dephased matrix. □

For fixed $T, D$, put $S = X+Y$, $Z = X-Y$. Block multiplication gives $2T^*T + DD^* = (3s+1)I$, $ST + TD^* = 0$, $SS^* + 2TT^* = (3s+1)I$ and $ZZ^* = (3s+1)I$. Since $TT^* = (s+1)I$, we have $S = -TD^*T^*/(s+1)$. Once one completion exists, another flat splitting of this $S$ gives a completion exactly when $ZZ^* = (3s+1)I$.

**Lemma 2.6.** *In Petrescu's array of order $3s+1$, fix $T, D$ with $s \geq 3$ and put $S = -TD^*T^*/(s+1)$. If $S$ has one zero in each row and column and $0 < |S_{ij}| < 2$ elsewhere, there are only finitely many flat completions.*

*Proof.* Each nonzero entry of $S$ has two ordered splittings into unit entries. Fix these choices and write $2u_i$ for the remaining entry of row $i$ of $Z$, with $|u_i| = 1$. Its products with the other rows give $A_{ik}u_i + B_{ik}\bar{u}_k + C_{ik} = 0$ with $A_{ik}B_{ik} \neq 0$. If some $C_{ik} \neq 0$, two distinct circles meet in at most two choices for $u_i$, each determining all other phases. Otherwise all products $u_iu_k$ are fixed, and three indices determine $u_i^2$. □

**Theorem 2.7.** *The displayed $T, D$ admit exactly four unimodular completions up to swaps within the paired rows and columns. All four are sixth-root matrices of dephased defect zero.*

*Proof.* Let $X^0, Y^0$ be the displayed blocks. The unique zero columns of $S$ in row order are $k_i = 5, 3, 6, 1, 2, 4$. There $Z_{ik_i} = 2X^0_{ik_i}z_i$, $|z_i| = 1$. Elsewhere $|S_{ij}| = 1$ and $Z_{ij} = \pm(X^0 - Y^0)_{ij}$. Pair swaps change signs of whole rows or columns of $Z$. Make all five signs of row 1 positive and the first off-zero sign in each other row positive. Encode its four remaining signs in column order by four bits, 0 for plus, most significant first.

Set the variable entries of $Z$ to zero to obtain $U$. The product of rows $i, j$ is $A_{ij}z_i + B_{ij}\bar{z}_j + C_{ij}$, where

$$A_{ij} = 2X^0_{ik_i}\bar{U}_{jk_i}, \quad B_{ij} = 2U_{ik_j}\bar{X}^0_{jk_j}, \quad C_{ij} = \sum_l U_{il}\bar{U}_{jl}.$$

Put $z = z_1$. The first row gives $\bar{z}_j = d_j + e_j z$, with $(d_j, e_j) = -(C_{1j}, A_{1j})/B_{1j}$. Using $\bar{z} = 1/z$, the modulus equation for $j$ and the pair equation for $1 < i < j$ become

$$(d_j + e_j z)(\bar{d}_j z + \bar{e}_j) - z = 0,$$
$$A_{ij}(\bar{d}_i z + \bar{e}_i) + B_{ij} z(d_j + e_j z) + C_{ij} z = 0.$$

Start with gcd zero in $\mathbb{Q}(w)[z]$. For each successive row try its 16 sign codes and take the gcd with its new equations, discarding nonzero constants. The successive numbers of surviving prefixes are $16, 28, 4, 4, 4$, each final monic gcd being $z^2 - 1$. After fixing the first-row operation (the simultaneous reversal of all rows and columns acts trivially), only the flip at column $k_1$ remains free, followed by row flips restoring the normalization. It reverses $z_1$, so take $z_1 = 1$ uniquely. Substitution gives $ZZ^* = 19I$ in the four cases below. The last column gives the minor from Proposition 2.5 modulo 101.

| Sign codes, rows 2–6 | $(z_1, z_2, z_3, z_4, z_5, z_6)$ | det mod 101 |
|---|---|---|
| $(0, 0, 0, 0, 0)$ | $(+, +, +, +, +, +)$ | 19 |
| $(2, 1, 2, 2, 2)$ | $(+, -, -, -, -, -)$ | 98 |
| $(9, 1, 5, 9, 14)$ | $(+, +, -, +, +, -)$ | 46 |
| $(11, 0, 7, 11, 12)$ | $(+, -, +, -, -, +)$ | 58 |

The phases are signs, so each pair consists of the two original sixth roots. All four minors are nonzero modulo 101, giving isolation. □

Szöllősi's broader question concerns all Petrescu-type matrices in $B(19, 6)$ [22, Problem 3.2.11]. Our four isolated completions rule out the displayed pair $(T, D)$ as a source of such a family. Taking nineteenth powers fixes $W_{19}$ entry by entry, whereas it takes $F_{19}$ to the all-ones matrix.

## 3 Recognizing the Fourier matrix from its rows

We return to the other case of Theorem 1.3. When the entrywise $p$th power has rank one, dephasing gives a Hadamard matrix with entries in $\mu_p$. For the rest of the paper we ask how much of the Fourier matrix we need to recognize it. We begin with one quotient of rows.

Put $w = e^{2\pi i/p}$ and use $\mathbb{F}_p$ to label the columns. The rows of $F_p$ are the characters

$$r_a(x) = w^{ax}, \qquad r_a \bar{r}_b = r_{a-b}.$$

If $a \neq b$, the map $x \mapsto (a-b)x$ runs once through the field, so these rows are orthogonal. Conversely, in any member of $B(p, p)$ a quotient of distinct rows contains every $p$th root once, by Corollary 1.4. We can therefore make any chosen pair into $r_0, r_1$: divide each column by its entry in the first row and order the columns by the exponents of the second. The issue is whether the same column ordering works for the other rows.

Multiply a third row by a scalar so its entry at $x = 0$ is one, and write it as $(w^{f(x)})_x$. It is orthogonal to $r_0, r_1$ exactly when both $f(x)$ and $f(x) - x$ permute $\mathbb{F}_p$. This leaves room for nonlinear $f$. At $p = 7$, for instance, put $f(0) = 0$ and take $f(x) = 3x$ on the nonzero squares and $f(x) = 5x$ on the nonsquares. Both multipliers are nonsquares, so $f$ exchanges the two classes. For $f(x) - x$ the multipliers are $2, 4$, both squares, so it preserves the two classes. This third row satisfies both orthogonality equations.

Each additional prescribed Fourier row $r_a$ asks that $f(x) - ax$ also be a permutation. How many such conditions force $f$ to be linear? We answer this first, then examine regular triples and their completions at order 11. Further on we will obtain Fourier rows from a cyclic symmetry or from a prescribed block of entries.

We recall the direction theorem of Rédei and Megyesi, in the form stated in [21, Theorem 1.1]: a set of $p$ points in $\mathbb{F}_p^2$ which is not a line determines at least $(p+3)/2$ directions. For a graph $(x, f(x))$,

the vertical direction is absent, and a finite slope $a$ occurs precisely when $f(x) - ax = f(y) - ay$ for some $x \neq y$. Thus every prescribed Fourier row removes a direction.

**Theorem 3.1.** *Let $p$ be an odd prime and $m = (p-1)/2$. If a Hadamard matrix $H$ of order $p$, either regular or Butson, contains $m$ distinct Fourier rows in a common column ordering, then $H \sim F_p$.*

*Proof.* At $p = 3$, three unit numbers summing to zero form a rotated $\mu_3$. After dephasing and a column permutation the first two rows are $r_0, r_1$, and orthogonality determines the third up to a scalar. For $p \geq 5$ there are at least two prescribed rows, and their quotient is a $p$-cycle. By Corollary 1.4, after dephasing all entries are $p$th roots. This dephasing preserves the form of the prescribed rows: using the row of slope $a_0$ as the first row replaces the prescribed slopes by $a - a_0$, and the column $x = 0$ is already one in these rows.

Write any additional dephased row as $(w^{f(x)})_x$, with $f(0) = 0$. As above, orthogonality to the prescribed row $r_a$ makes $f(x) - ax$ a permutation. Thus the graph of $f$ avoids at least $m$ finite directions, and determines at most $p - m = (p+1)/2$ directions. The direction theorem forces this graph to be a line. Hence $f(x) = bx$, and the row is Fourier. Orthogonality makes all the slopes distinct, so the $p$ rows give $F_p$ after a permutation. □

A partial Hadamard matrix is a $K \times N$ matrix $H$ with entries in $\mathbb{T}$ and $HH^* = NI_K$. For a partial matrix of width $p$ with $p$th-root entries, the same reasoning shows that any further $p$th-root row orthogonal to the $m$ Fourier rows is a scalar multiple of a Fourier row. Normalizing its entry at $x = 0$ to one fixes that scalar. The assertion for arbitrary regular or Butson levels uses squareness in the first step, through the power dichotomy. It does not assert that a partial regular matrix with these rows is automatically of level $p$.

There is also an elementary statement without any Butson or regularity assumption, when the prescribed slopes are consecutive.

**Proposition 3.2.** *Let $p = 2m+1$ be prime. A complex Hadamard matrix containing the $m$ Fourier rows of slopes $0, 1, \ldots, m-1$ is equivalent to $F_p$.*

*Proof.* For a remaining row $v$, orthogonality removes its Fourier coefficients at these $m$ frequencies. We can therefore write

$$v_x = w^{mx} P(w^x), \qquad P(z) = c_0 + c_1 z + \cdots + c_m z^m.$$

The Laurent polynomial $|P(z)|^2 - 1$ on the unit circle has exponents between $-m$ and $m$ and vanishes at all $p = 2m + 1$ $p$th roots. Multiplication by $z^m$ gives a polynomial of degree at most $2m < p$ with $p$ roots, so it is zero. If $c_r, c_s$ are the first and last nonzero coefficients and $r < s$, the coefficient at exponent $s - r$ in $|P|^2$ is $c_s \bar{c}_r \neq 0$, a contradiction. Thus $P$ is a single monomial of unit modulus. Every remaining row is a scalar multiple of a Fourier row, and orthogonality supplies all the missing slopes. □

For arbitrary slopes the first proof uses the $p$th roots to turn orthogonality into a statement about a graph. For consecutive slopes the second proof uses only the unit modulus of the entries. Both start with rows whose common column ordering is already known. We next go back to the point at which only the first two rows have been fixed.

## 4 Completing three rows at order 11

Fix the first two rows $r_0, r_1$ at $p = 11$ and suppose only that the other row quotients decompose into prime cycles. For a square matrix we already know the conclusion. Corollary 1.4 gives level 11, and the classification of $B(11, 11)$ in [12] gives $F_{11}$. At what stage of a completion does this rigidity appear? Already for three rows there are two possibilities. After a row scaling the third

row can have entries in $\mu_{11}$, in which case we have the permutation problem of Section 3. It can also involve smaller prime cycles, with a free phase surviving orthogonality. We describe these triples, then examine which ones fit inside a square matrix. At level 11 six mutually orthogonal rows already have Fourier slopes in the coordinates fixed by the first pair.

Write the triple as $(1; u; v)$, where $u_j = w^j$, $w = e^{2\pi i/11}$, and put $y_j = v_j/u_j$. A profile records the lengths in a chosen cycle decomposition. The partitions of 11 into primes are

$$\begin{array}{lll} A = 11, & B = 7+2+2, & C = 5+3+3, \\ D = 5+2+2+2, & E = 3+3+3+2, & F = 3+2+2+2+2. \end{array}$$

Thus $AEF$, for example, means that besides $u$, one of $v, y$ has profile $E$ and the other has profile $F$. The identity $u_j y_j = v_j$ restricts how the cycles in $y$ and $v$ can meet.

**Lemma 4.1.** *Let $(1; u; v)$ be a regular $3 \times 11$ triple with $u_j = w^j$, where $w = e^{2\pi i/11}$, and put $y_j = v_j/u_j$. If 2 of the row quotients have profile $A$, so does the third. If $y, v$ contain no 11-cycles, a cycle in $y$ and a cycle in $v$ meet in at most one column position.*

*Proof.* 2 11-cycle quotient vectors have all their entries in rotated copies of $\mu_{11}$. Their ratio also lies in a rotated $\mu_{11}$. By regularity, this third quotient decomposes into prime cycles. Each such cycle must have length 11, so the quotient is a single 11-cycle.

For the second assertion, suppose columns $j \neq k$ belong to the same $p$-cycle of $y$ and the same $q$-cycle of $v$. Then

$$w^{j-k} = \frac{v_j/v_k}{y_j/y_k} \in \mu_{\mathrm{lcm}(p,q)}.$$

As $p, q \neq 11$, this contradicts $j \neq k$ modulo 11. □

**Theorem 4.2.** *The possible chosen profile triples of regular $3 \times 11$ partial Hadamard matrices with an 11-cycle quotient are precisely:*

$$AAA, \qquad AEE, \qquad AEF, \qquad AFF.$$

*All 4 occur. This branch admits an exhaustive finite parametrization by fixed matrices and affine one-parameter families. The parametrization below is redundant; it is not a list of inequivalent matrices or families.*

*Proof.* If either remaining quotient has profile $A$, Lemma 4.1 gives $AAA$. Suppose now that neither does. Make a bipartite graph whose left vertices are the cycles of $y$, whose right vertices are the cycles of $v$, and whose edges are the 11 columns. The lemma says that it is simple. Its degrees are the respective cycle lengths. Every vertex has degree at least 2. A 7-cycle cannot occur, since there are at most 5 vertices on the other side. A 5-cycle requires 5 vertices on the other side, leaving only $ACF$ and $ADF$ as possible cases involving a 5-cycle.

These 2 cases are also impossible. In either graph, the 5-cycle is the unique vertex of degree 5; all other vertices have degree 2 or 3. Along graph edges, ratios of the cycle phases are products of roots of orders dividing 330. Within a connected component, factor out one common phase and project these roots onto their $\mu_5$ component. After removing the 5-cycle vertex, this component is constant on each remaining connected component. Its 5 neighbors must have 5 different $\mu_5$ components, because the 5 entries in the 5-cycle do. They must therefore belong to 5 different connected components after removal. Each neighbor has another left neighbor, because its original degree is at least 2. This requires at least 5 other left vertices. There are only 2 in profile $C$ and 3 in profile $D$, a contradiction.

For the graph parametrization put $w = e^{\pi i/33}$ and $\omega = w^{11} = e^{\pi i/3}$. Thus $w^6$ is the primitive 11th root used above. For $AEE, AEF, AFF$, all the other cycles have length 2 or 3. In each connected graph component, the edge equations force the cycle phases, relative to one common phase, to lie in $\mu_{66} = \mu_{11}\mu_6$. Consequently the data are:

1. A simple bipartite graph with 11 edges and the prescribed degrees.
2. An edge color $r_e \in \mathbb{Z}/6\mathbb{Z}$ such that the colors at a degree-$p$ vertex form one rotated $p$-cycle in $\mu_6$.
3. Labels $b_i, c_k \in \mathbb{Z}/11\mathbb{Z}$ on the left and right vertices, with the following multiset identity:

$$\{c_k - b_i : (i,k) \text{ is an edge}\} = \mathbb{Z}/11\mathbb{Z}.$$

4. One phase $t_s \in \mathbb{T}$ for each connected component.

For the edge $e = (i,k)$ of color $r_e$ in component $s$, set

$$j = c_k - b_i, \qquad y_j = t_s w^{6b_i}\omega^{r_e}, \qquad v_j = t_s w^{6c_k}\omega^{r_e}.$$

The differences enumerate the columns exactly once. Every vertex supplies its required prime cycle, and $v_j/u_j = y_j$. These conditions are sufficient as well as necessary. A common factor of all the $t_s$ is removed by a row factor. Thus a graph with $c$ connected components supplies $c-1$ continuous parameters.

Enumerate the simple bipartite graphs with the prescribed degrees, then all cycle colors and vertex labels satisfying these conditions. The color enumeration removes a common rotation in $\mu_6$ and orders cycles of equal length before matching their entries; the removed rotation is absorbed in the component phases. After graph isomorphism and the label normalization specified below, the retained presentations are listed in the next table. Here 123 denotes the neighbor set $\{1,2,3\}$ of a left vertex. Rows of a graph are listed in degree order. Colors and labels are retained finite presentations, not equivalence-class counts.

| Profiles | Left neighbor sets | Components | Colors | Labels |
|---|---|---|---|---|
| $EE$ | $(123, 123, 124, 34)$ | 1 | 4 | 40 |
| $EF$ | $(123, 234, 145, 15)$ | 1 | 2 | 368 |
| $FF$ | $(123, 12, 13, 45, 45)$ | 2 | 6 | 480 |
| $FF$ | $(123, 12, 14, 35, 45)$ | 1 | 2 | 3744 |
| $FF$ | $(123, 14, 24, 15, 35)$ | 1 | 1 | 2592 |
| $FF$ | $(234, 12, 13, 15, 45)$ | 1 | 1 | 2880 |

To normalize the labels, choose the first right vertex $k$ and its first two left neighbors $i, j$, and impose

$$b_i = 0, \qquad b_j = 1, \qquad c_k = 0.$$

The edge differences force $b_i \neq b_j$, so independent translations on the 2 sides followed by a common nonzero field scaling achieve this. In every other connected component, set its first vertex label to zero; its removed common label is absorbed into $t_s$. Indeed, translating all left and right labels by $B, C$, respectively, shifts the column index by $C - B$ and multiplies $y, v$ by $w^{6B}, w^{6C}$. These translations amount to column and row equivalences. To recover representatives up to these equivalences one must still allow all ten common nonzero field multipliers.

Only the third row of the table has more than one connected component. Its components have 7 and 4 edges. It gives affine one-parameter families; all the other graph presentations have no continuous parameter. The $AAA$ branch is the finite complete-mapping problem used again in the square-completion calculation below: after normalization it consists of permutations $\pi$ with $\pi(0) = 0$ and $j + \pi(j)$ also a permutation. There are 3441 such normalized maps. □

With the same $w = e^{\pi i/33}$, let $|q| = 1$. An explicit family from the disconnected $FF$ graph is

$$H(q)_{0j} = 1, \qquad H(q)_{1j} = w^{6j}, \qquad H(q)_{2j} = w^{a_j} q^{d_j}, \quad 0 \le j \le 10,$$

where

$$(a_j) = (0, 23, 56, 40, 2, 41, 22, 35, 8, 7, 44),$$
$$(d_j) = (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0).$$

Thus the $q$ factors occur precisely in columns $4, 5, 7, 8$, with columns numbered from zero. Writing the third row as $v$ and the second as $u$, explicit cycle supports are

$$\begin{array}{r|l} v & \{0,6,10\};\ \{1,2\};\ \{3,9\};\ \{4,7\};\ \{5,8\} \\ v/u & \{0,2,3\};\ \{1,10\};\ \{6,9\};\ \{4,5\};\ \{7,8\}. \end{array}$$

In each line, the first block is a 3-cycle and the remaining 4 blocks are antipodal pairs. On each block the power of $q$ is constant. These supports prove regularity for every $q \in \mathbb{T}$, and the middle row is the full 11-cycle. In particular $H(q)H(q)^* = 11I_3$ identically in $q$. The code independently verifies every Laurent coefficient of each row scalar product by reduction modulo $\Phi_{66}$ over the integers. The cross ratios $H_{ij}H_{k\ell}\bar{H}_{i\ell}\bar{H}_{kj}$ form a finite multiset invariant under equivalence. The cross ratio $qw^2$ therefore shows that each equivalence class meets this family in finitely many parameter values [10, 26].

Which of these triples survive completion? Corollary 1.4 already excludes the mixed triples in a square matrix. We give a second proof from the cycle decompositions, before counting how far the level-11 triples extend. Return to $w = e^{2\pi i/11}$ and let $H$ be a regular square matrix with a distinguished 11-cycle quotient. Normalize its distinguished rows to 1 and $u = (w^j)_{j=0}^{10}$. For any other row $v$, put $y = v/u$. Lemma 4.1 and the profile exclusion above show that either both $y, v$ are 11-cycles, or both have profiles $E$ or $F$. The same overlap graph therefore controls every row of the square matrix.

In the latter case their graph has at most 10 vertices and minimum degree 2. Each connected component has at least 4 vertices, so there are at most 2 components. Within a component, ratios of cycle phases belong to $\mu_{66}$. Consequently the entries of $v$ lie in the union of at most 2 rotated copies of $\mu_{66}$. The same conclusion holds for an $A$ row, which needs just one copy.

**Lemma 4.3.** *Let $H$ be a regular Hadamard matrix of order 11 with an 11-cycle row quotient. Every quotient of distinct rows of $H$ decomposes using only cycles of lengths 2, 3, and 11.*

*Proof.* Each row lies in at most 2 cosets of $\mu_{66}$, so the quotient of any 2 rows lies in at most 4 such cosets. A rotated 5-cycle or 7-cycle intersects a single coset of $\mu_{66}$ in at most one value: the ratio of 2 distinct common values would lie both in $\mu_{66}$ and in $\mu_5$ or $\mu_7$. 4 cosets cannot contain either cycle. Regularity and the list of prime partitions of 11 give the result. □

This argument uses only the graph size and the phase relations. It does not require the detailed enumeration of the 6 3-row support graphs.

**Proposition 4.4.** *Let $p$ be prime. Suppose a complex Hadamard matrix of order $p$ has every row quotient decomposable using only 2-, 3-, and $p$-cycles. If one row quotient is a $p$-cycle, then every row quotient is a $p$-cycle. In particular the matrix is equivalent to a member of $B(p, p)$.*

*Proof.* For $p = 2, 3$ the only allowed partition of $p$ is the single part $p$. Assume $p > 3$. Let $G \subset \mathbb{T}$ be generated by the entries of $H$, $\mu_6$ and $\mu_p$. Put $O = \mathbb{Z}[e^{2\pi i/3}]$ and form the commutative ring

$$R = \mathbb{Z}[G] \otimes_{\mathbb{Z}[\mu_6]} O,$$

using the usual inclusion of $\mu_6$ in $O$. It is free over $O$ on representatives of $G/\mu_6$. Write $[z]$ for the image of $z \in G$ and extend $[z]^* = [z^{-1}]$ by conjugation on coefficients. The sum of the absolute values of the coefficients defines $\|f\|_1$ independently of the representatives. Each nonzero coefficient has absolute value at least one, by the Eisenstein norm.

Put $S = \sum_{z \in \mu_p} [z]$ and $e = S/p$ in $R \otimes \mathbb{Q}$. Then $e^2 = e$. For $M = ([H_{ij}])$, a 2- or 3-cycle contributes zero to a row product and a $p$-cycle contributes a monomial times $S$. Hence $(1-e)MM^* = p(1-e)I$. Over the commutative ring with identity $1 - e$ a square right inverse is a left inverse, by the adjugate formula. Thus $(1-e)M^*M = p(1-e)I$ as well.

Every off-diagonal column product $f$ therefore satisfies $f = ef$ and is fixed by multiplication by $[z]$ for $z \in \mu_p$. These multiplications permute $G/\mu_6$ in orbits of length $p$, preserving coefficient

magnitudes. A nonzero orbit contributes at least $p$ to $\|f\|_1$. Yet $f$ is a sum of just $p$ monomials. If $f \neq 0$, all summands must occupy distinct cosets of one orbit. Invariance then identifies the original summands, one by one, as a rotated $p$-cycle.

Choose an integer $k \equiv 1 \pmod 6$, $k \equiv 0 \pmod p$. The map $[z] \mapsto z^k$ respects the coefficients in $O$. Applied to $M$, it gives a flat matrix in which distinct rows are orthogonal or proportional according to their original cycles. The column calculation gives the same alternative for the columns. The distinguished row pair becomes proportional, so Lemma 1.1 forces rank one. Every row quotient must therefore be a $p$-cycle, since a sum of 2- and 3-cycles would still vanish. Dephasing gives entries in $\mu_p$. □

**Theorem 4.5.** *Let $H$ be a regular complex Hadamard matrix of order 11. If some quotient of 2 rows is a single 11-cycle, then $H$ is equivalent to $F_{11} = (w^{ab})_{a,b=0}^{10}$, where $w = e^{2\pi i/11}$.*

*Proof.* Apply Proposition 4.4 with $p = 11$, using Lemma 4.3. It excludes every mixed regular square completion in the distinguished-11-cycle branch, including all values of the free phases in the previously obtained 3-row affine families.

We can now track completions inside $B(11, 11)$ row by row. After dephasing and permuting columns, its first 2 rows are 1 and $(w^j)_{j=0}^{10}$. Any further dephased row is $(w^{a_j})$, where

$$a_0 = 0, \qquad (a_j)_{j=0}^{10} \text{ and } (a_j - j)_{j=0}^{10} \text{ are permutations of } \mathbb{Z}/11\mathbb{Z}.$$

Indeed, a vanishing sum of 11 11th roots has one of each root: its exponent-count polynomial has degree at most 10 and is a multiple of $\Phi_{11} = 1 + x + \cdots + x^{10}$.

There are exactly 3441 such candidate rows. Form a graph $G$ by joining candidates $a, b$ when $(a_j - b_j)_{j=0}^{10}$ is a permutation. A square completion is exactly a clique of size 9 in this graph. This is the orthomorphism graph of Lazebnik and Thomason. Their Table 1 gives its 2016 edges, its unique 9-clique and the size 3 of its next-largest maximal clique [17]. Their Section 4.1 also identifies the isolated vertices and the six vertices of degree 162. Recomputing the graph gives the full degree distribution

| degree | 0 | 3 | 8 | 162 |
|---|---|---|---|---|
| number of vertices | 2640 | 660 | 135 | 6. |

The 9 Fourier candidates are $a_j = kj$, $k = 2, \ldots, 10$. 3 have degree 8 and 6 have degree 162; they form a complete graph $K_9$. All other vertices are excluded from a 9-clique as follows:

- 3300 have degree less than 8.
- The remaining 132 have degree exactly 8, but their 8 neighbors are not pairwise adjacent. For each one, the certificate lists an explicit nonadjacent pair of neighbors. A 9-clique containing that vertex would require its entire neighborhood to be complete.

Thus the Fourier $K_9$ is the unique square completion. This proves Theorem 4.5. □

Fix a nonlinear candidate $a$. The largest extension in which every quotient is an 11-cycle has $3 + \omega(G[N(a)])$ rows: the first two rows, $a$, and a clique in its neighborhood. We take the clique number of the empty graph to be zero. Counting by candidate gives

| Number of candidates | Largest total row count in an all-11-cycle extension |
|---|---|
| 2640 | 3 |
| 660 | 4 |
| 132 | 5 |

The six-row cutoff already follows from the maximal clique sizes in [17, Table 1]: four candidate rows must belong to the Fourier clique. The table above refines that cutoff for each normalized nonlinear third row. Its last line shows that five rows can occur. The exclusion of mixed triples from square completions uses Proposition 4.4.

**Corollary 4.6.** *Let $H$ be a regular complex Hadamard matrix of order 11. If the quotient of two columns is an 11-cycle, then $H$ is equivalent to $F_{11}$.*

*Proof.* Suppose no row quotient is an 11-cycle. Raising every entry of $H$ to the 11th power preserves each shorter prime cycle in its row quotients, since its length is coprime to 11. The resulting square matrix is therefore Hadamard. But the two specified columns become proportional, a contradiction. Thus some row quotient is an 11-cycle, and Theorem 4.5 applies. □

At order 11, one full cycle in a square matrix determined the entire Fourier class. At a larger prime every matrix in $B(p,p)$ already has such a cycle. To go further we use a feature of $F_p$ involving all rows and columns at once. Multiplication of the row labels by $g$ and the column labels by $g^{-1}$ preserves every entry $w^{ax}$. The choice of $g$ determines the lengths of the orbits.

## 5 Cyclic symmetries and quadratic residues

The circulant theorem of Hiranandani–Schlenker [11] says that a circulant member of $B(p,p)$ is equivalent to $F_p$. Its level assumption matters. Cocyclic members of $B(p,p)$ are also Fourier, by Egan–Flannery–Ó Catháin [7, Corollary 5.9]. Thus cocyclic development alone does not give a new prime-order theorem.

Another natural symmetry fixes one row and one column and cycles the remaining $p-1$ rows and columns. In dephased form this gives a circulant core. Its Fourier uniqueness follows from the classification of Costas polynomials over prime fields by Muratović-Ribić, Pott, Thomson and Wang [19]. To see the connection, choose a generator $a$ of $\mathbb{F}_p^\times$ and write a core row as $(w^{f(a^j)})_j$, where $f$ permutes $\mathbb{F}_p^\times$. Orthogonality says that every map $x \mapsto f(dx) - f(x)$, $d \neq 1$, permutes $\mathbb{F}_p^\times$. Their theorem gives $f(x) = cx^r$ with $(r, p-1) = 1$, which yields the Fourier matrix by reindexing.

We therefore consider the next orbit structure. Write $p = 2m+1$. Suppose the row and column permutations both have cycle lengths $1, m, m$ (at $p = 3$ both are the identity). Dephasing at the distinguished fixed row and column preserves the symmetry and gives

$$H = \begin{pmatrix} 1 & e^t & e^t \\ e & A & B \\ e & C & D \end{pmatrix}, \tag{5.1}$$

where $e$ is the all-ones column of length $m$ and $A, B, C, D$ are circulant $m \times m$ blocks. The superscript $t$ denotes transpose. The row and column permutations need not be the same permutation: the indexing is chosen separately on the 2 sides. The Fourier matrix has this symmetry by multiplying row labels by a generator of the squares and column labels by its inverse.

The regular Petrescu seed $P_7$ from Section 2 shows why the level matters here. In the numbering of [24, Example 5.4], the permutation $(1\,2\,4)(3\,6\,5)$ preserves the displayed matrix when applied to both indices. Dephasing at the fixed index 7 preserves this symmetry. The entries are sixth roots, so the entrywise seventh power is $P_7$ itself and has rank seven. By Theorem 1.3 this matrix is inequivalent to every member of $B(7,7)$.

We now assume $H \in B(p,p)$. Put $w = e^{2\pi i/p}$, and let $Q, N$ be the sets of nonzero squares and nonsquares in $\mathbb{F}_p$. Write $\chi$ for the quadratic character, with $\chi(0) = 0$.

**Theorem 5.1.** *For a dephased matrix $H \in B(p,p)$ of the form (5.1), after possibly interchanging the 2 noninitial row blocks, each row of $A, D$ has exponent set $Q$, and each row of $B, C$ has exponent set $N$.*

*Proof.* Every noninitial row and column of a dephased matrix in $B(p,p)$ contains all $p$th roots once. Let $a, b, c, d$ be the row sums of the 4 circulants, which are also their column sums. Orthogonality to the first row and column gives

$$a + b = c + d = a + c = b + d = -1.$$

Hence $a = d$ and $b = c$. Equal sums of $m$ $p$th roots have equal multiplicities: subtract their exponent-count polynomials, use divisibility by $1 + X + \cdots + X^{p-1}$, and evaluate at $X = 1$. Thus $A, D$ have the same exponent set $S$, while $B, C$ have its complement $T$ in $\mathbb{F}_p^\times$.

The vector $(0, e, -e)^t$ is an eigenvector of $H$, with eigenvalue

$$\alpha = a - b = \sum_{s \in S} w^s - \sum_{t \in T} w^t.$$

Since $HH^* = pI$, we have $\alpha\bar{\alpha} = p$. We explain the small cyclotomic argument which identifies its signs. In $K = \mathbb{Q}(w)$ the prime $p$ is totally ramified: $(p) = P^{p-1}$, where $P = (1 - w)$ is fixed by conjugation. The ideal identity $(\alpha)(\bar{\alpha}) = (p)$ therefore gives $(\alpha) = P^m$. The quadratic Gauss sum

$$\tau = \sum_{x \in \mathbb{F}_p} \chi(x) w^x$$

satisfies $\tau\bar{\tau} = p$, so $(\tau) = P^m$ as well. Consequently $u = \alpha/\tau$ is a unit. Every conjugate of both numerator and denominator has absolute value $\sqrt{p}$, hence every conjugate of $u$ has absolute value one. Kronecker's elementary lemma makes $u$ a root of unity: the monic polynomials of its positive powers have bounded integral coefficients, so only finitely many powers can occur. The roots of unity in $K$ are $\{\pm w^r\}$; these cyclotomic facts are recalled in [28].

We have $\alpha = \pm w^r \tau$. Both coefficient vectors, indexed by $\mathbb{F}_p$, have sum zero and exactly one zero coefficient. Equality of their values at $w$ implies equality of the vectors, since their difference is constant and has sum zero. The zero coefficient is at 0 on the left and at $r$ on the right. Thus $r = 0$, and the signs are $\chi$ or $-\chi$. Hence $S = Q$ or $N$. Interchanging the 2 noninitial row blocks selects $S = Q$. □

It remains to determine how the exponents are ordered. One formulation uses permutations of the field. Normalize one row of the first orbit by labelling columns with its exponents $x \in \mathbb{F}_p$. Then all exponent rows can be written

$$0, \quad h^i, \quad g \circ h^i \qquad (0 \le i < m), \tag{5.2}$$

where $h(0) = g(0) = 0$, $h$ is one cycle on $Q$ and one on $N$, and $g$ exchanges $Q$ and $N$. The notation $h^i$ means iteration, so $h^0(x) = x$. The difference of any 2 distinct functions in (5.2) must be a permutation of $\mathbb{F}_p$. Conversely these conditions give the required Hadamard matrix and orbit action.

If we could force $h(x) = ax$ for a generator $a$ of $Q$, the first orbit would already give $m$ Fourier rows, and Theorem 3.1 would finish the proof. One sufficient condition would be

$$\chi(h(x) - h(y)) = \chi(x - y) \qquad (x \ne y). \tag{5.3}$$

Indeed every secant slope of the graph of $h$ would then be a square, so the direction theorem would make $h$ linear. We next approach the ordering problem through the four sequences of exponents themselves.

## 6 Complementary blocks and their differences

The complementary submatrices of a unitary matrix carry the same singular values, apart from the extra copies of 1 on the larger side. Indeed, if $U = \left(\begin{smallmatrix} E & B \\ C & L \end{smallmatrix}\right)$ is unitary with $E, L$ square, then $I - E^*E = C^*C$ and $I - LL^* = CC^*$. The two right sides have the same nonzero spectrum, including multiplicities. This observation of Szöllősi is recalled in [2, Theorem 2.3]. Under a strict norm bound, the polar part of a complementary block of a real Hadamard matrix is given in [2, Lemma 3.2]. An $(m+1)$-square corner of a Hadamard matrix of order $2m+1$ already has norm $\sqrt{p}$, by the extra singular value. For this larger corner the stated strict bound of [2, Lemma 3.2]

fails. Lemma 6.6 gives the normalized identity also at this endpoint. Complementary minors in real Hadamard matrices are studied in [13, 14] and, for embedding questions and determinant values, by Christou, Mitrouli and Seberry [4].

For the four circulants in (5.1), apply the unitary observation separately at each cyclic frequency. Write their entries at position $(i, j)$ as $w^{a_{j-i}}, w^{b_{j-i}}, w^{c_{j-i}}, w^{d_{j-i}}$. Thus $a, d$ order $Q$ and $b, c$ order $N$. For any such sequence write

$$\Delta_s a = \{a_{j+s} - a_j : j \in \mathbb{Z}/m\}$$

as a multiset. We call an ordering $a$ of $Q$ and an ordering $b$ of $N$ complementary if

$$\Delta_s a \ \sqcup \ \Delta_s b = \mathbb{F}_p^\times \qquad (0 \neq s \in \mathbb{Z}/m). \tag{6.1}$$

**Proposition 6.1.** *In* (5.1) *the opposite blocks satisfy* $\Delta_s a = \Delta_s d$ *and* $\Delta_s b = \Delta_s c$ *for every* $s$. *Each of* $a, d$ *is complementary to each of* $b, c$. *The remaining row equations are*

$$\{a_{j+s} - c_j : j \in \mathbb{Z}/m\} \ \sqcup \ \{b_{j+s} - d_j : j \in \mathbb{Z}/m\} = \mathbb{F}_p^\times \qquad (s \in \mathbb{Z}/m). \tag{6.2}$$

*Conversely, the exponent sets, complementarity in the two row orbits, and* (6.2) *suffice for the Hadamard equations.*

*Proof.* Put $A_j = w^{a_j}$ and use the same convention for the other blocks. Write $\widehat{A}_k = \sum_j A_j v^{jk}$ with $v = e^{2\pi i/m}$. For $k \neq 0$, the two orbit vectors with coordinates $v^{jk}$ span a subspace on which $H/\sqrt{p}$ acts by the unitary matrix

$$\frac{1}{\sqrt{p}} \begin{pmatrix} \widehat{A}_k & \widehat{B}_k \\ \widehat{C}_k & \widehat{D}_k \end{pmatrix}.$$

The opposite entries have equal absolute value. For $k = 0$ we already have $\widehat{A}_0 = \widehat{D}_0$ and $\widehat{B}_0 = \widehat{C}_0$ by Theorem 5.1. Fourier inversion of $|\widehat{A}_k|^2 = |\widehat{D}_k|^2$ gives $\sum_j w^{a_{j+s}-a_j} = \sum_j w^{d_{j+s}-d_j}$. The two exponent multiplicity vectors agree by the cyclotomic argument of Theorem 5.1; the same reasoning applies to $b, c$.

Two rows in one orbit have difference zero at the border and must take each nonzero exponent once in the core. This proves complementarity for $a, b$ and $c, d$ and hence for all four adjacent pairs. Two rows in different orbits give (6.2), including $s = 0$. Conversely these three kinds of row pairs, together with the all-ones row, account for every scalar product. □

There is also a constraint on the positions themselves. For a nonzero symbol $x$ let $i_a(x)$ be its position in $a$ when $x \in Q$, and use the corresponding notation in the other blocks. Let $S(x)$ be the sum of its two positions in the core.

**Proposition 6.2.** *For every* $x \in \mathbb{F}_p^\times$ *we have* $S(x) = S(-x)$ *in* $\mathbb{Z}/m$. *In particular, for* $p \equiv 3 \pmod 4$ *and* $x \in Q$,

$$i_c(-x) = i_a(x) + i_d(x) - i_b(-x) \pmod m.$$

*Proof.* Fix $t \neq 0$. For a given ordered pair of row orbits and a given displacement $s$, exactly one core column gives field difference $t$, by (6.1) and (6.2). Omit $s = 0$ when the two row orbits coincide. The sum of these displacements over the four ordered pairs is $4\sum_{s=0}^{m-1} s = 0$ modulo $m$.

For either column orbit let $u(x)$ denote the position of $x$ in its unique seed block within that column orbit. The same sum, taken over that column orbit, is

$$\sum_{x \neq 0, -t} (u(x+t) - u(x)) = u(-t) - u(t).$$

Adding the two column orbits gives $S(-t) - S(t) = 0$. For $p \equiv 3 \pmod 4$, $x$ and $-x$ belong to opposite square classes, giving the stated formula. □

Shifting the indices preserves every difference multiset. So does negating the entries and reversing their cyclic order. Translating all symbols by a field constant also preserves differences, but a translation preserving $Q$ or $N$ must be zero: summing the $m$ symbols gives $m$ times the translation equal to zero. For $m > 1$, each coset has sum zero, so the same observation removes any additive constant in a negated reversal between opposite blocks. We examine shifts and negated reversals in turn.

**Proposition 6.3.** *If $d_j = a_{j+r}$ and $c_j = b_{j+t}$ for some $r, t \in \mathbb{Z}/m$, then $H \sim F_p$.*

*Proof.* Shift the origin of the second row orbit by $t$. The two off-diagonal blocks are now identical, and the lower diagonal block has exponents $a_{j-i+r-t}$. In additive notation form the abelian group

$$G = \langle h, k \mid mh = 0,\ 2k = (r-t)h,\ h + k = k + h \rangle.$$

It has order $2m$, and $\langle h \rangle$ has order $m$. Give the first and second row orbits the labels $ih, -k + ih$ and the column orbits the labels $jh, k + jh$. Every core exponent depends only on the column label minus the row label. Its values define a bijection $f : G \to \mathbb{F}_p^\times$ by $f(jh) = a_j$, $f(k + jh) = b_j$.

The two integer relations have determinant $2m$, and their coefficients have greatest common divisor $\gcd(2, m, r - t)$. By the Smith normal form, $G$ is cyclic unless $m, r - t$ are both even, when $G \simeq \mathbb{Z}/m \times \mathbb{Z}/2$. In the latter case put $u = f^{-1}$ and fix $t' \neq 0$ in the field. The differences $u(x + t') - u(x)$ for $x \neq 0, -t'$ run through $G \setminus \{0\}$ once, by row orthogonality. Their sum telescopes to $u(-t') - u(t')$. The sum of $G$ is zero, since its four elements killed by 2 sum to zero and all other elements cancel in pairs. This contradicts the injectivity of $u$. Thus $G$ is cyclic, and the circular Costas theorem [19, Theorem 3.4], as in Section 5, gives $H \sim F_p$. □

**Proposition 6.4.** *For every odd prime $p \neq 5$ and every $r \in \mathbb{Z}/m$, neither $d_j = -a_{r-j}$ nor $c_j = -b_{r-j}$ is possible in a solution of the Hadamard equations, where $m = (p-1)/2$.*

*Proof.* For $p = 3$ negation exchanges $Q, N$, whereas each proposed equality is between orderings of the same coset. At $p = 5$ both equalities occur in $F_5$. Index the row and column orbits by $(-1)^i, 2(-1)^i$. Then $a_j = (-1)^j$, $d_j = -a_{-j}$, and $c_j = b_j = 2(-1)^j = -b_{1-j}$. Now take $p \geq 7$ and suppose $d_j = -a_{r-j}$. Then $\widehat{D}_k = v^{kr}\overline{\widehat{A}_k}$. For $k \neq 0$, the coefficient $\widehat{A}_k$ cannot vanish. Indeed $1 + X + \cdots + X^{p-1}$ is irreducible over $\mathbb{Q}(v)$ since $(p, m) = 1$ and the cyclotomic degrees multiply. The polynomial $\sum_j v^{jk} X^{a_j}$ has distinct exponents, a zero constant coefficient and nonzero coefficients on $Q$. It therefore cannot be divisible by that cyclotomic polynomial. Orthogonality of the two rows in the frequency matrix now gives

$$\widehat{C}_k = -v^{kr}\overline{\widehat{B}_k} \qquad (k \neq 0).$$

Hence $C_j + \overline{B_{r-j}}$ is constant, say $z$. If $z \neq 0$, the $m$ distinct values of $C_j$ lie on both circles $|u| = 1$, $|u - z| = 1$, which have at most two common points. If $z = 0$, a $p$th root is the negative of a $p$th root, impossible for odd $p$. Interchanging the column orbits proves the assertion for $b, c$ by the same argument. □

One can also compare the minors in opposite blocks before imposing any symmetry. Koukouvinos, Mitrouli and Seberry [13], and Koukouvinos, Lappas, Mitrouli and Seberry [14], study the values of high-order minors of real Hadamard matrices. Christou, Mitrouli and Seberry [4] use Jacobi's complementary-minor identity for embeddings. In the prime-level setting the different possible absolute values of a $2 \times 2$ minor are distinguished by the prime cyclotomic polynomial. This gives the following exact multiplicities.

**Proposition 6.5.** *Let $p = 2m + 1$ be prime, let $H \in B(p, p)$, and choose any $m \times m$ block $A$ with complementary $(m + 1) \times (m + 1)$ block $D$. For $1 \le t \le m$ let $n_X(t)$ count the $2 \times 2$ submatrices of $X$ whose determinant has absolute value $2\sin(\pi t/p)$. Then*

$$n_D(t) = n_A(t) + m^2 \qquad (1 \le t \le m).$$

*Proof.* The difference of any two exponent rows of $H$ is a permutation, so every $2 \times 2$ determinant has one of the stated nonzero absolute values. Let $M_2(X)$ be the sum of their squares. By Cauchy–Binet it is the second elementary symmetric function of the squared singular values of $X$. The unnormalized blocks $A, D$ have the same singular values with one extra $\sqrt{p}$ for $D$. Therefore

$$M_2(D) - M_2(A) = p\ \mathrm{tr}(A^*A) = pm^2.$$

Put $c_t = n_D(t) - n_A(t)$. Counting all rectangles gives $\sum c_t = \binom{m+1}{2}^2 - \binom{m}{2}^2 = m^3$. Since the squared magnitude at $t$ is $2 - w^t - w^{-t}$, we obtain

$$m^2 + \sum_{t=1}^{m} c_t(w^t + w^{-t}) = 0.$$

Replacing $w^{-t}$ by $w^{p-t}$ gives a polynomial of degree at most $p - 1$ vanishing at $w$. It is $m^2(1 + X + \cdots + X^{p-1})$ by its constant coefficient. Hence $c_t = m^2$ for every $t$. □

For instance, take $p = 19$ and prescribe the Fourier $Q \times Q$ block. Each nonzero difference of two squares occurs four times among ordered pairs: the number is constant under square scalings and under negation, and $-1$ is a nonsquare. For a Fourier rectangle its cross-ratio exponent is the product of its row and column differences. For each nonzero product there are $18 \cdot 4^2$ ordered choices. Passing to products up to sign and to unordered row and column pairs gives $n_A(t) = 144$. The opposite $10 \times 10$ block must therefore contain exactly 225 minors of each of the nine magnitudes. By Jacobi's identity applied to $H/\sqrt{p}$, these also count the $(p - 2)$-square minors containing $A$, with magnitudes multiplied by $p^{(p-4)/2}$. This is an embedding test depending only on the two opposite blocks.

Complementation also answers a question about the Fourier rows of Section 3. Suppose we know the full rows of square slope and part of a row of nonsquare slope. Which entries of that row determine the rest? Here we allow arbitrary complex Hadamard matrices. The answer comes from the polar decomposition of the complementary block.

**Lemma 6.6.** *Write $U = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ for a complex unitary matrix with $A, D$ square and $A$ invertible. Put $R = (AA^*)^{1/2}$ and let $V$ be the unitary polar factor of $A$. The positive and unitary factors of $D$ are*

$$|D| = I - B^*(I + R)^{-1}B, \qquad \mathrm{Pol}(D) = D - CV^*(I + R)^{-1}B.$$

*In particular the 1-eigenspace of $|D|$ is $\ker B$.*

*Proof.* These are the normalized complex versions of the real formulas in [2, Lemma 3.2]. Put $T = |D|$. Block unitarity gives $T^2 = I - B^*B$, $R^2 = I - BB^*$ and $D^*C = -B^*A$. A singular value decomposition of $B$ gives $RB = BT$. Thus

$$B^*(I + R)^{-1}B = (I - T^2)(I + T)^{-1} = I - T.$$

Since $R$ is invertible, $\|B\| < 1$, so $T$ and $D$ are invertible. Using $AV^* = R$, left multiplication of the proposed unitary factor by $D^*$ gives

$$T^2 + B^*R(I + R)^{-1}B = T^2 + (I - T)T = T.$$

This characterizes $\mathrm{Pol}(D)$. The eigenspace assertion follows from $I - T^2 = B^*B$. The identities also apply when $\|A\| = 1$. □

Take now $U = F_p/\sqrt{p}$, with $Q$ first on both axes. Thus $A$ is the normalized $Q \times Q$ block, and the columns of $B$ are indexed by $\{0\} \cup N$. The square blocks with rows $Q$ and columns $Q$ or $N$ are invertible. Indeed, for a generator $h$ of $Q$ write the row index as $h^i$ and the column index as $ch^{-j}$, where $c = 1$ or $c \in N$. The block is circulant. Each eigenvalue, apart from normalization, is a sum $\sum_{k=0}^{m-1} v^{tk} w^{ch^k}$, with $v = e^{2\pi i/m}$. The minimal polynomial of $w$ over $\mathbb{Q}(v)$ is $1 + X + \cdots + X^{p-1}$, since $p$ and $m$ are coprime. Our sum has distinct nonzero exponents modulo $p$ and zero constant coefficient, so it cannot vanish. In particular $B$ has rank $m$, and $AA^* = I - BB^*$ gives $\|A\| < 1$: the smaller, unbordered corner satisfies the strict bound of [2, Lemma 3.2].

Put $s_N = \sum_{x \in N} w^x$. The columns indexed by $N$ sum to $s_N$ times the column indexed by 0. Consequently

$$\ker B = \mathbb{C}v_0, \qquad v_0 = (-s_N, 1, \ldots, 1)^t.$$

This line has a precise meaning for completion. Keep $A, B, C$ fixed and write $D_0$ for the Fourier fourth block. If $P$ denotes orthogonal projection onto $\mathbb{C}v_0$, all unitary completions have fourth block

$$D(q) = D_0(I + (q-1)P), \qquad |q| = 1.$$

Indeed $DB^* = -CA^*$ fixes $D$ on $(\ker B)^\perp$. On $\ker B$ it is an isometry into $\ker C^*$, also a line since $C = B^t$. Conversely, multiplying $U$ on the right by the block diagonal unitary with blocks $I$ and $I + (q-1)P$ gives each stated completion. The positive polar factor is fixed and the unitary factor varies by this one phase. Flatness imposes a stronger restriction, which can be applied to individual rows.

**Theorem 6.7.** *Let $p \geq 5$ be prime and fix the $m = (p-1)/2$ full Fourier rows of slopes $Q$. A unit-entry row orthogonal to them which agrees on the columns $Q$ with a Fourier row of slope $b \in N$ agrees with that row everywhere. In particular, among all complex Hadamard matrices, agreement with $F_p$ on its $Q$ rows and its $Q$ columns determines $F_p$ entry by entry.*

*Proof.* Subtract the row of slope $b$ from the given row. The difference vanishes on $Q$. Its conjugate on $\{0\} \cup N$ lies in $\ker B$. Thus on $N$ the given entries have the form $w^{bx} + t$ with a single $t \in \mathbb{C}$. The entry at 0 is $1 - \overline{s_N} t$. For $p \geq 7$ the $m \geq 3$ distinct points $w^{bx}$ lie on the unit circle both before and after translation by $t$. Two distinct circles meet in at most two points, so $t = 0$.

At $p = 5$ the two points are $w, w^{-1}$, since $bN = Q = \{1, -1\}$. The equations $|w+t| = |w^{-1}+t| = 1$ give $t = 0$ or $t = -(w + w^{-1})$. In the latter case the entry at 0 would be $1 + s_N(w + w^{-1}) = 0$, because $(w^2 + w^{-2})(w + w^{-1}) = -1$. Thus $t = 0$ here as well. For the matrix assertion this recovers every $N$ row. The last row is determined up to a scalar by orthogonality, and one prescribed entry fixes that scalar. □

The entrywise conclusion fails at $p = 3$. The constant row $(w^2, w^2, w^2)$ is orthogonal to $r_1$ and agrees with $r_2$ at the sole square column $x = 1$. In $F_3$ replace rows $r_0, r_2$ by $wr_2, w^2 r_0$, respectively. The resulting Hadamard matrix still agrees with $F_3$ on its square row and column.

For $p \geq 5$ one can recognize the Fourier equivalence class from fewer entries. Take an interval $I$ of $m$ consecutive nonzero slopes. Besides the full $Q$ rows, prescribe the Fourier entries on $(I \setminus Q) \times Q$. Theorem 6.7 recovers the missing entries of these rows. A column scaling shifts $I$ to $\{0, \ldots, m-1\}$, so Proposition 3.2 identifies the remaining rows up to their phases and order. For instance at $p = 19$, $I = \{1, \ldots, 9\}$ requires only the three extra row fragments of slopes $2, 3, 8$. No regularity or Butson assumption enters this argument.

For the two-orbit symmetry the entries of the four blocks are still unknown. What we have from complementation in that setting is the equality of the differences in opposite blocks. We now use these equalities to recover their cyclic orderings.

# 7 Ordering the squares and nonsquares

Suppose that $p \equiv 3 \pmod 4$, so $-Q = N$. Given an ordering of $Q$, its entrywise negative is an ordering of $N$. To decide when this is the only possible complement up to shift, we compare the positions of $x$ and $-x$. We begin with a single complementary pair, without assuming a solution of the mixed equations.

**Lemma 7.1.** *Let $p = 2m+1$ be prime with $m$ odd and suppose (6.1) holds. Define $u(x) \in \mathbb{Z}/m$ to be the position of $x$ in $a$ or $b$, according to its square class. Put $v(t) = u(t) - u(-t)$. For each $t \in \mathbb{F}_p^\times$,*

$$v(t) = \sum_{z \in Q} (\chi(z-1) - \chi(z+1)) v(tz) \quad \text{in } \mathbb{Z}/m. \tag{7.1}$$

*Proof.* Fix a nonzero field difference $t$. Among ordered pairs $(x, x+t)$ in the same square class, the position differences $u(x+t) - u(x)$ take each nonzero value of $\mathbb{Z}/m$ once by (6.1). Their sum is zero since $m$ is odd. In twice this sum the coefficient of $u(y)$, for $y \neq 0$, is

$$\chi(y)(\chi(y-t) - \chi(y+t)) - \mathbf{1}_{y=t} + \mathbf{1}_{y=-t}.$$

Indeed, for $y \neq 0$, twice the indicator that $z$ has the same nonzero square class as $y$ is $1 + \chi(y)\chi(z) - \mathbf{1}_{z=0}$. Changing $y$ to $-y$ in the term with $\chi(y+t)$ therefore gives $v(t) = \sum_{y \neq 0} v(y)\chi(y)\chi(y-t)$. Set $y = tz$ and pair $z$ with $-z$. Since $-Q = N$ and $v$ is odd, this gives (7.1). □

**Lemma 7.2.** *Let $p = 2m+1$ be prime with $m$ odd. If $g$ generates $Q$, put*

$$c(z) = \chi(z-1) - \chi(z+1), \qquad P(X) = \sum_{j=0}^{m-1} c(g^j) X^j - 1.$$

*Then $P(1) = 0$ in $\mathbb{Z}$ and $g^{P'(1)} = 4$ in $\mathbb{F}_p$.*

*Proof.* Inversion on $Q$ negates $\chi(z-1)$ and preserves $\chi(z+1)$. Thus $\sum_Q \chi(z-1) = 0$. Also

$$2 \sum_{z \in Q} \chi(z+1) = \sum_{x \neq 0} \chi(x+1) + \sum_{x \neq 0} \chi(1 + x^{-1}) = -2,$$

giving $P(1) = 0$. In the product $g^{P'(1)} = \prod_{z \in Q} z^{c(z)}$ the contribution from $\chi(z+1)$ cancels by inversion. Put $R = \{z \in Q : z - 1 \in Q\}$. As $\prod_{z \in Q} z = 1$, the remaining product is $(\prod_{z \in R} z)^2$.

The map $h(v) = (1+v)^2/(4v)$ on $Q$ takes $v = 1$ to 1. For $v \neq 1$, both $h(v)$ and $h(v) - 1 = (v-1)^2/(4v)$ are squares. Every $z \in R$ has the two distinct preimages $(\sqrt{z} \pm \sqrt{z-1})^2$ in $Q$. Consequently

$$\left( \prod_{z \in R} z \right)^2 = \prod_{v \in Q} \frac{(1+v)^2}{4v} = 4.$$

Here $4^m = 1$, and $\prod_{v \in Q}(1+v) = 2$ follows by evaluating $X^m - 1 = \prod_{v \in Q}(X - v)$ at $X = -1$. □

**Theorem 7.3.** *Let $p = 2m+1$ be prime, with $m = \ell^e$ a power of an odd prime $\ell$ and $e \geq 1$. Suppose 4 generates $Q$. If $a, b$ are complementary, then $b_j = -a_{j+k}$ for some $k \in \mathbb{Z}/m$. Consequently, if $a, d$ are orderings of $Q$ with $\Delta_s a = \Delta_s d$ for every $s$, and $a$ admits a complementary ordering of $N$, then $d$ is a cyclic shift of $a$.*

*Proof.* Let $T$ act on functions on $Q$ by $(Tf)(t) = f(tg)$. Lemma 7.1 gives $P(T)v = 0$. Write $P(X) = (X-1)V(X)$ in $\mathbb{Z}[X]$. By Lemma 7.2, $g^{V(1)} = 4$. As 4 has order $\ell^e$, $\ell \nmid V(1)$. Over $\mathbb{F}_\ell$, $X^m - 1 = (X-1)^m$, so $V(X)$ is relatively prime to $X^m - 1$. Since $T^m = I$, $V(T)$ is invertible modulo $\ell$. Its determinant is therefore a unit modulo $\ell^e$, and $V(T)$ is invertible over $\mathbb{Z}/m$. Hence $(T - I)v = 0$, so $v$ is constant on $Q$. If that constant is $k$, then $u(-a_j) = j - k$, giving $b_j = -a_{j+k}$. An ordering $d$ with the same difference lists as $a$ has the same complement $b$, so applying the first assertion to $d, b$ proves the second. □

**Theorem 7.4.** *Let $p = 2m + 1$ be prime with $m = \ell^e$ an odd prime power, and suppose 4 generates $Q$. Every $H \in B(p, p)$ admitting a simultaneous pure row and column symmetry of type $(1)(m)(m)$ is equivalent to $F_p$. In particular this holds whenever $m$ is an odd prime.*

*Proof.* Dephase using the fixed row and column. Their entries are constant on the corresponding orbits, so dephasing preserves the permutation symmetry. By Theorem 5.1 and Proposition 6.1, $a, d$ have the same differences and the common complement $b$. Theorem 7.3 makes them shifts. Both $b$ and $c$ are shifts of $-a$ by the same theorem. Proposition 6.3 now gives $H \sim F_p$. If $m$ is an odd prime, $4 \in Q$ and $4 \neq 1$, so 4 generates $Q$. □

This includes $p = 7, 11, 23, 47, 59$ by the prime case. It also covers $p = 19$ without an enumeration, since $|Q| = 9$ and $4^3 \equiv 7 \pmod{19}$. If $H$ starts at another Butson level, or is regular, a single $p$-cycle or the rectangle of Proposition 1.5 suffices to reach level $p$. Dephasing at the fixed row and column retains both the symmetry and the level-$p$ conclusion.

For general odd $m$, the proof gives a test involving only polynomials. With $P = (X - 1)V$ as above, suppose that

$$\gcd\left(V(X), X^m - 1\right) = 1 \quad \text{in } \mathbb{F}_\ell[X] \quad \text{for every prime } \ell \mid m.$$

Then the determinant of $V(T)$ is a unit at every prime divisor of $m$, hence a unit in $\mathbb{Z}/m$. The same argument gives shift uniqueness and Fourier recognition. A nonconstant gcd leaves the ordering question open by this argument.

For example, at $p = 67$ we can take $m = 33$ and $g = 4$. Modulo 3 it suffices to test against $X^{11} - 1$, and modulo 11 against $X^3 - 1$, since the omitted factors are repetitions in the corresponding characteristic. The two remainders of $V$ are

$$-X^{10} - X^6 + X^5 + X^4 - X^3 - X \pmod 3, \qquad -3X^2 + X + 3 \pmod{11}.$$

The Euclidean algorithm gives gcd 1 in both cases, so the symmetry recognizes $F_{67}$. The same test works at $p = 71$ with $g = 49$: the remainders of $V$ modulo $X^7 - 1$ over $\mathbb{F}_5$ and $X^5 - 1$ over $\mathbb{F}_7$ are $-2X^5 - 2X^3 + 2X^2 + X + 2$ and $-3X^4 - 2X^3 - 3$, each coprime to the corresponding modulus. At $p = 31$, with $m = 15$ and $g = 9$, we get $V(1) = -6$. The test therefore fails modulo 3. The next calculation settles this order using the difference multisets.

The following finite result uses the full multisets. It includes an even value of $m$ at $p = 29$ and an odd composite value at $p = 31$.

**Proposition 7.5.** *For every odd prime $p \leq 31$, the only member of $B(p, p)$ with the symmetry (5.1), up to equivalence, is $F_p$.*

*Proof.* For $p \leq 17$ this follows already from [12]. For the four remaining primes we enumerate the orderings as follows. Fix the origin of an ordering of $Q$ by $a_0 = 1$. For a partial ordering, retain a set of directed differences for each nonzero displacement modulo $m$. When a value is appended, insert the differences to and from every earlier position. A repetition within any one displacement rejects the prefix. Every admissible ordering has a unique path in this recursion. An independent enumeration used the equivalent test that all unordered pair sums of the points $(j, a_j)$ in $(\mathbb{Z}/m) \times \mathbb{F}_p$, including doubled points, are distinct. Indeed, an equality of two different unordered pair sums can be rearranged as an equality of two different directed differences, and conversely. Both enumerations gave identical lists.

Call $(\Delta_s a)_{s \neq 0}$ the signature of $a$. Fix a nonsquare $n$. Multiplication of the lists by $n$ gives every ordering of $N$ up to shifts. Match signatures by taking their set complements in $\mathbb{F}_p^\times$ at each displacement. The exact counts, using only rotations to normalize the individual sequences, are

| $p$ | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 |
|---|---|---|---|---|---|---|---|---|---|
| Admissible square orderings | 1 | 2 | 4 | 12 | 56 | 66 | 230 | 396 | 552 |
| Distinct signatures | 1 | 2 | 4 | 6 | 28 | 66 | 230 | 198 | 552 |
| Orderings admitting a complement | 1 | 2 | 4 | 2 | 4 | 6 | 10 | 6 | 8 |

At $19, 23, 31$ all the signatures are distinct. At 29 each signature consists of an ordering and its negated reversal. Every ordering in the last line of the table is geometric.

For the final test choose the origins of the two row and two column orbits so that $a_0 = 1$ and $b_0 = c_0 = n$. The block shifts are differences of a column origin and a row origin, so these three choices are independent. Select $a, d$ with identical signatures, and $b, c$ with the complementary signature. Run through all $m$ remaining shifts of $d$, and test (6.2) for every $s$, including 0. At $19, 23, 29, 31$ respectively, this makes $54, 110, 672, 120$ tests of quadruples and leaves $6, 10, 6, 8$. In each case the survivors have precisely the form

$$(a_j, b_j, c_j, d_j) = (g^j, ng^j, ng^j, n^2 g^j), \qquad \langle g \rangle = Q.$$

The core exponents are products of row labels $g^{-i}, ng^{-i}$ with column labels $g^j, ng^j$. Together with the border this gives $F_p$. □

We turn to even $m$, writing $p = 4h + 1$ and $m = 2h$. Fix a primitive root $n$ of $\mathbb{F}_p$, and put $K = \langle n^4 \rangle$. Both $Q$ and $N$ are unions of two cosets of $K$. Our first question is whether these cosets can be read from the parity of the positions in a complementary pair $a, b$.

For $1 \le y \le m$ let $S_y$ be $Q$ or $N$ according as $y \in Q$ or $y \in N$. Since $-1 \in Q$, $y$ represents the pair $\{y, -y\} \subset S_y$. Form the following matrix $M$ over $\mathbb{F}_2$, with $m$ columns. Its first $m$ rows and its two last rows are

$$M_{ty} = \mathbf{1}_{y-t \in S_y} + \mathbf{1}_{-y-t \in S_y} \quad (1 \le t, y \le m), \qquad (\mathbf{1}_{y \in Q})_y, \quad (\mathbf{1}_{y \in N})_y.$$

**Theorem 7.6.** *Let $p = 4h + 1$ be prime, $m = 2h$, and let $n$ be a primitive root modulo $p$. Put $K = \langle n^4 \rangle$ and suppose the matrix $M$ above has rank $m$ over $\mathbb{F}_2$. For any complementary pair, rotate the two orderings so that $a_0 = 1$ and $b_0 = n$. Their even and odd positions have the following exponent sets:*

$$\{a_{2j}\} = K, \qquad \{a_{2j+1}\} = n^2 K, \qquad \{b_{2j}\} = nK, \qquad \{b_{2j+1}\} = n^3 K.$$

*Proof.* Write $u(x)$ for the position of $x$ in its ordering, and put $z_y = u(y) + u(-y) \pmod 2$. For fixed $t \neq 0$, the pairs $x, x + t$ in the same square class give every nonzero position gap once, by (6.1). Summing their gaps modulo 2 gives $h$. The coefficient of $u(y)$ is the number modulo 2 of its neighbours $y - t, y + t$ in its class. This is also the coefficient of $u(-y)$, giving the first $m$ equations of $Mz = h\mathbf{1}$. The last two hold because each ordering has $h$ odd positions. The constant vector $z_y = h$ solves these equations: the coefficients in the row indexed by $t$ count the $m - 1$ ordered pairs of that difference and each of the two class rows has $h$ entries equal to one. Full rank now gives $u(-y) - u(y) \equiv h \pmod 2$ everywhere.

Set $w = e^{2\pi i/p}$ and form

$$A_1 = \sum_{x \in Q} (-1)^{u(x)} w^x, \qquad B_1 = \sum_{x \in N} (-1)^{u(x)} w^x.$$

In $|A_1|^2 + |B_1|^2$, the coefficient at each nonzero field difference is $\sum_{s=1}^{m-1} (-1)^s = -1$ and the coefficient at zero is $p - 1$. Hence $|A_1|^2 + |B_1|^2 = p$. The parity just proved gives $\bar{A}_1 = (-1)^h A_1$ and $\bar{B}_1 = (-1)^h B_1$. Thus $Z = A_1 + iB_1$ satisfies $Z\bar{Z} = p$.

In $\mathbb{Q}(i, w)$, each automorphism $\sigma_t : w \mapsto w^t$ fixing $i$ fixes both primes above $p$. Indeed $p$ splits in $\mathbb{Q}(i)$ and the $p$th cyclotomic extension is totally ramified at either prime (the polynomial $\Phi_p(1 + X)$ is Eisenstein there). The ideal of $Z$ is supported above $p$, so $\sigma_t(Z)/Z$ is a unit. All its conjugates have absolute value one, since the field is abelian and $Z\bar{Z} = p$. Kronecker's lemma and the roots of unity in this cyclotomic field give $\sigma_t(Z)/Z = \eta_t w^{r_t}$ with $\eta_t^4 = 1$ [28].

The coefficient function $f$ of $Z$ is zero at 0, has values $\pm 1$ on $Q$ and $\pm i$ on $N$, and has sum zero. Equality of sums in $w$ with coefficients in $\mathbb{Q}(i)$ determines these coefficients up to an additive constant, by $\Phi_p$. Both coefficient sums are zero, so the vectors coincide. Their unique zero gives $r_t = 0$. Consequently $f(t^{-1}x) = \eta_t f(x)$, and $f(x)/f(1)$ is a multiplicative character. Our rotations give $f(1) = 1$ and $f(n) = i$. Hence $f(n^j) = i^j$, which proves the four assertions. □

The mixed equations can now distinguish the two possible parities of a position gap. This gives a second matrix test, over the prime divisors of $h$. Its integer matrix $L$ has one column per element of $Q$ and one row per $(t, j)$ with $t \neq 0$ and $0 \leq j < 4$. Write $e_x$ for the coordinate row at $x \in Q$. For each pair $x, y \neq 0$ with $y - x = t$ and $y/x \in n^j K$, add the following to that row:

$$\begin{cases} e_y - e_x & j \text{ even and } x, y \in Q, \\ 0 & j \text{ even and } x, y \in N, \\ e_z & j \text{ odd, where } z \text{ is the square member of } \{x, y\}. \end{cases}$$

**Theorem 7.7.** *Let $p = 4h + 1$ be prime and put $m = 2h$. Suppose the quartic alternation of Theorem 7.6 holds for every complementary pair, and $L$ has rank $m - 1$ over $\mathbb{F}_\ell$ for each prime $\ell \mid h$. Then every $H \in B(p, p)$ with the symmetry* (5.1) *is equivalent to $F_p$.*

*Proof.* Use independent origins to make $a_0 = 1$ and $b_0 = c_0 = n$. The assumed alternation gives the position parities of $a, b, c$, since both $b$ and $c$ complement $a$. It gives those of $d$ up to a constant, since $d$ complements $b$. We determine that constant. At the alternating cyclic frequency, $B_1 = C_1$, and $D_1$ is either $A_1$ or $-A_1$. Here $C_1, D_1$ are the alternating sums defined as in the preceding proof. All four sums are nonzero by $\Phi_p$. If $D_1 = A_1$, the scalar product of the two frequency rows would be $A_1\bar{B}_1 + B_1\bar{A}_1 = 2(-1)^h A_1 B_1 \neq 0$. Thus $D_1 = -A_1$.

Take the reference Fourier words $a_j^0 = g^j$, $b_j^0 = c_j^0 = ng^j$, $d_j^0 = n^2 g^j$, with $g = n^2$. For each word $X$ its actual and reference positions have the same parity. Write their difference as $2E_X(x)$, with $E_X(x) \in \mathbb{Z}/h$. Set $W = E_a - E_d$ on $Q$ and $W' = E_b - E_c$ on $N$. We show $LW = 0$ and the corresponding equations on $N$ for $W'$.

For pairs in $Q$ with difference $t$, the parities of the position gaps are selected by the two classes $y/x \in K, n^2K$. At either parity, $a$ and $d$ have the same multiset of gaps by Proposition 6.1. The reference words have the same property. Subtract the reference sums from the actual sums and divide by two. This gives the even-$j$ equations for $W$. The same argument applies to $b, c$ on $N$.

For the odd-$j$ equations compare a mixed row difference and a mixed column difference. Write $(X, Y)$ when $y$ belongs to $X$, $x$ to $Y$, and the gap is $u_X(y) - u_Y(x)$. For each of the following three lists, as $y - x = t$ runs over its representations the gaps run through all of $\mathbb{Z}/m$ once:

$$((a, c), (b, d)), \qquad ((d, c), (b, a)), \qquad ((a, b), (c, d)).$$

These are respectively the mixed row equation, the reversed mixed column equation and the forward mixed column equation. Write $x = n^i$, $y = n^k$. In the first and third lists the reference gap has parity $(k - i + 1)/2 \pmod 2$; in the second it has parity $(k - i - 1)/2 \pmod 2$. This follows by substituting the four reference words above. Thus selecting $y/x \in n^j K$ selects one whole parity class for each list. The actual parities agree with the reference ones. The sum of the actual gaps therefore equals the sum of the reference gaps modulo $m$ for each selected list. Subtract and divide by two. Comparing the first list to the second leaves the sum of $W$ at the square endpoints. Comparing it to the third leaves the sum of $W'$ at the nonsquare endpoints. This proves the odd-$j$ equations.

Constants are in the kernel modulo $h$: even rows sum to zero and the odd rows count $h$ gaps of one parity. The matrix on $N$ is the same up to relabelling, by scaling $x, y, t$ by $n$. For each $\ell \mid h$ the rank hypothesis makes the kernel consist of constants modulo $\ell$. Subtract the value at one vertex and lift through the powers of $\ell$: a full-rank minor on the remaining $m - 1$ columns is a unit at $\ell$. Thus $W, W'$ are constant modulo $h$. The opposite words have constant differences of positions modulo $m$, since they do in the reference matrix. Proposition 6.3 finishes the proof. □

**Corollary 7.8.** *The two-orbit symmetry recognizes $F_p$ in $B(p,p)$ at each of the primes*

$$37,\ 41,\ 53,\ 61,\ 89,\ 149,\ 173,\ 197,\ 233.$$

*Proof.* Here are the ranks by integer row assembly as above and Gaussian elimination in the indicated prime fields. We use the least positive primitive root for $n$. The third column is over $\mathbb{F}_2$; each entry $\ell : r$ in the last column gives the rank $r$ of $L$ over $\mathbb{F}_\ell$.

| $p$ | $n$ | $M$ | $L$ | $p$ | $n$ | $M$ | $L$ |
|---|---|---|---|---|---|---|---|
| 37 | 2 | 18 | 3 : 17 | 89 | 3 | 44 | 2 : 43, 11 : 43 |
| 41 | 6 | 20 | 2 : 18, 5 : 19 | 149 | 2 | 74 | 37 : 73 |
| 53 | 2 | 26 | 13 : 25 | 173 | 2 | 86 | 43 : 85 |
| 61 | 2 | 30 | 3 : 29, 5 : 29 | 197 | 2 | 98 | 7 : 97 |
| | | | | 233 | 3 | 116 | 2 : 115, 29 : 115 |

Theorem 7.7 applies except at 41. There Theorem 7.6 still gives all four parity classes. We describe the remaining finite check, giving also 37 for comparison.

For a normalized complementary pair $a, b$, separate their even and odd slots into four words of length $h$, on $K, n^2K, nK, n^3K$, respectively. Generate all orderings of $K$ starting at 1. Retain a word when its $h$ directed differences at each displacement $1 \le s \le \lfloor h/2 \rfloor$ are distinct. Negative displacements give the negated lists. Scaling gives the normalized words on the other three cosets. Pair the words on $K, n^2K$ when their difference sets are disjoint at every such displacement. Match their unions with the complementary unions from the pair on $nK, n^3K$. These tests account for all nonzero even displacements of the interleaved words. Finally, try the $h$ rotations of each odd-slot word and test (6.1) at the odd displacements. The words in the even slots start at $1, n$ by normalization.

| $p$ | Words on $K$ | Disjoint pairs on $Q$ | Matched quadruples | Pairs $a, b$ | Both geometric |
|---|---|---|---|---|---|
| 37 | 9378 | 888 | 12 | 12 | 12 |
| 41 | 4620 | 520 | 32 | 16 | 16 |

The last column tests separately whether the successive ratios in $a$ and in $b$ are constant, including wraparound. Thus at 41 even a single complementary pair has geometric orderings. In a full matrix one geometric block suffices by Corollary 9.3. □

When the first rank test fails, its kernel gives a list of parity patterns $z$. One more consequence of the same differences can distinguish them. It uses only signs.

**Proposition 7.9.** *Let $p = 4h + 1$ be prime, put $m = 2h$, and let $z$ range over the solutions of $Mz = h\mathbf{1}$ over $\mathbb{F}_2$. For $1 \le y \le m$ introduce a bit $b_y$ and put*

$$s(y) = (-1)^{b_y}, \qquad s(-y) = (-1)^{b_y + z_y}.$$

*For each fixed $z$ the following congruences are affine linear equations over $\mathbb{F}_2$ in the bits $b_y$, after division by 4 whenever the constant term permits:*

$$\sum_{x \in Q} s(x) = \sum_{x \in N} s(x) = 0, \qquad 1 + \sum_{x, x+t \in Q \text{ or } x, x+t \in N} s(x)s(x+t) = 0 \pmod 8 \quad (1 \le t \le m).$$

*Every complementary pair supplies a solution. If the only surviving $z$ is the constant $h \bmod 2$, quartic alternation holds. This gives quartic alternation at $73, 97, 101, 109$, and Fourier recognition under the two-orbit symmetry at $73, 97, 101$.*

*Proof.* For a complementary pair take $s(x) = (-1)^{u(x)}$. Each word has equally many even and odd positions. For fixed $t \neq 0$ the position gaps of the indicated pairs run once through $1, \dots, m-1$, so the sum of their signs is $-1$. Both assertions hold over the integers.

To reduce a correlation modulo 8, pair $(x, y)$ with $(-y, -x)$, where $y = x + t$. Write $[x]$ for the representative of $\{x, -x\}$ in $1, \ldots, m$. A fixed pair contributes $(-1)^{z_{[x]}}$, independently of $b$. On an orbit of size two the terms cancel if $z_{[x]} \neq z_{[y]}$. Otherwise they add to $2e(-1)^{b_{[x]}+b_{[y]}}$, where $e$ is their sign at $b = 0$. Modulo 8 this is $2e + 4(b_{[x]} + b_{[y]})$. In either class sum the pair $x, -x$ likewise contributes zero or $2 + 4b_{[x]}$ modulo 8. Thus for each left side $F$ we first test $4 \mid F(0)$. If this holds, its equation over $\mathbb{F}_2$ has constant term $F(0)/4$ and coefficient $(F(e_y) - F(0))/4$ at $b_y$, where $e_y$ is the unit vector. If only the constant $z$ survives, the character argument in Theorem 7.6 gives the four quartic classes.

The counts below come from solving $Mz = h\mathbf{1}$, then eliminating in the displayed binary system for each solution. The last column gives the ranks of $L$ at the prime divisors of $h$, in increasing order.

| $p$ | $m$ | rank $M$ | Patterns $z$ | Surviving | Ranks of $L$ |
|---|---|---|---|---|---|
| 73 | 36 | 32 | 16 | 1 | 35, 35 |
| 97 | 48 | 40 | 256 | 1 | 47, 47 |
| 101 | 50 | 46 | 16 | 1 | 49 |
| 109 | 54 | 52 | 4 | 1 | 51 |

The Fourier pair supplies the constant pattern in every case. Theorem 7.7 applies at the first three primes. At 109 the remaining rank is 51 over $\mathbb{F}_3$, two below the required 53. □

We can sometimes recover the shifts even when the rank of $L$ falls short. Fix $p = 4h + 1$ and suppose the orderings have the quartic alternation of Theorem 7.6. For $x, y \in Q$ the parity of the gap from $x$ to $y$ in either square ordering is specified by $y/x \in K$ or $y/x \in Q \setminus K$, where $K$ is the group of fourth powers. For $t \neq 0$ and $e = 0, 1$, let $P_{te}$ consist of the ordered pairs $x, y \in Q$ with $y - x = t$ and with the specified gap parity $e$.

**Theorem 7.10.** *Let $p = 4h + 1$ be prime. Let $H \in B(p, p)$ have the form (5.1) with the quartic alternation of Theorem 7.6. Let $\ell$ be an odd prime divisor of $h$ and put $E = \ker_{\mathbb{F}_\ell} L$. Suppose every $v \in E$ satisfies $v(-x) = v(x)$. For each nonconstant $v \in E$, suppose the only even functions $s : Q \to \mathbb{F}_\ell$ satisfying*

$$\sum_{(x,y)\in P_{te}} (v(y) - v(x))(s(y) - s(x)) = 0 \qquad (t \neq 0,\ e = 0, 1)$$

*are the constants. Then in each pair of opposite blocks the difference of positions is constant modulo the full power of $\ell$ dividing $h$.*

*Proof.* Write $u_a, u_d$ for the positions in the square blocks, $U = u_a - u_d$ and $S = u_a + u_d$. By Proposition 6.2, $S$ is even. The proof of Theorem 7.7 gives $LU = 0$ modulo the $\ell$-part of $h$: $U$ differs from $2W$ by the constant difference of the reference positions, and $L$ kills constants modulo $h$. Thus $U$ is even modulo $\ell$. As 2 is invertible, $u_a, u_d$ are both even modulo $\ell$.

Suppose $U$ is nonconstant modulo $\ell^b$, where $\ell^b$ is the full power dividing $h$. Choose $k < b$ largest such that $U - U(1)$ is divisible by $\ell^k$ everywhere. Then $v = (U - U(1))/\ell^k \bmod \ell$ is a nonconstant member of $E$. For fixed $t, e$, the gaps in $a$ and $d$ on $P_{te}$ have identical multisets by Proposition 6.1. Their sums of squares therefore agree modulo $\ell^{k+1}$. Factoring the difference of the two squares gives

$$\sum_{(x,y)\in P_{te}} (U(y) - U(x))(S(y) - S(x)) = 0 \pmod{\ell^{k+1}}.$$

After division by $\ell^k$ the hypothesis makes $S$ constant modulo $\ell$, say $S = c$. In particular $u_d(x) = c - u_a(-x) \pmod{\ell}$.

We use a nontrivial character of $\mathbb{Z}/m$ of order $\ell$ to exclude this possibility. Put $z = e^{2\pi i/\ell}$ and write $A, B, C, D$ for the entries of the unnormalized frequency matrix in Proposition 6.1, so that $A = \sum_{x\in Q} z^{u_a(x)} w^x$ and likewise for the other words. The last congruence gives $D = z^c \bar{A}$.

As $A \neq 0$ by the minimal polynomial $\Phi_p$ over $\mathbb{Q}(z)$, row orthogonality gives $C = -z^c \bar{B}$. Both coefficient vectors in $w$ vanish at 0, so $\Phi_p$ forces equality of every coefficient. Since $-N = N$, at each $x \in N$ this requires

$$z^{u_c(x)} = -z^{c-u_b(-x)},$$

which is impossible for odd $\ell$. This proves the assertion for $a, d$. Scaling the symbols of $N$ by $n^{-1}$ identifies the equations for $b, c$ with those on $Q$. Interchanging the column orbits gives the same frequency contradiction. □

**Corollary 7.11.** *Every $H \in B(109, 109)$ admitting the two-orbit symmetry* (5.1) *is equivalent to $F_{109}$.*

*Proof.* Proposition 7.9 gives the quartic classes. Here $h = 27$ and $g = 36$ generates $Q$. Write $v_j = v(g^j)$ for $j \in \mathbb{Z}/54$. The first moment leaves three free values modulo 3, one on each residue class of $j$ modulo 3. In fact all these choices lift. We give the calculation to distinguish what the two moments tell us.

Set $Tv_j = v_{j+1}$, and for $t = 1, 6$ and $0 \leq r < 4$ form the row polynomial $B_{tr}(X) = \sum_{j=0}^{53} L_{(t,r),g^j} X^j$. Here 6 is a primitive root modulo 109. Every other row of $L$ is a cyclic translate of one of these eight, by square scaling. Modulo 27, each of the eight polynomials and $X^{54} - 1$ has zero remainder on division by

$$D(X) = X^3 + 3X^2 + 6X - 10.$$

These small divisions can be made by reducing each $X^j$, $j \geq 3$, to $10X^{j-3} - 6X^{j-2} - 3X^{j-1}$. Thus $D(T)v = 0$ gives solutions for arbitrary initial $v_0, v_1, v_2$. Modulo 3 these are precisely the 3-periodic functions, and account for the entire kernel since $\operatorname{rank}_{\mathbb{F}_3} L = 51$. The columns with $j \geq 3$ are consequently independent modulo 3 and have a minor which is a unit modulo 27. Each initial triple therefore has a unique solution at each modulus $3, 9, 27$. Up to constants the respective counts are $9, 81, 729$.

We now check the squared gaps. All 3-periodic $v$ are even, since $-1 = g^{27}$. Up to adding a constant, multiplying by a nonzero scalar and shifting $j$, the nonconstant triples are $(0, 0, 1)$ and $(0, 1, 2)$. For either triple, the space of even solutions $s$ in Theorem 7.10 is invariant under $T^3$ by square scaling. Evenness gives $s_{j+27} = s_j$, so $(T^3 - I)^9 = 0$ over $\mathbb{F}_3$. If the solution space modulo constants is nonzero, it has a nonzero class killed by $T^3 - I$. Subtracting $s_0$, we may therefore write

$$s_{3q+i} = c_i + qd, \qquad c_0 = 0, \quad i = 0, 1, 2.$$

Only three equations are needed. For $(t, e) = (1, 0), (1, 1), (2, 0)$ the coefficient matrices on $(c_1, c_2, d)$ for the two triples, respectively, are

$$\begin{pmatrix} 2 & 0 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 1 \\ 0 & 2 & 0 \end{pmatrix}.$$

For each row, sum over $0 \leq i, j < 54$ with $g^j - g^i = t$ and $j - i \equiv e \pmod 2$, weighting $s_j - s_i$ by $v_j - v_i$. Both determinants are 1 modulo 3, so only the constant solution survives. The theorem gives constant position differences modulo 27 for both opposite pairs. Quartic alternation already fixes these differences modulo 2. Together these give shifts modulo 54, and Proposition 6.3 completes the proof. □

We return to odd orbit length. At $p = 43$ we have $m = 21$, and the polynomial test alone leaves a gap. The polynomial $P$ determines the positions modulo 7, up to a common function on the squares. The mixed equations identify that function. We give the argument for any odd $m$ and any divisor $k > 1$ of $m$.

**Lemma 7.12.** *Let $p = 2m+1$ be prime with $m$ odd, and let $k > 1$ divide $m$. Let $H \in B(p,p)$ have the symmetry* (5.1) *and let $g$ generate $Q$. Suppose that each of*

$$i_b(-x) - i_a(x), \qquad i_c(-x) - i_a(x) \qquad (x \in Q)$$

*is constant modulo $k$. Then for some $r, h \in \mathbb{Z}/k$ with $(h,k) = 1$,*

$$i_a(g^j) = r + hj \pmod{k}.$$

*The three positions $i_b(-g^j), i_c(-g^j), i_d(g^j)$ have the same formula with possibly different constants $r$.*

*Proof.* Write $s, t$ for the respective constants. By Proposition 6.2, $i_d(x) = i_a(x) + s + t \pmod{k}$. Put $v = e^{2\pi i/k}$, $w = e^{2\pi i/p}$ and form the sums

$$A = \sum_{x \in Q} v^{i_a(x)} w^x, \qquad B = \sum_{x \in Q} v^{i_a(x)} w^{-x}.$$

At the cyclic frequency $v$, the four unnormalized entries of the frequency matrix of Proposition 6.1 are $A, v^s B, v^t B, v^{s+t} A$. Removing the row and column phases gives the matrix with diagonal entries $A$ and off-diagonal entries $B$. Its product with its adjoint is $pI_2$. Applying it to $(1,1)^t$ gives $Z\bar{Z} = p$ for $Z = A + B$.

Write $Z = \sum_x f(x) w^x$, where $f(0) = 0$ and $f(x) = f(-x) = v^{i_a(x)}$ for $x \in Q$. Since the positions in $a$ run through $\mathbb{Z}/m$, we have $\sum_x f(x) = 0$. As in the proof of Theorem 7.6, each automorphism $w \mapsto w^u$ fixing $v$ fixes every prime above $p$ in $\mathbb{Q}(v,w)$: $p \equiv 1 \pmod{k}$ splits in $\mathbb{Q}(v)$ and $\Phi_p(1+X)$ is Eisenstein at each such prime. Its action on $Z$ thus multiplies $Z$ by a unit whose conjugates all have absolute value one. This unit is a root of unity, of the form $\eta w^b$ with $\eta^{2k} = 1$ [28]. The corresponding two coefficient vectors in $w$ have sum zero. Since $\Phi_p$ is the minimal polynomial over $\mathbb{Q}(v)$, the vectors agree. Their unique zero gives $b = 0$, so $f(u^{-1}x) = \eta f(x)$ for every $x$. Taking $x = 1$ shows that $f(x)/f(1)$ is a multiplicative character on $\mathbb{F}_p^\times$. On $Q$ it takes every value of $\mu_k$, because all positions occur. Its value at $g$ therefore generates $\mu_k$, proving the formula. The three remaining formulas follow from the constant position differences. □

**Theorem 7.13.** *Every $H \in B(43,43)$ admitting the two-orbit symmetry* (5.1) *is equivalent to $F_{43}$.*

*Proof.* Take $g = 9$, of order 21 modulo 43. For any complementary pair let $v_j = u(g^j) - u(-g^j)$, as in Lemma 7.1. For the shift $Tv_j = v_{j+1}$ we have $P(T)v = 0$ and $T^{21} = 1$. Directly from the coefficients of Lemma 7.2 we get

$$\gcd(P, X^{21} - 1) = \begin{cases} (X-1)^2 & \text{over } \mathbb{F}_3, \\ X - 1 & \text{over } \mathbb{F}_7. \end{cases}$$

Indeed the remainders of $P$ modulo $X^7 - 1$ over $\mathbb{F}_3$ and $X^3 - 1$ over $\mathbb{F}_7$ are $-X^5 - X^3 - X^2 + X - 1$ and $3X^2 + 2X + 2$. Each has gcd $X - 1$ with its modulus. Modulo 3 the coefficients of $Y, Y^2$ in $P(1+Y)$ are $0, -1$, and modulo 7 the coefficient of $Y$ is $-1$. This gives the stated multiplicities.

Thus $v_j$ is constant modulo 7 and has constant first difference modulo 3. Equivalently, $v_j = c + 7ej \pmod{21}$ for some $c \in \mathbb{Z}/21$ and $e \in \mathbb{Z}/3$. In particular Lemma 7.12 applies with $k = 7$. The pairs $a, b$ and $d, b$ have a common nonsquare ordering, so subtracting their formulas gives

$$i_d(g^j) - i_a(g^j) = c' + 7e'j \pmod{21}.$$

The same reasoning with the common square ordering $a$ gives such a formula for $i_c(-g^j) - i_b(-g^j)$.

We show that the coefficient $e'$ vanishes. In both $a$ and $d$, the position gap from $x$ to $y$ is zero modulo 7 exactly when $y/x \in \langle g^7 \rangle = \{1, 6, 36\}$. Among pairs of squares with $y - x = 1$, just one has this property. Indeed $y = 6x$ gives $(26, 27)$, both nonsquares, and $y = 36x$ gives $(16, 17)$,

both squares. The difference lists of $a$ and $d$ agree at every displacement by Proposition 6.1. The displacement of this unique pair must therefore agree in the two words modulo 21. Now $16 = g^{12}$ and $17 = g^{19}$, so $7e'(19-12) = 0 \pmod{21}$ and hence $e' = 0$. Applying the same argument on $-Q$ to the negated pair $(-16, -17)$ of field difference $-1$ shows that the position difference between $b$ and $c$ is constant too. Both opposite blocks are shifts, and Proposition 6.3 gives $H \sim F_{43}$. □

**Corollary 7.14.** *For every odd prime $p \leq 109$, a matrix in $B(p,p)$ admitting a simultaneous row and column symmetry of cycle type $(1)(m)(m)$ on each side, with $m = (p-1)/2$, is equivalent to $F_p$.*

*Proof.* Proposition 7.5 covers $p \leq 31$. Corollary 7.8 gives $37, 41, 53, 61, 89$ and Theorem 7.13 gives 43. The prime case of Theorem 7.4 gives $47, 59, 83, 107$. The odd-order polynomial test above gives $67, 71$. For $79, 103$ take $g = 9, 25$, respectively. Direct division gives $\gcd(V, X^{39} - 1) = 1$ modulo $3, 13$ at 79 and $\gcd(V, X^{51} - 1) = 1$ modulo $3, 17$ at 103. Proposition 7.9 gives $73, 97, 101$, and Corollary 7.11 gives 109. □

# 8 An inverse ordering which cannot be completed

The distinction between sets and orderings is already visible in the following partial matrix. Suppose $p \equiv 1 \pmod 4$, and retain $m, Q, N, w$ from the preceding section. For $a \in Q$ define

$$f_a(0) = 0, \qquad f_a(x) = \begin{cases} ax & x \in Q, \\ a^{-1}x & x \in N. \end{cases} \tag{8.1}$$

Let $P$ have the all-ones row together with the $m$ rows $(w^{f_a(x)})_{x \in \mathbb{F}_p}$. The 2 cosets are ordered in opposite multiplicative directions.

**Theorem 8.1.** *For every prime $p \equiv 1 \pmod 4$, the matrix $P$ is a partial Hadamard matrix with $(p+1)/2$ rows. It admits an additional orthogonal row with entries in $\mu_p$ if and only if $p = 5$.*

*Proof.* Each $f_a$ is a permutation. For $a \neq b$, its difference with $f_b$ has multipliers $a - b$ on $Q$ and

$$a^{-1} - b^{-1} = -\frac{a-b}{ab}$$

on $N$. These multipliers have the same quadratic character because $-1, a, b \in Q$. Their images of the 2 cosets are complementary, so $f_a - f_b$ is a permutation. The cyclotomic criterion proves the partial Hadamard property.

At $p = 5$ inversion fixes both elements of $Q = \{1, -1\}$, so $P$ consists of rows of $F_5$. Otherwise $p \geq 13$. Suppose that an additional row exists. Multiply it by a $p$th root to write it as $(w^{g(x)})_x$ with $g(0) = 0$. The maps $g$ and $g - f_a$ are permutations. For fixed $x \in Q$, the set $\{f_a(x) : a \in Q\}$ is $Q$. Since $g - f_a$ already vanishes at 0, it cannot also vanish at $x$. Thus $g(x) \in N$. The same argument for $x \in N$ gives $g(x) \in Q$: the permutation $g$ exchanges the cosets.

We now work entirely over $\mathbb{F}_p$. For $1 \leq k \leq m-2$, the power sum of the permutation $g - f_a$ vanishes, so

$$\sum_{x \in Q} (g(x) - ax)^k + \sum_{x \in N} (g(x) - a^{-1}x)^k = 0 \qquad (a \in Q). \tag{8.2}$$

Reduce this Laurent polynomial modulo $a^m - 1$. Its coefficients vanish, since its reduced degree is less than $m$ and it vanishes at all $m$ elements of $Q$. The coefficient of $a$ receives only the term with binomial index 1 from the first sum: a term from the second would need index $m-1$, which exceeds $k$. Similarly the coefficient of $a^{-1}$ receives only index 1 from the second sum. Hence

$$\sum_{x \in Q} xg(x)^r = \sum_{x \in N} xg(x)^r = 0 \qquad (0 \leq r \leq m-3). \tag{8.3}$$

On either coset, write the restriction of $u = g^{-1}$ as its unique polynomial of degree less than $m$. Substituting $y = g(x)$ in (8.3) gives $\sum_y u(y)y^r = 0$ on that coset for $0 \le r \le m-3$. On a multiplicative coset of size $m$, the sum of the $d$th powers vanishes unless $m \mid d$. The equation $r = 0$ therefore kills the constant coefficient; the successive equations kill the coefficients of degrees $m-1, m-2, \ldots, 3$. Consequently

$$u(y) = Ay + By^2$$

on each coset, with potentially different $A, B$ on the 2 cosets.

The map $u$ exchanges the cosets, so $A + By = u(y)/y$ is always a nonsquare. If $B \neq 0$, the affine map $y \mapsto A + By$ is injective on its coset and therefore maps it onto $N$. Summing gives $mA = 0$, hence $A = 0$. But $By^2$ is not injective on this coset, since $-1 \in Q$ and $y, -y$ belong to the same coset. Thus $B = 0$ on both cosets. Inverting these linear restrictions shows that

$$g(x) = cx \ (x \in Q), \qquad g(x) = dx \ (x \in N), \qquad c, d \in N.$$

For $g - f_a$ to permute $\mathbb{F}_p$, its 2 nonzero multipliers must have equal quadratic character. Euler's criterion gives

$$(c-a)^m = (d - a^{-1})^m \qquad (a \in Q).$$

Reduce once more modulo $a^m - 1$. Since $m$ is even, comparison of the coefficients of $a$ and $a^2$ gives, respectively,

$$c^{m-1} = d, \qquad c^{m-2} = d^2.$$

The binomial coefficients cancelled here are nonzero modulo $p$, and $m \ge 6$ keeps these coefficients distinct from the constant term. Multiplication by $c$ and $c^2$ now gives

$$cd = c^m = -1, \qquad (cd)^2 = c^m = -1,$$

a contradiction. □

The obstruction concerns additional rows with entries in $\mu_p$. In the other congruence class $p \equiv 3 \pmod 4$, the construction gives two Fourier rows at $p = 3$. For $p \ge 7$ there are distinct $a, b \in Q$, and their difference multipliers have opposite characters, so these rows fail to be orthogonal.

Deleting one of the rows $f_a$ allows that row to be put back. When does the smaller matrix have a full completion?

**Corollary 8.2.** *Let $p \equiv 1 \pmod 4$ be prime. Delete any one noninitial row $f_b$ from the partial matrix in Theorem 8.1. The remaining $m$ rows have a completion in $B(p,p)$ if and only if $p = 5$.*

*Proof.* At $p = 5$ the matrix completes to $F_5$. Assume $p \ge 13$. Suppose a completion exists and normalize its first column to one by row scalings. In a column $x \in Q$ the prescribed exponents are 0 and all of $Q$ except $bx$. Since the whole column is a permutation of $\mathbb{F}_p$, exactly one of the $m+1$ additional rows has exponent $bx$ in that column. Across the $m$ columns of $Q$ there are only $m$ such occurrences. Some additional row, with exponents $g(x)$, therefore maps $Q$ into $N$. It is a permutation fixing 0, so it exchanges $Q$ and $N$.

For $1 \le k \le m-2$, let $P_k(a)$ denote the left side of (8.2) for this $g$. It vanishes for $a \in Q \setminus \{b\}$. Its average on $Q$ is $\sum_x g(x)^k = 0$: every nonconstant power $a^j$ that occurs has $0 < |j| < m$ and sums to zero. Hence $P_k(b) = 0$ as well. The coefficient argument of (8.3) and the coset argument following it now apply unchanged. They give $g(x) = cx$ on $Q$ and $g(x) = dx$ on $N$, with $c, d \in N$.

Consider $D(a) = (c-a)^m - (d - a^{-1})^m$. Orthogonality gives $D(a) = 0$ for $a \in Q \setminus \{b\}$. Its average on $Q$ is $(c^m + 1) - (d^m + 1) = 0$, since $m$ is even and $c^m = d^m = -1$. Thus $D(b) = 0$. The nonzero multipliers $c - b$ and $d - b^{-1}$ have the same quadratic character, so $g - f_b$ is a permutation too. This row would extend the original partial matrix, contrary to Theorem 8.1. □

## 9 A Fourier corner determines the matrix

We can now combine the obstruction with a theorem about a small graph. For $p \equiv 1 \pmod 4$, make a graph on $Q$ by joining $a, b$ when $a - b \in Q$. Muzychuk and Kovács [20] determine its full automorphism group. Over a prime field its elements are precisely

$$a \longmapsto ca \quad \text{and} \quad a \longmapsto c/a \qquad (c \in Q).$$

Thus an automorphism of the induced graph fixing 1 is either the identity or inversion.

For $p \equiv 3 \pmod 4$, orient the pair $x, y \in Q$ from $x$ to $y$ when $y - x \in Q$. Since $-1 \in N$, this gives a tournament. The next argument recovers the character of a sum from the directions of the edges.

**Lemma 9.1.** *Let $p \equiv 3 \pmod 4$ be prime. Every permutation $f$ of $Q$ preserving the character of differences is of the form $f(x) = cx$ for $c \in Q$.*

*Proof.* For $p = 3$, $Q = \{1\}$. Otherwise $m = |Q|$ is odd and $m > 1$. Over $\mathbb{F}_2$ form the matrix $M_{xy} = \mathbf{1}_{y-x \in Q}$ for $x, y \in Q$. Multiplication by a square preserves its entries, so $M$ is a sum of the commuting permutation matrices $R_t$ given by $(R_t)_{xy} = \mathbf{1}_{y=xt}$, $t \in Q$. Writing $M = \sum c_t R_t$ gives

$$M^{2^j} = \sum_{t \in Q} c_t R_{t^{2^j}} \qquad \text{over } \mathbb{F}_2.$$

Choose $j \geq 0$ with $2^{j+1} \equiv 1 \pmod m$. The inverse on $Q$ of $t \mapsto t^{2^j}$ is squaring. Consequently $(M^{2^j})_{xy} = M_{x^2,y^2}$. A permutation preserving $M$ also preserves this matrix. For distinct $x, y \in Q$, their squares are distinct, so $f$ preserves both $\chi(y - x)$ and $\chi(y^2 - x^2)$. Their product is $\chi(y + x)$. For $x = y$ the same conclusion follows from $\chi(2x) = \chi(2)$.

Extend $f$ to a permutation $F$ of $\mathbb{F}_p$ by $F(0) = 0$ and $F(-x) = -f(x)$ for $x \in Q$. Differences within $Q$ and within $-Q$ have the original character. Differences between the two cosets have the correct character by the sum identity. For a pair involving 0 this follows from $F(Q) = Q$ and $F(-Q) = -Q$. Thus every secant slope of the graph of $F$ is a square. There are at most $m$ such directions, so the direction theorem in Section 3 makes the graph a line. Since $F(0) = 0$ we obtain $F(x) = cx$, with $c = f(1) \in Q$. □

There is a reason to use the graph and the tournament here. In each, multiplication by $Q$ is transitive on the vertices, so all vertices have the same degree (outdegree in the tournament). An isomorphism between two copies with one vertex deleted extends on putting the two missing vertices in correspondence. Indeed, at each surviving vertex its degree in the smaller graph records whether it was joined to the deleted vertex. In the tournament its outdegree records the direction of that edge.

**Theorem 9.2.** *Let $H$ be a complex Hadamard matrix of odd prime order $p$, either regular or Butson. Put $m = (p-1)/2$, $S = \{0\} \cup Q$ and $w = e^{2\pi i/p}$. The dephased Fourier corner $(w^{ax})_{a,x \in S}$ determines $H$ up to equivalence: $H \sim F_p$. One may omit any one square-indexed row or any one square-indexed column of the corner. In particular, for $b \in Q$ it suffices to have, after dephasing and indexing,*

$$H_{ax} = w^{ax} \qquad (a \in S \setminus \{b\},\ x \in S).$$

*Proof.* At $p = 3$ every complex Hadamard matrix is Fourier up to equivalence, as in the proof of Theorem 3.1. For $p \geq 5$ the surviving rectangle has area $m(m+1) > p$, so Proposition 1.5 puts the dephased matrix in $B(p, p)$. We can now transpose to reduce a column deletion to a row deletion. At $p = 5$ uniqueness in $B(5, 5)$ [12] suffices.

Assume $p \geq 7$ and write $A = Q \setminus \{b\}$. Relabel the square indices by $(a, x) \mapsto (ta, t^{-1}x)$ with $t \in Q$ so that $1 \in A$. Write $H_{ax} = w^{L(a,x)}$. Every noninitial row and column of $L$ and every difference of distinct rows or columns is a permutation. Each row $a \in A$ already takes the values

$\{0\} \cup Q$ on $S$, so it takes the values $N$ on the remaining columns. Label those columns by $y \in N$ using row 1, so that $L(1, y) = y$.

For fixed $y \in N$, the values $L(a, y)$ on $A$ are distinct. For $a, a' \in A$ distinct, their row difference on $S$ exhausts $\{0\} \cup (a - a')Q$, whence

$$\chi(L(a, y) - L(a', y)) = -\chi(a - a').$$

Thus $a \mapsto L(a, y)/y$ preserves the character of differences. Its domain and image each omit one vertex of $Q$, and the map fixes 1. By the degree argument above it extends to an automorphism of the graph or tournament on $Q$ fixing 1.

For $p \equiv 3 \pmod 4$, Lemma 9.1 gives the identity. We now have the $m$ full Fourier rows with slopes $\{0\} \cup A$, enough for Theorem 3.1. For $p \equiv 1 \pmod 4$ we have $p \geq 13$. The graph theorem of [20] gives the two possibilities

$$L(a, y) = ya \quad (a \in A), \qquad \text{or} \qquad L(a, y) = y/a \quad (a \in A). \tag{9.1}$$

If columns $y, z$ used opposite choices, then $-z/y \in Q$. The involution $a \mapsto (-z/y)/a$ on $Q$ has at most two fixed points. Excluding these, $b$, and its partner leaves a pair of distinct $a, a' \in A$ with $aa' = -z/y$, since $m \geq 6$. Then

$$(ya - z/a) - (ya' - z/a') = (a - a')\left(y + \frac{z}{aa'}\right) = 0,$$

contrary to the column-difference permutation. Thus all columns have the same choice. Inversion would give exactly the $m$ rows excluded by Corollary 8.2. The ordinary choice supplies $m$ Fourier rows, and Theorem 3.1 finishes the proof. □

At $p = 19$ a $9 \times 10$ dephased corner suffices, and at $p = 23$ an $11 \times 12$ corner suffices. The remaining border entries are part of the dephasing. Finding a copy of the square block in an arbitrary representative, with its row and column phases free, is a different hypothesis.

**Corollary 9.3.** *Let $p$ be an odd prime and let $H \in B(p, p)$ have the form (5.1). If one of its 4 core blocks, with suitable cyclic indexing, has the form*

$$\left(w^{ca^{i-j}}\right)_{0 \leq i,j < m},$$

*where $c \in \mathbb{F}_p^\times$ and $a$ generates $Q$, then $H \sim F_p$.*

*Proof.* Move the chosen block to the upper left of the core. Apply the cyclotomic automorphism $w \mapsto w^{c^{-1}}$; it preserves the Hadamard equations. Index this block's rows by $a^i$ and columns by $a^{-j}$. Together with the dephasing border it is the corner of Theorem 9.2. The transformed matrix is Fourier up to permutations, and undoing the cyclotomic automorphism leaves the Fourier equivalence class unchanged. □

Thus a geometric ordering in a single core block suffices at every odd prime. At a prime outside the range of Theorem 7.4, this gives another route to the symmetry problem. It suffices to identify one ordering among the four.

There is a second way to obtain an $m \times m$ rectangle: delete a square-indexed row and a square-indexed column together, retaining the dephasing row and column. The missing column can sometimes be recovered from just two of its entries. The following test takes place entirely in $\mathbb{F}_p$.

**Proposition 9.4.** *Let $H$ be a dephased regular or Butson Hadamard matrix of odd prime order $p$. Suppose it agrees with $F_p$ on the corner of Theorem 9.2 after one square-indexed row and one square-indexed column have been deleted. Then $H \sim F_p$ for $p \leq 103$.*

*For any odd prime $p$, put $A = \{0\} \cup (Q \setminus \{1\})$ and $D = N \cup \{1\}$. The same conclusion holds if some $u \in A \setminus \{0\}$ makes the identity the only map $f : A \to \mathbb{F}_p$ satisfying*

$$f(0) = 0, \qquad f(u) = u, \qquad \frac{f(a) - f(b)}{a - b} \in D \quad (a, b \in A,\ a \neq b).$$

*Proof.* At orders 3 and 5 every complex Hadamard matrix is Fourier up to equivalence, by the elementary order-3 argument above and Haagerup's theorem [10], respectively. In particular its dephased entries are $p$th roots, since they are Fourier cross ratios. Now let $p \geq 7$. The surviving rectangle has area $m^2 > p$, so the dephased matrix belongs to $B(p, p)$. If the two omitted indices are $b, c \in Q$, relabel the rows and columns by $a/b, x/c$, respectively, and apply the cyclotomic automorphism $w \mapsto w^{(bc)^{-1}}$. Then both omitted indices are 1 and the prescribed exponent rectangle is $(ax)_{a,x \in A}$. These operations preserve the Fourier equivalence class in both directions.

On the known columns, row $u$ takes the exponents $uA$, which omit $u$. There is a unique other column in which it takes the value $u$. Let $f$ be that column on the known rows. For $a \neq b$ in $A$, the difference of those rows has already used all values $(a-b)A$ on the known columns. Thus the slope of $f$ lies in $D$. The hypothesis forces $f(a) = a$ on $A$, recovering the missing Fourier column. Theorem 9.2 now applies.

For $7 \leq p \leq 17$ the area test and [12] suffice. For $19 \leq p \leq 103$ take $u$ to be the least positive member of $A$. Here is the exact recursion for the assertion about $f$. Start with the assignment $P = \{(0,0), (u,u)\}$. At each step take the least unassigned $a \in A$ and branch over

$$v \in \bigcap_{(b,t) \in P} (t + (a-b)D), \qquad P \longmapsto P \cup \{(a,v)\}.$$

Count every visited assignment, including each initial and complete one. Summing over the primes in each interval gives

| Interval | Primes tested | Assignments | Complete |
|---|---|---|---|
| 19–31 | 4 | 737 | 4 |
| 37–59 | 6 | 9256 | 6 |
| 61–79 | 5 | 28336 | 5 |
| 83–103 | 5 | 125984 | 5 |

The identity occurs at every prime. The last column therefore accounts for all complete assignments. □

In the one-deletion proof inversion appeared as a possible symmetry of the squares. With two deletions we can say exactly when a quadratic or fractional linear map for the normalized column can differ from the identity on $A$.

**Proposition 9.5.** *Let $p$ be an odd prime other than 7, with $A, D$ as in Proposition 9.4. Fix $u \in A \setminus \{0\}$ and suppose $f$ satisfies the slope and normalization conditions there. If $f$ agrees on $A$ with a fractional linear map defined there, or with a polynomial of degree at most two, then $f(x) = x$ throughout $A$.*

*Proof.* At $p = 3$ there is no such $u$, and at $p = 5$ the normalization fixes both points of $A = \{0, u\}$. Hence assume $p \geq 11$. An affine function fixing $0, u$ is the identity. Any remaining fractional linear possibility has the form $f(x) = (1+cu)x/(1+cx)$ with $c \neq 0$. Its secant slope at $x, y$ is

$$(1+cu)/((1+cx)(1+cy)).$$

All denominators and the numerator are nonzero. Every square slope must be 1, and for each $x$ at most one $y \neq x$ gives that slope. Split $A$ by the sign of $\chi(1+cx)$. If $1+cu$ is a square, every two points in the same class give a square slope. Each class then has at most two points. If $1+cu$ is a nonsquare, the classes contain 0 and $u$ on opposite sides, and every cross pair gives a square slope. Each class then has at most one point. Both counts contradict $|A| = (p-1)/2 \geq 5$.

For a quadratic $f(x) = ax^2 + bx + c$ with $a \neq 0$, the slopes are $a(x+y) + b$ for distinct $x, y \in A$. The restricted sum theorem of Dias da Silva and Hamidoune [6] gives at least $2|A| - 3$ distinct sums here. This exceeds $|D| = |A| + 1$ for $|A| \geq 5$. □

At $p = 7$ take $A = \{0, 2, 4\}$ and $u = 2$. The map $f(x) = x^2 - x$ takes the values $0, 2, 5$ on $A$. Its three slopes are $1, 3, 5$, all in $D = \{1, 3, 5, 6\}$. On $A$ it also equals $2x/(1 + 4x)$. This gives the exception for both classes of functions. By Proposition 9.4, any square completion at order 7 is equivalent to $F_7$. In its dephased exponent matrix every column is a scalar multiple of a prescribed nonzero column, so this particular map cannot occur.

So far we have considered one candidate column at a time. The remaining columns of a square completion have to provide all the missing slopes together. Keep $A = \{0\} \cup (Q \setminus \{1\})$ and $D = N \cup \{1\}$. By the small-order argument or the area test in Proposition 9.4, we can work with exponents in $\mathbb{F}_p$. Write $f_c : A \to \mathbb{F}_p$ for the exponents of an unprescribed column $c$ on the known rows. There are $m + 1$ such columns and $f_c(0) = 0$. For any distinct $a, b \in A$ their slopes satisfy the multiset identity

$$\left\{ \frac{f_c(a) - f_c(b)}{a - b} : c \text{ unprescribed} \right\} = D.$$

Indeed the row difference has already used $(a - b)A$ in the prescribed columns.

**Proposition 9.6.** *Let $p$ be an odd prime and put $m = (p - 1)/2$. In the two-deletion problem of Proposition 9.4, for each $d \in D$ count the unprescribed columns in which at least one pair of distinct known rows has slope $d$. At $p = 3$ the count is zero. At every other odd prime it is either 1 or at least $1 + \sqrt{m}$. When the count is one, that column has $f_c(a) = da$ on $A$. For $d = 1$ this recovers the missing Fourier column. In any completion inequivalent to $F_p$, at least $\lceil (m + 3)/2 \rceil$ of the unprescribed columns are nonlinear on $A$, and at least as many distinct slopes occur in $1 + \sqrt{m}$ or more columns.*

*Proof.* At $p = 3$ there is only one known row, and all completions are equivalent to $F_3$. For $p \geq 5$, fix $d$. The slope multiset gives count one at $p = 5$, since $A$ then contains just one pair. In general, each column partitions $A$ into the fibers of $a \mapsto f_c(a) - da$. Every pair of points belongs to a common fiber in exactly one column. Let $r$ be the number of columns containing such a pair. If $r = 1$ its partition has a single fiber. The constant on it is zero at $a = 0$. For $d = 1$ we can restore the column and apply Theorem 9.2.

If $r > 1$, take any fiber of size $s \geq 2$ and a point outside it. This point must meet the $s$ members in $s$ different columns: two meetings in the same column would repeat the pair of members. Thus $s \leq r - 1$. Fixing a point of $A$ and counting its $m - 1$ partners over the $r$ columns gives $m - 1 \leq r(r - 2)$, as required. In case of equality, writing $q = r - 1$, all fibers in those columns have size $q$ and $m = q^2$. The $q + 1$ partitions then give the parallel classes of an affine plane of order $q$: two points determine one fiber, and a fiber meets each fiber of any other partition once.

Every linear column takes a different slope. If all are linear they exhaust $D$, including 1. Otherwise the graph of any nonlinear $f_c$ is a set of $m$ noncollinear points in $\mathbb{F}_p^2$. By Szőnyi's direction theorem [25, Theorem 5.2] it determines at least $(m + 3)/2$ slopes. None can occur in a linear column, by the multiset identity. There are equally many unprescribed columns and missing slopes, so at least this many columns are nonlinear. Each of the indicated slopes occurs in more than one column, by the first assertion. □

We can also ask how many entries of the deleted column we need to restore before its remaining entries are forced. The answer is logarithmic in $p$ if we choose the rows.

**Theorem 9.7.** *Let $p$ be any odd prime, $m = (p-1)/2$ and $R = Q \setminus \{1\}$. In the dephased two-deletion problem of Proposition 9.4, with the omitted indices normalized to 1, there is a set $B \subseteq R$, depending only on $p$, such that prescribing $H_{bc} = w^b$ for $b \in B$ in a single unprescribed column $c$ forces $H \sim F_p$. For $p \le 103$, Fourier equivalence already holds with $B = \varnothing$. For $p \ge 11$ there is a choice of $B$ which also identifies the specified column, forcing $H_{ac} = w^a$ for all $a \in A = \{0\} \cup R$, with*

$$|B| \le \min\left\{m-1,\ 1 + \left\lfloor \frac{\log(m(m-1))}{\log(1/\rho)} \right\rfloor \right\}, \qquad \rho = \frac{m-1+\sqrt{p}}{2(m-1)}.$$

*In particular $2\log_2 p + O(1)$ entries suffice. The same conclusion holds with rows and columns interchanged.*

*Proof.* Proposition 9.4 gives the assertion with $B = \varnothing$ through 103. To prove the bound and the assertion for all larger primes, take $p \ge 11$ and write $f = f_c$. For $x \in R$, the slope with 0 gives either $f(x) = x$ or $f(x) = y \in N$. If $f(b) = b$, a pair $(x, y) \in R \times N$ can survive only when $b \ne x$ and $\chi((x-b)(y-b)) = -1$: its slope with $b$ cannot be 1. We choose $B$ to rule out every such pair.

For fixed $x \in R$, $y \in N$, put $P(b) = (b-x)(b-y)$. The sum of $\chi(P(b))$ over the field is $-1$, by the substitution $(b-x)/(b-y)$ for $b \ne y$. As $\chi(P(0)) = \chi(xy) = -1$, summing over the nonzero squares gives

$$\sum_{b \in Q} \chi(P(b)) = \frac{1}{2} \sum_{b \in \mathbb{F}_p} \chi(b(b-x)(b-y)).$$

The cubic has three distinct roots, so the last sum has absolute value at most $2\sqrt{p}$ by the Weil bound [18, Theorem 5.41]. Equivalently it is the Frobenius trace up to sign of the elliptic curve $v^2 = b(b-x)(b-y)$. There is exactly one zero of $P$ in $Q$. Consequently at most $(m-1+\sqrt{p})/2$ of the $m-1$ available rows in $R$ can leave this pair alive.

Initially there are $m(m-1)$ pairs. Averaging over $b \in R$ gives a row leaving at most a fraction $\rho$ of the current pairs. Repeat until none remain. Here $\rho = 1/2 + \sqrt{p}/(p-3)$ is less than one exactly when $p > 9$ in the range $p > 3$. Thus the asserted bound follows, with the option of taking all of $R$. We now have $f(x) = x$ on $A$, so Theorem 9.2 applies. Transposition is available after the area test gives level $p$. □

For a nonempty set $B$ chosen by the construction, the pair $0, b$ takes slope 1 in a unique column for each $b \in B$. If these columns coincide, that column supplies the entries in the theorem. Conversely, in a dephased Fourier matrix up to equivalence, the exponents have the form $(r_i - r_0)(s_j - s_0)$. Any nonzero prescribed column makes the first factor proportional to $a$ on $A$, so all the pairs select the same column. Thus it suffices to check concurrence on the chosen rows.

For example at $p = 503$, there are 250 surviving nonzero rows. Choosing at each step a row that leaves the fewest pairs, and breaking ties by the least positive representative, gives

$$B = \{2, 16, 231, 104, 286, 392, 144, 66, 197, 134, 376, 4\}.$$

These twelve entries suffice. This construction is related to the separating sets of Fijavž and Mohar for Paley graphs [8]. Here the rows must lie in $R$ and the pairs to be excluded have opposite character signs at every chosen row.

The logarithmic scale has a precise limitation. Fix $B$ of size $k$ and $x \in R \setminus B$. To survive the comparisons with $B$ and 0, a value $y$ needs the $k+1$ signs $\chi(y) = -1$ and $\chi(y-b) = -\chi(x-b)$ for $b \in B$. For $t$ distinct shifts $b_i$ and prescribed signs $e_i$, expand $2^{-t}\prod_i(1 + e_i\chi(y-b_i))$ and sum over $y$. The constant contributes $p/2^t$, and each nonempty product is bounded in absolute value by $(t-1)\sqrt{p}$ after summation, by the same Weil bound. Removing the $t$ shifts costs at most $t$. Thus at least $p/2^t - (t-1)\sqrt{p} - t$ values have the prescribed signs. For fixed $\epsilon > 0$, if $k \le (1/2 - \epsilon)\log_2 p$ and $p$ is sufficiently large, this number is positive with $t = k+1$. Even a false value at an individual row can then pass every comparison with $B$. Extending those values to a whole column, and making the columns satisfy the joint slope identity, impose further conditions.

We return to the corner with no extra entries prescribed. If several columns take slope 1 on different pairs, how many independent functions of the known row index do they require? Here rank means rank over $\mathbb{F}_p$ of the dephased exponent matrix $L$, where $H_{ax} = w^{L(a,x)}$. A dephased matrix equivalent to $F_p$ has exponent rank one, since its exponents are $(r_a - r_0)(s_x - s_0)$.

**Theorem 9.8.** *For every odd prime $p$, a regular or Butson completion $H$ of the doubly deleted Fourier corner has exponent rank one or at least five. Normalize both omitted indices to 1 as in Proposition 9.4, let $L$ be the resulting dephased exponent matrix over $\mathbb{F}_p$, and put $A = \{0\} \cup (Q \setminus \{1\})$. If $L_{A,\mathbb{F}_p}$ or $L_{\mathbb{F}_p,A}$ has rank at most two, then $H \sim F_p$.*

*Proof.* Proposition 9.4 settles $p \le 17$ and gives level $p$ for larger primes. Assume $p \ge 19$ and $H \not\sim F_p$. Write $i(a) = a$ on $A$. By the joint slope identity every pair of known rows takes slope 1 in a unique unprescribed column. Any linear column supplying this slope would be $i$ on $A$ and would restore the Fourier corner by Theorem 9.2. Thus all columns supplying slope 1 are nonlinear.

Suppose these columns, together with $i$, lie in a common space of dimension two. Choose one of them, $g$, as the second basis vector. Its graph is noncollinear since $g(0) = 0$ and $g$ is nonlinear. Its set $T$ of secant slopes has size $k \ge (m+3)/2 = (p+5)/4$ by Szőnyi's direction theorem [25, Theorem 5.2]. For a column $\alpha i + \beta g$ the slope on a pair where $g$ has slope $t$ is $\alpha + \beta t$. In particular, for each $t \in T$ the column supplying slope 1 on such a pair supplies it on every pair of that slope. It has $\beta \neq 0$ and gives an affine function $l_t$ satisfying

$$l_t(t) = 1, \qquad l_t(v) \in N \quad (v \in T \setminus \{t\}),$$

since 1 is the only square in $D$. Write $l_t(v) = \beta_t(v - h_t)$. The $h_t$ are distinct. Indeed, two affine functions with the same root are proportional. At a third point of $T$ both values are nonsquares, so their ratio is a square, whereas at the distinguished point of either function the ratio is a nonsquare.

Put $S(h) = \sum_{v \in T} \chi(v - h)$. Each of the $k$ distinct roots gives $|S(h_t)| = k - 2$. On the other hand,

$$\sum_{h \in \mathbb{F}_p} S(h)^2 = k(p-k).$$

The diagonal terms in the expansion sum to $p - 1$ each. For $u \neq v$, the sum of $\chi((u-h)(v-h))$ is $-1$, by the substitution $(u-h)/(v-h)$. It follows that $(k-2)^2 + k \le p$. But at $k = (p+5)/4$ the left side exceeds $p$ by $(p^2 - 18p + 29)/16 > 0$ for $p \ge 19$, and it increases with $k$. This excludes the common two-dimensional space.

Let $r$ be the rank of the strip consisting of all known rows of $L$, and $s$ the corresponding rank for the known columns. The first strip contains $i$ up to a nonzero multiple among its prescribed columns, so $r \ge 3$. Transposing gives $s \ge 3$. Now restrict the column space of $L$ to the coordinates in $A$. Its image has dimension $r$. The known columns span a space of dimension $s$ whose image has dimension one, since their restriction is the block $(ax)_{a,x \in A}$. The kernel therefore has dimension at least $s - 1$, giving $\operatorname{rank} L \ge r + s - 1 \ge 5$. □

In fact, in any completion inequivalent to $F_p$, no three columns supplying slope 1 belong to the same two-dimensional space with $i$. To see this, take three such columns, choose one as $g$, and use $T$ as above. Their affine functions have distinct distinguished points $t_j$ by the joint slope identity, and distinct roots $h_j$ by the same ratio argument. Outside those three points each $\chi(v - h_j)$ has a prescribed sign $e_j$ on $T$. Summing $\prod_{j=1}^{3}(1 + e_j\chi(v - h_j))/8$ over the field bounds the size of this common sign class from above. The three linear sums vanish, the three quadratic sums have absolute value one, and the cubic sum has absolute value at most $2\sqrt{p}$ by the Weil bound [18, Theorem 5.41]. Thus

$$\frac{p+5}{4} \le |T| \le 3 + \frac{p + 3 + 2\sqrt{p}}{8},$$

which is impossible for $p \ge 29$. Proposition 9.4 covers the smaller primes. Together with Proposition 9.6, this shows that the columns supplying slope 1 in a counterexample would occupy at least $\lceil (1 + \sqrt{m})/2 \rceil$ different planes of the form $\operatorname{span}\{i, f_c\}$. The same holds on the row side.

At rank five there is a further compatibility between the two strips. Pivot on a nonzero entry $L(u,v) = uv$ of the prescribed block and put $E_{ax} = L(a,x) - L(a,v)L(u,x)/(uv)$. Clearing the pivot gives $\operatorname{rank} E = 4$. With the known indices first on both sides, write

$$E = \begin{pmatrix} 0 & F \\ G & K \end{pmatrix}.$$

The two strip ranks of $L$ are both three, since $r + s - 1 \le 5$ and $r, s \ge 3$. Clearing the pivot on each strip gives $\operatorname{rank} F = \operatorname{rank} G = 2$. Projection of the column space of $E$ onto the known coordinates has image $\operatorname{im} F$, so its kernel is two-dimensional and equals $0 \oplus \operatorname{im} G$. Hence $K(\ker F) \subseteq \operatorname{im} G$. In particular the two side blocks prescribe the space in which $Kz$ must lie for every relation $Fz = 0$ among the columns of the first strip.

We can eliminate the opposite block from this test. Fix the full strips on the surviving rows and columns. The linear orthogonality equations then leave at most one complex parameter in the opposite block. At level $p$ the Galois action on the entries determines that parameter. The argument works for any Fourier minor of the following size.

**Theorem 9.9.** *Let $p$ be an odd prime. Prescribe $r$ full rows and $s$ full columns of a matrix of order $p$, where $r, s \ge 2$ and $r + s = p - 1$. Suppose their intersection is an $r \times s$ submatrix of $F_p$. There is at most one completion in $B(p,p)$, entry by entry. When it exists, linear equations over $\mathbb{Q}(e^{2\pi i/p})$ recover it from the two strips.*

*Proof.* Put $w = e^{2\pi i/p}$ and write the matrix in blocks as $\left(\begin{smallmatrix} P & B \\ C & X \end{smallmatrix}\right)$, with only $X$ unknown. Assume a completion exists. The prescribed rows give $BB^* = pI_r - PP^*$. In the Fourier matrix the same right side is the Gram matrix of the $r$ rows restricted to the $r + 1$ columns outside $P$. This restriction has rank $r$ by Chebotarëv's theorem on Fourier minors [27, Lemma 1.3]. Thus $B$ has rank $r$, and likewise $C$ has rank $s$. Orthogonality gives the linear equations

$$XB^* = -CP^*, \qquad C^*X = -P^*B.$$

Their homogeneous solutions form a line spanned by $uv^*$, with $u$ spanning $\ker C^*$ and $v$ spanning $\ker B$. Choose a position where $uv^*$ is nonzero and use its entry in $X$ as parameter $t$. Solving over $\mathbb{Q}(w)$ gives $X(t) = U + tV$ with $V$ of rank one.

Every $2 \times 2$ minor of a matrix in $B(p,p)$ is nonzero, since each quotient of two distinct rows is a rotated $p$-cycle. Its $3 \times 3$ minors are nonzero as well. Indeed, a dependence would express the third restricted row as $\alpha$ times the first plus $\beta$ times the second with $\alpha\beta \ne 0$. The three distinct quotients $z$ of the first row by the second would all satisfy $|z| = |\alpha z + \beta| = 1$. The second circle has center $-\beta/\alpha \ne 0$, so it meets the unit circle in at most two points. Also $u$ and $v$ each have at least three nonzero coordinates, since a dependence on one or two rows of $C$, or columns of $B$, contradicts flatness or a nonzero $2 \times 2$ minor. Thus the support of $V$ is a rectangle $I \times J$ containing a $3 \times 3$ submatrix.

Let $\sigma$ send $w$ to $w^2$. On $I \times J$ put

$$W_{ij} = \frac{\sigma(V_{ij})}{V_{ij}}, \qquad Z_{ij} = \frac{\sigma(U_{ij}) - U_{ij}^2}{V_{ij}}.$$

The matrix $W$ has rank one, by factoring $V$ into a column and a row over $\mathbb{Q}(w)$. In a completion, $\sigma(t) = t^2$ and $\sigma(X_{ij}) = X_{ij}^2$. Substituting $X = U + tV$ and dividing entrywise by $V$ gives

$$2tU - t^2(W - V) = Z \qquad \text{on } I \times J.$$

On this rectangle $U$ lies outside $\operatorname{span}\{V, W\}$. Otherwise $X = U + tV$ would be a sum of two rank-one matrices, contrary to its nonzero $3 \times 3$ minors. Thus the coefficient of $U$ in $Z$ along $W - V$ is uniquely determined and equals $2t$. If $W = V$ a single nonzero entry of $U$ gives it. Otherwise $U$ and $W - V$ are linearly independent as matrices, and two entries with independent coefficient pairs suffice. This determines $t$ and hence the entire block. □

The same Galois calculation explains the uniqueness geometrically. If $H, H'$ in $B(p,p)$ differ by a matrix $D$ of complex rank one, then on its support rectangle the entries of $H'+H$ are $\sigma(D_{ij})/D_{ij}$. Their matrix has rank one there, so $H$ has rank at most two on the rectangle. The nonzero $3\times 3$ minors force all changes into at most two rows or at most two columns. Two full fixed strips as in the proof exclude either possibility.

This gives a test for proposed strips. Check that the prescribed entries lie in $\mu_p$, and that the prescribed rows are mutually orthogonal, as are the prescribed columns. For a Fourier intersection these checks force the two required ranks. The test also works for any intersection with $\operatorname{rank} B = r$ and $\operatorname{rank} C = s$. Solve the block equations and reject inconsistent data. A support rectangle with fewer than three rows or columns also rules out a completion, by the minor argument above. On the rectangle solve $hU + k(W - V) = Z$ for $h$. If the system is inconsistent or $U \in \operatorname{span}\{V, W\}$, reject the strips. Otherwise put $X = U + (h/2)V$ and check that its entries are in $\mu_p$ and that $HH^* = pI$. These checks decide existence. For the doubly deleted corner we use $r = s = m$ at every prime $p \geq 5$. At $p = 3$ the surviving strips are just the dephasing row and column, shared by $F_3$ and $\bar{F}_3$.

For two strips of exponent rank three, the recovered block gives an exact rank-five test. With $E, F, G, K$ as above, let $\bar{K}$ be the map from $\ker F$ to $\mathbb{F}_p^{m+1}/\operatorname{im} G$ induced by $K$. Projection of $\operatorname{im} E$ onto the known coordinates has image $\operatorname{im} F$ and kernel $0 \oplus (\operatorname{im} G + K(\ker F))$. Restoring the pivot yields

$$\operatorname{rank}_{\mathbb{F}_p} L = 1 + \operatorname{rank} F + \operatorname{rank} G + \operatorname{rank} \bar{K} = 5 + \operatorname{rank} \bar{K}.$$

Thus a pair of strips of rank three gives a rank-five completion exactly when it passes the reconstruction test and $\bar{K} = 0$. The remaining choice is the pair of strips itself.

## 10 Recovering the border of a Fourier block

We now suppose that the only data given are the $Q \times Q$ block itself, up to row and column phases and permutations. The surrounding entries, including the position and phases of a possible dephasing border, are free. We will recover that border in two steps. Row differences locate a column which is constant along $Q$, and column differences locate a row of the same kind. Their intersection leaves a single phase to determine.

Consider the graph on $Q$ when $p \equiv 1 \pmod 4$ and the tournament on $Q$ when $p \equiv 3 \pmod 4$, as in Section 9. A set $M$ of vertices is called a module if every vertex outside $M$ has the same relation to each of its members. In the graph this means that the vertex is adjacent to all of $M$ or to none. In the tournament it means that all the edges between it and $M$ point the same way.

**Lemma 10.1.** *Let $p$ be an odd prime and let $g$ generate $Q$. Any module containing $1$ and $g$ is all of $Q$.*

*Proof.* At $p = 3$ the set $Q$ is a singleton, and at $p = 5$ it is $\{1, g\}$. Now assume $p \geq 7$. In the tournament the pairs $x, gx$, as $x$ runs over $Q$, form a directed cycle through all vertices, since multiplication by $Q$ preserves orientation. Thus the tournament is strongly connected.

In the graph case $p \geq 13$ and $m \geq 6$. Both the graph and its complement are connected. Indeed both have the same automorphisms, $x \mapsto cx$ and $x \mapsto c/x$ for $c \in Q$, by [20]. Each nonidentity automorphism fixes at most two vertices. If the graph under consideration were disconnected, multiplication by $Q$ would permute components transitively. If they were singletons a transposition would fix $m - 2 > 2$ vertices. Otherwise choose two distinct vertices in one component and multiply by their quotient, so that this component is preserved. Within that component perform this multiplication and outside it fix every vertex. This is a nonidentity automorphism fixing at least $m/2 > 2$ vertices.

Two intersecting modules have a union which is a module, since an outside vertex sees both sets uniformly and they share a vertex. If a proper module $M$ contained $1, g$, take the successive unions of $M, gM, g^2M, \ldots$. Consecutive translates intersect, and these unions eventually cover $Q$. At the

first such step two intersecting proper modules $U, V$ have union $Q$. Each of $U \setminus V$, $U \cap V$, $V \setminus U$ is nonempty. In the graph, adjacency between these three parts must be everywhere present or everywhere absent, contradicting connectedness of the complement or the graph. In the tournament, if an edge points from $U \setminus V$ to $V \setminus U$, then all edges point from the first part to the middle part and from the middle part to the last, as well as from the first to the last. Reversing the initial edge reverses this order. Both possibilities contradict strong connectivity. □

**Theorem 10.2.** *Let $H$ be a complex Hadamard matrix of odd prime order $p$, either regular or Butson, and put $w = e^{2\pi i/p}$. If $H$ contains a submatrix equivalent, by permutations and unit scalings of its rows and columns, to*

$$\left(w^{ax}\right)_{a,x\in Q},$$

*then $H \sim F_p$.*

*Proof.* At $p = 3$ a dephased row orthogonal to the first contains the three cube roots, which determine the last row up to a scalar. At $p = 5$ use Haagerup's order-5 classification [10]. Assume $p \geq 7$. The block has $p$th-root cross ratios and area $m^2 > p$. By Proposition 1.5, take a representative in $B(p, p)$. We may also arrange that its prescribed block is exactly $(w^{ax})$. Indeed, after the permutations the quotients between the desired and actual entries on this block form a rank-one matrix with entries in $\mu_p$. Factoring it using one row and one column gives row and column factors in $\mu_p$. Write $L$ for the exponent matrix in this representative. The difference of any two rows or two columns is a permutation of $\mathbb{F}_p$.

For a column outside the block put $f(a) = L(a, y)$ on $Q$. For $a \neq b$ the difference of rows $a, b$ already takes the values $(a - b)Q$ on the block. Thus whenever $f(a) \neq f(b)$,

$$\chi(f(a) - f(b)) = -\chi(a - b).$$

Every fiber of $f$ is a module. Indeed, for a vertex $b$ outside it the left side is the same for every $a$ in that fiber. Now take the pair of rows $1, g$, where $g$ generates $Q$. Their difference must take the value zero in some column, necessarily outside the block. For this column $1, g$ belong to one fiber. By Lemma 10.1, the column is constant on $Q$. Interchanging rows and columns gives a row outside the block which is constant on its $Q$ columns.

Dephase at the intersection of this row and column. On $Q \times Q$ the exponents now have the form $ax + t$ for one $t \in \mathbb{F}_p$. Put

$$s = \sum_{x\in Q} w^x, \qquad z = w^t s.$$

Let $v$ be the indicator of the $Q$ columns. The entry of $Hv$ on the dephasing row is $m$, and each of the $Q$ rows gives $z$. In every $Q$ column the known exponents are 0 on the dephasing row and $Q + t$ on the $Q$ rows. They are distinct, since the column is a permutation of exponents. Hence on the remaining rows the entries in those columns use the same set $C = \mathbb{F}_p \setminus (\{0\} \cup (Q + t))$. Each remaining row is itself a permutation of exponents and so uses every element of $C$ on those $m$ columns. There its sum is $-1 - z$.

The identity $\|Hv\|^2 = p\|v\|^2$ gives $m^2 + m|z|^2 + m|1 + z|^2 = pm$, or $|1 + 2z| = \sqrt{p}$. This is also a complementary-minor calculation. On the normalized indicators of the three column classes and the corresponding row classes, $H/\sqrt{p}$ acts by the unitary matrix

$$\frac{1}{\sqrt{p}} \begin{pmatrix} 1 & \sqrt{m} & \sqrt{m} \\ \sqrt{m} & z & -1 - z \\ \sqrt{m} & -1 - z & z \end{pmatrix}.$$

The upper left entry and the lower right $2 \times 2$ minor have equal absolute value, giving the same equation. For $F_p$ it holds with $s$ in place of $z$. Since $|z| = |s|$, we get $\operatorname{Re} z = \operatorname{Re} s$, whence $z = s$ or $z = \bar{s}$. Thus the sums of $w^x$ on $Q + t$ and on one of $Q, -Q$ coincide. Two equally large subsets of $\mathbb{F}_p$ with equal sums of these roots coincide: the difference of their indicator polynomials is divisible

by $1 + X + \cdots + X^{p-1}$ and vanishes at $X = 1$. Consequently $Q + t = Q$ or $Q + t = -Q$. Summing these elements in $\mathbb{F}_p$, and using $\sum_{x \in Q} x = 0$, gives $mt = 0$. We have recovered the full bordered corner with $t = 0$. Theorem 9.2 yields $H \sim F_p$. □

How much of the square block itself must be visible? Suppose that one entry has the wrong exponent. Whenever that change would make a $2 \times 2$ minor vanish, at least one of its three other entries must also have changed. We first count the rectangles to which this applies.

**Lemma 10.3.** *Let $Q$ be the nonzero squares in $\mathbb{F}_p$, for $p$ an odd prime. For every $k \neq 0$ the number $n(k)$ of ordered pairs $u, v \in Q$ with $(u-1)(v-1) = k$ satisfies*

$$n(k) \;\geq\; \frac{p - 7 - 2\sqrt{p}}{4}.$$

*Proof.* Write $z = u - 1$, so $v = 1 + k/z$. Omit $0, -1, -k$ from the sum over $z$. On the remaining set the indicator of the two square conditions is

$$(1 + \chi(1 + z))(1 + \chi(1 + k/z))/4.$$

For $k \neq 1$ the two single-character sums are both $-1 - \chi(1 - k)$, by $z \mapsto k/z$. The product of the characters is $\chi(z(z+1)(z+k))$, which vanishes at the omitted points. Hence

$$4n(k) = p - 5 - 2\chi(1 - k) + \sum_{z \in \mathbb{F}_p} \chi(z(z+1)(z+k)).$$

The cubic has three distinct roots, so the Weil bound [18, Theorem 5.41] bounds the last sum in absolute value by $2\sqrt{p}$. For $k = 1$ we omit just $0, -1$. Each single sum is $-1$ and the product is $\chi(z)$ on the remaining set, giving $4n(1) = p - 4 - \chi(-1)$. □

**Theorem 10.4.** *For every odd prime $p$, put $m = (p-1)/2$. Let $H$ be a regular or Butson Hadamard matrix of order $p$. Suppose that after row and column permutations and unit scalings, an $m \times m$ block agrees with $(w^{ax})_{a,x \in Q}$ except at unspecified positions. If each row and each column of the block has at most $\lfloor m/32 \rfloor$ unspecified entries, then all those entries are forced in the chosen coordinates and $H \sim F_p$.*

*Proof.* Let $t$ be the largest number of unspecified entries in a row or column. For $t = 0$ use Theorem 10.2. Otherwise $m \geq 32$, so $p \geq 67$. On the square block of $H^{\circ p}$ all specified entries are one. Testing this block against the normalized all-ones vectors on both sides gives real part at least $m - 2t > \sqrt{p}$. Theorem 1.3 gives rank one and puts $H$ in $B(p, p)$ up to equivalence. Any two block rows share a specified column since $2t < m$. Their rank-one row factors are therefore equal, and each column has a specified entry. The whole block of $H^{\circ p}$ is thus one, so we can write its original entries as $w^{L(a,x)}$. Every $2 \times 2$ minor of $H$ is nonzero by Corollary 1.4, since the quotient of two rows takes distinct values.

Let $E$ consist of the positions where $L(a, x) \neq ax$, and suppose $e = |E| > 0$. For $(b, c) \in E$ put $h = L(b, c) - bc$. Consider on $Q \times Q$ the curve

$$(a - b)(x - c) = -h.$$

If $(a, c), (b, x), (a, x)$ all retained their Fourier entries, the minor on rows $a, b$ and columns $x, c$ would vanish, since $(ax + bc + h) - (ac + bx) = 0$. The curve has at least $(p - 7 - 2\sqrt{p})/4$ points by Lemma 10.3, on dividing $a, x$ by $b, c$. Its points have distinct first coordinates and distinct second coordinates. At most $2(t-1)$ can therefore have $(a, c) \in E$ or $(b, x) \in E$. All the other points of the curve belong to $E$.

Put $d = \lceil (p - 7 - 2\sqrt{p})/4 \rceil - 2(t-1)$. Each of the $e$ curves thus contains at least $d$ points of $E$. Two distinct curves meet in at most two points: their graphs are the fractional linear functions

$x = c - h/(a-b)$, with different poles $b$ or different values $c$ at infinity. For each $P \in E$ let $j_P$ count the curves through $P$. Counting pairs of curves through each point gives

$$\sum_{P \in E} j_P(j_P - 1) \le 2e(e-1).$$

Since the average of $j_P$ is at least $d$, convexity gives $d(d-1) \le 2(e-1) \le 2(mt-1)$ whenever $d \ge 1$.

But $\sqrt{p} \le p/8$ for $p \ge 67$, and $t \le m/32 < p/64$. Hence $d > 5p/32 + 1/4 > 1 + p/8$, whereas $\sqrt{2mt} \le m/4 < p/8$. This contradiction gives $E = \varnothing$. The full square block is recovered, and Theorem 10.2 applies. □

The proof gives a sharper test at an individual prime. It suffices that $m - 2t > \sqrt{p}$, $d \ge 1$ and $d(d-1) > 2(mt-1)$. For instance, at $p = 113$ one may leave two entries unspecified in every row and every column of the $56 \times 56$ block: $d = 20$ and $380 > 222$. More generally, for $t = \lfloor \delta m \rfloor$ with $0 < \delta < (2 - \sqrt{3})/4$, these inequalities hold for all sufficiently large primes. Indeed $d/p$ tends to $1/4 - \delta$, and $(1/4 - \delta)^2 > \delta/2$.

We return to the dephased corner with one square row and one square column deleted. Proposition 9.4 recovers the matrix through 103. For arbitrary $p$, Theorem 9.7 prescribes $O(\log p)$ entries in one column, at rows chosen in advance from the arithmetic of $p$. How many entries suffice if their positions are arbitrary?

**Proposition 10.5.** *For every odd prime $p$, normalize the omitted indices to 1 and put $A = \{0\} \cup (Q \setminus \{1\})$. In a regular or Butson completion, let $f(a)$ be the exponent of an unprescribed column on $A$. If $f(a) = a$ at more than $2\sqrt{p} + 6$ rows of $A$, then $H \sim F_p$. More generally, in a completion inequivalent to $F_p$, every fiber of $a \mapsto f(a) - a$ has size at most $2\sqrt{p} + 12$.*

*Proof.* By Proposition 9.4 we may assume $p \ge 107$ and work in $\mathbb{F}_p$. Write $S = \{a \in A : f(a) = a + h\}$, $s = |S|$, $B = A \setminus S$ and $k = |B|$. If $B$ is empty then $f(0) = 0$ gives $h = 0$ and Theorem 9.2 applies. Suppose $k > 0$. For $b \in B$ put $y_b = f(b) - h$. We have $b \ne y_b$, and the $y_b$ are distinct since every secant slope of $f$ belongs to $N \cup \{1\}$. For $a \in S$ the slope from $b$ to $a$ is $(a - y_b)/(a - b)$ and differs from 1. Consequently

$$\chi((a-b)(a-y_b)) = -1 \qquad (a \in S,\ b \in B).$$

First fix one $b \in B$. Since $S \subseteq Q \cup \{0\}$, we have

$$4s \le 4 + \sum_{z \in \mathbb{F}_p} (1 + \chi(z))(1 - \chi((z-b)(z-y_b))) \le p + 5 + 2\sqrt{p}.$$

Indeed the quadratic character sum is $-1$ and the cubic sum is bounded by $2\sqrt{p}$ as in Lemma 10.3; if either root is zero, cancelling a square factor bounds the cubic sum by 1 in absolute value. Thus $k = m - s \ge (p - 7 - 2\sqrt{p})/4 \ge p/6$.

Now put $T(z) = \sum_{b \in B} \chi((z-b)(z-y_b))$. We have $T(a) = -k$ on $S$. In the expansion of $\sum_z T(z)^2$, identical unordered pairs $\{b, y_b\}$ contribute at most $p$ each. There are at most $2k$ such ordered terms, since an unordered pair has at most two orientations. Every other term is at most $2\sqrt{p}$. With one common root, cancelling its square gives a quadratic sum with one point omitted. With four distinct roots, choose one root $r$ and substitute $t = 1/(z - r)$. The sum becomes the character sum of a squarefree cubic with constant term 1, minus its term at $t = 0$. The cubic bound gives the stated upper bound. Hence

$$sk^2 \le \sum_z T(z)^2 \le 2kp + 2\sqrt{p}\,k^2, \qquad s \le 2\sqrt{p} + 12.$$

For $h = 0$ each $b \in B$ is a square, and $y_b = f(b)$ is a nonsquare by the slope condition with 0. The unordered pairs now occur just once, so $2kp$ improves to $kp$ and $s \le 2\sqrt{p} + 6$. □

At exponent rank five the known row vectors span a three-dimensional space, as do the known column vectors. We can now bound how many of them lie in one affine plane. We can also exclude equality in the slope count of Proposition 9.6 at this rank.

**Theorem 10.6.** *For every odd prime $p$, consider a completion of the doubly deleted corner as above, inequivalent to $F_p$. Every affine plane over $\mathbb{F}_p$ contains at most $2\sqrt{p}+12$ of the known full exponent rows. The same holds for the known full exponent columns. If $m = q^2$ and just $q+1$ columns supply slope 1 on pairs of known rows, then the full exponent rank is at least $q+3$. In particular, at rank five at least $q+2$ columns supply this slope, and likewise for rows.*

*Proof.* Write $R_a$ for the full exponent row indexed by $a \in A$. Projection onto any fixed nonzero prescribed column $x$, followed by division by $x$, is a linear functional $\pi$ with $\pi(R_a) = a$. Suppose an affine plane contains the rows indexed by $I \subseteq A$, with $|I| \geq 3$. The normalized differences $(R_a - R_b)/(a-b)$ for distinct $a, b \in I$ lie on the line $\pi = 1$ in the direction space of that plane. Every such vector has a unique unprescribed coordinate equal to 1, and all its other unprescribed coordinates are nonsquares. If the same coordinate supplies 1 for every pair, then $f(a) - a$ is constant on $I$ for that column, and Proposition 10.5 applies. This includes the case of collinear rows.

Otherwise choose affine coordinates $(a, u_a)$ on the plane, using $\pi$ as first coordinate. The normalized differences are parametrized by the distinct secant slopes $t = (u_a - u_b)/(a-b)$; denote their set by $T$ and its size by $k$. The points are noncollinear, so $k \geq (|I|+3)/2$ by Szőnyi's direction theorem [25, Theorem 5.2]. Each supplying coordinate on the line is an affine function of $t$, equal to 1 at its own point and a nonsquare elsewhere on $T$. The character calculation in the proof of Theorem 9.8 therefore gives $(k-2)^2 + k \leq p$. In fact the $k$ functions have distinct roots, and each root $z$ gives $|\sum_{t \in T} \chi(t-z)| = k-2$. It follows that $|I| \leq \sqrt{4p-7}$. Transposition proves the column assertion.

Finally assume $m = q^2$ and that $q+1$ columns supply slope 1. By the equality case of Proposition 9.6, the fibers of the functions $h_c(a) = f_c(a) - a$ form the parallel classes of an affine plane of order $q$ on $A$. These $q+1$ functions are linearly independent even modulo constants. Indeed, suppose $\sum_c \lambda_c h_c$ is constant. Sum this relation on two distinct fibers of one class $c$ and subtract. Each fiber meets every fiber of any other class once, so all the other terms cancel. If the two values in class $c$ are $u, v$, this gives $q\lambda_c(u-v) = 0$ in $\mathbb{F}_p$, whence $\lambda_c = 0$.

The known-row strip contains $a \mapsto a$ in its column space and hence also contains every $h_c$. Its rank is at least $q+1$. The opposite strip has rank at least three and the two ranks add to at most the full rank plus one, by Theorem 9.8. This gives the bound $q+3$. A counterexample would have $p > 103$, hence $q > 2$, so rank five excludes equality in the slope count on either side. □

Regarding the code, available at https://github.com/teobanica, the archive there contains the programs, inputs and certificates for the finite calculations in this paper. The folders follow the order in which the problems arise.

| Section | Folder | Calculation |
|---|---|---|
| 2 | w19/ | Completions of the displayed $T, D$ and their defects. |
| 4 | order11/a_branch/ | Three-row graphs, cycle colors and normalized labels. |
| 4 | order11/a_square/ | Compatible rows, cliques and extension sizes. |
| 6 | minors/ | Multiplicities of minor magnitudes in opposite blocks. |
| 7 | orbits/ | Cyclic orderings, polynomial tests and finite-field ranks. |
| 8–9 | corners/ | Column searches, selected rows and strip reconstruction. |

At order 11 the files retain each of the 3441 normalized candidate rows. For any nonlinear candidate of degree eight, the certificate gives two of its neighbors which cannot occur together. For $5 \leq p \leq 31$ in Section 7, two independent programs generate the same orderings, one using directed differences and the other unordered pair sums. At 109 a separate calculation checks the recurrence modulo 27 and the two squared-gap matrices modulo 3. For the doubly deleted corner, the recursion through 103 counts every visited assignment. At 103 it visits 38060 assignments with $u = 2$ and only the identity reaches the last row. The strip examples at $5, 7, 11$ recover the missing entries over the cyclotomic field.

After extracting the archive, install requirements.txt as described in README.md and run python3 run.py from the extracted code folder. To reproduce just the corner calculations, use python3 run.py corners. The programs use Python and C++17. The finite counts and certificates use exact arithmetic. A separate numerical check illustrates the polar decomposition in Section 6.

# References


[1] T. Banica, J. Bichon and J.-M. Schlenker, Representations of quantum permutation algebras, *J. Funct. Anal.* **257** (2009), 2864–2910.

[2] T. Banica, I. Nechita and J.-M. Schlenker, Submatrices of Hadamard matrices: complementation results, *Electron. J. Linear Algebra* **27** (2014), 197–212.

[3] B. C. Berndt and R. J. Evans, The determination of Gauss sums, *Bull. Amer. Math. Soc. (N.S.)* **5** (1981), 107–129.

[4] D. Christou, M. Mitrouli and J. Seberry, Embedding and extension properties of Hadamard matrices revisited, *Spec. Matrices* **6** (2018), 155–165.

[5] D. Czifra, M. Matolcsi and F. Szöllősi, A nonexistence criterion and new constructions for Butson Hadamard matrices, *J. Algebraic Combin.* **64** (2026), article 29.

[6] J. A. Dias da Silva and Y. O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.* **26** (1994), 140–146.

[7] R. Egan, D. Flannery and P. Ó Catháin, Classifying cocyclic Butson Hadamard matrices, in *Algebraic design theory and Hadamard matrices*, Springer Proc. Math. Stat. **133** (2015), 93–106.

[8] G. Fijavž and B. Mohar, Rigidity and separation indices of Paley graphs, *Discrete Math.* **289** (2004), 157–161.

[9] GPT and Teo, Regular complex Hadamard matrices of order 7,8, hexagon:2611.00079 (2026).

[10] U. Haagerup, Orthogonal maximal abelian $*$-subalgebras of the $n \times n$ matrices and cyclic $n$-roots, in *Operator algebras and quantum field theory*, International Press (1997), 296–323.

[11] G. Hiranandani and J.-M. Schlenker, Small circulant complex Hadamard matrices of Butson type, *European J. Combin.* **51** (2016), 306–314.

[12] M. Hirasaka, K.-T. Kim and Y. Mizoguchi, Uniqueness of Butson Hadamard matrices of small degrees, *J. Discrete Algorithms* **34** (2015), 70–77.

[13] C. Koukouvinos, M. Mitrouli and J. Seberry, An algorithm to find formulae and values of minors for Hadamard matrices, *Linear Algebra Appl.* **330** (2001), 129–147.

[14] C. Koukouvinos, E. Lappas, M. Mitrouli and J. Seberry, An algorithm to find formulae and values of minors for Hadamard matrices. II, *Linear Algebra Appl.* **371** (2003), 111–124.

[15] P. H. J. Lampio, P. R. J. Östergård and F. Szöllősi, Butson matrices up to monomial equivalence, electronic catalogue, Aalto University.

[16] P. H. J. Lampio, P. R. J. Östergård and F. Szöllősi, Orderly generation of Butson Hadamard matrices, *Math. Comp.* **89** (2020), 313–331.

[17] F. Lazebnik and A. Thomason, Orthomorphisms and the construction of projective planes, *Math. Comp.* **73** (2004), 1547–1557.

[18] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge University Press (1997).

[19] A. Muratović-Ribić, A. Pott, D. Thomson and Q. Wang, On the characterization of a semi-multiplicative analogue of planar functions over finite fields, *Contemp. Math.* **632** (2015), 317–325.

[20] M. Muzychuk and I. Kovács, A solution of a problem of A. E. Brouwer, *Des. Codes Cryptogr.* **34** (2005), 249–264.

[21] G. Somlai, A new proof of Rédei's theorem on the number of directions, *Arch. Math.* **122** (2024), 575–580.

[22] F. Szöllősi, *Construction, classification and parametrization of complex Hadamard matrices*, Ph.D. thesis, Central European University (2011).

[23] F. Szöllősi, A note on the existence of $BH(19, 6)$ matrices, *Australas. J. Combin.* **55** (2013), 31–34.

[24] F. Szöllősi, Exotic complex Hadamard matrices, and their equivalence, *Cryptogr. Commun.* **2** (2010), 187–198.

[25] T. Szőnyi, Around Rédei's theorem, *Discrete Math.* **208/209** (1999), 557–575.

[26] W. Tadej and K. Życzkowski, A concise guide to complex Hadamard matrices, *Open Syst. Inf. Dyn.* **13** (2006), 133–177.

[27] T. Tao, An uncertainty principle for cyclic groups of prime order, *Math. Res. Lett.* **12** (2005), 121–127.

[28] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics **83**, Springer (1997).