

The circulant Hadamard conjecture

OpenAI (with community contributions)

October 18, 2026

Abstract

We prove the circulant Hadamard conjecture: a real circulant Hadamard matrix has order 1 or 4. As a consequence, Barker sequences of length greater than one exist exactly at lengths 2, 3, 4, 5, 7, 11, 13, proving the Barker-sequence conjecture.

1 Introduction

A real Hadamard matrix of order n is a matrix H with entries in $\{-1, 1\}$ such that $HH^\top = nI_n$. It is *circulant* if there are signs $h_0, \dots, h_{n-1}$ for which

$$H_{ij} = h_{j-i \bmod n} \quad (0 \leq i, j < n).$$

Thus every row is a cyclic shift of the first. For such a sign matrix, define the periodic autocorrelations by

$$P_h(t) = \sum_{j=0}^{n-1} h_j h_{j+t \bmod n} \quad (0 \leq t < n).$$

Here $P_h(0) = n$, and the Hadamard condition is equivalent to $P_h(t) = 0$ for every $1 \leq t < n$. The circulant Hadamard conjecture, traditionally attributed to Ryser [15, 7], asserts that the only possible orders are 1 and 4. We prove this conjecture.

Theorem 1.1. *For a positive integer n , a real circulant Hadamard matrix of order n exists if and only if $n \in \{1, 4\}$.*

The theorem also completes the classification of Barker-sequence lengths. For an integer $n > 1$, a sign sequence $a = (a_0, \dots, a_{n-1}) \in \{-1, 1\}^n$ is a *Barker sequence* if its nontrivial aperiodic autocorrelations satisfy

$$|C_a(t)| \leq 1 \quad (1 \leq t < n), \quad C_a(t) = \sum_{j=0}^{n-t-1} a_j a_{j+t}.$$

The Barker-sequence conjecture asserts that no such sequence has length greater than 13. Turyn and Storer established the odd-length nonexistence theorem [19]; we use the later proof of Schmidt and Willms [17] for the exact list. For even length greater than two, the Barker inequalities imply that all nontrivial periodic autocorrelations vanish [19, 20]. Theorem 1.1 therefore settles the remaining even case.

Corollary 1.2 (Barker-sequence lengths). *For an integer $n > 1$, a Barker sequence of length n exists if and only if*

$$n \in \{2, 3, 4, 5, 7, 11, 13\}.$$

Section 5 gives the short periodic-autocorrelation argument and records examples at every listed length.

Context and prior work

The sign and cyclic conditions connect the problem to cyclic difference sets. Let $D = \{j : h_j = -1\} \subseteq \mathbb{Z}/n\mathbb{Z}$, and put $k = |D|$. If $N_D(t)$ counts ordered pairs $(a, b) \in D^2$ with $a - b = t$, then

$$P_h(t) = n - 4k + 4N_D(t).$$

A cyclic (v, k, λ) difference set is a k -element subset of a cyclic group of order v for which every nonzero difference occurs exactly λ times. For a circulant Hadamard row, the identity $(\sum_j h_j)^2 = \sum_{t=0}^{n-1} P_h(t) = n$ shows that the row sum is $\pm 2u$ when $n = 4u^2$. Complementing D when necessary makes that sum $2u$, and hence $k = 2u^2 - u$. The autocorrelation identity then says precisely that D is a cyclic difference set with parameters

$$(v, k, \lambda) = (4u^2, 2u^2 - u, u^2 - u).$$

Conversely, such a difference set supplies a circulant Hadamard row by assigning a negative sign to its elements. This equivalence holds for every positive u ; the restriction to odd u is an additional arithmetic conclusion.

Turyn studied these cyclic difference sets through the arithmetic of cyclotomic character sums and the Fourier relations imposed by their common coefficient array [20, pp. 319–323]. His nonexistence results show that an order greater than four must be $4u^2$, where u is odd and not a prime power [20, Corollary 2 to Theorem 6, p. 333, and Theorem 8 with its Corollary, pp. 335–336]. The proof in Section 2 gives a streamlined group-ring form of his descent for the 2-primary coefficients.

The symmetric case was settled early. In 1964, Johnsen proved -1 cannot be a multiplier of a nontrivial cyclic difference set [4], which implies there is no symmetric circulant Hadamard matrix of order greater than 4. Contemporaneously, Brualdi supplied an elementary matrix proof of the multiplier theorem [1] based on Newman’s techniques in [12] and credited Newman for observing the connection to Hadamard matrices.

Later work sharpened the arithmetic restrictions. For a positive integer M , let ζ_M be a primitive M -th root of unity. For $X \in \mathbb{Z}[\zeta_M]$ with $X\overline{X} = m \in \mathbb{Z}_{>0}$, Bernhard Schmidt’s field descent places a multiple of X by a root of unity in a cyclotomic subfield determined explicitly by the ambient conductor M and m [16]. Leung and Schmidt developed group-ring decompositions that refine these restrictions [6], followed by further exclusions in their 2012 work and their anti-field-descent method [7, 8]. Logan and Mossinghoff’s 2017 computation, using searches for double Wieferich prime pairs, excluded all but 4489 integers n with $4 < n \leq 4 \cdot 10^{30}$ as possible circulant Hadamard orders [9]. These 4489 integers remained as candidates under those tests.

Complementary work examines the coefficients more directly. Euler, Gallardo and Ravandrainy obtained combinatorial restrictions on the blocks of signs in the first row [2]. Approximate orthogonality has a different range of possibilities: Steinerberger used flat Littlewood polynomials, which have sign coefficients and uniformly controlled modulus on the unit circle, to show that in every order there is a real sign circulant whose singular values lie between two fixed positive multiples of $\sqrt{n}$ [18]. The conjecture requires exact equality of all singular values to $\sqrt{n}$. Complete proofs of the conjecture have also been claimed in [13, 14, 11, 3, 10].

The comparison of character values also has precedents in Turyn’s work. His preliminary fact (4) obtains a root-of-unity quotient from equality of principal ideals and absolute values. His Theorem 5 fixes a character and compares the values obtained by multiplying it by characters in a subgroup. It assumes equality of their principal ideals and that the subgroup order is coprime

to both the difference-set norm parameter $k - \lambda$ and the order of the fixed character [20, p. 321, item (4), and Theorem 5, pp. 328–329].

Group-ring notation

For a finite abelian group V and a subring $R \subseteq \mathbb{C}$, the group ring $R[V]$ consists of sums $f = \sum_{z \in V} f_z z$, with multiplication induced by the group law. Scalars denote multiples of the identity element. When R is stable under complex conjugation, put

$$f^* = \sum_{z \in V} \overline{f_z} z^{-1}.$$

We write C_N for the cyclic group of order N , and use $R[C_N] = R[X]/(X^N - 1)$ when a generator X is chosen. The *augmentation* $f(1)$ sends every group element to 1. A character evaluation sends group elements to roots of unity, and a quotient of groups induces a projection of group rings. Partial character evaluation commutes with the involution, which conjugates the evaluated coefficients on the remaining group ring.

All coefficient rings below are subrings of $\mathbb{C}$, hence domains. A localization $R_{\mathfrak{m}}$ at a maximal ideal allows denominators in $R \setminus \mathfrak{m}$, and its residue field is $R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}}$. The notation $\bar{z}$ always denotes complex conjugation; residues will be expressed by congruences modulo the indicated maximal ideal.

Proof strategy

Represent the first row by $h = \sum_j h_j X^j \in \mathbb{Z}[C_n]$. Orthogonality gives the scalar norm identity $hh^* = n$. Section 2 first proves the classical order restriction $n = 4u^2$ with u odd. Its cyclotomic basis turns divisibility of a primitive character value into divisibility of the coefficients of its remainder; at the prime two, repeated projection then rules out a larger power of two in the order.

Suppose $u > 1$, put $P = C_{u^2}$, and let I be the set of primes dividing u . For each $p \in I$, choose a generator of the p -primary component and a primitive p -th root ρ_p . Use the character sending that generator to ρ_p , and put $B = \mathbb{Z}[i, \{\rho_p : p \in I\}]$. For $S \subseteq I$, let x_S denote the value of $x \in \mathbb{Z}[i][P]$ at those characters for $p \in S$ and at the trivial character on the remaining components. The norm $xx^* = u^2$ gives $|x_S| = u$, so the alternating product

$$\Delta(x) = \prod_{S \subseteq I} x_S^{(-1)^{|S|}} \in \text{Frac}(B)$$

is defined.

Orthogonality of translates over any finite abelian group likewise gives a scalar group-ring norm. Here each $p \in I$ divides the scalar u^2 , and the p -component of P is cyclic of order p^e with $e = v_p(u^2)$. Lemma 3.1 uses this match. At each descent step, projection divides the group order by p ; division of one projected factor by p then lowers the scalar valuation by one. Both character ratios are preserved. It follows that $x_{S \cup \{p\}}/x_S$ is a local unit of residue one at every maximal ideal of B containing p . Pairing the factors of $\Delta(x)$ in each prime direction controls it at those ideals; the norm identity controls the remaining ideals. Thus $\Delta(x)$ is an algebraic integer. The alternating exponents sum to zero, so its images under every unital homomorphism $B \rightarrow \mathbb{C}$ have absolute value one. Kronecker's criterion makes it a root of unity,

and the local residues restrict its order to a power of every $p \in I$. In particular, that order is odd. Proposition 3.4 applies to every $x \in \mathbb{Z}[i][P]$ satisfying $xx^* = u^2$.

The cyclic factor C_4 supplies the remaining link with the signs. Write $C_{4u^2} = C_4 \times P$, with Z a generator of C_4 . Define the three normalized partial evaluations by

$$c = \frac{1}{2}h|_{Z=1}, \quad d = \frac{1}{2}h|_{Z=-1}, \quad g = \frac{1}{2}h|_{Z=i}.$$

The common sign coefficients make them integral in $\mathbb{Z}[i][P]$, and each has norm u^2 . Thus $\Delta(d)/\Delta(c)$ and $\Delta(g)/\Delta(c)$ have odd order.

Section 4 uses the same coefficients at a maximal ideal above two, where the odd norm makes every c_S a unit. The binary coefficients place the ratios d_S/c_S and g_S/c_S in the forms $1 + 2L_{r,S}$ and $1 + (1 + i)L_{w,S}$, with both L -terms integral in one local ring. Hence the two alternating ratio products have residue one; their odd order makes them exactly one. The first-order terms of exact products have alternating sum zero in the common residue field. But the coefficient identity gives

$$L_{r,S} + L_{w,S} \equiv J_S/c_S, \quad J = \sum_{z \in P} z.$$

Every nontrivial character annihilates J , while its trivial value is the odd unit u^2 . The resulting alternating sum therefore has one nonzero term, which is the contradiction.

2 The order restriction

We begin with the classical restriction that a circulant Hadamard order greater than one has the form $4u^2$ with u odd. The descent below is a group-ring version of Turyn's argument for the 2-primary coefficients [20, Lemma 6 through Theorem 8 and its Corollary, pp. 334–336]. We first isolate the cyclotomic divisibility fact that the descent uses.

Let H be a real circulant Hadamard matrix of order $n > 1$, and represent its first row by

$$h = \sum_{j=0}^{n-1} h_j X^j \in \mathbb{Z}[C_n].$$

The coefficient of X^a in hh^* is $\sum_j h_j h_{j-a}$, the inner product of row zero and row a . Consequently orthogonality is exactly

$$hh^* = n. \tag{2.1}$$

Augmentation gives $n = h(1)^2$, so n is a square. The inner product of two distinct rows is a sum of n signs and is zero, so n is even. We may therefore write

$$n = 2^{2s}u^2, \quad s \geq 1, \quad u > 0 \text{ odd}. \tag{2.2}$$

The remaining task is to prove $s = 1$. A primitive character value of a projection of h will force congruences between its coefficients. The following lemma makes that passage from a value to coefficients precise.

2.1 Cyclotomic divisibility

The coefficient rings in this lemma are localizations of cyclotomic integer rings. Its basis and ramification properties are classical; see, for example, [20, pp. 320–321]. We prove the local form, including the coefficient statement needed in both later uses.

Lemma 2.1. *Let p be a prime, let η be a primitive L -th root of unity with $p \nmid L$, and let A be the localization of $A_0 = \mathbb{Z}[\eta]$ at a maximal ideal containing p . The case $L = 1$ is allowed. Then A has maximal ideal pA , and every nonzero element of A is a unit times a nonnegative integral power of p .*

For $k \geq 1$, let ξ be a primitive p^k -th root, and put

$$\Phi_{p^k}(X) = \sum_{j=0}^{p-1} X^{jp^{k-1}}, \quad D = (p-1)p^{k-1}.$$

The ring $A[\xi]$ is free over A with basis $1, \xi, \dots, \xi^{D-1}$. It is local with maximal ideal $(\xi - 1)$, and p is a unit times $(\xi - 1)^D$. Every nonzero element is a unit times a power of $\xi - 1$. Consequently its fraction field has an additive valuation v , normalized by

$$v(p) = 1, \quad v(\xi - 1) = 1/D.$$

For every integer $\ell \geq 0$ and $z \in A[\xi]$,

$$v(z) \geq \ell \iff z \in p^\ell A[\xi], \quad (2.3)$$

where $v(0) = +\infty$. In particular, for $R(X) = \sum_{j=0}^{D-1} r_j X^j \in A[X]$, these conditions for $z = R(\xi)$ are equivalent to $r_j \in p^\ell A$ for every j .

Proof. A ring generated over $\mathbb{Z}$ by finitely many roots of unity is finitely generated as an abelian group: products of bounded powers of the roots span it. It is torsion-free because it is a subring of $\mathbb{C}$, and hence is free of finite rank. Every ideal, as a subgroup of this free abelian group, is finitely generated. Such a ring is therefore Noetherian, as are its localizations. This applies to A and to $A[\xi]$, which is a localization of $\mathbb{Z}[\eta, \xi]$.

We first determine the maximal ideal of A . Since $p \nmid L$, the polynomial $X^L - 1$ has no repeated factor over $\mathbb{F}_p$. Thus $\mathbb{F}_p[X]/(X^L - 1)$ is a product of fields. Its quotient A_0/pA_0 is also a product of fields. Localizing at the chosen maximal ideal selects one field factor, so A/pA is a field and the maximal ideal of A is pA .

In a Noetherian local domain whose nonzero maximal ideal is generated by t , a nonzero nonunit can be divided by t . This division cannot continue indefinitely: the successive quotients would generate a strictly increasing chain of principal ideals, since equality at one step would, by cancellation, make t a unit. Thus every nonzero element is a unit times a power of t . Applied to A , this gives its integral valuation, with value 1 at p .

We now adjoin ξ . The polynomial $\Phi_{p^k}(1 + Y)$ is monic of degree D , has constant term p , and reduces to Y^D modulo p . The last assertion follows by reducing

$$\Phi_{p^k}(X)(X^{p^{k-1}} - 1) = X^{p^k} - 1$$

in characteristic p . It is irreducible over $\text{Frac}(A)$ by Eisenstein's argument. Here is the needed form of that argument. For a nonzero polynomial over $\text{Frac}(A)$, the minimum valuation of its coefficients is additive under multiplication: after scaling both polynomials to minimum zero, their nonzero reductions have nonzero product over the field A/pA . If a monic integral polynomial factors into monic polynomials, the two minima are at most zero and sum to zero; hence both factors have coefficients in A . A nontrivial factorization of $\Phi_{p^k}(1 + Y)$ would therefore reduce to two monic positive-degree factors of Y^D . Both constant terms would be divisible by p , contradicting the constant term p of their product.

It follows that $A[\xi] \simeq A[X]/(\Phi_{p^k}(X))$, giving the asserted basis. Every maximal ideal of this finite A -algebra contracts to a maximal ideal of A . Indeed, the quotient by such a maximal ideal is a field finite as a module over the corresponding quotient domain of A . The adjugate-matrix argument for multiplication on a finite generating set makes every element of that field integral over the subdomain. Applying a monic relation to the inverse of a nonzero element of the subdomain puts that inverse in the subdomain. The subdomain is therefore a field.

Write $\pi = \xi - 1$ and $k_0 = A/pA$. The reduction

$$A[\xi]/pA[\xi] \simeq k_0[Y]/(Y^D)$$

has one maximal ideal. Thus $A[\xi]$ is local with maximal ideal (p, π) . The equation $\Phi_{p^k}(1 + \pi) = 0$ has the form

$$\pi^D = -p u_\pi, \quad u_\pi = 1 + \sum_{j=1}^{D-1} c_j \pi^j, \quad c_j \in A,$$

with the sum empty when $D = 1$. The element u_π has residue one and is a unit. Hence the maximal ideal is (π) , and p is a unit times π^D . The principal-ideal argument above now shows that every nonzero element of $A[\xi]$ is a unit times a power of π , giving the stated valuation. Since p^ℓ is a unit times $\pi^{\ell D}$, this description proves (2.3). The coefficient assertion follows from uniqueness in the free A -basis. $\square$

2.2 Descent at the prime two

We apply the coefficient statement in Lemma 2.1 to the 2-primary projection of the row. In the $A = \mathbb{Z}_{(2)}$ specialization used here, complex conjugation preserves the valuation on $A[\xi]$, so the norm determines the valuation of the character value itself.

Proposition 2.2. *If a real circulant Hadamard matrix has order $n > 1$, then $n = 4u^2$ for an odd positive integer u .*

Proof. For the matrix under consideration, the row norm (2.1) has already given $n = 2^{2s}u^2$ as in (2.2). It remains to show $s = 1$.

Project C_n onto $C_{2^{2s}}$. The image T of h has odd integer coefficients, each being a sum of u^2 signs, and

$$TT^* = 2^{2s}u^2.$$

Suppose $s \geq 2$. We describe an operation starting with

$$T \in \mathbb{Z}[C_{2^k}], \quad TT^* = 2^{2t}u^2, \quad k \geq 1, \quad t \geq 2, \quad (2.4)$$

where every coefficient of T is odd. Use Lemma 2.1 with $A = \mathbb{Z}_{(2)}$ and a primitive 2^k -th root ξ . Complex conjugation preserves $A[\xi]$ and sends $\xi - 1$ to the associate $-\xi^{-1}(\xi - 1)$. It therefore preserves the normalized valuation. Evaluating (2.4) gives

$$v(T(\xi)) = t, \quad T(\xi) \in 2^t A[\xi].$$

Write $T = \sum_{j=0}^{2^k-1} t_j X^j$. Its remainder modulo $\Phi_{2^k}(X) = 1 + X^{2^{k-1}}$ is

$$\sum_{j=0}^{2^{k-1}-1} (t_j - t_{j+2^{k-1}}) X^j.$$

The coefficient statement in Lemma 2.1, with $\ell = t$, shows that every displayed difference belongs to $2^t \mathbb{Z}_{(2)}$. Each difference is an integer, so it is divisible by 2^t in $\mathbb{Z}$.

Let $q : \mathbb{Z}[C_{2^k}] \rightarrow \mathbb{Z}[C_{2^{k-1}}]$ be the group projection. The coefficients of $q(T)/2$ are

$$\frac{t_j + t_{j+2^{k-1}}}{2}.$$

They are odd integers: the two odd summands are congruent modulo 4, since $t \geq 2$. Thus $T' = q(T)/2$ belongs to the smaller integer group ring. Projection commutes with the involution, and division of the projected norm by 4 gives

$$T' T'^* = 2^{2(t-1)} u^2.$$

Starting with $k = 2s$ and $t = s$, perform this operation $s - 1$ times. After j steps the indices are $k = 2s - j$ and $t = s - j$; every step starts with $t \geq 2$. The final element has 2^{s+1} odd integer coefficients and product with its star equal to $4u^2$. The identity coefficient of that product is the sum of the squares of those coefficients. Each odd square is 1 modulo 8, and 2^{s+1} is divisible by 8. The sum is therefore 0 modulo 8, whereas $4u^2$ is 4 modulo 8. This contradiction proves $s = 1$. $\square$

3 Alternating character products

For the rest of the argument, fix an odd integer $u > 1$, put $P = C_{u^2}$, and let I be the nonempty set of primes dividing u . Decompose P into its cyclic primary components. For each $p \in I$, choose a generator X_p of the p -component and a primitive p -th root ρ_p . These choices remain fixed. For $S \subseteq I$, let χ_S be the character determined by

$$\chi_S(X_p) = \begin{cases} \rho_p, & p \in S, \\ 1, & p \notin S, \end{cases} \quad x_S = \sum_{z \in P} x_z \chi_S(z) \quad \text{for } x = \sum_{z \in P} x_z z \in \mathbb{Z}[i][P].$$

All these values lie in the same ring

$$B = \mathbb{Z}[i, \{\rho_p : p \in I\}], \quad \varepsilon_S = (-1)^{|S|}. \quad (3.1)$$

If $x \in \mathbb{Z}[i][P]$ satisfies $xx^* = u^2$, character evaluation gives

$$x_S \overline{x_S} = u^2. \quad (3.2)$$

In particular every x_S is nonzero, so we may form

$$\Delta(x) = \prod_{S \subseteq I} x_S^{\varepsilon_S} \in \text{Frac}(B). \quad (3.3)$$

This product combines comparisons between pairs of characters. When $I = \{p, q\}$, for example,

$$\begin{aligned} \Delta(x) &= \frac{x_{\emptyset} x_{\{p, q\}}}{x_{\{p\}} x_{\{q\}}} \\ &= \frac{x_{\emptyset} / x_{\{p\}}}{x_{\{q\}} / x_{\{p, q\}}} = \frac{x_{\emptyset} / x_{\{q\}}}{x_{\{p\}} / x_{\{p, q\}}}. \end{aligned}$$

The two expressions on the second line pair the same four values in the p - and q -directions. A comparison in one direction controls primes above that prime; the same product admits a pairing in every direction. We will use these pairings to make $\Delta(x)$ integral. The norm identity and Kronecker's criterion will then give finite order, and the local residue-one conditions will force that order to be odd.

3.1 Comparison of two character values

For $p \in I$, write p^e for the order of the p -component of P . Then $e = v_p(u^2)$: the scalar norm has exactly the same p -valuation as the exponent in the component order. This is the case treated by the following local statement. It applies to two separate factors, and its proof uses only the sum of their valuations.

Lemma 3.1 (Character comparison). *Let A be as in Lemma 2.1. Suppose that $e \geq 1$ and*

$$F, K \in A[C_{p^e}], \quad FK = p^e b, \quad b \in A^\times.$$

For a primitive p -th root ρ , both ratios

$$\frac{F(\rho)}{F(1)}, \quad \frac{K(\rho)}{K(1)}$$

are units in $A[\rho]$ with residue 1 at its maximal ideal.

Proof. All the values in the denominators are nonzero, since the product of the two corresponding values is the nonzero scalar $p^e b$. The ratios therefore begin as elements of $\text{Frac}(A[\rho])$.

For $e = 1$, the nonnegative integral valuations of $F(1)$ and $K(1)$ sum to 1, so one is a unit of A . Evaluation at ρ is congruent to evaluation at 1 modulo $\rho - 1$. For that factor, the ratio is therefore a unit of residue 1. The two ratios multiply to 1, proving the same assertion for the other factor.

Suppose $e \geq 2$. Let $q : A[C_{p^e}] \rightarrow A[C_{p^{e-1}}]$ be the projection sending the chosen generator to the chosen generator. We will show that the projection of one factor is divisible by p in the smaller group ring. Evaluate at a primitive p^{e-1} -th root ξ , and put $D = (p - 1)p^{e-1}$ as in Lemma 2.1. The two nonnegative valuations sum to e , so at least one is at least 1. Interchange the factors if necessary so that $F(\xi) \in pA[\xi]$.

Choose a polynomial representative of F and divide by the monic cyclotomic polynomial:

$$F = Q\Phi_{p^e} + R, \quad Q, R \in A[X], \quad \deg R < D.$$

Since $R(\xi) = F(\xi)$, the coefficient statement in Lemma 2.1 makes every coefficient of R divisible by p . Moreover $q(\Phi_{p^e}) = p$. Thus $q(F) \in pA[C_{p^{e-1}}]$, as required. Define

$$F' = q(F)/p, \quad K' = q(K).$$

Then $F'K' = p^{e-1}b$. Cancellation of p is valid here because the target group ring is a free A -module. The evaluations at 1 and ρ factor through q , and scalar division cancels from their ratio. Thus both original comparison ratios are unchanged. Induction proves the assertion, whether the same factor or the other factor is divided at the next step. $\square$

Remark 3.2. The scalar valuation in Lemma 3.1 cannot uniformly be allowed to exceed the exponent in the cyclic group order. For an odd prime p and a primitive p -th root ρ , put $J = 1 + X + \cdots + X^{p-1}$ in $\mathbb{Z}[C_p]$ and $F = p - 2J$. Since $J^2 = pJ$ and $J^* = J$, one has $FF^* = p^2$, but $F(\rho)/F(1) = -1$, whose residue is not 1. Here the group has order p , while the scalar has p -valuation 2. In the case used above and below, both exponents start at e , and every projection is accompanied by division of one factor by p , reducing both exponents by one.

3.2 From local units to roots of unity

The comparison supplies control at the primes dividing u . The norm identity supplies both the remaining local control and the complex absolute values. We use two elementary facts to turn these properties into an order restriction. The first is Kronecker's criterion [5, Statement I].

Lemma 3.3.

- (i) *Let $B \subseteq \mathbb{C}$ be generated over $\mathbb{Z}$ by finitely many roots of unity. If $z \in B$ satisfies $|\sigma(z)| = 1$ for every unital ring homomorphism $\sigma : B \rightarrow \mathbb{C}$, then z is a root of unity.*
- (ii) *In a local domain with residue characteristic p , a root of unity with residue 1 has p -power order. In particular, if its order is coprime to p , it equals 1.*

Proof. For (i), let d be the finite rank of the free additive group of B , as in the proof of Lemma 2.1. Multiplication by an element of B is thus an integer matrix. On complexifying this representation, the matrices for the generating roots of unity commute and have finite order. Each is diagonalizable, since its minimal polynomial divides some $X^m - 1$, which has distinct complex roots. They are simultaneously diagonalizable: the eigenspaces of one are invariant under the others, and one repeats the argument on those eigenspaces.

On a common eigenvector, multiplication by any $b \in B$ acts as a scalar $\sigma(b)$. This is a well-defined unital ring homomorphism because it comes from the multiplication representation, so all relations between the root generators are respected. The multiplication matrix of z is diagonal in the same basis, with eigenvalues $\lambda_1, \dots, \lambda_d$ of modulus one. For each positive integer a , its a -th power has an integer characteristic polynomial. The coefficient of degree $d - j$ has absolute value at most $\binom{d}{j}$. Only finitely many such polynomials can occur, so the union of their sets of roots is finite. Each sequence λ_j^a therefore takes only finitely many values. Since $\lambda_j \neq 0$, two equal powers imply that λ_j has finite order. A common multiple of these orders makes the multiplication matrix the identity; applying it to $1 \in B$ proves that a positive power of z is 1.

For (ii), write the order as $p^a m$ with $p \nmid m$. If $m > 1$, raising the root to the p^a -th power gives an element ζ of order m and residue 1. In a domain, $(\zeta - 1)(1 + \zeta + \dots + \zeta^{m-1}) = 0$ then implies

$$1 + \zeta + \dots + \zeta^{m-1} = 0.$$

Its reduction says $m = 0$ in the residue field, a contradiction. Thus $m = 1$. □

Proposition 3.4. *Suppose $x \in \mathbb{Z}[i][P]$ satisfies $xx^* = u^2$. Then the alternating product $\Delta(x)$ defined in (3.3) belongs to B and is a root of unity. For each $p \in I$, its order is a power of p . In particular, its order is odd; if u has at least two distinct prime divisors, then $\Delta(x) = 1$.*

Proof. Fix $p \in I$ and a maximal ideal $\mathfrak{m}$ of B containing p . Let

$$A_0 = \mathbb{Z}[i, \{\rho_q : q \in I \setminus \{p\}\}], \quad \mathfrak{m}_0 = \mathfrak{m} \cap A_0, \quad A = (A_0)_{\mathfrak{m}_0}.$$

Put

$$\eta = i \prod_{q \in I \setminus \{p\}} \rho_q, \quad L = 4 \prod_{q \in I \setminus \{p\}} q,$$

with empty products equal to 1. The root orders 4 and $q \in I \setminus \{p\}$ are pairwise coprime, so η is a primitive L -th root, $p \nmid L$, and each original root is a power of η . Thus $A_0 = \mathbb{Z}[\eta]$ has the form required by Lemma 2.1. The ideal $\mathfrak{m}_0$ is maximal: it is prime and contains p , and A_0/pA_0 is a product of fields as in that lemma.

Let p^e be the order of the p -component, so $e = v_p(u^2)$. For $p \notin S$, evaluate every other component in $xx^* = u^2$ according to χ_S , leaving the p -generator as a variable. This ring homomorphism produces two factors $F, K \in A_0[C_{p^e}]$ with

$$FK = p^e b, \quad b = u^2/p^e \in A^\times.$$

Both factors already have coefficients in A_0 : in the image of x^* , Gaussian coefficients are conjugated and the evaluated roots are inverted, and these operations preserve A_0 . After localization, Lemma 3.1 therefore applies to these two factors. It gives

$$\frac{x_{S \cup \{p\}}}{x_S} \in A[\rho_p]^\times, \quad \frac{x_{S \cup \{p\}}}{x_S} \equiv 1 \pmod{\rho_p - 1}. \quad (3.4)$$

Every denominator inverted in A lies outside $\mathfrak{m}$, so the natural inclusion of $A[\rho_p]$ in $B_{\mathfrak{m}}$ is defined. In the residue field of $B_{\mathfrak{m}}$, characteristic p gives $(\rho_p - 1)^p = \rho_p^p - 1 = 0$. Hence $\rho_p - 1$ has residue zero, and the units in (3.4) retain residue 1 in $B_{\mathfrak{m}}$. Pairing S with $S \cup \{p\}$ yields the identity

$$\Delta(x) = \prod_{\substack{S \subseteq I \\ p \notin S}} \left(\frac{x_S}{x_{S \cup \{p\}}} \right)^{\varepsilon_S}. \quad (3.5)$$

Thus $\Delta(x)$ is a unit of residue 1 in $B_{\mathfrak{m}}$. The left side of (3.5) is the same element when the pairing direction changes. Applying the argument for every $p \mid u$ and every maximal ideal over p gives this local conclusion at all of those ideals.

At a maximal ideal containing none of the prime divisors of u , the scalar u^2 is a unit. Equation (3.2) then makes every x_S a unit there. Consequently $\Delta(x)$ belongs to $B_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ of B . The intersection of these localizations inside $\text{Frac}(B)$ is B . Indeed, if $z \notin B$, the ideal

$$D_z = \{b \in B : bz \in B\}$$

is proper. A maximal ideal $\mathfrak{m}$ containing it cannot have $z \in B_{\mathfrak{m}}$: such membership would give $z = a/s$ with $s \notin \mathfrak{m}$, whereas $sz = a \in B$ puts s in D_z . This proves $\Delta(x) \in B$.

Every unital homomorphism $\sigma : B \rightarrow \mathbb{C}$ sends the root generators to roots of unity and commutes with complex conjugation on their integer polynomials. Applying it to (3.2) gives $|\sigma(x_S)| = u$. In particular these images are nonzero. Let P_0 and Q_0 be the products of the x_S with $\varepsilon_S = 1$ and $\varepsilon_S = -1$, respectively. Then $\Delta(x) = P_0/Q_0$, and the preceding nonvanishing gives $\sigma(Q_0) \neq 0$. Applying σ to $Q_0\Delta(x) = P_0$ in B therefore evaluates the fraction in (3.3). Since $I \neq \emptyset$,

$$\sum_{S \subseteq I} \varepsilon_S = (1 - 1)^{|I|} = 0.$$

It follows that $|\sigma(\Delta(x))| = 1$. Lemma 3.3(i) makes $\Delta(x)$ a root of unity.

For each $p \in I$, there is a maximal ideal of B containing p : the additive group of B is free of positive finite rank, so $B/pB \neq 0$. At that ideal $\Delta(x)$ has residue 1, so Lemma 3.3(ii) makes its order a power of p . The assertions about odd order and two distinct prime divisors follow. $\square$

The single-prime conclusion can be nontrivial. If $u = p^a$, where p is an odd prime and $a \geq 1$, and X is the chosen generator of $C_{p^{2a}}$, then $x = p^a X$ satisfies $xx^* = u^2$, while $\Delta(x) = \rho_p^{-1}$ has order p . The final argument will therefore use odd torsion, without requiring each alternating product to equal 1.

4 The binary coefficient identity

Proposition 3.4 applies to every $x \in \mathbb{Z}[i][P]$ satisfying $xx^* = u^2$. We now use the common array of signs to relate three such elements. The following elementary map records the first-order term of a unit $1 + tL$ and turns products into sums in the residue field. Its common target will let us compare the two divisibilities supplied by the sign array.

Lemma 4.1. *Let O be a local domain with maximal ideal $\mathfrak{n}$, let $k = O/\mathfrak{n}$, and let $0 \neq t \in \mathfrak{n}$. Then $1 + tO$ is a subgroup of $O^\times$, and*

$$\lambda_t : 1 + tO \longrightarrow (k, +), \quad \lambda_t(1 + tL) = L \bmod \mathfrak{n}$$

is a group homomorphism.

Proof. The expression $1 + tL$ is a unit because it has residue 1, and L is unique because O is a domain and $t \neq 0$. The exact identities

$$\frac{(1 + tL)(1 + tM) - 1}{t} = L + M + tLM, \quad \frac{(1 + tL)^{-1} - 1}{t} = -\frac{L}{1 + tL}$$

prove closure under multiplication and inversion. Reducing modulo $\mathfrak{n}$ proves additivity and the inverse rule. $\square$

Proof of Theorem 1.1. The 1×1 matrix (1) is an example, as is the circulant matrix with first row $(1, 1, 1, -1)$ at order four; its three nontrivial autocorrelations vanish.

Suppose there were an example of another order. By Proposition 2.2, its order is $4u^2$ with $u > 1$ odd. Write $P = C_{u^2}$ and use the coprime decomposition $C_{4u^2} = C_4 \times P$. For a generator Z of C_4 , write the first-row element as

$$h = H_0 + ZH_1 + Z^2H_2 + Z^3H_3, \quad H_j \in \mathbb{Z}[P].$$

This decomposition reindexes the coefficients of the row, so every coefficient of every H_j is a sign. Turyn's Lemma 8 [20, p. 337] studies the four coset counts under an additional hypothesis on the ideals generated by the three nonprincipal character values; here each H_j records the signs at all elements of P . The normalized partial evaluations at $Z = 1, -1, i$ are

$$\begin{aligned} c &= \tfrac{1}{2}h|_{Z=1} = \frac{H_0 + H_1 + H_2 + H_3}{2}, \\ d &= \tfrac{1}{2}h|_{Z=-1} = \frac{H_0 - H_1 + H_2 - H_3}{2}, \\ g &= \tfrac{1}{2}h|_{Z=i} = \frac{H_0 - H_2}{2} + i\frac{H_1 - H_3}{2}. \end{aligned} \tag{4.1}$$

The fourth normalized evaluation, at $Z = -i$, is the coefficientwise conjugate of g . The coefficients of c and d are integers because their numerators are sums of four odd integers. The two half-differences in g are integral as well. Hence $c, d \in \mathbb{Z}[P]$ and $g \in \mathbb{Z}[i][P]$. Evaluation at $Z = 1, -1, i$ commutes with the involution, so $hh^* = 4u^2$ gives

$$xx^* = u^2 \quad (x = c, d, g). \tag{4.2}$$

Use the fixed notation $I, B, \chi_S, x_S, \varepsilon_S$ from Section 3, and set

$$R = \frac{\Delta(d)}{\Delta(c)}, \quad W = \frac{\Delta(g)}{\Delta(c)}.$$

Proposition 3.4 shows that R and W are roots of unity of odd order. Indeed, a quotient of roots whose orders divide odd integers m and n has order dividing mn . This applies even when an individual alternating product is nontrivial.

Choose a maximal ideal $\mathfrak{m}$ of B containing 2, which exists because $B/2B \neq 0$, and put

$$O = B_{\mathfrak{m}}, \quad \mathfrak{n} = \mathfrak{m}B_{\mathfrak{m}}, \quad k = O/\mathfrak{n}.$$

All residues in the rest of the proof lie in this one field k . Every c_S, d_S, g_S is a unit of O , since its product with its complex conjugate is the odd integer u^2 . The image of i in k is 1: in characteristic two, $(i-1)^2 = 0$, and k is a field. Thus $2, 1+i, 1-i$ belong to $\mathfrak{n}$, and 2 and $1+i$ are nonzero in the characteristic-zero domain O .

For every $S \subseteq I$, define the local units

$$r_S = \frac{d_S}{c_S}, \quad w_S = \frac{g_S}{c_S}. \quad (4.3)$$

Expanding the alternating products gives

$$R = \prod_{S \subseteq I} r_S^{\varepsilon_S}, \quad W = \prod_{S \subseteq I} w_S^{\varepsilon_S}. \quad (4.4)$$

We now compare how these two families differ from 1.

Put $b = (H_1 + H_3)/2 \in \mathbb{Z}[P]$. Direct subtraction in $\mathbb{Z}[i][P]$ gives the two exact differences

$$d - c = -2b, \quad g - c = (i-1)b - (H_2 + iH_3). \quad (4.5)$$

The common sign coefficients control the last bracket. Let $J = \sum_{z \in P} z$. Each coefficient of $H_2 + iH_3$ has the form $\alpha + i\beta$, with $\alpha, \beta \in \{-1, 1\}$, and differs from $1+i$ by an element of $2\mathbb{Z}[i]$. Hence

$$H_2 + iH_3 = (1+i)J + 2U, \quad U \in \mathbb{Z}[i][P]. \quad (4.6)$$

The first difference in (4.5) has a factor 2. After substituting (4.6), the second has a factor $1+i$, because $i-1 = i(1+i)$ and $2 = (1+i)(1-i)$. Evaluating and dividing by the unit c_S therefore gives the following integral first-order terms in O :

$$L_{r,S} := \frac{r_S - 1}{2} = -\frac{b_S}{c_S}, \quad (4.7)$$

$$L_{w,S} := \frac{w_S - 1}{1+i} = i\frac{b_S}{c_S} - \frac{J_S}{c_S} - (1-i)\frac{U_S}{c_S}. \quad (4.8)$$

The right sides establish the integrality of the two quotients. In particular

$$r_S \in 1 + 2O, \quad w_S \in 1 + (1+i)O.$$

Adding the exact formulas makes the contribution of b_S disappear after reduction:

$$L_{r,S} + L_{w,S} = -\frac{J_S}{c_S} - (1-i)\frac{b_S + U_S}{c_S} \equiv \frac{J_S}{c_S} \pmod{\mathfrak{n}}. \quad (4.9)$$

The displayed subgroup memberships give residue 1 for every r_S and w_S , and therefore for R and W . The orders of R and W are odd, so Lemma 3.3(ii) in residue characteristic two gives the exact equalities

$$R = W = 1. \quad (4.10)$$

A related character comparison of Leung and Schmidt also forces a root of unity of odd order to equal one by reducing modulo two [7, author manuscript, proof of Theorem 3.5, p. 10]. Lemma 4.1 applies with $t = 2$ and with $t = 1 + i$. For the two families it gives

$$\lambda_2(r_S) = L_{r,S} \bmod \mathfrak{n}, \quad \lambda_{1+i}(w_S) = L_{w,S} \bmod \mathfrak{n}.$$

Both maps take values in k , reducing their respective integral quotients modulo the same maximal ideal $\mathfrak{n}$. Apply them to the products in (4.4), using (4.10); the homomorphism and inverse rules give

$$\sum_{S \subseteq I} \varepsilon_S L_{r,S} \equiv 0 \pmod{\mathfrak{n}}, \quad \sum_{S \subseteq I} \varepsilon_S L_{w,S} \equiv 0 \pmod{\mathfrak{n}}.$$

Adding these identities in k and using (4.9) yields

$$\sum_{S \subseteq I} \varepsilon_S \frac{J_S}{c_S} \equiv 0 \pmod{\mathfrak{n}}. \quad (4.11)$$

For $S \neq \emptyset$, the character χ_S is nontrivial. Choose $z \in P$ with $\chi_S(z) \neq 1$. Since multiplication by z permutes the summands of J , evaluation gives $(\chi_S(z) - 1)J_S = 0$ in the domain B , and hence $J_S = 0$. For $S = \emptyset$, one has $J_\emptyset = |P| = u^2$ and $\varepsilon_\emptyset = 1$. The sum in (4.11) is therefore the unit $u^2/c_\emptyset$ of O . Its residue cannot be zero. This contradiction excludes every order greater than four. $\square$

Remark 4.2. The hypothesis $u > 1$ is used when the nonempty prime set I produces odd torsion in Proposition 3.4. At order four, I is empty and there is still one subset, $S = \emptyset$. For the example $(1, 1, 1, -1)$, one has $c = d = 1$ and $g = i$, giving $R = 1$ and $W = i$. Although i has residue 1 in characteristic two, its order is even, so the deduction (4.10) is unavailable.

5 Barker sequences

We finish by proving the length classification stated in Corollary 1.2. The new input is the circulant Hadamard theorem for even lengths; the odd-length classification is classical.

Proof of Corollary 1.2. Suppose first that a is a Barker sequence of even length $n > 2$. Its periodic autocorrelation at a nontrivial shift is

$$P_a(t) = \sum_{j=0}^{n-1} a_j a_{j+t \bmod n} = C_a(t) + C_a(n-t) \quad (1 \leq t < n).$$

The product of the n sign summands in $P_a(t)$ is $(\prod_j a_j)^2 = 1$, so an even number of those summands are negative. Consequently $P_a(t) \equiv n \pmod{4}$. Also $C_a(t) \equiv n - t \pmod{2}$. For $t = 2$, both $C_a(2)$ and $C_a(n-2)$ are even; the Barker bound makes them zero. Thus $P_a(2) = 0$, and $4 \mid n$. For every nontrivial shift, the Barker bounds give $|P_a(t)| \leq 2$, while the congruence

gives $P_a(t) \equiv 0 \pmod{4}$. Hence all these periodic autocorrelations vanish. The cyclic shifts of a form a real circulant Hadamard matrix. This classical implication appears in Turyn and Storer [19, p. 395, footnote 2]; see also [20, p. 330]. Theorem 1.1 now forces $n = 4$. The only possible even lengths are therefore 2 and 4.

For odd $n > 1$, Turyn and Storer proved nonexistence above length 13 [19]; the later proof of Schmidt and Willms [17, Theorem 1] gives the exact list $n \in \{3, 5, 7, 11, 13\}$. Examples exist at every listed length. The following table uses the examples recorded in [17, Section 1]. Here $+$ and $-$ denote 1 and -1 ; direct substitution in $C_a(t)$ verifies the Barker property in each row.

n	a	n	a
2	++	7	+++--+
3	+-	11	+++--+--+
4	+++	13	++++--+--+
5	++++		

□

If length one is admitted, it is also possible: there are no nontrivial shifts, so the Barker condition is vacuous.

References

- [1] R. A. Brualdi. A note on multipliers of difference sets. *Journal of Research of the National Bureau of Standards, Section B: Mathematics and Mathematical Physics*, 69B:87–89, 1965.
- [2] Reinhardt Euler, Luis H. Gallardo, and Olivier Rahavandrainy. Combinatorial properties of circulant Hadamard matrices. In Carlos M. da Fonseca, Dinh Van Huynh, Steve Kirkland, and Vu Kim Tuan, editors, *A Panorama of Mathematics: Pure and Applied*, volume 658 of *Contemporary Mathematics*, pages 9–19. American Mathematical Society, Providence, RI, 2016. Manuscript posted as arXiv:2406.10748 in 2024.
- [3] Luis H. Gallardo. Ryser’s conjecture and stochastic matrices, 2024. arXiv:2405.13033v1.
- [4] E. C. Johnsen. The inverse multiplier for abelian group difference sets. *Canadian Journal of Mathematics*, 16:787–796, 1964.
- [5] Leopold Kronecker. Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten. *Journal für die reine und angewandte Mathematik*, 53:173–175, 1857.
- [6] Ka Hin Leung and Bernhard Schmidt. The field descent method. *Designs, Codes and Cryptography*, 36(2):171–188, 2005.
- [7] Ka Hin Leung and Bernhard Schmidt. New restrictions on possible orders of circulant Hadamard matrices. *Designs, Codes and Cryptography*, 64(1–2):143–151, 2012. Author manuscript: <https://personal.ntu.edu.sg/bernhard/Publications/pub/chdm.pdf>.
- [8] Ka Hin Leung and Bernhard Schmidt. The anti-field-descent method. *Journal of Combinatorial Theory, Series A*, 139:87–131, 2016.

- [9] Brooke Logan and Michael J. Mossinghoff. Double Wieferich pairs and circulant Hadamard matrices. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 101:145–156, 2017.
- [10] Pankaj Kumar Manjhi and Jitendra Kumar. Construction of regular Hadamard matrices from circulant Hadamard matrices and Ryser’s conjecture. *Communications in Mathematics and Applications*, 16(3):923–927, 2025.
- [11] Joshua Morris. A proof of Ryser’s circulant Hadamard conjecture, 2023. arXiv:2302.08346v1.
- [12] Morris Newman. Multipliers of difference sets. *Canadian Journal of Mathematics*, 15:121–124, 1963.
- [13] Yoshimasa Oh-Hashi. A proof of Turyn’s conjecture: nonexistence of circulant Hadamard matrices for order greater than four. *IEICE Transactions on Communications*, E99-B(7):1395–1407, 2016.
- [14] Ronald Orozco López. Proof of the circulant Hadamard conjecture, 2019. arXiv:1907.12683v3.
- [15] Herbert John Ryser. *Combinatorial Mathematics*, volume 14 of *Carus Mathematical Monographs*. Mathematical Association of America, 1963.
- [16] Bernhard Schmidt. Cyclotomic integers and finite geometry. *Journal of the American Mathematical Society*, 12(4):929–952, 1999.
- [17] Kai-Uwe Schmidt and Jürgen Willms. Barker sequences of odd length. *Designs, Codes and Cryptography*, 80(2):409–414, 2016.
- [18] Stefan Steinerberger. A note on approximate Hadamard matrices. *Designs, Codes and Cryptography*, 92:3125–3131, 2024.
- [19] R. Turyn and J. Storer. On binary sequences. *Proceedings of the American Mathematical Society*, 12(3):394–399, 1961.
- [20] Richard J. Turyn. Character sums and difference sets. *Pacific Journal of Mathematics*, 15(1):319–346, 1965.