Journal of Algebraic Combinatorics (2022) 55:201–215
https://doi.org/10.1007/s10801-021-01033-x

Cocyclic two-circulant core Hadamard matrices

Santiago Barrera Acevedo[1] · **Padraig Ó Catháin**[2] · **Heiko Dietrich**[1]

Received: 17 February 2020 / Accepted: 8 March 2021 / Published online: 30 March 2021

Abstract
The two-circulant core (TCC) construction for Hadamard matrices uses two sequences with almost perfect autocorrelation to construct a Hadamard matrix. A research problem of K. Horadam asks whether such matrices are cocyclic. Using techniques from the theory of permutation groups, we prove that the order of a cocyclic TCC matrix coincides with the order of a Hadamard matrix of Paley type, of Sylvester type or certain multiples of these orders. We show that there exist cocyclic TCC Hadamard matrices at all allowable orders ≤ 1000 with at most one exception. Of the four families of TCC matrices known in the literature, we establish that two are cocyclic, prove that one is not cocyclic, and leave one undecided. The undecided family consists of matrices of 2-power order; we show that these are inequivalent to the Sylvester matrices. As a generalisation of the TCC construction, we introduce quadruple-circulant core (QCC) Hadamard matrices; our results give a complete description of the orders that admit cocyclic QCC Hadamard matrices.

Keywords Hadamard matrix · Twin circulant core · Cocyclic matrix · Legendre pair

Mathematics Subject Classification 05B10 · 05B20 · 20J06

1 Introduction

A Hadamard matrix (HM) of order n is an $n \times n$ matrix H over $\{-1, 1\}$ such that $HH^\intercal = nI_n$ where I_n is the $n \times n$ identity matrix. Two HMs are *(Hadamard) equiv-*

✉ Padraig Ó Catháin
pocathain@wpi.edu

Santiago Barrera Acevedo
Santiago.Barrera.Acevedo@monash.edu

Heiko Dietrich
heiko.dietrich@monash.edu

[1] School of Mathematics, Monash University, Clayton, VIC 3800, Australia

[2] Mathematical Sciences Department, Worcester Polytechnic Institute, Worcester, MA, USA

alent if one can be obtained from the other by swapping rows and columns and by multiplying rows and columns by -1. A square matrix $M = (m_{i,j})_{i,j}$ of order n is *circulant* if $m_{i,j} = m_{0,j-i}$ for all i and j, where arithmetic of the indices is modulo n. Recall that the $n \times n$ circulant matrices with complex entries form a commutative algebra that is closed under transposition and isomorphic to $\mathbb{C}C_n$, the complex group algebra of the cyclic group of order n.

Let J_m be the all 1's matrix of order m. We write $\mathbf{1}$ for the all 1's row vector (whose length will be determined by the context); similarly, $\mathbf{0}$ denotes the all 0's row vector. A *two-circulant core* (TCC) HM is a HM of order $n = 2m + 2$ that is equivalent to a matrix of the form

$$\begin{bmatrix} 1 & 1 & \mathbf{1} & \mathbf{1} \\ 1 & -1 & \mathbf{1} & -\mathbf{1} \\ \mathbf{1}^\mathsf{T} & \mathbf{1}^\mathsf{T} & A & B \\ \mathbf{1}^\mathsf{T} & -\mathbf{1}^\mathsf{T} & B^\mathsf{T} & -A^\mathsf{T} \end{bmatrix} \tag{1}$$

where A and B are circulant $\{\pm 1\}$-matrices of order m. Note that a matrix of this shape is a HM if and only if

$$AA^\mathsf{T} + BB^\mathsf{T} = (2m + 2)I_m - 2J_m \qquad \text{and} \qquad A\mathbf{1} = B\mathbf{1} = -\mathbf{1}.$$

Disregarding the trivial case $m = 0$, we note that m must be odd since otherwise 4 does not divide the order of H. Fletcher, Gysin, and Seberry [6] introduced TCC HMs and reported three infinite families, called (F1), (F2), and (F3) below. Kotsireas, Koukouvinos, and Seberry [10] performed an exhaustive search for TCC HMs (which they consider as a pair of sequences with autocorrelation -2, called *Legendre pairs*) with $3 \le m \le 45$, and partial searches for $47 \le m \le 75$. They found another family of TCC HMs, called (F4) below, and conjectured that TCC HMs exist for all m. The constructions leading to families (F1), (F3), and (F4) come from the Paley, Sylvester, and Stanton–Sprott cyclic difference sets, while (F2) comes from the so-called Szekeres difference families. The orders of the circulant cores in the families (F1)–(F4) are as follows:

(F1) all orders m where m is a prime;
(F2) all orders m where $q = 2m + 1$ is a prime power $q \equiv 3 \bmod 4$;
(F3) all orders m where $m = 2^k - 1$ with $k \ge 2$;
(F4) all orders m where $m = p(p + 2)$ where p and $p + 2$ are both primes.

To state the results of this paper, it is necessary to briefly introduce some terminology; the reader is referred to the monographs of Horadam [7] and Flannery and de Launey [3] for more background information.

1.1 Terminology

All groups are finite and written multiplicatively. A matrix M is *group-developed* over a group G if its rows and columns can be labelled by the elements of G, say $M = (m_{g,h})_{g,h\in G}$, such that there exists a function $\varphi\colon G \to \mathbb{C}$ with $m_{g,h} = \varphi(gh)$ for

all $g, h \in G$. The labelling of rows and columns may be distinct under our convention. Thus, back-circulant matrices and circulant matrices are group-developed over a cyclic group (taking row labels equal to column labels in the first case, and row labels the inverses of column labels in the second). The order of a group-developed HM is necessarily a perfect square, see [16], so not every HM is group-developed. Pioneered by de Launey and Horadam, *cocyclic development* is an algebraic approach to the study of HMs that relates regular subgroups of the automorphism group of a HM to functional identities on the matrix entries. Specifically, cocyclic HMs (CHMs) generalise group-developed HMs: the entries of a CHM M satisfy $m_{g,h} = \psi(g, h)\varphi(gh)$ where $\psi : G \times G \to \{\pm 1\}$ is a *2-cocycle* and $\varphi : G \to \{\pm 1\}$ a function.

1.2 Results

The *cocyclic Hadamard conjecture* [7, Research Problem 38] was proposed by de Launey and Horadam. It suggests that the Hadamard conjecture could be resolved through a study of CHMs. To date, there is some substantial evidence in favour of the conjecture: computational classifications have found CHMs at many small orders, and certain infinite families of matrices are known to be cocyclic; likewise certain families are proved not to be cocyclic; see [1] and the references therein. Horadam posed the problem of deciding when a TCC HM is cocyclic, see [7, Research problem 42]. We apply results from the theory of permutation groups to establish strong conditions on the order of a cocyclic TCC HM; our main result is the following.

Theorem 1.1 *If H is a cocyclic TCC HM of order $n = 2m + 2$ with m odd, then:*

(A) $n = q + 1$ where $q \equiv 3 \bmod 4$ is a prime power, or
(B) $n = 2p + 2$ where p is an odd prime, or
(C) $n = 2^t$ where $t \geq 2$ is an integer.

There exist cocyclic TCC HMs for all orders of type (A)*, for all orders as in* (B) *for which $p \equiv 1 \bmod 4$ or for which $p \leq 500$, and for all orders as in* (C) *with $t \leq 8$. In particular, the only order less than 1,000 for which the existence of a cocyclic TCC HM is open is 512.*

One novelty of our work is a precise description of the orders at which a cocyclic TCC matrix can exist. In contrast to previous work, this yields infinitely many orders at which cocyclic TCC matrices exist and infinitely many orders at which no TCC matrix is cocyclic. Seberry [6] conjectured that TCC matrices exist at every admissible order, so our result provides an interesting contrast to the cocyclic Hadamard conjecture.

In Sect. 2, we introduce some notation and discuss preliminary results. In Sect. 3, we present the classification of transitive permutation groups of degree $2m+2$ containing an element with cyclic structure $1+1+m+m$; this will be used in our classification of the admissible permutation representation groups for cocyclic TCC HMs. In Sect. 4, we show that Paley I and II HMs are TCC, we discuss equivalence of TCC matrices in family (F3) with Sylvester matrices, and we propose a new family of quadruple core circulant HMs. We conclude the paper with some directions for future work.

2 Preliminaries

We give an overview of some well-known group theoretic concepts that are required in Sects. 3 and 4 .

2.1 General groups

We denote by $\mathrm{Sym}(\Omega)$ and $\mathrm{Alt}(\Omega)$ the symmetric and alternative groups on a finite set Ω; when Ω has size n, we identify $\Omega = \{1, \ldots, n\}$ and write Sym_n and Alt_n. If T is a permutation group of degree k and H is some group, then $H \wr T$ denotes the wreath product $(H \times \cdots \times H) \rtimes T$ where T permutes the k-copies of H via its natural action. If q is a prime power, then $\mathrm{PGL}_n(q)$ and $\mathrm{PSL}_n(q)$ denote the projective linear and projective special linear groups of degree n over the field $\mathbb{F}_q$ with q elements. Analogously, $\mathrm{AGL}_n(q)$ and $\mathrm{A\Gamma L}_n(q)$ are the groups of n-dimensional affine (semi-linear) transformations over $\mathbb{F}_q$.

2.2 Permutation groups

A group G acts on the set Ω if there is a homomorphism $\alpha\colon G \to \mathrm{Sym}(\Omega)$; the image of $\omega \in \Omega$ under $\alpha(g)$ is usually denoted $\omega^g = \omega^{\alpha(g)}$. The action is *faithful* if $\ker\alpha$ is trivial. The G-action on Ω is *transitive* if for any $\alpha, \beta \in \Omega$ there exists $g \in G$ such that $\alpha^g = \beta$; it is n-transitive if the induced action on n-tuples over Ω with pairwise distinct entries is transitive. The stabiliser of $\omega \in \Omega$ is the subgroup $G_\omega = \{g \in G : \omega^g = \omega\}$; the action is *semi-regular* if $G_\omega = \{1\}$ for every $\omega \in \Omega$. The action is *regular* if it is semi-regular and transitive: for each pair $\alpha, \beta \in \Omega$, there is a unique $g \in G$ with $\alpha^g = \beta$.

The G-orbit of $\omega \in \Omega$ is $\omega^G = \{\omega^g : g \in G\}$. A *block* of G is a subset $B \subseteq \Omega$ such that for every $g \in G$ either $B = B^g$ or $B \cap B^g = \emptyset$. The *trivial blocks* are $B = \Omega$ and singletons $B = \{\omega\}$. A transitive action is *imprimitive* if there is a non-trivial block, and *primitive* otherwise. If B is a non-trivial block, then G acts transitively on $\{B^g : g \in G\}$ and the latter is a *system of imprimitivity* for G. Every such system partitions Ω into subsets of the same size; in particular, if Ω is finite, then $|B|$ divides $|\Omega|$. Every transitive permutation group is a subdirect product of primitive groups, and a taxonomy of primitive groups is given by the famous O'Nan–Scott theorem, see [4, Chapter 4]. A primitive group is of *affine type* if it contains a normal elementary abelian group acting regularly, and of *non-affine type* otherwise.

Now, let G be transitive. An *orbital* of G is a G-orbit in $\Omega \times \Omega$, and the number of *orbitals* is the rank of G. There is a bijection between the orbitals of G and the orbits of G_ω for every $\omega \in \Omega$. The G_ω-orbits on Ω are *suborbits*, and their cardinalities are the *subdegrees* of G; since G is assumed to be transitive, the latter are independent of ω. If Ω is finite, then a permutation $g \in \mathrm{Sym}(\Omega)$ has cycle type $c_1 + \cdots + c_k$ if the $\langle g\rangle$-orbits on Ω have size $c_1, \ldots, c_k$ with $c_1 + \cdots + c_k = |\Omega|$; equivalently, the disjoint cycle notation of g is a product of cycles of lengths $c_1, \ldots, c_k$.

2.3 A permutation representation of Aut(H)

A matrix M is a $\mathbb{Z}A$-matrix (A-matrix), with A being a group, if all entries lie in the group ring $\mathbb{Z}A$ (in the group A). It is monomial if every row and every column contains exactly one nonzero entry. The group $\mathrm{Mon}_n(A)$ of all A-monomial matrices under matrix multiplication. We abbreviate the direct product $\mathrm{Mon}_n(A) \times \mathrm{Mon}_n(A)$ as $\mathrm{Mon}_n^2(A)$; this group acts on the set of A-matrices of size n via $(P, Q) \cdot M = PMQ^\mathsf{T}$. Matrices in the same orbit are *A-equivalent*, written $M \equiv_A M'$. Let $\mathrm{Perm}(n) \leq \mathrm{Mon}_n(A)$ be the subgroup of permutation matrices isomorphic to Sym_n, and let $\mathrm{Diag}_n(A) \leq \mathrm{Mon}(A)$ be the subgroup of all diagonal matrices. The map that takes $M \in \mathrm{Mon}_n(A)$ and replaces every $a \in A$ by $1 \in \mathbb{Z}$ is a group homomorphism onto $\mathrm{Perm}(n)$ with kernel $\mathrm{Diag}_n(A)$; in particular, every $M \in \mathrm{Mon}_n(A)$ can be written uniquely as

$$M = P_M D_M \tag{2}$$

with $D_M \in \mathrm{Diag}_n(A)$ and $P_M \in \mathrm{Perm}(n)$.

We are interested in the case where A is the multiplicative group $\langle \pm \rangle = \{\pm 1\}$ and H is a HM of order n; in the following, we write $\equiv$ for $\equiv_{\langle \pm \rangle}$. The *automorphism group* of H is defined as the stabiliser

$$\mathrm{Aut}(H) = \{(R, S) \in \mathrm{Mon}_n^2(\langle \pm \rangle) \colon RHS^\mathsf{T} = H\}.$$

Note that if $(R, S) \in \mathrm{Aut}(H)$, then $S = H^{-1}RH$, hence S is determined by H and R, and the projection $\pi : (R, S) \to R$ is injective. In particular, $\mathrm{Aut}(H) \to \mathrm{Perm}(n)$, given by $(R, S) \mapsto P_R$, is a group homomorphism; we denote its image by

$$\mathcal{A}(H) = \{P_R \in \mathrm{Perm}(n) : (R, S) \in \mathrm{Aut}(H)\}.$$

We conclude this section with a result on $\mathcal{A}(H)$ where H is a cocyclic TCC matrix.

Proposition 2.1 *Let H be a HM of order $n = 2m + 2$. If H is cocyclic, then $\mathcal{A}(H)$ is transitive. If H is TCC, then $\mathcal{A}(H)$ contains an element of cycle type $1 + 1 + m + m$.*

Proof The first claim is [14, Lemma 6]. For the second claim, assume that H has shape (1), and let M be the $m \times m$ permutation matrix corresponding to the standard m-cycle (acting on row vectors). Note that $MXM^\mathsf{T} = X$ for each circulant $X \in \{A, B, A^\mathsf{T}, B^\mathsf{T}\}$. The block diagonal matrix $\sigma = \mathrm{diag}(I_2, M, M)$ yields an automorphism $(\sigma, \sigma) \in \mathrm{Aut}(H)$ whose image in $\mathcal{A}(H)$ has cycle type $1 + 1 + m + m$. □

3 Automorphisms of a cocyclic TCC HM

In this section, we study $\mathcal{A}(H)$ for cocyclic TCC HMs. Our main tool is a classification of transitive permutation groups of degree $n = 2m + 2$, with m odd, that contain an element of cycle type $1+1+m+m$; such a group is not regular and has rank at most 4.

3.1 Groups containing elements with cycle structure $1+1+m+m$

We first study the suborbit lengths of transitive and primitive permutation groups; this will be required in our proof of Theorem 3.4.

Lemma 3.1 *Let $G \leq \mathrm{Sym}(\Omega)$ be transitive, $|\Omega| \geq 3$, and $\alpha \in \Omega$. If G_α has exactly two fixed points in Ω, say $\alpha, \beta \in \Omega$, then G is imprimitive and $\{\alpha, \beta\}$ is a non-trivial block for G.*

Proof Since G is transitive, the Orbit–Stabiliser Theorem implies $|G_\alpha| = |G_\beta|$; since $G_\alpha \leq G_\beta$, we have $G_\alpha = G_\beta$. Let $h \in G$ such that $\{\alpha, \beta\}^h \cap \{\alpha, \beta\} \neq \emptyset$. If $\alpha^h = \alpha$, then $h \in G_\alpha = G_\beta$; hence, $\{\alpha, \beta\}^h = \{\alpha, \beta\}$. Now, suppose $\alpha^h = \beta$; we will show that $\beta^h = \alpha$, and then, it follows that $\{\alpha, \beta\}$ is a block of imprimitivity, as claimed. If $x \in G_\alpha = G_\beta$, then $\alpha^{hxh^{-1}} = \alpha$, so $hxh^{-1} \in G_\alpha = G_\beta$, which shows that $\beta^{hxh^{-1}} = \beta$. This implies that $\beta^{hx} = \beta^h$; that is, every $x \in G_\alpha$ stabilises β^h. By assumption, the only fixed points of $G_\alpha = G_\beta$ are $\{\alpha, \beta\}$, which forces $\beta^h \in \{\alpha, \beta\}$; hence, $\beta^h = \alpha$ and $\{\alpha, \beta\}^h = \{\alpha, \beta\}$. □

The next result from [4] collects some observations on the subdegrees of a primitive permutation group.

Lemma 3.2 *Let $G \leq \mathrm{Sym}(\Omega)$ be primitive with subdegrees $n_1 \leq \cdots \leq n_r$ and $r > 2$. If G is not regular, then $n_1 < n_2$ and $\gcd(n_r, n_i) \neq 1$ for all $i \geq 2$; moreover, $p \leq n_2$ for each prime p dividing $n_3, \ldots, n_r$.*

Proof This follows from [4, p. 72 and Exercise 1.6.5] and [4, Lemma 3.2B and Exercise 3.2.24]. □

The next theorem of Jones [9, Theorem 1.2, Remark 1.5] constitutes the main ingredient in our proof of Theorem 3.4. In the following, M_{11}, M_{12}, M_{24} are three of the five Mathieu groups, see [15, Section 7.4]; note that below M_{11} is considered in its 3-transitive permutation representation on 12 points.

Proposition 3.3 *Let T be a transitive permutation group of degree $k > 2$. If T contains a cycle fixing exactly one point, then T is 2-transitive (hence primitive) and isomorphic to one of the following:*

1. $\mathrm{AGL}_d(q) \leq T \leq \mathrm{A\Gamma L}_d(q)$ *with $k = q^d$ for some prime power q,*
2. $T = \mathrm{PSL}_2(p)$ *or* $T = \mathrm{PGL}_2(p)$ *with $k = p + 1$ for some prime $p > 3$,*
3. $T \in \{M_{11}, M_{12}, M_{24}\}$ *with $k = 12, 12, 24$, respectively,*
4. $\mathrm{Alt}_k \leq T$.

The main result of this section is:

Theorem 3.4 *Let $G \leq \mathrm{Sym}(\Omega)$ be transitive of degree $n = 2m + 2$ with odd m. If G has an element of cycle type $1 + 1 + m + m$, then there is T as in Proposition 3.3 with $k = m + 1$ such that*

i) G is 2-transitive, or

ii) G is imprimitive with blocks of size 2, and the induced action of G on blocks is T, that is, $G \leq C_2 \wr T$ with surjective projection $G \to T$, or
iii) $G = T \wr C_2$.

Proof Let $\sigma \in G$ be the element with cycle type $1+1+m+m$. Let $\alpha \in \Omega$ be a fixed point of σ and note that $\langle \sigma \rangle \leq G_\alpha$ has four orbits of size $1, 1, m, m$. This implies that G has rank $r \in \{2, 3, 4\}$, and we make a case distinction. If $r = 2$, then the subdegrees are $1, 2m+1$ and G_α acts transitively on the remaining points; this implies that G is 2-transitive.

If $r = 4$ with subdegrees $1, 1, m, m$, or $r = 3$ with subdegrees $1, 1, 2m$, then G_α has exactly two fixed points; hence, G admits a system of imprimitivity of size 2 by Lemma 3.1. Since σ has odd order m and blocks have size 2, the element σ cannot fix a block without fixing it element-wise. This implies that σ fixes precisely one block and so acts transitively on the remaining m blocks: this follows from the Orbit–Stabiliser Theorem and the fact that for each $i \in \{1, \ldots, m-1\}$, the permutation σ^i has odd order and the same fixed points as σ. A permutation of order m that acts transitively on m blocks must be an m-cycle on those blocks. In particular, the G-action on those $m+1$ blocks is 2-transitive; this implies that this G-action is one of the groups listed in Proposition 3.3 with $k = m+1$; these groups are listed under ii).

Lastly, let $r = 3$ with subdegrees $1, m, m+1$. Lemma 3.2 implies that G is imprimitive. Let B be a non-trivial block containing a fixed point x of σ, then G_x has orbits $\{x\}, U, V$ with $|U| = m$ and $|V| = m+1$. If $g \in G_x$, then $B^g = B$ since $x \in B$ is fixed by g. But this requires that U or V is contained in B; that is, B has size $m+1$ or $m+2$. Since $m+2$ does not divide $|\Omega| = 2m+2$, the only non-trivial block size is $m+1$. The cycle type of σ implies that the action of G_α on the suborbit of length $m+1$ has cycle type $1+m$; in particular, the induced action is 2-transitive and one of the groups in Proposition 3.3 with $k = m+1$. There are two blocks, so this yields the groups in case iii). □

3.2 The order of cocyclic TCC HMs

Now, we work towards applying Theorem 3.4 in the case that $G = \mathcal{A}(H)$. The fact that $\mathcal{A}(H)$ is a quotient of the automorphism group of a HM implies a bound on the number of fixed points of a non-identity element.

Lemma 3.5 *Let H be a HM of order n and write $\pi : \mathrm{Aut}(H) \to \mathcal{A}(H)$ for the projection of Sect. 2.3. If $\pi(P, Q)$ is non-trivial, then $\pi(P, Q)$ fixes at most $n/2$ points.*

Proof Since $(P, Q) \in \mathrm{Aut}(H)$, it follows that $PH = HQ$. The matrix HQ is a rearrangement of the columns of H up to signs. If c_i is a column of H, then Pc_i is a column of HQ; if c_j is another column of H, then the inner product of Pc_i and c_j is 0 by the orthogonality of columns in H. Suppose, for a contradiction, that P fixes more than $n/2$ rows and let c_i be a column of H with $Pc_i \neq \pm c_i$. Then, c_i and Pc_i have more than $n/2$ entries in common, so there are more than $n/2$ positive terms in the inner product, contradicting orthogonality of columns. □

Theorem 3.6 *Let H be a cocyclic TCC HM of order $n = 2m+2$ with m odd. Then, one of the following holds, where p denotes a prime and q denotes a prime power:*

A) $\mathcal{A}(H)$ *is non-affine 2-transitive and contains* M_{12} *or* $\mathrm{PSL}_2(q)$ *as a normal subgroup, or*
B) $\mathcal{A}(H)$ *is affine 2-transitive and contains* $\mathrm{AGL}_n(2)$ *as a normal subgroup, or*
C) $\mathcal{A}(H) \leq C_2 \wr T$ *with surjective projection* $\mathcal{A}(H) \to T$*, where* $T \in \{\mathrm{PSL}_2(p), \mathrm{PGL}_2(p)\}$ *with* $m = p$ *a prime, or* $T \in \{M_{11}, M_{12}, M_{24}\}$ *with* $m+1 = 12, 12, 24$*, respectively, or,*
D) $\mathcal{A}(H) \leq C_2 \wr T$ *with surjective projection* $\mathcal{A}(H) \to T$*, and* $\mathrm{AGL}_1(q) \leq T \leq \mathrm{A\Gamma L}_1(q)$.

Proof Parts A) and B) are primitive non-affine and primitive affine respectively. Parts C) and D) are imprimitive, but with induced primitive non-affine and affine actions on blocks. For $m \in \{1, 3\}$, there exists a unique equivalence class of HMs of order $n = 2m + 2$; these matrices are cocyclic and TCC. Each matrix is equivalent to a Sylvester matrix and so has $\mathcal{A}(H)$ 2-transitive of affine type, leading to a group of type B). Thus, in the following, let $m \geq 5$. Proposition 2.1 implies that $G = \mathcal{A}(H)$ satisfies the hypotheses of Theorem 3.4; we proceed through the three cases.

Case i): Here, G is 2-transitive. It follows from [8, Proposition 1] that if G is non-affine, then G is M_{12}, contains $\mathrm{PSL}_2(q)$ with $q \equiv 3 \bmod 4$ a prime power, or $n = 36$. We can exclude $n = 36$: there is a unique equivalence class of HMs of order 36 for which $\mathcal{A}(H)$ is doubly transitive, [13, Theorem 16]. For this matrix, $\mathcal{A}(H) \cong \mathrm{Sp}_6(2)$ has order not divisible by $m = 17$, violating Proposition 2.1. There exists (up to equivalence) a unique HM of order 12, and this matrix has $\mathcal{A}(H) \cong M_{12}$. For each prime power $q \equiv 3 \bmod 4$ with $q \geq 19$, there exists a unique HM of order $q + 1$ for which $\mathrm{PSL}_2(q) \leq \mathcal{A}(H)$. All such matrices are of Paley type I (see Sect. 4.1 for a further discussion); this gives the HMs under A).

In the case that G is 2-transitive of affine type, unpublished work of Moorhouse shows that the only real HMs which arise are equivalent to Sylvester matrices, [11, Theorem 1.2]; this is covered by B).

Case ii): Let $\mathcal{A}(H) \leq C_2 \wr T$ with surjective projection $\mathcal{A}(H) \to T$, where $\mathcal{A}(H)$ is a group of rank at least 3. First, suppose $\mathrm{AGL}_d(q) \leq T \leq \mathrm{A\Gamma L}_d(q)$ and $m+1 = k = q^d$ for some even prime power q; recall that m is odd. Let $a = \mathrm{diag}(\alpha, 1, \ldots, 1) \in \mathrm{GL}_d(q) \leq T$ where α is a non-trivial element of the finite field $\mathbb{F}_q$. Let $b \in G$ be any preimage of a under the projection $G \to T$. It follows that b^2 fixes at least $2q^d - 2q = 2(m+1) - 2\sqrt[d]{m+1}$ elements. If $d > 1$, then $n/2 = m + 1 < 2(m+1) - 2\sqrt[d]{m+1}$; Lemma 3.5 shows that this is not possible, and hence, $d = 1$; this gives the HMs under D).

Second, suppose T contains Alt_k, so T has a 3-cycle fixing $k - 2$ elements. If $b \in G$ is any preimage of that cycle under the projection $G \to T$, then b^2 fixes at least $(2m + 2) - 6 = 2m - 4$ elements. Since $m \geq 5$, this is again not possible by Lemma 3.5. Lastly, suppose $T \in \{\mathrm{PSL}_2(p), \mathrm{PGL}_2(p), M_{11}, M_{12}, M_{24}\}$. A direct computation shows that every non-trivial element in M_{11} and in M_{12} (on 12 points) fixes at most 4 points, and every non-trivial element of M_{24} (on 24 points) fixes at most 8 points. Thus, the previous argument cannot exclude the case that $G \leq C_2 \wr T$ with $T \in \{M_{11}, M_{12}, M_{24}\}$. Similarly, every non-trivial element in $\mathrm{PSL}_2(p)$, acting on $p + 1$ points, fixes at most 2 points; this yields the HMs under C).

Case iii): Here, $G = T \wr C_2$. By Proposition 3.3, there is a non-trivial element $a \in T$ that has a fixed point; hence, $(a, 1) \in T \times T \leq G$ fixes more than $n/2$ elements; this is not possible by Lemma 3.5. □

Going through the list of possibilities in Theorem 3.6, we conclude:

Corollary 3.7 *The order of a cocyclic TCC HM has the form $q + 1$, $2p + 2$, or 2^t for some prime power $q \equiv 3 \bmod 4$, prime $p \geq 3$, and integer $t \geq 2$, respectively.*

4 Existence of cocyclic TCC HMs

We now discuss the existence of cocyclic TCC HMs.

4.1 Paley type I and type II HMs

Let $\mathbb{F}_q$ be the finite field of odd size q, with primitive element $\omega \in \mathbb{F}_q$. The quadratic character $\chi : \mathbb{F}_q \to \mathbb{C}$ is defined by $\chi(g) = g^{(q-1)/2}$; that is, if $g \in \mathbb{F}_q^\times$, then $\chi(g) = 1$ if g is a square in $F^\times$, and $\chi(g) = -1$ otherwise. We order the elements of $\mathbb{F}_q$ as $g_0 = 0$ and $g_i = \omega^i$ for $i \in \{1, \ldots, q-1\}$. Let $Q = [\chi(g_i - g_j)]_{i,j \in \{0,\ldots,q-1\}}$ and define R as the $(q+1) \times (q+1)$ matrix

$$R = \begin{bmatrix} 0 & \chi(-1)\mathbf{1} \\ \mathbf{1}^\mathsf{T} & Q \end{bmatrix}.$$

Now, the Paley type I and type II matrices can be defined as follows:

$$P_{\mathrm{I}} = R + I_{q+1} \quad \text{and} \quad P_{\mathrm{II}} = \begin{bmatrix} R + I_{q+1} & R - I_{q+1} \\ R - I_{q+1} & -R - I_{q+1} \end{bmatrix}. \tag{3}$$

Theorem 4.1 *[3, Chapter 17] Paley matrices are cocyclic. A P_{I} matrix is Hadamard if and only if $q \equiv 3 \bmod 4$ and a P_{II} matrix is Hadamard if and only if $q \equiv 1 \bmod 4$. All P_{I} matrices of the same order are equivalent, as are all P_{II} matrices of the same order. A P_{I} matrix is equivalent to a P_{II} matrix if and only if the order of the matrix is at most 12.*

We now study when Paley HMs are TCC.

Proposition 4.2 *The Paley type I HMs are TCC for all prime powers $q \equiv 3 \bmod 4$. The Paley type II HMs are TCC if and only if $q \equiv 1 \bmod 4$ is a prime.*

Proof First, consider Paley I; that is, let $q \equiv 3 \bmod 4$ be a prime power. In this case, $\chi(-1) = -1$, and

$$\chi(x - y) = \chi(-1)\chi(y - x) = -\chi(y - x)$$

for all $x, y \in \mathbb{F}_q$. Let ω be a primitive element of $\mathbb{F}_q^\times$ and define

$$\mathcal{R} = \{\omega^{2i} : i \in \{1, \ldots, (q-1)/2\}\} \quad \text{and} \quad \mathcal{N} = \{\omega^{2i+1} : i \in \{1, \ldots, (q-1)/2\}\},$$

with this ordering. Let M be the matrix that arises from P_{I} by fixing the labels of the first row and column, and by labelling the remaining rows and columns by $0, \mathcal{R}, \mathcal{N}$ and $0, \mathcal{N}, \mathcal{R}$, respectively. Then, $P_{\mathrm{I}} \equiv M$, and, by construction,

$$M = \begin{bmatrix} 1 & -1 & -\mathbf{1} & -\mathbf{1} \\ 1 & 1 & \mathbf{1} & -\mathbf{1} \\ \mathbf{1}^{\mathsf{T}} & \mathbf{1}^{\mathsf{T}} & A & B \\ \mathbf{1}^{\mathsf{T}} & -\mathbf{1}^{\mathsf{T}} & C & D \end{bmatrix}.$$

We show that $C = B^{\mathsf{T}}$ and $D = -A^{\mathsf{T}}$. For this note that

$$B = I_{(q-1)/2} + \left[\chi(\omega^{2i} - \omega^{2j})\right]_{i,j\in\{1,\ldots,(q-1)/2\}} \quad \text{and}$$
$$C = I_{(q-1)/2} + \left[\chi(\omega^{2i+1} - \omega^{2j+1})\right]_{i,j\in\{1,\ldots,(q-1)/2\}}.$$

Now, $C = B^{\mathsf{T}}$ follows from $\chi(\omega^{2i+1}-\omega^{2j+1}) = \chi(\omega)\chi(\omega^{2i}-\omega^{2j}) = -\chi(\omega^{2i}-\omega^{2j}) = \chi(\omega^{2j}-\omega^{2i})$. Similarly, we have

$$A = \left[\chi(\omega^{2i} - \omega^{2j+1})\right]_{i,j\in\{1,\ldots,(q-1)/2\}} \quad \text{and}$$
$$D = \left[\chi(\omega^{2i+1} - \omega^{2j})\right]_{i,j\in\{1,\ldots,(q-1)/2\}}.$$

and $D = -A^{\mathsf{T}}$ follows from $\chi(\omega^{2i+1} - \omega^{2j}) = -\chi(\omega^{2j} - \omega^{2i+1})$. By construction, A and B are circulant matrices. We obtain the required TCC structure for M by multiplying all columns but the first by -1, and swapping the last two row blocks and column blocks.

Now, consider Paley II, that is, let $q \equiv 1 \bmod 4$ be a prime power; in this case, $\chi(-1) = 1$. It is straightforward to check that P_{II} is equivalent to

$$\begin{bmatrix} 1 & 1 & \mathbf{1} & \mathbf{1} \\ 1 & -1 & 1 & -1 \\ \mathbf{1}^{\mathsf{T}} & \mathbf{1} & -Q - I_q & Q - I_q \\ \mathbf{1}^{\mathsf{T}} & -\mathbf{1}^{\mathsf{T}} & Q - I_q & Q + I_q \end{bmatrix} \equiv P_{\mathrm{II}}.$$

Since $\chi(x - y) = \chi(-1)\chi(y - x) = \chi(y - x)$, the blocks $Q + I_q$ and $Q - I_q$ are symmetric; this proves that P_{II} is TCC if and only if these blocks are circulant. This occurs if and only if the additive group of the field $\mathbb{F}_q$ is cyclic, which occurs precisely when q is prime.

Lastly, we mention that the Paley II matrices are not equivalent to a TCC matrix when q is not prime. To see this, let H be a HM equivalent to the Paley II matrix of order $2q + 2$, where $q \equiv 1 \bmod 4$ is a prime power $q = p^a$. By [3, Theorem 17.2.6] and its proof, if $q > 5$, then the Sylow p-subgroup of $\mathrm{Aut}(H)$ has order q and is cyclic if and only if q is a prime. Hence, if $\mathcal{A}_H$ contains an element with cycle structure $1 + 1 + q + q$, then q is a prime; as shown above, the Paley II matrices are TCC precisely in this case. □

Recall that the Kronecker product of cocyclic HMs is cocyclic [3, Lemma 16.4.1]. Thus, the Kronecker product of a Paley I matrix of prime order $p \equiv 3 \bmod 4$ with the HM of order 2 is equivalent to a cocyclic HM. Together with the Paley II HMs, there exist cocyclic HMs of order $2q+2$ for all odd prime powers q. Moreover, there exist TCC HMs of order $2p+2$ where $p \equiv 3 \bmod 4$ is a prime, namely

$$\begin{bmatrix} P_{\mathrm{I}} & P_{\mathrm{I}} \\ P_{\mathrm{I}}^{\mathsf{T}} & -P_{\mathrm{I}}^{\mathsf{T}} \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & \mathbf{1} & \mathbf{1} \\ 1 & -1 & 1 & -1 \\ \mathbf{1}^{\mathsf{T}} & \mathbf{1} & -Q - I_q & -Q - I_q \\ \mathbf{1}^{\mathsf{T}} & -\mathbf{1}^{\mathsf{T}} & (-Q - I_q)^{\top} & (Q + I_q)^{\mathsf{T}} \end{bmatrix} \tag{4}$$

which is in TCC form. We did not manage to prove that this matrix is cocyclic; however, for every prime $p \equiv 3 \bmod 4$ with $7 \le p \le 500$, we have verified this computationally using techniques developed previously [12]. We also showed that this matrix is inequivalent to the Kronecker product of a HM of order 2 with P_{I}.

Proposition 4.3 *For every prime $p \equiv 3 \bmod 4$ with $7 \le p \le 500$, the matrices of the form (4) are cocyclic TCC HMs over the dihedral group of order $2p+2$.*

We can now prove our main result.

Proof of Theorem 1.1 The first claim follows from Corollary 3.7. The Paley type I matrices are cocyclic and equivalent to TCC matrices by Theorem 4.1; this establishes the existence of cocyclic TCC HMs with orders in (A). Existence of TCC HMs of orders in (B) is established for primes $p \equiv 1 \bmod 4$ by Theorem 4.1, and for primes $p \equiv 3 \bmod 4$ less than 500 by Proposition 4.3. Since $2^t - 1$ is prime for $t = 3, 5, 7$, the first power of 2 not covered by Theorem 4.1 or by Proposition 4.3 is 512. □

4.2 TCC HMs of 2-power order

We continue with a discussion of TCC HMs of 2-power order. The family of Sylvester HMs is iteratively constructed as

$$\mathrm{Syl}_{n+1} = \begin{bmatrix} \mathrm{Syl}_n & \mathrm{Syl}_n \\ \mathrm{Syl}_n & -\mathrm{Syl}_n \end{bmatrix} \quad \text{where} \quad \mathrm{Syl}_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

It is well known that the Sylvester matrix is Hadamard equivalent to a matrix of the form

$$S_n = \left[\begin{array}{c|c} 1 & \mathbf{1} \\ \hline \mathbf{1}^{\mathsf{T}} & D_n \end{array}\right], \tag{5}$$

where D_n is circulant. Let $w \in \mathbb{F}_{2^n}$ be a primitive element, then $D_n = [(-1)^{\mathrm{Tr}(\omega^{i-j})}]_{i,j=1,\ldots,2^n-1}$ satisfies $D_n D_n^{\top} = 2^n I_{2^n} - J_{2^n}$, see [7, Lemma 2.14]; we note that Horadam chooses an ordering of columns different from ours to obtain a symmetric back-circulant matrix. The Sylvester matrices are known to be cocyclic

over many non-isomorphic groups [5], see also [3, Lemma 21.1.1]. The TCC HMs in family (F3) have the form

$$S'_{n+1} = \begin{bmatrix} S_n & S_n \\ S_n^\mathsf{T} & -S_n^\mathsf{T} \end{bmatrix}.$$

Since the Hadamard matrices of orders 4 and 8 are unique up to equivalence, the first order at which these matrices could be distinct is 16. A computational investigation shows that the matrices have distinct automorphism groups. At order 32, the matrix S'_5 is *not* cocyclic, while the Sylvester matrices are always cocyclic. Our main result in this section is that the families S_n and S'_n are inequivalent as Hadamard matrices for $n \geq 4$. For this, we require the following preliminary result.

For a square $\{\pm 1\}$-matrix H, let $[H]_2$ be the $\mathbb{F}_2$-matrix arising from H where every 1 is replaced by 0, and every -1 is replaced by 1. The 2-rank of H is defined to be the (usual) rank of $[H]_2$ over $\mathbb{F}_2$.

Lemma 4.4 *Let H and K be square $\{\pm 1\}$-matrices. If H and K are Hadamard equivalent, then the 2-ranks of H and K differ by at most 2; this bound is sharp. If H arises from K by row and column permutations, then H and K have the same 2-rank.*

Proof By assumption, $RHC = K$ for signed permutation matrices R and C. Write $R = D_R P_R$ and $C = P_C D_C$ as in (2), and define $H' = P_R H P_C$. By construction, H' and H have the same 2-rank, so it remains to show that the 2-ranks of $K = D_R H' D_C$ and H' differ at most by 2. Note that multiplication of a row of H' by -1 corresponds to adding all (-1)'s vector to the respective row of $[H']_2$. Thus, if $i_1, \ldots, i_k$ are the indices of those rows of D_R that contain -1, then $[D_R H']_2 = [H']_2 + D$ where the entries of D are $d_{i,j} = 1$ if $i \in \{i_1, \ldots, i_k\}$ and $d_{i,j} = 0$ otherwise. This shows that the (row) ranks of $[D_R H']_2$ and $[H']_2$ differ by at most 1. The same argument shows that the (column) ranks of $[D_R H']_2$ and $[D_R H' D_C]_2 = [K]_2$ differ by at most 1, so the claim follows. Lastly, note that

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} -1 & -1 & 1 \\ 1 & 1 & -1 \\ 1 & 1 & -1 \end{bmatrix}$$

are equivalent and have 2-ranks 0 and 2, respectively. □

Proposition 4.5 *If $n \geq 3$, then S'_{n+1} is not equivalent to* Syl_{n+1}.

Proof Since $\mathrm{Syl}_n \equiv S_n$ and $\mathrm{Syl}_{n+1} = \mathrm{Syl}_1 \otimes \mathrm{Syl}_n$, it follows that $\mathrm{Syl}_{n+1} \equiv \mathrm{Syl}_1 \otimes S_n$; to simplify notation, in the following we write

$$S = \begin{bmatrix} S_n & S_n \\ S_n & -S_n \end{bmatrix} \quad \text{and} \quad S' = S'_{n+1} = \begin{bmatrix} S_n & S_n \\ S_n^\mathsf{T} & -S_n^\mathsf{T} \end{bmatrix}.$$

It suffices to prove that the 2-ranks of S and S' differ by more than 2; then, $S \not\equiv S'$ by Lemma 4.4.

By definition,

$$[S_n]_2 = \left[\begin{smallmatrix} 0 & \mathbf{0} \\ \mathbf{0}^\mathsf{T} & [D_n]_2 \end{smallmatrix}\right] \quad \text{and} \quad [S]_2 = \left[\begin{smallmatrix} [S_n]_2 & [S_n]_2 \\ [S_n]_2 & [S_n]_2 + J \end{smallmatrix}\right],$$

where $J = J_{2^n}$; thus, the 2-rank of S is the 2-rank of $[S_n]_2$ plus 1. Since Syl_n has 2-rank n, see [2, Theorem 1.3], it follows from Lemma 4.4 that the 2-rank of S is between $n-1$ and $n+3$.

Now, consider S'. Let R be the $(2^n-1)\times(2^n-1)$ matrix with 1's on its back-diagonal and 0's elsewhere, so that $RD_n^\mathsf{T} = D_n R$. This can be used to show that

$$S' \equiv \begin{bmatrix} 1 & \mathbf{1} & 1 & \mathbf{1} \\ \mathbf{1}^\mathsf{T} & D_n & \mathbf{1}^\mathsf{T} & D_n R \\ 1 & \mathbf{1} & -1 & -\mathbf{1} \\ \mathbf{1}^\mathsf{T} & D_n R & -\mathbf{1}^\mathsf{T} & -D_n \end{bmatrix}, \quad [S']_2 = \begin{bmatrix} 0 & \mathbf{0} & 0 & \mathbf{0} \\ \mathbf{0}^\mathsf{T} & [D_n]_2 & \mathbf{0}^\mathsf{T} & [D_n R]_2 \\ 0 & \mathbf{0} & 1 & \mathbf{1} \\ \mathbf{0}^\mathsf{T} & [D_n R]_2 & \mathbf{1}^\mathsf{T} & [D_n]_2 + J \end{bmatrix}$$

where J is a suitable all 1's matrix. By Lemma 4.4, the 2-rank of S' is 1 plus the rank of

$$A_n = \left[\begin{smallmatrix} [D_n]_2 & [D_n]_2 + [D_n R]_2 \\ [D_n]_2 + [D_n R]_2 & \mathbf{0} \end{smallmatrix}\right].$$

Note that $[D_n]_2 = [\mathrm{Tr}(\omega^{i-j})]_{i,j=1,\ldots,2^n-1}$, and $[D_n R]_2$ arises from $[D_n]_2$ by reversing the ordering of the columns, that is, $[D_n R]_2 = [\mathrm{Tr}(\omega^{i+j})]_{i,j=1,\ldots,2^n-1}$. Thus, the ranks of $[D_n]_2$ and $[D_n R]_2$ equal the 2-rank of S_n, which lies between $n-2$ and $n+2$: recall that $S_n \equiv \mathrm{Syl}_n$ and Syl_n has 2-rank n.

Since the trace function is a $\mathbb{F}_2$-linear map, the column space of $[D_n]_2$ is spanned by the columns labelled by a $\mathbb{F}_2$-basis of $\mathbb{F}_{2^n}$. Note that $[D_n]_2 + [D_n R]_2 = [\mathrm{Tr}(\omega^i(\omega^j + \omega^{-j}))]_{i,j=1,\ldots,2^n-1}$, so the columns of $[D_n]_2 + [D_n R]_2$ are exactly those columns of $[D_n]_2$ labelled by $\{\omega^i + \omega^{-i} : i = 1, \ldots, 2^n - 1\}$. Since the latter contains a $\mathbb{Z}_2$-basis[1] of $\mathbb{F}_{2^n}$, it follows that the rank of $[D_n]_2 + [D_n R]_2$ is the same as $[D_n]_2$.

Let B be the matrix such that $B[D_n]_2$ has row echelon form; if r is the rank of $B[D_n]_2$, then $B[D_n]_2$ has exactly r nonzero rows. By construction, $B[D_n R]_2$ arises from $B[D_n]_2$ by reversing the ordering of the columns. This shows that if row i in $B[D_n]_2$ is zero, then also row i in $B[D_n]_2 + B[D_n R]_2$ is zero; thus, $B[D_n]_2 + B[D_n R]_2$ has at most r nonzero rows. Since $[D_n]_2$ and $[D_n]_2 + [D_n R]_2$ have the same rank, it follows that $B[D_n]_2 + B[D_n R]_2$ has exactly r nonzero rows, and those rows are linearly independent; in particular, row i in $B[D_n]_2$ is nonzero if and only if row i in $B[D_n]_2 + B[D_n R]_2$ is nonzero. Together with the structure of A_n, this implies that the rank of A_n is twice the rank of $[D_n]_2$.

Now, we can conclude. Since the rank of $[D_n]_2$ is between $n-2$ and $n+2$, the rank of A_n is between $2n-4$ and $2n+4$. Thus, the 2-rank of S' lies between $2n-3$

[1] Note that $\mathcal{B} = \{\omega, \omega^2, \ldots, \omega^n\}$ is an $\mathbb{F}_2$-basis of $\mathbb{F}_{2^n}$. We claim that $\mathcal{C} = \{\omega + \omega^{-1}, \ldots, \omega^n + \omega^{-n}\}$ is also a basis. Let R be the $n \times n$ matrix with 1s on the back-diagonal, and let M be the matrix that describes multiplication by ω^{-n-1} with respect to $\mathcal{B}$. Then, the matrix $R + M$ describes the linear map defined by $\omega^i \mapsto \omega^{n+1-i} + \omega^{-n-1+i}$. Note that $R + M$ maps $\mathcal{B}$ to $\mathcal{C}$, and the claim follows from the non-singularity of $R + M$: if v is in the kernel of $R + M$, then $vR = vM$, and so $v = vR^2 = vM^2$; the matrix M^2 describes multiplication by $\omega^{-2n-2} \neq 1$, which forces $v = 0$.

and $2n+5$. As shown above, the 2-rank of S is between $n-1$ and $n+3$. If $n \geq 9$, then $2n-3$ and $n+3$ are more than 2 apart, which proves that $S \not\equiv S'$. For $4 \leq n \leq 8$, a direct computation shows that S and S' are not equivalent. □

4.3 QCC matrices and further research

The conclusions of Proposition 2.1 and Theorem 3.6 hold for a broader class of HMs than just the TCC matrices. Motivated by these results, we propose the class of *quadruple-circulant core* (QCC) HMs of order $n = 2m+2$, as any HM equivalent to a matrix of the form

$$\begin{bmatrix} 1 & 1 & \mathbf{1} & \mathbf{1} \\ 1 & -1 & \mathbf{1} & -\mathbf{1} \\ \mathbf{1}^\mathsf{T} & \mathbf{1}^\mathsf{T} & A & B \\ \mathbf{1}^\mathsf{T} & -\mathbf{1}^\mathsf{T} & C & -D \end{bmatrix}$$

where A, B, C, D are $\{\pm 1\}$-circulant blocks of order m. Note that a matrix of this shape is a HM if and only if

$$AA^\mathsf{T} + BB^\mathsf{T} = CC^\mathsf{T} + DD^\mathsf{T} = (2m+2)I_m - 2J_m,$$
$$AC^\mathsf{T} = BD^\mathsf{T}, \quad \text{and} \quad A\mathbf{1} = B\mathbf{1} = C\mathbf{1} = D\mathbf{1} = -\mathbf{1}.$$

Theorem 3.6 holds verbatim for QCC matrices. Since the Sylvester matrices and the Paley matrices belong to the class of QCC matrices, we have determined completely the spectrum of cocyclic QCC matrices: they exist at every order listed in Corollary 3.7.

In collaboration with R. Stafford, the third author developed strong restrictions on cocyclic HMs of order $n = 1+m$ whose automorphism groups contain elements of cycle structure $1+m$, see [14]. This was later developed into a full classification of such matrices, see [13]. The results of the present paper limit the possibilities for CHMs of order $n = 2m+2$ whose automorphism groups contain elements of cycle structure $1+1+m+m$. Based on these results, we propose the following questions for future research.

(R1) Horadam's [7, Research problem 40] concerns the family of Kimura HMs, which can be shown to have an automorphism with cycle structure $1+1+1+1+m+m+m+m$. Classification results or non-existence results for transitive permutation groups of degree $4m+4$ containing an element with this cycle structure could lead to classification results for those HMs. Conversely, a detailed structure analysis for such permutation groups could lead to new classes of HMs with specified circulant block structure (or more generally, group-invariant block structure).

(R2) Let G be a group with two monomial representations ρ_1 and ρ_2. Then, $\rho_1(g)H\rho_2(g^{-1}) = H$ for all $g \in G$ if and only if H belongs to the *intertwiner* of ρ_1 and ρ_2. In future work, the authors intend to develop methods for working with intertwiners of monomial representations of (covers of) permutation groups of small rank. An immediate application of this work would be the

classification of HMs for which $\mathcal{A}(H)$ is isomorphic to a subgroup of $C_2 \wr G$ where G is 2-transitive. This would provide a description of all HMs in cases b) and c) of Theorem 3.6, replacing the computational evidence of Proposition 4.3 with a formal classification result.

Acknowledgements The authors express their gratitude to Professor Ilias Kotsireas for helpful discussions and sharing computational data on TCC matrices. The authors also thank Dr. Ronan Egan for discussions on cocyclic development.

References

1. Barrera Acevedo, S., Ó Catháin, P., Dietrich, H.: Constructing cocyclic Hadamard matrices of order $4p$. J. Combin. Des. **27**, 627–642 (2019)
2. Bella, T., Olshevsky, V., Sakhnovich, L.: Ranks of Hadamard matrices and equivalence of Sylvester–Hadamard and pseudo-noise matrices. Oper. Theory: Adv. Appl. **179**, 35–46 (2007)
3. de Launey, W., Flannery, D.L.: Algebraic Design Theory. Mathematical Surveys and Monographs, vol. 175. American Mathematical Society, Providence, RI (2011)
4. Dixon, J.D., Mortimer, B.: Permutation Groups. Graduate Texts in Mathematics, vol. 163. Springer-Verlag, New York (1996)
5. Egan, R., Flannery, D.L.: Automorphisms of generalized Sylvester Hadamard matrices. Discrete Math. **340**, 516–523 (2017)
6. Fletcher, R.J., Gysin, M., Seberry, J.: Application of the Discrete fourier transform to the search for generalised Legendre pairs and Hadamard matrices. Australas. J. Combin. **23**, 75–86 (2001)
7. Horadam, K.J.: Hadamard Matrices and Their Applications. Princeton University Press, Princeton (2007)
8. Ito, N.: Hadamard matrices with "doubly transitive" automorphism groups. Arch. Math. (Basel) **35**((1–2)), 100–111 (1980)
9. Jones, G.A.: Primitive permutation groups containing a cycle. Bull. Aust. Math. Soc. **89**, 159–165 (2014)
10. Kotsireas, I.S., Koukouvinos, C., Seberry, J.: Hadamard ideals and Hadamard matrices with two circulant cores. European J. Combin. **27**, 658–668 (2006)
11. Moorhouse, G.E.: The 2-transitive complex Hadamard matrices. Preprint: ericmoorhouse.org/pub/complex.pdf
12. Ó Catháin, P., Röder, M.: The cocyclic Hadamard matrices of order less than 40. Des. Codes Cryptogr. **58**, 73–88 (2011)
13. Ó Catháin, P.: Difference sets and doubly transitive actions on Hadamard matrices. J. Combin. Theory Ser. A. **6**(119), 1235–1249 (2012)
14. Ó Catháin, P., Stafford, R.M.: On twin prime power Hadamard matrices. Cryptogr. Commun. **2**, 261–269 (2010)
15. Robinson, D.J.S.: A course in the theory of groups. Graduate Texts in Mathematics, 2nd edn, vol. 80. Springer-Verlag, New York (1996)
16. Wallis, W.D.: Combinatorial Designs. Marcel Dekker, NY (1988)