On twin prime power Hadamard matrices

Padraig Ó Catháin [*]

School of Mathematics, Statistics and Applied Mathematics,

National University of Ireland, Galway.

Richard M. Stafford [†]

National Security Agency

9800 Savage Road, Fort George G. Meade, MD 20755-6565, USA

October 23, 2009

Abstract

In this paper, we show that no Hadamard matrix constructed using the twin prime power method is cocyclic, with the exception of the matrix of order 16. We achieve this by showing that the action of the automorphism group of a cocyclic twin prime power matrix induces a 2-transitive action on the rows of the matrix. We then use Ito's classification of Hadamard matrices with 2-transitive automorphism groups to show that no twin prime power Hadamard matrix is cocyclic. This work answers a research problem posed by K.J. Horadam, and exhibits the first known infinite family of Hadamard matrices which are not cocyclic.

[*] *E-mail: p.ocathain1@nuigalway.ie*

[†] *E-mail: rmsfeb47@gmail.com*

1 Introduction

Cocyclic development was introduced to the study of combinatorial designs by de Launey and Horadam in the early 1990s. The relation between group development of matrices and the existence of regular subgroups of the automorphism group of that matrix is well known. Cocyclic development generalises this concept to a study of the action of quotient groups on distinguished submatrices of a group developed matrix. In [6, p.135, Research Problem 39], Horadam asks whether the Hadamard matrices derived from twin prime power designs are cocyclic. In this paper we answer this question in the negative. Several constructions for Hadamard matrices have been shown to always produce cocyclic matrices. This is the first proof that a construction method for Hadamard matrices never yields cocyclic Hadamard matrices.

In Section 2 we give a very brief overview of the theory of cocyclic development. Then in Section 3, we discuss twin prime power difference sets and their automorphism groups. Section 4 is devoted to an analysis of the finite 2-transitive groups, relying in particular on work of Ito. We conclude with a research problem.

2 Cocyclic Development

In this section, we briefly recall some facts about cocyclic development. A convenient reference that contains proofs of the results listed in this section is [9]. For definitive coverage of the theory, we refer the reader to [3]. The other main purpose of this section is to recall such facts as we require about the automorphism group of a cocyclic matrix, and to describe a particular induced action of the automorphism group. First we recall the definition of an automorphism of a Hadamard matrix.

Definition 1. Let H be a Hadamard matrix. An automorphism of H is a pair, (P, Q) of $\{\pm 1\}$-monomial matrices, such that

$$H = PHQ^{\top}.$$

The automorphisms of H form a group under the operation

$$(P_1, Q_1)(P_2, Q_2) = (P_1P_2, Q_1Q_2).$$

We denote the group of all automorphisms of H as $\mathrm{Aut}(H)$.

We denote by PermAut(H) the subgroup of Aut(H) consisting of all pairs (P, Q) of permutation matrices. This concept generalises naturally to matrices over an arbitrary ring: we say that the ordered pair of permutation matrices (P, Q) is an automorphism of M if $PMQ^\top = M$. Next, we introduce what may be loosely described as an action of Aut(H) on H.

Definition 2. Denote the full group of $\{\pm 1\}$-monomial matrices of degree n by $\mathcal{M}$. Every element, X, of $\mathcal{M}$ has a unique factorization $D_X E_X$ where D_X is a diagonal matrix, and E_X is a permutation matrix. Now let H be a Hadamard matrix. Let $(P, Q) \in \mathrm{Aut}(H)$, and define $\nu(P, Q) = E_P$. In this way (P, Q) induces a permutation on the rows of H. In fact, ν gives a permutation representation of Aut(H) in the symmetric group on the rows of H.

It is this action that we mean when we refer to the action of Aut(H) in the remainder of this paper. Note that a similar action exists on the columns of the matrix, and our results could be stated with equal validity in that context. Now, we give a definition of group development, which is a special case of cocyclic development.

Definition 3. Let G be a group of order n and let M be an $n \times n$ array with entries in an abelian group A. We say that M is *group developed over* G if there exist a set map $\phi : G \to A$ and two orderings $g_1, g_2 \ldots, g_n$ and $h_1, h_2 \ldots h_n$ of the elements of G such that

$$M = [\phi(g_i h_j)]_{1 \leq i,j \leq n}\,.$$

In the remainder of this paper, we shall assume without comment the existence of suitable orderings for the elements of G and denote such arrays by $[\phi(gh)]_{g,h\in G}$, or even $[\phi(gh)]$ where the indexing group is understood.

Theorem 4. *The matrix M is group developed over G if and only if there exists a regular subgroup of* PermAut(M) *isomorphic to G.*

Proof. See Theorem 2 of [9]. □

Definition 5. Let G be a finite group. A binary *(2-)cocycle* is a map $\psi : G \times G \to \langle -1 \rangle$ which obeys the following identity for all $g, h, k \in G$.

$$\psi(g, h)\, \psi(gh, k) = \psi(g, hk)\, \psi(h, k)$$

An $n \times n$ Hadamard matrix H is *cocyclic* if there exists a group G of order n, and a cocycle $\psi : G \times G \to \langle -1 \rangle$ such that

$$H = [\psi(g, h)]_{g,h \in G} \,.$$

We say that ψ *is a cocycle of* H.

This definition generalises naturally to matrices with entries in an arbitrary abelian group. There is an analogue of Theorem 4 for cocyclic matrices but we do not require that material in this paper. We provide only what is necessary for our purpose, which is a proof that, for a cocyclic Hadamard matrix H, $\nu(\mathrm{Aut}(H))$ acts transitively on the rows of H.

Lemma 6. *Let H be a cocyclic Hadamard matrix. Then $\nu(\mathrm{Aut}(H))$ is transitive.*

Proof. Let H be a cocyclic Hadamard matrix, with cocycle $\psi : G \times G \to \langle -1 \rangle$. For an elementary abelian 2-group, the cocycle equation can be written as

$$\psi(g, hk) = \psi(g, h)\psi(gh, k)\psi(h, k).$$

Now define $\delta^{xa}_y = 1$ if $y = xa$, and 0 otherwise. Define the following monomial matrices for all $a \in G$:

$$P_a = [\psi(x, a)\delta^{xa}_y]_{x,y \in G}, \quad Q^\top_a = [\psi(a, a^{-1}y)\delta^x_{a^{-1}y}]_{x,y \in G}.$$

Then (P_a, Q_a) is an automorphism of H for all $a \in G$:

$$\begin{aligned} P_a H Q^\top_a &= \left[\sum_{z,w \in G} \psi(x, a)\delta^{xa}_z \psi(z, w)\psi(a, a^{-1}y)\delta^w_{a^{-1}y}\right]_{x,y \in G} \\ &= \left[\psi(x, a)\psi(xa, a^{-1}y)\psi(a, a^{-1}y)\right]_{x,y \in G} \\ &= [\psi(x, y)]_{x,y \in G} \\ &= H \end{aligned}$$

Note that in the second last line, we use the cocycle equation, with $g = x$, $h = a$ and $k = a^{-1}y$.

Now, $\nu((P_a, Q_a)) = \left[\delta^{xa}_y\right]_{x,y \in G}$, and so $\nu(\mathrm{Aut}(H))$ contains the subgroup $\left\{ \left[\delta^{xa}_y\right]_{x,y \in G} \mid a \in G \right\} \cong G$ acting regularly on the rows of H. Thus $\nu(Aut(H)$ is transitive on the rows of H. □

3 Twin prime power difference sets

In this section we discuss some aspects of the theory of twin prime power difference sets. By twin prime powers, we mean a pair of odd positive integers, q and $q+2$, each of which is a prime power. We begin by recalling the standard definition of a difference set.

Definition 7. Let G be a group of order v, and let $\mathcal{D}$ be a subset of G of cardinality k. We say that $\mathcal{D}$ is a (v, k, λ)-*difference set* if it obeys the following group ring equation:

$$\mathcal{D}\mathcal{D}^{-1} = (k - \lambda) + \lambda \sum_{g \in G} g.$$

Let $\chi_{\mathcal{D}}$ denote the characteristic function of $\mathcal{D}$. Then the *development* of $\mathcal{D}$ is the matrix

$$Dev(\mathcal{D}) = [\chi_{\mathcal{D}}(gh)]_{g,h \in G}.$$

We note that twin prime power difference sets are a generalisation of twin prime difference sets, which were seemingly first discovered by Gruner in 1939. As Baumert observes, these difference sets 'seem to belong to that special class of mathematical objects which are prone to independent rediscovery'. They seem to be well understood, with Baumert giving a detailed description of their properties and generalisations in [1, p. 131-142]. The twin prime power case is as follows.

Definition 8. Let q and $q+2$ be twin prime powers, let $4n-1 = q(q+2)$. Denote by $\mathbb{F}_q$ the Galois field of size q, and by χ the standard quadratic residue function. Then

$$\{(g, 0) \mid g \in \mathbb{F}_q\} \bigcup \{(g, h) \mid g \in \mathbb{F}_q, h \in \mathbb{F}_{q+2}, \chi(g)\,\chi(h) = 1\}$$

is a $(4n-1, 2n-1, n-1)$-difference set in $(\mathbb{F}_q, +) \times (\mathbb{F}_{q+2}, +)$. We refer to such a difference set as a *TPP-difference set.*

For a proof that this is indeed a difference set, see Theorem 8.2 of [2]. Now let $\mathcal{D}$ be a difference set in a finite group G. We define $\mathrm{Aut}(\mathcal{D})$ to be $\mathrm{PermAut}(\mathrm{Dev}(\mathcal{D}))$. (Note that this is in fact the automorphism group of the underlying 2-design of $\mathcal{D}$.)

Lemma 9. *Let $\mathcal{D}$ be a difference set in a group G. Then* $\mathrm{Aut}(\mathcal{D})$ *contains a regular subgroup isomorphic to G.*

Proof. Since

$$\mathrm{Dev}(\mathcal{D}) = \left[\chi_{\mathcal{D}}(gh)\right]_{g,h\in G},$$

$\mathrm{Dev}(\mathcal{D})$ satisfies Definition 3. It follows from Theorem 4 that a subgroup of $\mathrm{Aut}(\mathcal{D})$ isomorphic to G acts regularly on $\mathrm{Dev}(\mathcal{D})$. □

In particular, we note that $\mathrm{Aut}(\mathcal{D})$ is transitive. The following Lemma describes how a $(4n-1, 2n-1, n-1)$-difference set gives rise to a Hadamard matrix, and how the automorphism group of the difference set embeds into the automorphism group of the Hadamard matrix.

Lemma 10. *Let $\mathcal{D}$ be a $(4n-1, 2n-1, n-1)$-difference set. Define D to be $2\,\mathrm{Dev}\,(\mathcal{D}) - J$, and $\overline{1}$ to be the all 1s vector of length $4n-1$. Then*

$$H = \begin{pmatrix} 1 & \overline{1} \\ \overline{1}^\top & D \end{pmatrix}$$

is a Hadamard matrix. Furthermore, $\mathrm{PermAut}(H) \cong \mathrm{Aut}(\mathcal{D})$.

Proof. Let I be the identity matrix of order $4n-1$, and J the $(4n-1)\times(4n-1)$ all ones matrix. From

$$\mathrm{Dev}(\mathcal{D})\,\mathrm{Dev}(\mathcal{D})^\top = nI + (n-1)J,$$

and the fact that $\mathrm{Dev}(\mathcal{D})$ has constant row sum $2n-1$, it follows that

$$DD^\top = 4nI - J.$$

Adding an initial row and column of +1s gives us a matrix, H, which satisfies the defining property of a Hadamard matrix:

$$HH^\top = 4nI_{4n}.$$

Now, $\mathrm{PermAut}(H)$ fixes the first row and column of H and permutes the remaining rows and columns amongst themselves. Any such automorphism is necessarily also an automorphism of $\mathrm{Dev}(\mathcal{D})$. In the other direction, we note that by definition, any automorphism of $\mathrm{Dev}(\mathcal{D})$ induces a permutation automorphism of H. □

We refer to a Hadamard matrix developed from a TPP-difference set as a TPP-Hadamard matrix. The following theorem gives a strong condition on the automorphism group of a TPP-Hadamard matrix that leads to our main result.

Theorem 11. *Let H be a TPP-Hadamard matrix. Then H is cocyclic only if $\nu(\mathrm{Aut}(H))$ acts 2-transitively on the rows of H.*

Proof. Recall that the action of a permutation group G on a set Ω is 2-transitive if and only if G is transitive on Ω, and the point stabiliser G_α is transitive on $\Omega - \alpha$, for any $\alpha \in \Omega$.

Suppose H is cocyclic. Then $\nu(\mathrm{Aut}(H))$ is transitive by Lemma 6. Furthermore, H is normalised, and so its first row is stabilised by $\mathrm{PermAut}(H)$. By Lemmas 9 and 10, the stabiliser of the first row in $\nu(\mathrm{Aut}(H))$ is transitive on the remaining rows. Hence, $\nu(\mathrm{Aut}(H))$ acts 2-transitively on the rows of H. $\square$

In the next section, we adapt the method of [4] to show that no 2-transitive group acts on a TPP-Hadamard matrix of order greater than 16, thus proving the following theorem:

Theorem 12. *Let H be a TPP-Hadamard matrix. Then H is cocyclic if and only if $|H| = 16$.*

4 Doubly transitive groups

The study of multiply transitive groups has a long history. An important early result in the field is due to Burnside.

Theorem 13 (Burnside)**.** *Let G be a 2-transitive group. Then the socle of G is either a regular elementary abelian p-group, or a non-regular nonabelian simple group.*

Thus the Classification of Finite Simple Groups (CFSG) yields a classification of 2-transitive groups, see Section 7.7 of [5] for a summary. They fall into 8 infinite families, with 10 exceptional groups (and some exceptional actions at small orders). We will seperate them into two types: affine (i.e. having a regular elementary abelian p-group as a socle) and non-affine. Even prior to the publication of the CFSG, Ito published a list of all Hadamard matrices with non-affine 2-transitive automorphism groups [7]. (The CFSG later proved his list of 2-transitive groups to be complete.) Moorhouse has recently extended this result to a classification of all complex Hadamard matrices with 2-transitive automorphism groups [8].

4.1 Ito's Theorem

In [7], Ito considers each of the known families of non-affine 2-transitive groups in turn and shows that none of them act on a Hadamard matrix, with the following exceptions.

Theorem 14 (Ito)**.** *Let Γ be a non-affine doubly transitive permutation group acting on the set of rows, Ω, of a Hadamard matrix, H. Then the action of Γ is one of the following:*

- *Γ on Ω is M_{12} and H is the unique Hadamard matrix of order 12.*
- *Γ on Ω contains $PSL_2(p^k)$ as a normal subgroup, for $p^k \equiv 3 \mod 4$, $p^k \neq 3, 11$.*
- *Γ on Ω is $Sp(6,2)$, and H is of order 36.*

The action considered by Ito is essentially the same as that given in Definition 2. None of the matrices on Ito's list are of twin prime power type. The Hadamard matrix of order 12 cannot be of TPP type since 11 is not a product of twin primes. The matrix of order 36 is ruled out by construction of the unique TPP-Hadamard matrix of order 36: it has an intransitive automorphism group.

This leaves only the infinite family of matrices acted upon by $PSL_2(p^k)$. Recall that $PSL_2(p^k)$ has a unique 2-transitive action on p^k+1 points. These are ruled out by the following observation: suppose H is a TPP-Hadamard matrix, of order $q(q+2)+1$. Then

$$p^k = q(q+2).$$

The only solution to this equation in positive integers has $p = q = 2$, which is not a valid solution (since $PSL_2(8)$ acts 2-transitively on 9 points).

This concludes our analysis of the non-affine 2-transitive groups. It is also possible to prove this result directly. With the exception of the projective special linear groups of dimension 3, it is possible via elementary counting arguments to show that no non-affine group acts 2-transitively on the rows of a TPP-Hadamard matrix.

4.2 Affine Groups

We observe first that if H is a TPP Hadamard matrix, then H necessarily has square order:

$$q(q+2)+1=(q+1)^2.$$

By Theorem 13, an affine group has an elementary abelian socle acting regularly on its underlying set. Thus we may restrict our attention to affine groups acting on 2^{2n} points, for $n \in \mathbb{N}$. Zsigmondy's theorem, given below, will be used in the proof of the next lemma.

Theorem 15 (Zsigmondy). *Let a, b and n be positive integers such that $(a,b)=1$. Then there exists a prime p with the following properties:*

- $p \mid a^n - b^n$
- $p \nmid a^k - b^k$ *for all* $k < n$.

with the following exceptions: $a=2, b=1, n=6$ *and* $a+b=2^k, n=2$.

Lemma 16. *The number $(2)^{2n}-1$ is not a product of twin prime powers, unless $n=2$ or $n=3$.*

Proof. Assume $2^{2n}-1$ is a product of twin prime powers.

$$2^{2n}-1=(2^n+1)(2^n-1)=p_1^s p_2^r$$

Without loss of generality, $p_1^s = 2^n - 1$. There are two cases to consider: either $2^n \equiv 1 \mod 3$, or $2^n \equiv 2 \mod 3$.

In the first case, $p_1 = 3$. Then we apply Zsigmondy's theorem to the equation $2^n - 1 = 3^s$, to obtain $n=2$ and $s=1$.

In the second case, $p_2 = 3$, and we have $3^r - 1 = 2^n$. Zsigmondy's theorem gives us that $r=1$ or $r=2$. The first of these is a vacuous solution however, as it gives $4-1=3\times 1$. □

This leads immediately to the following result.

Corollary 17. *Let H be a TPP-Hadamard matrix of order 2^n. Then H is either of order 16 or of order 64.*

It turns out that the TPP-Hadamard matrix of order 16 is equivalent to the Sylvester matrix of that order, and as such is cocyclic and has a 2-transitive automorphism group. By construction, the matrix of order 64 has an intransitive automorphism group and thus is not cocyclic. This completes the proof of Theorem 12.

5 Conclusion

As remarked in the text, our treatment of TPP-Hadamard matrices is broadly similar to that of [4]. In particular, we used the existence of a transitive automorphism group for the incidence matrix of the underlying difference set to force 2-transitivity of the automorphism group of the corresponding Hadamard matrix. Most other constructions for Hadamard matrices do not have such rigid algebraic structures underlying them. In fact, computer generation of all Hadamard 2-designs for small orders suggests that most such designs have small or trivial automorphism groups. As a result, it seems unlikely that this method can be generalised to many other classes of Hadamard matrices.

We conclude this paper with the following remarks and research problem. Let $q = p^n$, and $q + 2 = r^m$, where p and r are prime, and let $\mathcal{D}$ the TPP difference set of order $q(q + 2)$. We observed in Lemma 9 that $\mathrm{Aut}(\mathcal{D})$ contains a regular subgroup isomorphic to $C_p^n \times C_r^m$. In fact, it is possible to say more: denote an arbitrary element of $\mathbb{F}_q \times \mathbb{F}_{q+2}$ by (x, y). Then $\mathrm{Dev}(\mathcal{D})$ has automorphisms of the following types.

- $t_{a,b} : (x, y) \mapsto (x + a, y + b)$ for $a \in \mathbb{F}_q$ and $b \in \mathbb{F}_{q+2}$
- $m_{c,d} : (x, y) \mapsto (cx, dy)$ for $c \in \mathbb{F}_q^*$, $d \in \mathbb{F}_{q+2}$ and $\chi(c)\chi(d) = 1$
- $\sigma_p : (x, y) \mapsto (x^p, y)$, $\sigma_r : (x, y) \to (x, y^r)$.

Research Problem 1. *Show that*

$$\left\langle (-I, -I)\,, t_{a,b}, m_{c,d}\sigma_p, \sigma_r : a \in \mathbb{F}_q, b \in \mathbb{F}_{q+2}, c \in \mathbb{F}_q^*, d \in \mathbb{F}_{q+2}^* \right\rangle, \chi(c)\chi(d) = 1$$

generates the full automorphism group of the TPP-Hadamard matrix arising from q and $q + 2$, of order $mn(q + 2)(q + 1)(q)(q - 1)$. Determine its isomorphism type.

The following table, computed by the authors as part of the investigation supports the conjecture, proving it for all TPP-Hadamard matrices of order less than $1,000$.

Twin prime powers	Matrix order	Order of Automorphism Group
5, 7	36	840
7, 9	64	6048
9, 11	100	15840
11, 13	144	17160
17, 19	324	93024
23, 25	576	607200
25, 27	676	2527200
27, 29	784	1710072
29, 31	900	755160

Table 1: Order of automorphism groups of small TPP-Hadamard matrices

Acknowledgements

The authors would like to acknowlede the de Brún Centre for Computational Algebra and N.U.I., Galway for financial support. The authors would also like to thank Warwick de Launey for suggesting an approach to this problem, and Dane Flannery for his advice and support.

References

[1] Leonard D. Baumert. *Cyclic difference sets*. Lecture Notes in Mathematics, Vol. 182. Springer-Verlag, Berlin, 1971.

[2] Thomas Beth, Dieter Jungnickel, and Hanfried Lenz. *Design theory. Vol. I*, volume 69 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1999.

[3] Warwick de Launey and Dane Flannery. *Algebraic Design Theory*. Mathematical Surveys and Monographs. American Mathematical Society, to appear.

[4] Warwick de Launey and Richard M. Stafford. On the automorphisms of Paley's type II Hadamard matrix. *Discrete Math.*, 308(13):2910–2924, 2008.

[5] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[6] K. J. Horadam. *Hadamard matrices and their applications*. Princeton University Press, Princeton, NJ, 2007.

[7] Noboru Ito. Hadamard matrices with "doubly transitive" automorphism groups. *Arch. Math. (Basel)*, 35(1-2):100–111, 1980.

[8] G. Eric Moorhouse. The 2-transitive complex Hadamard matrices. *Preprint*.

[9] Padraig Ó Catháin and Marc Röder. Classification of cocyclic Hadamard matrices of order less than 40. *Submitted*, Preprint available at `http://www.maths.nuigalway.ie/~padraig/research.shtml`.