Automorphisms of generalized Sylvester Hadamard matrices

R. EGAN *

Department of Mathematics, *University of Rijeka, Croatia*

D. L. FLANNERY

School of Mathematics, Statistics and Applied Mathematics

National University of Ireland, Galway

September 14, 2016

Abstract

We examine the cocyclic development of the generalized Sylvester (also called Drake) Hadamard matrix. In particular, we give detailed results about the permutation automorphism group and full automorphism group. Following on from this, we derive existence conditions for the indexing and extension groups of each matrix viewed as a cocyclic pairwise combinatorial design.

1 Introduction

This paper is inspired by work of de Launey and Stafford. In [3, 4, 5] they determine the automorphism and extension groups of the Paley conference matrix and Paley Hadamard matrices. We embark on the analogous program for generalized Sylvester (Hadamard) matrices—another infinite family of pairwise combinatorial designs with a rich algebraic structure, incorporating the ordinary Sylvester

* *Corresponding author (ronan.egan@math.uniri.hr)*

2010 Mathematics Subject Classification: 05B20, 20B25, 20J06

Keywords: generalized Hadamard matrix, automorphism group, cocyclic development

Hadamard matrices. Apart from special cases, little has been said previously about the cocyclic development of this family. (For example, when the indexing group is elementary abelian, an account of all cocycles and Hadamard groups for the Sylvester Hadamard matrices appears in [2, Chapter 21].) Our main concern is describing all possible indexing and extension groups of a generalized Sylvester matrix.

Algebraic design theory has grown to encompass a range of theoretical and computational techniques. So we are now well-equipped to expand the list of case studies of cocyclic pairwise combinatorial designs, especially those which have received less attention than (ordinary) cocyclic Hadamard matrices. Our paper is a contribution toward this goal.

Drake matrices are suitable for such a case study. They have large automorphism groups and consequently an abundance of indexing and extension groups. New existence or classification results for them would be valuable in applied contexts that use knowledge of complex and generalized Hadamard matrices. Most notably of late this occurs in quantum information theory; see [10, Section 4.4] for other examples.

We summarize the paper's content. Section 2 provides background material on the generalized Sylvester matrix, its automorphism group, and cocyclic development. In Section 3, we explain how certain important subgroups of the automorphism group act; this includes a determination of the permutation automorphism group. In Section 4, we derive restrictions on the indexing and extension groups of a generalized Sylvester matrix, and identify them as regular affine groups. The concluding Section 5 illustrates our main results with output from MAGMA [1] experiments with reasonably small generalized Sylvester Hadamard matrices.

Parts of this paper draw on the PhD thesis [8] of the first author.

2 Background

Notation and definitions are mostly as in [2]. Rings are associative and unital; groups are finite. The $n \times n$ identity matrix is denoted I_n and the $n \times n$ all 1s matrix is denoted J_n.

2.1 Generalized Hadamard matrices

Let K be a finite group, and $n > 1$ be an integer divisible by $|K|$. A *generalized Hadamard matrix* $\mathrm{GH}(n, K)$ of order n over K is an $n \times n$ matrix H whose entries lie in K and such that

$$HH^* = nI_n + \frac{n}{|K|}\big(\textstyle\sum_{x\in K} x\big)(J_n - I_n).$$

Here the matrix algebra is carried out over the integral group ring $\mathbb{Z}K$, and H^* is the conjugate transpose $[h_{ji}^{-1}]$ of $H = [h_{ij}]$. For example,

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & a & b & ab \\ 1 & b & ab & a \\ 1 & ab & a & b \end{bmatrix}$$

is a $\mathrm{GH}(4, \mathrm{C}_2 \times \mathrm{C}_2)$. All known $\mathrm{GH}(n, K)$ have K of prime-power order.

Let p be a prime and V_k be the k-dimensional vector space over $\mathbb{F} = \mathrm{GF}(p^m)$. The V_k-indexed matrix

$$D_{p,m,k} := [xy^\top]_{x,y\in V_k} = [xy]_{x,y\in V_1} \otimes \cdots \otimes [xy]_{x,y\in V_1} \ (k \text{ factors})$$

is a $\mathrm{GH}(p^{mk}, \mathrm{C}_p^m)$ with entries in the additive group V_1 of $\mathbb{F}$, the Kronecker multiplication being performed over $\mathbb{Z}V_1$. We call $D_{p,m,k}$ a *generalized Sylvester matrix* or *Drake matrix* (see [7, Propositions 1.5, 1.6]). Sometimes the entries of $D_{p,m,k}$ will also be treated as elements of a multiplicative group.

An $n \times n$ matrix H with entries in $\langle\zeta_t\rangle$, where $\zeta_t = e^{2\pi\sqrt{-1}/t}$, is a *Butson Hadamard matrix* $\mathrm{BH}(n, t)$ if $HH^* = nI_n$. (Here H^* is the usual Hermitian, i.e., complex conjugate transpose of H.) A $\mathrm{GH}(n, \mathrm{C}_p)$ and a $\mathrm{BH}(n, p)$ are basically the same design. To elaborate, let $K = \langle x\rangle \cong \mathrm{C}_p$ and define the ring epimorphism $\eta_p : \mathbb{Z}K \to \mathbb{Z}[\zeta_p]$ by $\eta_p : \sum_{i=0}^{p-1} a_i x^i \mapsto \sum_{i=0}^{p-1} a_i \zeta_p^i$. Then a K-matrix H of order n is a $\mathrm{GH}(n, K)$ if and only if $\eta_p(H)$ is a $\mathrm{BH}(n, p)$. We may write $D_{p,1,k}$ for $\eta_p(D_{p,1,k})$; so $D_{2,1,k}$ is the Sylvester Hadamard matrix of order 2^k.

2.2 Automorphism groups

Let $\mathrm{Perm}(n)$ be the group of $n \times n$ permutation matrices over a ring R. We identify $\mathrm{Perm}(n)$ with $\mathrm{Sym}(n)$ via the permutation isomorphism defined by $\alpha \mapsto P_\alpha :=$

$[\delta^i_{\alpha(j)}]_{1\le i,j\le n}$ (using Kronecker delta notation: δ^r_s is 1 if $r = s$ and 0 otherwise). Let M be an $n \times n$ R-matrix. Pre-multiplication of M by P_α shifts row i to row $\alpha(i)$; post-multiplication of M by $P_\alpha^\top$ shifts column j to column $\alpha(j)$. The *permutation automorphism group* of M is

$$\mathrm{PAut}(M) = \{(P, Q) \mid P, Q \in \mathrm{Perm}(n) \text{ and } PMQ^\top = M\}.$$

In other words, $\mathrm{PAut}(M)$ is the stabilizer of M under the action of $\mathrm{Perm}(n)^2 := \mathrm{Perm}(n) \times \mathrm{Perm}(n)$ on the ring $\mathrm{Mat}(n, R)$ of $n \times n$ R-matrices defined by $(P, Q)X = PXQ^\top$. The associated $\mathrm{Perm}(n)^2$-orbit of M is its *permutation equivalence class*. We write $X \sim Y$ if X and Y are permutation equivalent.

Working over the ambient ring $\mathbb{Z}K$, let $\mathrm{Mon}(n, K)$ be the group of $n \times n$ monomial matrices with non-zero entries in the group K. The (full) *automorphism group* $\mathrm{Aut}(M)$ of an $n \times n$ $(0, K)$-matrix M is the stabilizer of M under the obvious $\mathrm{Mon}(n, K)^2$-action on the set of $n \times n$ $(0, K)$-matrices. That is,

$$\mathrm{Aut}(M) = \{(P, Q) \mid P, Q \in \mathrm{Mon}(n, K) \text{ and } PMQ^* = M\}$$

where Q^* is the matrix obtained from $Q^\top$ by inverting each non-zero entry. Of course $\mathrm{PAut}(M) \le \mathrm{Aut}(M)$. If X, Y are in the same $\mathrm{Mon}(n, K)^2$-orbit then they are *equivalent*, denoted $X \approx Y$.

Note that $X \sim Y \Rightarrow \mathrm{PAut}(X) \cong \mathrm{PAut}(Y)$, and $X \approx Y \Rightarrow \mathrm{Aut}(X) \cong \mathrm{Aut}(Y)$. However, $X \approx Y$ need not imply that $\mathrm{PAut}(X) \cong \mathrm{PAut}(Y)$.

Example 2.1. Let K_{2n} be the nth Kronecker power of the back-circulant matrix K_2 with first row $1\ 1\ 1\ -1$. We have $K_{2n} \approx D_{2,1,2n}$ and therefore $\mathrm{Aut}(K_{2n}) \cong \mathrm{Aut}(D_{2,1,2n})$. According to [12], $\mathrm{PAut}(K_{2n}) \cong \mathrm{GF}(2)^{2n} \rtimes \mathrm{Sp}(2n, 2)$. Although its full automorphism group is the same as that of K_{2n}, Theorem 3.2 shows that $D_{2,1,2n}$ for $n > 1$ has a much larger permutation automorphism group.

The automorphism group of the Drake matrix is worked out in [2, pp. 101–103]. Except when $k = m = 1$ and $p = 2$, [†]

$$\mathrm{Aut}(D_{p,m,k}) \cong (Z \times \mathrm{C}_p^{mk}) \rtimes \mathrm{AGL}(k, \mathbb{F}) \tag{1}$$

[†] Wherever necessary in the sequel, $D_{2,1,1}$ is implicitly excluded.

where the center $Z \cong \mathrm{C}_p^m$ consists of all scalar pairs $(aI_{p^{mk}}, aI_{p^{mk}})$. The affine group $\mathrm{AGL}(k, \mathbb{F})$ permutes column indices as expected (the second components of its elements are permutation matrices). That is, each pair $A \in \mathrm{GL}(k, \mathbb{F})$, $y \in V_k$ sends $x \in V_k$ to $xA + y$. Also $\mathrm{AGL}(k, \mathbb{F})$ fixes the row of $D_{p,m,k}$ labeled by the zero vector. Let Σ_k be the translation subgroup $\{\pi_v \mid v \in V_k\}$ of $\mathrm{AGL}(k, \mathbb{F})$, where $\pi_v \in \mathrm{Sym}(V_k)$ for $v \in V_k$ is defined by $\pi_v : x \mapsto x + v$. Then the middle factor C_p^{mk} in (1) acts as Σ_k permuting row indices.

Remark 2.2. Given an automorphism (P, Q) of $D_{p,m,k}$, saying what P does to rows determines what Q does to columns, and vice versa, because $D_{p,m,k}$ is invertible.

Let H be a $\mathrm{GH}(n, K)$. The *expanded design* of H is the block matrix

$$\mathcal{E}_H = [aHb]_{a,b \in K}.$$

If K is abelian then clearly $\mathcal{E}_H = [ab]_{a,b \in K} \otimes H$. The following is a specialization of [2, Theorem 9.6.12].

Theorem 2.3. $\mathrm{Aut}(H) \cong \mathrm{PAut}(\mathcal{E}_H)$.

We make the isomorphism in Theorem 2.3 explicit. If $M \in \mathrm{Mon}(n, K)$ then there are unique disjoint $(0, 1)$-matrices M_x such that $M = \sum_{x \in K} xM_x$. Let

$$S_x = [\delta^a_{xb}]_{a,b \in K} \quad \text{and} \quad T_x = [\delta^{ax}_b]_{a,b \in K}. \tag{2}$$

Next, let $\theta_1(M) = \sum_{x \in K} T_x \otimes M_x$ and $\theta_2(M) = \sum_{x \in K} S_x \otimes M_x$. Then

$$\Theta \colon (P, Q) \mapsto (\theta_1(P), \theta_2(Q)) \tag{3}$$

defines an isomorphism Θ of $\mathrm{Aut}(H)$ onto $\mathrm{PAut}(\mathcal{E}_H)$.

2.3 Cocyclic development

Denote by ρ_1, ρ_2 the epimorphisms onto first and second components, respectively, of $\mathrm{Mat}(n, R)^2$. Let M be an $n \times n$ indexed matrix over the ring R. Whenever it is convenient to do so, we regard $\rho_i(\mathrm{PAut}(M))$ as a subgroup of $\mathrm{Sym}(n)$ via the isomorphism mentioned at the beginning of Subsection 2.2. A subgroup S of $\mathrm{PAut}(M)$ is *regular* if the induced actions by $\rho_1(S)$ on the set of row indices and

$\rho_2(S)$ on the set of column indices are both regular. Note that one of these induced actions can be regular without the other being regular; also, ρ_i may or may not be injective (e.g., both are injective when M is invertible). If M is symmetric (as are the designs of interest in this paper) then there is a duality within its automorphism group: a statement about induced action on the rows of M translates into a matching statement about action on columns, and vice versa.

We say that M is *group-developed* over a group G if there is a map $\phi : G \to R$ such that $M \sim [\phi(gh)]_{g,h\in G}$.

Proposition 2.4. *M is group-developed over a group G of order n if and only if $\mathrm{PAut}(M)$ has a regular subgroup isomorphic to G.*

Proof. See, e.g., [2, Theorem 10.3.8]. □

Example 2.5. Recall Example 2.1. Since K_2 is group-developed over C_4 and C_2^2, K_{2n} is group-developed over $\mathrm{C}_2^{2i} \times \mathrm{C}_4^{n-i}$ for $0 \le i \le n$ (if M_i is group-developed over G_i, $1 \le i \le 2$, then $M_1 \otimes M_2$ is group-developed over $G_1 \times G_2$). The equivalent design $D_{2,1,n}$ has a constant row (and constant column) so is not group-developed. We confirmed by a MAGMA computation that K_6 is group-developed over exactly 171 of the groups of order 64. This agrees with [6, p. 289].

Let G be a group and U be an abelian group. A map $\psi : G \times G \to U$ is a *cocycle* if $\psi(g,h)\psi(gh,k) = \psi(g,hk)\psi(h,k)$ for all $g, h, k \in G$. We may assume that our cocycles ψ are *normalized*, i.e., $\psi(g,1) = \psi(1,g) = 1$ for all $g \in G$. Each normalized set map $\phi : G \to U$ gives rise to a cocycle $\partial\phi$, called a *coboundary*, where $\partial\phi(g,h) = \phi(g)^{-1}\phi(h)^{-1}\phi(gh)$.

Denote by E_ψ the canonical central extension of U by G corresponding to a cocycle $\psi : G \times G \to U$. The group E_ψ has element set $\{(g,u) \mid g \in G,\ u \in U\}$ and multiplication defined by $(g,u)(h,v) = (gh, uv\psi(g,h))$.

We say that an $n \times n$ U-matrix M is *cocyclic*, with *indexing group* G and cocycle $\psi : G \times G \to U$, if $M \approx [\psi(g,h)]_{g,h\in G}$. (This definition can be widened to accommodate matrices with zero entries [2, Chapter 13].) Any group isomorphic to E_ψ for some cocycle ψ of M is an *extension group* of M. A group-developed U-matrix $[\phi(gh)]_{g,h\in G}$ is cocyclic, with cocycle $\partial\phi$.

Let H be a $\mathrm{GH}(n, U)$, and S_u, T_u for $u \in U$ be as in (2). Define

$$\Theta_U = \{(T_u \otimes I_n, S_u \otimes I_n) \mid u \in U\} \leq \mathrm{Perm}(n|U|)^2.$$

That is, Θ_U is the image under Θ of the central subgroup $\{(uI_n, uI_n) \mid u \in U\} \leq \mathrm{Mon}(n, U)^2$. A regular subgroup of $\mathrm{PAut}(\mathcal{E}_H)$ whose center contains Θ_U is called *centrally regular*. Let $\psi : G \times G \to U$ be a cocycle; a monomorphism $E_\psi \to \mathrm{PAut}(\mathcal{E}_H)$ is a *centrally regular embedding* if its image is regular, and it maps $(1, u)$ to $(T_u \otimes I_n, S_u \otimes I_n)$ for all $u \in U$.

Theorem 2.6. *A generalized Hadamard matrix H over an abelian group is cocyclic with cocycle ψ if and only if there is a centrally regular embedding of E_ψ into $\mathrm{PAut}(\mathcal{E}_H)$.*

Proof. See [2, Theorem 14.6.4]. □

Certainly $D_{p,m,k}$ is cocyclic; e.g., $\psi : \Sigma_k \times \Sigma_k \to V_1$ defined by $\psi(\pi_x, \pi_y) = xy^\top$ is a cocycle of $D_{p,m,k}$.

3 Automorphism group actions

To prepare for the next section, in this section we explain how the automorphisms of a generalized Sylvester matrix act.

We first deal with the permutation automorphism group.

Lemma 3.1. *Let $(P, Q) \in \mathrm{PAut}(D_{p,m,k})$, where*

$$P = [\delta_y^{\pi(x)}]_{x,y \in V_k} \quad \textit{and} \quad Q = [\delta_y^{\phi(x)}]_{x,y \in V_k}$$

for π, $\phi \in \mathrm{Sym}(V_k)$. Then there is $A \in \mathrm{GL}(k, \mathbb{F})$ such that

$$\pi(x) = xA \quad \textit{and} \quad \phi(x) = x(A^{-1})^\top \quad \forall\, x \in V_k.$$

Proof. We have

$$\begin{aligned}
[xy^\top]_{x,y \in V_k} &= PD_{p,m,k}Q^\top \\
&= [\delta_t^{\pi(x)}]_{x,t}[ts^\top]_{t,s}[\delta_y^{\phi(s)}]_{s,y}^\top \\
&= [\textstyle\sum_t \delta_t^{\pi(x)} ts^\top]_{x,s}[\delta_s^{\phi(y)}]_{s,y} \\
&= [\textstyle\sum_s \pi(x)s^\top \delta_s^{\phi(y)}]_{x,y} \\
&= [\pi(x)\phi(y)^\top]_{x,y},
\end{aligned}$$

and so $\pi(x)\phi(y)^\top = xy^\top$. Then for any $a, b \in \mathbb{F}$ and $t \in V_k$,

$$\pi(ax + bt)\phi(y)^\top = a\pi(x)\phi(y)^\top + b\pi(t)\phi(y)^\top.$$

As this holds universally, $\pi(ax + bt) = a\pi(x) + b\pi(t)$; i.e., π is $\mathbb{F}$-linear on V_k. By the same reasoning, ϕ is too. Hence there are $A, B \in \mathrm{GL}(k, \mathbb{F})$ such that $\pi(x) = xA$ and $\phi(x) = xB$. Then $xy^\top = xAB^\top y^\top$ for all x, y implies that $AB^\top$ is the identity matrix. □

Theorem 3.2. $\mathrm{PAut}(D_{p,m,k}) \cong \mathrm{GL}(k, \mathbb{F})$.

Proof. Define $f : \mathrm{PAut}(D_{p,m,k}) \to \mathrm{GL}(k, \mathbb{F})$ by $f : (P, Q) \mapsto A$, where A is determined by $P = [\delta_y^{\pi(x)}]_{x,y}$ as per Lemma 3.1. Let $(X, Y) \in \mathrm{PAut}(D_{p,m,k})$, say $X = [\delta_y^{\mu(x)}]_{x,y}$ and $f((X, Y)) = B$. Now $PX = [\delta_y^{\mu\pi(x)}]_{x,y}$ and $\mu\pi(x) = xAB$. Thus f is a homomorphism. If $A = B$ then $\pi = \mu$, so $P = X$; and $Q = Y$ by Lemma 3.1 (or Remark 2.2). Finally, if $C \in \mathrm{GL}(k, \mathbb{F})$ then $\eta : x \mapsto xC$ and $\nu : x \mapsto x(C^{-1})^\top$ are permutations of V_k such that $([\delta_y^{\eta(x)}]_{x,y}, [\delta_y^{\nu(x)}]_{x,y})$ is an automorphism of $D_{p,m,k}$. □

Let M be a $p^{mk} \times p^{mk}$ matrix indexed by V_k. The translation group Σ_k of V_k *embeds naturally* into $\mathrm{PAut}(M)$ if $(P_{\pi_v}, P_{\pi_{-v}}) \in \mathrm{PAut}(M)$ for all $v \in V_k$, where $P_\phi = [\delta^x_{\phi(y)}]_{x,y \in V_k} \in \mathrm{Perm}(p^{mk})$ in our usual notation. More generally, when $\mathrm{Aut}(M)$ is defined, we say that Σ_k *acts naturally* on the rows of M if $\Sigma_k \leq \rho_1(\mathrm{Aut}(M))$. The definition of natural action by Σ_k on columns of M replaces ρ_1 by ρ_2.

The following is a variant of Proposition 2.4.

Lemma 3.3. Σ_k *embeds naturally in* $\mathrm{PAut}(M)$ *if and only if* M *is group-developed over* C_p^{mk}.

Since $D_{p,m,k}$ is normalized and thus not group-developed, Σ_k does not embed naturally into $\mathrm{PAut}(D_{p,m,k})$. Of course Σ_k may embed non-naturally. By way of Theorem 3.2, the next lemma pinpoints when this happens.

Lemma 3.4. $\mathrm{PAut}(D_{p,m,k})$ *has a subgroup isomorphic to* C_p^{mk} *if and only if* $k \geq 4$.

Proof. Let $t_{ij}(a) \in \mathrm{GL}(k, \mathbb{F})$ be the matrix with main diagonal of 1s, a in position (i, j), and zeros elsewhere. Let $\{1, b, \ldots, b^{m-1}\}$ be a $\mathrm{GF}(p)$-basis of $\mathbb{F}$. If $k \geq 4$ then $\{t_{1j}(b^i), t_{2j}(b^i) \mid 0 \leq i \leq m-1,\ 3 \leq j \leq k\}$ generates an elementary abelian p-group of rank $(2k-4)m$, containing a subgroup of rank mk.

If $1 \leq k \leq 2$ then C_p^{mk} is larger than any p-subgroup of $\mathrm{GL}(k, \mathbb{F})$; whereas a Sylow p-subgroup of $\mathrm{GL}(3, \mathbb{F})$ has order p^{3m}, but is non-abelian. □

Remark 3.5. We already knew that $\mathrm{Aut}(D_{2,1,2k})$ has a subgroup isomorphic to C_2^{2k}, because $D_{2,1,2k} \approx K_{2k}$.

Although $\mathrm{PAut}(D_{p,m,k})$ does not have regular subgroups, the next lemma shows that Σ_k induces separate regular actions on the rows and, by duality, on the columns of $D_{p,m,k}$. (Actually, this point was alluded to earlier, in the comment after (1) about the factor $\mathrm{C}_{p^{mk}}$.)

Lemma 3.6. *There are diagonal matrices B_v such that $\{(P_{\pi_v}, B_v) \mid v \in V_k\} \leq \mathrm{Aut}(D_{p,m,k})$. Hence Σ_k is isomorphic to a subgroup of $\mathrm{Aut}(D_{p,m,k})$ acting naturally on the rows (resp., columns) of $D_{p,m,k}$, but not moving any column (resp., row).*

Proof. Take B_v to be the V_k-indexed diagonal matrix with $-v \cdot y$ in position y on its main diagonal. □

Denote the zero vector of V_k by $\mathbf{0}$. Let M be a $p^{mk} \times p^{mk}$ matrix indexed by V_k. Let Γ be the stabilizer in $\rho_1(\mathrm{PAut}(M))$ of the $\mathbf{0}$-row. Usually we label the first row $\mathbf{0}$, and label columns in the same order as rows.

Lemma 3.7. *If $\Sigma_k \leq \rho_1(\mathrm{PAut}(M))$ then each element P of $\rho_1(\mathrm{PAut}(M))$ has the form P_ϕ where $\phi \in \mathrm{Sym}(V_k)$ is uniquely expressible as $\pi_v g$ for some $\pi_v \in \Sigma_k$ and $g \in \Gamma$.*

Proof. Since $\pi_{-\phi(\mathbf{0})}\phi \in \Gamma$, we have $\phi \in \Sigma_k\Gamma$. Uniqueness is just as straightforward. □

Lemma 3.8. *Suppose that $\Sigma_k \leq \rho_1(\mathrm{PAut}(M))$. Then Γ acts additively on the rows of M if and only if $\rho_1(\mathrm{PAut}(M)) = \Sigma_k \rtimes \Gamma$.*

Proof. By Lemma 3.7, it suffices to observe that Γ acting additively on rows is equivalent to Γ normalizing Σ_k, i.e., $\pi_v^g = \pi_{g^{-1}(v)}$ for all $g \in \Gamma$, $v \in V_k$. $\square$

We use the isomorphism Θ defined in (3) to describe more precisely how the permutation automorphism group acts on $\mathcal{E}_{D_{p,m,k}}$. Since this expanded design is symmetric, a familiar row/column duality holds. Also note that ρ_1 and ρ_2 on $\mathrm{PAut}(\mathcal{E}_{D_{p,m,k}})$ are injective: this follows from the definition of Θ and the fact that ρ_1, ρ_2 on $\mathrm{Aut}(D_{p,m,k})$ are injective.

Hereafter, $v \circ x$ stands for the concatenation of vectors v and x.

Proposition 3.9. $\mathrm{PAut}(\mathcal{E}_{D_{p,m,k}}) = N \rtimes L$ *where*

(i) $N \cong \mathrm{C}_p^{m(k+1)}$ *acts in the natural way as* Σ_{k+1} *on the rows of* $\mathcal{E}_{D_{p,m,k}}$.

(ii) $L \cong \mathrm{AGL}(k, \mathbb{F})$ *acts additively and as* Γ *on the rows of* $\mathcal{E}_{D_{p,m,k}}$.

(iii) $N = N_1 \times N_2$, $N_1 \cong \mathrm{C}_p^{mk}$ *fixes column* $rp^{mk} + 1$ *for* $0 \le r \le p^m - 1$, *and* N_2 *permutes these columns regularly.*

(iv) *Each set of* p^{mk} *successive columns of* $\mathcal{E}_{D_{p,m,k}}$ *starting from the first column is a single orbit under* L, *and* L *acts identically on each orbit as* $\mathrm{AGL}(k, \mathbb{F})$ *(i.e.,* $g \in L$ *shifts column* i *to column* j, $1 \le i, j \le p^{mk}$, *if and only if* g *shifts column* $rp^{mk} + i$ *to column* $rp^{mk} + j$ *for* $1 \le r \le p^m - 1$*).*

Proof. We rely on the discussion of $\mathrm{Aut}(D_{p,m,k})$ after Example 2.1.

Select orderings of V_k and $\mathbb{F}$ (starting at the zero elements), which then impose the ordering of $V_{k+1} = \{v \circ x \mid v \in V_k, x \in \mathbb{F}\}$ defined by $v_1 \circ x_1 < v_2 \circ x_2 \Leftrightarrow x_1 < x_2$, or $x_1 = x_2$ and $v_1 < v_2$. Label rows and columns of $\mathcal{E}_{D_{p,m,k}}$ by the elements of V_{k+1} under this ordering.

The center Z of $\mathrm{Aut}(D_{p,m,k})$ is all constant scalar pairs in $\mathrm{Mat}(p^{mk}, \mathbb{F})^2$. Applying (3), we see that Θ maps $(xI_{p^{mk}}, xI_{p^{mk}}) \in Z$ to $(P_{\pi_{\mathbf{0} \circ (-x)}}, P_{\pi_{\mathbf{0} \circ x}})$.

Let W be the group $\{(P_{\pi_v}, B_v) \mid v \in V_k\}$ of Lemma 3.6. Since $\theta_1(P_{\pi_v})$ is a block diagonal matrix with P_{π_v} down its main diagonal, $\Theta(W)$ acts on rows of the expanded design as translations $P_{\pi_{v \circ 0}}$. On the other hand, $\theta_2(B_v)$ fixes the columns labeled by vectors $\mathbf{0} \circ x$. This completes verification of (i) and (iii) for $N = \Theta(\langle W, Z \rangle)$.

Recall that $\mathrm{Aut}(D_{p,m,k})$ splits over $Z \times W$, with a complement $\tilde{L}$ that fixes the zero row and permutes columns as $\mathrm{AGL}(k, \mathbb{F})$. So $L = \Theta(\tilde{L})$ fixes the zero row and acts on columns as claimed in (iv). Then we are done by Lemma 3.8. □

We continue with the notation and conventions of Proposition 3.9 and its proof.

Lemma 3.10. *The element of L corresponding to $\pi_a A \in \mathrm{AGL}(k, \mathbb{F})$ shifts row $v \circ e$ of $\mathcal{E}_{D_{p,m,k}}$ for $v \in V_k$ and $e \in \mathbb{F}$ to row $vA^\top \circ (e - aA^2v^\top)$.*

Proof. By [2, p. 103], $t \in \rho_1(L)$ has the form $\theta_1([\delta^x_{\phi(y)} g(x)]_{x,y \in V_k})$ where $\phi(x) = xA^\top$ and $g(x) = aAx^\top$. The result then follows from the definition of θ_1, which says that t shifts row $v \circ e$ to row $\phi(v) \circ (e - g(\phi(v)))$. □

We can now strengthen Proposition 3.9 (ii).

Corollary 3.11. *L acts linearly on the rows of $\mathcal{E}_{D_{p,m,k}}$.*

Proof. It is routine to check that the permutation of V_{k+1} defined in Lemma 3.10 is linear. □

Remark 3.12. Corollary 3.11 is an instance of the fact that $\mathrm{AGL}(k, \mathbb{E})$ embeds into $\mathrm{GL}(k+1, \mathbb{E})$ for any field $\mathbb{E}$.

4 Indexing and extension groups

Ó Catháin and Röder [14] classified all indexing and extension groups of the Sylvester matrices $D_{2,1,k}$ for $k \leq 4$. The authors and Ó Catháin [9] give the same kind of classification for the cocyclic $\mathrm{BH}(n, p)$ with p an odd prime and $np \leq 100$. In this section we characterize the indexing and extension groups of $D_{p,m,k}$ in broader terms, for all m, $k \geq 1$ and primes p.

4.1 The main theorems

Our first theorem is a direct consequence of Proposition 3.9 and Corollary 3.11.

Theorem 4.1. *Each extension group of $D_{p,m,k}$ is isomorphic to a regular subgroup of $\mathrm{AGL}(k+1, \mathbb{F})$.*

We proceed to our second main result. Define $C = \{\mathbf{0} \circ x \mid x \in \mathbb{F}\} \subseteq V_{k+1}$. Let G be an indexing group of $D_{p,m,k}$ with centrally regular extension E. For $S \leq \mathrm{PAut}(\mathcal{E}_{D_{p,m,k}})$, we also denote the isomorphic images $\rho_1(S)$, $\rho_2(S)$ in $\mathrm{Sym}(V_{k+1})$ by S. With this understanding, E is a regular subgroup of $N \rtimes L$ where N, L are as in Proposition 3.9, whose center contains $X := \{\pi_c \mid c \in C\} = \rho_i(\Theta(Z))$ for $i = 1, 2$. Furthermore $E/X \cong G$.

For the moment we focus on column action. Since $X \subseteq E$ and all point stabilizers of E are trivial, $E \cap N = X$ by Proposition 3.9 (iii). Hence $\Lambda := L \cap NE \cong E/(E \cap N) \cong G$ has order p^{mk}.

Lemma 4.2. *Λ is regular on each set of p^{mk} successive columns of $\mathcal{E}_{D_{p,m,k}}$, starting from the first column.*

Proof. The orbit of the zero column under N is C. For E to be transitive on V_{k+1}, the orbit of the zero column under Λ must consist of the first p^{mk} columns. □

Proposition 3.9 and Lemma 4.2 yield

Theorem 4.3. *Each indexing group of $D_{p,m,k}$ is isomorphic to a regular subgroup of $\mathrm{AGL}(k, \mathbb{F})$.*

Remark 4.4. While related partial classifications have been obtained (see, e.g., [13]), classifying regular subgroups of $\mathrm{AGL}(k, \mathbb{F})$ is difficult. Theorems 4.1 and 4.3 indicate that completely classifying the indexing and extension groups of $D_{p,m,k}$ would be similarly difficult.

We say a little more about the indexing and extension groups of $D_{p,m,k}$, by considering the row action on $\mathcal{E}_{D_{p,m,k}}$. Now E, N, L, X will stand for the images of their namesakes under ρ_1. Once again $E \cap N = X$.

Lemma 4.5. (i) *$N \leq E\Lambda$; equivalently, $E \cap L = 1$.*

(ii) *$\Lambda(c) = c$ for all $c \in C$.*

Proof. Proposition 3.9 (ii) and regularity of E give (i). If $\pi_v g \in E$ then $\pi_c \pi_v g = \pi_v g \pi_c = \pi_v \pi_{g(c)} g$, so $g(c) = c$. □

Remark 4.6. Part (i) is not apparent from the column action on $\mathcal{E}_{D_{p,m,k}}$. As for part (ii), the image of $\mathrm{AGL}(k,\mathbb{F})$ in $\mathrm{GL}(k+1,\mathbb{F})$ under the (faithful) representation arising from the row action stated in Lemma 3.10 fixes C elementwise.

Our last result in this subsection is another criterion for the row action of Λ, that depends on what we already know about its column action. For $v \in V_{k+1}$, let B_v denote the set of vectors labeling rows of $\mathcal{E}_{D_{p,m,k}}$ with $0_{\mathbb{F}}$ in column v. If $h \in \mathrm{PAut}(\mathcal{E}_{D_{p,m,k}})$ then $h(B_v) = \{h(w) \mid w \in B_v\}$ is the set of vectors labeling rows with $0_{\mathbb{F}}$ in some column u of the expanded design; i.e., $h(B_v) = B_u$. Thus $\mathrm{PAut}(\mathcal{E}_{D_{p,m,k}})$ acts on the set of all B_v.

Lemma 4.7. *Under the action defined above, Λ is regular on $\mathcal{B}_x := \{B_{u \circ x} \mid u \in V_k\}$ for each $x \in \mathbb{F}$.*

Proof. Lemma 4.2 implies that $\Lambda(\mathcal{B}_x) = \mathcal{B}_x$. Since $B_w = B_{w'}$ only if $w = w'$, and E is regular on columns, every B_v has trivial Λ-stabilizer. □

Lemmas 4.5 (i) and 4.7 suggest that the converse of Theorem 4.3 will be false in general. This is demonstrated in Section 5.

4.2 Exponent bounds

We can readily construct indexing groups of a Drake matrix as direct products via Kronecker multiplication and classifications at smaller orders (cf. Example 2.5). Such groups will have relatively low exponent. An easy argument establishes this property in general.

Proposition 4.8. *An indexing group and an extension group of $D_{p,m,k}$ have exponent dividing $p^{\lceil \log_p(k+1) \rceil}$ and $p^{\lceil \log_p(k+2) \rceil}$ respectively.*

Proof. The exponent of a p-subgroup of $\mathrm{GL}(k,\mathbb{F})$ divides $p^{\lceil \log_p k \rceil}$ (see, e.g., [15, p. 192]). Since $\mathrm{AGL}(k,\mathbb{F})$ is isomorphic to a subgroup of $\mathrm{GL}(k+1,\mathbb{F})$, the bounds are then immediate from Theorems 4.1 and 4.3. □

Example 4.9. A group over which K_{2n} is developed is a regular subgroup of $\mathrm{PAut}(K_{2n}) \cong \Sigma_{2n} \rtimes \mathrm{Sp}(2n,2)$, so has exponent at most $2^{\lceil \log_2(2n+1) \rceil}$. Indeed, this bound holds for every indexing group of K_{2n} by Proposition 4.8.

Remark 4.10. Ito proved that a cocyclic Hadamard matrix of order greater than 2 cannot have cyclic or dihedral extension groups [11, Propositions 6 and 7]. For Sylvester Hadamard matrices of order $2^k > 16$, Proposition 4.8 imposes a much stronger restriction.

5 Experimental results

For various (necessarily small) p, m, k, we used MAGMA to compute the centrally regular subgroups of $\mathrm{PAut}(\mathcal{E}_{D_{p,m,k}})$, and thereby found all indexing and extension groups for $D_{p,m,k}$. Table 1 displays some of the data.

m	p	k	r	r'	r''	s	s'
1	2	1	1	1	1	1	1
		2	4	3	2	2	2
		3	10	9	3	8	4
		4	113	34	12	39	12
	3	1	2	1	1	1	1
		2	8	4	1	2	1
		3	56	9	4	12	4
	5	1	2	1	1	1	1
		2	12	2	1	2	1
	7	1	2	1	1	1	1
		2	28	2	1	2	1
2	2	1	8	4	1	1	1
		2	502	39	4	4	4
	3	1	23	2	1	1	1

r: number of conjugacy classes of the centrally regular subgroups of $\mathrm{PAut}(\mathcal{E}_{D_{p,m,k}})$

r': number of isomorphism types of the centrally regular subgroups of $\mathrm{PAut}(\mathcal{E}_{D_{p,m,k}})$

r'': number of isomorphism types of the indexing groups of $D_{p,m,k}$

s: number of conjugacy classes of the regular subgroups of $\mathrm{AGL}(k, \mathbb{F})$

s': number of isomorphism types of the regular subgroups of $\mathrm{AGL}(k, \mathbb{F})$

Table 1

The Sylvester matrix of order 8 is not cocyclic over the quaternion group Q_8. This accounts for the sole disparity between columns r'' and s' of Table 1, and it is the only example that we discovered of a regular subgroup of $\mathrm{AGL}(k, \mathbb{F})$ not isomorphic to an indexing group of $D_{p,m,k}$. Comparing columns r' and s' in subsequent rows reveals greater disparity between the number of extension groups of $D_{2,1,k}$ and the number of regular subgroups of $\mathrm{AGL}(k+1, \mathbb{F})$.

For a regular subgroup $G \leq \mathrm{AGL}(k, \mathbb{F})$ to be an indexing group of $D_{p,m,k}$, there should exist a regular extension $E \leq \mathrm{AGL}(k+1, \mathbb{F})$ of V_1 by G with E and G satisfying extra conditions such as those in Lemma 4.5 (i) and Lemma 4.7. The question of precisely when G extends to E could be settled by investigating the cocycles $\psi : G \times G \to V_1$ of $D_{p,m,k}$.

In conclusion, we note that the exponent bounds in Proposition 4.8 are met for all values of (p, k) covered by Table 1.

Acknowledgments

R. Egan was supported by the Irish Research Council (Government of Ireland Postgraduate Scholarship) and National University of Ireland, Galway (Hardiman Fellowship).

References

[1] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997), 235–265.

[2] W. de Launey and D. L. Flannery, *Algebraic design theory*, Math. Surveys Monogr., vol. 175, American Mathematical Society, Providence, RI (2011).

[3] W. de Launey and R. M. Stafford, On cocyclic weighing matrices and the regular group actions of certain Paley matrices, Discrete Appl. Math. 102 (2000), 63–101.

[4] W. de Launey and R. M. Stafford, On the automorphisms of Paley's type II Hadamard matrix, Discrete Math. 308, no. 13 (2008), 2910–2924.

[5] W. de Launey and R. M. Stafford, The regular subgroups of the Paley type II Hadamard matrix, preprint.

[6] J. F. Dillon, Some REALLY beautiful Hadamard matrices, Cryptogr. Commun. 2, no. 2 (2010), 271–292.

[7] D. A. Drake, Partial λ-geometries and generalized Hadamard matrices over groups, Canad. J. Math. 31, no. 3 (1979), 617–627.

[8] R. Egan, *Topics in cocyclic development of pairwise combinatorial designs*, PhD thesis, National University of Ireland, Galway (2015).

[9] R. Egan, D. L. Flannery, and P. Ó Catháin, Classifying cocyclic Butson Hadamard matrices, *Algebraic Design Theory and Hadamard Matrices*, Springer Proceedings in Mathematics & Statistics 133 (2015), 93–106.

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

[11] N. Ito, On Hadamard groups, J. Algebra 168 (1994), 981–987.

[12] W. M. Kantor, Symplectic groups, symmetric designs and line ovals, J. Algebra 33 (1975), 43–58.

[13] M. W. Liebeck, C. E. Praeger, and J. Saxl, *Regular subgroups of primitive permutation groups*, Mem. Amer. Math. Soc. 203, no. 952 (2010).

[14] P. Ó Catháin and M. Röder, The cocyclic Hadamard matrices of order less than 40, Des. Codes Cryptogr. 58, no. 1 (2011), 73–88.

[15] D. A. Suprunenko, *Matrix groups*, Transl. Math. Monogr., vol. 45, American Mathematical Society, Providence, RI (1976).