A System of Equations for Describing Cocyclic Hadamard Matrices

V. Álvarez, J. A. Armario, M. D. Frau, P. Real
Dpto. Matemática Aplicada I, Universidad de Sevilla, Avda. Reina Mercedes s/n 41012 Sevilla, Spain, E-mail: valvarez@us.es; armario@us.es; mdfrau@us.es; real@us.es

Abstract: Given a basis $\mathcal{B} = \{f_1, \ldots, f_k\}$ for 2-cocycles $f : G \times G \to \{\pm 1\}$ over a group G of order $|G| = 4t$, we describe a nonlinear system of $4t - 1$ equations and k indeterminates x_i over $\mathbb{Z}_2, 1 \leq i \leq k$, whose solutions determine the whole set of cocyclic Hadamard matrices over G, in

the sense that $(x_1, \ldots, x_k)$ is a solution of the system if and only if the 2-cocycle $f = f_1^{x_1} \cdots f_k^{x_k}$ gives rise to a cocyclic Hadamard matrix $M_f = (f(g_i, g_j))$. Furthermore, the study of any isolated equation of the system provides upper and lower bounds on the number of coboundary generators in $\mathcal{B}$ which have to be combined to form a cocyclic Hadamard matrix coming from a special class of cocycles. We include some results on the families of groups $\mathbb{Z}_2^2 \times \mathbb{Z}_t$ and D_{4t}. A deeper study of the system provides some more nice properties. For instance, in the case of dihedral groups D_{4t}, we have found that it suffices to check t instead of the $4t$ rows of M_f, to decide the Hadamard character of the matrix (for a special class of cocycles f).

Keywords: *Hadamard matrix; cocyclic matrix; coboundary matrix*

1. INTRODUCTION

The Hadamard conjecture about the existence of Hadamard matrices $H = (h_{ij})$ (such that $H \cdot H^T = 4t \cdot I$) in all orders $|H| = 4t$ has remained open for more than a century.

Finding out the whole set of Hadamard matrices of size $4t$ by exhaustion requires solving a nonlinear system of $\binom{4t}{2}$ equations (one for each different pair of rows) and $16t^2$ unknowns (the indeterminates h_{ij}), which can be handled only for small values of t.

Checking whether a single matrix is Hadamard is an easier task. Let $M = (m_{ij})$ be a square matrix of size $4t$ over $\{\pm 1\}$. Determining if M is Hadamard

consists of checking whether the rows of M are pairwise orthogonal. This requires $O(t^3)$ operations.

A more economical test is achieved if the matrix M is known to be *cocyclic*, that is, whenever a group G of order $|G| = 4t$ and a 2-cocycle $f : G \times G \to \{\pm 1\}$ exist such that $M = (f(g_i, g_j))$. The *cocyclic test* [12] asserts that a cocyclic matrix M is Hadamard if and only if the summation of each row but the first is zero. This requires $O(t^2)$ operations.

Cocyclic Hadamard matrices have been shown to exist in all orders $4t$ up to $t \leq 46$ [16]. Furthermore, groups such as $\mathbb{Z}_t \times \mathbb{Z}_2^2$ or dihedral groups D_{4t} seem to provide many cocyclic Hadamard matrices [1,2,5,10,14], so that a cocyclic Hadamard conjecture arises in turn [15].

Three different methods have been proposed in order to calculate a full basis $\mathcal{B}$ for 2-cocycles over a group G, from which an exhaustive search for cocyclic Hadamard matrices may be performed. The first one applies to abelian groups and was described in [11,12]. The second one takes advantage of the inflation and transgression maps and was settled in [13] for those groups for which the word problem is solvable. The third one applies to groups for which a homological model is known [6–8], and has been implemented in *Mathematica* [3,4]. The theoretical background is explained in [5].

Unfortunately an exhaustive search for cocyclic Hadamard matrices is only feasible for orders up to $4t \leq 28$. In spite of this fact, some alternate methods have been designed in order to provide a few cocyclic Hadamard matrices for groups of higher order, in terms of image restorations [9] and genetic algorithms [2]. But once again the size allowed for these matrices is limited (up to $4t \leq 68$), since these methods are not practical for groups of higher orders.

We intend to provide here a new insight in the subject, in terms of a nonlinear system describing the whole set of cocyclic Hadamard matrices over a group G. The study of any isolated equation of the system provides upper and lower bounds on the number of coboundary generators in $\mathcal{B}$ which have to be combined to form a cocyclic Hadamard matrix coming from a special class of cocycles (see Propositions 5 and 10). This is one of the main achievements in the article. Consequently, the search space for cocyclic Hadamard matrices might reduce in turn, though it would possibly remain exponentially sized (e.g., for the groups $\mathbb{Z}_2^2 \times \mathbb{Z}_t$ and D_{4t}, see Remarks 4 and 5 below).

A deeper study of the system may provide some more nice properties. For instance, in the case of the dihedral group family D_{4t}, we have found that for a special class of cocycles f, it suffices to check $t - 1$ instead of the $4t$ rows of the cocyclic matrix M_f, to decide the Hadamard character of the matrix (see Theorem 2). Even though this could presumably have an effect on the computational aspect, unfortunately this is not that significant, since the cocyclic test still requires $O(t^2)$ operations. Nevertheless, the authors have taken advantage of this fact in [2], where an improved version of a genetic algorithm looking for cocyclic Hadamard matrices over dihedral groups has provided some matrices at orders that could not be reached from the general version of the genetic algorithm. However, it is beyond all doubt that the main restriction on computer searches for cocyclic Hadamard matrices is that the search space is exponential in size, so that the reduction in the number of rows which must be checked in order to guarantee that a matrix is a cocyclic Hadamard matrix, reveals to be a minor point.

We organize the article as follows. Section 2 is devoted to describing the nonlinear system characterizing the whole set of cocyclic Hadamard matrices over G, in terms of a basis $\mathcal{B}$ for 2-cocycles over G. In section 3, every equation of the system is shown to provide upper and lower bounds on the number of generators in $\mathcal{B}$ which must be combined in order to

get a cocyclic Hadamard matrix. Section 4 is devoted to analyzing the case of the abelian groups $\mathbb{Z}_t \times \mathbb{Z}_2^2$. Section 5 is devoted to analyzing the case of dihedral groups D_{4t}. There is a last section for final comments.

2. A SYSTEM OF EQUATIONS CHARACTERIZING COCYCLIC HADAMARD MATRICES

Let $G = \{g_1 = 1, g_2, \ldots, g_{4t}\}$ be a finite group of order $4t$ and $\mathcal{B} = \{f_1, \ldots, f_k\}$ be a basis for normalized 2-cocycles over G. The term *normalized* refers to a cocyclic matrix $M_f = (f(g_i, g_j))$ with the first row and column all of 1s, formed from a normalized 2-cocycle f, so that $f(1, g_j) = f(g_i, 1) = 1$ for all $g_i, g_j \in G$.

We describe here a system of $4t$ equations and k unknowns, whose solutions are precisely the whole set of normalized cocyclic Hadamard matrices over G. In the sequel, every 2-cocycle or cocyclic matrix is understood to be normalized.

In these circumstances, every 2-cocycle over G admits a unique representation as a product of the generators in $\mathcal{B}$, $f = f_1^{\alpha_1} \cdots f_k^{\alpha_k}, \alpha_i \in \{0, 1\}$. The tuple $(\alpha_1, \ldots, \alpha_k)_{\mathcal{B}}$ defines the coordinates of f with regards to $\mathcal{B}$. Accordingly, every cocyclic matrix $M_f = (f(g_i, g_j))$ for $f = (\alpha_1, \ldots, \alpha_k)_{\mathcal{B}}$ admits a unique decomposition as the Hadamard (pointwise) product $M_f = M_{f_1}^{\alpha_1} \cdots M_{f_k}^{\alpha_k}$.

A row is said to be Hadamard if its summation is zero. Thus the Hadamard matrices are precisely those matrices which are built up from Hadamard rows.

Let m_{ij}^d denote the (i, j) entry of M_{f_d}. Consequently, the (i, j) entry of M_f is $(m_{ij}^1)^{\alpha_1} \cdots (m_{ij}^k)^{\alpha_k}$. In these circumstances, the ith row of M_f is Hadamard if and only if the equation $\sum_{j=1}^{4t} (m_{ij}^1)^{\alpha_1} \cdots (m_{ij}^k)^{\alpha_k} = 0$ is satisfied. Moreover

Theorem 1. *The matrix M_f is Hadamard if and only if the vector of coordinates $(\alpha_1, \ldots, \alpha_k)_{\mathcal{B}}$ of f with regards to $\mathcal{B}$ satisfies*

$$\begin{cases} (m_{2,1}^1)^{\alpha_1} \cdots (m_{2,1}^k)^{\alpha_k} + \ldots + (m_{2,4t}^1)^{\alpha_1} \cdots (m_{2,4t}^k)^{\alpha_k} = 0 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ (m_{4t,1}^1)^{\alpha_1} \cdots (m_{4t,1}^k)^{\alpha_k} + \ldots + (m_{4t,4t}^1)^{\alpha_1} \cdots (m_{4t,4t}^k)^{\alpha_k} = 0 \end{cases} \tag{1}$$

Trying to solve this system may be as complicated as performing an exhaustive search for cocyclic Hadamard matrices.

In spite of this fact, studying how to solve an isolated equation of the preceding system, leads to the establishment of upper and lower bounds on the number of cocycles in $\mathcal{B}$ to use in order to get a cocyclic Hadamard matrix. Section 3 is devoted to explaining this fact.

As a straightforward consequence, the search space for cocyclic Hadamard matrices reduces in turn. The cases of the groups $\mathbb{Z}_t \times \mathbb{Z}_2^2$ and D_{4t} will be detailed in Sections 4 and 5, respectively.

3. DETERMINING UPPER AND LOWER BOUNDS

In order to determine upper and lower bounds for the number of generators in $\mathcal{B}$ to combine so that a Hadamard matrix is formed, we need to introduce some notations and definitions.

Every *elementary coboundary* ∂_d is constructed from the characteristic set map $\delta_d : G \to \{\pm 1\}$ associated to an element $g_d \in G$, so that

$$\partial_d(g_i, g_j) = \delta_d(g_i)\delta_d(g_j)\delta_d(g_i g_j) \quad \text{for} \quad \delta_d(g_i) = \begin{cases} -1 & g_d = g_i, \\ 1 & g_d \neq g_i. \end{cases} \tag{2}$$

Although the elementary coboundaries generate the set of all coboundaries, they might not be linearly independent (see [5] for instance).

Since the elementary coboundary ∂_{g_1} related to the identity element in G is not normalized, we may assume that $\partial_{g_1} \notin \mathcal{B}$.

Lemma 1. *Assume $d \neq 1$. Then every row $s \neq 1, d$ in M_{∂_d} contains precisely two -1s, which are located at the positions (s, d) and (s, e), for $g_e = g_s^{-1} g_d$. Furthermore, the first row is always formed by 1s, while the dth row is formed all by -1s, excepting the positions $(d, 1)$ and (d, d).*

Proof. The proof follows from particularizing (2) to the normalized cocycle ∂_d. □

Remark 1. *Notice that the dth row of M_{∂_d} uniquely determines g_d, and vice versa.*

Definition 1. *The dth-generalized coboundary matrix results from negating the dth row of M_{∂_d}. It will also be denoted M_{∂_d}.*

We will use generalized coboundary matrices instead of classical coboundary matrices. Since a row is Hadamard if and only if its summation is 0, the negation of a row does not modify the Hadamard character of the row. This way, every row but the first is assumed to contain precisely two -1 entries, which are located at the positions (s, d) and (s, e), for $g_e = g_s^{-1} g_d$.

The number of negative entries that a set of generalized coboundary matrices share will be relevant in the sequel. For this reason, it is important to know the way in which a negative entry may be shared. The lemmas below help in this task.

Lemma 2. *No more than two generalized coboundary matrices could share a negative entry at the same position.*

Proof. As we showed before, every generalized coboundary matrix M_{∂_d} contains two negative entries at the sth row, $2 \leq s \leq 4t$, located at the positions (s, d) and (s, e), for $g_e = g_s^{-1} g_d$.

Fix a generalized coboundary matrix M_{∂_d}. Let $M_{\partial_f} \neq M_{\partial_d}$ be another generalized coboundary matrix which shares a negative entry with M_{∂_d} at the sth row. There are only two possibilities:

- The shared position is (s, d).
  Since $f \neq d$, it follows that $g_d = g_s^{-1} g_f$.
- The shared position is (s, e), for $g_e = g_s^{-1} g_d$.
  Since $g_s^{-1} g_f = g_s^{-1} g_d$ implies $f = d$ and we know that $f \neq d$, it follows that $f = e$.

From these data, it is readily checked that if a generalized coboundary matrix M_{∂_h} shares the same negative entry at the sth row with M_{∂_d} and M_{∂_f}, then either $h = d$ or $h = f$ necessarily. □

Lemma 3. *If two generalized coboundary matrices share their two negative entries at the sth row, then* $g_s^2 = 1$. *Furthermore, in these circumstances the set of generalized coboundary matrices* $\{M_{\partial_i} : i \neq 1, s\}$ *admits a partition into pairs, so that coboundary matrices belonging to the same pair share the same two negative entries at the sth row.*

Proof. Assume $f \neq d$. Let M_{∂_d} and M_{∂_f} be two generalized coboundary matrices sharing their two negative entries at the sth row. From Lemma 2 we know that $g_d = g_s^{-1} g_f$ and $g_f = g_s^{-1} g_d$, so that $g_d = g_s^{-1} g_s^{-1} g_d$ and consequently $g_s^2 = 1$.

Now assume $g_s^2 = 1$. It is readily checked that for every $d \neq 1$, the generalized coboundary matrices M_{∂_d} and M_{∂_f} share the two negative entries at the sth row, for $g_f = g_s^{-1} g_d$, so that the set of generalized coboundary matrices may be partitioned into pairs, sharing their negative entries at the sth row. □

Remark 2. *Assume G is the dihedral group* D_{4t}. *The lemma above applies to rows s in the range* $2t + 1 \leq s \leq 4t$ (*see Proposition* 8 *below*). *Assume now that G is the direct product* $\mathbb{Z}_t \times \mathbb{Z}_2^2$. *Then Lemma* 3 *applies to the second, third, and fourth rows. In other words, under the chosen indexing of the rows, the rows stated correspond to the involutions in each of the groups.*

Definition 2. *A set* $\{M_{\partial_{i_j}} : 1 \leq j \leq w\}$ *of generalized coboundary matrices defines a n-walk if these matrices may be ordered in a sequence* $(M_{l_1}, \ldots, M_{l_w})$ *so that consecutive matrices share at least one negative entry at the n th row. Such a walk is called a path if the initial (equivalently, the final) matrix share a* -1 *entry with a generalized coboundary matrix which is not in the walk itself, and a cycle otherwise. This notion may be easily extended to any set of matrices* (*not necessarily coboundary ones*).

Remark 3. *In Graph Theory, a walk is an ordered sequence of vertices so that every vertex is adjacent to the preceding one. If a walk does not repeat any vertex, the walk is termed either cycle or path, depending on whether the final vertex is adjacent to the initial one. We adopt the same terminology in our article. Consequently, if we do not know whether the initial and final matrices of an ordered sequence are 'adjacent' or not, we will use the term walk, which includes both of the path and cycle possibilities. This explains the terminology which will be used in Proposition* 8.

The ordered sequence $(M_{l_1}, \ldots, M_{l_w})$ is uniquely determined by the given set of generalized coboundary matrices (up to cycling or reversion, depending on whether the walk is a cycle or a path), since from Lemma 2 no more than two generalized coboundary matrices share a common -1 entry at the same position. Thus choosing any M_i as starting point, the way in which the walk is expanded at each of the sides of M_i is uniquely determined, and hence the ordered sequence $(M_{l_1}, \ldots, M_{l_w})$ itself. Consequently, every set of generalized coboundary matrices may be partitioned in disjoint subsets, each of them defining *maximal* n-walks. Here the term maximal refers to a n-walk which cannot be extended to a longer n-walk. Accordingly every n-path contributes exactly two negative entries to the nth row of the product of the corresponding generalized coboundary matrices, whereas every n-cycle does not contribute any negative entry at all.

Counting the number of maximal n-paths in a given set of generalized coboundaries leads to a translation of the cocyclic Hadamard test for the nth row, as the proposition below indicates. More concretely, let $M = M_{\partial_{i_1}} \ldots M_{\partial_{i_w}} \cdot R$ be a decomposition of a cocyclic matrix, in terms of some generalized coboundary matrices $M_{\partial_{i_j}}$ and a matrix R formed from representative cocycles (coming from inflation and transgression). We may now re-write

the $(n-1)$th equation of Theorem 1 for testing whether the nth row is Hadamard, in terms of the number c of maximal n-paths in $\{M_{\partial_{i_1}}, \ldots, M_{\partial_{i_w}}\}$, the number r of -1s in the nth row of R and the number I of positions in which R and $M_{\partial_{i_1}} \ldots M_{\partial_{i_w}}$ share a common -1 in their nth row (obviously, $0 \leq I \leq r$).

Proposition 1. *In the circumstances above, the nth row of M is Hadamard if and only if* $2c + r - 2I = 2t$.

Corollary 1. $\left\lceil \frac{2t-r}{2} \right\rceil \leq c \leq \left\lfloor \frac{2t+r}{2} \right\rfloor$.

Proof. For a given value of r, the smallest value for c in the equation $2c + r - 2I = 2t$ occurs precisely when $I = 0$, so that $\left\lceil \frac{2t-r}{2} \right\rceil \leq c$.

Analogously the biggest value for c in the equation $2c + r - 2I = 2t$ occurs precisely when $I = r$, so that $c \leq \left\lfloor \frac{2t+r}{2} \right\rfloor$. □

These general bounds may be tightened depending on the group G. We study the cases of $\mathbb{Z}_t \times \mathbb{Z}_2^2$ and D_{4t} in the sections below. In the sequel, $[n]_m$ denotes $n \bmod m$ for short. We use $A \otimes B$ for denoting the usual Kronecker product of matrices, that is, the block matrix whose blocks are $a_{ij}B$.

4. THE $\mathbb{Z}_t \times \mathbb{Z}_2^2$ CASE

Consider the group $G = \mathbb{Z}_t \times \mathbb{Z}_2^2$, $t > 1$ odd, with ordering

$$G = \{(0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), \ldots, (t,1,1)\},$$

indexed as $\{1, \ldots, 4t\}$. A basis $\mathcal{B} = \{\partial_2, \ldots, \partial_{4t-2}, \beta_1, \beta_2, \gamma\}$ for 2-cocycles over G is described in [5], and consists of $4t-3$ coboundaries ∂_k, two cocycles β_i coming from inflation and one cocycle γ coming from transgression.

As usual, ∂_i refers to the coboundary associated to the ith element in G. The corresponding matrices M_{∂_i} are 4×4-block back diagonal square matrices of size $4t$, starting from the $\left\lceil \frac{i}{4} \right\rceil$th column:

$$M_{\partial_i} = \begin{array}{c} \scriptstyle \left\lceil \frac{i}{4} \right\rceil \\ \left(\begin{array}{cccc} & & A_{[i]_4} & \\ & \iddots & & \\ A_{[i]_4} & & & \\ & & & A_{[i]_4} \\ & & \iddots & \\ & A_{[i]_4} & & \end{array} \right) \end{array}.$$

These 4×4-blocks $A_{[i]_4}$ depend on the coset of i modulo 4, as follows:

$$A_0 = \begin{pmatrix} & & & - \\ & & - & \\ & - & & \\ - & & & \end{pmatrix} \; A_1 = \begin{pmatrix} - & & & \\ & - & & \\ & & - & \\ & & & - \end{pmatrix} \; A_2 = \begin{pmatrix} & - & & \\ - & & & \\ & & & - \\ & & - & \end{pmatrix} \; A_3 = \begin{pmatrix} & & - & \\ & & & - \\ - & & & \\ & - & & \end{pmatrix}.$$

Let BN_k denote the back negacyclic matrix of size $k \times k$,

$$BN_k = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & & \iddots & -1 \\ \vdots & \iddots & \iddots & \vdots \\ 1 & -1 & \cdots & -1 \end{pmatrix}_{k \times k}.$$

The cocyclic matrices coming from inflation may be described in terms of back negacyclic matrices, so that $M_{\beta_1} = 1_{2t} \otimes BN_2$ and $M_{\beta_2} = 1_t \otimes BN_2 \otimes 1_2$.

The transgression cocyclic matrix M_γ is $M_\gamma = 1_t \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix}$.

It has been observed that cocyclic Hadamard matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$ mostly use all the three representative cocycles β_1, β_2, and γ simultaneously (see [10] for details). We will assume that every cocyclic matrix M is obtained as a product $M = M_{\partial_{i_1}} \cdots M_{\partial_{i_w}} \cdot R$ for $R = 1_t \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix}$ and $2 \le i_1 < \cdots < i_w \le 4t-2$, where $R = M_{\beta_1} \cdot M_{\beta_2} \cdot M_\gamma$.

In order to get bounds on the number of elementary coboundaries to use so that a cocyclic Hadamard matrix may be formed, we need to know about s-paths in a set of generalized coboundaries $\{M_{\partial_{i_1}}, \ldots, M_{\partial_{i_w}}\}$, for every row s.

Proposition 2. *For every $1 \le i \le 4t$, $(M_{\partial_i}, M_{\partial_f})$ constitutes a s-walk, for $f = \big[4\big(1 + \lceil \frac{i}{4} \rceil - \lceil \frac{s}{4} \rceil\big) - \big[(-1)^s(i-1) - s\big]_4\big]_{4t}$.*

Proof. It may be checked by inspection, attending to the diagonal block form of the matrices M_{∂_i} and $A_{[i]_4}$ described above. □

We now focus on the case of nth rows, for $[n]_4 = 1$.

Let c be the number of maximal n-paths in $\{M_{\partial_{i_1}}, \ldots, M_{\partial_{i_w}}\}$, for $n = 4m+1$ and $1 \le m \le t-1$. Since R contains no negative entries at the nth row, we may re-write Proposition 1 as follows.

Proposition 3. *Assume $n = 4m+1$. In the circumstances above, the nth row of M is Hadamard if and only if $c = t$.*

Fix such an $n = 4m+1$. We now look for n-walks of coboundaries.

Proposition 4. *Every M_{∂_i} contributes two -1 in the nth row, which are located at positions (n, i) and $(n, [i-4m]_{4t}) = (n, [i-n+1]_{4t})$.*

Proof. It suffices to substitute $s = n = 4m+1$ in Lemma 1 or Proposition 2. □

Corollary 2. *For every $1 \leq i \leq 4t$, $\left(M_{\partial_{[i-n+1]_{4t}}}, M_{\partial_i}, M_{\partial_{[i+n-1]_{4t}}}\right)$ constitutes a n-walk.*

For instance, we can distinguish the following maximal 5-walks. In the sequel, we make use of parentheses for denoting 5-paths, whereas brackets refer to 5-cycles:

n	n-walks
5	$[M_{\partial_2}, M_{\partial_6}, \ldots, M_{\partial_{4t-2}}]$, $(M_{\partial_3}, M_{\partial_7}, \ldots, M_{\partial_{4t-5}})$ $(M_{\partial_4}, M_{\partial_8}, \ldots, M_{\partial_{4t-4}})$, $(M_{\partial_5}, M_{\partial_9}, \ldots, M_{\partial_{4t-3}})$

For $n = 4m+1$, $m \geq 2$, each of these maximal 5-walks will eventually split into smaller n-walks, depending on the coset $[t]_m$. For example, if $n = 13$ and $t = 9$,

n	n-walks
13	$[M_{\partial_2}, M_{\partial_{14}}, M_{\partial_{26}}]$, $[M_{\partial_6}, M_{\partial_{18}}, M_{\partial_{30}}]$, $[M_{\partial_{10}}, M_{\partial_{22}}, M_{\partial_{34}}]$, $[M_{\partial_3}, M_{\partial_{15}}, M_{\partial_{27}}]$, $[M_{\partial_7}, M_{\partial_{19}}, M_{\partial_{31}}]$, $(M_{\partial_{11}}, M_{\partial_{23}})$, $[M_{\partial_4}, M_{\partial_{16}}, M_{\partial_{28}}]$, $[M_{\partial_8}, M_{\partial_{20}}, M_{\partial_{32}}]$, $(M_{\partial_{12}}, M_{\partial_{24}})$, $[M_{\partial_5}, M_{\partial_{17}}, M_{\partial_{29}}]$, $[M_{\partial_9}, M_{\partial_{21}}, M_{\partial_{33}}]$, $(M_{\partial_{13}}, M_{\partial_{25}})$

Proposition 5. *The number w of elementary coboundaries in B to combine in order to get a cocyclic Hadamard matrix over $\mathbb{Z}_t \times \mathbb{Z}_2^2$ of the type $M = M_{\partial_{i_1}} \cdots M_{\partial_{i_w}} \cdot R$ for $2 \leq i_1 < \cdots < i_w \leq 4t-2$ and $R = \beta_1 \cdot \beta_2 \cdot \gamma$, satisfies $t \leq w \leq 3t$, for $t > 1$ odd.*

Proof. Let M be a cocyclic matrix obtained as a product $M = M_{\partial_{i_1}} \cdots M_{\partial_{i_w}} \cdot R$ for $2 \leq i_1 < \cdots < i_w \leq 4t-2$ and $R = \beta_1 \cdot \beta_2 \cdot \gamma$.

We have just proved that a necessary condition for M in order to be a Hadamard matrix is that the number c of maximal n-paths in $\left\{M_{\partial_{i_1}}, \ldots, M_{\partial_{i_w}}\right\}$ must be exactly t.

On one hand, since every n-path consists of at least one coboundary, it follows that $t \leq w$.

On the other hand, since the basis for coboundaries splits into three maximal 5-paths (the other one is a 5-cycle), it is necessary to delete at least $t-3$ coboundaries from that basis. Consequently, $w \leq 4t-3-(t-3) = 3t$. □

Remark 4. *The full basis $\mathcal{B}$ for 2-cocycles over G consists of $4t$ generators. Hence the search space for cocyclic Hadamard matrices which use R consists of 2^{4t-3} matrices. Taking Proposition 5 into account, the search space reduces to $\sum_{w=t}^{3t} \binom{4t-3}{w}$ matrices. Unfortunately, the amount of cocyclic matrices is still exponential in size.*

The following table organizes the set of cocyclic Hadamard matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$ with regards to the number w of elementary coboundaries in $\mathcal{B}$ that are used in each case, for $t = 3, 5$. All these matrices use $R = \beta_1\beta_2\gamma$ (the same behavior been observed for all $t > 1$, though there is no proof of this fact). We also include the size of the total search space, $\text{tot}_t = 2^{4t-3}$, as well as the size of the reduced search space, $\text{red}_t = \sum_{w=t}^{3t} \binom{4t-3}{w}$. Calculations for $t \leq 50$ suggest that asymptotically $\text{tot}_t \simeq \text{red}_t$.

$t\backslash w$	3	4	5	6	7	8	9	10	11	12	13	14	total	tot_t	red_t
3	5	9	6	2	1	1							24	512	466
5				19	32	13	16	24	6	3	6	1	120	131072	127840

Thus, the bounds in Proposition 5 seem to be reasonably tight.

To conclude this example, we include some partial results about the Hadamard character of some rows, in terms of the cocycles involved.

Proposition 6. *The second, third, and fourth rows of any cocyclic matrix formed from R and any combination of coboundaries, are always Hadamard rows.*

Proof. From Remark 2, we know that the set of generalized coboundary matrices admits a partition into s-cycles, for $2 \leq s \leq 4$, since $g_s^2 = 1$. Moreover, from Lemma 1, it is clear that these s-cycles are of the type $\left[M_{\partial_{[1]_4}}, M_{\partial_{[2]_4}}\right]$ and $\left[M_{\partial_{[0]_4}}, M_{\partial_{[3]_4}}\right]$ for $s = 2$, $\left[M_{\partial_{[0]_4}}, M_{\partial_{[2]_4}}\right]$ and $\left[M_{\partial_{[1]_4}}, M_{\partial_{[3]_4}}\right]$ for $s = 3$, and $\left[M_{\partial_{[0]_4}}, M_{\partial_{[1]_4}}\right]$ and $\left[M_{\partial_{[2]_4}}, M_{\partial_{[3]_4}}\right]$ for $s = 4$. Consequently, any s-path, for $2 \leq s \leq 4$, shares exactly one -1 occurrence at the sth row with $R = 1_t \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix}$. Thus, the number $2t$ of -1 occurrences remains unchanged.

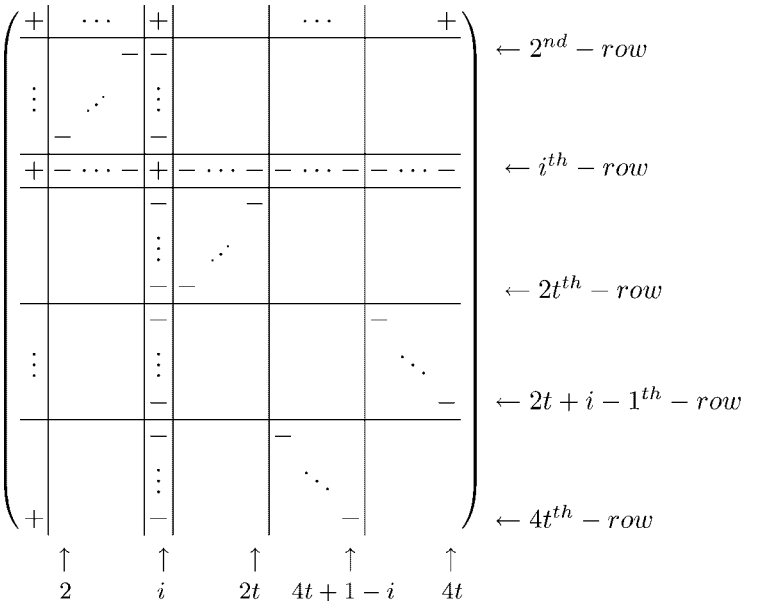
5. THE D_{4t} CASE

Let $H = D_{4t} = \mathbb{Z}_{2t} \rtimes_{\chi} \mathbb{Z}_2$, $\chi(1, a) = [-a]_{2t}$, $\chi(0, a) = a$, with ordering

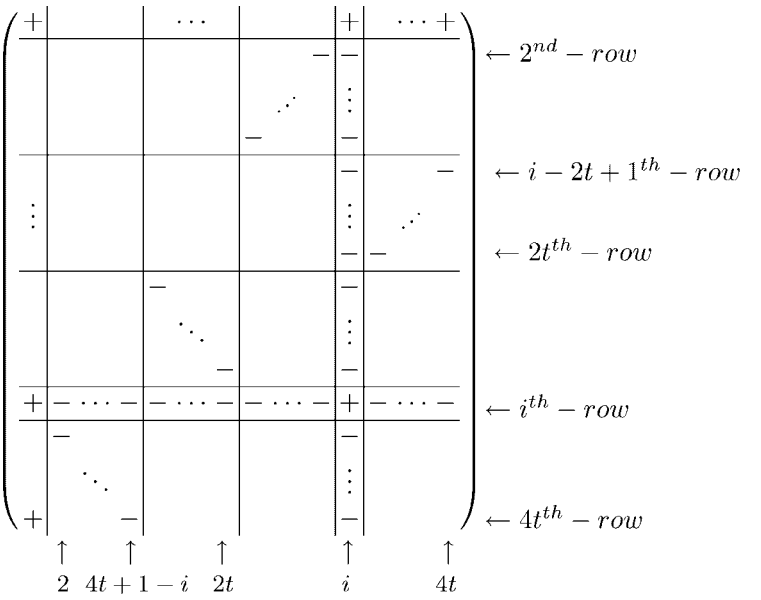
$$\{(0, 0), (0, 1), \ldots, (0, 2t-1), (1, 0), \ldots, (1, 2t-1)\},$$

indexed as $\{1, \ldots, 4t\}$. A basis $\mathcal{B}$ for 2-cocycles over H is described in [5]. For $t > 2$, the basis consists of $4t - 3$ coboundaries ∂_k, two cocycles β_i coming from inflation and one cocycle γ coming from transgression, so that $\mathcal{B} = \{\partial_2, \ldots, \partial_{4t-2}, \beta_1, \beta_2, \gamma\}$. In the sequel we assume $t > 2$.

For $2 \leq i \leq 2t$, the matrices M_{∂_i} have the form:



For $2t+1 \leq i \leq 4t-2$ the matrices M_{∂_i} have the form:



The cocyclic matrices coming from inflation are $M_{\beta_1} = 1_{2t} \otimes BN_2$ and $M_{\beta_2} = BN_2 \otimes 1_{2t}$.

The transgression cocyclic matrix M_γ is $M_\gamma = \begin{pmatrix} A & A \\ B & B \end{pmatrix}$ for

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & & \iddots & -1 \\ \vdots & \iddots & \iddots & \vdots \\ 1 & -1 & \cdots & -1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & -1 & \cdots & -1 \\ \vdots & \ddots & \ddots & \vdots \\ 1 & & \ddots & -1 \\ 1 & 1 & \cdots & 1 \end{pmatrix}. \tag{3}$$

It has been observed that cocyclic Hadamard matrices over D_{4t} mostly use $\beta_2 \cdot \gamma$ and do not use β_1 (see [2,14] for instance). In the sequel, we consider only cocyclic matrices $M = M_{\partial_{i_1}} \cdots M_{\partial_{i_w}} \cdot R$, for some generalized coboundary matrices such that $2 \leq i_1 < \cdots < i_w \leq 4t-2$ and $R = M_{\beta_2} \cdot M_\gamma = \begin{pmatrix} A & A \\ B & -B \end{pmatrix}$.

Consider the full set of elementary coboundaries, $\{\partial_1, \ldots, \partial_{4t}\}$. We now characterize the n-walks in this set, for $2 \leq n \leq 4t$.

Proposition 7. *For $1 \leq n \leq 2t$:*

- *For $1 \leq i \leq 2t$, $\left(M_{\partial_i}, M_{\partial_{2t-[n-1-i]_{2t}}}\right)$ constitutes a n-walk.*
- *For $2t+1 \leq i \leq 4t$, $\left(M_{\partial_i}, M_{\partial_{4t-[n-1+2t-i]_{2t}}}\right)$ constitutes a n-walk.*

Similarly, for $2t+1 \leq n \leq 4t$*:*

- *For* $1 \leq i \leq n-2t$, $\left[M_{\partial_i}, M_{\partial_{n+1-i}}\right]$ *constitutes a n-cycle.*
- *For* $n-2t+1 \leq i \leq 2t$, $\left[M_{\partial_i}, M_{\partial_{n+1+2t-i}}\right]$ *constitutes a n-cycle.*

Accordingly,

- *For* $1 \leq n \leq 2t$*, a maximal n-walk consists of a maximal subset in*

$$(M_{\partial_1}, \ldots, M_{\partial_{2t}}) \quad or \quad (M_{\partial_{2t+1}}, \ldots, M_{\partial_{4t}})$$

formed from matrices $(\ldots, M_i, M_j, \ldots)$ *which are cyclically separated in* $n-1$ *positions (i.e.,* $i \pm (n-1) \equiv j \bmod 2t$*).*
- *For* $2t+1 \leq n \leq 4t$*, a maximal n-path consists of just one* M_{∂_j}*, since matrices symmetrically displayed with regards to the double vertical lines in*

$$(M_{\partial_1}, \ldots, M_{\partial_{n-2t}} \| M_{\partial_{2t+1}}, \ldots, M_{\partial_n}) \text{ or } (M_{\partial_{n-2t+1}}, \ldots, M_{\partial_{2t}} \| M_{\partial_{n+1}}, \ldots, M_{\partial_{4t}})$$

give rise to n-cycles, of the form $[M_{\partial_{n-2t-k}}, M_{\partial_{2t+1+k}}]$*, for* $0 \leq k \leq n-2t-1$*, and* $[M_{\partial_{2t-h}}, M_{\partial_{n+1+h}}]$*, for* $0 \leq h \leq 4t-n-1$*.*

Proof. It is seen by inspection. □

Since the second row in R is the one with fewest negative entries (excepting the first row, of course!), we focus on this case. We now look for 2-walks of coboundaries in $\{\partial_2, \ldots, \partial_{4t-2}\}$.

Corollary 3. *We can distinguish the following maximal* 2*-cycles:*

n	*n-walks*
2	$[M_{\partial_1}, M_{\partial_2}, \ldots, M_{\partial_{2t}}]$, $[M_{\partial_{2t+1}}, M_{\partial_{2t+2}}, \ldots, M_{\partial_{4t}}]$

We now particularize Proposition 1 and Corollary 1 for $n = 2$.

Proposition 8. *The* 2*nd row of M is Hadamard if and only if* $2c + 2 - 2I = 2t$*.*

Recall that the value I above indicates the number of negative positions that R shares with $M_{\partial_{i_1}} \ldots M_{\partial_{i_w}}$ in their second row, and c denotes the number of maximal 2-paths in $\{M_{\partial_{i_1}}, \ldots, M_{\partial_{i_w}}\}$.

Corollary 4. $t-1 \leq c \leq t+1$.

Proof. Since the second row in R consists of two -1, the value I in Proposition 8 is in the range $0 \leq I \leq 2$, so that $2c-2 \leq 2t \leq 2c+2$ and the result follows. □

Proposition 9. *Provided that* $R = M_{\beta_2} M_\gamma$ *(i.e.,* β_1 *is not used), the number w of elementary coboundaries in* $\mathcal{B}$ *to combine in order to get a cocyclic Hadamard matrix over* D_{4t} *coming from the class of R satisfies* $t-1 \leq w \leq 3t$*.*

Proof. Let M be a cocyclic matrix obtained as a product $M = M_{\partial_{i_1}} \ldots M_{\partial_{i_w}} \cdot R$ for $2 \leq i_1 < \ldots < i_w \leq 4t-2$ and $R = M_{\beta_2} \cdot M_\gamma$.

We have just proved that a necessary condition for M in order to be a Hadamard matrix is that the number c of maximal 2-paths in $\{M_{\partial_{i_1}}, \ldots, M_{\partial_{i_w}}\}$ is in the range $t-1 \leq c \leq t+1$.

On one hand, since every 2-path consists of at least one coboundary matrix, it follows that $t-1 \leq w$.

On the other hand, since the basis for coboundary matrices splits into two maximal 2-paths, it is necessary to delete at least $t-3$ coboundary matrices from that basis. Consequently, $w \leq 4t-3-(t-3) = 3t$. □

Proposition 10. *In fact,* $t-1 \leq w \leq 3t-2$.

Proof. Attending to the positions at which the -1 of the second row in R are located, it follows that

$$(M_{\partial_2}, \ldots, M_{\partial_{2t}}, \gamma, M_{\partial_{2t+1}}, \ldots, M_{\partial_{4t-2}})$$

constitutes a maximal 2-path.

Furthermore, in these circumstances Proposition 8 implies that the list above must split into t disjoint 2-paths.

Consequently, the number w of coboundaries in $\mathcal{B}$ to combine in order to get a cocyclic matrix over D_{4t} coming from the class of R satisfies $w \geq t-1$ and $w \leq 4t-3-(t-1) = 3t-2$ (it is necessary to extract at least $t-1$ coboundaries from the list above). □

Remark 5. *The full basis $\mathcal{B}$ for 2-cocycles over H consists of $4t$ generators. Hence the search space for cocyclic Hadamard matrices which use R and do not use β_1 consists of 2^{4t-3} matrices. Taking Proposition 10 into account, the search space reduces to $\sum_{w=t-1}^{3t-2} \binom{4t-3}{w}$ matrices. Unfortunately, the amount of cocyclic matrices is still exponential in size.*

The following table organizes the set of cocyclic Hadamard matrices over $D_{4t}, t > 2$, that use $R = M_{\beta_2} M_\gamma$ and do not use β_1, with regards to the number w of elementary coboundaries in B that are used in each case. The third last column indicates the total number of cocyclic Hadamard matrices over D_{4t} for each t (those using R are included). We also include the size of the total search space, $\mathrm{tot}_t = 2^{4t-3}$, as well as the size of the reduced search space, $\mathrm{red}_t = \sum_{w=t-1}^{3t-2} \binom{4t-3}{w}$. Calculations for $t \leq 50$ suggest that asymptotically $\mathrm{tot}_t \simeq \mathrm{red}_t$.

$t\backslash w$	2	3	4	5	6	7	8	9	10	11	12	13	with R	total	tot_t	red_t
3	6	12	18	18	12	6							72	72	512	492
4		20	52	84	100	100	84	52	20				512	768	8192	8008
5			8	88	152	212	240	240	212	152	88	8	1400	2200	131072	129404

From these data, it is readily checked that the bounds in Proposition 10 are optimally tightened.

To conclude this example, we include some partial results about the Hadamard character of some rows, in terms of the cocycles involved.

Let $M = M_{\partial_{i_1}} \ldots M_{\partial_{i_w}} \cdot R$.

Proposition 11. *The rows from $2t+1$ to $4t$ in M are always Hadamard rows.*

Proof. On one hand, we know from (3) that the nth row in R, for $2t+1 \leq n \leq 4t$, contains precisely $2t$ negative entries, which are consecutively distributed from the $(n-2t+1)$th column to the nth column.

From Proposition 7, we know that the generalized coboundary matrices constructed from $\mathcal{B}$ give rise to n-cycles of length 2 of the form $[M_{\partial_{n-2t-k}}, M_{\partial_{2t+1+k}}]$, for $0 \leq k \leq n-2t-1$, and $[M_{\partial_{2t-h}}, M_{\partial_{n+1+h}}]$, for $0 \leq h \leq 4t-n-1$, depending on whether they are symmetrically displayed with regards to the double vertical lines in

$$(M_{\partial_1}, \ldots, M_{\partial_{n-2t}} \| M_{\partial_{2t+1}}, \ldots, M_{\partial_n}) \text{ or } (M_{\partial_{n-2t+1}}, \ldots, M_{\partial_{2t}} \| M_{\partial_{n+1}}, \ldots, M_{\partial_{4t}}).$$

In particular, notice that any two generalized coboundary matrices either share the same two negative entries at the nth row, or contribute four different negative entries at the nth row.

Furthermore, attending to the n-cycles above, the two negative entries in M_{∂_j} at the nth row correspond to negative and positive entries in R at the same row, so that the number $2t$ of negative entries remains unchanged. Hence the nth row is Hadamard. □

Proposition 12. *The $(t+1)$th row in M is Hadamard.*

Proof. The argument of the proof is similar to the preceding one.

From (3), it is clear that the $(t+1)$th row in R contains precisely $2t$ negative entries, which are distributed in two blocks of t consecutive -1, from the $(t+1)$th column to the $2t$th column, and from the $(3t+1)$th column to the $4t$th column.

Proposition 7 implies that the set of generalized coboundary matrices splits into a partition of $(t+1)$-cycles of length 2, of the type $[M_{\partial_i}, M_{\partial_{i+t}}]$ and $[M_{\partial_{2t+i}}, M_{\partial_{3t+i}}]$, for $1 \leq i \leq t$. Consequently, any two generalized coboundary matrices either share the same two negative entries at the $(t+1)$th row, or contribute four different negative entries at the $(t+1)$th row. What is more, the two negative entries in M_{∂_j} at the $(t+1)$th row correspond to negative and positive entries in R at the same row, so that the number $2t$ of negative entries remains unchanged. Hence the $(t+1)$th row is Hadamard. □

Proposition 13. *For $2 \leq n \leq t$, the nth row in M is Hadamard if and only if the $(2t+2-n)$th row is Hadamard as well.*

Proof. Notice that, for $2 \leq n \leq t$, the nth row of R is equal to the negation of the $(2t+2-n)$th row cyclically rotated to the left by $n-1$ positions.

Similarly, for $2 \leq n \leq t$, the nth row of the generalized coboundary matrix M_{∂_i} equals the $(2t+2-n)$th row cyclically rotated to the left by $n-1$ positions.

This way, for any cocyclic matrix $M = M_{\partial_{i_1}} \ldots M_{\partial_{i_w}} \cdot R$, the nth row in M is Hadamard if and only if the $(2t+2-n)$th row is Hadamard as well, $2 \leq n \leq t$. □

Theorem 2. *The matrix M is Hadamard if and only if rows from 2 to t are Hadamard.*

Proof. It suffices to collect Propositions 11 through 13. □

Thus, the cocyclic Hadamard test for such a matrix M runs four times faster than usual. The authors have taken advantage of this fact in [2], so that an adapted version of a genetic algorithm for looking for cocyclic Hadamard matrices has provided new cocyclic Hadamard matrices at dimensions $4t \leq 68$ where exhaustive computations could not be handled before (see Table 6.2 in [15], p. 132). It is a remarkable fact that the general (not adapted) version of the genetic algorithm did not give matrices at dimensions $44 \leq 4t \leq 68$ (see [2] for details).

6. FINAL COMMENTS

One could try to fix another basis group, different from $\mathbb{Z}_t \times \mathbb{Z}_2^2$ or D_{4t}. For practical computations, a basis group should be selected such that:

1. The number of elementary coboundaries involved in a cocyclic Hadamard matrix is bounded as tightly as possible (that would narrow down the search space of cocycles).
2. For a given cocyclic matrix, there are only a few rows whose sums must be checked in order to guarantee that the matrix is Hadamard (that would improve the checking time required for each cocycle).

Although both of the families of groups $\mathbb{Z}_t \times \mathbb{Z}_2^2$ and D_{4t} have a nice behavior with regards to point 1 (see Propositions 5 and 10), the checking process runs 4 times faster for dihedral groups than for $\mathbb{Z}_t \times \mathbb{Z}_2^2$ (see Theorem 2).

We hope that the analysis of n-walks and the correspondent equations in (1) over $\mathbb{Z}_t \times \mathbb{Z}_2^2$, D_{4t}, and other nice groups (see [5] for instance) will reveal more valuable information about cocyclic Hadamard matrices in the near future.

In particular, it would be interesting if something new (apart from the results explained here) could be said about the way in which coboundary matrices have to be combined in order to give rise to cocyclic Hadamard matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$ and D_{4t}.

ACKNOWLEDGMENTS

The authors want to express their gratitude to the referees for their many valuable advices and suggestions, which have led to a significant number of improvements of the article. We also are indebted to Prof. Kathy Horadam. Her articles about cocyclic matrices have inspired our research from the very beginning. Furthermore, we have had the opportunity of many interesting discussions with her over the last year, from which we obtained the strength and support required to develop (among other articles) this work. All authors are partially supported by the PAICYT research project FQM-296 from Junta de Andalucía (Spain).

REFERENCES

[1] V. Álvarez, J. A. Armario, M. D. Frau, and P. Real, An Algorithm for Computing Cocyclic Matrices Developed Over Some Semidirect Products, AAECC-14 Proceedings, LNCS 2227, S. Boztas and I. E. Shparlinski (Editors), Springer-Verlag, Berlin Heidelberg, 2001, pp. 287–296.

[2] V. Álvarez, J. A. Armario, M. D. Frau, and P. Real, A Genetic Algorithm for Cocyclic Hadamard Matrices, AAECC-16 Proceedings, LNCS 3857, M. Fossorier, H. Imai, and A. Poli (Editors), Springer Verlag, Berlin Heidelberg, 2006, pp. 144–153.

[3] V. Álvarez, J. A. Armario, M. D. Frau, and P. Real, Calculating Cocyclic Hadamard Matrices in Mathematica: Exhaustive and Heuristic Searches, ICMS-2 Proceedings, LNCS 4151, A. Iglesias and N. Takayama (Editors), Springer Verlag, Berlin Heidelberg, 2006, pp. 419–422.

[4] V. Álvarez, J. A. Armario, M. D. Frau, and P. Real, A Mathematica Notebook for Computing the Homology of Iterated Products of Groups, ICMS-2 Proceedings, LNCS 4151, A. Iglesias and N. Takayama (Editors), Springer Verlag, Berlin Heidelberg, 2006, pp. 47–57.

[5] V. Álvarez, J. A. Armario, M. D. Frau, and P. Real, The homological reduction method for computing cocyclic Hadamard matrices, J Symb Comput (to appear).

[6] V. Álvarez, J. A. Armario, M. D. Frau, and P. Real, Comparison Maps for Relatively Free Resolutions, CASC-06 Proceedings, LNCS 4194, V. G. Ganzha, E. W. Mayr, and E. V. Vorozhtsov (Editors), Springer Verlag, Berlin Heidelberg, 2006, pp. 1–22.

[7] V. Álvarez, J. A. Armario, M. D. Frau, and P. Real, Algebra structures on the twisted Eilenberg–Zilber theorem, Commun Algebra 35 (2007), 3273–3291.

[8] V. Álvarez, J. A. Armario, M. D. Frau, and P. Real, (Co)homology of iterated semidirect products of abelian groups, preprint, 2006.

[9] A. Baliga and J. Chua, Self-Dual Codes Using Image Resoration Techniques, AAECC-14 Proceedings, LNCS 2227, S. Boztas and I. E. Shparlinski (Editors), Springer-Verlag, Berlin Heidelberg, 2001, pp. 46–56.

[10] A. Baliga and K. J. Horadam, Cocyclic Hadamard matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$, Australas, J Combin 11 (1995), 123–134.

[11] K. J. Horadam and W. de Launey, Cocyclic development of designs, J Algebraic Combin 2(3) (1993), 267–290. Erratum: J Algebraic Combin 3 (1994), 129.

[12] K. J. Horadam and W. de Launey, Generation of cocyclic Hadamard matrices, Math Appl 325 (1995), 279–290.

[13] D. L. Flannery, Calculation of cocyclic matrices, J Pure Appl Algebra 112 (1996), 181–190.

[14] D. L. Flannery, Cocyclic Hadamard matrices and Hadamard groups are equivalent, J Algebra 192 (1997), 749–779.

[15] K. J. Horadam, Hadamard Matrices and Their Applications, Princeton University Press, Princeton, New Jersey, 2007.

[16] N. Ito, On Hadamard groups IV, J Algebra 234 (2000), 651–663.