On $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices

Víctor Álvarez, Félix Gudiel, and María Belén Güemes

December 20, 2011

Abstract

A characterization of $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices is described, depending on the notions of distributions, ingredients and recipes. In particular, these notions lead to the establishment of some bounds on the number and distribution of 2-coboundaries over $\mathbb{Z}_t \times \mathbb{Z}_2^2$ to use and the way in which they have to be combined in order to obtain a $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrix. Exhaustive searches have been performed, so that the table in p. 132 in [4] is corrected and completed. A deeper look at the results obtained leads to the definition of some transformations which preserve the $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard character of a matrix, and which give rise to orbits of $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices. This will be explained in a subsequent paper [3], due to space limitations.

1 Introduction

Hadamard matrices are $n \times n$ square matrices $H$ with entries in $\{1, -1\}$ such that every pair of rows (respectively, columns) are orthogonal, that is, $HH^T = nI_n$.

Due to this nice combinatorial property, Hadamard matrices have many applications in a wide variety of fields, such as Signal Processing, Coding Theory and Cryptography (see [6] for details). Consequently, there is a real interest in knowing enough Hadamard matrices for practical use.

It is a straightforward exercise to prove that the order of a Hadamard matrix has to be 1, 2 or a multiple of 4 (as soon as three or more rows have to be simultaneously orthogonal one to each other). Unfortunately, the Hadamard Conjecture about the existence of these matrices for every order $4t$ remains unproved since the XIXth Century.

Nowadays, there are three orders less than 1000 for which no Hadamard matrix is known: $668 = 4 \cdot 167$, $716 = 4 \cdot 179$, and $892 = 4 \cdot 223$. Furthermore,
there are 10 orders in the range \([1000, 2000]\) for which no Hadamard matrix is known (see \[9\] for details).

One of the most promising techniques for constructing Hadamard matrices is the cocyclic approach (see \[7, 8\]). A cocyclic matrix \(M_f\) over a group \(G\) is a matrix \(M_f = (f(g, h))\), for \(f\) being a 2-cocycle over \(G\), that is, a function \(f : G \times G \to \{1, -1\}\) such that for every \(a, b, c \in G\),
\[
f(a, b) \cdot f(ab, c) \cdot f(a, bc) \cdot f(b, c) = 1.
\]

Actually, many well known families of Hadamard matrices, such as Sylvester’s, Paley’s, Williamson’s and Ito’s, have shown to be cocyclic over appropriated groups (see \[6\] for details). This has provided inspiration for the Cocyclic Hadamard Conjecture, which states that cocyclic Hadamard matrices exist for every order \(4t\).

In this paper we are interested in characterizing cocyclic Hadamard matrices over \(\mathbb{Z}_t \times \mathbb{Z}_2^2\), which include the family of symmetric Williamson Hadamard matrices.

Following the indications of \[1\], we will describe bounds on the number of 2-coboundaries over \(\mathbb{Z}_t \times \mathbb{Z}_2^2\) to be combined, as well as their distribution (in terms of what we call ingredients and recipes), in order to construct a \(\mathbb{Z}_t \times \mathbb{Z}_2^2\)-cocyclic Hadamard matrix. A preliminary version of this work can be found in \[5\].

This information will allow us to design an exhaustive search for \(\mathbb{Z}_t \times \mathbb{Z}_2^2\)-cocyclic Hadamard matrices for \(3 \leq t \leq 13\), so that the table in p. 132 in \[4\] is corrected and completed.

Taking a deeper insight on the results obtained, some relations seem to play an special role among \(\mathbb{Z}_t \times \mathbb{Z}_2^2\)-cocyclic Hadamard matrices. These observations have lead to ask some questions, which will be analyzed in a subsequent paper \[3\], due to space limitations. In particular, in the second series of these papers we will define four different transformations on \(\mathbb{Z}_t \times \mathbb{Z}_2^2\)-cocyclic Hadamard matrices which are Hadamard-preserving, so that the set of \(\mathbb{Z}_t \times \mathbb{Z}_2^2\)-cocyclic Hadamard matrices splits in orbits. Furthermore, the knowledge of just one \(\mathbb{Z}_t \times \mathbb{Z}_2^2\)-matrix completely characterizes its corresponding orbit. With this information at hand, we have been able to extend the table in p. 132 in \[4\] for values of \(t\) in the range \(3 \leq t \leq 23\).

We organize the paper as follows. Section II is dedicated to describe all about \(\mathbb{Z}_t \times \mathbb{Z}_2^2\)-cocyclic Hadamard matrices, as it is described in \[4\] and \[1\]. In Section III, we introduce the notions of distribution, ingredients and recipes, in terms of which we find some upper and lower bounds on the number of 2-coboundaries over \(\mathbb{Z}_t \times \mathbb{Z}_2^2\) which have to be combined in order to get \(\mathbb{Z}_t \times \mathbb{Z}_2^2\)-cocyclic Hadamard matrices, as well as the way in which they have to be distributed. Section IV is devoted to calculations. Last section is dedicated to conclusions and further work.
2 $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices

Consider the group $G = \mathbb{Z}_t \times \mathbb{Z}_2^2 = \langle x, u, v : x^t = u^2 = v^2 = 1, uv = vu \rangle$, $t > 1$ odd, with ordering

$$(x^i, 1) < (x^i, u) < (x^i, v) < (x^i, uv), \ 0 \leq i < t,$$

$$(x^i, uv) < (x^{i+1}, 1), \ 0 \leq i < t - 1.$$

A basis $B = \{\partial_2, \ldots, \partial_{4t-2}, \beta_1, \beta_2, \gamma\}$ for $2$-cocycles over $G$ is described in [2], and consists of $4t-3$ coboundaries $\partial$, two cocycles $\beta_i$ coming from inflation and one cocycle $\gamma$ coming from transgression.

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

Let $BN_k$ denote the back negacyclic matrix of size $k \times k$, $BN_k = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \ddots & \ddots & \ddots \\ \vdots & \ddots & \ddots & \ddots \\ 1 & -1 & \cdots & -1 \end{pmatrix}_{k \times k}$.

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 $M_{\beta_2} = 1_{t} \otimes BN_2 \otimes 1_2$. Here we use $A \otimes B$ for denoting the usual Kronecker product of matrices, that is, the block matrix whose blocks are $a_{ij}B$.

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

It has been observed that cocyclic Hadamard matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$ mostly use all the three representative cocycles $\beta_1, \beta_2$ and $\gamma$ simultaneously (see [4] for details). We will assume that every cocyclic matrix $M$ is obtained as a product

$M = M_{\beta_{i_1}} \cdots M_{\beta_{i_w}} \cdot R$ for $R = 1_t \otimes \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & -1 & -1 \\ 1 & 1 & -1 \end{pmatrix}$ and $2 \leq i_1 < \ldots < i_w \leq 4t - 2$, where $R = M_{\beta_1} \cdot M_{\beta_2} \cdot M_\gamma$.

As usual, $\partial_i$ refers to the coboundary associated to the $i^{th}$-element in $G$. The corresponding matrices $M_{\partial_i}$ are $4 \times 4$-block back diagonal square matrices of size $4t$, starting from the $[4]^{th}$-column:
\[
M_{\partial_t} = \begin{pmatrix}
   & A_{[i]_4} & \\
   A_{[i]_4} & \ddots & A_{[i]_4} \\
   & \ddots & A_{[i]_4}
\end{pmatrix}
\]

with the \(i^{th}\)-row and the \(i^{th}\)-column negated. Here we adopt the notation \(|m|_n\) instead of \(m \mod n\) for brevity.

The \(4 \times 4\)-blocks \(A_{[i]_4}\) depend on the coset of \(i\) modulo 4, as follows:

\[
A_0 = \begin{pmatrix}
   - & - & - & - \\
   - & - & - & -
\end{pmatrix},
\quad
A_1 = \begin{pmatrix}
   - & - & - & - \\
   - & - & - & -
\end{pmatrix},
\quad
A_2 = \begin{pmatrix}
   - & - & - & - \\
   - & - & - & -
\end{pmatrix},
\quad
A_3 = \begin{pmatrix}
   - & - & - & - \\
   - & - & - & -
\end{pmatrix}.
\]

Negating the \(i^{th}\)-row gives a matrix with exactly two negative entries in each row, excepting the first one (consisting only of 1s). More concretely, the coboundary matrices \(\partial g\) may be expressed as linear combinations of elements in \(B\): \(M_{\partial_1}, M_{\partial_{4t-1}}\) and \(M_{\partial_t}\). It may be checked that:

\[
M_{\partial_t} = -\prod_{i=1}^{t-1} M_{\partial_{4i+1}} \prod_{i=0}^{t-1} M_{\partial_{4i+2}}.
\]

\[
M_{\partial_{4t-1}} = \prod_{i=0}^{t-2} M_{\partial_{4i+3}} \prod_{i=0}^{t-1} M_{\partial_{4i+2}}.
\]

\[
M_{\partial_t} = \prod_{i=1}^{t-1} M_{\partial_{4i}} \prod_{i=0}^{t-1} M_{\partial_{4i+2}}.
\]

Consequently, every \(\mathbb{Z}_4 \times \mathbb{Z}_2^2\)-cocyclic matrix \(M_f\) using \(R\) may be expressed as a pointwise product of matrices in \(\{M_{\partial_1}, \ldots, M_{\partial_t}\}\) in 8 different ways, just one of which does not use neither of \(M_{\partial_1}, M_{\partial_{4t-1}}\) and \(M_{\partial_t}\) (and gives precisely the expression of \(M_f\) as a linear combination of elements in \(B\)). Actually, suppose that \(M_f = R \prod_{k=1}^{4} \prod_{j_k \in J_k} M_{\partial_{j_k}}\), where \(J_k \subset \{1, \ldots, 4t\}\) is a subset of indexes which are congruent to \(k\) modulo 4. Then \(M_f\) may be expressed as the pointwise product of the coboundary matrices of indexes belonging to any of the following 8 subsets: \((J_1, J_2, J_3, J_4), (\bar{J}_1, J_2, J_3, J_4), (J_1, J_2, \bar{J}_3, J_4), (J_1, J_2, J_3, \bar{J}_4),\)
\((J_1, J_2, J_3, J_4), (J_1, J_2, J_3, J_4), (J_1, J_2, J_3, J_4), (J_1, J_2, J_3, J_4)\), where \(J_k = \{k + 4i : 0 \leq i \leq t - 1\}\). \(J_k\) denotes the complementary subset of \(J_k\).

It is known that a cocyclic matrix is Hadamard if and only if the summation of each row but the first is zero (this is the cocyclic Hadamard test, see \[8, 4\] for instance). Furthermore, following the proof of this fact, it is easy to prove that the summation of the row corresponding to \(g_i\) is zero if and only if the summation of the row corresponding to \(g_{i-1}\) is zero as well.

Consequently, the summation of the row \(n\) of a \(\mathbb{Z}_t \times \mathbb{Z}_2^2\)-cocyclic matrix is zero if and only if the summation of the row \(4t + 4 - 4\lceil \frac{n}{4} \rceil + 1 + [n - 1 \mod 4]\) is zero as well, for \(5 \leq n \leq 2t + 2\).

Furthermore, as proved in \[1\], the summation of each of the second, third and fourth rows is always zero.

This way, a \(\mathbb{Z}_t \times \mathbb{Z}_2^2\)-cocyclic matrix is Hadamard if and only if the summation of each of the rows from 5 to \(2t + 2\) is 0.

In \[1\], an equivalent characterization of the cocyclic Hadamard test is described in terms of \textit{paths} and \textit{intersections}.

A set \(\{M_{\partial_j} : 1 \leq j \leq w\}\) of generalized coboundary matrices defines a \textit{n-walk} if these matrices may be ordered in a sequence \((M_{t_1}, \ldots, M_{t_w})\) so that consecutive matrices \(M_{t_i}\) and \(M_{t_{i+1}}\) share a negative entry at the \(n\)-th row, precisely at the position \((n, l_{i+1}), 1 \leq i \leq w - 1\). Such a walk is called a \textit{path} if the initial (equivalently, the final) matrix shares a \(-1\) entry with a generalized coboundary matrix which is not in the walk itself, and a \textit{cycle} otherwise.

With this notation at hand, the summation of the \(n\)-th row of a matrix \(M_{\partial_1} \ldots M_{\partial_w} \cdot R\) is zero if and only if \(2c_n + r_n - 2I_n = 2t\), where \(c_n\) is the number of maximal \(n\)-paths in \(\{M_{\partial_1}, \ldots, M_{\partial_w}\}\), \(r_n\) is the number of \(-1\)s in the \(n\)-th row of \(R\) and \(I_n\) is the number of positions in which \(R\) and \(M_{\partial_1} \ldots M_{\partial_w}\) share a common \(-1\) in their \(n\)-th row (obviously, \(0 \leq I_n \leq r_n\)).

\textbf{Corollary 1} In particular, for \(\mathbb{Z}_t \times \mathbb{Z}_2^2\)-cocyclic matrices:

1. the summation of a row \(n \equiv 1 \mod 4\) is zero if and only if \[c_n = t, \tag{4}\]

2. the summation of a row \(n \equiv 0, 2, 3 \mod 4\) is zero if and only if \[c_n = I_n. \tag{5}\]

In the following section we analyze the number \(c_n\) of \(n\)-paths of a \(\mathbb{Z}_t \times \mathbb{Z}_2^2\)-cocyclic matrix. Focusing in rows \(n \equiv 1 \mod 4\), we will obtain upper and lower bounds on the number of coboundaries to combine in order to get a \(\mathbb{Z}_t \times \mathbb{Z}_2^2\)-cocyclic Hadamard matrix. Furthermore, we will characterize the distribution of these coboundaries in terms of \textit{ingredients} and \textit{recipes}.
3 Distributions, ingredients and recipes

Firstly, we analyze the way in which \( n \)-paths are generated on \( \mathbb{Z}_t \times \mathbb{Z}_2^2 \)-cocyclic matrices, depending on the value of \( n \) modulo 4.

**Lemma 1** Characterization of \( n \)-paths of coboundaries on \( \mathbb{Z}_t \times \mathbb{Z}_2^2 \)-cocyclic matrices:

1. If \( n \equiv 1 \mod 4 \), \( M_{\partial_{i-n+1}} \) forms an \( n \)-path with \( M_{\partial_i} \).
2. If \( n \equiv 2 \mod 4 \), \( M_{\partial_{i-n+2-(-1)^i}} \) forms an \( n \)-path with \( M_{\partial_i} \).
3. If \( n \equiv 3 \mod 4 \), \( M_{\partial_{i-n+3-2(-1)^i}} \) forms an \( n \)-path with \( M_{\partial_i} \).
4. If \( n \equiv 0 \mod 4 \), \( M_{\partial_{i-n+4+(-1)^i(1-4(1-\lfloor \frac{n+4}{4} \rfloor))}} \) forms an \( n \)-path with \( M_{\partial_i} \).

**Proof.**
This may be checked by direct inspection. \( \square \)

**Corollary 2** In particular, the set of coboundaries \( \{\partial_1, \ldots, \partial_4\} \) splits into four 5-cycles of length \( t \),

\[
[\partial_{4t-3}, \partial_{4t-7}, \ldots, \partial_5, \partial_1], \quad [\partial_{4t-2}, \partial_{4t-6}, \ldots, \partial_6, \partial_2],
\]

\[
[\partial_{4t-1}, \partial_{4t-5}, \ldots, \partial_7, \partial_3], \quad [\partial_{4t}, \partial_{4t-4}, \ldots, \partial_8, \partial_4],
\]

Now we focus our attention on rows \( n \equiv 1 \mod 4 \). From Lemma 1, it is apparent that \( n \)-paths consists of groups of coboundaries in the same coset modulo 4.

**Lemma 2** Given \( 1 \leq i \neq j \leq 4t \), \( i \equiv j \mod 4 \), there exists one and only one row \( n \), \( 5 \leq n \leq 2t+2 \), \( n \equiv 1 \mod 4 \), such that \( M_{\partial_i} \) and \( M_{\partial_j} \) form an \( n \)-path.

**Corollary 3** Along the \( \frac{t-1}{2} \) rows \( n \equiv 1 \mod 4 \), \( 5 \leq n \leq 2t+2 \), any \( k \) coboundaries \( \partial_{i_1}, \ldots, \partial_{i_k} \) in the same coset modulo 4 give rise to a total amount of \( \frac{k(t-k)}{2} \) paths.

**Proof.**
Along the \( \frac{t-1}{2} \) rows \( n \equiv 1 \mod 4 \), \( 5 \leq n \leq 2t+2 \), any \( k \) coboundaries \( \partial_{i_1}, \ldots, \partial_{i_k} \) in the same coset modulo 4 might give rise to \( k \frac{t-k}{2} \) paths. Actually, this is not the case, since we know from Lemma 2 that every pair of such coboundaries forms a path at one and only one of these rows \( n \). Thus the total amount of paths has to be reduced in the number of pairs in which the \( k \) coboundaries may be grouped. This gives \( k \frac{t-k}{2} - k \frac{(k-1)}{2} = k \frac{k-1}{2} \), as claimed. \( \square \)

Table 1 shows the total amount \( \frac{k(t-k)}{2} \) of paths produced by \( k \) coboundaries in the same coset modulo 4, for odd values of \( t \).
Table 1: Paths produced from $k$ coboundaries in rows $n \equiv 1 \mod 4$.

|     | 1    | 1    | $t = 3$ |
|-----|------|------|---------|
| 2   | 3    | 3    | 2       |
| 3   | 5    | 6    | 5       |
| 4   | 7    | 9    | 10      |
| 5   | 9    | 12   | 14      |
| :   | :    | :    | :       |
| $t - 1$ | $t + 1$ | $t - 1$ | 1 $k$ |

Proposition 1 Table 1 has many valuable combinatorial properties:

1. The table is symmetric.
2. The numbers in the central columns are triangular numbers, of the type $\frac{n(n+1)}{2}$.
3. Subtracting from a number in the central columns any of the numbers of the same row, gives as result a triangular number as well.
4. Reciprocally, subtracting from a number in the central columns any triangular number gives as result a number of the same row.

Proof.

1. The table is symmetric, since $k$ coboundaries give rise to $\frac{k(t-k)}{2}$ paths, exactly the same amount of paths produced by $t-k$ coboundaries, $\frac{(t-k)k}{2}$.
2. The numbers in the central columns are triangular numbers. Actually, $\frac{t-1}{2}$ coboundaries give rise to $\frac{t-1}{2} \cdot \frac{t+1}{2} = \frac{t^2-1}{8}$ paths.
3. Subtracting from a number in the central columns any of the numbers of the same row, gives as result a triangular number as well. Indeed, subtracting $\frac{k(t-k)}{2}$ paths from $\frac{t^2-1}{8}$ gives $\frac{t^2-1-4kt+4k^2}{8} = \frac{(t-2k)^2-1}{8}$.
4. The argument above fits here as well.

Attending to the condition (4), in order to get a $\mathbb{Z}_4 \times \mathbb{Z}_2^2$-cocyclic Hadamard matrix, a necessary (but not sufficient!) condition is to select $k$ coboundaries in the coset $i \mod 4$, such that there is a total amount of $\frac{t^2-1}{2}$ paths along the $\frac{t^2}{2}$ rows $n \equiv 1 \mod 4, 5 \leq n \leq 2t + 2$. This motivates the following definition.
**Definition 1** A distribution is an ordered tuple \((\frac{k_0(t-k_0)}{2}, \frac{k_1(t-k_1)}{2}, \frac{k_2(t-k_2)}{2}, \frac{k_3(t-k_3)}{2})\), \(0 \leq k_j \leq \frac{t-1}{2}\) for \(j \geq 1\), such that

\[
\sum_{i=0}^{3} \frac{k_i(t-k_i)}{2} = \frac{t(t-1)}{2}.
\]

**Proposition 2** For any odd \(t\), there always exists at least one distribution \((\frac{k_0(t-k_0)}{2}, \frac{k_1(t-k_1)}{2}, \frac{k_2(t-k_2)}{2}, \frac{k_3(t-k_3)}{2})\).

Proof.

The maximum possible number of paths is \(4 \frac{t^2-1}{8} = \frac{t^2-1}{2}\), obtained when \(k_0 = k_1 = k_2 = k_3 = \frac{t-1}{2}\), so that the relation (6) fails to hold by a difference \(m = \frac{t^2-1}{2} - \frac{t(t-1)}{2}\).

In 1796 Gauss proved that any positive integer can be decomposed as the summation of three (not necessarily different) triangular numbers, some of which may be eventually zero. Consequently, there exist three triangular numbers \(0 \leq t_1, t_2, t_3 \leq \frac{t^2-1}{8}\) such that \(m = t_1 + t_2 + t_3\).

Thus \(\frac{t^2-1}{2} = 4 \frac{t^2-1}{8} - m = \frac{t^2-1}{8} + (\frac{t^2-1}{8} - t_1) + (\frac{t^2-1}{8} - t_2) + (\frac{t^2-1}{8} - t_3)\). Taking into account Proposition 1 there exist integers \(0 \leq k_3 \leq k_2 \leq k_1 \leq \frac{t^2-1}{2}\) such that \((\frac{t^2-1}{8} - t_i) = \frac{k_i(t-k_i)}{2}\), and therefore \((\frac{t^2-1}{8}, \frac{k_1(t-k_1)}{2}, \frac{k_2(t-k_2)}{2}, \frac{k_3(t-k_3)}{2})\) is a distribution, in the sense of Definition 1.

\(\square\)

**Proposition 3** Furthermore, there are as many different distributions as many different decompositions of \(\frac{t-1}{2}\) as the summation of four triangular numbers.

Proof.

This is a straightforward consequence of the argument explained in the proof of Proposition 2.

\(\square\)

Propositions 2 and 3 give a method for finding the set of distributions for a given \(t\), in terms of decompositions of \(\frac{t-1}{2}\) as the summation of four triangular numbers \(0 \leq t_0 \leq t_1 \leq t_2 \leq t_3 \leq \frac{t^2-1}{8}\).

**Proposition 4** Let \(k\) be a positive integer. Then:

1. \(k\) is a triangular number if and only if \(\frac{-1+\sqrt{1+8k}}{2}\) is an integer.

2. The greatest triangular number less or equal to \(k\) is \(t_n\), for \(n = \lfloor \frac{-1+\sqrt{1+8k}}{2} \rfloor\).

3. If \(k\) is decomposed as the summation of \(m\) triangular numbers \(t_{ij}\), \(1 \leq j \leq m\), then \(\max \{t_{ij}\} \geq t_n\), for \(n = \lfloor \frac{-1+\sqrt{1+8k}}{2} \rfloor\).
Proof.
It suffices to notice that \( k \) is a triangular number if and only if there exists an integer \( n \) such that \( t_n = n(n+1)/2 = k \). Equivalently, if and only if the equation \( \frac{n^2}{2} + \frac{n}{2} - k \) has a positive integer solution (which, a fortiori, is \( \frac{-1+\sqrt{1+8k}}{2} \)). \( \square \)

Proposition 4 leads straightforwardly to the following algorithm for constructing the full set of distributions for a given \( t \).

**Algorithm 1** Constructing the set of distributions for \( t \).

**Input:** \( t \)

\[
k = \{ \} \\
\text{for } i_1 \text{ from } \left\lceil \frac{-1+\sqrt{1+4(t-\frac{t_1}{2})}}{2} \right\rceil \text{ to } \left\lfloor \frac{-1+\sqrt{1+4(t-\frac{t_1}{2})}}{2} \right\rfloor \text{ do} \\
\text{for } i_2 \text{ from } \left\lceil \frac{-1+\sqrt{1+4(t-\frac{t_1}{2})}}{2} \right\rceil \text{ to } \min(i_1, \left\lceil \frac{-1+\sqrt{1+4(t-\frac{t_1}{2})}}{2} \right\rceil) \text{ do} \\
\text{for } i_3 \text{ from } \left\lceil \frac{-1+\sqrt{1+4(t-\frac{t_1}{2})}}{2} \right\rceil \text{ to } \min(i_2, \left\lceil \frac{-1+\sqrt{1+4(t-\frac{t_1}{2})}}{2} \right\rceil) \text{ do} \\
x = \frac{-1+\sqrt{1+4(t-\frac{t_1}{2})}}{2(i_2+1)} \text{ if } x \text{ is an integer, then } k = k \cup \{(x, i_3, i_1, i_2)\} \text{ fi} \\
\text{od} \\
\text{od} \\
l = \{ \} \\
\text{for } i \text{ from } 1 \text{ to length}(k) \text{ do} \\
l = l \cup \{(\frac{t^2-1}{8} - k_{i,1}, \frac{t^2-1}{8} - k_{i,2}, \frac{t^2-1}{8} - k_{i,3}, \frac{t^2-1}{8} - k_{i,4})\} \\
\text{od} \\
\text{Output: } l
\]

Table 2 shows the complete set of distributions obtained from Algorithm 1 for \( 3 \leq t \leq 25 \).

Notice that the knowledge of the full set of distributions implies the knowledge about the number of coboundaries which have to be used in order to get a \( \mathbb{Z}_t \times \mathbb{Z}_2^2 \)-cocyclic Hadamard matrix, since each summand \( k_i(t-k_i) \) is in one to one correspondence to the values \( k_i \) and \( t-k_i \) (see Table 1). In spite of this fact, we may bound the number of coboundaries to be combined a bit further.

**Proposition 5** Let \( (\frac{k_0(t-k_0)}{2}, \frac{k_1(t-k_1)}{2}, \frac{k_2(t-k_2)}{2}, \frac{k_3(t-k_3)}{2}) \) be a distribution. Call \( n = k_0 + k_1 + k_2 + k_3 \). Then

\[
1. \quad \left\lfloor \frac{t - \sqrt{4t-3}}{2} \right\rfloor \leq k_3 \leq \left\lceil \frac{t + \sqrt{4t-3}}{2} \right\rceil. \tag{7}
\]
Table 2: Distributions in terms of decompositions of $\frac{t-1}{2} = t_0 + t_1 + t_2 + t_3$.

| $t$ | $\frac{t(t-1)}{2}$ | distributions | $t_0 + t_1 + t_2 + t_3 = \frac{t-1}{2}$ |
|-----|------------------|----------------|---------------------------------|
| 3   | 3                | (1,1,1,0)      | 0 + 0 + 0 + 1 = 1               |
| 5   | 10               | (3,3,2,2)      | 0 + 0 + 1 + 1 = 2               |
| 7   | 21               | (6,6,6,3)      | 0 + 0 + 0 + 3 = 3               |
|     |                  | (6,5,5,5)      | 0 + 1 + 1 + 1 = 3               |
| 9   | 36               | (10,10,9,7)    | 0 + 0 + 1 + 3 = 4               |
|     |                  | (9,9,9,9)      | 1 + 1 + 1 + 1 = 4               |
| 11  | 55               | (15,14,14,12)  | 0 + 1 + 1 + 3 = 5               |
| 13  | 78               | (21,21,21,15)  | 0 + 0 + 0 + 6 = 6               |
|     |                  | (21,21,18,18)  | 0 + 0 + 3 + 3 = 6               |
|     |                  | (20,20,20,18)  | 1 + 1 + 1 + 3 = 6               |
| 15  | 105              | (28,28,27,22)  | 0 + 0 + 1 + 6 = 7               |
|     |                  | (28,27,25,25)  | 0 + 1 + 3 + 3 = 7               |
| 17  | 136              | (36,35,35,30)  | 0 + 1 + 1 + 6 = 8               |
|     |                  | (35,35,33,33)  | 1 + 1 + 3 + 3 = 8               |
| 19  | 171              | (45,45,42,39)  | 0 + 0 + 3 + 6 = 9               |
|     |                  | (45,42,42,42)  | 0 + 3 + 3 + 3 = 9               |
|     |                  | (44,44,44,39)  | 1 + 1 + 1 + 6 = 9               |
| 21  | 210              | (55,55,55,45)  | 0 + 0 + 0 + 10 = 10             |
|     |                  | (55,54,52,49)  | 0 + 1 + 3 + 6 = 10              |
|     |                  | (54,52,52,52)  | 1 + 3 + 3 + 3 = 10              |
| 23  | 253              | (66,66,65,56)  | 0 + 0 + 1 + 10 = 11             |
|     |                  | (65,65,63,60)  | 1 + 1 + 3 + 6 = 11              |
| 25  | 300              | (78,78,72,72)  | 0 + 0 + 6 + 6 = 12              |
|     |                  | (78,77,77,68)  | 0 + 1 + 1 + 10 = 12             |
|     |                  | (78,75,75,73)  | 0 + 3 + 3 + 6 = 12              |
|     |                  | (75,75,75,75)  | 3 + 3 + 3 + 3 = 12              |

$$[2(t - \sqrt{t})] \leq n \leq [2(t + \sqrt{t})].$$  \hspace{1cm} (8)$$

**Proof.**

Let $(k_0, k_1, k_2, k_3)$ generate a distribution $(\frac{k_0(t-k_0)}{2}, \frac{k_1(t-k_1)}{2}, \frac{k_2(t-k_2)}{2}, \frac{k_3(t-k_3)}{2})$. 

2.
On one hand, attending to condition (6), necessarily
\[
\frac{t(t - 1)}{2} - \frac{3t^2 - 1}{8} \leq \frac{k_3(t - k_3)}{2}.
\]
Simplifying this expression, we get
\[
4k_3^2 - 4k_3t + t^2 - 4t + 3 \leq 0 \iff
\]
\[
\left\lceil \frac{t - \sqrt{t^2 - 3}}{2} \right\rceil \leq k_3 \leq \left\lfloor \frac{t + \sqrt{t^2 - 3}}{2} \right\rfloor,
\]
which proves (7).

On the other hand, simplifying (6), we get
\[
t \sum_{i=0}^{3} k_i - t^2 + t = \sum_{i=0}^{3} k_i^2.
\]
Call \( n = \sum_{i=0}^{3} k_i \). Since
\[
\sum_{i=0}^{3} k_i^2 \geq \sum_{i=0}^{3} \left( \frac{n}{4} \right)^2,
\]
we get
\[	n - t^2 + t \geq \frac{n^2}{4} \iff
\]
\[
\left\lceil 2(t - \sqrt{t}) \right\rceil \leq n \leq \left\lfloor 2(t + \sqrt{t}) \right\rfloor,
\]
as stated in (8).

\[\square\]

Remark 1 Condition (8) may be tightened, depending on the coset of \( n = k_0 + k_1 + k_2 + k_3 \) modulo 4, substituting the lower bound in (9) by the most homogeneously distributed partition of \( n \) into four parts:

- If \( n \equiv 0 \mod 4 \), \( \sum_{i=0}^{3} k_i^2 \geq 4 \left( \frac{n}{4} \right)^2 \), so that
  \[
  \left\lceil 2(t - \sqrt{t}) \right\rceil \leq n \leq \left\lfloor 2(t + \sqrt{t}) \right\rfloor.
  \]

- If \( n \equiv 1 \mod 4 \), \( \sum_{i=0}^{3} k_i^2 \geq 3 \left( \frac{n - 1}{4} \right)^2 + \left( \frac{n + 3}{4} \right)^2 \), so that
  \[
  \left\lceil 2(t - \sqrt{t - \frac{3}{4}}) \right\rceil \leq n \leq \left\lfloor 2(t + \sqrt{t - \frac{3}{4}}) \right\rfloor.
  \]
Figure 1: Visual trace of the relation $n_1^2 + n_2^2 \geq 2(\frac{n_1 + n_2}{2})^2$.

- If $n \equiv 2 \mod 4$, $\sum_{i=0}^{3} k_i^2 \geq 2(\frac{n-2}{4})^2 + 2(\frac{n+2}{4})^2$, so that
  
  $[2(t - \sqrt{t-1})] \leq n \leq [2(t + \sqrt{t-1})].$

- If $n \equiv 3 \mod 4$, $\sum_{i=0}^{3} k_i^2 \geq (\frac{n-3}{4})^2 + 3(\frac{n+1}{4})^2$, so that
  
  $[2(t - \sqrt{t-\frac{3}{4}})] \leq n \leq [2(t + \sqrt{t-\frac{3}{4}})].$

Remark 2 In spite of the fact that one may be immediately convinced about the validity of the condition (9), and its variants in Remark 1, actually these relations cannot be proved so easily. Although we are not going to prove these relations rigourously here, since this is out of the scope of the paper, we will however give a visual trace of this fact for the case of two summands.

Actually, given an integer $n$, it is apparent that for every decomposition of $n$ into two summands, say $n = n_1 + n_2$, the area obtained by the summation of the squares of sides $n_1$ and $n_2$ is greater than or equal to twice the area of the square of side $\frac{n}{2}$, as Fig. 1 illustrates.

The argument above would straightforwardly fit to prove the more general case. In fact, one could check that

$$\sum_{i=1}^{k} n_i^2 - \frac{1}{k} \left( \sum_{i=1}^{k} n_i \right)^2 = \frac{1}{k} \sum_{1 \leq j < i \leq k} (n_i - n_j)^2 \geq 0.$$  \hspace{1cm} (10)

Remark 3 The bounds in Proposition 2 are very tight, as it have been checked experimentally. The first gap occurs for $t = 71$, and consists in just one coboundary.

Once we know that a distribution is available for a given value of $t$, the next step is looking for appropriated subsets of $n_i$ coboundaries in the cosets $i \mod 4$ in $B$ such that the amount of $n$-paths along rows $n \equiv 1 \mod 4$, $5 \leq n \leq 2t-1$ fits that distribution.

Definition 2 An ingredient produced by a subset of $m$ coboundaries in $B$ in the same coset modulo 4 is the column vector whose entries are the number of $n$-paths produced by these $m$ coboundaries along rows $n \equiv 1 \mod 4$, $5 \leq n \leq 2t-1$. 

12
A recipe is a collection of 4 ingredients (one for each different coset \( i \) modulo 4), arranged as a matrix of 4 columns, such that the sum of each of the rows is \( t \).

Consequently, if a subset of \( \{n_1, n_2, n_3, n_4\} \) coboundaries in \( \mathcal{B} \) defines a recipe, this subset of coboundaries satisfies the condition (1), and therefore the summation of each of the rows \( n \equiv 1 \ mod \ 4, \ 5 \leq n \leq 2t - 1 \) is zero.

**Proposition 6** The notion of recipe does not depend on the order of its ingredients.

**Proof.**

Attending to Lemma 1, \( \partial_i \) forms an \( n \)-path with \( \partial_{i-n+1} \), independently on the coset \( i \mod 4 \), for \( n \equiv 1 \ mod \ 4, \ 5 \leq n \leq 2t - 1 \). In particular, \( n \)-paths are constructed from those coboundaries in \( \mathcal{B} \) in the same coset \( i \mod 4 \), which differ in \( \frac{n}{4} \) positions in the cycles of Corollary 2.

This way, if a subset of coboundaries of the coset \( i \mod 4 \) produces an ingredient, the same ingredient is produced by the translation of this subset to any other coset \( j \mod 4 \).

Eventually, this translation could produce a coboundary \( \partial_i \) which is not in \( \mathcal{B} \). This is not a source of difficulties, since from the relations (1), (2) and (3), such prohibited subsets of coboundaries may be substituted by their complements in the cycles of Corollary 2. Since the substitution of any amount of paths by their complementary in a cycle does not change the total amount of paths, this operation preserves the ingredient.

Finding a recipe is the first step in the process of constructing a \( \mathbb{Z}_t \times \mathbb{Z}_2^2 \) cocyclic Hadamard matrix, since any subset of coboundaries in \( \mathcal{B} \) defining a recipe satisfies condition (4). The following proposition gives a condition about when the relation (5) is also satisfied (and hence a \( \mathbb{Z}_t \times \mathbb{Z}_2^2 \)-cocyclic Hadamard matrix has been found).

**Proposition 7** A subset of coboundaries in \( \mathcal{B} \) satisfies (5) (i.e. the summation of the \( n \)-th row is zero, for \( n \equiv 0, 2, 3 \mod 4, \ 6 \leq n \leq 2t + 2 \)), if and only if the number of \( n \)-paths of length even is itself even, half of them starting and ending with coboundaries in cosets \( i_1, i_2 \mod 4 \), the other half starting and ending in coboundaries in cosets \( i_3, i_4 \mod 4 \), \( i_j \neq i_k \) for \( j \neq k \).

**Proof.**

As we commented in Section II, we are using \( R = 1_t \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix} \) as the matrix coming from representative cocycles.

Consequently, intersections in rows \( n \equiv 2 \mod 4 \) can occur in positions \( (n, i) \), for \( i \equiv 2, 0 \mod 4 \). Similarly, intersections in rows \( n \equiv 3 \mod 4 \) can
occur in positions \((n, i)\), for \(i \equiv 2, 3 \mod 4\). Finally, intersections in rows \(n \equiv 0 \mod 4\) can occur in positions \((n, i)\), for \(i \equiv 3, 0 \mod 4\).

Taking into account Lemma 1, it follows that \(n\)-paths consists in properly alternating coboundaries in:

- Either cosets \((1, 2) \mod 4\), either cosets \((3, 0) \mod 4\), for \(n \equiv 2 \mod 4\).
- Either cosets \((2, 0) \mod 4\), either cosets \((1, 3) \mod 4\), for \(n \equiv 3 \mod 4\).
- Either cosets \((2, 3) \mod 4\), either cosets \((1, 0) \mod 4\), for \(n \equiv 0 \mod 4\).

Hence any \(n\)-path of odd length produces exactly one intersection (i.e. shares exactly one negative entry) with \(R\) at the \(n\)-th row. On the other hand, \(n\)-paths of even length produces either 2 or 0 intersections, depending on the cosets modulo 4 of \(n\) and the initial coboundary of the \(n\)-path. More precisely:

- If \(n \equiv 2 \mod 4\), then an \(n\)-path of even length will produce two intersections at the \(n\)-th row if and only if the coset \(i\) of the initial coboundary is \(i \equiv 2, 0 \mod 4\).
- If \(n \equiv 3 \mod 4\), then an \(n\)-path of even length will produce two intersections at the \(n\)-th row if and only if the coset \(i\) of the initial coboundary is \(i \equiv 2, 3 \mod 4\).
- If \(n \equiv 0 \mod 4\), then an \(n\)-path of even length will produce two intersections at the \(n\)-th row if and only if the coset \(i\) of the initial coboundary is \(i \equiv 3, 0 \mod 4\).

Summing up, odd \(n\)-paths produces 1 intersection, and even \(n\)-paths produces either 2 or 0 intersections. Hence, the only circumstance in which the amounts of intersections and \(n\)-paths both coincide is precisely when half the even \(n\)-paths give rise to 2 intersections, whereas the remaining half of even \(n\)-paths do not produce any intersections at all, as stated.

Now it is straightforward to design an algorithm searching exhaustively for \(\mathbb{Z}_t \times \mathbb{Z}_2^2\)-cocyclic Hadamard matrices for odd \(t\).

**Algorithm 2** Exhaustive search for \(\mathbb{Z}_t \times \mathbb{Z}_2^2\)-Hadamard matrices.

**Input:** \(t\).

*Calculate the valid distributions for \(t\).*
*Calculate all the ingredients associated to every distribution.*
*Construct the set of recipes corresponding to each distribution.*
*Check whether these subsets satisfy the balanced distribution of even \(n\)-paths for \(n \equiv 2, 3, 0 \mod 4\), \(6 \leq n \leq 2t + 2\).*

**Output:** the full set of \(\mathbb{Z}_t \times \mathbb{Z}_2^2\)-Hadamard matrices.
Table 3: $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices from Algorithm 2

| $t$  | distribution | #ingred. | #rec. | #H.r. | #H. |
|------|--------------|----------|-------|-------|-----|
| 3    | (1, 1, 1, 0) | (1, 1, 1, 1) | 4     | 4     | 24  |
| 5    | (3, 3, 2, 2) | (2, 2, 1, 1) | 12    | 12    | 120 |
| 7    | (6, 6, 3)    | (4, 4, 4, 1) | 28    | 24    | 336 |
|      | (6, 5, 5)    | (4, 3, 3, 3) | 60    | 36    | 504 |
| 9    | (10, 10, 9, 7)| (10, 10, 7, 4) | 756   | 108   | 1944|
| 9    | (9, 9, 9, 9) | (7, 7, 7, 7) | 60    | 24    | 432 |
| 11   | (15, 14, 14, 12)| (26, 20, 20, 10) | 5580  | 120   | 2640|
| 13   | (21, 21, 21, 15)| (74, 74, 74, 14) | 19320 | 144   | 3744|
|      | (21, 21, 18, 18)| (74, 74, 34, 34) | 29208 | 72    | 1872|
|      | (20, 20, 20, 18)| (57, 57, 57, 34) | 21612 | 108   | 2808|

4 Calculations and examples

Table 3 shows an exhaustive calculation of $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices (last column) for odd $t$, $3 \leq t \leq 13$, in terms of distributions (second column), ingredients (third column) and recipes (fourth column) by means of Algorithm 2. The fifth column shows how many of the recipes are “productive”, in the sense that they actually give rise to $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices.

5 Conclusions

We wonder about the consistence of the observations listed below. Are there any reasons for these behaviors? Can these properties be demonstrated?

1. As far as we have been able to check, if a $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrix exists associated to a recipe, it seems that there also exist $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices associated to any recipe obtained by permuting columns from it. Nevertheless, this is not always true for row permutations.

2. Furthermore, as far as we have been able to check, given a $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrix meeting a distribution, it seems that there also exists another $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrix meeting the same distribution, but using the complementary number of coboundaries ($t - k_i$ instead of $k_i$) for generating some of the entries $k_i(t - k_i)$ of the distribution.

3. $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices seem to come from special recipes, those involving *singular* ingredients. Here, for a “singular” ingredient we mean one for which the set of subsets of coboundaries providing this
ingredient has minimum size. This would imply that these subsets of coboundaries must be somehow symmetrically distributed.

4. The set of symmetric Williamson type Hadamard matrices seems to be in proportion $\frac{1}{t}$ with respect to the full set of $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices.

We will devote another paper to analyze these facts. In particular, in the second series of this paper we will define a visual scheme (called diagram) for working with $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic matrices. With these diagrams at hand, the condition of symmetry will be apparent. The remaining conditions cited above imply the existence of some Hadamard-preserving transformations. In particular, assuming this condition of symmetry, the set of $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic matrices may be organized in orbits, $\frac{1}{t}$ of which will be proved to be symmetric Williamson type Hadamard matrices. We have been able to calculate the full set of orbits for $3 \leq t \leq 23$, and one orbit for $t = 25$. Furthermore, since the knowledge of just one $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic matrix completely characterizes its corresponding orbit, our method may be used to calculate orbits from the symmetric Williamson type Hadamard matrices listed in [9] (this is an exhaustive list for odd $t \leq 39$, partial for $41 \leq t \leq 63$).

References

[1] V. Álvarez, J.A. Armario, M.D. Frau and P. Real, "A system of equations for describing cocyclic Hadamard matrices", J. Comb. Des., vol. 16, pp. 276–290, 2008.

[2] V. Álvarez, J.A. Armario, M.D. Frau and P. Real, "The homological reduction method for computing cocyclic Hadamard matrices", J. Symb. Comput., vol. 44, pp. 558-570, 2009.

[3] V. Álvarez, F. Gudiel and M.B. Güemes, "Some new operations on $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices". Preprint. Submitted to journal.

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

[5] M. B. Güemes, "Cocyclic Hadamard matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$. Description, classification and search. PhD thesis (English translation), University of Seville, 2011.

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

[7] K.J. Horadam and W. de Launey, "Cocyclic development of designs", J. Algebraic Combin., vol. 2, no. 3, pp. 267–290, 1993. Erratum, J. Algebraic Combin., vol. 3, pp. 129, 1994.
[8] K.J. Horadam and W. de Launey, "Generation of cocyclic Hadamard matrices", in: Proc. Computational Algebra and Number Theory, Sydney, 1992, in Math. Appl., vol. 325, Kluwer Acad. Publ., Dordrecht, 1995, pp. 279–290.

[9] C. Koukouvinos, web page. http://www.math.ntua.gr/~ckoukov/