Gröbner bases and cocyclic Hadamard matrices

Víctor Álvarez, José Andrés Armario, Raúl M. Falcón, María Dolores Frau, Félix Gudiel

Dpto. Matemática Aplicada I, Univ. Sevilla, Avda. Reina Mercedes s/n, 41012 Sevilla, Spain

Keywords:
Hadamard matrix
Basis of cocycles
Polynomial ring
Ideal

A B S T R A C T

Hadamard ideals were introduced in 2006 as a set of nonlinear polynomial equations whose zeros are uniquely related to Hadamard matrices with one or two circulant cores of a given order. Based on this idea, the cocyclic Hadamard test enables us to describe a polynomial ideal that characterizes the set of cocyclic Hadamard matrices over a fixed finite group G of order $4t$. Nevertheless, the complexity of the computation of the reduced Gröbner basis of this ideal is $2^{O(t^2)}$, which is excessive even for very small orders. In order to improve the efficiency of this polynomial method, we take advantage of some recent results on the inner structure of a cocyclic matrix to describe an alternative polynomial ideal that also characterizes the aforementioned set of cocyclic Hadamard matrices over G. The complexity of the computation decreases in this way to $2^{O(t)}$. Particularly, we design two specific procedures for looking for $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices and D_{4t}-cocyclic Hadamard matrices, so that larger cocyclic Hadamard matrices (up to $t \leq 39$) are explicitly obtained.

1. Introduction

A binary *Hadamard matrix* H of order n is an $n \times n$ matrix with every entry either 1 or -1, which satisfies $HH^T = nI$, where I is the identity matrix of order n. Although it is well-known that n has to be necessarily 1, 2 or a multiple of 4 (as soon as three or more rows have to be simultaneously

orthogonal), there is no certainty whether such a Hadamard matrix exists at every possible order. Currently, the smallest order for which no Hadamard matrix is known is 668, and there are only 12 such orders below 2000 (Đokovic et al. (2014)). The *Hadamard conjecture* asserts that there exists a Hadamard matrix of order $4t$ for every natural number t.

There exist many different constructions for Hadamard matrices: Sylvester, Paley, Williamson, Ito, Goethals–Seidel, one and two circulant cores or cocyclic matrices, amongst others (see Horadam (2007)). Nevertheless, most of them fail to yield Hadamard matrices for every order which is a multiple of 4 and therefore are not suitable candidates for a proof of the Hadamard conjecture. Among all these constructions, it seems that the most promising are the two circulant cores matrices (Fletcher et al. (2001); Kotsireas et al. (2006b)), the Goethals–Seidel arrays (Goethals and Seidel (1967); Seberry and Yamada (1992)) and the cocyclic constructions (Horadam (2007)). Actually, the one and two circulant cores constructions have recently been described to be somehow cocyclic-based (the cores themselves are cocyclic over $\mathbb{Z}_{4t-1}$ and D_{4t-2}, respectively, see Álvarez et al. (2017) for details). A stronger version of the Hadamard conjecture, posed by Horadam and de Launey (1995) is the *cocyclic Hadamard conjecture:* this states that there exists a cocyclic Hadamard matrix at every possible order. Currently the smallest order for which no cocyclic Hadamard matrix is known is 188 (Horadam (2007)).

Kotsireas et al. (2006a) introduced the concept of *Hadamard ideal* as a set of nonlinear polynomial equations whose zeros determine the set of Hadamard matrices with one circulant core. Shortly after, Kotsireas et al. (2006b) used the same ideal together with a series of new polynomials in order to determine the set of Hadamard matrices with two circulant cores, by means of which they computed the Hadamard matrices with two circulant cores up to order 52.

In this paper, we define several *cocyclic Hadamard ideals*, whose zeros determine the set of cocyclic Hadamard matrices over a finite group G of order $4t$. Based on the cocyclic test of Horadam and de Launey (1995), our first approach (Theorem 2) gives rise to a procedure `CocGM(`t, G, opt`)` which works just for very small t, actually $t \leq 3$.

In order to improve the efficiency of this polynomial method and provided a basis of G-cocycles is known (which is always the case, see Flannery and O'Brien (2000); Flannery and Egan (2015)), we define in Theorem 5 an alternative ideal based upon the system of equations described by Álvarez et al. (2008), which also characterizes the set of G-cocyclic Hadamard matrices. This gives a procedure `CocCB(`t, G, opt`)` suitable for larger values of t.

Furthermore, from the knowledge of the properties of cocyclic matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$ and D_{4t} described by Álvarez et al. (2015, 2016), improved versions of this procedure (`CocAH(`$t, col, dist, H$`)` and `CocDH(`$t, dist, opt, H$`)`, based on Theorems 7 and 9, respectively) are used to perform local searches for $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices and D_{4t}-cocyclic Hadamard matrices.

All the procedures have been implemented as a library *hadamard.lib* in the open computer algebra system for polynomial computations SINGULAR, developed by Decker et al. (2016). Examples illustrating the use of this library and the library itself are available online at `http://personales.us.es/raufalgan/LS/hadamard.lib`. Further, all the computations that are exposed throughout the paper are implemented in a system with an *AMD Opteron 6348, with a 2.8 GHz processor (48 cores), 256 GB RAM and 3 TB Hard Drive*. Running the procedures on this system, cocyclic Hadamard matrices have been found up to order $4t \leq 156$.

The remainder of the paper is organized as follows. The first part of Section 2 is devoted to describing some preliminary concepts and results on Hadamard matrices and Algebraic Geometry, that are used in the rest of the paper. Later, we define a zero-dimensional ideal that determines the set of cocyclic Hadamard matrices over a given group G of order $4t$, which comes from a straightforward translation of the cocyclic Hadamard test of Horadam and de Launey (1995). In Section 3, we propose an alternative to the previous construction by defining a new zero-dimensional ideal, based on the results of Álvarez et al. (2008). Actually, we specialize this procedure for $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices and D_{4t}-cocyclic Hadamard matrices, attending to the properties described by Álvarez et al. (2015, 2016). The last section is devoted to conclusions and outlines for further work.

2. Preliminaries

We describe in this section some basic concepts and results on Hadamard matrices and Algebraic Geometry that are used throughout the paper. We refer to the monographs of Mac Lane (1995), Horadam (2007), De Launey and Flannery (2011) and Cox et al. (1998, 2007) for more details about these topics.

2.1. Hadamard matrices

Assume throughout that $G = \{g_1 = 1, \ldots, g_{4t}\}$ is a multiplicative finite group of $4t$ elements, not necessarily abelian. A function $\psi : G \times G \to \langle -1 \rangle \cong \mathbb{Z}_2$ is said to be a *(binary) cocycle* over G, or simply G-cocycle for short, if it satisfies that

$$\psi(g_i, g_j)\psi(g_i g_j, g_k) = \psi(g_j, g_k)\psi(g_i, g_j g_k), \text{ for all } g_i, g_j, g_k \in G. \tag{1}$$

The cocycle ψ is naturally displayed as a *cocyclic matrix* M_ψ of order $4t \times 4t$, whose (i, j)th entry is $\psi(g_i, g_j)$ for all $g_i, g_j \in G$. Since it must be $\psi(1, g_j) = \psi(g_i, 1)$ for all $g_i, g_j \in G$, the first row and column of M_ψ are all either 1 or -1. In the first case, the cocycle ψ and its cocyclic matrix M_ψ are said to be *normalized*. There is a one to one correspondence between normalized and non normalized cocycles. Without loss of generality, we will assume that all cocycles considered hereafter are normalized, and will be termed simply cocycles for short.

Let $g_d \in G$. The *elementary coboundary* ∂_d is the cocycle over G defined as

$$\partial_d(i, j) := \delta_{g_d}(g_i)\delta_{g_d}(g_j)\delta_{g_d}(g_i g_j),$$

where $\delta_{g_d} : G \to \langle -1 \rangle$ is the characteristic set map such that $\delta_{g_d}(g_i) = -1$ if $g_i = g_d$ and 1, otherwise. The *generalized coboundary matrix* $\overline{M}_{\partial_d}$ consists of negating the dth-row of the matrix M_{∂_d}. Note that negating a row or a column of a matrix does not change its Hadamard character. This is just a particular case of a more general set: there is an equivalence relation (termed *Hadamard equivalence*) on Hadamard matrices, so that two matrices are Hadamard equivalent whenever they differ in a series of row and/or column negations and/or permutations. These Hadamard equivalence classes may be grouped by means of a broader notion of equivalence relation which incorporates some different orthogonality preserving moves, termed *switching operations*. The interested reader is referred to Orrick (2008) and the references therein for details.

The following technical result summarizes some properties which are satisfied by generalized coboundary matrices, as described in Álvarez et al. (2008), and will be of interest for later use.

Lemma 1 *(Álvarez et al. (2008)). The next results hold.*

a) $\overline{M}_{\partial_d}$ *contains exactly two negative entries in each row* $s \neq 1$*, which are located at positions* (s, d) *and* (s, e)*, for* $g_e = g_s^{-1} g_d$*.*
b) *Given* $g_s \neq 1$ *and* g_c *in* G*, there are exactly two generalized coboundary matrices (*$\overline{M}_{\partial_c}$ *and* $\overline{M}_{\partial_d}$*), with a negative entry in the position* (s, c)*, where* $g_d = g_s g_c$*.*
c) *Two generalized coboundary matrices share their two negative entries at the* s*th row if and only if* $g_s^2 = 1$*.*

A *basis* $\mathbf{B} = \{\psi_1, \ldots, \psi_k\}$ of cocycles over G consists of some elementary coboundaries ∂_i and some representative cocycles. Since the elementary coboundary ∂_1 related to the identity element $1 \in G$ is not normalized, we may assume that $\partial_1 \notin \mathbf{B}$. A basis for coboundaries consists of $4t - r - 1$ elements, for r being the rank of the Sylow 2-subgroup of $G/[G, G]$, and may be calculated straightforwardly (see Horadam and de Launey (1995); Flannery and Egan (2015)). A basis for representative cocycles consists of r cocycles coming from $\mathrm{Ext}(G/[G, G], \mathbb{Z}_2)$ and $k - 4t + 1$ cocycles (one for each 2-power component of $H_2(G)$) coming from $\mathrm{Hom}(H_2(G), \mathbb{Z}_2)$, and may be calculated by means of a Magma (Bosma et al. (1997)) procedure as described in Flannery (1996); Flannery and O'Brien (2000).

Every cocycle over G admits a unique representation as a product of the generators in $\mathbf{B}$, $\psi = \psi_1^{x_1} \cdots \psi_k^{x_k}$, $x_i \in \{0, 1\}$. The tuple $(x_1, \ldots, x_k)_{\mathbf{B}}$ defines the *coordinates* of ψ with regards to $\mathbf{B}$. Accordingly, every cocyclic matrix $M_\psi = (\psi(i, j))$, for $\psi = (x_1, \ldots, x_k)_{\mathbf{B}}$, admits a unique decomposition $M_\psi = M_{\psi_1}^{x_1} \cdots M_{\psi_k}^{x_k}$ as the Hadamard pointwise product of those matrices M_{ψ_i} corresponding to entries $x_i = 1$. In what follows, we use generalized coboundary matrices instead of classical coboundary matrices. Let us point out that any matrix obtained as the Hadamard product of generalized coboundary matrices and representative cocycles is Hadamard equivalent to a cocyclic matrix by means of negations of certain rows.

A cocycle ψ (over G) is said to be *orthogonal* if its cocyclic matrix M_ψ is Hadamard. In such a case, M_ψ is said to be a *cocyclic Hadamard matrix over* G or a G*-cocyclic Hadamard matrix*. The set of cocyclic Hadamard matrices over G is denoted by $\mathcal{H}_G$. The *cocyclic Hadamard test* of Horadam and de Launey (1995) asserts that a cocyclic matrix M_ψ is Hadamard if and only if

$$\sum_{j \in G} \psi(i, j) = 0, \text{ for all } i \in G \setminus \{1\}. \tag{2}$$

A row of M_ψ is termed *Hadamard row* precisely when its summation is zero. Therefore, M_ψ is Hadamard if and only if every row (but the first) is a Hadamard row.

2.2. Algebraic geometry

Let $\{X\}$ and $\mathbb{K}[X]$ be, respectively, the set of m variables $\{x_1, \ldots, x_m\}$ and the associated multivariate polynomial ring over a field $\mathbb{K}$. The *affine variety* $V(I)$ of an ideal $I \subseteq \mathbb{K}[X]$ is the set of points in $\mathbb{K}^m$ that are zeros of all the polynomials of I. The ideal I is said to be *zero-dimensional* if $V(I)$ is finite. It is said to be *radical* if every polynomial $p \in \mathbb{K}[X]$ belongs to I whenever there exists a natural number n such that $p^n \in I$. A *term order* $<$ on the set of monomials of $\mathbb{K}[X]$ is a multiplicative well-ordering that has the constant monomial 1 as its smallest element. The largest monomial of a polynomial p of I with respect to the term order $<$ is its *leading monomial*. The ideal generated by the leading monomials of all the non-zero elements of I is its *initial ideal* $I_<$. Those monomials of polynomials of I that are not leading monomials of any polynomial of I are called *standard monomials*. If the ideal I is zero-dimensional, then the number of standard monomials of I coincides with the dimension of $\mathbb{K}[X]/I$ over $\mathbb{K}$, which is greater than or equal to the number of points of $V(I)$. The equality holds when I is radical. This dimension can be obtained by computing the *Hilbert function* $\mathrm{HF}_{\mathbb{K}[X]/I}$, which maps each non-negative integer d onto $\dim_{\mathbb{K}}(\mathbb{K}[X]_d/I_d)$, where $\mathbb{K}[X]_d$ denotes the set of homogeneous polynomials in $\mathbb{K}[X]$ of degree d and $I_d = \mathbb{K}[X]_d \cap I$. In particular, $\dim_{\mathbb{K}}(\mathbb{K}[X]/I) = \sum_{0 \le d} \mathrm{HF}_{\mathbb{K}[X]/I}(d)$. If the ideal I is zero-dimensional, then the number $\mathrm{HF}_{\mathbb{K}[X]/I}(d)$ coincides with the set of standard monomials of degree d, regardless of the term order. As a consequence, the Hilbert function of $\mathbb{K}[X]/I$ coincides with that of $\mathbb{K}[X]/I_<$, for any term order $<$, which can be obtained by using for instance the algorithm of Mora and Möller (1983). Previously, it was required to determine the initial ideal $I_<$. In any case, Bayer and Stillman (1992) already proved that the problem of computing Hilbert functions is NP-complete.

A *Gröbner basis* (Buchberger (2006)) of the ideal I is any subset GB of polynomials of I whose leading monomials with respect to a given term order generate the initial ideal $I_<$. It is *reduced* if all its polynomials are monic and no monomial of a polynomial in GB is generated by the leading monomials of the rest of polynomials in the basis. There exists a unique reduced Gröbner basis of the ideal I. This basis generates the initial ideal $I_<$ and can be used, therefore, to determine the cardinality of its affine variety $V(I)$. Further, the points of this variety can be enumerated once the reduced Gröbner basis is decomposed into finitely many disjoint subsets, each of them being formed by the polynomials of a triangular system of polynomial equations, whose factorization and subsequent resolution are easier than the system related to the generators of the original ideal I. See in this regard the articles of Hillebrand (1999), Lazard (1992) and Möller (1993).

Gröbner bases can, therefore, be used to determine both the cardinality and the elements of the set $\mathcal{H}_G$ of cocyclic Hadamard matrices over a multiplicative finite group G of $4t$ elements. To this

end, let $\mathbb{Q}[X_G]$ be the polynomial ring over the field $\mathbb{Q}$ of rational numbers, with set of $16t^2$ variables $\{X_G\} = \{x_{i,j} :\ g_i, g_j \in G\}$ and let us define the polynomial

$$p_{i,j,k}(\mathrm{X}) := x_{i,j}x_{ij,k} - x_{j,k}x_{i,jk},\ \text{for all } g_i, g_j, g_k \in G,$$

where the products ij and jk are induced by the group law in G. The next result shows how the set $\mathcal{H}_G$ of cocyclic Hadamard matrices over G can be identified with the affine variety defined by a zero-dimensional radical ideal of nonlinear polynomials in $\mathbb{Q}[X_G]$.

Theorem 2. *The set $\mathcal{H}_G$ can be identified with the set of zeros of the zero-dimensional ideal $I_G = I_G^1 + I_G^2 + I_G^3 + I_G^4 \subset \mathbb{Q}[X_G]$ consisting in the summation of the following four subideals:*

$$\begin{cases} I_G^1 = \langle\, x_{i,j}^2 - 1 :\ i, j \in G \,\rangle, \\ I_G^2 = \langle\, p_{i,j,k}(X) :\ i, j, k \in G \,\rangle, \\ I_G^3 = \langle\, x_{1,i} - 1, x_{i,1} - 1 :\ i \in G \,\rangle, \\ I_G^4 = \langle\, \sum_{j \in G} x_{i,j} :\ i \in G \setminus \{1\} \,\rangle. \end{cases}$$

Besides, $|\mathcal{H}_G| = \dim_{\mathbb{Q}}(\mathbb{Q}[X_G]/I_G)$.

Proof. Let $P = (p_{1,1}, \ldots, p_{4t,4t})$ be a point of the affine variety $V(I_G)$. Attending to I_G^1, every component $p_{i,j}$ of P is either 1 or -1, for all $i, j \in G$. Let $\psi : G \times G \to \{\pm 1\}$ be defined such that $\psi(i, j) = p_{i,j}$, for all $g_i, g_j \in G$. Since I_G^2 implies by construction that ψ satisfies identity (1) for all $g_i, g_j, g_k \in G$, the point P can be identified with the cocyclic matrix M_ψ related to ψ (which is, in addition, normalized, because of the definition of the subideal I_G^3). Finally, I_G^4 implies that M_ψ satisfies identity (2) and hence, M_ψ is Hadamard. The affine variety $V(I_G)$ coincides, therefore, with the set $\mathcal{H}_G$, whose finiteness involves the ideal I_G to be zero-dimensional.

Besides, since $I_G \cap \mathbb{Q}[x_{i,j}] = \langle\, x_{i,j}^2 - 1 \,\rangle \subseteq I_G$ for all $i, j \in G$ and all these polynomials are square-free, Proposition 2.7 of Cox et al. (1998) implies that

$$\sqrt{I_G} = I_G + \sum_{i,j} I_G \cap \mathbb{Q}[x_{i,j}] = I_G,$$

so I_G is therefore radical. And hence, $|\mathcal{H}_G| = |V(I_G)| = \dim_{\mathbb{Q}}(\mathbb{Q}[X_G]/I_G)$. □

Notice that, as defined, each of the subideals I_G^1, I_G^2, I_G^3 and I_G^4 are generated by $16t^2$, $64t^3$, $8t - 1$ and $4t - 1$ polynomials over the set of $16t^2$ variables X_G. Nevertheless, some of these polynomials are redundant and may straightforwardly be removed from a system of generators for I_G. Namely, it is easy to check that $I_G^3 \subset \langle x_{1,1} - 1 \rangle + I_G^2$, as the result of a standard proof on the fact that any cocycle is either normalized or unnormalized (see Lemma 1.3 of Horadam and de Launey (1995) for details). Furthermore, the $8t - 1$ polynomials $\{x_{1,i}^2 - 1, x_{i,1}^2 - 1 : i \in G\}$ in I_G^1 may be removed as well, since they are also in I_G^3. Anyway, the set of polynomials generating I_G which we have just described consists of $O(t^3)$ polynomials of degree up to 2 over $O(t^2)$ variables.

It is a remarkable fact that the computation of the reduced Gröbner basis of a zero-dimensional ideal is extremely sensitive to the number of variables. See in this regard the articles of Hashemi (2009), Hashemi and Lazard (2011), Lakshman (1991) and Lakshman and Lazard (1991). In the last reference, the authors proved that the complexity of our computation is $d^{O(n)}$, where d is the maximal degree of the generators of ideal and n is the number of variables. In the case of Theorem 2, this complexity is $2^{O(t^2)}$, which renders the computation only possible for very low values of t.

The procedure `CocGM(t, G, opt)` (included in the library *hadamard.lib* which is available online for free at the personal web page of one of the authors, as noticed before) provides an implementation of the method that runs on SINGULAR (Decker et al. (2016)). It is specifically designed for the group $\mathbb{Z}_t \times \mathbb{Z}_2^2$ (taking $G = 1$ as input) and the dihedral group D_{4t} (taking $G = 2$ as input), though it might be straightforwardly modified to fix for any other group G. It would suffice to include the

polynomials generating the subideal I_G^2, attending to the particular group law of G. Depending on whether the parameter `opt` is equal to 1 or 2, the procedure calculates either just the number of cocyclic Hadamard matrices over G or the explicit full set of these matrices. Notice that it makes use of the SINGULAR procedures `elimlinearpart` and `tolessvars` which speed up and simplify the calculations, reducing the number of variables and polynomials in turn.

Example 3. As an illustration of the method, consider the group $G = \mathbb{Z}_2^2$. The ideal I_G, as described in Theorem 2, is defined over the set of 16 variables $\{X_G\} = \{x_{i,j} : g_i, g_j \in G\}$ and initially consists of 90 generating polynomials, although we already pointed out before that some of these polynomials are redundant and may be removed straightforwardly from the very beginning. Assuming $x_{1,i} = x_{i,1} = 1$ for $1 \leq i \leq 4$, we reduce to 9 variables, namely $x_{i,j}$, for $2 \leq i, j \leq 4$.

A reduced Gröbner basis for I_G with respect to the degree reverse lexicographical order consists of the following 14 polynomials: $p_1 = x_{4,2} + x_{4,3} + x_{4,4} + 1$, $p_2 = x_{3,2} + x_{3,3} + x_{3,4} + 1$, $p_3 = x_{2,4} + x_{3,4} + x_{4,4} + 1$, $p_4 = x_{2,3} + x_{3,3} + x_{4,3} + 1$, $p_5 = x_{2,2} + x_{2,3} + x_{2,4} + 1$, $p_6 = x_{4,4}^2 - 1$, $p_7 = x_{4,3}x_{4,4} + x_{4,3} + x_{4,4} + 1$, $p_8 = x_{3,4}x_{4,4} + x_{3,4} + x_{4,4} + 1$, $p_9 = x_{4,3}^2 - 1$, $p_{10} = x_{3,4}x_{4,3} + x_{3,3}x_{4,4} - x_{3,3} - x_{3,4} - x_{4,3} - x_{4,4} - 2$, $p_{11} = x_{3,3}x_{4,3} - x_{3,3} - x_{4,3} - 1$, $p_{12} = x_{3,4}^2 - 1$, $p_{13} = x_{3,3}x_{3,4} - x_{3,3} - x_{3,4} - 1$, $p_{14} = x_{3,3}^2 - 1$.

These polynomials consist of monomials which may be organized into two subsets, leader monomials $LM = \{x_{2,2}, x_{2,3}, x_{2,4}, x_{3,2}, x_{4,2}, x_{3,3}^2, x_{3,3}x_{3,4}, x_{3,3}x_{4,3}, x_{3,4}^2, x_{3,4}x_{4,3}, x_{3,4}x_{4,4}, x_{4,3}^2, x_{4,3}x_{4,4}, x_{4,4}^2\}$ and standard monomials $SM = \{1, x_{3,3}, x_{3,4}, x_{4,3}, x_{4,4}, x_{3,3}x_{4,4}\}$. Since $|SM| = 6$, the affine variety $V(I_G)$ consists of 6 points $P_k = (x_{2,2}^{(k)}, x_{2,3}^{(k)}, x_{2,4}^{(k)}, x_{3,2}^{(k)}, x_{3,3}^{(k)}, x_{3,4}^{(k)}, x_{4,2}^{(k)}, x_{4,3}^{(k)}, x_{4,4}^{(k)})$, $1 \leq k \leq 6$, as well. These points

$$\begin{cases} P_1 = (-1,-1,1,-1,1,-1,1,-1,-1), \\ P_2 = (-1,1,-1,-1,-1,1,1,-1,-1), \\ P_3 = (-1,-1,1,1,-1,-1,-1,1,-1), \\ P_4 = (1,-1,-1,-1,-1,1,-1,1,-1), \\ P_5 = (-1,1,-1,1,-1,-1,-1,-1,1), \\ P_6 = (1,-1,-1,-1,1,-1,-1,-1,1), \end{cases}$$

provide the 6 normalized cocyclic Hadamard matrices over $\mathbb{Z}_2^2$, consisting of 3×3 cores with exactly one positive entry at each row i and at each column j, $2 \leq i, j \leq 4$. ◁

As a matter of fact, running the procedure `CocGM(t, G, opt)` in our computer system, the computation of the reduced Gröbner bases of the ideals related to the group $\mathbb{Z}_t \times \mathbb{Z}_2^2$ and the dihedral group D_{4t} are only feasible for $t \leq 3$ (see Table 1). Unfortunately, for higher orders, the system runs out of memory, and some new insight is needed to improve the method.

In Section 3 we define another ideal J_G for computing $\mathcal{H}_G$ in a more subtle way, based on the previous work of Álvarez et al. (2008). Unfortunately, it will still be extremely hard to compute $\mathcal{H}_G$ for large $|G|$. Nevertheless, taking advantage of the properties of cocyclic matrices over D_{4t} and $\mathbb{Z}_t \times \mathbb{Z}_2^2$ described by Álvarez et al. (2015, 2016), this ideal J_G may be specifically simplified for computing $\mathcal{H}_{D_{4t}}$ and $\mathcal{H}_{\mathbb{Z}_t \times \mathbb{Z}_2^2}$ in a better way.

3. Ideals built from a basis for G-cocycles

In order to reduce the complexity of the computation of the reduced Gröbner basis that has been described in the previous section, we consider a new zero-dimensional radical ideal J_G related to the set $\mathcal{H}_G$, where we diminish the number of variables and the maximal degree of the polynomials. For this purpose, what is needed is just knowing an explicit basis for cocycles over G, which the methods of Horadam and de Launey (1995); Flannery (1996); Flannery and O'Brien (2000); Flannery and Egan (2015); Álvarez et al. (2009) provide.

Let G be a multiplicative finite group of order $4t$, $\mathbf{B} = \{\psi_1, \ldots, \psi_k\}$ be a basis for normalized cocycles over G and ψ be a normalized cocycle over G of coordinates $(x_1, \ldots, x_k)_{\mathbf{B}}$ with regards to $\mathbf{B}$,

so that $\psi = \psi_1^{x_1} \cdots \psi_k^{x_k}$, for some $x_i \in \{0,1\}$, $1 \leq i \leq k$. Let $m_{i,j}^d$ denote the (i,j)th entry of M_{ψ_d}, so that the (i,j)th entry of M_ψ is $(m_{i,j}^1)^{x_1} \cdots (m_{i,j}^k)^{x_k}$. Recall that cocyclic Hadamard matrices are precisely those matrices that are built up from Hadamard rows (excepting the first row, consisting all of 1s). In these circumstances, the ith-row of the previous matrix M_ψ is Hadamard if and only if

$$\sum_{j=1}^{4t} (m_{i,j}^1)^{x_1} \cdots (m_{i,j}^k)^{x_k} = 0.$$

The next result holds.

Theorem 4 *(Álvarez et al. (2008)). The matrix M_ψ is Hadamard if and only if the vector of coordinates $(x_1, \ldots, x_k)_{\mathbf{B}}$ of ψ with regards to $\mathbf{B}$ satisfies the following system of $4t-1$ equations and k unknowns*

$$\begin{cases} (m_{2,1}^1)^{x_1} \ldots (m_{2,1}^k)^{x_k} + \ldots + (m_{2,4t}^1)^{x_1} \ldots (m_{2,4t}^k)^{x_k} & = 0 \\ & \vdots \\ (m_{4t,1}^1)^{x_1} \ldots (m_{4t,1}^k)^{x_k} + \ldots + (m_{4t,4t}^1)^{x_1} \cdots (m_{4t,4t}^k)^{x_k} & = 0 \end{cases} \tag{3}$$

The solutions of the system (3) constitute precisely the whole set of normalized cocyclic Hadamard matrices over G. Trying to solve this system may be as complicated as performing an exhaustive search for cocyclic Hadamard matrices over G. Instead, we intend to translate the system (3) in terms of a set of nonlinear $\mathbb{Q}[X]$-polynomial equations over the set of variables $\{X\} = \{x_1, \ldots, x_k\}$ (whose $0,1$ values are related to the coordinates of G-cocycles with regards to $\mathbf{B}$), and to study the structure of the associated ideal.

A succinct algebraic description of the quadratic constraints $\{X\} \subset \{0,1\}^k$ is provided by the following set of k algebraic equations:

$$x_i(x_i - 1) = 0, \quad \text{for all } i \in \{1, \ldots, k\}. \tag{4}$$

In order to define the rest of polynomial equations that arise from the system (3), we use the next two main ideas for simplifications:

- From a practical point of view, we may assume we work with a fixed representative cocycle ρ among all of the possible choices of representative cocycles. In fact, empirically, in the groups most intensively studied, there always exists a choice ρ of representative cocycle that tends to be the most successful for providing Hadamard matrices. See in this regard the works of Álvarez et al. (2008, 2015, 2016), Baliga and Horadam (1995), Flannery (1997) and Horadam (2007). We will denote by $M_\rho = (r_{i,j})$ the matrix related to this representative cocycle ρ. Obviously, this pruning in the searching space leads to the circumstance that some G-cocyclic Hadamard matrices are lost (namely, if they do exist, those lying on a cocyclic equivalence class different to that of ρ). For instance, this is the case of the 1400 cocyclic Hadamard matrices over $D_{4\cdot 5}$, listed in Table 1, where 800 matrices M_ψ are missing from the total amount of 2200 $D_{4\cdot 5}$-cocyclic Hadamard matrices. If we want to find the whole set of cocyclic Hadamard matrices, we have to perform an analogous search for the other possible choices of M_ρ. In what follows we assume that $\psi_1, \ldots, \psi_{k-m} \in \mathbf{B}$ are G-coboundaries, $\psi_{k-m+1}, \ldots, \psi_k \in \mathbf{B}$ are representative G-cocycles and $\rho = \prod_{i=k-m+1}^{k} \psi_i^{x_i}$ is a fixed linear combination of these representative cocycles.
- The second property of Lemma 1 implies that the hth summand of the lth equation in (3) reduces to be $r_{l+1,h}(m_{l+1,h}^i)^{x_i}(m_{l+1,h}^j)^{x_j}$, for i and j defining the (unique) two generalized coboundaries $\overline{M}_{\partial_i}$ and $\overline{M}_{\partial_j}$ sharing a negative entry in the position $(l+1,h)$. Namely, $\{i,j\} = \{h,(l+1)h\}$. Notice that, eventually, one or even both of these coboundaries $\partial_h, \partial_{(l+1)h}$ might not be in $\mathbf{B}$.

Actually, the monomial $s_{l,h}(\mathrm{X})$ related to the aforementioned hth summand of the lth equation in (3) depends on whether the two, just one or none of the coboundaries $\partial_h, \partial_{(l+1)h}$ (precisely those whose related generalized coboundary matrices contribute a negative entry at position $(l+1,h)$) are in $\mathbf{B}$. More concretely,

- If both $\partial_h, \partial_{(l+1)h}, \in \mathbf{B}$, then

$$s_{l,h}(\mathrm{X}) := r_{l+1,h}\,(1-2x_h)(1-2x_{(l+1)h}).$$

- If just one of them is in $\mathbf{B}$, say $\{i\} = \{h, (l+1)h\} \cap \mathbf{B}$, then

$$s_{l,h}(\mathrm{X}) := r_{l+1,h}\,(1-2x_i).$$

- If both $\partial_h, \partial_{(l+1)h} \notin \mathbf{B}$, then

$$s_{l,h}(\mathrm{X}) := r_{l+1,h}.$$

Let $S_l(\mathrm{X}) := \sum_{j=1}^{4t} s_{l,j}(\mathrm{X})$ and let $\mathcal{H}_G^\rho$ be the set of solutions of (3) of the form $\psi = \rho \prod_{i=1}^{k-m} \psi_i^{x_i}$. The set $\mathcal{H}_G^\rho$ coincides with the set of solutions of the system of polynomial equations

$$\begin{cases} x_i(x_i-1) = 0, & \text{if } 1 \le i \le k-m, \\ S_l(\mathrm{X}) = 0, & \text{if } 1 \le l \le 4t-1. \end{cases}$$

Similarly to Theorem 2, the next result holds.

Theorem 5. *The set $\mathcal{H}_G^\rho$ can be identified with the set of zeros of the zero-dimensional ideal $J_G = J_G^1 + J_G^2 \subset \mathbb{Q}[X]$ consisting in the summation of the following two subideals:*

$$\begin{cases} J_G^1 = \langle\, x_i^2 - x_i :\ i \in \{1,\dots,k-m\}\,\rangle, \\ J_G^2 = \langle\, S_l(X) :\ l \in \{1,\dots 4t-1\}\,\rangle. \end{cases}$$

Moreover, $|\mathcal{H}_G^\rho| = \dim_{\mathbb{Q}}(\mathbb{Q}[X]/J_G)$.

Proof. Similarly to Theorem 2, let $P = (p_1,\dots,p_{k-m})$ be a point of the affine variety $V(J_G)$. Attending to J_G^1, every component p_i of P is either 1 or 0, for all $1 \le i \le k-m$. Let $\psi : G \times G \to \{\pm 1\}$ be defined such that

$$\psi = \rho \prod_{i=1}^{k-m} \psi_i^{x_i}.$$

Since J_G^2 implies by construction that M_ψ satisfies (4), the point P can be identified with the cocyclic Hadamard matrix M_ψ related to ψ. The affine variety $V(J_G)$ coincides, therefore, with the set $\mathcal{H}_G$, whose finiteness involves the ideal J_G to be zero-dimensional.

Besides, since $J_G \cap \mathbb{Q}[x_i] = \langle\, x_i^2 - x_i \,\rangle \subseteq J_G$ for all $1 \le i \le k-m$ and all these polynomials are square-free, Proposition 2.7 of Cox et al. (1998) implies that

$$\sqrt{J_G} = J_G + \sum_i J_G \cap \mathbb{Q}[x_i] = J_G,$$

so J_G is therefore radical. And hence, $|\mathcal{H}_G^\rho| = |V(J_G)| = \dim_{\mathbb{Q}}(\mathbb{Q}[X]/J_G)$. □

Notice that, as defined, the ideal J_G is generated by $O(t)$ polynomials of degree up to 2 over the set of $O(t)$ variables $\{x_1,\dots,x_{k-m}\}$. Observe in particular that, according to Lakshman and Lazard, the

Table 1
Running times related to *CocGM* and *CocCB*.

t	$\lvert\mathcal{H}^{\rho}_{\mathbb{Z}_t\times\mathbb{Z}_2^2}\rvert$	Running time in seconds		$\lvert\mathcal{H}^{\rho}_{D_{4t}}\rvert$	Running time in seconds	
		CocGM	*CocCB*		*CocGM*	*CocCB*
1	6	0 (0)	0 (0)	6	0 (0)	0 (0)
3	24	102 (4255)	0 (0)	72	–	0 (0)
5	120	–	7 (93)	1400	–	11 (5826)
7	–	–	–	7488	–	52282 (–)

complexity of the computation of the reduced Gröbner decreases from $2^{O(t^2)}$ in Theorem 2 to $2^{O(t)}$ in Theorem 5.

The procedure `CocCB(t, G, opt)` (included in the library *hadamard.lib* as well) provides an implementation of this method. It is specifically designed for the group $\mathbb{Z}_t \times \mathbb{Z}_2^2$ (taking $G = 1$ as input and using (5) as the representative cocycle ρ) and the dihedral group D_{4t} (taking $G = 2$ as input and using (6) as the representative cocycle ρ), though it might be straightforwardly modified to fix for any other group G. It would suffice to actualize the polynomials $S_l(X)$, attending to the particular group law of G and the corresponding representative cocycle ρ. Once again, depending on whether the parameter `opt` is equal to 1 or 2, the procedure calculates either just the number of cocycle Hadamard matrices over G or the explicit full set of these matrices.

In order to check the efficiency of this alternative, the procedure has been tested in the computation of the number of cocycle Hadamard matrices developed over the group $\mathbb{Z}_t \times \mathbb{Z}_2^2$ and the dihedral group D_{4t} of order $4t$. Running times to compute this number on our computer system are exposed in Table 1, where we also indicate in parentheses the running time that is required to determine the explicit full set of matrices.

Notice that although there are actually 2200 cocycle Hadamard matrices over $D_{4\cdot 5}$, just 1400 of them lies on the cocycle equivalence class $[\rho]$ of ρ as defined in (6) (see Álvarez et al. (2008) for details). This explains the output of the procedure, which limits to compute those cocycle Hadamard matrices lying on the cocycle equivalence class of $[\rho]$. Anyway, this is not a source of problems as we commented before, since this case seems to provide most of the D_{4t}-cocycle Hadamard matrices known so far (see Flannery (1997); Álvarez et al. (2008, 2016)).

Actually, this procedure `CocCB(t, G, opt)` might be improved if a deeper knowledge about the inner structure of cocycle matrices over G is known. In particular, building on the works of Álvarez et al. (2015, 2016), we have been able to design two specific procedures for looking for $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocycle Hadamard matrices and D_{4t}-cocycle Hadamard matrices, so that larger cocycle Hadamard matrices (up to $t \leq 39$) are obtained. The details are described in the next two subsections.

3.1. The group $\mathbb{Z}_t \times \mathbb{Z}_2^2$

Let G be the abelian group $\mathbb{Z}_t \times \mathbb{Z}_2^2 = \langle a, b, c : a^t = b^2 = c^2 = 1\rangle$, $t > 1$ odd, with ordering

$$\{1, c, b, bc, a, ac, ab, abc, \ldots, a^{t-1}, a^{t-1}c, a^{t-1}b, a^{t-1}bc\},$$

indexed as $\{1, \ldots, 4t\}$. A basis $\mathbf{B} = \{\partial_2, \ldots, \partial_{4t-2}, \beta_1, \beta_2, \beta_3\}$ for cocycles over G is described by Álvarez et al. (2008, 2009), and consists of $4t - 3$ coboundaries and three representative cocycles. As usual, ∂_i refers to the coboundary associated to the ith-element in G. An explicit description of these cocycles may be found in Álvarez et al. (2008). Notice that all cocycle Hadamard matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$ known so far use all the three representative cocycles β_1, β_2 and β_3 simultaneously (see the paper of Baliga and Horadam (1995) for details). Thus, we assume

$$M_\rho = 1_t \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix} \tag{5}$$

and hence, we restrict (4) to the equations related to the $4t-3$ coboundaries, that is,

$$x_i(x_i-1)=0, \quad \text{for all } i\in\{1,\dots,4t-3\}.$$

Let us point out that the system (3) is equivalent to the one built up with the equations from the 4th to the $(2t+1)$th (see the works of Álvarez et al. (2008, 2015)). So, we have only $2t-2$ polynomials of the form $S_l(\mathrm{X})=s_{l,1}(\mathrm{X})+\ldots+s_{l,4t}(\mathrm{X})$. In order to describe an explicit expression for the monomials $s_{l,h}(\mathrm{X})$, we state the following lemma.

Lemma 6. *Given the position (s,c) with $5\le s\le 2t+2$ and $1\le c\le 4t$, the two generalized coboundary matrices with entries -1 at the position (s,c) are $\overline{M}_{\partial_c}$ and $\overline{M}_{\partial_{j(s,c)}}$ where*

$$j(s,c):=1+4\left(\left\lfloor\frac{s-1}{4}\right\rfloor+\left\lfloor\frac{c-1}{4}\right\rfloor \bmod t\right)+$$
$$2\left(\left\lfloor\frac{s-1 \bmod 4}{2}\right\rfloor+\left\lfloor\frac{c-1 \bmod 4}{2}\right\rfloor \bmod 2\right)+(s+c \bmod 2).$$

Proof. On one hand, attending to the choices of presentation and ordering of G described above, any $1\le s\le 4t$ in G may be expressed uniquely as $g_s=a^{s_a}b^{s_b}c^{s_c}$ in terms of the generators a,b,c of the given presentation of the group, for $s_a=\lfloor\frac{s-1}{4}\rfloor$, $s_b=\lfloor\frac{(s-1) \bmod 4}{2}\rfloor$ and $s_c=(s-1) \bmod 2$. Reciprocally, the group element $g_s=a^ib^jc^k$ corresponds to the element $s=1+4i+2j+k$ in the given ordering.

On the other hand, as pointed out in the second property of Lemma 1, the indices of the two generalized coboundary matrices which share a negative entry at the position (s,c) are c and $j(s,c)$, for $g_{j(s,c)}=g_s\cdot g_c$, for $1\le s,c\le 4t$ in G. Now the lemma follows straightforwardly. □

Taking into account this lemma and the basis $\mathbf{B}$ of cocycles, we compute the monomials

$$s_{l,h}(\mathrm{X}):=r_{l+4,h}\,(1-2x_{h-1})^{\chi_{\mathbf{B}}(h)}\,(1-2x_{j(l+4,h)-1})^{\chi_{\mathbf{B}}(j(l+4,h))},$$

for $1\le l\le 2t-2$ and $1\le h\le 4t$, where

$$\chi_{\mathbf{B}}(i):=\begin{cases}1, & \text{if } \partial_i\in\mathbf{B},\\ 0, & \text{otherwise.}\end{cases}$$

In these circumstances, Theorem 5 reads as follows.

Theorem 7. *The set $\mathcal{H}^{\rho}_{\mathbb{Z}_t\times\mathbb{Z}_2^2}$ can be identified with the set of zeros of the following zero-dimensional ideal of $\mathbb{Q}[X]$.*

$$J_{\mathbb{Z}_t\times\mathbb{Z}_2^2}:=\langle\, x_i^2-x_i:\ i\in\{1,\dots,4t-3\}\,\rangle+\langle\sum_{h=1}^{4t}s_{l,h}(X):\ l\in\{4,\dots 2t+1\}\,\rangle.$$

Besides, $|\mathcal{H}^{\rho}_{\mathbb{Z}_t\times\mathbb{Z}_2^2}|=\dim_{\mathbb{Q}}(\mathbb{Q}[X]/J_{\mathbb{Z}_t\times\mathbb{Z}_2^2})$.

Actually, some additional assumptions, as those described in Álvarez et al. (2015), may be considered. Coboundaries ∂_i on $\mathbb{Z}_t\times\mathbb{Z}_2^2$-cocyclic Hadamard matrices

$$M_\psi=M_\rho\prod_{i\in I}M_{\partial_i}$$

are somehow symmetrically distributed, in the sense that the relation $4k+j\in I\Leftrightarrow 4t-4k+j\in I$, $1\le k\le\frac{t-1}{2}$, $1\le j\le 4$, holds. Furthermore, the number c_k of coboundaries of each subset $\{4k+j\in I:\ 1\le j\le 4\}$, for a fixed $2\le k\le t$, satisfies $c_1-c_k\equiv 1 \bmod 2$. And the number r_j of coboundaries

Table 2
Auxiliary matrix method related to the group $\mathbb{Z}_t \times \mathbb{Z}_2^2$.

t	col	dist	Initial coboundaries	Running time in seconds	Final coboundaries
3	4	2,2,2,2	–	0	4FC
5	2,2	2,2,2,2	–	0	43CC0
7	0,2,2	2,2,2,2	–	0	203CC30
9	0,2,2,2	2,2,4,4	–	0	E0A7546A
11	2,2,2,2,0	4,6,2,4	–	0	2C65900956C
13	1,3,3,1,1,1	8,4,4,4	–	0	54BE818818EB4
15	1,3,3,3,1,3,1	10,4,8,8	–	5	64BB78B88B87BB4
17	1,3,3,3,1,1,1,1	8,6,4,10	–	16	68D7D21188112D7D8
19	0,4,2,0,2,2,2,2,2	6,8,8,10	–	23	10FC0A35355353A0CF0
21	0,0,4,0,2,2,2,0,2,4	8,8,8,8	–	0	400F033C0CFFC0C330F00
23	1,1,3,3,3,1,3,1,3,3,1	8,14,12,12	6	22508	689CFA564FA23AE565AFC88
25	2,2,2,2,4,2,2,2,2,0,2,2	14,14,8,12	9,12,14,16,18	6844	392ABF4B8C153340D8B5EAB3
27	1,3,3,1,3,3,3,1,3,1,1,1,1	16,8,14,12	19,26,41,47,49	3651	58EB2E7B1D82811828D1B7E2BE8
29	1,1,3,1,1,1,3,1,3,3,3,3,3,1	14,12,18,12	5,9,18,23	17004	6887428B27B7BE44EB7B72B824788
31	0,4,2,4,2,2,2,2,0,2,2,0,4,2,2	12,18,18,12	14,15,21	12614	10F6F96990660F6666F06609969F6F0
33	2,4,2,2,2,2,2,2,2,2,0,2,0,2,2	12,18,14,16	5,6,14,18,19,22,24,25,27,29,32,35	13392	4CF565A93AC506035530605CA39A565FC
37	0,2,4,4,2,2,4,2,2,2,0,2,2,2,2,2,2,2	22,14,20,20	9,11,23,24,25,26,33,34,37,39	12325	70AFF3CFCAA09396593395693 90AACFC3FFA0
39	0,0,2,4,2,2,2,2,4,2,2,2,2,2,4,2,2,2,4	24,22,22,16	13,14,23,24,25,27,30,32,33,35,41,42	1653	100CF3A5AFCCA6AF53CFFC35FA6ACCFA5A3FC00

of each subset $\{4k + j \in I : 1 \le k \le t\}$, for $1 \le j \le 4$, give rise to a tuple $dist = (r_1, r_2, r_3, r_4)$ (termed *distribution* by Álvarez et al. (2015)) which certainly satisfies some additional properties.

Any $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic matrix $M_\psi = M_\rho \prod_{i \in I} M_{\partial_i}$ may be uniquely identified as a $(4 \times t)$ binary matrix $D_\psi = (d_{jk})$ (termed *diagram* by Álvarez et al. (2015)), such that $d_{jk} = 1$ if and only if $4(k-1) + j \in I$. The conditions described above have a straightforward translation in terms of D_ψ. More concretely,

- column i of D_ψ is equal to column $t + 2 - i$, for $2 \le i \le \frac{t+1}{2}$;
- the sum of column $2 \le j \le t$ of D_ψ is of different parity of that of column 1 of D_ψ;
- the sum of each row of D_ψ gives the distribution $dist = (r_1, r_2, r_3, r_4)$.

Thus the method may be improved, as soon as the distribution *dist* and the number of coboundaries per column $col = (c_2, \ldots, c_{\frac{t+1}{2}})$ are provided. We have implemented this method as a SINGULAR procedure called `CocAH(t, col, dist, H)`. Since exhaustive calculations are not feasible for $t \ge 11$, we have included in this procedure a new parameter $H = (x_1, \ldots, x_{2t+1})$, which determines which coboundaries are fixed ($x_i = 1$ means ∂_{i+1} is used, whereas $x_i = 0$ implies ∂_{i+1} is not used), and which of them are unknowns to be settled in the search (those corresponding to values $x_i = 2$). The procedure outputs the set of cocyclic Hadamard matrices meeting these constraints, if any exist.

Running the procedure on our computer system, after many attempts and essaying with different parameters, we have been able to find some $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard, up to $t \le 39$, as Table 2 shows. The latter are written row after row, where each row is represented by three digits in hexadecimal form. To this end, after replacing each -1 by 0, the resulting row in binary form is translated to its equivalent hexadecimal form, in such a way that every possible nibble (group of 4 bits) from 0000 to 1111 is encoded as its corresponding hexadecimal digit from 0 to F, as usual.

Notice that there is no example for $t = 35$. As explained in Álvarez et al. (2015), $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices of the type we are looking for (using the representative cocycle ρ as described in (5)), are in one to one correspondence with the Williamson Hadamard matrices, which are known not to exist on order $t = 35$ among others (see Holzmann et al. (2008) for details).

3.2. The dihedral group D_{4t}

Let G be the dihedral group $D_{4t} = \langle a, b : a^{2t} = b^2 = 1, bab = a^{-1} \rangle$ with ordering

$$\{1, a, \ldots, a^{2t-1}, b, ab, \ldots, a^{2t-1}b\},$$

indexed as $\{1, \ldots, 4t\}$. A basis $\mathbf{B}$ for cocycles over G is explicitly described by Álvarez et al. (2008, 2009). For $t > 2$, the basis consists of $4t - 3$ coboundaries ∂_k and three representative cocycles β_i,

so that $\mathbf{B} = \{\partial_2, \ldots, \partial_{4t-2}, \beta_1, \beta_2, \beta_3\}$. In the sequel we assume $t > 2$. Flannery (1997) observed that cocyclic Hadamard matrices over D_{4t} mostly use $\beta_2 \cdot \beta_3$ and do not use β_1. So, we assume

$$M_\rho = M_{\beta_2} \cdot M_{\beta_3} = \begin{pmatrix} A & A \\ B & -B \end{pmatrix}, \tag{6}$$

for $2t \times 2t$ matrices $A = (a_{i,j})$ and $B = (b_{i,j})$ such that $a_{i,j} = \begin{cases} 1, & \text{if } j < 2t+2-i, \\ -1, & \text{otherwise.} \end{cases}$ and $b_{i,j} = \begin{cases} 1, & \text{if } j \le i, \\ -1, & \text{otherwise.} \end{cases}$

Therefore, in this case, (4) is rewritten as

$$x_i(x_i - 1) = 0, \quad \text{for all } i \in \{1, \ldots, 4t-3\}.$$

According to Álvarez et al. (2008), the last $3t$ equations in the system (3) are superfluous for D_{4t}-cocyclic Hadamard matrices. So, we have only $t-1$ polynomials of the form $S_l = s_{l,1} + \ldots + s_{l,4t}$, $1 \le l \le t-1$. In order to describe an explicit expression for the monomials $s_{l,h}(X)$, we state the following lemma.

Lemma 8. *The two generalized coboundary matrices with entries -1 in a position $(s,c) \in \{2, \ldots, t\} \times \{1, \ldots, 4t\}$ are $\overline{M}_{\partial_c}$ and $\overline{M}_{\partial_{j(s,c)}}$, where*

$$j(s,c) = 1 + (s + c - 2 \bmod 2t) + 2t\lfloor \frac{c-1}{2t} \rfloor.$$

Proof. On one hand, attending to the choices of presentation and ordering of G described above, any $1 \le s \le 4t$ in G may be expressed uniquely as $g_s = a^{s_a} b^{s_b}$ in terms of the generators a, b of the given presentation of the group, for $s_a = s - 1 \bmod 2t$ and $s_b = \lfloor \frac{s-1}{2t} \rfloor$. Reciprocally, the group element $g_s = a^i b^j$ corresponds to the element $s = 1 + i + 2tj$ in the given ordering.

On the other hand, as pointed out in the second property of Lemma 1, the indices of the two generalized coboundary matrices which share a negative entry at the position (s,c) are c and $j(s,c)$, for $g_{j(s,c)} = g_s \cdot g_c$, for $1 \le s, c \le 4t$ in G. Now the lemma follows straightforwardly. □

Taking into account this lemma and the basis of cocycles $\mathbf{B}$, an explicit description of the monomials $s_{l,h}$ consists in

$$s_{l,h} := r_{l+1,h} \, (1 - 2x_{h-1})^{\chi_{\mathbf{B}}(h)} \, (1 - 2x_{j(l+1,h)-1})^{\chi_{\mathbf{B}}(j(l+1,h))},$$

for $1 \le l \le t-1$ and $1 \le h \le 4t$. In these circumstances, Theorem 5 reads as follows.

Theorem 9. *The set $\mathcal{H}^{\rho}_{D_{4t}}$ can be identified with the set of zeros of the following zero-dimensional ideal of $\mathbb{Q}[X]$.*

$$J_{D_{4t}} := \langle x_i^2 - x_i : \ 1 \le i \le 4t-3 \rangle + \langle \sum_{h=1}^{4t} s_{l,h}(X) : \ 1 \le l \le t-1 \rangle.$$

Besides, $|\mathcal{H}^{\rho}_{D_{4t}}| = \dim_{\mathbb{Q}}(\mathbb{Q}[X]/J_{D_{4t}})$.

We have implemented this method as a SINGULAR procedure called `CocDH(t, dist, opt, H)`. As before, the parameter *opt* indicates whether to compute the cardinality or the full set $\mathcal{H}^{\rho}_{D_{4t}}$ of D_{4t}-cocyclic matrices. And the auxiliary parameter $H = (x_1, \ldots, x_{4t-3})$ once again determines which coboundaries are fixed ($x_i = 1$ means ∂_{i+1} is used, whereas $x_i = 0$ implies ∂_{i+1} is not used), and which of them are unknowns to be settled in the search (those corresponding to values $x_i = 2$).

Table 3
Auxiliary matrix method related to the group D_{4t}.

t	*dist*	Initial coboundaries	Running time in seconds	Final coboundaries
3	2,2	-	0	774
5	2,2,2,2	-	0	5D798
7	2,2,0,2,0,2	-	0	472E4A0
9	1,2,3,2,3,3,3,4	-	0	4FB3AF4F4
11	2,2,1,3,1,3,1,2,3,2	-	29	47942777A2C
13	1,2,2,2,3,1,1,2,1,1,4,2	-	20	703BBDA249518
15	1,1,0,1,1,3,1,1,3,3,3,1,3,2	-	308	6E7DCCA16A9A08
17	1,2,1,2,2,2,0,0,3,0,2,3,2,2,2,2	-	1477	44343445C42F44938
19	1,0,3,1,2,1,1,2,3,2,2,2,1,3,2,3,3,4	6,36,42	2591	25876E0A44EBD737D04
21	2,1,3,1,3,3,0,3,2,1,0,2,3,3,3,3,2,1,1,2	3,6,41,81	3903	91B8A9E69EB33ED0A0BC
23	1,2,3,0,3,3,3,3,1,3,3,2,0,3,2,2,2,2,2,1,2,1,2	3,6,7,8,38,45,88	15248	48668F0A9FD3BDD146DC8E4
25	1,1,4,3,2,2,3,2,2,2,2,1,2,3,4,3,2,3,1,2,2,0,2,1	7,12,47,50,52,66,82,83	12894	3437D0D4FCBD5EEB9045CC34C
27	0,1,3,3,3,1,2,2,3,0,2,3,2,2,4,0,2,0,2,1,1,2,1,2,4,2	4,6,43,50,63,75,86	17226	2EBEA5DE050438EC782296C4D98
29	2,3,0,1,2,1,4,1,2,2,1,1,4,2,3,1,3,2,3,3,2,0,2,1,1,2,2,1	11,19,35,51,53,62,73,83,89	15918	422ECA4033547CF4B33C2BE1CDA50
31	1,1,2,2,3,3,2,3,0,1,0,4,2,2,3,2,3,2,2,0,0,3,1,1,2,1,3,2,2,3	5,6,17,36,48,63,64,84,95,115,117	19702	21172424E984E2E3FC6B06D5527CA70
33	1,2,3,2,3,1,2,1,2,1,3,1,4,3,2,2,1,2,2,3,2,1,3,3,2,3,2,3,1,2,1,2	3,28,31,38,56,59,62,66,72,77,78,83,88	22180	5A2D1A6666661BC21CFBFA5D41AFDE1514
35	2,0,3,1,2,1,1,3,3,2,2,2,2,4,3,2,2,3,0,2,3,3,0,2,3,1,1,1,2,1,2,2,2,3	6,7,9,44,45,53,107,111,113, 119,120,137,138	28447	276EDC8AEF1EC38456867D34250290B2F98
37	1,2,4,3,1,2,3,2,3,2,3,2,2,3,2,1,2,2,2,2,1,2,2,2,2,2,1,2,3,3,2,2,2,2,2,1	36,45,46,64,75,78,79,81,90,95,135,140	24382	73A6D3FF5982AB0E7B3A3B5A83281F1214E6C
39	2,1,2,2,1,3,1,4,3,1,2,1,2,2,2,3,1,2,2,2,3,2,1,2,0,1,3,0,0,1,3,2,3,2,2,1,4,3	5,9,10,38,43,56,58,72,80,84,94,95,124,126,127	29281	D617D23BBCD1123D7A78603300AB32A694F9AC

Additionally, beyond the help list H, in order to improve the process of calculating a D_{4t}-cocyclic Hadamard matrix one may impose some extra constraints by means of an initial distribution $dist = (d_2, \ldots, d_t)$ concerning to the number d_l of coboundaries which give an *intersection* (as termed in Álvarez et al. (2008)) at row l for the first time, $2 \leq l \leq t$. Actually, attending to the work in Álvarez et al. (2016), this translates to some extra polynomial constraints of the kind $d_2 = x_{2t-1} + x_{2t}$, $d_3 = x_1 + x_{2t-2} + x_{2t+1}$ and $d_l = x_{l-2} + x_{2t-l+1} + x_{2t+l-2} + x_{4t-l+1}$, $4 \leq l \leq t$, for some prefixed values d_l, $0 \leq d_2 \leq 2$, $0 \leq d_3 \leq 3$ and $0 \leq d_l \leq 4$, for $4 \leq l \leq t$.

The procedure outputs the set of D_{4t}-cocyclic Hadamard matrices meeting these constraints, if any exist. Running the procedure on our computer system, after many attempts and essaying with different parameters, we have been able to find some D_{4t}-cocyclic Hadamard matrices, up to $t \leq 39$, as Table 3 shows. In the table, those initial coboundaries that are not permitted to be used are underlined, and the matrices are written once again row after row in hexadecimal form.

Although some work has been done, there is still no way to know which vectors $H = (x_1, \ldots, x_{4t-3})$ and $dist = (d_2, \ldots, d_t)$ are suitable for providing large D_{4t}-cocyclic Hadamard matrices. Getting an example for the case $t = 47$ should be the main concern in the short term, as it is the smallest order for which no cocyclic Hadamard matrix is known yet (see Horadam (2007)).

4. Conclusions and further work

By means of various techniques in Algebraic Geometry, this paper has been concerned with the computation of cocyclic Hadamard matrices over a fixed group G of order $4t$, as the affine varieties of certain zero-dimensional radical ideals. All the procedures that are described in the paper have been implemented in the open computer algebra system for polynomial computations SINGULAR and are included in the library *hadamard.lib*, which is available online at `http://personales.us.es/raufalgan/LS/hadamard.lib`.

Based on the classic cocyclic test of Horadam and de Launey (1995), our first approach (Theorem 2) has excessive complexity even for very small t. In order to improve the efficiency of this polynomial method, we have used recent results on the inner structure of a cocyclic matrix and we have defined a different ideal that also characterizes the set of G-cocyclic Hadamard matrices (Theorem 5). Improved versions of this procedure (`CocAH(`$t, col, dist, H$`)` and `CocDH(`$t, dist, opt, H$`)`, based on Theorems 7 and 9, respectively) have been used to perform local searches for $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices and D_{4t}-cocyclic Hadamard matrices, so that matrices of order up to $4t \leq 156$ have been found. To this end, an auxiliary list H is needed to perform these local searches, for $t \geq 11$ (an exhaustive search is only feasible for $t < 11$). More concretely, the list H indicates which coboundaries are fixed (either used or not), and which of them are considered unknowns to be settled. A very interesting future work is trying to characterize if there exist some types of structures for H such that the existence of cocyclic Hadamard matrices over either $\mathbb{Z}_t \times \mathbb{Z}_2^2$ or D_{4t} is predicted.

Acknowledgements

The authors want to express their gratitude to the anonymous referees for their pertinent comments and suggestions, which have permitted to improve the readability and understandability of the paper. This work was made possible by the facilities of the *Centro Informático Científico de Andalucía* (CICA) and *Instituto de Matemáticas de la Universidad de Sevilla* (IMUS), which provided access to the computer server AnonIMUS915, consisting in an *AMD Opteron 6348, with a 2.8 GHz processor (48 cores), 256 GB RAM and 3 TB Hard Drive*. All authors are partially supported by the research project FQM-016 from Junta de Andalucía (JJAA).

References

Álvarez, V., Armario, J.A., Falcón, R.M., Frau, M.D., Gudiel, F., Güemes, M.B., 2017. Cocyclic structured hadamard matrices. Preprint.

Álvarez, V., Armario, J.A., Frau, M.D., Gudiel, F., Güemes, M.B., Osuna, A., 2016. On D_{4t}-cocyclic Hadamard matrices. J. Comb. Des. 24 (8).

Álvarez, V., Armario, J.A., Frau, M.D., Real, P., 2008. A system of equations for describing cocyclic Hadamard matrices. J. Comb. Des. 16 (4), 276–290.

Álvarez, V., Armario, J.A., Frau, M.D., Real, P., 2009. The homological reduction method for computing cocyclic Hadamard matrices. J. Symb. Comput. 44 (5), 558–570.

Álvarez, V., Gudiel, F., Güemes, M.B., 2015. On $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices. J. Comb. Des. 23 (8), 352–368.

Baliga, A., Horadam, K.J., 1995. Cocyclic Hadamard matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$. Australas. J. Comb. 11, 123–134.

Bayer, D., Stillman, M., 1992. Computation of Hilbert functions. J. Symb. Comput. 14 (1), 31–50.

Bosma, W., Cannon, J., Playoust, C., 1997. The Magma algebra system. I. The user language. In: Computational Algebra and Number Theory, London, 1993. J. Symb. Comput. 24 (3–4), 235–265.

Buchberger, B., 2006. An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. J. Symb. Comput. 41 (3–4), 475–511.

Cox, D.A., Little, J.B., O'Shea, D., 1998. Using Algebraic Geometry. Springer-Verlag, New York.

Cox, D.A., Little, J.B., O'Shea, D., 2007. Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer, New York.

De Launey, W., Flannery, D.L., 2011. Algebraic Design Theory. Mathematical Surveys and Monographs. American Mathematical Society.

Decker, W., Greuel, G.-M., Pfister, G., Schönemann, H., 2016. Singular 4-0-2 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de.

Đokovic, D.Ž., Golubitsky, O., Kotsireas, I.S., 2014. Some new orders of Hadamard and skew-Hadamard matrices. J. Comb. Des. 22 (6).

Flannery, D.L., 1996. Calculation of cocyclic matrices. J. Pure Appl. Algebra 112 (2), 181–190.

Flannery, D.L., 1997. Cocyclic Hadamard matrices and Hadamard groups are equivalent. J. Algebra 192 (2), 749–779.

Flannery, D.L., Egan, R., 2015. On linear shift representations. J. Pure Appl. Algebra 219 (8), 3482–3494.

Flannery, D.L., O'Brien, E.A., 2000. Computing 2-cocycles for central extensions and relative difference sets. Commun. Algebra 28 (4), 1939–1955.

Fletcher, R.J., Gysin, M., Seberry, J., 2001. Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices. Australas. J. Comb. 23.

Goethals, J.M., Seidel, J.J., 1967. Orthogonal matrices with zero diagonal. Can. J. Math. 19.

Hashemi, A., 2009. Nullstellensätze for zero-dimensional Gröbner bases. Comput. Complex. 18 (1), 155–168.

Hashemi, A., Lazard, D., 2011. Sharper complexity bounds for zero-dimensional Gröbner bases and polynomial system solving. Int. J. Algebra Comput. 21 (5), 703–713.

Hillebrand, D., 1999. Triangulierung nulldimensionaler ideale — implementierung und vergleich zweier algorithmen. Master's thesis. Universitaet Dortmund, Fachbereich Mathematik.

Holzmann, W.H., Kharaghani, H., Tayfeh-Rezaie, B., 2008. Williamson matrices up to order 59. Des. Codes Cryptogr. 46 (3), 343–352.

Horadam, K.J., 2007. Hadamard Matrices and Their Applications. Princeton University Press, Princeton, NJ.

Horadam, K.J., de Launey, W., 1995. Generation of cocyclic Hadamard matrices. Math. Appl. 325, 279–290.

Kotsireas, I.S., Koukouvinos, C., Seberry, J., 2006a. Hadamard ideals and Hadamard matrices with circulant core. J. Comb. Math. Comb. Comput. 57, 47–63.

Kotsireas, I.S., Koukouvinos, C., Seberry, J., 2006b. Hadamard ideals and Hadamard matrices with two circulant cores. Eur. J. Comb. 27 (5), 658–668.

Lakshman, Y.N., 1991. A single exponential bound on the complexity of computing Gröbner bases of zero-dimensional ideals. In: Effective Methods in Algebraic Geometry. Castiglioncello, 1990. In: Prog. Math., vol. 94. Birkhäuser Boston, Boston, MA, pp. 227–234.

Lakshman, Y.N., Lazard, D., 1991. On the complexity of zero-dimensional algebraic systems. In: Effective Methods in Algebraic Geometry. Castiglioncello, 1990. In: Prog. Math., vol. 94. Birkhäuser Boston, Boston, MA, pp. 217–225.

Lazard, D., 1992. Solving zero-dimensional algebraic systems. J. Symb. Comput. 13 (2), 117–131.

Mac Lane, S., 1995. Homology, reprint of the 1975 edition. Classics in Mathematics. Springer-Verlag, Berlin.

Möller, H.M., 1993. On decomposing systems of polynomial equations with finitely many solutions. Appl. Algebra Eng. Commun. Comput. 4 (4), 217–230.
Mora, F., Möller, H.M., 1983. The computation of the Hilbert function. In: Computer Algebra. London, 1983. In: Lect. Notes Comput. Sci., vol. 162. Springer, Berlin, pp. 157–167.
Orrick, W.P., 2008. Switching operations for Hadamard matrices. SIAM J. Discrete Math. 22 (1).
Seberry, J., Yamada, M., 1992. Hadamard matrices, sequences, and block designs. In: Dinitz, J.H., Stinson, D.R. (Eds.), Contemporary Design Theory: A Collection of Surveys. Wiley, New York. Chapter 11.