Shift-equivalence and cocyclic self-dual codes

A. Rao [1] [2]

Abstract

In the theory of cocyclic self-dual codes three types of equivalences are encountered: cohomology or the equivalence of cocycles, Hadamard equivalence or the equivalence of Hadamard matrices and the equivalence of binary linear codes. There are some results relating the latter two equivalences, see Ozeki [12], but not when the Hadamard matrices are un-normalised.

Recently Horadam [9] discovered shift action, whereby every finite group G acts as a group of automorphisms of $Z = Z^2(G, C)$, the finite abelian group of cocycles from $G \times G \longrightarrow C$, for each abelian group C. These automorphisms fix the subgroup of coboundaries $B \leq Z$ setwise. This shift action of G on Z partitions each cohomology class of Z.

Here we show that shift-equivalent cocycles generate equivalent Hadamard matrices and that shift-equivalent cocyclic Hadamard matrices generate equivalent binary linear codes.

1 Introduction

In [1, 2, 3], the $[I, A]$ construction was used to obtain doubly-even self-dual codes from $\mathbf{Z}_2^2 \times \mathbf{Z}_t$ and D_{4t} - cocyclic Hadamard matrices for t odd, $t \leq 9$. The equivalence classes of the codes obtained from all these groups were also catalogued. The internal structure of these Hadamard matrices permitted substantial cut-downs in the search time for each code found. In addition, there was no longer any need for generating the entire matrix A before a search could take place.

While generating the self-dual codes from cocyclic Hadamard matrices it was felt that the algebraic nature of these Hadamard matrices should lend itself to the task of checking the equivalence of the self-dual codes.

Recently Horadam [9] dicovered shift action, whereby each group G acts as a group of automorphisms of $Z^2(G, C)$, the abelian group of cocycles from

[1] Formerly A. Baliga

[2] Part of this paper was presented at the invited talk at the Sixteenth Midwest Conference on Combinatorics, Cryptography and Computing, 16MCCCC, Southern Illinois University, Carbondale, Nov 7 - 9, 2002.

$G \times G \longrightarrow C$, for each choice of abelian group C. It will be shown here that cocyclic Hadamard matrices which are shift equivalent indeed generate equivalent self-dual codes.

We assume that the reader is familiar with the basic facts of the theory of Hadamard matrices, (see [8, 13, 14]) and of binary linear codes (see [11]).

A code C is *self-dual* if it equals its dual code $C^{\perp}$. A code is *doubly-even* if all codewords have weights divisible by four. A code is *singly-even* if all codewords have even weights. It is known that the minimum distance d of a self-dual, doubly-even code of length n, satisfies $d \leq 4\left[\frac{n}{24}\right] + 4$, (see [11]). C is *extremal* if this theoretical maximum is attained.

The paper is organised in the following manner: In Section 2 we explain the necessary background algebra relating to cocycles and their equivalences. Section 3 gives some background information on Hadamard matrices and describes the effect of shift equivalence on cocyclic Hadamard matrices. Section 4 details the structure of the cocyclic Hadamard matrices used to generate self-dual codes and looks at the relationship between shift-equivalent cocyclic Hadamard matrices and the self-dual codes they generate. Section 5 catalogues the self-dual codes found so far in terms of shift-equivalence classes.

2 Shift equivalence

If G is a group and C is an abelian group, a (2-dimensional, normalised) cochain is a mapping $\psi : G \times G \longrightarrow C$ satisfying $\psi(1,1) = \psi(g,1) = \psi(1,g) = 1, \ \forall g \in G$.

A cochain is a cocycle if it satisfies the cocycle equation:

$$\psi(g,h)\psi(gh,k) = \psi(g,hk)\psi(h,k) \tag{1}$$

A cocycle may be represented as a cocyclic matrix

$$M_{\psi} = [\psi(g,h)]_{g,h \in G} \tag{2}$$

once an indexing of the elements of G has been chosen.

The set $C^2(G,C)$ of all cochains from G to C forms an abelian group under pointwise multiplication and the set $Z^2(G,C)$ of all cocycles forms a subgroup. The identity $1 \in C^2(G,C)$ is the cochain which maps every element of $G \times G$ to $1 \in C$.

A cocycle is a coboundary $\partial\phi$ if there exists a set mapping $\phi : G \longrightarrow C$ with $\phi(1) = 1$ such that $\partial\phi(a,b) = \phi(a)^{-1}\phi(b)^{-1}\phi(ab)$.

The set of coboundaries $B^2(G,C)$ forms a subgroup of $Z^2(G,C)$. Two cocycles ψ and ψ' are cohomologous if there exists a coboundary $\partial\phi$ such that $\psi' = \psi\partial\phi$. Cohomology is an equivalence relation and the cohomology class of ψ is denoted by $[\psi]$. In particular, $[1] = B^2(G,C)$.

A stronger equivalence relation, called shift equivalence, is described in [9].

Definition 2.1 *The shift action of G on $C^2(G,C)$ is defined for $a \in G, \psi \in C^2(G,C)$ to be $\psi \cdot a \in C^2(G,C)$ where*

$$(\psi \cdot a)(g,h) = \psi(ag,h)\psi(a,h)^{-1}.$$

We say that ψ and $\psi \cdot a$ are shift equivalent.

For $a \in G$ and $\psi \in C^2(G,C)$, let $\psi_a : G \longrightarrow C$ be the set mapping $\psi_a(g) = \psi(a,g), g \in G$. Also let $\partial\psi_a$ be the corresponding coboundary.

Hence if ψ is a cocycle, then

$$\psi \cdot a = \psi\partial\psi_a, \quad \forall a \in G, \ \psi \in Z^2(G,C).$$

i.e., ψ is equivalent (cohomologous) to $\psi \cdot a$.

Thus the shift equivalence partitions each cohomology class, and is consequently a stronger equivalence relation.

3 Shift equivalence and cocyclic Hadamard matrices

A Hadamard matrix of order m is a square matrix $[h(i,j)]$ with entries $h(i,j) = \pm 1$, $1 \leq i,j \leq m$, whose row vectors are pairwise orthogonal. A Hadamard matrix must have order 1, 2 or a multiple of 4, but no other restrictions on the order of a Hadamard matrix are known, and the century-old *Hadamard Conjecture* proposes that a Hadamard matrix exists for every $m \equiv 0 \pmod 4$.

If we take C in (2) to be the group $Z_2 = \{1, -1\}$ then M_ψ is a cocyclic binary matrix and it is computationally easy to check whether M_ψ is a Hadamard matrix, as we only need to check whether the dot product of the first row with each other row is 0, see [4].

Recall two binary matrices are Hadamard equivalent if one can be obtained from the other by a sequence of row or column permutations or negations.

The question arises as to whether there is a relation between shift equivalence and Hadamard equivalence. This is particularly interesting since two cocycles which are cohomologous need not generate Hadamard equivalent matrices. Further if a cocycle generates a Hadamard matrix then a cohomologous cocycle need not even generate a Hadamard matrix.

Proposition 3.1 *Let $M_\psi = [\psi(g,h)]_{g,h\in G}$ be the cocyclic matrix of ψ. From the definition of shift equivalence $M_{\psi\cdot a} = [\psi(ag,h)\psi(a,h)^{-1}]_{g,h\in G}$. Consequently, $M_{\psi\cdot a}$ can be obtained from M_ψ for $a \in G$ by the following steps:*

1. *Change the order of the elements of G from $g \in G$ to $g' = ag \in G$.*
2. *Rearrange the rows of M_ψ with respect to this indexing obtaining $M' = [\psi(ag,h)]_{g,h\in G}$. Now the first row of M' is indexed by a.*
3. *Obtain $M_{\psi\cdot a}$ from M' by multiplying every row of M' point-wise by the first row of M'.*

Clearly $M_{\psi\cdot a}$ is Hadamard equivalent to M_ψ, since the only operations are interchanging rows and multiplying specific columns by -1.

Thus if two cocyclic matrices are shift-equivalent then they are Hadamard equivalent, but Hadamard equivalence does not necessarily imply shift equivalence.

4 Shift-equivalence and self-dual codes

In [10], Horadam and Perera define cocyclic codes as follows: A code over a ring R is termed *cocyclic* if it can be constructed using cocycles or the rows of cocyclic matrices or is equivalent to such a code.

In [1, 3] Hadamard matrices H over $Z_2^2 \times Z_t$ and over D_{4t} were used in the $[I, A]$ construction to generate doubly-even and singly-even self-dual codes.

We will look at the structure of dihedral cocyclic matrices to understand the relation between shift-equivalent Hadamard matrices and the codes they generate.

In the case of the dihedral group D_{4t} of order $4t$ where t is odd, cocyclic Hadamard matrices developed over D_{4t} can exist only in the cases

$$(A,B,K) = (1,1,1),(1,-1,1),(1,-1,-1),(-1,1,1)$$

for t odd. Here A and B are the inflation variables and K is the transgression variable.

In the cases $(A, B, K) = (1, 1, 1)$ or $(A, B, K) = (-1, 1, 1)$, for a D_{4t}-cocyclic Hadamard matrix to exist t must be a sum of two squares. This is certainly true for $t = 5$, but no Hadamard matrices were found. $(A, B, K) = (1, -1, -1)$ was the case which yielded the most number of Hadamard matrices and self-dual codes.

In this case, the D_{4t}-cocyclic Hadamard matrices are $\sim_h$ (Hadamard equivalent) to

$$\begin{bmatrix} M, & N \\ ND, & -MD \end{bmatrix} \tag{3}$$

where M and N are $2t \times 2t$ matrices each the entrywise product of a back-circulant and a back-negacyclic matrix with first row $\vec{m} = (m_1, m_2, \ldots m_{2t})$ and $\vec{n} = (n_1, n_2, \ldots n_{2t})$ respectively. If C_{2t} is the back circulant $2t \times 2t$ permutation matrix with first row

$$1\,0\,0\,0\,\ldots\,0$$

then D is the $2t \times 2t$ matrix obtained by negating every non-initial column of C_{2t}. See [7] for more details.

H is fully determined by the ordered pair $(\vec{m}, \vec{n})$. For example for $t = 3$,

$$M = \begin{bmatrix} m_1 & m_2 & m_3 & m_4 & m_5 & m_6 \\ m_2 & m_3 & m_4 & m_5 & m_6 & -m_1 \\ m_3 & m_4 & m_5 & m_6 & -m_1 & -m_2 \\ m_4 & m_5 & m_6 & -m_1 & -m_2 & -m_3 \\ m_5 & m_6 & -m_1 & -m_2 & -m_3 & -m_4 \\ m_6 & -m_1 & -m_2 & -m_3 & -m_4 & -m_5 \end{bmatrix}$$

and similarly for N.

H is a cocyclic Hadamard matrix if and only if

$$M^2 + N^2 = 4tI_{2t} \tag{4}$$

This equation was used to generate D_{4t}-cocyclic Hadamard matrices for $t = 3, 5, 7$ and 9. One of the major problems in such a search has always been exponential growth of the search space. Image restoration techniques (explained in [3] and [6]) were used to mitigate some of these effects.

These matrices were then used to generate self-dual codes, which by [10] are D_{4t}-cocyclic self-dual codes.

One of the intriguing consequences of this search for extremal self-dual codes, was codes with only one code word of minimum weight. This interesting case was first encountered in the case $t = 5$, and only among the doubly-even codes in that case. In the case $t = 7$ singly-even codes with one codeword of minimum weight were found, whereas in the case $t = 9$ there are both singly-even and doubly-even codes of this type.

All the self-dual codes were classified into code equivalence classes except for the codes with one codeword of minimum weight. The question arose as to whether there is a relation between the many codes with this property. Recall that two binary codes are said to be equivalent if one can be obtained from the other by interchanging columns. Ozeki [12] showed that equivalent normalised Hadamard matrices give equivalent self-dual codes, but it is easy to see that equivalent un-normalised Hadamard matrices need not generate equivalent linear codes.

The question is whether shift-equivalent cocyclic matrices give equivalent codes.

Proposition 4.1 *Let us consider the effect of the following operations on a matrix of type (3).*

1. *Multiplying all rows of a Hadamard matrix, M, of type (3), entry-wise by the first row. and all columns entry-wise by the first column gives a normalised D_{4t} - cocyclic Hadamard matrix M_ψ.*

2. *Rearranging the rows of M_ψ according to the indexing $\{ag\}$ $g \in G$ and then multiplying all rows pointwise by the resulting first row, we obtain the shift equivalent matrix $M_{\psi \cdot a}$.*

3. *Suppose M' was the matrix obtained from M by rearranging the rows according to the indexing $\{ag\}$ $g \in G$. Then normalising M' as in step 1, we would get $M_{\psi \cdot a}$.*

Clearly M' and M are obtained from shift-equivalent cocycles. The matrices used in the $[I, A]$ construction are M and M'. Since M and M' differ only by a permutation of the rows, they will generate equivalent codes.

Following is a small example which clarifies the above point. We use a matrix which is Hadamard equivalent to a Z_2^2- cocyclic matrix. The basic theory is outlined in [4]. The first row and column give the index of the remaining rows and columns.

$M =$

$*$	e	a	b	ab
e	n	x	y	z
a	x	An	z	Ay
b	y	Kz	Bn	Bkx
ab	z	Aky	Bx	$ABKn$

On performing step (1) we get

$M =$

$*$	e	a	b	ab
e	1	1	1	1
a	1	A	$nxyz$	$Anxyz$
b	1	$Knxyz$	B	$BKnxyz$
ab	1	$AKnxyz$	$Bnxyz$	ABK

This matrix is a Z_2^2- cocyclic matrix.

Let $g = b$. Indexing the rows according to the new index $\{bg : g \in G\}$, that is, $\{b, ab, e, a\}$ and performing the operations in step (2) we get

$M_{\psi \cdot b} =$

$*$	e	a	b	ab
b	1	1	1	1
ab	1	A	$nxyz$	$ABKnxyz$
e	1	$Knxyz$	B	$BKnxyz$
a	1	$AKnxyz$	$Bnxyz$	ABK

Consider the matrix M' obtained from M by rearranging the rows according to the index $\{b, ab, e, a\}$

$M =$

$*$	e	a	b	ab
b	y	Kz	Bn	Bkx
ab	z	Aky	Bx	$ABKn$
e	n	x	y	z
a	x	An	z	Ay

Normalising M' using step (1), we get $M_{\psi \cdot b}$.

It can now be seen that matrix M' can be obtained from M by simple rearrangement of the rows of M according to the indexing $\{bg : g \in G\} = \{b, ab, e, a\}$.

Consequently M and M' would generate equivalent codes. Thus shift-equivalent cocyclic Hadamard matrices generate equivalent codes. We can now classify the self dual codes according to shift equivalence classes.

5 Computational results

Here by shift-equivalent, we mean that if we normalised the Hadamard matrices as described in step (1) of Proposition 4.1, we would get shift-equivalent cocyclic Hadamard matrices.

Tests were conducted on all Hadamard matrices cocyclic over D_{20} which had resulted in doubly-even self-dual codes. Firstly, we checked whether any of the cocyclic matrices could be obtained from each other by rearrangement of the rows according to the Cayley table of D_{20}. None of the matrices were found to be row-rearrangements of each other. This was not surprising, since rearrangement of the rows results in a very different pattern to the one (3) used for generating the D_{4t} - cocyclic Hadamard matrices.

When the normalised D_{4t} - cocyclic Hadamard matrices (normalised as in step (1) of Proposition (4.1)) were tested for shift equivalence, 35 shift-equivalence classes were found, each with 160 matrices. Table 1 classifies the self-dual codes found in [1] according to shift-equivalence classes. A representative of each class is given in the form $\{\vec{m}; \vec{n}\}$. The vectors $\vec{m}$ and $\vec{n}$ are given in the form of integers. The corresponding vectors are generated by converting the integers to binary, and then replacing all 0's by -1's.

Note that there are two code equivalence classes associated with some of the shift-equivalence classes. This may seem to be contradictory to the theoretical result in section 4 but can be explained easily:

It was noted in [1] that the structure of the dihedral-cocyclic Hadamard matrices was too restrictive to produce doubly-even or singly-even codes using the $[I, A]$ construction. The following steps were used to identify "good" Hadamard matrices, i.e., those that give doubly-even self-dual codes.

1. Generate all Hadamard matrices cocyclic over D_{4t} for t odd.
2. Keep all matrices with the number of +1s in each row congruent to either 3 (mod 4) or 1 (mod 4).
3. To produce doubly-even codes multiply every row with the number of +1s congruent to 1 (mod 4) by -1.

It is now clear that the Hadamard matrices used for generating the self-dual codes are no longer truly cocyclic, but we thought it still an interesting exercise to classify the code classes obtained according to the shift-equivalence classes.

The code class 0 is the class of codes with one code word of minimum weight. This class of codes cannot actually be called an equivalence class

Table 1: Code classes distributed into shift-equivalence classes

C-e Class	Rep cocylic matrix $\{\vec{m};\vec{n}\}$	S-e Class	C-e Class	Rep cocylic matrix $\{\vec{m};\vec{n}\}$	S-e Class
0	33; 425	31	9	32; 202	34
0	77; 161	21	10	18; 98	25
0	61; 202	26	10	22; 232	13
1	12; 372	27	11	18; 185	24
1	12; 82	35	11	22; 371	12
2	18; 280	23	12	34; 208	4
2	22; 92	15	12	20; 475	16
2	12; 331	28	12	34; 188	7
2	12; 162	34	12	20; 118	20
3	22; 462	11	13	34; 304	1
3	12; 186	32	13	20; 440	17
3	12; 181	33	13	34; 244	3
3	18; 465	21	13	20; 285	18
4	12; 466	26	13	34; 179	8
4	22; 197	14	13	20; 145	19
4	12; 276	31	14	66; 188	6
4	18; 395	22	14	34; 44	10
5	12; 302	29	15	34; 50	9
5	12; 296	30	16	34; 194	6
6	61; 306	27	16	66; 50	10
6	33; 345	35	17	34; 268	2
7	33; 405	32	17	34; 203	5
7	32; 332	33	18	77; 117	25
8	62; 172	29	19	77; 482	23
8	61; 172	30	20	77; 471	22
9	62; 212	28	21	77; 376	24

as we have not exhaustively checked whether the codes are equivalent to each other. The computer algebra package, MAGMA [5] stalls when asked to check the equivalence of these codes.

6 Acknowledgement:

The author is grateful to Mr. Joselito Chua for his assistance with the computational aspects of this paper.

References

[1] A. Baliga, Cocyclic codes of length 40, *Des., Codes and Cryptogr.* 24(2) (2001) pp. 171-179.

[2] A. Baliga, New self-dual codes from cocyclic Hadamard matrices, *J. Combin. maths. Combin. Comput.*, 28 (1998) pp. 7-14.

[3] A. Baliga and J.J. Chua, Self-dual codes using image restoration techniques, *Lecture Notes in Computer Science LNCS 2227*, Eds. S. Boztas, I.E. Shparlinski, Springer (2001) pp. 46-56.

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

[5] W. Bosma, J. Cannon, C. Playoust, The MAGMA algebra system I: the user language, *J. Symbolic Comput.*, 24, (1997) pp. 235-265 .

[6] J.J. Chua and A. Baliga, An application of Adaptive Image Restoration techniques in a heuristic search for cocyclic Hadamard matrices (preprint, 2003).

[7] D.L. Flannery, Cocyclic Hadamard matrices and Hadamard groups are equivalent, *J. Algebra*, 192 (1997), pp 749-779.

[8] A. Hedayat and W. D. Wallis, Hadamard matrices and their applications, *Ann. Statist.*, 6, (1978) pp. 1184-1238.

[9] K.J. Horadam, The shift action on 2-cocycles, 2002 (preprint).

[10] K. J. Horadam and A. A. I. Perera, Codes from cocycles, in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes; 12th International Symposium, AAECC-12, Toulouse, France, June 1997, proceedings*, Lecture Notes in Computer Science 1255, Springer-Verlag, Berlin, (1997), pp. 151–163.

[11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting codes*, North-Holland, Amsterdam, (1977).

[12] M. Ozeki, Hadamard matrices and doubly-even self-dual error-correcting codes, J. of Combin. Theory, Series A 44 (1987), pp. 274-287.

[13] J. Seberry and M. Yamada, Hadamard matrices, sequences and block designs, in *Contemporary Design Theory*, eds J. H. Dinitz and D. R. Stinson, John Wiley & Sons, (1992), pp. 431–560.

[14] W. D. Wallis, A. P. Street and J. S. Wallis, *Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices*, Lecture Notes in Math. 292, Springer-Verlag, Berlin, (1972).