New Self-Dual Codes from Cocyclic Hadamard Matrices

A. Baliga *†
Department of Mathematics, RMIT.,
GPO Box 2476V, Melbourne, VIC 3001, Australia.

Dedicated to Anne Penfold Street.

Abstract

The structure of cocyclic Hadamard matrices is such as to allow us a much faster and more systematic search for binary, self-dual codes. Here we consider $\mathbf{Z}_2^2 \times \mathbf{Z}_t$ - cocyclic Hadamard matrices for t = 3, 5, 7 and 9 to give binary self-dual codes of length 24, 40, 56 and 72. We show that the extended Golay code cannot be obtained as a member of this class and also show the existence of four apparently new codes - a [56,28,8] and three [72,36,8].

1 Introduction

In [16] Tonchev gives a general method unifying the known constructions of binary self-orthogonal codes from designs. This work is extended by Bussemaker and Tonchev [4, 5], and Kimura [13]. We show here that these constructions are highly effective when used with cocyclic Hadamard matrices. We present the search for binary self-dual codes using $\mathbf{Z}_2^2 \times \mathbf{Z}_t$ - cocyclic Hadamard matrices for t odd. The internal structure of the Hadamard matrices permits substantial cut-downs in the search time for each code found. In addition, it avoids the need for generating entire matrices before a search can take place.

We also look at the weight distributions of these codes. Comparing our list to the one by Beth et al., [2], we note four apparently new codes, three of which fit the thinned binomial Hamming weight distribution better than the comparable codes in the list in [2].

*This paper was presented at the 3rd International Conference on Combinatorial Mathematics and Combinatorial Computing, Melbourne.

†This research is supported by an RMIT Faculty of Applied Science Research Grant.

We assume that the reader is familiar with the basic facts of the theory of Hadamard matrices, (see [8, 15, 17]) and of binary linear codes (see [14]).

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. The minimum distance d of a self-dual, doubly-even code of length n, satisfies $d \leq 4\left[\frac{n}{24}\right] + 4$. C is *extremal* if this theoretical maximum is attained ([14]).

If G is a finite group (written multiplicatively with identity 1), a *binary cocycle* (over G) is a set mapping $f : G \times G \rightarrow \mathbf{Z}_2$ which satisfies $f(a,b)f(ab,c) = f(a,bc)f(b,c)$, $\forall a,b,c \in G$. A cocycle is *normalised* if $f(1,1) = 1$. A $v \times v$ binary matrix M is G - *cocyclic* (developed by f) if there exists a set mapping $g : G \rightarrow \mathbf{Z}_2$ and a cocycle f such that $M = [f(a,b)g(ab)]$, $\forall a,b \in G$. For further definitions, see [1, 10].

See [1] for the theory of cocyclic matrices, in particular, $\mathbf{Z}_t \times \mathbf{Z}_2^2$ - cocyclic Hadamard matrices.

In [11], 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. So the codes we obtain here are $\mathbf{Z}_t \times \mathbf{Z}_2^2$ - cocyclic codes.

In Section 2, we review the construction given in [16, 4] and extend it to include construction of [72,36,16] codes. We apply this construction to cocyclic Hadamard matrices and present the algebraic cut downs obtained by this application. In Section 3, we give the computational results obtained, including the fact that the extended Golay code is not a $\mathbf{Z}_t \times \mathbf{Z}_2^2$ - cocyclic code.

Section 4 gives the comparison of the weight enumerators of these codes with the thinned binomial Hamming weight distribution.

2 Construction of doubly-even codes from $\mathbf{Z}_t \times \mathbf{Z}_2^2$ - cocyclic Hadamard matrices.

¿From [16], we have the following construction of doubly-even, self-dual codes. Here I is the identity matrix, J is the all 1's matrix of order n and, given a Hadamard matrix H of order $n = 8s + 4$, $\bar{H} = (H + J)/2$.

If the number of $+1$'s in each row and column of H is $\equiv 3 \pmod 4$ then the matrix $[I, \bar{H}]$ generates a binary, doubly-even, self-dual $[2n, n]$ code C. The minimum weight of C is at least 8 if and only if each row of H contains at least 7 $+1$'s.

This construction was used to find extremal, doubly-even, self-dual codes of length 24 and 40 from selected Hadamard matrices of order 12 and 20, respectively (see [16, 5]). It was extended (see [4, 13]) and used by Kimura and Bussemaker and Tonchev, to find extremal self-dual codes of length 56.

It is easy to extend the construction of [16, 13] to the $n = 72$ case, to show that the following conditions apply:

Proposition 2.1 *If the number of +1's in each row and column of H is $\equiv 3 \pmod 4$ then the matrix $[I, \bar{H}]$ generates a binary, doubly-even, self-dual $[72, 36]$ code C which would be extremal if and only if*

1. *Each row (and column) of H contains at least 15 +1's.*
2. *Every linear combination of 3, 4, 5 or 6 rows of $[I, \bar{H}]$ and $[\bar{H}^t, I]$ has weight at least 16.*

The importance of using cocyclic Hadamard matrices for the construction is that we can obtain cut downs to the search space from the listing of the first row only of the Hadamard matrix, without computing (or storing) the rest of the matrix.

¿From [1] the structure of a $\mathbf{Z}_t \times \mathbf{Z}_2^2$ - cocyclic matrix, t odd, is $\sim_h$ to a $t \times t$ block-backcirculant matrix W with top row $W_1, W_2, \ldots, W_t$, where

$$W_i = \begin{bmatrix} n_i & x_i & y_i & z_i \\ x_i & An_i & z_i & Ay_i \\ y_i & Kz_i & Bn_i & BKx_i \\ z_i & AKy_i & Bx_i & ABKn_i \end{bmatrix}, \quad 1 \le i \le t. \tag{1}$$

and all the variables take values in $\{\pm 1\}$. Hence the sum of the rows is given by

$$\begin{aligned} &\sum_{i=1}^{t}(n_i + x_i + y_i + z_i) \\ &\sum_{i=1}^{t}(An_i + x_i + Ay_i + z_i) \\ &\sum_{i=1}^{t}(Bn_i + BKx_i + y_i + Kz_i) \\ &\sum_{i=1}^{t}(ABKn_i + Bx_i + AKy_i + z_i) \end{aligned} \tag{2}$$

Similar formulae hold for the sums of columns.

The "transgression" generator K appears to play the most significant role in the behaviour of W. Clearly, W is a symmetric matrix if and only if $K = 1$. If, in addition $A = B = 1$ then W is $\sim_h$ to a group developed matrix and, if it is to be Hadamard then t must be a perfect square.

The author has previously computed lists of all $\mathbf{Z}_t \times \mathbf{Z}_2^2$ - cocyclic Hadamard matrices for $t = 1, 3, 5, 7$ and 9, obtaining 6, 192, 960, 6720 and 27920, respectively. Every example has $A = B = K = -1$.

In [1], as a consequence of this computational evidence, it has been conjectured that there are no symmetric $\mathbf{Z}_t \times \mathbf{Z}_2^2$ - cocyclic Hadamard matrices for odd $t > 1$.

Hence taking A, B and $K = -1$ and assuming that the number of n_i's which are $+1$ is a, and the corresponding numbers for x_i, y_i and z_i are b, c and d we can simplify the four row sums.

For the existence of doubly-even self-dual codes the number of $+1$'s in each row and column must be $\equiv 3 \pmod 4$. We thus get the following set of equations:

$$\begin{array}{rcccccccl} & a & + & b & + & c & + & d & \equiv 3 \pmod 4 \\ 2t & - & a & + & b & - & c & + & d \equiv 3 \pmod 4 \\ 2t & - & a & + & b & + & c & - & d \equiv 3 \pmod 4 \\ 2t & - & a & - & b & + & c & + & d \equiv 3 \pmod 4 \end{array} \tag{3}$$

We conclude that either a is odd and b, c and d are even or a is even and b, c and d are odd.

In [1] it has been shown that if W is a Hadamard matrix then $4t$ is a sum of four odd squares. Specifically,

$$4t = (-t+2a)^2 + (-t+2b)^2 + (-t+2c)^2 + (-t+2d)^2 \tag{4}$$

with a, b, c and d as above.

Putting the conditions (3) and (4) together, we can compute the values of a, b, c and d for which self-dual, doubly-even codes do exist. For example, for $t = 3$, only 4 out of the 64 possible values of a, b, c and d which satisfy (4), yield binary, doubly-even, self-dual codes.

Further W is a $\{\pm 1\}$ matrix. Rewriting W as $(W + J)/2$, we get a $\{0, 1\}$ block back-circulant matrix, V with top row $V_1, V_2, \ldots, V_t$, where

$$V_i = \begin{bmatrix} \bar{n}_i & \bar{x}_i & \bar{y}_i & \bar{z}_i \\ \bar{x}_i & 1+\bar{n}_i & \bar{z}_i & 1+\bar{y}_i \\ \bar{y}_i & 1+\bar{z}_i & 1+\bar{n}_i & \bar{x}_i \\ \bar{z}_i & \bar{y}_i & 1+\bar{x}_i & 1+\bar{n}_i \end{bmatrix}, \quad 1 \le i \le t. \tag{5}$$

and addition is modulo 2.

Also the sum of the first four rows of V is a vector of the form

$$(s_1, s_1, s_1, s_1, \ldots, s_i, s_i, s_i, s_i, \ldots, s_t, s_t, s_t, s_t)$$

where $s_i = \bar{n}_i + \bar{x}_i + \bar{y}_i + \bar{z}_i$.

For the [56, 28] code to be extremal this vector must have at least 8 $+1$'s. Hence at least 2 out of 7 quadruples $(\bar{n}_i, \bar{x}_i, \bar{y}_i, \bar{z}_i)$ must have either one $+1$ or 3 $+1$'s. Similarly to obtain a [72, 36, 16] code, this vector must have at least 12 $+1$'s. Hence at least 3 out of 9 quadruples $(\bar{n}_i, \bar{x}_i, \bar{y}_i, \bar{z}_i)$ must have either one $+1$ or 3 $+1$'s.

3 Computational Results

Using the conditions above, the search for $\mathbf{Z}_t \times \mathbf{Z}_2^2$-cocyclic Hadamard matrices, for $t = 3$, 5, 7 and 9, which yield self-dual, doubly-even codes, was carried out.

In the case $t = 3$, there are 24 cocyclic Hadamard matrices which give self-dual codes of which 12 are doubly-even but none of these, extremal. Thus it is clear that the extended Golay code is not $\mathbf{Z}_3 \times \mathbf{Z}_2^2$ - cocyclic. This is not surprising as the Hadamard matrix used in the generator matrix of the Golay code is Type 2 Paley while the $\mathbf{Z}_3 \times \mathbf{Z}_2^2$ - cocyclic Hadamard matrices are Type 1 Paley. We expect the Golay code to be D_{12}-cocyclic. It is worth noting here that Ito [12] gives a Hadamard matrix of order 24, D_{24}-cocyclic (not D_{12}), which generates the extended Golay code [24, 12, 8].

On the other hand, it will be shown elsewhere that the singly-even $\mathbf{Z}_3 \times \mathbf{Z}_2^2$-cocyclic codes obtained are equivalent to the unique "Odd Golay code".

For $t = 5$, 120 self-dual codes were found. 60 were doubly-even and extremal and classified into one equivalence class.

In the case $t = 7$, there are 840 Hadamard matrices which yield self-dual codes. Of these 420 are doubly-even - giving two distinct [56, 28, 8] codes. Of these, one does not appear in the known lists. It has only 7 code words of weight 8. Its weight enumerator is given below:

weight	no. of codewords
0	1
8	7
12	8232
16	621733
20	11701984
24	64905043
28	113961456
32	64905043
36	11701984
40	621733
44	8232
48	7
56	1

For $t = 9$, 3240 Hadamard matrices produce self-dual codes of which 1620 are doubly-even. The weight enumerators show that three new codes are obtained. One has only 9 code words of weight 8. The weight enumerators are as below:

weight	count		
0	1	1	1
8	9	45	153
12	1128	1956	5088
16	242532	257472	294516
20	18153936	18099720	17979840
24	462712212	462519720	461799684
28	4398147864	4399546140	4404061728
32	16601136894	16597738602	16587030510
36	25758687584	25763149424	25777133696
40	16601136894	16597738602	16587030510
44	4398147864	4399546140	4404061728
48	462712212	462519720	461799684
52	18153936	18099720	17979840
56	242532	257472	294516
60	1128	1956	5088
64	9	45	153
72	1	1	1

4 Weight Distribution

Beth et al.,[3] have shown that binary block codes with binomially distributed Hamming distances (Hamming weights for linear codes) lie on the Gilbert Varshamov Curve when $N \longrightarrow \infty$. In the binary case, the curve represents not only a lower bound on the maximal minimum Hamming distance for binary block codes of rate $R \in (0,1)$, but, also, the curve determines the error exponent of the Binary Symmetric Channel (BSC) in the interval between the critical rate R_{crit} and the rate R_c of the BSC.

In [2], Beth et al., compare the weight distributions of some binary doubly-even, self-dual codes to the values of the corresponding binomial distributions. Using a variation of the $[I, A]$ construction, they tabulate the relative error terms $\epsilon(N, d_H)$ found in the conjectured weight formula

$$A_{d_H} = 4.2^{K-N}\,(N, d_H)\,(1 + \epsilon(N, d_H)); \quad 0 \leq d_H \equiv 0 \bmod 4 \leq N,$$

for the first 12 examples they find.

Example 4.1 *Let M be a $\mathbf{Z}_t \times \mathbf{Z}_2^2$-cocyclic Hadamard matrix. For $t = 3, 5, 7,$ and 9, the [8t,4t] binary doubly-even self-dual codes with generator matrix [I, $\bar{M}$] have weight distributions which differ from the thinned binomial Hamming distribution according to the following table of relative*

errors $\epsilon(N, d_H)$.

no.	1	2	3	4	5	6	7
N	24	40	56	56	72	72	72
wt							
$N/2$	−0.0190	−0.0006	−0.0001	+0.0005	$+4.1 \times 10^{-5}$	$+2.1 \times 10^{-4}$	$+7.5 \times 10^{-4}$
$(N/2) \pm 4$	+0.0233	+0.0009	+0.0002	−0.0007	-4.9×10^{-5}	-2.5×10^{-4}	-9×10^{-4}
$(N/2) \pm 8$	−0.4196	−0.0015	−0.0039	+0.0019	$+7.8 \times 10^{-5}$	$+3.9 \times 10^{-4}$	$+1.4 \times 10^{-3}$
$(N/2) \pm 12$		−0.0285	+0.0018	−0.0094	1.16×10^{-4}	-5.3×10^{-4}	-2.1×10^{-3}
$(N/2) \pm 16$			−0.0106	+0.0499	-5.3×10^{-4}	−0.0035	−0.0101
$(N/2) \pm 20$			−0.6693	+3.2991	0.01223	+0.0746	+0.2291
$(N/2) \pm 24$					+0.2614	+0.187	+4.6896
$(N/2) \pm 28$					+11.918	+63.5913	+218.61

We find that four of the codes obtained from $\mathbf{Z}_t \times \mathbf{Z}_2^2$-cocyclic Hadamard matrices do not appear in the list given in [2]. These are codes no. 3 (a [56,28,8] code) and 5, 6 and 7 ([72,36,8] codes). Only code 4 appears in the list (No. 5) in [2]. Codes 3, 5 and 6 also fit the binomial distribution better than the most comparable codes (Nos. 5, 8 and 9) given in [2].

Acknowledgment:

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

References

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

[2] Th. Beth, H. Kalouti and D.E. Lazic, Which families of long binary linear codes have a binomial weight distribution?, in *Proc. AAECC-11*, Lecture Notes in Computer Science 948, eds. G. Cohen, M. Guisti, T. Mora (Springer-Verlag,1995), 120–130.

[3] Th. Beth, D.E. Lazic and V. Senk, The generalized Gilbert-Varshamov distance of a code family and its influence on the family's error exponent, *Proceedings of the International Symposium on Information Theory and its Applications* (Sydney, Australia, 1994).

[4] F.C. Bussemaker and V.D. Tonchev, New extremal doubly-even codes of length 56 derived from Hadamard matrices of order 28, *Discrete Math.* **76** (1989), 45–49.

[5] F.C. Bussemaker and V.D. Tonchev, Extremal doubly-even codes of length 40 derived from Hadamard matrices of order 20, *Discrete Math.* **82** (1990), 317–321.

[6] J.H. Conway and N. J. A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Transactions on Information Theory* **36** (1990), 1319–1333.

[7] M. Harada and V.D. Tonchev, Singly-even self-dual codes and Hadamard matrices, in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes; 11th International Symposium, AAECC-11, Paris, France, July 1995, proceedings*, Lecture Notes in Computer Science 948 (Springer-Verlag, Berlin, 1995), 279–284.

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

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

[10] K. J. Horadam and W. de Launey, Generation of cocyclic Hadamard matrices, Chap. 20 in *Computational Algebra and Number Theory*, eds. W. Bosma, A. van der Poorten (Kluwer Academic, Dordrecht, 1995), 279–290.

[11] 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), 151–163.

[12] N. Ito, Personal Communication, 14 July, 1997.

[13] H. Kimura, Extremal doubly-even (56,28,12) codes and Hadamard matrices of order 28, *Australas. J. Combin.* **10** (1994), 153–161.

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

[15] 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), 431–560.

[16] V.D. Tonchev, Self-orthogonal designs and extremal doubly-even codes, *J. Combinatorial Theory* **52A** (1989), 197–205.

[17] 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).