Volume 4 Issue No. 1 December 2001
P-ISSN: 2244-4432 • E-ISSN: 2984-7125
National Peer Reviewed Journal
DOI: https://doi.org/10.59120/drj.v4i1.62

The [72,36] Type II Self Dual Codes from Hadamard Matrices

Rowena T. Baylon-CABRIZOS[1]
[1]Instructor, Mathematical Sciences Department,
Davao Oriental State College of Science and Technology, Mati, Davao Oriental

Abstract

Consider a code [n,k,d] of length n, dimension k and of minimum distance d. Let R be a rate defined by the equation R = k/n. Mathematically, the main problem of coding theory is to find codes with large R (for efficiency) and large d (to correct many errors). This paper diseuses the binary [72,36] code constructed from Hadamard matrices.

Keywords: code, self-dual, Hadamard matrices, doubly even, weight enumerator, minimum distance

Introduction

Coding theory began in the late 1940's with the works of Golay (1949), Hamming (1950) and Shannon (1948). Codes were invented to correct errors on noisy communication channels. Suppose there is a telegraph wire from Manila to Davao down which o's and I's can be sent. Usually, when a 0 is sent the same number is received. But there are cases that a O will be received I or vice versa. When the message sent does not coincide with the message received, we say that an error has occurred during the transmission. Thus, the main problem of coding theory is to correct such errors.

We now define some basic concepts about codes. A *binary linear code* is defined as a subspace of the vector space F_2^n over GF (2), the Galois field whose elements are 0 and 1. Let $v = v_1, v_2 \ldots$, where v' are either 0 or 1 for $i = 1, \ldots, n$. An element *v* of [n, k] is called a *codeword*. Denote [n, k] as a code of length n and dimension k. The *hamming weight* of a codeword v denoted by *wt(v)* is the number of nonzero coordinates of *v*. Consider $v = v1, v2 \ldots$, and $w = w1, w2 \ldots, wn$. The hamming distance *d(v, w)* between 2 codewords *v* and *w* is the number Of *i*'s where w_i is not equal to v_i. The *minimum distance* d of a linear code [n, k] is the minimum weight of a nonzero codeword. This time, we denote our linear code as the inner product between v and w is defined as

$$(v,w) = \sum_{i=1}^{n} v_i w_i \quad = \begin{cases} 0 \text{ if } (v,w) \quad 0 \bmod 2 \\ 1 \quad \text{Otherwise} \end{cases}$$

If $(v,w) = 0$, we say that our codewords are *orthogonal.* For all v in [n,k,d], the set of all vectors w in $\mathbf{F_2^n}$ which are orthogonal to v forms the *dual* of the code [n,k,d] and is denoted by [n,k,d]. If [n,k,d] is a subset of [n,k,d]', we say that our linear code is *self-orthogonal*. In particular, if [n,k,d]=[n,k,d]', then our linear code is said to be *self-dual*. We focus our study on self-dual codes as such codes have interesting properties. There are two types of self-dual codes namely: *singly-even* or type I if and only if the weight or all its codewords are divisible by two and; *doubly-even* or type II if and only if the weight of all its codewords is divisible by four.

A famous theorem by Mallows and Sloane (1973) gives us the bound for the minimum distance d of a code.

Theorem 1: Let [n,k,d] be type II binary linear code. Then

$$d \; 4\,[n/24] + 4.$$

Note: We read [n/24] as the greatest integer of (n divided by 24).

If equality is attained in the above theorem, such code is said to be extremal. Another important invariant of a code is the weight *enumerator*. The weight enumerator of a code C is a polynomial in and y defined as follows:

$$\mathbf{W}_c(\chi, y) = \sum_{i=0}^{n} \mathbf{A}_i \, \chi^{n-i} y^i,$$

where A_i denotes the number of codewords of weight i.

The following is a famous theorem by MacWilliams (1963) relating the weight enumerator of code C with its dual C'.

Theorem 2: $W_{c'}(x, y) =$ **(1/1c1)** $W_c(x+y, x-y)$

Volume 4 Issue No. 1 December 2001
P-ISSN: 2244-4432 • E-ISSN: 2984-7125
National Peer Reviewed Journal
DOI: https://doi.org/10.59120/drj.v4i1.62

We also define the generator matrix G as a matrix whose rows are base vectors of C, (i.e., G generates the code C).

Methodology

In this section, we will discuss some concepts of Hadamard matrices and a method of constructing [72,36] codes.

Hadamard Matrix

A *hadamard matrix* H_n of order n is defined to be a square matrix of order n, whose entries consist of 1 's and -1 's, satisfying

$$\mathbf{H_n\,{}^tH_n = I_n}$$

where $\mathbf{{}^tH_n}$ is the transpose of $\mathbf{H_n}$ and $\mathbf{I}_n$ is the *identity matrix* of order n. We. will use Ozeki's (1987) definition of a normalized hadamard matrix, $\mathbf{NH_n}$. A hadamard matrix of the form,

$$\begin{bmatrix} -1 & 1 & 1 & . & . & . & \cdots & 1 \\ 1 & & & & & & & \\ . & & & & & & & \\ . & & & & & & * & \\ . & & & & & & & \\ 1 & & & & & & & \end{bmatrix}$$

is said to be normalized *hadamard matrix* and will be denoted as $\mathbf{NH_n}$. In other words, $\mathbf{NH_n}$ is a hadamard matrix whose first row and first column entries are all I, except for the first entry which is -1. here are some known facts about hadamard matrices.

1. Hadamard matrices **Hn** exists only when n = 2 or n is a multiple of 4.

2. Two hadamard matrices $H_n^{(1)}$ and $H_n^{(2)}$ of the same order n are said to be Hadamard equivalent (or H-*equivalent*) if $\mathbf{H_n}^{(2)}$ is obtained from $\mathbf{H_n}^{(1)}$ by a sequence of operations of

   (i) exchanging two rows (columns) of $\mathbf{H_n}$ or

   (ii) multiplying some rows (or columns) of $\mathbf{H_n^{(1)}}$ **by -1.**

3. Every hadamard matrix $\mathbf{H_n}$ is equivalent to a normalized hadamard matrix $\mathbf{NH_n}$.

The Construction

We now discuss our method of constructing codes from the normalized hadamard matrices. Note that this construction was introduced by Ozeki (1987).

Consider **Hn**, n 4 mod 8. Transform such matrix to its normalized form (being assured that this is possible in no. 3 property), $\mathbf{NH_n}$. Let $\mathbf{J_n}$ be a square matrix of order n whose entries are all 1. We put

$$\mathbf{K_n - 1/2(NH_n + J_n)}$$

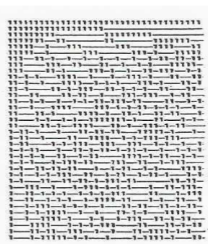
Obviously, the new matrix $\mathbf{K_n}$ is a (0,1) matrix. Let C_n (I_n, K_n) be the *n x 2n* matrix formed by the juxtaposition of I_n and K_n . The following theorems by Ozeki (1987) assure us that Cn is a generator matrix of a code C_{2n} = $\mathbf{C(NH_n)}$ with parameters [2n, n].

Theorem 4: Assume n 4 mod 8. Suppose $\mathbf{NH_n^{(1)}}$ and $\mathbf{NH_n^{(2)}}$ are two normalized and H-equivalent hadamard matrices of order. Then the codes $\mathbf{C(NH_n^{(1)})}$ and $\mathbf{C(NH_n^{(2)})}$ are equivalent.

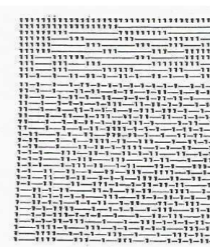
For a particular n, we woi-k on the hadamard matrices of order 36 and obtain the (72, 36) code. Hadamard matrices of order 36 are not yet completely classified thus the existing ones found in Seberry's homepage (http://www.uow.edu.au/-jennie/hadamard.html). There are 191 existing H36 in which 1 1 of them were enumerated by Tonchev (1986), 1 by Janko* and the rest were from Spence*.

Results and Discussion

Constructions and computations of the 191 codes from hadamard • matrices were done with the help of the computer software, MAGMA. We also obtained 191 type II self-dual linear codes and computed their' respective minimum distance d. Out of the 191 codes, 7 of them are [72,36,12] type II codes and the rest are [72,36,8] type II codes. Figure 1 shows the 7 hadamard matrices which obtained the [72,36, 12] codes.



h179



h180

*dates were not cited in the homepage reference

National Peer Reviewed Journal
DOI: https://doi.org/10.59120/drj.v4i1.62

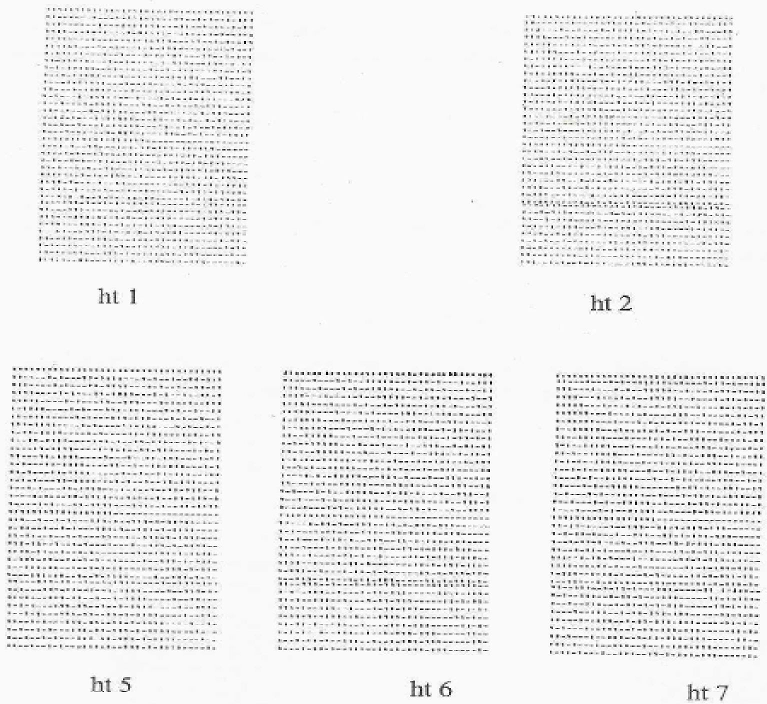


Fig. 1.The 7 hadamard matrices which obtained the [72,36,12] codes

The Weight Enumerator

If extremality is attained for a [72,36] code, d must be 16. No one has ever succeeded in Ending such a code thus, we arc yet uncertain whether such a code exists. In our obtained results, since the value nearest to 16 is 12, we try to

$W_{[72,36,12]}(1,y) = 1 + (4398 + \alpha)y^{12} + (197073 - 12\alpha)y^{16} + (18396972 + 66\alpha) y^{20} + (-220\alpha + 461995395)y^{24} + (4399519410 + 495\alpha)y^{28} + (16599232683-792\alpha)y^{32} + (25760784872 +924\alpha^{36} + \ldots)$

This polynomial was given by Dougherty, et al., (1997). We obtained the bound for α as – 4398 α 16422.

Doughety et al., (1997) obtained 32 different values of α from at least 32 inequivalent codes and is tabulated below.

Table 1. Different [72,36] codes by Dougherty *et al.*, (1997) with their respective α

Code	α	Code	α
C_1	-3744	C_{17}	-3798
C_2	-3774	C_{18}	-3828
C_3	-3768	C_{19}	-3678
C_4	-3714	C_{20}	-3816
C_5	-3762	C_{21}	-3846
C_6	-3792	C_{22}	-3654
C_7	-3732	C_{23}	-3648
C_8	-3702	C_{24}	-3690
C_9	3756	C_{25}	-3822
C_{10}	3750	C_{26}	-3696
C_{11}	3738	C_{28}	-3660
C_{12}	3726	C_{29}	-3684
C_{13}	3708	C_{30}	-3642
C_{14}	3720	C_{30}	-3672
C_{15}	3786	C_{qr}	-1416
C_{16}	3810	C_{dc}	-3936

Table 2. New [72,36] codes with their respective α

Code	α
h180	-3000
h179	-3432
ht1	-3684(same as C_{29})
ht2	-3684
ht5	-3378
ht6	-3378
ht7	-3888

National Peer Reviewed Journal
DOI: https://doi.org/10.59120/drj.v4i1.62

Even though the codes htl and ht2 as well as ht5 and ht6 have the same α value, equivalence of such codes is still unknown.

Conclusions and Recommendations

The problem of finding the extremal [72,36, 1 61 codes has been a problem in coding theory since early 1970's. Until now, no one has successfully found such a code. The method introduced by Tonchev (1989), and Tonchev and Bussemaker (1990), such as negation of rows and Columns of the normalized hadamard matrix, obtained a number of external codes of lengths 40 and 56. Using the same method and applying $\mathbf{H}_{36}$, may lead to a possibility of finding one. To work on such a method requires a lot of patience. In the paper of Sloane (1972) the weight enumerator of a [72, 36,16] code if such code exists is given. Lastly, a necessary and sufficient condition for a type II self-dual code to exist is that n = 0 mod 8 (MacWi11iamsetal., 1972).

Compared to some other value of n, 72 has some unique properties. studying and discovering the uniqueness of 72 is a good mathematical exercise or the readers to start with.

Acknowledgment

The author gratefully acknowledges the comments of Dr. Blesilda P. Raposa, Professor or the Department of Mathematics, College of Science of the De La Salle University, Manila.

Bibliography

Dougherty, S.T., T.A. Gulliver and M. Harada. 1997. External Binary Self Dual Codes. IEEE Trans. on Info. Theory. 43(6):2,036-2.

Golay, M.J, E. 1949. Notes on Digital Coding. Proc. I.E.E.E. 37:657
A).

Hamming, R. W. 1950. Error Detecting and Error Correcting Codes. Bell Syst. Tech. J. 29:147-160 (LA).

MacWilliams, F.J_ 1963. A Theorem on the Distribution of Weights in a Systematic Code. Bell Syst. Tech. J. 42:79-94.

MacWilliams, F.J., N.J.A. Sloane and J.G. Thompson. 1972. Good Self-Dual Codes Exist. Discrete Mathematics. 3.153-162.

Mallows, C.L. and N.J-A- Sloane. 1973. An Upper Bound for Self-mal Codes. Info. and Control J. 22: 188-200.

Ozeki, M. 1987. Hadamard Matrices and Doubly-Even Self-Dual Error Correcting Codes. J. of Combination Theory. A444:274-287.

Shannon, C.E. 1948. A Mathematical Theory of Communication. Bell Syst. Tech. J. 27:379-423, 623-656.

Sloane, NIA. 1972. Is There a (72,36) d 16 Self-mal Code? IEEE Trans. Info. Theory, IT-19:251.

Tonchev, V.D. 1989. Self-Orthogonal Designs and External Doubly Even Codes J. of Combination Theory A (52): 197-205.

Tonchev, V.D. and F.C. Bussemaker. 1990. External Doubly-Even Codes of Length 40 Derived from Hadamard Matrices of Order 20. Discrete Mathematics. 82: 317-321.

www.uow.edu.au/-jennie/hadamard.html