JOURNAL OF COMBINATORIAL THEORY, Series A 52, 197–205 (1989)

Self-Orthogonal Designs and Extremal Doubly Even Codes

VLADIMIR D. TONCHEV

Department of Mathematics and Computing Science,
*University of Technology, Eindhoven, The Netherlands**

Communicated by J. H. van Lint

Received January 15, 1988

A general method unifying the known constructions of binary self-orthogonal codes from designs is described. As an application more than 70 inequivalent extremal doubly even self-dual codes of length 40 are constructed from Hadamard matrices of order 20. Some of these codes do not admit nontrivial automorphisms of odd orders, and there is a code with trivial automorphism group. © 1989 Academic Press, Inc.

1. SELF-ORTHOGONAL CODES AND DESIGNS

We assume that the reader is familiar with the basic notions and facts from design and coding theory (cf., e.g., [2, 6]).

A binary (n, k) code C is a k-dimensional subspace of the n-dimensional vector space V_n over $GF(2)$. Given an (n, k) code C, the $(n, n-k)$ code $C^\perp = \{x \in V_n \colon yx = 0 \text{ for each } y \in C\}$ is called the orthogonal, or dual of C. A matrix with the property that the linear span of its rows generates the code C, is a generator matrix of C. The generator matrices of the dual code $C^\perp$ are called parity check matrices of C. We refer to the elements of a code as code words, or words only. The weight of a code word is the number of its nonzero positions, and the minimum weight of a code is the weight of a lightest nonzero code word. An (n, k, d) code is an (n, k) code with minimum weight d.

A code C is self-orthogonal (resp. self-dual) if $C \subset C^\perp$ (resp. $C = C^\perp$). The weights of all words in a binary self-orthogonal code are even. If, in addition, all weights are divisible by 4, the code is called doubly even. A

* On leave from the Institute of Mathematics of the Bulgarian Academy of Sciences and the University of Sofia. Research partially supported by the NCSCMB, Contract 37/1987 and a Research fellowship from the University of Technology, Eindhoven.

0097-3165/89 $3.00

doubly even self-dual $(n, n/2)$ code exists if and only if $n \equiv 0 \pmod 8$, and the minimum weight d of such a code is bounded by

$$d \leqslant 4[n/24]+4$$

(cf. [6]). A code satisfying the equality in the above bound is called extremal. The words of minimum weight in an extremal code yield 1-, 3-, or 5-design provided that $n \equiv 16, 8$, or $0 \pmod{24}$. The number of extremal codes is finite (but unknown).

Let $X=\{x_1, ..., x_v\}$ be a finite set of "points." We call a family $B=\{B_j\}_{j=1}^{b}$ of subsets of X a *weakly self-orthogonal design* if the following conditions are satisfied:

(a) $|B_i| \equiv |B_j| \pmod 2$ for any $i, j \in \{1, ..., b\}$.

(b) $|B_i \cap B_j| \equiv |B_k \cap B_m| \pmod 2$ for $i, j, k, m \in \{1, ..., b\}$, $i \neq j$, $k \neq m$.

There are four possible tupes of weakly self-orthogonal designs according to the parity of the block size and the cardinality of intersection of pairs of blocks:

(i) $|B_i \cap B_j| \equiv |B_k| \equiv 0 \pmod 2$.

(ii) $|B_i \cap B_j| \equiv |B_k| \equiv 1 \pmod 2$.

(iii) $|B_i \cap B_j| \equiv 1 \pmod 2$, $|B_k| \equiv 0 \pmod 2$.

(iv) $|B_i \cap B_j| \equiv 0 \pmod 2$, $|B_k| \equiv 1 \pmod 2$.

A design of type (i) is called *properly self-orthogonal*, or *self-orthogonal*, only. The term "self-orthogonal" is due to the following easily checked but useful connection between such designs and binary self-orthogonal codes.

THEOREM 1.1. *If A is a block-point $b \times v$ incidence matrix of a self-orthogonal design, then A generates a self-orthogonal binary code of length v.*

Designs of type (ii), (iii), or (iv) are easily extendable to self-orthogonal designs of type (i) by adding one or two new points to each block in an appropriate way.

Suppose that $D=(X, B)$ is a weakly self-orthogonal design. Define the sets X', X'', X^* and the families of blocks B', B'', B^* as follows: $X'=X \cup \{x_{v+1}\}$, $X''=X \cup \{x_{v+1}, ..., x_{v+b}, x_{v+b+1}\}$, $X^*=X'' \setminus \{x_{v+b+1}\}$; $B'=\{B_j \cup \{x_{v+1}\}\colon j=1, ..., b\}$, $B''=\{B_j \cup \{x_{v+j}, x_{v+b+1}\}\colon j=1, ..., b\}$, $B^*=\{B_j \cup \{x_{v+j}\}\colon j=1, ..., b\}$. Then the following assertions are easily verified:

(1) If D is of type (ii), then $D'=(X', B')$ is self-orthogonal, i.e., of type (i).

(2) If D is of type (iii) then $D''=(X'', B'')$ is of type (i).

(3) If D is of type (iv) then $D^*=(X^*, B^*)$ is of type (i).

In other words, if A is a $b \times v$ incidence matrix of a weakly self-orthogonal design D, then the following matrix

$$\begin{pmatrix} & 1 \\ A & \vdots \\ & 1 \end{pmatrix} \tag{4}$$

generates a binary self-orthogonal code of length $v+1$ provided that D is of type (ii); the matrix

$$\begin{pmatrix} & 1 \\ I_b, A & \vdots \\ & 1 \end{pmatrix} \tag{5}$$

generates a self-orthogonal code of length $b+v+1$ provided that D is of type (iii). Let us mention that if v is odd, then one can add one more block consisting of all old points plus one new point x_{v+b+2}, so that a self-orthogonal design with $v+b+2$ points and $b+1$ blocks is obtained. In coding terms, the following matrix

$$\begin{pmatrix} & 1 \cdots 1 & 0 \\ & & 1 \\ I_{b+1}, & A & \vdots \\ & & 1 \end{pmatrix} \tag{6}$$

generates a self-orthogonal code of length $v+b+2$. Finally, the matrix

$$(I_b, A) \tag{7}$$

generates a self-orthogonal code of length $b+v$ provided that D is of type (iv).

Familiar examples of weakly self-orthogonal designs are provided by symmetric 2-designs. In such a case the corresponding codes generated by matrices of the form (6) or (7) are in fact self-dual and the construction is well known [1]. In particular, if A is an incidence matrix of a Hadamard symmetric $2-(4t-1, 2t, t)$ design with odd t then the matrix (6) generates a doubly even self-dual code of length $8t$. As proved in [8], any such code has minimum weight at least 8 provided that $t>0$; in particular, the codes derived from Hadamard designs with $t \leqslant 5$ are extremal. The last result was recently "rediscovered" by Ozeki [7] (without the bound $d \geqslant 8$; the extremality has been checked by computer in [7]). Hadamard 2-designs which are extendable to isomorphic Hadamard 3-designs, produce equivalent codes [8]. In particular, there are three nonisomorphic Hadamard

3-(20, 10, 4) designs producing three extremal doubly even (40, 20, 8) codes [8]. An interesting theorem from [7] states that designs arising from equivalent adamard matrices yield equivalent codes.

Exploring the concept of a self-orthogonal design, we generalize the construction of self-dual codes based on Hadamard designs to a construction using (0, 1)-Hadamard matrices. This general construction can produce inequivalent codes from equivalent Hadamard matrices. As an application, we demonstrate that at least 79 (and perhaps many more) inequivalent extremal doubly even (40, 20) codes are obtained from the Hadamard matrices of order 20. Many of these codes do not possess any automorphisms of an odd prime order, and there is at least one code with trivial automorphism group. This seems to be the first example of an extremal doubly even code without any nontrivial automorphisms.

2. Self-Orthogonal Designs Obtained from Hadamard Matrices

Given a Hadamard matrix H of order $n=4t$, define incidence between rows and columns of H, a row and a column being incident if they intersect in $+1$. We call the incidence structure thus defined *the design of H.* An incidence matrix of the design of H is $(H+J)/2$, where J is the all–one matrix.

An essential property of a Hadamard matrix of order n is that the Hamming distance between each pair of rows is $n/2$. Consequently, the parity of the number of $+1$'s in a row is the same for all rows if $n>2$. Using this, it is straightforward to prove the following theorem.

THEOREM 2.1. *The design of a Hadamard matrix H of order $n>2$ such that the numbers of $+1$'s in all rows of H are congruent modulo 4, is weakly self-orthogonal.*

Suppose now that H is a Hadamard matrix of order $n=8t+4$ with some row (and hence all rows) containing an odd number of $+1$'s. Note that if the number of $+1$'s in a row is $\equiv 1 \pmod 4$, then multiplying that row by -1 transforms it in a row containing a number of $+1$'s $\equiv 3 \pmod 4$.

THEOREM 2.2. *Let H be a Hadamard matrix of order $n=8t+4$ such that the number of $+1$'s in each row is $\equiv 3 \pmod 4$. Then the matrix*

$$(I, A), \tag{8}$$

where $A=(H+J)/2$ is the incidence matrix of the design of H, generates a *self-dual doubly even code C of length $2n$. The minimum distance of C is at least 8 if and only if each row and column of H contains at least seven $+1$'s.*

Proof. The self-orthogonality of the code follows from the fact that the design of H is self-orthogonal of type (iv). The code C is doubly even since the weights of all rows of the generator matrix (9) are divisible by 4.

Suppose that the minimum weight d is less than 8, i.e., $d=4$. Since the matrix A is non-sigular over $GF(2)$, a code word of weight 4 must be a sum of at most three rows of (8). A row of (8) can be of weight 4 only if some row of H contains exactly three $+1$'s. Since H is a Hadamard matrix, the weight of the sum of any two rows of (8) is $2+n/2>4$ for $n>4$. If there is a code word of weight 4 being a sum of three rows of (8) then this word must be a row of the matrix

$$(A^{\mathrm{T}}, I), \tag{9}$$

which is, due to the self-duality of C, both parity check and generator matrix of C. However, (9) can have a row of weight 4 only if H contains a column with exactly three $+1$'s. ∎

Let us mention that if H is of the form

$$H=\begin{pmatrix} -1 & 1\cdots 1 \\ 1 & \\ \vdots & H' \\ 1 & \end{pmatrix} \tag{10}$$

then H' is an $(+1, -1)$ incidence matrix of a symmetric Hadamard $2-(n-1, n/2, n/4)$ design, thus the condition of Theorem 2.2 is fullfiled if $n>4$. Hence Theorem 2.2 generalizes a similar result from [8].

Theorem 2.2 gives a simple criterium for extremality of codes arising from Hadamard matrices of order 8, 12, or 20. Since the only doubly even self-dual code of length 8 is the extended Hamming code, and there is a unique extremal code of length 24, namely the extended Golay code, we illustrate our method on codes of length 40 derived from Hadamard matrices of order 20.

Starting from a particular Hadamard matrix, one can transform it into many different (but equivalent) matrices by multiplying comumns and rows with -1 so that all columns and rows contain a number of $+1$'s congruent to 3 mod 4. We have carried out an incomplete computer search for extremal codes derived from Hadamard matrices of order 20. In the cases where we obtained an extremal code we investigated the set of all 285 minimum weight code words. As known [2, 6], this set forms a 285×40 incidence matrix of a $1-(40, 8, 57)$ design. Classifying the 40 columns of

TABLE I

The 2 – (19, 10, 5) Designs

III	IV	QR
0000000001111111111	0000000001111111111	{0,2,3,8,10,12,13,14,
0000111110000011111	0000111110000011111	
0001011110111100001	0001011110111100001	15,18} (mod 19).
0011100111001100110	0011100111001101110	
0101100111110011000	0101100111110011000	
0110011011010101010	0110011011010101010	
0110011101101010100	0110011101101010100	
0111101000011010011	0111101000011010011	
0111110000100101101	0111110000100101101	
1001111001001111000	1001111001011001100	
1010101010110110100	1010101010101111000	
1010110100111001010	1010110101010110001	
1011001101010001101	1011001101100001011	
1011010011100010011	1011010010110010110	
1100101101100100011	1100101100110100110	
1100110011011000101	1100110011101000011	
1101001010101001110	1101001011000110101	
1101010100010110110	1101010100001111010	
1110000110001111001	1110000110011001101	

this matrix according to their scalar products with the remaining 39 columns, or equivalently, counting for each point of the relevant 1 – (40, 8, 57) design the number of points different from it and such that both points occur together in a certain number of blocks, we get an isomorphism invariant distinguishing the codes well enough. We found in this way at least 79 inequivalent extremal doubly even (40, 20) codes. The results are listed in Table II. For each code we indicate the Hadamard matrix producing the code, the columns which have to be negated, and the "type" of the code, giving the classification of the 40 code coordinates according to the invariant described above. For instance, the type "4(2) 8(4)" means that the set of 40 coordinates is partitioned into six subsets each consisting of coordinates with identical characteristics: 2 subsets of cardinality 4 and 4 subsets of cardinality 8. The Hadamard matrices we have started with all have the form (10). The particular 2 – (19 10, 5) designs we have used are listed in Table I. Designs III and IV are taken from [4].

3. Comments

3.1. Codes from Table II are divided into 70 classes by their type. Only the following classes contain more than one code: {1, 17}, {2, 15}, {8, 22}, {10, 12, 32, 80}, {11, 19}, {13, 29}, {16, 48}, {37, 65}. Most of these codes are also inequivalent, which can be seen by a comparison of the

TABLE II

Extremal (40, 20) Codes Derived from Hadamard Matrices of Order 20

Code	H	Negated columns	Type
1	III	1 2 3 4	4(1) 8(1) 12(1) 16(1)
2		1 2 3 6	2(7) 4(4) 10(1)
3		1 2 5 6	2(4) 8(4)
4		1 2 5 10	16(1) 24(1)
5		1 2 5 11	4(3) 8(1) 20(1)
6		1 2 5 15	4(4) 8(1) 16(1)
7		1 2 6 13	8(3) 16(1)
8		1 2 6 16	4(4) 8(3)
9		1 2 15 16	12(2) 16(1)
10		1 2 15 17	40(1)
11		1 2 15 18	8(1) 16(2)
12		1-8	40(1)
13		1-6 11 15	8(5)
14		1-6 11 16	8(1) 32(1)
15	IV	1 2 3 4	2(7) 4(4) 10(1)
16		1 2 3 8	4(2) 8(4)
17		1 2 3 10	4(1) 8(1) 12(1) 16(1)
18		1 2 3 11	1(11) 2(3) 4(3) 5(1) 6(1)
19		1 2 3 19	8(1) 16(2)
20		1 2 4 10	1(5) 2(4) 3(1) 4(6)
21		1 2 4 11	2(10) 4(1) 8(2)
22		1 2 4 13	4(4) 8(3)
23		1 2 4 16	2(4) 4(4) 8(2)
24		1 2 8 11	2(2) 4(5) 8(2)
25		1 2 10 16	2(8) 4(3) 6(2)
26		1 2 11 12	2(3) 4(5) 6(1) 8(1)
27		1 2 11 13	4(1) 6(3) 18(1)
28		1 2 11 14	2(6) 4(3) 6(1) 10(1)
29		1 2 11 15	8(5)
30		1 2 11 16	1(6) 2(7) 4(5)
31		1 2 12 18	1(1) 2(1) 3(5) 4(1) 6(3)
32		1-8	40(1)
33		1-6 11 15	2(3) 4(4) 6(3)
34		1-6 11 19	2(9) 4(4) 6(1)
35		1-6 12 16	2(11) 4(3) 6(1)
36		1-5 10 11 15	4(2) 8(1) 12(2)
37		1-5 10 11 17	4(6) 8(2)
38		1-5 10 12 19	2(6) 4(4) 6(2)
39		1-5 11 12 17	1(6) 2(7) 4(3) 8(1)
40		1-8 11 15 17 18	4(1) 6(4) 12(1)
41	QR	1 2 3 4	1(12) 2(5) 3(3) 4(1) 5(1)
42		1 2 3 5	1(12) 2(7) 3(2) 4(2)
43		1 2 3 7	2(6) 4(2) 6(1) 14(1)
44		1 2 3 8	2(9) 4(2) 6(1) 8(1)
45		1 2 3 9	2(4) 4(1) 6(1) 10(1) 12(1)
46		1 2 3 10	1(5) 2(5) 3(3) 4(4)
47		1 2 3 11	1(13) 2(5) 3(2) 4(1) 7(1)
48		1 2 3 13	4(2) 8(4)
49		1 2 3 15	1(15) 2(4) 3(3) 4(2)
50		1 2 3 16	1(4) 2(3) 3(5) 4(1) 5(1) 6(1)
51		1 2 3 17	1(10) 2(6) 3(1) 4(2) 7(1)
52		1 2 4 8	1(5) 2(1) 3(3) 4(1) 6(2) 8(1)
53		1 2 4 10	1(12) 2(4) 3(1) 4(3) 5(1)
54		1 2 4 13	1(14) 2(7) 3(1) 4(1) 5(1)
55		1 2 4 15	2(1) 4(3) 6(3) 8(1)
56		1 2 4 16	1(9) 2(2) 3(4) 4(1) 6(1)
57		1 2 4 18	2(5) 4(2) 8(1) 14(1)
58		1 2 5 6	1(10) 2(4) 3(1) 4(2) 5(1) 6(1)
59		1 2 5 14	1(11) 2(2) 3(3) 5(2) 6(1)
60		1 2 10 1	4(1) 12(3)
61		1-8	2(5) 4(2) 6(2) 10(1)
62		1-7 10	2(4) 4(2) 6(1) 8(1) 10(1)
63		1-7 12	2(5) 4(4) 14(1)
64		1-7 13	1(7) 2(5) 3(5) 4(2)
65		1-6 8 10	4(6) 8(2)
66		1-6 8 12	1(9) 4(1) 5(1) 6(1) 8(2)
67		1-6 8 18	1(4) 2(3) 4(1) 5(2) 8(2)
68		1-6 9 10	2(4) 4(1) 6(1) 8(1) 14(1)
69		1-6 10 18	2(10) 4(2) 6(2)
70		1-6 11 17	2(3) 4(1) 6(2) 8(1) 10(1)
71		1-6 12 16	2(1) 3(2) 4(1) 5(2) 6(3)
72		1-6 12 17	2(2) 4(2) 6(1) 8(1) 14(1)
73		1-11 14	2(4) 4(3) 6(2) 8(1)
74		1-11 16	2(3) 4(3) 10(1) 12(1)
75		1-10 12 15	1(1) 2(1) 3(6) 6(2) 7(1)
76		1-10 13 16	1(2) 2(1) 3(6) 6(3)
77		1-10 15 16	4(2) 8(1) 12(2)
78		1-10 16 17	2(1) 4(6) 14(1)
79		1-9 11 12 18	4(1) 12(1) 24(1)
80		None	40(1)

characteristics of coordinates belonging to subsets with the same cardinality with respect to our isomorphism invariant. For instance, given a coordinate of the code 10, the remaining 39 coordinates are partitioned into three groups containing 1, 16, and 21 coordinates respectively, while for a coordinate of the code 12 there is a group containing 37 coordinates. The only two codes with identical types and characteristics are 2 and 15. We do not know whether these two codes are equivalent or not. Therefore, Table 2 contains at least 79 inequivalent codes.

3.2. A powerful method for the construction of self-dual codes that has recently been developped considerably, is based on consideration of automorphisms (cf., e.g., [3, 5, 9]). An essential feature of this method is that it is applicable only for automorphism groups of order not divisible by the characteristic of the underlying field. In particular, for binary codes only automorphisms of an odd order are handled. It was proved in [9] that the only odd primes that can be orders of automorphisms of an extremal doubly even self-dual code of length 40 are 19, 7, 5, and 3, and there are precisely three inequivalent codes with automorphisms of order 19 and 5 codes with automorphisms of order 7. Moreover, an automorphism of order 19 fixes exactly two coordinates; an automorphism of order 7 fixes five coordinates; an automorphism of order 5 fixes either 20 or no coordinates; and an automorphism of order 3 fixes at most 22 coordinates [9]. It follows from this and the data of Table II that at least 11 codes, namely 21, 30, 35, 39, 41, 42, 47, 49, 51, 53, 54, do not possess any nontrivial automorphisms of an odd order.

In fact, some of these codes do not admit any nontrivial automorphisms at all. We have checked this for the code 41 in the following way. Consider the set of all code words of weight 8. The Hamming distance between any two such words is 8, 12, or 16. For each code word of weight 8 we compute the characteristic (n_8, n_{12}, n_{16}), where n_i is the number of code words of weight 8 being at distance i from the given word. The set of all 285 code words of weight 8 is divided into five subsets of cardinalities 5, 13, 53, 82, 132, respectively, according to their characteristics (n_8, n_{12}, n_{16}). The columns of the 53×40 matrix having as rows the words of the subset of cardinality 53 are completely distinguished by the distribution of their scalar products with the remaining columns. Thus the code 41 cannot admit any nontrivial automorphism.

Acknowledgments

The author thanks the University of Technology, Eindhoven, for the hospitality during the preparation of this paper. Thanks are due also to the referees for their useful remarks.

References

1. V. K. Bhargava and J. M. Stein, (v, k, λ) configurations and self-dual codes, *Inform. and Control* **28** (1975), 352–355.
2. P. J. Cameron and J. H. van Lint, "Graphs, Codes and Designs," Cambridge Univ. Press, Cambridge, 1980.
3. J. H. Conway and V. Pless, On primes dividing the group order of a doubly-even (72, 36, 16) code and the group order of a quaternary (24, 12, 10) code, *Discrete Math.* **38** (1982), 143–156.
4. P. B. Gibbons, "Computing Techniques for the Construction and Analysis of Block Designs," Technical Report 92, Dept. of Computer Science, University of Toronto, 1976.
5. W. C. Huffman, Automorphisms of codes with applications to extremal doubly-even codes of length 48, *IEEE Trans. Inform. Theory*, **28** (1982), 511–521.
6. F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.
7. M. Ozeki, Hadamard matrices and doubly-even self-dual error-correcting codes, *J. Combin. Theory Ser. A* **44** (1987), 274–287.
8. V. D. Tonchev, Block designs of Hadamard type and self-dual codes, *Problemy Peredachi Informatsii* **19**, No. 4 (1983), 25–30. [Russian] English translation, *Problems Inform. Transmission*, April (1984), 270–275.
9. V. Y. Yorgov, Binary self-dual codes with an automorphism of an odd order, *Problemy Peredatchi Informatsii* **19** No. 4 (1983), 11–24. [Russian] English translation, *Problems Inform. Transmission*, April (1984) 260–270.