Hadamard matrices of order 36 and double-even self-dual [72,36,12] codes

Iliya Bouyukliev[1]†, Veerle Fack[2] and Joost Winne[2]

[1] *Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, POBox 323, 5000 Veliko Tarnovo, Bulgaria. email: stefka_iliya@yahoo.com*
[2] *Research Group on Combinatorial Algorithms and Algorithmic Graph Theory, Department of Applied Mathematics and Computer Science, Ghent University, Krijgslaan 281–S9, B–9000 Ghent, Belgium. email: Joost.Winne@ugent.be, Veerle.Fack@ugent.be*

Before this work, at least 762 inequivalent Hadamard matrices of order 36 were known. We found 7238 Hadamard matrices of order 36 and 522 inequivalent $[72, 36, 12]$ double-even self-dual codes which are obtained from all 2-$(35, 17, 8)$ designs with an automorphism of order 3 and 2 fixed points and blocks.

Keywords: Hadamard designs, double-even self-dual codes

1 Introduction

A *balanced incomplete block design* (BIBD) [1] with parameters 2-(v, b, r, k, λ) (short 2-(v, k, λ)) is a pair (V, B) where V is a v-set (elements are called points) and B is a collection of b k-subsets (elements are called blocks) of V such that each point is contained in exactly r blocks and any pair of points is contained in exactly λ blocks.

A *Hadamard matrix* of order n is an $n \times n$ $(1, -1)$-matrix satisfying $HH^t = nI$. Each Hadamard matrix can be normalized, i.e. replaced by an equivalent Hadamard matrix whose first row and column are ones. When deleting the first row and column of a normalized Hadamard matrix of order $4m$, a symmetric 2-$(4m-1, 2m-1, m-1)$ design is obtained which is called a *Hadamard design*.

Hadamard matrices have been classified up to order 28. For higher orders, only partial classifications are known. Lin, Wallis and Zhu [3] found 66104 inequivalent Hadamard matrices of order 32. Extensive results on order 32 appear in [4] and [5]. Before this work, at least 762 inequivalent Hadamard matrices of order 36 were known, see [2], [6] and [7].

We found 7238 Hadamard matrices of order 36, which are obtained from all 2-$(35, 17, 8)$ designs with an automorphism of order 3 and 2 fixed points and blocks. In order to be sure about our computer results, we made two independent implementations.

A linear code with block length n, dimension k, and minimum distance d is referred to as an $[n, k, d]$-code. Hadamard designs are related to self-dual codes, see [9] and [10]. Let A be the incidence matrix

†Partially supported by the Bulgarian National Science Fund under Contract MM1304/2003.

of the inverse 2-$(35, 18, 9)$ design of 2-$(35, 17, 8)$, and $A^+ = \begin{pmatrix} A & U^t \\ U & 0 \end{pmatrix}$, where U is the all one vector of dimension 35. A generator matrix of a double-even self-dual code of length 72 can be obtained as $\begin{pmatrix} A^+ & I_{36} \end{pmatrix}$. 522 inequivalent $[72, 36, 12]$ codes are obtained from all 2-$(35, 17, 8)$ designs with an automorphism of order 3 and 2 fixed points and blocks. We obtained codes with 33 new weight enumerators different from previously known $[72, 36, 12]$ codes [8].

2 Enumeration of 2-(v, k, λ) designs with an automorphism of order 3

We briefly describe the main approach which was used for the enumeration of all 2-$(35, 17, 8)$ designs with an automorphism of order 3 and 2 fixed points and blocks.

Let A be the incidence matrix of a 2-(v, k, λ) symmetric design, with a row for each point and a column for each block. Assume an automorphism of order 3 with f fixed points and blocks which works on both the rows and columns of the incidence matrix as

(1) (2) . . . (f) (f+1 f+2 f+3) (f+4 f+5 f+6). . . (v-2 v-1 v)

Thus the first f rows and columns are fixed. We can structure the incidence matrix as

$A = \begin{pmatrix} F_{f,f} & G_{f,v-f} \\ H_{v-f,f} & X_{v-f,v-f} \end{pmatrix}$.

2.1 Generation scheme

The generation scheme can be split into the following phases:

1. Find all possible configurations for the fixed parts F, G and H.
2. For each of these fixed configurations, generate $X_{v-f,v-f}$, which is structured into $\frac{v-f}{3} \times \frac{v-f}{3}$ order 3 circulants.
   (a) Generate all $\frac{v-f}{3} \times \frac{v-f}{3}$ orbit matrices M meeting constraints derived from the design parameters. An entry in M stands for the number of ones in a row of the circulant.
   (b) Extend each unique solution for M to a full matrix X by replacing each entry m_{ij} of M by all the possible 3×3 circulants for that entry.

2.2 Orbit Matrix Generation Phase

Define $n = \frac{v-f}{3}$, h_i the number of ones in row $3i$ (or $3i-1$ or $3i-2$) of H $(1 \le i \le n)$, g_j the number of ones in column $3j$ of G $(1 \le j \le n)$, h_{pq} the scalar product between rows $3p$ and $3q$ of H and g_{pq} the scalar product between columns $3p$ and $3q$ of G. From double counting arguments on the number of ones in each row (column) and the number of (1,1) intersections between two rows (columns), the following constraints for the $n \times n$ orbit matrix M with entries m_{ij} $(1 \le i, j \le n)$ are derived:

(1) $\sum_{j=1}^{n} m_{ij} = k - h_i$; $1 \le i \le n$

(2) $\sum_{i=1}^{n} m_{ij} = k - g_j$; $1 \le j \le n$

(3) $\sum_{j=1}^{n} m_{ij}^2 = 2\lambda + k - 3h_i;$; $1 \le i \le n$

(4) $\sum_{i=1}^{n} m_{ij}^2 = 2\lambda + k - 3g_j; \; ; \; 1 \le j \le n$

(5) $\sum_{j=1}^{n} m_{pj} m_{qj} = 3(\lambda - h_{pq}) \; ; \; 1 \le p < q \le n$

(6) $\sum_{i=1}^{n} m_{ip} m_{iq} = 3(\lambda - g_{pq}) \; ; \; 1 \le p < q \le n$

In order to speed up the search, dynamic programming is used. We first determine all possible row patterns meeting constraints (1) and (3), all possible column patterns meeting constraints (2) and (4), all possible row-row intersection patterns meeting (5) and all possible column-column intersection patterns meeting (6). In the backtracking algorithm which enumerates all orbit matrices, we check after each binding of an entry (to one of the four possible values), if there remains at least one pattern which can be met (for all constraints). We use a standard backtracking algorithm which fills the matrix entry by entry, row by row. We shall call this *row order generation*. Isomorphs are partially rejected by generating rows and columns in some lexical order imposed by the fixed points and blocks.

2.3 Orbit Matrix Expanding Phase

For all obtained orbit matrices with entries from $\{0,1,2,3\}$ we extend each entry to all possible circulants. For 0 and 3 there is only a single possible circulant, but for 1 and 2 there are three possible circulants.

Row and column regularity constraints (design parameters $k = r$) are trivially satisfied. Row scalar product constraints are always satisfied between all three rows of a single extension of one row (column) of M. Here again, we use the same dynamic programming technique for all the different possible intersection patterns between two rows (columns).

When the automorphism group of the orbit matrix is trivial, we don't generate in a fixed row order generation, but select the next entry to fill which has the smallest number of possible entries left. This means we combine a backtracking algorithm with a forward checking method which reduces the possible entries after each expanding of an orbit matrix entry to a circulant.

However, when the automorphism group of the orbit matrix solution M is not trivial, we first reorder the orbit matrix based on its automorphism group, this decreases the size of the search space. The reason for this is the use of a partial isomorph rejection technique based on the automorphism group of the orbit matrix M.

The orbit matrix extension X together with the fixed parts F, G and H form the incidence matrix of the 2-(v, k, λ) Hadamard design.

3 Results

We found 63635 2-$(35, 17, 8)$ Hadamard designs with an automorphism of order 3 with 2 fixed points and blocks. These were then converted to Hadamard matrices, of which 7238 turned out to be non-isomorphic, these are summarized in Table 1.

522 inequivalent $[72, 36, 12]$ codes are obtained from all 2-$(35, 17, 8)$ designs with an automorphism of order 3 and 2 fixed points and blocks. The number of different weight enumerators is 70. In Table 2, we list all the α values of the weight enumerators written in the form

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

4 Future Work

2-$(35, 17, 8)$ and 2-$(31, 15, 7)$ designs will be further considered with an automorphism of order 3. 2-$(31, 15, 7)$ designs relate to Hadamard matrices of order 32, the first open case.

$\|Aut\|$	Non Isomorphic	$\|Aut\|$	Non Isomorphic	$\|Aut\|$	Non Isomorphic
ALL	7238				
6	6754	144	3	972	1
12	243	162	1	1152	1
18	24	192	7	1296	1
24	84	216	7	1728	1
36	23	288	2	2304	1
42	1	324	1	3072	1
48	40	336	1	3456	1
54	12	384	3	8640	1
72	4	432	3	31104	1
96	4	648	1	2903040	1
108	7	768	3		

Tab. 1: 7238 Hadamard matrices of order 36.

α	Unique	α	Unique	α	Unique	α	Unique
ALL	522						
(1) -3426	16	(19) -3450	22	(37) -3330	9	(55) -3510	3
(2) -3480	8	(20) -3360	16	(38) -3204	3	(56) -3180	1
(3) -3390	21	(21) -3324	14	(39) -3318	7	(57) -3540	1
(4) -3354	12	(22) -3024	1	(40) -3348	14	(58) -3504	9
(5) -3444	11	(23) -3252	4	(41) -3534	1	(59) -3192	1
(6) -3408	11	(24) -3294	7	(42) -3486	8	(60) -3516	2
(7) -3372	8	(25) -3300	9	(43) -3522	7	(61) -3162	2
(8) -3336	7	(26) -3384	17	(44) -3270	2	(62) -3234	2
(9) -3378	21	(27) -3264	3	(45) -3492	8	(63) -3072	1
(10) -3432	19	(28) -3462	12	(46) -3342	12	(64) -3684	1
(11) -3468	9	(29) -3228	2	(47) -3396	27	(65) -3090	1
(12) -3558	1	(30) -3456	9	(48) -3222	3	(66) -2910	1
(13) -3414	26	(31) -3420	14	(49) -3240	2	(67) -2928	1
(14) -3276	9	(32) -3402	13	(50) -3078	1	(68) -3564	2
(15) -3312	6	(33) -3474	8	(51) -3438	3	(69) -3210	1
(16) -3258	3	(34) -3282	6	(52) -3546	2	(70) -3156	1
(17) -3288	11	(35) -3552	3	(53) -3498	2		
(18) -3198	1	(36) -3366	16	(54) -3306	5		

Tab. 2: 522 double-even self-dual [72,36,12] codes.

Acknowledgements

This work was done during a visit of I. Bouyukliev in the Institute for Algebra and Geometry of the Otto-von-Guericke-University Magdeburg. He would like to thank his hosts for the nice working conditions and hospitality.

References

[1] C. Colbourn and J. Dinitz. *The CRC Handbook of Combinatorial Designs*, Boca Raton, FL., CRC Press, 7:3-41, 1996.

[2] S. Georgiou, C. Koukouvinos and J. Seberry. Hadamard matrices, orthogonal designs and construction algorithms. *Designs 2002: Further Combinatorial and Constructive Design Theory*, eds. W. D. Wallis, Kluwer, Academic Publishers, Norwell, Massachusetts, 133-205, 2002.

[3] C. Lin, D. Wallis and Zhu Lie. Generalized 4-profiles of Hadamard matrices. *J. Comb. Inf. Syst. Sci.*, 18:397-400, 1993.

[4] C. Lin, D. Wallis and Zhu Lie. Hadamard matrices of Order 32 II. Preprint 93-05, Department of Mathematical Science, University of Nevada, Las Vegas, Nevada.

[5] D. K. J. Lin and N. R. Draper. Screening properties of certain two-level designs. *Metrika*, 42:99-118, 1995.

[6] Z. Janko. The existence of a Bush-type Hadamard matrix of order 36 and two new infinite classes of symmetric designs. *J. Combin. Theory Ser. A*, 95:360-364, 2001.

[7] J. Seberry and M. Yamada. Hadamard matrices, sequences and block designs. *Contemporary Design Theory: A Collection of Surveys*, eds. J. Dinitz and D. Stinson, J. Wiley, New York, 431-560, 1992.

[8] R. Dontcheva, A. J. van Zanten, S. M. Dodunekov. Binary self-dual codes with automorphisms of composite order. *IEEE Transactions on Information Theory*, 50(2):311-318, 2004.

[9] V. D. Tonchev. Symmetric designs without ovals and extremal self-dual codes. *Annals of Discrete Math.*, 37:451-458, 1988.

[10] E. Spence, V. D. Tonchev. Extremal self-dual codes from symmetric designs. *Discrete Math.*, 110:265-268, 1992.