

Some new Menon designs with parameters (196, 91, 42)

DEAN CRNKOVIĆ*

Abstract. *There are exactly 54 symmetric (196,91,42) designs admitting an automorphism group isomorphic to $Frob_{13.6} \times Z_3$ acting with orbit size distribution (1,13,13,13,39,39,39,39) for blocks and points. For 50 of these designs the full automorphism group has order 234 and is isomorphic to $Frob_{13.6} \times Z_3$. The remaining four designs have $Frob_{13.6} \times Frob_{7.3}$ as a full automorphism group. Among these designs there are 18 self-dual designs and 18 pairs of mutually dual ones. The derived designs (with respect to the fixed block) of the four designs with a full automorphism group of order 1638 are cyclic.*

Key words: *symmetric design, Menon design, Hadamard matrix, automorphism group*

AMS subject classifications: 05B05

Received November ?, 2005

Accepted December ?, 2005

1. Introduction

A 2 -(v, k, λ) design is a finite incidence structure $(\mathcal{P}, \mathcal{B}, I)$, where \mathcal{P} and \mathcal{B} are disjoint sets and $I \subseteq \mathcal{P} \times \mathcal{B}$, with the following properties:

1. $|\mathcal{P}| = v$;
2. every element of \mathcal{B} is incident with exactly k elements of \mathcal{P} ;
3. every pair of distinct elements of \mathcal{P} is incident with exactly λ elements of \mathcal{B} .

The elements of the set \mathcal{P} are called points and the elements of the set \mathcal{B} are called blocks. If $|\mathcal{P}| = |\mathcal{B}| = v$ and $2 \leq k \leq v - 2$, then a 2 -(v, k, λ) design is called a symmetric design.

Given two designs $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1, I_1)$ and $\mathcal{D}_2 = (\mathcal{P}_2, \mathcal{B}_2, I_2)$, an isomorphism from \mathcal{D}_1 onto \mathcal{D}_2 is a bijection which maps points onto points and blocks onto blocks preserving the incidence relation. An isomorphism from a symmetric design \mathcal{D} onto

*Department of Mathematics, Faculty of Philosophy, University of Rijeka, Omladinska 14, 51 000 Rijeka, Croatia, e-mail: deanc@mapef.ffri.hr

itself is called an automorphism of \mathcal{D} . The set of all automorphisms of the design \mathcal{D} forms a group; it is called the full automorphism group of \mathcal{D} and denoted by $\text{Aut}\mathcal{D}$.

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ be a symmetric (v, k, λ) design and G a subgroup of $\text{Aut}\mathcal{D}$. The action of G produces the same number of point and block orbits (see [5, Theorem 3.3, p. 79]). We denote that number by t , the point orbits by $\mathcal{P}_1, \dots, \mathcal{P}_t$, the block orbits by $\mathcal{B}_1, \dots, \mathcal{B}_t$, and put $|\mathcal{P}_r| = \omega_r$ and $|\mathcal{B}_i| = \Omega_i$. We shall denote the points of the orbit \mathcal{P}_r by $r_0, \dots, r_{\omega_r-1}$, (i.e. $\mathcal{P}_r = \{r_0, \dots, r_{\omega_r-1}\}$). Further, we denote by γ_{ir} the number of points of \mathcal{P}_r which are incident with a representative of the block orbit \mathcal{B}_i . The numbers γ_{ir} are independent of the choice of the representative of the block orbit \mathcal{B}_i . For those numbers the following equalities hold (see [4]):

$$\sum_{r=1}^t \gamma_{ir} = k, \quad (1)$$

$$\sum_{r=1}^t \frac{\Omega_j}{\omega_r} \gamma_{ir} \gamma_{jr} = \lambda \Omega_j + \delta_{ij} \cdot (k - \lambda). \quad (2)$$

Definition 1. Let (\mathcal{D}) be a symmetric (v, k, λ) design and $G \leq \text{Aut } \mathcal{D}$. Further, let $\mathcal{P}_1, \dots, \mathcal{P}_t$ be the point orbits and $\mathcal{B}_1, \dots, \mathcal{B}_t$ the block orbits with respect to G , and let $\omega_1, \dots, \omega_t$ and $\Omega_1, \dots, \Omega_t$ be the respective orbit lengths. We call $(\mathcal{P}_1, \dots, \mathcal{P}_t)$ and $(\mathcal{B}_1, \dots, \mathcal{B}_t)$ the orbit distributions, and $(\omega_1, \dots, \omega_t)$ and $(\Omega_1, \dots, \Omega_t)$ the orbit size distributions for the design and the group G . A $(t \times t)$ -matrix (γ_{ir}) with entries satisfying conditions (1) and (2) is called an orbit structure for the parameters (v, k, λ) and orbit distributions $(\mathcal{P}_1, \dots, \mathcal{P}_t)$ and $(\mathcal{B}_1, \dots, \mathcal{B}_t)$.

The first step – when constructing designs for given parameters and orbit distributions – is to find all compatible orbit structures (γ_{ir}) . The next step, called indexing, consists of determining exactly which points from the point orbit \mathcal{P}_r are incident with a chosen representative of the block orbit \mathcal{B}_i for each number γ_{ir} . Because of a large number of possibilities, it is often necessary to involve a computer in both steps of construction.

Definition 2. The set of all indices of points of the orbit \mathcal{P}_r which are incident with a fixed representative of the block orbit \mathcal{B}_i is called the index set for the position (i, r) of the orbit structure and the given representative.

A Hadamard matrix of order m is an $(m \times m)$ -matrix $H = (h_{i,j})$, $h_{i,j} \in \{-1, 1\}$, satisfying $HH^T = H^T H = mI$, where I is the unit matrix. A Hadamard matrix is regular if the row and column sums are constant. It is well known that the existence of a symmetric design with parameters $(4u^2, 2u^2 - u, u^2 - u)$ is equivalent to the existence of a regular Hadamard matrix of order $4u^2$ (see [10, Theorem 1.4 p. 280]). Such symmetric designs are called Menon designs. If $2u + 1$ and $2u - 1$ are prime powers, there exists a symmetric Hadamard matrix with constant diagonal of order $4u^2$ (see [10, Corollary 5.12 p. 342]). Symmetric $(196, 91, 42)$ designs are the smallest Menon designs that do not belong to that family of Menon designs, since 15 is not a prime power. A.E. Brower and J.H. van Lint constructed the first symmetric $(196, 91, 42)$ design on 1983 (see [9]). Another symmetric $(196, 91, 42)$ design has been constructed recently as a member of a series of Menon designs (see [2]). As far as we know, these are the only known symmetric $(196, 91, 42)$ designs.

2. Symmetric (196,91,42) designs

Lemma 1. *Let ρ be an automorphism of a symmetric (196,91,42) design \mathcal{D} . If $|\langle \rho \rangle| = 13$, then ρ fixes exactly one point and one block of \mathcal{D} .*

Proof. By [5, Theorem 3.1 p. 78], $\langle \rho \rangle$ fixes the same number of points and blocks. Denote that number by f . Obviously, $f \equiv 1 \pmod{13}$. Using the formula $f \leq v - 2(k - \lambda)$ (see [5, Corollary 3.7 p. 82]) we get $f \in \{1, 14, 27, 40, 53, 66, 79, 92\}$. Suppose that $f = 14$. Since a fixed block must be a union of $\langle \rho \rangle$ -orbits of points, every fixed block contains 0 or 13 fixed points. Two fixed blocks must intersect at 3 fixed points, since $\lambda = 42$. Therefore each fixed block contains 13 fixed points, and the fixed structure must be a symmetric (14,13,3) design, which is impossible. This is impossible, so $f \neq 14$. In a similar way one can prove that $f \notin \{27, 40, 53, 66, 79, 92\}$. \square

We shall assume that an automorphism group isomorphic to $Frob_{13.6} \times Z_3$ acts on the symmetric (196,191,42) designs to be constructed with orbit size distribution (1,13,13,13,39,39,39,39) for blocks and points. That means that the permutation of order six has precisely 16 fixed points and 16 fixed blocks, and a direct factor Z_3 fixes precisely 40 points and 40 blocks.

Lemma 2. *Let the group $Frob_{13.6}$ act as an automorphism group of a symmetric (196, 91, 42) design \mathcal{D} in such a way that the permutation of order six fixes exactly 16 points of \mathcal{D} . Then $Frob_{13.6}$ acts on the design \mathcal{D} semistandardly with one fixed block and point and 15 orbits of length 13, with the orbit structure OS1 or OS2 shown below:*

$$OS1 = \begin{pmatrix} 0 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 7 & 7 & 7 & 7 & 7 & 7 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ 1 & 7 & 0 & 7 & 7 & 7 & 7 & 7 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ 1 & 7 & 7 & 0 & 7 & 7 & 7 & 7 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ 1 & 7 & 7 & 7 & 0 & 7 & 7 & 7 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ 1 & 7 & 7 & 7 & 7 & 0 & 7 & 7 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ 1 & 7 & 7 & 7 & 7 & 7 & 0 & 7 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ 0 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 0 & 7 & 7 & 7 & 7 & 7 & 7 \\ 0 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 7 & 0 & 7 & 7 & 7 & 7 & 7 \\ 0 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 7 & 7 & 0 & 7 & 7 & 7 & 7 \\ 0 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 7 & 7 & 7 & 0 & 7 & 7 & 7 \\ 0 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 7 & 7 & 7 & 7 & 0 & 7 & 7 \\ 0 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 7 & 7 & 7 & 7 & 7 & 0 & 7 \\ 0 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 7 & 7 & 7 & 7 & 7 & 7 & 0 \end{pmatrix}$$

$$OS2 = \begin{pmatrix} 0 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 0 & 7 & 7 & 7 & 7 & 7 \\ 1 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 7 & 0 & 7 & 7 & 7 & 7 \\ 1 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 7 & 7 & 0 & 7 & 7 & 7 \\ 1 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 7 & 7 & 7 & 0 & 7 & 7 \\ 1 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 7 & 7 & 7 & 7 & 0 & 7 \\ 1 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 7 & 7 & 7 & 7 & 7 & 0 \\ 0 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 7 & 7 & 7 & 7 & 7 & 0 \\ 0 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 0 & 7 & 7 & 7 & 7 & 7 & 7 \\ 0 & 0 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 6 & 6 & 6 & 6 & 6 & 6 \\ 0 & 7 & 0 & 7 & 7 & 7 & 7 & 7 & 7 & 6 & 6 & 6 & 6 & 6 & 6 \\ 0 & 7 & 7 & 0 & 7 & 7 & 7 & 7 & 7 & 6 & 6 & 6 & 6 & 6 & 6 \\ 0 & 7 & 7 & 7 & 0 & 7 & 7 & 7 & 7 & 6 & 6 & 6 & 6 & 6 & 6 \\ 0 & 7 & 7 & 7 & 7 & 0 & 7 & 7 & 7 & 6 & 6 & 6 & 6 & 6 & 6 \\ 0 & 7 & 7 & 7 & 7 & 7 & 0 & 7 & 7 & 6 & 6 & 6 & 6 & 6 & 6 \\ 0 & 7 & 7 & 7 & 7 & 7 & 7 & 0 & 7 & 6 & 6 & 6 & 6 & 6 & 6 \end{pmatrix}$$

where the first row and column correspond to the fixed block and point, respectively.

Proof. Let the group G be isomorphic to the Frobenius group $Frob_{13.6}$. Since there is only one isomorphism class of such groups of order 78 we may write

$$G = \langle \rho, \sigma \mid \rho^{13} = 1, \sigma^6 = 1, \rho^\sigma = \rho^4 \rangle.$$

The Frobenius kernel $\langle \rho \rangle$ of order 13 acts on \mathcal{D} semistandardly with one fixed block and point and 15 orbits of length 13. Since $\langle \rho \rangle \triangleleft G$, the element σ of order 6 maps $\langle \rho \rangle$ -orbits onto $\langle \rho \rangle$ -orbits. The permutation σ fixes exactly 16 points, so G acts on \mathcal{D} with one fixed block and point and 15 orbits of length 13 for blocks and points.

The stabilizer of each block from a block orbit of length 13 is conjugate to $\langle \sigma \rangle$. Therefore, the entries of the orbit structures corresponding to point and block orbits of length 13 must satisfy the condition $\gamma_{ir} \equiv 0, 1 \pmod{6}$. Solving equations (1) and (2), we get – up to isomorphism – exactly two solutions, the orbit structures $OS1$ and $OS2$. \square

Let G_1 be isomorphic to the group $Frob_{13.6} \times Z_3$. We may write

$$G_1 = \langle \rho, \sigma, \tau \mid \rho^{13} = 1, \sigma^6 = 1, \tau^3 = 1, \rho^\sigma = \rho^4, \rho^\tau = \rho, \sigma^\tau = \sigma \rangle.$$

Theorem 1. *There are exactly 54 symmetric (196, 91, 42) designs admitting an automorphism group isomorphic to $Frob_{13.6} \times Z_3$ acting with orbit size distribution (1, 13, 13, 13, 39, 39, 39, 39) for blocks and points. For 50 of these designs the full automorphism group has order 234 and is isomorphic to $Frob_{13.6} \times Z_3$. The remaining four designs have $Frob_{13.6} \times Frob_{7.3}$ as full automorphism group. Among these designs there are 18 self-dual designs and 18 pairs of mutually dual ones.*

Proof. The designs have been constructed by the method described in [1] and [3]. We denote the points by $1_0, 2_i, \dots, 16_i, i = 0, 1, \dots, 12$ and put $G_1 = \langle \rho, \sigma, \tau \rangle$ where the generators for G_1 are permutations defined as follows:

$$\rho = (1_0)(I_0 I_1 \dots I_{12}), \quad I = 2, \dots, 16,$$

$$\sigma = (1_0)(K_0)(K_1 K_4 K_3 K_{12} K_9 K_{10}) (K_2 K_8 K_6 K_{11} K_5 K_7), \quad K = 2, \dots, 16,$$

$$\tau = (1_0)(2_i)(3_i 4_i 5_i)(6_i 7_i 8_i)(9_i)(10_i)(11_i 12_i 13_i)(14_i 15_i 16_i), \quad i = 0, 1, \dots, 12.$$

Indexing the fixed part of an orbit structure is a trivial task. Therefore, we shall consider only the right-lower part of the orbit structure of order 15. To eliminate isomorphic structures during the indexing process we have used the permutation which – on each $\langle \rho \rangle$ -point-orbit – acts as $x \mapsto 2x \pmod{13}$, and those automorphisms of the orbit structures $OS1$ and $OS2$ which commute with τ .

As representatives for the block orbits we chose blocks fixed by $\langle \sigma \rangle$. Therefore, the index sets – numbered from 0 to 4 – which could occur in the designs are among the following:

$$\begin{aligned} 0 &= \emptyset, & 1 &= \{1, 3, 4, 9, 10, 12\}, & 2 &= \{2, 5, 6, 7, 8, 11\}, & 3 &= \{0, 1, 3, 4, 9, 10, 12\}, \\ 4 &= \{0, 2, 5, 6, 7, 8, 11\}. \end{aligned}$$

The indexing process of the orbit structure $OS1$ led to 18 designs denoted by $\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_{18}$. The orbit structure $OS2$ produces 36 designs denoted by $\mathcal{D}_{19}, \mathcal{D}_{20}, \dots, \mathcal{D}_{54}$. Comparing statistics of intersections of any three blocks and using Nauty [6], we found out that the designs $\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_{54}$ are mutually non-isomorphic. The designs $\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_{18}$ are self-dual, and the other designs are dual in pairs.

We have determined the automorphism groups of the designs constructed using GAP [7] and a program by V. D. Tonchev [8]. Self-dual designs \mathcal{D}_1 and \mathcal{D}_2 , and mutually dual designs \mathcal{D}_{19} and \mathcal{D}_{20} , have the full automorphism group isomorphic to $Frob_{13.6} \times Frob_{7.3}$. The other fifty designs have the full automorphic group isomorphic to $Frob_{13.6} \times Z_3$.

We write down base blocks for designs \mathcal{D}_1 , \mathcal{D}_2 and \mathcal{D}_{19} in terms of the index sets defined above:

\mathcal{D}_1	\mathcal{D}_2
0 3 3 3 4 4 4 1 2 1 1 1 2 2 2	0 3 3 3 4 4 4 1 2 1 1 1 2 2 2
4 0 3 4 3 3 4 1 1 1 2 2 1 2 2	4 0 3 4 3 3 4 1 2 1 2 2 1 1 2
4 4 0 3 4 3 3 1 1 2 1 2 2 1 2	4 4 0 3 4 3 3 1 2 2 1 2 2 1 1
4 3 4 0 3 4 3 1 1 2 2 1 2 2 1	4 3 4 0 3 4 3 1 2 2 2 1 1 2 1
3 4 3 4 0 4 3 1 2 2 2 1 1 1 2	3 4 3 4 0 4 3 1 1 1 2 2 2 2 1
3 4 4 3 3 0 4 1 2 1 2 2 2 1 1	3 4 4 3 3 0 4 1 1 2 1 2 1 2 2
3 3 4 4 4 3 0 1 2 2 1 2 1 2 1	3 3 4 4 4 3 0 1 1 2 2 1 2 1 2
2 2 2 2 2 2 2 0 4 4 4 4 4 4 4	2 2 2 2 2 2 2 0 4 4 4 4 4 4 4
1 2 2 2 1 1 1 3 0 3 3 3 4 4 4	1 1 1 1 2 2 2 3 0 4 4 4 3 3 3
2 2 1 1 1 2 1 3 4 0 3 4 3 4 3	2 2 1 1 2 1 1 3 3 0 4 3 3 4 4
2 1 2 1 1 1 2 3 4 4 0 3 3 3 4	2 1 2 1 1 2 1 3 3 3 0 4 4 3 4
2 1 1 2 2 1 1 3 4 3 4 0 4 3 3	2 1 1 2 1 1 2 3 3 4 3 0 4 4 3
1 2 1 1 2 1 2 3 3 4 4 3 0 4 3	1 2 1 2 1 2 1 3 4 4 3 3 0 3 4
1 1 2 1 2 2 1 3 3 3 4 4 3 0 4	1 2 2 1 1 1 2 3 4 3 4 3 4 0 3
1 1 1 2 1 2 2 3 3 4 3 4 4 3 0	1 1 2 2 2 1 1 3 4 3 3 4 3 4 0

$$\mathcal{D}_{19}$$

1	1	1	1	2	2	2	2	0	3	3	3	4	4	4
1	1	2	2	1	1	2	2	4	0	3	4	3	3	4
1	2	1	2	2	1	1	2	4	4	0	3	4	3	3
1	2	2	1	1	2	1	2	4	3	4	0	3	4	3
2	2	1	1	1	1	2	2	3	4	3	4	0	4	3
2	1	2	1	2	1	1	2	3	4	4	3	3	0	4
2	1	1	2	1	2	1	2	3	3	4	4	4	3	0
2	2	2	2	2	2	2	0	4	4	4	4	4	4	4
0	3	3	3	4	4	4	4	2	2	2	2	1	1	1
4	0	3	4	3	4	3	4	2	2	1	1	1	2	2
4	4	0	3	3	3	4	4	2	1	2	1	2	1	2
4	3	4	0	4	3	3	4	2	1	1	2	2	2	1
3	4	4	3	0	4	3	4	1	2	1	2	2	1	2
3	3	4	4	3	0	4	4	1	2	2	1	2	2	1
3	4	3	4	4	3	0	4	1	1	2	2	1	2	2

From these “small” incidence matrices it is easy to obtain incidence matrices in the ordinary form. \square

The design \mathcal{D}_1 is isomorphic to a member of the series of Menon designs described in [2].

Let \mathcal{D} be a symmetric (v, k, λ) design and let x be a block of \mathcal{D} . Remove x and all points that do not belong to x from other blocks. The result is a 2 - $(k, \lambda, \lambda - 1)$ design, a derived design of \mathcal{D} with respect to the block x .

A 2 - (v, k, λ) design with an automorphism group G is called cyclic if G contains a cycle of length v . The derived design of \mathcal{D}_1 , \mathcal{D}_2 , \mathcal{D}_{19} and \mathcal{D}_{20} with respect to the first block are cyclic 2 - $(91, 42, 41)$ designs.

References

- [1] D. CRNKOVIĆ, *Symmetric $(70, 24, 8)$ designs having $\text{Frob}_{21} \times Z_2$ as an automorphism group*, Glas. Mat., III. Ser. Vol. **34(54)**(1999), 109–121.
- [2] D. CRNKOVIĆ, *A series of regular Hadamard matrices*, Des. Codes Cryptogr., to appear.
- [3] Z. JANKO, *Coset enumeration in groups and constructions of symmetric designs*, Combinatorics **90**(1992), 275–277.
- [4] Z. JANKO, T. VAN TRUNG, *Construction of a new symmetric block design for $(78, 22, 6)$ with the help of tactical decomposition*, J. of Comb. Theory, Series A **40**(1985), 451–455.
- [5] E. LANDER, *Symmetric Designs: An Algebraic Approach*, Cambridge University Press, 1983.

- [6] B. D. MCKAY, *Nauty Users Guide (version 1.5) Technical report TR-CS-90-02*, Department of Computer Science, Australian National University, 1990.
- [7] M. SCHÖNERT ET AL., *GAP - Groups, Algorithms and Programming*, Lehrstuhl für Mathematik, RWTH Aachen, 1995.
- [8] V. D. TONCHEV, *MTU*, private communication via Z. Janko of Universität Heidelberg.
- [9] T. VAN TRUNG, *Symmetric designs*, in: *The CRC Handbook of Combinatorial Designs*, (C. J. Colbourn and J. H. Dinitz, Eds.), CRC Press, 1996, 75–87.
- [10] W. D. WALLIS, A. P. STREET, J. S. WALLIS, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard matrices*, Springer Verlag, Berlin-Heidelberg-New York, 1972.