Applied Mathematics E-Notes, 7(2007), 124-130 © ISSN 1607-2510
Available free at mirror sites of http://www.math.nthu.edu.tw/∼amen/

Construction Of Menon Designs With Parameters (784,378,182) And (900,435,210)*

Dean Crnković†

Received 7 March 2007

Abstract

We describe a construction of symmetric designs with parameters (784,378,182) and (900,435,210) having an automorphism group isomorphic to $Frob_{29\cdot 14} \times Z_{13}$ and $Frob_{31\cdot 15} \times Z_{14}$, respectively. The derived designs of the constructed designs, with respect to the fixed block, are 1-rotational.

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 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 $Aut\mathcal{D}$.

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ be a symmetric (v, k, λ) design and G a subgroup of $Aut\mathcal{D}$. The action of G produces the same number of point and block orbits (see [9, Theorem 3.3, pp. 79]). We denote that number by t, the point orbits by $\mathcal{P}_1, \ldots, \mathcal{P}_t$, the block orbits by $\mathcal{B}_1, \ldots, \mathcal{B}_t$, 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 $r_0, \ldots, r_{\omega_r - 1}$, (i.e. $\mathcal{P}_r = \{r_0, \ldots, r_{\omega_r - 1}\}$). Further, we denote by γ_{ir} the number of points of $\mathcal{P}_r$ which are incident with a representative of the block orbit $\mathcal{B}_i$.

*Mathematics Subject Classifications: 05B05

†Department of Mathematics, Faculty of Philosophy, University of Rijeka, Omladinska 14, 51000 Rijeka, Croatia

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 [8]):

$$\sum_{r=1}^{t} \gamma_{ir} = k, \tag{1}$$

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

DEFINITION 1. Let $(\mathcal{D})$ be a symmetric (v, k, λ) design and $G \leq Aut\ \mathcal{D}$. Further, let $\mathcal{P}_1, \ldots, \mathcal{P}_t$ be the point orbits and $\mathcal{B}_1, \ldots, \mathcal{B}_t$ the block orbits with respect to G, and let $\omega_1, \ldots, \omega_t$ and $\Omega_1, \ldots, \Omega_t$ be the respective orbit lengths. We call $(\mathcal{P}_1, \ldots, \mathcal{P}_t)$ and $(\mathcal{B}_1, \ldots, \mathcal{B}_t)$ the orbit distributions, and $(\omega_1, \ldots, \omega_t)$ and $(\Omega_1, \ldots, \Omega_t)$ 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 $(\mathcal{P}_1, \ldots, \mathcal{P}_t)$ and $(\mathcal{B}_1, \ldots, \mathcal{B}_t)$.

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 in 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 the large number of possibilities, it is often necessary to involve a computer in both steps of the 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 $HH^T = H^T H = mI_m$, where I_m is an $(m \times m)$ identity matrix. Two Hadamard matrices are equivalent if one can be transformed into the other by a series of row or column permutations and negations. A Hadamard matrix is normalized if all entries in its first row and column are 1. If we delete the first row and column of a normalized Hadamard matrix of order m and replace -1 by 0, we obtain the incidence matrix of a symmetric $(m-1, \frac{m}{2}-1, \frac{m}{4}-1)$ design (see [9]). From any symmetric design with parameters $(m-1, \frac{m}{2}-1, \frac{m}{4}-1)$ we my in turn recover a normalized Hadamard matrix. Such a symmetric design is called a Hadamard design. The complement od such a design is a symmetric $(m-1, \frac{m}{2}, \frac{m}{4})$ design.

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 [15, Theorem 1.4 pp. 280]). Such symmetric designs are called Menon designs.

Designs find their application in various fields, including coding theory, threshold schemes, visual cryptography, and design of experiments (see e.g. [1], [2], [12], and [13]). Hadamard matrices also have wide range of application (see e.g. [11]), which includes construction of maximal codes, achieving the Plotkin bound.

An (n, M, d) code is a binary code C of length n, minimum distance d, and size $M = |C|$. Let A be the incidence matrix of a symmetric Hadamard $(m-1, \frac{m}{2}, \frac{m}{4})$ design. Then (see [13, Examples 1.160 and Theorem 1.161 pp. 698]):

1. The rows of A and the zero vector form a maximal $(m-1, m, \frac{m}{2})$ code C_m.

2. The words of C_m together with their complements, obtained by replacing 0 by 1 and vice versa, form a maximal $(m-1, 2m, \frac{m}{2}-1)$ code.

3. The words of C_m beginning with zero after deleting the first coordinate form a maximal $(m-2, \frac{m}{2}, \frac{m}{2})$ code.

Thus, from symmetric (784,378,182) designs we can construct maximal (783,784,392), (783,1568,391), and (782,392,392) codes, which could correct up to 195 errors. In the same way from symmetric (900,435,210) designs one constructs maximal (899,900,450), (899,1800,449), and (898,450,450) codes, which could correct up to 224 errors.

Further, the code designed from an $(m \times m)$ Hadamard matrix H in the following way:

$$\begin{bmatrix} H \\ -H \end{bmatrix}$$

has the minimum distance equal to $\frac{m}{2}$, and therefore has maximal error correcting capability for a given length of a codeword (see [11]). Symmetric (784,378,182) designs lead to (784,1568,392) codes, which could correct up to 195 errors. Similarly, symmetric (900,435,210) designs produce (900,1800,450) codes, which correct up to 224 errors.

For each of Menon designs described in this paper we compute 2-rank of its incidence matrix, i.e., the dimension of the binary linear code spanned by the incidence matrix.

It is known that Menon designs with parameters $(4n^2, 2n^2-n, n^2-n)$ exist whenever $2n-1$ and $2n+1$ are both prime powers (see [6]). Therefore, Menon designs with parameters (784,378,182) and (900,435,210) have been known to exist. However, only a few examples of designs with these parameters have been constructed so far.

2 Orbit Structures

For $v \in N$ we denote by j_v the all-one vector of dimension v, by 0_v the zero-vector of dimension v, and by J_v the all-one matrix of dimension $(v \times v)$.

LEMMA 1. Let n be a positive integer. The matrix

$$OS = \left[\begin{array}{c|c|c|c} 1 & (2n+1)j_{n-1}^T & 0 & 0_{n-1}^T \\ \hline j_{n-1} & (n+1)J_{n-1} - nI_{n-1} & nj_{n-1} & nJ_{n-1} \\ \hline 0 & nj_{n-1}^T & 1 & (n+1)j_{n-1}^T \\ \hline 0_{n-1} & nJ_{n-1} & (n+1)j_{n-1} & (n+1)J_{n-1} - nI_{n-1} \end{array}\right]$$

is an orbit structure for the parameters $(4n^2, 2n^2-n, n^2-n)$ and the orbit size distribution $(1, 2n+1, 2n+1, \ldots, 2n+1)$.

PROOF. The matrix OS satisfies equalities (1) and (2).

In [10] M.-O. Pavčević used orbit matrices of the type OS when $2n+1$ is a prime.

3 Symmetric (784,378,182) Designs

To our knowledge, none symmetric (784,378,182) design has been constructed and studied so far. In our construction of symmetric (784,378,182) designs we use the group

$$G_1 = \langle \rho, \sigma, \tau |\ \rho^{29} = 1,\ \sigma^{14} = 1,\ \tau^{13} = 1,\ \rho^{\sigma} = \rho^4,\ \rho^{\tau} = \rho,\ \sigma^{\tau} = \sigma \rangle.$$

isomorphic to $Frob_{29\cdot 14} \times Z_{13}$. We shall assume that an automorphism group $H_1 \leq G_1$ isomorphic to $Frob_{29\cdot 14}$ acts on the symmetric (784,378,182) designs to be constructed with one fixed points (and blocks), and 27 orbits of size 29. That means that the permutation of order 14 has precisely 28 fixed points (and 28 fixed blocks). Orbit structure of the type OS, for $n = 14$, corresponds to such action of H_1 on a symmetric (784,378,182) design. We shall proceed with indexing of the orbit structure OS by the method described in [7], having in mind the action of τ on the H_1-orbits, as described in [3].

We denote the points of the design by $1_0, 2_i, \ldots, 28_i$, $i = 0, 1, \ldots, 28$, and put $G_1 = \langle \rho, \sigma, \tau \rangle$, where the generators for G_1 are permutations defined as follows:

$$\rho = (1_0)(I_0 I_1 \ldots I_{28}),\ I = 2, \ldots, 28,$$

$$\sigma = (1_0)(K_0)(K_1 K_4 K_{16} K_6 K_{24} K_9 K_7 K_{28} K_{25} K_{13} K_{23} K_5 K_{20} K_{22})$$
$$(K_2 K_8 K_3 K_{12} K_{19} K_{18} K_{14} K_{27} K_{21} K_{26} K_{17} K_{10} K_{11} K_{15}),\ K = 2, \ldots, 28,$$

$$\tau = (1_0)(2_i 3_i 4_i 5_i 6_i 7_i 8_i 9_i 10_i 11_i 12_i 13_i 14_i)(15_i)$$
$$(16_i 17_i 18_i 19_i 20_i 21_i 22_i 23_i 24_i 25_i 26_i 27_i 28_i),\ i = 0, 1, \ldots, 28.$$

As representatives for the block orbits we chose blocks fixed by $\langle \sigma \rangle$. Therefore, the index sets which could occur in the designs are among the following:
$0 = \{0\},\ \ 1 = \{1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28\}$,
$2 = \{2, 3, 8, 10, 11, 12, 14, 15, 17, 18, 19, 21, 26, 27\}$,
$3 = \{0, 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28\}$,
$4 = \{0, 2, 3, 8, 10, 11, 12, 14, 15, 17, 18, 19, 21, 26, 27\}$.

The indexing process of the orbit structure OS leads to three designs, denoted by $\mathcal{D}_1^1$, $\mathcal{D}_2^1$, and $\mathcal{D}_3^1$. These designs are self-dual. The designs $\mathcal{D}_1^1$, $\mathcal{D}_2^1$, and $\mathcal{D}_3^1$ have the full automorphism group of order 15834, isomorphic to $Frob_{29\cdot 14} \times Frob_{13\cdot 3}$, and their 2-rank is 366. A computer program by Vladimir D. Tonchev [14] computes the order as well as generators of the full automorphism group for each of the designs found. Another computer program by V. D. Tonchev [14] computes 2-rank of the designs. The group structures have been determined with the help of GAP [5].

We write down base blocks for the designs $\mathcal{D}_1^1$, $\mathcal{D}_2^1$ and $\mathcal{D}_3^1$, in terms of the index sets defined above. Since indexing the fixed part of an orbit stucture is a trivial task, we write down base blocks omitting the fixed part. It is sufficient to write down representatives of the 2^{nd}, 15^{th}, and 16^{th} H_1-orbit, since the other H_1-orbits could be obtained as their $\langle \tau \rangle$-images.

$\mathcal{D}_1^1$
033343344344411112122121222
222222222222204444444444444
211121211212230444344334333

$\mathcal{D}_2^1$
033343344344411112221212212
222222222222204444444444444
212112121112230444344334333

$\mathcal{D}_3^1$
033343344344411121212112222
222222222222204444444444444
211112212121230444344334333

4 Symmetric (900,435,210) Design

Six symmetric designs with parameters (900,435,210) are described in [4]. Although symmetric designs with parameters (900,435,210) have been known to exist for a long time, as far as we know these are the only known symmetric (900,435,210) designs.

Let us describe a construction of a symmetric (900,435,210) design using the group

$$G_2 = \langle \rho, \sigma, \tau |\ \rho^{31} = 1,\ \sigma^{15} = 1,\ \tau^{14} = 1,\ \rho^{\sigma} = \rho^7,\ \rho^{\tau} = \rho,\ \sigma^{\tau} = \sigma \rangle$$

isomorphic to $Frob_{31\cdot 15} \times Z_{14}$. We denote the points of the design by $1_0, 2_i, \ldots, 30_i$, $i = 0, 1, \ldots, 30$, and put $G_2 = \langle \rho, \sigma, \tau \rangle$, where the generators for G_2 are permutations defined as follows:

$\rho = (1_0)(I_0 I_1 \ldots I_{30}),\ I = 2, \ldots, 30,$

$\sigma = (1_0)(K_0)(K_1 K_7 K_{18} K_2 K_{14} K_5 K_4 K_{28} K_{10} K_8 K_{25} K_{20} K_{16} K_{19} K_9)$
$(K_3 K_{21} K_{23} K_6 K_{11} K_{15} K_{12} K_{22} K_{30} K_{24} K_{13} K_{29} K_{17} K_{26} K_{27}),\ K = 2, \ldots, 30,$

$\tau = (1_0)(2_i 3_i 4_i 5_i 6_i 7_i 8_i 9_i 10_i 11_i 12_i 13_i 14_i 15_i)(16_i)$
$(17_i 18_i 19_i 20_i 21_i 22_i 23_i 24_i 25_i 26_i 27_i 28_i 29_i 30_i),\ i = 0, 1, \ldots, 30.$

Orbit structure OS led to one design, denoted by $\mathcal{D}_1^2$. Base blocks of $\mathcal{D}_1^2$, with respect to the group G_2 in terms of index sets are given below:

$\mathcal{D}_1^2$
033443434344331111121222211122
111111111111110333333333333333
122112222121113044334343433344

The index sets which occur in the designs are:
$0 = \{0\},\ \ 1 = \{1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\},$
$2 = \{3, 6, 11, 12, 13, 15, 17, 21, 22, 23, 24, 26, 27, 29, 30\},$
$3 = \{0, 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\},$
$4 = \{0, 3, 6, 11, 12, 13, 15, 17, 21, 22, 23, 24, 26, 27, 29, 30\}.$

The design $\mathcal{D}_1^2$ is self-dual, and the full automorphism group of $\mathcal{D}_1^2$ is isomorphic to $Frob_{31\cdot 15} \times Z_{14}$. Six symmetric designs with parameters (900,435,210) described in [4] have the full automorphism group isomorphic to $Frob_{29\cdot 14} \times Z_{13}$, so the design $\mathcal{D}_1^2$

can not be isomorphic to any of these designs. It is known that $p-$rank of a symmetric (v,k,λ) design is v if p does not divide $k(k-\lambda)$ (see [13, Theorem 1.86, pp. 686]). Thus, 2-rank of the design $\mathcal{D}_1^2$ is 900.

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 $\mathcal{D}$ is called $k-$rotational if some automorphism of $\mathcal{D}$ has one fixed point and k cycles each of length $\frac{v-1}{k}$. The derived designs of $\mathcal{D}_1^1$, $\mathcal{D}_2^1$, and $\mathcal{D}_3^1$ with respect to the fixed block are 1-rotational 2-(378,182,181) designs. Similarly, the derived design of $\mathcal{D}_1^2$ with respect to the fixed block is a 1-rotational 2-(435,210,209) design.

5 Hadamard Designs with Parameters (783,391,195) and (899,449,224)

The designs $\mathcal{D}_1^1$, $\mathcal{D}_2^1$ and $\mathcal{D}_3^1$, by normalizing the incidence matrices and then deleting the first row and column, produce Hadamard designs with parameters (783,391,195) having the full automorphism groups of order 15834, 15834, and 855036, respectively. The 2-rank of each of these three designs equals 365. The automorphism group of order 855036 possesses the subgroup of order 783, isomorphic to $E_{27} \times Z_{29}$, which acts regularly on the Hadamard design obtained from $\mathcal{D}_3^1$. The Hadamard design obtained from the design $\mathcal{D}_3^1$, by normalizing the incidence matrix and then deleting the first row and column, is the development of a twin prime power difference set (see [2, Theorem 8.2 pp. 354]).

Normalizing the incidence matrix of $\mathcal{D}_1^2$ and then deleting the first row and column leads us to the Hadamard design with parameters (899,449,224), which is the development of a twin prime power difference set. This Hadamard design has the full automorphism group of order 377580. The derived subgroup of $Aut\mathcal{D}_1^2$ is the cyclic group of order 899, which acts regularly on the design. Clearly, the 2-rank of this design is 899.

References

[1] E. F. Assmus Jr., J. D. Key, Designs and Their Codes, Cambridge University Press, Cambridge, 1992.

[2] T. Beth, D. Jungnickel, H. Lenz, Design Theory, 2^{nd} ed., Cambridge University Press, Cambridge, 1999.

[3] D. Crnković, Symmetric (70,24,8) designs having $Frob_{21} \times Z_2$ as an automorphism group, Glas. Mat. Ser. III, 34(54)(1999), 39-45.

[4] D. Crnković, On Some Menon Designs, Int. Math. Forum, 2(43)(2007), 2099–2107.

[5] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4, `http://www.gap-system.org` (2004).

[6] Y. J. Ionin, Tran van Trung, Symmmetric Designs, in: Handbook of Combinatorial Designs, 2^{nd} ed., (C. J. Colbourn and J. H. Dinitz, Eds.), Chapman & Hall/CRC, Boca Raton, 2007, 110–124.

[7] Z. Janko, Coset Enumeration in Groups and Constructions of Symmetric Designs, Combinatorics '90 (1992), 275–277.

[8] Z. Janko, Tran van Trung, Construction of a new symmetric block design for (78,22,6) with the help of tactical decomposition, J. Combin. Theory Ser. A, 40(2)(1985), 451–455.

[9] E. Lander, Symmetric Designs: An Algebraic Approach, Cambridge University Press, Cambridge, 1983.

[10] M.-O. Pavčević, Symmetric designs of Menon series admitting an action of Frobenius groups, Glas. Mat. Ser. III, 31(51)(1996), 209–223.

[11] J. Seberry, B. J. Wysocki, T. A. Wysocki, On some application of Hadamard matrices, Metrika, 62(2-3)(2005), 221–239.

[12] D. R. Stinson, Combinatorial Designs with Selected Application, Lecture Notes, University of Manitoba, 1996.

[13] V. D. Tonchev, Codes, in: Handbook of Combinatorial Designs, 2^{nd} ed., (C. J. Colbourn and J. H. Dinitz, Eds.), Chapman & Hall/CRC, Boca Raton, 2007, 667–702.

[14] V. D. Tonchev, Private communication via Z. Janko.

[15] W. D. Wallis, A. P. Street, J. S. Wallis, Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices, Springer Verlag, Berlin-Heidelberg-New York, 1972.