On some Menon designs and related structures

Dean Crnković
Department of Mathematics
University of Rijeka
Croatia

ALCOMA 15, March 2015

A $t-(v,k,\lambda)$ **design** is a finite incidence structure $\mathcal{D}=(\mathcal{P},\mathcal{B},\mathcal{I})$ satisfying the following requirements:

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

Every element of $\mathcal{P}$ is incident with exactly $r=\frac{\lambda(v-1)}{k-1}$ elements of $\mathcal{P}$. The number of blocks is denoted by b.
If $|\mathcal{P}|=|\mathcal{B}|$ (or equivalently $k=r$) then the design is called **symmetric**.

A **Hadamard matrix** of order m is a $(m \times m)$ 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. A Hadamard matrix is **regular** if the row and column sums are constant.

The existence of a symmetric design with parameters $(4n-1, 2n-1, n-1)$ is equivalent to the existence of a Hadamard matrix of order $4n$. Such a simmetric design is called a **Hadamard design**.

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 $4u^2$. Such symmetric designs are called **Menon designs**.

In 2006 there were just two values of $k \leq 100$ for which the existence of a regular Hadamard matrix of order $4k^2$ was still in doubt, namely $k = 47$ and $k = 79$.
In 2007 T. Xia, M. Xia and J. Seberry presented the following result:

There exist regular Hadamard matrices of order $4k^2$ for $k = 47$, 71, 151, 167, 199, 263, 359, 439, 599, 631, 727, 919, $5q_1, 5q_2N, 7q_3$, where q_1, q_2 and q_3 are prime power such that $q_1 \equiv 1 \ (mod\ 4)$, $q_2 \equiv 5 \ (mod\ 8)$ and $q_3 \equiv 3 \ (mod\ 8)$, $N = 2^a 3^b t^2$, $a, b = 0$ or 1, $t \neq 0$ is an arbitrary integer.
(T. Xia, M. Xia and J. Seberry, Some new results of regular Hadamard matrices and SBIBD II, Australas. J. Combin. 37 (2007), 117–125.)

Theorem 1 [DC, 2006]

Let p and $2p-1$ be prime powers and $p \equiv 3 \ (mod\ 4)$. Then there exists a symmetric $(4p^2, 2p^2-p, p^2-p)$ design.

That proves that there exists a regular Hadamard matrix of order $4 \cdot 79^2 = 24964$.

The smallest k for which the existence of a regular Hadamard matrix of order $4k^2$ is sill undecided is $k = 103$.

Sketch of the proof:

Let p be a prime power, $p \equiv 3 \ (mod\ 4)$ and F_p be a field with p elements. Then a $(p \times p)$ matrix $D = (d_{ij})$, such that

$$d_{ij} = \begin{cases} 1, & \text{if } (i-j) \text{ is a nonzero square in } F_p, \\ 0, & \text{otherwise.} \end{cases}$$

is an incidence matrix of a symmetric $(p, \frac{p-1}{2}, \frac{p-3}{4})$ design (Paley design). Let $\overline{D}$ be an incidence matrix of a complementary symmetric design with parameters $(p, \frac{p+1}{2}, \frac{p+1}{4})$.

Since D is a skew matrix, $D + I_p$ and $\overline{D} - I_p$ are incidence matrices of symmetric designs with parameters $(p, \frac{p+1}{2}, \frac{p+1}{4})$ and $(p, \frac{p-1}{2}, \frac{p-3}{4})$, respectively. (We say that a $(0,1)$-**matrix** X is **skew** if $X + X^t$ is a $(0,1)$-matrix.)

Let q be a prime power, $q \equiv 1 \ (mod\ 4)$, and $C = (c_{ij})$ be a $(q \times q)$ matrix defined as follows:

$$c_{ij} = \begin{cases} 1, & \text{if } (i-j) \text{ is a nonzero square in } F_q, \\ 0, & \text{otherwise.} \end{cases}$$

C is a symmetric matrix with zero diagonal.

(The set of nonzero squares in F_q is a partial difference set (Paley partial difference set). The matrices C, $C + I_q$, $\overline{C}$ and $\overline{C} - I_q$ are developments of partial difference sets.
C and $\overline{C} - I_q$ are adjacency matrices of SRGs with parameters $(q, \frac{1}{2}(q-1), \frac{1}{4}(q-5), , \frac{1}{4}(q-1))$.)

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, by $0_{v \times v}$ the zero-matrix of dimension $v \times v$, and by J_p the all-one $(p \times p)$ matrix.

Put $q = 2p - 1$. Then $q \equiv 1 \ (mod\ 4)$.

Let D, $\overline{D}$, C, $\overline{C}$ be defined as above. The $(4p^2 \times 4p^2)$ matrix M defined as follows is the incidence matrix of a symmetric $(4p^2, 2p^2 - p, p^2 - p)$ design.

$$
M = \left[\begin{array}{c|c|c|c}
0 & 0_q^T & j_{p\cdot q}^T & 0_{p\cdot q}^T \\ \hline
0_q & 0_{q\times q} & (\overline{C} - I_q) \otimes j_p^T & \overline{C} \otimes j_p^T \\ \hline
j_{p\cdot q} & C \otimes j_p & (C + I_q) \otimes D + \overline{C} \otimes (\overline{D} - I_p) & C \otimes D + (\overline{C} - I_q) \otimes \overline{D} \\ \hline
0_{p\cdot q} & (C + I_q) \otimes j_p & C \otimes (D + I_p) + (\overline{C} - I_q) \otimes (\overline{D} - I_p) & (C + I_q) \otimes (\overline{D} - I_p) + \overline{C} \otimes D
\end{array}\right]
$$

To prove that M is the incidence matrix of a symmetric $(4p^2, 2p^2 - p, p^2 - p)$ design, it is sufficient to show that

$$M \cdot J_{4p^2} = (2p^2 - p)J_{4p^2}$$

and

$$M \cdot M^T = (p^2 - p)J_{4p^2} + p^2 I_{4p^2}.$$

□

If p and $2p-1$ are primes, then $(Z_p : Z_{\frac{p-1}{2}}) \times (Z_{2p-1} : Z_{p-1})$ act as an automorphism group of the Menon design from Theorem 1, and the derived design of that design, with respect to the fixed block for an automorphism group $(Z_p : Z_{\frac{p-1}{2}}) \times (Z_{2p-1} : Z_{p-1})$, is cyclic.

Corollary 1

Let p and $2p-1$ be primes and $p \equiv 3 \ (mod\ 4)$. Then there exists a cyclic 2-$(2p^2-p, p^2-p, p^2-p-1)$ design having an automorphism group isomorphic to $(Z_p : Z_{\frac{p-1}{2}}) \times (Z_{2p-1} : Z_{p-1})$.

Parameters of Menon designs belonging to the described series, for $p \leq 100$, are given below.

TABLE 1. Table of parameters for $p \leq 100$

p	$q = 2p - 1$	$4p^2$	Menon Designs
3	5	36	(36,15,6)
7	13	196	(196,91,42)
19	37	1444	(1444,703,342)
27	53	2916	(2916,1431,702)
31	61	3844	(3844,1891,930)
79	157	24964	(24964,12403,6162)

Theorem 2

Let p and $2p+3$ be prime powers and $p \equiv 3 \ (mod\ 4)$. Further, let us put $q = 2p+3$ and define the matrices D, C and M as in the proof of Theorem 1. Then $M + I_{4(p+1)^2}$ is the incidence matrix of a a symmetric $(4(p+1)^2, 2p^2+3p+1, p^2+p)$ design.

Corollary 2

Let p and $2p+3$ be primes and $p \equiv 3 \ (mod\ 4)$. There exists a 1-rotational 2-$(2p^2+3p+1, p^2+p, p^2+p-1)$ design having an automorphism group isomorphic to $(Z_p : Z_{\frac{p-1}{2}}) \times (Z_{2p+3} : Z_{p+1})$.

Parameters of Menon $(4(p+1)^2, 2p^2+3p+1, p^2+p)$ designs belonging to the described series, for $p \leq 100$, are given below.

TABLE 2. Table of parameters for $p \leq 100$

p	$q = 2p+3$	$4(p+1)^2$	Menon Designs
3	9	64	(64,28,12)
7	17	256	(256,120,56)
19	41	1600	(1600,780,380)
23	49	2304	(2304,1128,552)
43	89	7744	(7744,3828,1892)
47	97	9216	(9216,4560,2256)
67	137	18496	(18496,9180,4556)

If there exists a Hadamard matrix of order m, then there exists a Bush-type Hadamard matrix of order m^2 (H. Kharaghani, 1985).

For a prime power p, $p \equiv 3 \ (mod\ 4)$, there is a Hadamard matrix of order $p+1$ (from a Paley design with parameters $(p, \frac{p-1}{2}, \frac{p-3}{4})$), hence there is a Hadamard matrix of order $2(p+1)$ (Kronecker product construction).

Since Bush-type Hadamard matrices are regular, the existence of regular Hadamard matrices of order $4(p+1)^2$, where p is a prime power and $p \equiv 3 \ (mod\ 4)$, follows from H. Kharaghani's result from 1985. Therefore, Theorem 2 does not prove the existence of regular Hadamard matrices with these parameters.

Let K be a subset of positive integers. A **pairwise balanced design** $PBD(v, K, \lambda)$ 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. if an element of $\mathcal{B}$ is incident with k elements of $\mathcal{P}$, then $k \in K$;
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.

A 2-(v, k, λ) design is a $PBD(v, K, \lambda)$ with $K = \{k\}$.

Let p and $q = 2p - 1$ be prime powers, $p \equiv 3 \ (mod\ 4)$. We define the matrix M_1 as follows:

$$\left[\begin{array}{c|c|c|c}
0 & j_{p\cdot q}^T & 0_q^T & 0_{p\cdot q}^T \\
\hline
j_{p\cdot q} & \begin{array}{c} D \otimes (C + I_q) \\ + \\ (\overline{D} - I_p) \otimes \overline{C} \end{array} & j_p \otimes C & \begin{array}{c} D \otimes C \\ + \\ \overline{D} \otimes (\overline{C} - I_q) \end{array} \\
\hline
0_q & j_p^T \otimes (\overline{C} - I_q) & 0_{q\times q} & j_p^T \otimes \overline{C} \\
\hline
0_{p\cdot q} & \begin{array}{c} (D + I_p) \otimes C \\ + \\ (\overline{D} - I_p) \otimes (\overline{C} - I_q) \end{array} & j_p \otimes (C + I_q) & \begin{array}{c} (\overline{D} - I_p) \otimes (C + I_q) \\ + \\ D \otimes \overline{C} \end{array}
\end{array}\right]$$

and the matrix M_2 is defined in the following way:

$$\left[\begin{array}{c|c|c|c} 0 & j_{p\cdot q}^T & 0_q^T & 0_{p\cdot q}^T \\ \hline 0_{p\cdot q} & \begin{array}{c} D\otimes(C+I_q) \\ + \\ (\overline{D}-I_p)\otimes\overline{C} \end{array} & j_p\otimes\overline{C} & \begin{array}{c} D\otimes C \\ + \\ \overline{D}\otimes(\overline{C}-I_q) \end{array} \\ \hline 0_q & j_p^T\otimes(\overline{C}-I_q) & 0_{q\times q} & j_p^T\otimes\overline{C} \\ \hline j_{p\cdot q} & \begin{array}{c} (D+I_p)\otimes C \\ + \\ (\overline{D}-I_p)\otimes(\overline{C}-I_q) \end{array} & j_p\otimes(\overline{C}-I_q) & \begin{array}{c} (\overline{D}-I_p)\otimes(C+I_q) \\ + \\ D\otimes\overline{C} \end{array} \end{array}\right]$$

M_1 and M_2 are incidence matrices of Menon designs with parameters $(4p^2, 2p^2-p, p^2-p)$.

A $\{0, \pm 1\}$-matrix S is called a Siamese twin design sharing the entries of I, if $S = I + K - L$, where I, K, L are non-zero $\{0, 1\}$-matrices and both $I + K$ and $I + L$ are incidence matrices of symmetric designs with the same parameters. If $I + K$ and $I + L$ are incidence matrices of Menon designs, then S is called a Siamese twin Menon design.

The incidence matrices M_1 and M_2 share the entries of

$$I = \left[\begin{array}{c|c|c|c} 0 & j_{p\cdot q}^T & 0_q^T & 0_{p\cdot q}^T \\ \hline 0_{p\cdot q} & \begin{array}{c} D \otimes (C + I_q) \\ + \\ (\overline{D} - I_p) \otimes \overline{C} \end{array} & 0_{p\cdot q\times q} & \begin{array}{c} D \otimes C \\ + \\ \overline{D} \otimes (\overline{C} - I_q) \end{array} \\ \hline 0_q & j_p^T \otimes (\overline{C} - I_q) & 0_{q\times q} & j_p^T \otimes \overline{C} \\ \hline 0_{p\cdot q} & \begin{array}{c} (D + I_p) \otimes C \\ + \\ (\overline{D} - I_p) \otimes (\overline{C} - I_q) \end{array} & 0_{p\cdot q\times q} & \begin{array}{c} (\overline{D} - I_p) \otimes (C + I_q) \\ + \\ D \otimes \overline{C} \end{array} \end{array}\right]$$

Theorem 3

Let p and $q = 2p - 1$ be prime powers, $p \equiv 3 \ (mod\ 4)$, and let the matrices M_1, M_2 and I be defined as above. The matrix $S = I + M_1 - M_2$ is a Siamese twin design with parameters $(4p^2, 2p^2 - p, p^2 - p)$ sharing the entries of I.

The matrix I can be written as

$$I = \left[\begin{array}{c|c|c|c} 0 & j_{p\cdot q}^T & 0_q^T & 0_{p\cdot q}^T \\ \hline 0_{4p^2-1} & X & 0_{(4p^2-1)\times q} & Y \end{array} \right].$$

The matrix X is the incidence matrix of a 2-$(2p^2-p, p^2-p, p^2-p-1)$ design, and Y is the incidence matrix of a pairwise balanced design $PBD(2p^2-p, \{p^2, p^2-p\}, p^2-p-1)$. X is the incidence matrix of the derived design of the Menon designs with incidence matrices M_1 and M_2, with respect to the first block. When p and $2p-1$ are primes, the derived design and the pairwise balanced design are cyclic.

Two square matrices M and N of order n are said to be amicable if $MN^T = NM^T$.

The matrices M_1 and M_2 give rise to amicable regular Hadamard matrices.

Codes constructed from block designs have been extensively studied.

- E. F. Assmus Jnr, J. D. Key, Designs and their codes, Cambridge University Press, Cambridge, 1992.
- A. Baartmans, I. Landjev, V. D. Tonchev, On the binary codes of Steiner triple systems, Des. Codes Cryptogr. 8 (1996), 29–43.
- I. Bouyukliev, V. Fack, J. Winne, 2-$(31, 15, 7)$, 2-$(35, 17, 8)$ and 2-$(36, 15, 6)$ designs with automorphisms of odd prime order, and their related Hadamard matrices and codes, Des. Codes Cryptogr., **51** (2009), no. 2, 105–122.
- V. D. Tonchev, Quantum Codes from Finite Geometry and Combinatorial Designs, Finite Groups, Vertex Operator Algebras, and Combinatorics, Research Institute for Mathematical Sciences, **1656**, (2009) 44-54.

Theorem 4 [M. Harada, V. D. Tonchev, 2003]

Let $\mathcal{D}$ be a 2-(v, k, λ) design with a **fixed-point-free** and **fixed-block-free automorphism** ϕ of order q, where q is prime. Further, let M be the orbit matrix induced by the action of the group $G = \langle \phi \rangle$ on the design $\mathcal{D}$. If p is a prime dividing r and λ then the **orbit matrix** M generates a **self-orthogonal code** of length $b|q$ over $\mathbf{F}_p$.

Using Theorem 4 Harada and Tonchev constructed a ternary [63,20,21] code with a record breaking minimum weight from the symmetric 2-(189,48,12) design found by Janko.

Theorem 5 [V. D. Tonchev]

If G is a cyclic group of a prime order p that does not fix any point or block and $p|(r-\lambda)$, then the rows of the orbit matrix M generate a self-orthogonal code over $\mathbf{F}_p$.

Theorem 6

Let $\mathcal{D}$ be a symmetric (v,k,λ) design with an automorphism group G which acts on $\mathcal{D}$ with f fixed points (and f fixed blocks) and $\frac{v-f}{w}$ orbits of length w. If p is a prime that divides w and $r-\lambda$, then the rows and columns of the non-fixed part of the orbit matrix M for automorphism group G generate a self-orthogonal code of length $\frac{v-f}{w}$ over $\mathbb{F}_p$.

The following matrix is an obit matrix of the Menon design with the incidence matrix M described in Theorem 1:

$$O_M = \left[\begin{array}{c|c|c|c} 0 & 0_q^T & p\ j_q^T & 0_q^T \\ \hline 0_q & 0_{q\times q} & p\,(\overline{C}-I_q) & p\ \overline{C} \\ \hline j_q & C & \frac{p-1}{2}J_q+\frac{p-1}{2}I_q & \frac{p-1}{2}C+\frac{p+1}{2}(\overline{C}-I_q) \\ \hline 0_q & C+I_q & \frac{p+1}{2}C+\frac{p-1}{2}(\overline{C}-I_q) & \frac{p-1}{2}J_q+\frac{p-1}{2}I_q \end{array}\right]$$

The matrix O_M is an orbit matrix of a symmetric design for parameters $(4p^2, 2p^2-p, p^2-p)$ and the orbit length distribution with $q+1$ fixed points and $2q$ orbits of length p for points and blocks, whenever q is a prime power, $q \equiv 1\ (mod\ 4)$, and $p = \frac{q+1}{2}$.

Let q be a prime power, $q \equiv 1$ $(mod\ 4)$, and p be a prime dividing $\frac{q+1}{2}$. It follows from Theorem 6 that the rows of the matrix

$$R = \left[\begin{array}{c|c} \frac{q-1}{4}J_q + \frac{q-1}{4}I_q & \frac{q-1}{4}C + \frac{q+3}{4}(\overline{C} - I_q) \\ \hline \frac{q+3}{4}C + \frac{q-1}{4}(\overline{C} - I_q) & \frac{q-1}{4}J_q + \frac{q-1}{4}I_q \end{array} \right]$$

span a self-orthogonal code over $\mathbf{F}_p$ of length $2q$.

The dimension of this code is $q-1$.

q	p	parameters of the code	parameters of the dual code
5	3	$[10, 4, 6]_3$ *	$[10, 6, 4]_3$ *
9	5	$[18, 8, 8]_5$ *	$[18, 10, 6]_5$ *
13	7	$[26, 12, 10]_7$	$[26, 14, 8]_7$
17	3	$[34, 16, 12]_3$ *	$[34, 18, 10]_3$ *
29	3	$[58, 28, 18]_3$ *	$[58, 30, 16]_3$ *
	5	$[58, 28, 18]_5$	$[58, 30, 16]_5$
41	3	$[82, 40, 21]_3$ *	$[82, 42, 19]_3$ *

Table: Parameters of the self-orthogonal codes

* Largest minimum distance among all known codes of the given length and dimension.

The rows of the matrix S, obtained from R by adding first two rows and last two columns,

$$S = \left[\begin{array}{c|c|c|c} 0_q & 0_q & \frac{q-1}{4}J_q + \frac{q-1}{4}I_q & \frac{q-1}{4}C + \frac{q+3}{4}(\overline{C} - I_q) \\ \hline 0_q & 0_q & \frac{q+3}{4}C + \frac{q-1}{4}(\overline{C} - I_q) & \frac{q-1}{4}J_q + \frac{q-1}{4}I_q \\ \hline 1 & 0 & j_q^T & 0_q^T \\ \hline 0 & 1 & 0_q^T & j_q^T \end{array}\right]$$

span a self-dual $[2q+2, q+1]$ code over $\mathbf{F}_p$.

If q is a prime and $q = 12m + 5$, where m is a non-negative integer, then the code spanned by S is equivalent to the Pless symmetry code $C(q)$.

q	p	parameters of the code	q	p	parameters of the code
5	3	$[12, 6, 6]_3$ *	29	3	$[60, 30, 18]_3$ *
9	5	$[20, 10, 8]_5$ *		5	$[60, 30, 18]_5$
13	7	$[28, 14, 10]_7$	41	3	$[84, 42, 21]_3$ *
17	3	$[36, 18, 12]_3$ *			

Table: Parameters of the self-dual codes

* Largest minimum distance among all known codes of the given length and dimension.