Designs, Codes and Cryptography, 39, 247–251, 2006

A Series of Regular Hadamard Matrices

DEAN CRNKOVIĆ deanc@mapef.ffri.hr
Department of Mathematics, Faculty of Philosophy, Omladinska 14, 51000 Rijeka, Croatia

Communicated by: P. Wild

Received March 24, 2005; Revised July 12, 2005; Accepted July 13, 2005

Abstract. Let p and $2p-1$ be prime powers and $p \equiv 3 \pmod 4$. Then there exists a symmetric design with parameters $(4p^2, 2p^2-p, p^2-p)$. Thus there exists a regular Hadamard matrix of order $4p^2$.

Keywords: regular Hadamard matrix, symmetric design, Menon design

AMS Classification: 05B20, 05B05

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.

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 $(4u^2, 2u^2-u, u^2-u)$ design is equivalent to the existence of a regular Hadamard matrix of order $4u^2$ (see [3, Theorem 1.4, p. 280]). Such symmetric designs are called Menon designs.

If $n+1$ and $n-1$ are prime powers there exists a symmetric Hadamard matrix with constant diagonal of order n^2 (see [3, Corollary 5.12, p. 342]).

Xia et al. proved (see [4]) the following statement:
When $k = q_1, q_2, q_1q_2, q_1q_4, q_2q_3N, q_3q_4N$, where q_1, q_2 and q_3 are prime powers, $q_1 \equiv 1 \pmod 4$, $q_2 \equiv 3 \pmod 8$, $q_3 \equiv 5 \pmod 8$, $q_4 = 7$ or 23, $N = 2^a 3^b t^2$, $a, b = 0$ or 1, $t \neq 0$ is an arbitrary integer, there exist regular Hadamard matrices of order $4k^2$.

The existence of some regular Hadamard matrice of order $4p^2$, when p is a prime, $p \equiv 7 \pmod{16}$, is established in [2].

According to [2,4], there are just two values of $k \leq 100$ for which the existence of a regular Hadamard matrix of order $4k^2$ is still in doubt, $k = 47$ and $k = 79$.

2. Nonzero Squares in Finite Fields

Let p be a prime power, $p \equiv 3 \pmod 4$ 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. Such a symmetric design is called a Paley design (see [1]). Let $\overline{D}$ be an incidence matrix of a complementary symmetric design with parameters $(p, \frac{p+1}{2}, \frac{p+1}{4})$. Since -1 is not a square in F_p, D is a skew-symmetric matrix. Further, D has zero diagonal, so $D + I_p$ and $\overline{D} - I_p$, where I_p is an $(p \times p)$ identity matrix, 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. Matrices D and $\overline{D}$ have the following properties:

$$D \cdot \overline{D}^T = (\overline{D} - I_p)(D + I_p)^T = \frac{p+1}{4} J_p - \frac{p+1}{4} I_p,$$

$$[\ D \mid \overline{D} - I_p\ ] \cdot [\ \overline{D} - I_p \mid D\ ]^T = \frac{p-1}{2} J_p - \frac{p-1}{2} I_p,$$

$$[\ D \mid D\ ] \cdot [\ D + I_p \mid \overline{D} - I_p\ ]^T = \frac{p-1}{2} J_p,$$

$$[\ \overline{D} \mid D\ ] \cdot [\ \overline{D} - I_p \mid \overline{D} - I_p\ ]^T = \frac{p-1}{2} J_p,$$

where J_p is the all-one matrix of dimension $(p \times p)$.

Let $\Sigma(p)$ denote the group of all permutations of F_p given by

$$x \mapsto a\sigma(x) + b,$$

where a is a nonzero square in $F(p)$, b is any element of $F(p)$ and σ is an automorphism of the field $F(p)$. $\Sigma(p)$ is an automorphism group of symmetric designs with incidence matrices D, $D + I_p$, $\overline{D}$ and $\overline{D} - I_p$ (see [1, p. 9]). If p is a prime, $\Sigma(p)$ is isomorphic to a semidirect product $Z_p : Z_{\frac{p-1}{2}}$.

Let q be a prime power, $q \equiv 1 \pmod 4$, 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, since -1 is a square in F_q. There are as many non-zero squares as nonsquares in $F(q)$, so each row of C has $\frac{q-1}{2}$ elements equal 1 and $\frac{q+1}{2}$ zeros. Let $i \neq j$ and $C_i = [c_{i1} \ldots c_{iq}]$, $C_j = [c_{j1} \ldots c_{jq}]$ be the ith and the jth row of the matrix C, respectively. Then

$$C_i \cdot C_j^T = \begin{cases} \frac{q-1}{4} & \text{if } c_{ij} = c_{ji} = 0, \\ \frac{q-1}{4} - 1 & \text{if } c_{ij} = c_{ji} = 1. \end{cases}$$

The matrix $\overline{C} - I_q$ has the same property. Let $i \neq j$ and $\overline{C}_i = [\overline{c}_{i1} \ldots \overline{c}_{iq}]$, $\overline{C}_j = [\overline{c}_{j1} \ldots \overline{c}_{jq}]$ be the ith and the jth row of the matrix $\overline{C}$, respectively. Then

$$\overline{C}_i \cdot \overline{C}_j^T = \begin{cases} \frac{q-1}{4} & \text{if } \overline{c}_{ij} = \overline{c}_{ji} = 0, \\ \frac{q-1}{4} + 1 & \text{if } \overline{c}_{ij} = \overline{c}_{ji} = 1. \end{cases}$$

The matrix $C + I_q$ has the same property. Further,

$$C \cdot (C + I_q)^T = \overline{C} \cdot (\overline{C} - I_q)^T = \frac{q-1}{4} J_q + \frac{q-1}{4} I_q,$$

$$C \cdot (\overline{C} - I_q)^T = \frac{q-1}{4} J_q - \frac{q-1}{4} I_q,$$

$$(C + I_q) \cdot \overline{C}^T = \frac{q+3}{4} J_q - \frac{q-1}{4} I_q,$$

$$[\ C \mid C + I_q\ ] \cdot [\ C \mid C + I_q\ ]^T = \frac{q-1}{2} J_q + \frac{q+1}{2} I_q,$$

$$[\ \overline{C} \mid \overline{C} - I_q\ ] \cdot [\ \overline{C} \mid \overline{C} - I_q\ ]^T = \frac{q-1}{2} J_q + \frac{q+1}{2} I_q,$$

$$[\ C \mid C + I_q\ ] \cdot [\ \overline{C} \mid \overline{C} - I_q\ ]^T = \frac{q+1}{2} J_q - \frac{q+1}{2} I_q.$$

$\Sigma(q)$ acts as an automorphism group of incidence structures with incidence matrices C, $C + I_q$, $\overline{C}$ and $\overline{C} - I_q$.

3. Regular Hadamard Matrices

Let $H = (h_{ij})$ and K be $m \times n$ and $m_1 \times n_1$ matrices, respectively. Their Kronecker product is a $mm_1 \times nn_1$ matrix

$$H \otimes K = \begin{bmatrix} h_{11}K & h_{12}K & \ldots & h_{1n}K \\ h_{21}K & h_{22}K & \ldots & h_{2n}K \\ \vdots & \vdots & & \vdots \\ h_{m1}K & h_{m2}K & \ldots & h_{mn}K \end{bmatrix}.$$

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 $0_{v \times v}$ the zero-matrix of dimension $v \times v$.

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

Proof. Put $q = 2p-1$. Then $q \equiv 1 \pmod 4$. Let D, $\overline{D}$, C, $\overline{C}$ be defined as above. Define a $(4p^2 \times 4p^2)$ matrix M in the following way:

$$M = \begin{bmatrix} 0 & 0_q^T & j_{p\cdot q}^T & 0_{p\cdot q}^T \\ 0_q & 0_{q\times q} & (\overline{C}-I_q)\otimes j_p^T & \overline{C}\otimes j_p^T \\ j_{p\cdot q} & C\otimes j_p & \begin{matrix}(C+I_q)\otimes D \\ + \\ \overline{C}\otimes(\overline{D}-I_p)\end{matrix} & \begin{matrix} C\otimes D \\ + \\ (\overline{C}-I_q)\otimes\overline{D}\end{matrix} \\ 0_{p\cdot q} & (C+I_q)\otimes j_p & \begin{matrix} C\otimes(D+I_p) \\ + \\ (\overline{C}-I_q)\otimes(\overline{D}-I_p)\end{matrix} & \begin{matrix}(C+I_q)\otimes(\overline{D}-I_p) \\ + \\ \overline{C}\otimes D\end{matrix} \end{bmatrix}.$$

Let us show that M is an incidence matrix of a Menon design with parameters $(4p^2, 2p^2-p, p^2-p)$. It is easy to see that $M \cdot J_{4p^2} = (2p^2-p)J_{4p^2}$. We have to prove that $M \cdot M^T = (p^2-p)J_{4p^2} + p^2 I_{4p^2}$. Using properties of the matrices D, $\overline{D}$, C and $\overline{C}$ which we have menitioned before, one computes that the product of block matrices M and M^T is:

$$M\cdot M^T = \begin{bmatrix} pq & (p^2-p)j_q^T & (p^2-p)j_{pq}^T & (p^2-p)j_{pq}^T \\ (p^2-p)j_q & \begin{matrix}(p^2-p)J_q \\ + \\ p^2 I_q\end{matrix} & (p^2-p)J_{q\times pq} & (p^2-p)J_{q\times pq} \\ (p^2-p)j_{pq} & (p^2-p)J_{pq\times q} & \begin{matrix}(p^2-p)J_{pq} \\ + \\ p^2 I_{pq}\end{matrix} & (p^2-p)J_{pq\times pq} \\ (p^2-p)j_{pq} & (p^2-p)J_{pq\times q} & (p^2-p)J_{pq\times pq} & \begin{matrix}(p^2-p)J_{pq} \\ + \\ p^2 I_{pq}\end{matrix} \end{bmatrix},$$

where $J_{m\times n}$ is the all-one matrix of dimension $m \times n$. Thus,

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

which means that M is an incidence matrix of a symmetric design with parameters $(4p^2, 2p^2-p, p^2-p)$. ■

COROLLARY 1. *Let p and $2p-1$ be prime powers and $p \equiv 3 \pmod 4$. Then there exists a regular Hadamard matrix of order $4p^2$.*

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

Incidence matrices of the Menon designs from Theorem 1 lead us to conclusion that the groups $\Sigma(p) \times \Sigma(2p-1)$ act as automorphism groups of these designs, semistandardly with one-fixed point (and block), one orbit of length $2p-1$, and two orbits of length $2p^2-p$. If p and $2p-1$ are primes, then $\Sigma(p)\times\Sigma(2p-1)\cong(Z_p:Z_{\frac{p-1}{2}})\times(Z_{2p-1}:Z_{p-1})$, and the derived designs of the Menon designs from Theorem 1 with respect to the first block, i.e., the fixed block for an automorphism group $(Z_p:Z_{\frac{p-1}{2}})\times(Z_{2p-1}:Z_{p-1})$, are cyclic. That proves the following corollary:

COROLLARY 2. *Let p and $2p-1$ be primes and $p\equiv 3 \pmod 4$. 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 series described in this paper, for $p\leq 100$, are given below (Table 1).

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

p	$q=2p-1$	$4p^2$	Parameters of 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)

References

1. E. Lander, *Symmetric Designs: An Algebraic Approach,* Cambridge University Press, Cambridge (1983).
2. K. H. Leung, S. L. Ma and B. Schmidt, New Hadamard matrices of order $4p^2$ obtained from Jacobi sums of order 16, preprint.
3. W. D. Wallis, A. P. Street and J. S. Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices,* Springer-Verlag, Berlin–Heidelberg–New York (1972).
4. T. Xia, M. Xia and J. Seberry, Regular Hadamard matrices, maximum excess and SBIBD, *Australasian Journal of Combinatorics,* Vol. 27 (2003) pp. 263–275.