A construction of regular Hadamard matrices and related codes

Dean Crnković

Department of Mathematics
University of Rijeka
Croatia

5th Workshop on Real and Complex Hadamard Matrices and Applications
Budapest, Hungary, July 2017

This work has been fully supported by Croatian Science Foundation under the project 1637.

A Hadamard matrix is **regular** if the row and column sums are constant. A regular Hadamard matrix is necessarily of order $4k^2$ with constant row sum $2k$. It was conjectured that a regular Hadamard matrix of order $4k^2$ exists for every positive integer k.

A matrix A is **skew-symmetric** if $A^T = -A$. A Hadamard matrix H of order $4k$ is **skew-type** if $H = A + I_{4k}$, where $A^T = -A$. It was conjectured by J. Seberry that a skew-type Hadamard matrix exists if and only if n=1,2, or $4k$, where k is a positive integer (smallest open case $4k = 276$).

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 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**.

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 2-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**.

A $(0,1)$-matrix D is **skew** if $D + D^T$ is a $(0,1)$-matrix. A skew-type Hadamard matrix corresponds to a Hadamard 2-design with the skew incidence matrix, and vice versa.

A **graph** is **regular** if all the vertices have the same valency. A regular graph is **strongly regular** of type (v, k, λ, μ) if it has v vertices, valency k, and if any two adjacent vertices are together adjacent to λ vertices, while any two non-adjacent vertices are together adjacent to μ vertices.

T. Xia, M. Xia and J. Seberry had proved 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, $q_1 \equiv 1 \ (mod\ 4)$, $q_2 \equiv 3 \ (mod\ 8)$, $q_3 \equiv 5 \ (mod\ 8)$, $q_4 = 7$ or 23, $N = 2^a3^bt^2$, $a, b = 0$ or 1, $t \neq 0$ is an arbitrary integer, there exist regular Hadamard matrices of order $4k^2$.
(T. Xia, M. Xia and J. Seberry, Regular Hadamard matrices, maximum excess and SBIBD, Australas. J. Combin. 27 (2003), 263–275.)

The existence of some regular Hadamard matrice of order $4p^2$, p a prime, $p \equiv 7 \ (mod\ 16)$, is established by K. H. Leung, S. L. Ma and B. Schmidt.
(K. H. Leung, S. L. Ma and B. Schmidt. New Hadamard matrices of order $4p^2$ obtained from Jacobi sums of order 16, J. Combin. Theory Ser. A (2006), 822-838).

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 construction is based on Paley designs (Paley difference sets) and Paley graphs (Paley partial difference sets).

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.

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 $(p \times p)$ 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 $(q, \frac{1}{2}(q-1), \frac{1}{4}(q-5), \frac{1}{4}(q-1))$.)

Let $i \neq j$ and $C_i = [c_{i1} \dots c_{iq}]$, $C_j = [c_{j1} \dots c_{jq}]$ be the i^{th} and the j^{th} row of the matrix C, respectively. Then

$$C_i \cdot C_j^T = \begin{cases} \frac{q-1}{4}, & \text{if } c_{ij} = c_{ji} = 0, \\ \frac{q-5}{4}, & \text{if } c_{ij} = c_{ji} = 1. \end{cases}$$

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

$$\overline{C}_i \cdot \overline{C}_j^T = \begin{cases} \frac{q-1}{4}, & \text{if } \overline{c}_{ij} = \overline{c}_{ji} = 0, \\ \frac{q+3}{4}, & \text{if } \overline{c}_{ij} = \overline{c}_{ji} = 1. \end{cases}$$

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

Further, the following equalities hold:

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

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

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

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

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

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

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 $v \times v$.

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

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

□

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)

A **conference matrix** of order n is a $(n \times n)$ $(0, \pm 1)$-matrix W satisfying $WW^T = (n-1)I_n$. If W is a conference matrix of order n, then either $n \equiv 0$ $(mod\ 4)$ and W is equivalent to a skew-symmetric matrix, or W is is equivalent to a symmetric matrix.

If W is a symmetric conference matrix of order n, then $n \equiv 2$ $(mod\ 4)$ and $n-1$ is the sum of two squares.

If there exists a symmetric conference matrix of order n, then there exists a strongly regular graph with parameters $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$, where $v = n - 1$. Strongly regular graphs with parameters $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$ are called **conference graphs**.

The following theorem is a generalization of Theorem 1.

Theorem 2 [DC, 2016]

Let there exist a Hadamard 2-$(m, \frac{m-1}{2}, \frac{m-3}{4})$ design with the skew incidence matrix, and a conference graph with v vertices, where $v = 2m - 1$. Then there exists a regular Hadamard matrix of order $4m^2$.

Proof:

Let D be the skew incidence matrix of a Hadamard 2-$(m, \frac{m-1}{2}, \frac{m-3}{4})$ design, and let C be the adjacency matrix of a conference graph with $v = 2m - 1$ vertices.

We define matrix M in a similar way as in the proof of Theorem 1.

There are 111 values of $k < 1000$ for which the existence of a regular Hadamard matrix of order $4k^2$ is still undetermined. These values are:

103, 127, 141, 191, 209, 213, 217, 223, 237, 239, 253, 309, 329, 341, 355, 357, 369, 377, 381, 383, 385, 395, 403, 423, 425, 431, 437, 453, 455, 463, 465, 473, 479, 481, 483, 487, 493, 497, 501, 503, 515, 517, 527, 553, 561, 573, 589, 595, 597, 611, 615, 627, 629, 635, 647, 649, 657, 663, 665, 669, 689, 693, 697, 705, 711, 713, 715, 717, 719, 721, 737, 743, 751, 755, 759, 765, 781, 789, 793, 801, 805, 813, 817, 823, 833, 835, 837, 839, 861, 863, 869, 873, 887, 889, 893, 899, 901, 903, 911, 913, 923, 927, 933, 935, 949, 955, 969, 983, 989, 991, 995.

The cases solved by Theorem 2 are k=231, 255, 399, 639, 651, 775, 799, 987.

It was conjectured that a skew-type Hadamard matrix exists if and only if n=1,2, or $4k$, where k is a positive integer. In case that this conjecture holds true, Theorem 2 would also imply the existence of a regular Hadamard matrix of order $4k^2$ for k=255, 715, 835.

A matrix S is called a **Siamese twin design** sharing the entries of I, if $S = I + K - L$, where I, K, and 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**.

Let K be a set of positive integers. A **pairwise balanced design** $\mathrm{PBD}(v, K, \lambda)$ 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:

- $|\mathcal{P}| = v$,
- if an element of $\mathcal{B}$ is incident with k elements of $\mathcal{P}$, then $k \in K$,
- every pair of distinct elements of $\mathcal{P}$ is incident with exactly λ elements of $\mathcal{B}$.

Theorem 3 [DC, R. Egan, 2017]

If there exists a skew Hadamard 2-$(m, \frac{m-1}{2}, \frac{m-3}{4})$ design, and a conference graph with $2m-1$ vertices, then there is a Siamese twin Menon design $S = I + K - L$ with parameters $(4m^2, 2m^2-m, m^2-m)$, where

$$I = \left[\begin{array}{c|c|c|c} 0 & j_{m\cdot v}^{\top} & 0_v^{\top} & 0_{m\cdot v}^{\top} \\ \hline 0_{4m^2-1} & X & 0_{4m^2-1\times v} & Y \end{array}\right].$$

Moreover, X is the incidence matrix of a 2-$(2m^2-m, m^2-m, m^2-m-1)$ design, and Y is the incidence matrix of a $\mathrm{PBD}(2m^2-m, \{m^2, m^2-m\}, m^2-m-1)$.

$M_1 = I + K$ and $M_2 = I + L$, the incidence matrices of Menon designs from Theorem 3, are constructed in a similar way as the matrix M from Theorem 2.

The Hadamard matrices H_1 and H_2 associated with M_1 and M_2 are regular.

Let A be the incidence matrix of a design $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$. A **decomposition** of A is any partition $B_1, \ldots, B_s$ of the rows of A (blocks of $\mathcal{D}$) and a partition $P_1, \ldots, P_t$ of the columns of A (points of $\mathcal{D}$).

For $i \leq s$, $j \leq t$ define

$$\alpha_{ij} = |\{P \in P_j |\ P\mathcal{I}x\}|, \text{ for } x \in B_i \text{ arbitrarily chosen,}$$
$$\beta_{ij} = |\{x \in B_i |\ P\mathcal{I}x\}|, \text{ for } P \in P_j \text{ arbitrarily chosen.}$$

We say that a decomposition is **tactical** if the α_{ij} and β_{ij} are well defined (indipendent from the choice of $x \in B_i$ and $P \in P_j$, respectively).

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a $2-(v,k,\lambda)$ design and $G \leq Aut(\mathcal{D})$. We denote the $G-$orbits of points by $\mathcal{P}_1, \ldots, \mathcal{P}_n$, $G-$orbits of blocks by $\mathcal{B}_1, \ldots, \mathcal{B}_m$, and put $|\mathcal{P}_r| = \omega_r$, $|\mathcal{B}_i| = \Omega_i$, $1 \leq r \leq n$, $1 \leq i \leq m$.

The **group action** of G induces a **tactical decomposition of** $\mathcal{D}$. Denote by γ_{ij} the number of points of $\mathcal{P}_j$ incident with a representative of the block orbit $\mathcal{B}_i$. For these numbers the following equalities hold:

$$\sum_{j=1}^{n} \gamma_{ij} = k \,, \tag{1}$$

$$\sum_{i=1}^{m} \frac{\Omega_i}{\omega_j} \gamma_{ij}\gamma_{is} = \lambda\omega_s + \delta_{js} \cdot (r - \lambda) \,. \tag{2}$$

Definition 1

A $(m \times n)$-matrix $M = (\gamma_{ij})$ with entries satisfying conditions (1) and (2) is called an **orbit matrix** for the parameters $2-(v,k,\lambda)$ and orbit lengths distributions $(\omega_1,\ldots,\omega_n)$, $(\Omega_1,\ldots,\Omega_m)$.

Orbit matrices are often used in construction of designs with a presumed automorphism group.

The intersection of rows and columns of an orbit matrix M that correspond to non-fixed points and non-fixed blocks form a submatrix called the **non-fixed part of the orbit matrix** M.

Example

Incidence matrix for the symmetric (7,3,1) design

$$\left[\begin{array}{c|ccc|ccc} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ \hline 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right]$$

Corresponding orbit matrix for Z_3

$$\begin{array}{c||c|cc} & 1 & 3 & 3 \\ \hline\hline 1 & 0 & 3 & 0 \\ \hline 3 & 1 & 1 & 1 \\ 3 & 0 & 1 & 2 \end{array}$$

Codes

Let $\mathbf{F}_q$ be the finite field of order q. A **linear code** of **length** n is a subspace of the vector space $\mathbf{F}_q^n$. A k-dimensional subspace of $\mathbf{F}_q^n$ is called a linear $[n, k]$ code over $\mathbf{F}_q$.
For $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbf{F}_q^n$ the number $d(x, y) = |\{i \,|1 \leq i \leq n, \, x_i \neq y_i\}|$ is called a Hamming distance. A **minimum distance** of a code C is $d = min\{d(x, y) \,|x, y \in C, x \neq y\}$.
A linear $[n, k, d]$ code is a linear $[n, k]$ code with minimum distance d.
An $[n, k, d]$ linear code can correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.
The **dual** code $C^\perp$ is the orthogonal complement under the standard inner product $(,)$. A code C is called **self-orthogonal** if $C \subseteq C^\perp$. C is called **self-dual** if $C = C^\perp$.

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 $\mathbf{F}_p$.

Theorem 5 [DC, L. Simčić, 2012]

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 5 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 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 codes of the given length and dimension.

The **support** of a non-zero vector $x \in \mathbb{F}_q^n$ is the set of indices of its non-zero coordinates. The **support design** of a code of length n for a given non-zero weight w is the design with points the n coordinate indices and blocks the supports of all codewords of weight w. The support designs for the minimum weight of the first five codes in the family of Pless symmetry codes are 5-designs.

We obtained 3-designs as support designs of some of the constructed codes. Information on the obtained t-designs are given in the following table.

q	p	parameters of the code	design $\mathcal{D}$	Aut($\mathcal{D}$)
5	3	$[10,6,4]_3$	3-(10,4,1)	$(A_6.C_2):C_2$
5	3	$[10,6,4]_3$	3-(10,5,6)	$(A_6.C_2):C_2$
5	3	$[10,4,6]_3$, $[10,6,4]_3$	3-(10,6,5)	$(A_6.C_2):C_2$
9	5	$[20,10,8]_5$	3-(20,8,28)	$C_2\times((A_6:C_2):C_2)$
9	5	$[20,10,8]_5$	3-(20,10,616)	$C_2\times((A_6:C_2):C_2)$
9	5	$[20,10,8]_5$	3-(20,11,2640)	$C_2\times((A_6:C_2):C_2)$
17	3	$[34,18,10]_3$	3-(34,10,45)	$C_2\times(C_{17}:C_{16})$
17	3	$[34,18,10]_3$	3-(34,11,270)	$C_2\times(C_{17}:C_{16})$
17	3	$[34,16,12]_3$, $[34,18,10]_3$	3-(34,12,345)	$C_2\times(C_{17}:C_{16})$
17	3	$[34,18,10]_3$	3-(34,13,5577)	$C_2\times(C_{17}:C_{16})$
17	3	$[34,18,10]_3$	3-(34,14,21294)	$C_2\times(C_{17}:C_{16})$
17	3	$[34,16,12]_3$, $[34,18,10]_3$	3-(34,15,17745)	$C_2\times(C_{17}:C_{16})$
17	3	$[34,18,10]_3$	3-(34,16,209685)	$C_2\times(C_{17}:C_{16})$
17	3	$[34,18,10]_3$	3-(34,17,539190)	$C_2\times(C_{17}:C_{16})$
17	3	$[34,16,12]_3$, $[34,18,10]_3$	3-(34,18,305541)	$C_2\times(C_{17}:C_{16})$
17	3	$[34,18,10]_3$	3-(34,19,2438973)	$C_2\times(C_{17}:C_{16})$
17	3	$[34,16,12]_3$, $[34,18,10]_3$	3-(34,21,1673805)	$C_2\times(C_{17}:C_{16})$
29	3	$[58,28,18]_3$	3-(58,18,25092)	$C_2\times((C_{29}:C_7):C_4)$