Orbit matrices of Hadamard matrices and related codes

Dean Crnković (deanc@math.uniri.hr)
Ronan Egan (ronan.egan@math.uniri.hr)
and
Andrea Švob (asvob@math.uniri.hr)

Department of Mathematics
University of Rijeka
Radmile Matejčić 2, 51000 Rijeka, Croatia

Abstract

In this paper we introduce the notion of orbit matrices of Hadamard matrices with respect to their permutation automorphism groups and show that under certain conditions these orbit matrices yield self-orthogonal codes. As a case study, we construct codes from orbit matrices of some Paley type I and Paley type II Hadamard matrices. In addition, we construct four new symmetric (100,45,20) designs which correspond to regular Hadamard matrices, and construct codes from their orbit matrices. The codes constructed include optimal, near-optimal self-orthogonal and self-dual codes, over finite fields and over $\mathbb{Z}_4$.

2010 Mathematics Subject Classification: 05B20, 94B05.
Keywords: Hadamard matrix, orbit matrix, self-orthogonal code.

1 Introduction

A *Hadamard matrix* of order n is a $n \times n$ $\{\pm 1\}$ matrix H such that $HH^\top = nI_n$. It is well known that a Hadamard matrix of order n can exist only if $n = 1$, 2 or $n \equiv 0 \mod 4$. The Hadamard conjecture states that these necessary conditions are also sufficient. Since the discovery of a Hadamard matrix of order 428, the smallest open case is $n = 668$ [23].

A *code* C of length n over the alphabet Q is a subset $C \subseteq Q^n$. Elements of a code are called *codewords*. A code C is called a q-ary *linear code* of dimension m if $Q = \mathbb{F}_q$, for a prime power q, and C is an m-dimensional subspace of a vector space $(\mathbb{F}_q)^n$. For $Q = \mathbb{F}_2$ a code is called *binary*.

Let $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n) \in \mathbb{F}_q^n$. The *Hamming distance* between words x and y is the number $d(x, y) = |\{i : x_i \neq y_i\}|$. The *minimum distance* of the code C is defined by $d = \min\{d(x, y) : x, y \in C,\ x \neq y\}$. The *weight* of a codeword x is

$w(x) = d(x, 0) = |\{i : x_i \neq 0\}|$. For a *linear code* the minimum distance equals the minimum weight: $d = \min\{w(x) : x \in C, x \neq 0\}$.

A q-ary linear code of length n, dimension k, and distance d is called a $[n, k, d]_q$ code. A linear $[n, k, d]$ code can detect at most $d-1$ errors in one codeword and correct at most $t = \lfloor \frac{d-1}{2} \rfloor$ errors. An $[n, k]$ linear code C is said to be a *best known* linear $[n, k]$ code if C has the highest minimum weight among all known $[n, k]$ linear codes. An $[n, k]$ linear code C is said to be an *optimal* linear $[n, k]$ code if the minimum weight of C achieves the theoretical upper bound on the minimum weight of $[n, k]$ linear codes, and *near-optimal* if its minimum distance is at most 1 less than the largest possible value.

The *dual* code $C^\perp$ is the orthogonal complement under the standard inner product $(\cdot\,, \cdot)$, i.e. $C^\perp = \{v \in F^n | (v, c) = 0 \text{ for all } c \in C\}$. A code C is *self-orthogonal* if $C \subseteq C^\perp$ and *self-dual* if equality is attained. Two linear codes are *isomorphic* if one can be obtained from the other by permuting the coordinate positions. An *automorphism* of the code C is an isomorphism from C to C. Two codes are *equivalent* if one of the codes can be obtained from the other by permuting the coordinates and permuting the symbols within one or more coordinate positions.

In this paper we introduce the notion of an orbit matrix of a Hadamard matrix with respect to a permutation automorphism group of the matrix. We use these orbit matrices to construct self-orthogonal codes. The orbit matrix of a Hadamard matrix H is defined in a way that the entry at the position (i, j) denotes the row (or column) sum of a submatrix of H determined by the i^{th} row orbit and the j^{th} column orbit. This definition of an orbit matrix of a Hadamard matrix is a generalization of the definition of an orbit matrix of an incidence structure. For a Hadamard matrix H, the matrix $B = \frac{1}{2}(H + J)$, where J denotes the all-one matrix, is called the binary Hadamard matrix associated to H. In comparison to the usual orbit matrices of the binary Hadamard matrix B associated to a Hadamard matrix H (i.e. orbit matrices obtained by considering B as the incidence matrix of an incidence structure), with this approach we have a wider range of choices for an automorphism group G in the construction of orbit matrices of H from which we obtain self-orthogonal codes. Another advantage of this generalization of the definition of orbit matrices is that it can be applied to a wider range of matrices, not just to $\{0, 1\}$ matrices (incidence matrices of incidence structures). This allows us to construct orbit matrices of the matrices $H + kI$ in Section 3, where H is a Hadamard matrix, and obtain the corresponding self-dual codes.

The codes constructed in this paper have been constructed and examined using Magma [2]. Minimum distances are compared to known codes and bounds at [12].

2 Orbit matrices of Hadamard matrices

P. Dembowski introduced the notion of a tactical decomposition of an incidence structure and showed that the orbits of an automorphism group acting on an incidence structure $\mathcal{I}$ induce a tactical decomposition of $\mathcal{I}$ (see [9]). Tactical decompositions induced by the action of an automorphism group leads us to orbit matrices of incidence structures, which have been successfully used for a construction of block designs since the 1980s (see [5, 18]). Construction of self-orthogonal codes from orbit matrices of block designs was introduced

in [15] and further developed in [4]. In this paper we define orbit matrices of Hadamard matrices and show that under certain conditions these orbit matrices yield self-orthogonal codes.

M. Hall defined an *automorphism* of a Hadamard matrix H of order n as a pair (P, Q) of $n \times n$ monomial matrices such that $PHQ = H$ (see [13]). A *permutation automorphism* of a $\{\pm 1\}$-matrix H is defined to be a permutation g of rows and columns of H that maps H to itself, i.e. $Hg = H$. The permutations g can be considered as an ordered pair $g = (\alpha, \beta)$, where α is a permutation of rows of H and β is a permutation of columns of H. To these permutations α and β we can associate a pair of permutation matrices (P, Q) such that $PHQ^\top = H$. We transpose the righthand component so that the product $(P, Q)(R, S) = (PR, QS)$ of automorphisms (P, Q) and (R, S) is an automorphism.

The next three theorems follow from Theorems 3.1, 3.2 and 3.3 of [21] on orbits of points and blocks of a symmetric design under the action of an automorphism. For completeness we include proofs specific to Hadamard matrices.

Theorem 2.1. *A permutation automorphism g of a Hadamard matrix fixes an equal number of rows and columns.*

Proof. If g is an automorphism of a Hadamard matrix H, then there exist permutation matrices P and Q such that $PHQ^\top = H$. Since the matrix H is regular and since the inverse of a permutation matrix is its transpose, then $HQH^{-1} = P$. Thus the matrices Q and P are similar and $tr(P) = tr(Q)$.

Since the number of fixed points of a permutation is equal to the trace of the associated permutation matrix, it follows that g fixes an equal number of rows and columns. □

The Möbius function μ is defined by

$$\mu(n) = \begin{cases} 0, & \text{if } n \text{ has one or more repeated prime factors}, \\ 1, & \text{if } n = 1, \\ (-1)^k, & \text{if } n \text{ is a product of } k \text{ distinct primes}, \end{cases}$$

for a positive integer n. So $\mu(n) \neq 0$ if and only if n is squarefree. The Möbius inversion formula states that if f and g are functions that map positive integers to complex numbers, satisfying

$$g(n) = \sum_{d|n} f(d),$$

for every positive integer n, then

$$f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d}),$$

where μ is the Möbius function and the sums run over all positive divisors d of n.

Theorem 2.2. *Let $g = (\alpha, \beta)$ be a permutation automorphism of a Hadamard matrix H, where α is a permutation of rows and β is a permutation of columns of H. Then the permutations α and β have the same cycle structure.*

Proof. Let $f_\alpha(d)$ and $f_\beta(d)$ be the number of cycles of length d in the cycle decomposition of α and β, respectively. For every positive integer m the number of fixed points of α^m is $\sum_{d|m} f_\alpha(d)$, and the number of fixed points of β^m is $\sum_{d|m} f_\beta(d)$. By Theorem 2.1

$$\sum_{d|m} f_\alpha(d) = \sum_{d|m} f_\beta(d)$$

for all positive integers m. By applying the Möbius inversion formula we get $f_\alpha(d) = f_\beta(d)$ for all d. □

The set of all permutation automorphisms of a Hadamard matrix H form the full permutation automorphism group of H under the obvious multiplication, denoted $\mathrm{PAut}(H)$. Any subgroup of $\mathrm{PAut}(H)$ is called a permutation automorphism group of H.

Theorem 2.3. *Any subgroup $G \leq \mathrm{PAut}(H)$ has equally as many orbits on rows as on columns of H.*

Proof. By the Cauchy-Frobenius Lemma (sometimes called Burnside's Lemma) the number t of orbits of the group G is given by

$$t = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|,$$

where $\mathrm{Fix}(g)$ is the set of fixed points of g. The statement follows from Theorem 2.1. □

Let G be a permutation automorphism group of a Hadamard matrix $H = [h_{ij}]$, acting in t orbits on the set of rows and the set of columns of H. Let us denote the G-orbits on rows and columns of H by $\mathcal{R}_1, \ldots, \mathcal{R}_t$ and $\mathcal{C}_1, \ldots, \mathcal{C}_t$, respectively, and put $|\mathcal{R}_i| = \Omega_i$ and $|\mathcal{C}_i| = \omega_i,\ i = 1, \ldots, t$.

Let H_{ij} be the submatrix of H consisting of the rows belonging to the row orbit $\mathcal{R}_i$ and the column belonging to $\mathcal{C}_j$. We denote by Γ_{ij} and γ_{ij} the sum of a row and column of H_{ij}, respectively. The numbers Γ_{ij} and γ_{ij} are well-defined, i.e. they do not depend on the choice of the row and the column, because the sums of entries of any two rows (or columns) of H_{ij} are equal. The $t \times t$ matrix $R = [\Gamma_{ij}]$ is called a *row orbit matrix* of H with respect to G. The $t \times t$ matrix $C = [\gamma_{ij}]$ is called a *column orbit matrix* of H with respect to G.

Lemma 2.4. *Let G be a permutation automorphism group of a Hadamard matrix $H = [h_{ij}]$ of order n, and let $\mathcal{R}_1, \ldots, \mathcal{R}_t$ and $\mathcal{C}_1, \ldots, \mathcal{C}_t$ be the G-orbits on the rows and columns of the matrix H, respectively. Further, let Γ_{ij} and γ_{ij} be defined as above. Then*

$$\sum_{j=1}^{t} \Gamma_{ij}\gamma_{sj} = \delta_{is} n,$$

where δ_{is} is the Kronecker delta.

Proof. Let x be a row from the row orbit $\mathcal{R}_i$, and y be a column from the column orbit $\mathcal{C}_j$. Then

$$\sum_{j=1}^{t} \Gamma_{ij}\gamma_{sj} = \sum_{j=1}^{t} \big(\sum_{z\in\mathcal{C}_j} h_{xz}\big)\big(\sum_{w\in\mathcal{R}_s} h_{wy}\big) = \sum_{j=1}^{t}\sum_{z\in\mathcal{C}_j}\sum_{w\in\mathcal{R}_s} h_{xz}h_{wy} = \sum_{j=1}^{t}\sum_{z\in\mathcal{C}_j}\sum_{w\in\mathcal{R}_s} h_{xz}h_{wz}$$

$$= \sum_{j=1}^{t}\sum_{w\in\mathcal{R}_s}\sum_{z\in\mathcal{C}_j} h_{xz}h_{wz} = \sum_{w\in\mathcal{R}_s}\sum_{j=1}^{t}\sum_{z\in\mathcal{C}_j} h_{xz}h_{wz} = \sum_{w\in\mathcal{R}_s}\sum_{z=1}^{n} h_{xz}h_{wz}.$$

If $i \neq s$, then

$$\sum_{w\in\mathcal{R}_s}\sum_{z=1}^{n} h_{xz}h_{wz} = \sum_{w\in\mathcal{R}_s} 0 = 0.$$

If $i = s$, then

$$\sum_{w\in\mathcal{R}_s}\sum_{z=1}^{n} h_{xz}h_{wz} = (\Omega_s - 1)0 + n = n,$$

where Ω_s is the length of the orbit $\mathcal{R}_s$. □

Theorem 2.5. *Let G be a permutation automorphism group of a Hadamard matrix H, and let $\mathcal{R}_1, \ldots, \mathcal{R}_t$ and $\mathcal{C}_1, \ldots, \mathcal{C}_t$ be the G-orbits on the rows and columns of the matrix H, respectively. Further, let Ω_i, ω_j, Γ_{ij} and γ_{ij} be defined as above. Then*

$$\sum_{j=1}^{t} \frac{\Omega_s}{\omega_j}\Gamma_{ij}\Gamma_{sj} = \delta_{is}n,$$

where δ_{is} is the Kronecker delta.

Proof. The sum of entries of the submatrix H_{sj} is $\Omega_s\Gamma_{sj}$. On the other hand, this sum is equal to $\omega_j\gamma_{sj}$, so

$$\gamma_{sj} = \frac{\Omega_s}{\omega_j}\Gamma_{sj}.$$

□

In Theorems 2.6 and 2.7 we show that under some conditions orbit matrices of Hadamard matrices, or their submatrices, span self-orthogonal codes.

Theorem 2.6. *Let H be a Hadamard matrix of order n and G be a permutation automorphism group of H acting with all orbits of the same length w. Further, let R be the row orbit matrix of H with respect to G. If p is a prime dividing n, and $q = p^m$ is a prime power, then the linear code spanned by the matrix R over the field $\mathbb{F}_q$ is a self-orthogonal code of length t.*

Proof. By Theorem 2.5 we have

$$\sum_{j=1}^{t} \frac{\Omega_s}{\omega_j}\Gamma_{ij}\Gamma_{sj} = \sum_{j=1}^{t} \frac{w}{w}\Gamma_{ij}\Gamma_{sj} = \sum_{j=1}^{t} \Gamma_{ij}\Gamma_{sj} = \delta_{is}n.$$

□

Theorem 2.7. *Let H be a Hadamard matrix of order n, G be a permutation automorphism group of H, and R the corresponding row orbit matrix. Further, let ω_j, $j = 1, \ldots, t$, be the lengths of the G-orbits on columns of H, and $w \in \{\omega_j |\ j = 1, \ldots, t\}$. Let $q = p^m$ be a prime power, where p is a prime dividing n, and let the lengths of the column G-orbits of H have a property that $p\omega_j | w$ if $\omega_j < w$, and $pw | \omega_j$ if $w < \omega_j$. Then the submatrix of R corresponding to row orbits and column orbits of length w span a self-orthogonal code over $\mathbb{F}_q$.*

Proof. Let the i^{th} and the s^{th} row orbit have length w, i.e. $\Omega_i = \Omega_s = w$. Then

$$\sum_{j=1}^{t} \frac{\Omega_s}{\omega_j} \Gamma_{ij}\Gamma_{sj} = \sum_{j,\ \omega_j<w} \frac{\Omega_s}{\omega_j} \Gamma_{ij}\Gamma_{sj} + \sum_{j,\ \omega_j=w} \frac{\Omega_s}{\omega_j} \Gamma_{ij}\Gamma_{sj} + \sum_{j,\ \omega_j>w} \frac{\Omega_s}{\omega_j} \Gamma_{ij}\Gamma_{sj}$$

$$= \sum_{j,\ \omega_j<w} \frac{w}{\omega_j} \Gamma_{ij}\Gamma_{sj} + \sum_{j,\ \omega_j=w} \frac{w}{w} \Gamma_{ij}\Gamma_{sj} + \sum_{j,\ \omega_j>w} \frac{w}{\omega_j} \Gamma_{ij}\Gamma_{sj}.$$

Therefore,

$$\sum_{j,\ \omega_j=w} \Gamma_{ij}\Gamma_{sj} = \sum_{j=1}^{t} \frac{\Omega_s}{\omega_j} \Gamma_{ij}\Gamma_{sj} - \sum_{j,\ \omega_j<w} \frac{w}{\omega_j} \Gamma_{ij}\Gamma_{sj} - \sum_{j,\ \omega_j>w} \frac{w}{\omega_j} \Gamma_{ij}\Gamma_{sj}$$

$$= \delta_{is} n - \sum_{j,\ \omega_j<w} \frac{w}{\omega_j} \Gamma_{ij}\Gamma_{sj} - \sum_{j,\ \omega_j>w} \frac{w}{\omega_j} \Gamma_{ij}\Gamma_{sj}.$$

If $\omega_j < w$ then $p | \frac{w}{\omega_j}$. If $w < \omega_j$, then $\frac{w}{\omega_j}\Gamma_{ij}\Gamma_{sj} = \frac{w}{\omega_j}\frac{\omega_j}{w}\gamma_{ij}\frac{\omega_j}{w}\gamma_{sj}$ and $p | \frac{\omega_j}{w}$. Hence,

$$\sum_{j,\ \omega_j=w} \Gamma_{ij}\Gamma_{sj} \equiv 0 \ mod\ p.$$

□

The submatrix of an orbit matrix R corresponding to the fixed rows and fixed columns is called the fixed part of the orbit matrix R. The submatrix of R corresponding to the orbits of rows and columns of lengths greater than 1 is called the non-fixed part of the orbit matrix R. As a direct consequence of Theorem 2.7 we have the following corollary.

Corollary 2.8. *Let H be a Hadamard matrix, G be a permutation automorphism group of H, and R the corresponding row orbit matrix. Further, let ω_j, $j = 1, \ldots, t$, be the lengths of the G-orbits on columns of H, and p be a prime that divides ω_j if $\omega_j > 1$. Then the rows of the fixed part of R span a self-orthogonal code over the field $\mathbb{F}_q$, where $q = p^m$.*

3 Codes from orbit matrices of Paley type Hadamard matrices

The full automorphism groups of the Paley type I and Paley type II Hadamard matrices were determined by Kantor [22], and de Launey and Stafford [8] respectively. The full

automorphism group of a Hadamard matrix is preserved up to isomorphism by Hadamard equivalence. That is, if $H_1 \approx H_2$, then $\mathrm{Aut}(H_1) \cong \mathrm{Aut}(H_2)$. However it is not necessarily true that $\mathrm{PAut}(H_1) \cong \mathrm{PAut}(H_2)$, unless the matrices H_1 and H_2 are also permutation equivalent.

Example 3.1. Let $H_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$ and $H_2 = \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix}$.
Then $\mathrm{PAut}(H_1) \cong \mathrm{Sym}(3)$ and $\mathrm{PAut}(H_2) \cong \mathrm{Sym}(4)$.

As permutation automorphism groups are a key component of our method, it is pertinent to explicitly describe our construction of the Paley type matrices, and their permutation automorphism groups. Let $F = \mathbb{F}_q$ be the finite field of order q and let $\chi : F \to \{0, 1, -1\}$ be the quadratic character where $\chi(0) = 0$, $\chi(x) = 1$ if x is a quadratic residue, and $\chi(x) = -1$ otherwise. Let $A = [\chi(y - x)]_{x,y \in F}$ and $S = \begin{bmatrix} 0 & \mathbf{1} \\ \mathbf{1}^\top & -A \end{bmatrix}$, where $\mathbf{1}$ is a row of 1s.

- When $q \equiv 3 \mod 4$ the Paley type I matrix $\mathcal{P}_1(q)$ of order $q + 1$ is of the form $\begin{bmatrix} 1 & -\mathbf{1} \\ \mathbf{1}^\top & -A + I_q \end{bmatrix}$.
- When $q \equiv 1 \mod 4$ the Paley type II matrix $\mathcal{P}_2(q)$ of order $2(q + 1)$ is of the form $\begin{bmatrix} S + I_{q+1} & S - I_{q+1} \\ S - I_{q+1} & -S - I_{q+1} \end{bmatrix}$.

Note that by this construction $\mathcal{P}_1(q)$ is skew, with all 1s on the main diagonal. This implies that for any integer k,

$$(\mathcal{P}_1(q) + kI_{q+1})(\mathcal{P}_1(q) + kI_{q+1})^\top = (k^2 + 2k + q + 1)I_{q+1}. \tag{1}$$

3.1 Automorphisms of $\mathcal{P}_1(q)$

Let $q = p^m$ for a prime p and positive integer m. The full automorphism group of $\mathcal{P}_1(q)$ is described in the paper by Hall [13] and later verified to be complete by Kantor [22]; from this description we determine $\mathrm{PAut}(\mathcal{P}_1(q))$. Label the rows and columns of $\mathcal{P}_1(q)$ by $\infty, 0, x_1, \ldots, x_{q-1}$. In particular, let ∞ label the first row and column which has a different row sum and column sum respectively to all others. Any element of $\mathrm{PAut}(\mathcal{P}_1(q))$ fixes this row and column. For any element $s \in F$ and square t^2 such that $t \in F$, let $\alpha_s(x) = x + s$ and $\beta_{t^2}(x) = xt^2$ for all $x \in F$. Further let $\alpha_s(\infty) = \beta_{t^2}(\infty) = \infty$ for all choices of s and t^2. Then α_s and β_{t^2} are permutations of the symbols $\infty, 0, x_1, \ldots, x_{q-1}$, to which we associate the permutation matrices $P(\alpha_s)$ and $P(\beta_{t^2})$. Finally, let $\theta \in \mathrm{Aut}(F)$ be the Frobenius automorphism of order m that generates $\mathrm{Aut}(F)$, i.e., $\theta(x) = x^p$ for all $x \in F$. Under the added assumption that $\theta(\infty) = \infty$ we associate to θ the permutation matrix $P(\theta)$.

Lemma 3.2. *Adhering to the notation above:*

- *for each* $s \in F$, $(P(\alpha_s)^\top, P(\alpha_s)^\top) \in \mathrm{PAut}(\mathcal{P}_1(q))$;
- *for each* $t^2 \in F$, $(P(\beta_{t^2})^\top, P(\beta_{t^2})^\top) \in \mathrm{PAut}(\mathcal{P}_1(q))$;
- *for each* $1 \le i \le m$, $(P(\theta^i)^\top, P(\theta^i)^\top) \in \mathrm{PAut}(\mathcal{P}_1(q))$.

Proof. See [13, Section 2]. □

Corollary 3.3. *There is a subgroup* $G \le \mathrm{PAut}(\mathcal{P}_1(q))$ *of order* $mq(q-1)/2$.

Let G be the group described in Corollary 3.3. It is easily verified that $\mathrm{PAut}(\mathcal{P}_1(3)) \cong \mathrm{Sym}(3)$, which is of order twice that of G. We further check when $q \in \{7, 11\}$, that $G \cong \mathrm{PAut}(\mathcal{P}_1(q))$. For all $q > 11$, the result of Kantor [22, Theorem 6] proves that $G \cong \mathrm{PAut}(\mathcal{P}_1(q))$.

Theorem 3.4. *For all* $q = p^m \equiv 3 \mod 4$ *with* $q \neq 3$ *and* p *a prime,* $\mathrm{PAut}(\mathcal{P}_1(q))$ *is a group of order* $mq(q-1)/2$*, generated by the pairs of permutation matrices of Lemma 3.2.*

The first and second component of the automorphisms described above are equal, and so permute the entries on the main diagonal of $\mathcal{P}_1(q)$ amongst themselves. In particular, we have the following.

Corollary 3.5. *For any integer* k, $\mathrm{PAut}(\mathcal{P}_1(q) + kI_{q+1}) \cong \mathrm{PAut}(\mathcal{P}_1(q))$.

3.2 Examples from $\mathcal{P}_1(q)$

In the tables presenting codes over fields $*$ denotes that the code is best known, and SO denotes that the code is self-orthogonal.

In this section we list the $\mathbb{F}_p$ codes constructed from orbit matrices of Paley type I Hadamard matrix, up to order 200 ($q+1 = 200$). Here p is a prime not dividing q. Among the examined Hadamard matrices there are no examples of matrices and their permutation automorphism groups satisfying Theorem 2.7. For the examples given in Table 1, p divides $n(= q+1)$ but the divisibility conditions for orbit lengths are not satisfied. The codes spanned by the non-fixed parts of the orbit matrices are not self-orthogonal. However, the dual codes of the obtained codes are self-orthogonal.

$q+1$	$G \le \mathrm{PAut}(\mathcal{P}_1(q))$	C	$\mathrm{Dual}(C)$	$\lvert\mathrm{Aut}(C)\rvert$
72	Z_5	$[14, 8, 4]_3$	$[14, 6, 6]_3 *$ SO	672
72	Z_7	$[10, 6, 4]_3 *$	$[10, 4, 6]_3 *$ SO	2880
80	Z_3	$[26, 14, 7]_5$	$[26, 12, 9]_5$ SO	104
132	Z_5	$[26, 14, 7]_3 *$	$[26, 12, 9]_3 *$ SO	52
140	Z_3	$[46, 24, 12]_5$	$[46, 22, 12]_5$ SO	184
192	Z_5	$[38, 20, 8]_3$	$[38, 18, 9]_3$ SO	76
200	Z_{11}	$[18, 10, 4]_5$	$[18, 8, 4]_5$ SO	5184
200	Z_9	$[22, 12, 6]_5$	$[22, 10, 6]_5$ SO	88

Table 1: Codes constructed from non-fixed parts of orbit matrices

Remark 3.6. Some of the best known codes listed in Table 1 are optimal and some of them are near-optimal. The optimal codes are $[14, 6, 6]_3$, $[10, 6, 4]_3$ and $[10, 4, 6]_3$, and the near-optimal codes are $[14, 8, 4]_3$, $[26, 14, 7]_3$ and $[26, 12, 9]_3$.

A Hadamard matrix H is called skew-Hadamard if $H + H^T = 2I$. A Paley type I Hadamard matrix of order n is a skew-Hadamard matrix. In [14] Harada and Munemasa used skew-Hadamard matrices of order 20 to classify self-dual $[20, 10, 9]_7$ codes. They used the following lemma that can be found in [14], which is based on Munemasa's results presented in [24].

Lemma 3.7. *Let F be a square matrix all of whose entries are integers. If $FF^T = kI$ and p is a prime divisor of k such that $p^2 \not| k$, then F generates a self-dual code over $\mathbb{F}_p$.*

Combining the idea from Lemma 3.7 with the result from Theorem 2.7 we constructed self-orthogonal codes presented in Table 2. Moreover, the constructed codes are self-dual. We take a Paley type I Hadamard matrix H, which is skew-Hadamard, and construct the orbit matrix of $H' = H + I$ with respect to the cyclic group of order five. The codes generated by the rows of the non-fixed parts of the orbit matrices are self-dual. In Table 2 we give the list of self-dual codes constructed from non-fixed parts of orbit matrices of $H' = H + I$, corresponding to the Paley type I matrix for orders up to 332.

Remark 3.8. The constructed $[14, 7, 6]_5$ code is optimal.

$q+1$	$G \leq \mathrm{PAut}(H)$	C	$\lvert\mathrm{Aut}(C)\rvert$
32	Z_5	$[6, 3, 2]$	3072
72	Z_5	$[14, 7, 6]$ $*$	56
132	Z_5	$[26, 13, 8]$	104
152	Z_5	$[30, 15, 8]$	120
192	Z_5	$[38, 19, 10]$	152
212	Z_5	$[42, 21, 12]$	168
252	Z_5	$[50, 25, 10]$	200
272	Z_5	$[54, 27, 14]$	216
312	Z_5	$[62, 31, 14]$	248
332	Z_5	$[66, 33, 16]$	264

Table 2: Self-dual codes over $\mathbb{F}_5$ constructed from non-fixed parts of orbit matrices of $H' = H + I$

3.3 Automorphisms of $\mathcal{P}_2(q)$

Assume now that $q = p^m \equiv 1 \mod 4$, and let the permutation matrices $P(\alpha_s)$, $P(\beta_{t^2})$ and $P(\theta)$ be constructed as in the Section 3.1. Applying the same system of labeling of rows and columns of $\mathcal{P}_1(q)$ to the matrix $S + I_{q+1}$, Hall's proof that the automorphisms of Lemma 3.2 are contained in $\mathrm{PAut}(\mathcal{P}_1(q))$ holds for the matrix $S + I_{q+1}$. Therefore by applying Corollary 3.5 we have that $(P(\rho)^\top, P(\rho)^\top) \in \mathrm{PAut}(S + I_{q+1})$ for any $\rho \in \{\alpha_s, \beta_{t^2}, \theta\}$. The same applies to the matrices $S - I_{q+1}$ and $-S - I_{q+1}$, and for the remainder of this section we note that we can make the same inferences about $S - I_{q+1}$ and $-S - I_{q+1}$ that are made for $S + I_{q+1}$. By construction we get the following.

Lemma 3.9. *Let $P(\alpha_s), P(\beta_{t^2})$ and $P(\theta^i)$ be defined as in Section 3.1 with $q \equiv 1 \mod 4$. Then*

- *for each $s \in F$, $(I_2 \otimes P(\alpha_s)^\top, I_2 \otimes P(\alpha_s)^\top) \in \mathrm{PAut}(\mathcal{P}_2(q))$;*
- *for each $t^2 \in F$, $(I_2 \otimes P(\beta_{t^2})^\top, I_2 \otimes P(\beta_{t^2})^\top) \in \mathrm{PAut}(\mathcal{P}_2(q))$;*
- *for each $1 \leq i \leq m$, $(I_2 \otimes P(\theta^i)^\top, I_2 \otimes P(\theta^i)^\top) \in \mathrm{PAut}(\mathcal{P}_2(q))$.*

Lemma 3.10. *The group $\mathrm{PAut}(\mathcal{P}_2(q))$ divides the rows/columns of $\mathcal{P}_2(q)$ into four orbits; two of length 1, and two of length q. In particular $\mathrm{PAut}(\mathcal{P}_2(q)) \cong \mathrm{PAut}(-A + I_q)$.*

Proof. The automorphisms given in Lemma 3.9, by construction, fix the first $q+1$ and second $q+1$ rows and columns setwise. Now observe that the row sum in $\mathcal{P}_2(q)$ is equal to $2(q+1)$ for the first row, equal to 2 for the following q rows, and equal to -2 for the remaining $q+1$ rows. As such any permutation automorphism of $\mathcal{P}_2(q)$ must fix the first $q+1$ and second $q+1$ rows setwise. We further observe that the $(q+2)^{\text{th}}$ row is fixed by any permutation automorphism, as the sum of the first $q+1$ entries is $q-1$, which is different to that of any other row. We make the same observations for columns as $\mathcal{P}_2(q)$ is symmetric. The final claim follows from the fact that each automorphism fixes the four $q \times q$ submatrices of each quadrant obtained by removing the first rows and columns. □

Let $\Gamma\mathrm{L}(2,q) \cong \mathrm{GL}(2,q) \rtimes \mathrm{Aut}(F)$ denote the general semilinear group, and let Q denote the subgroup of $\mathrm{GL}(2,q)$ comprised of scalar maps $x \to \lambda^2 x$ where $\lambda \in F^*$. De Launey and Stafford [7] prove that $\mathrm{Aut}(S + I_{q+1}) \cong \Gamma\mathrm{L}(2,q)/Q$, see also [6, Theorem 17.2.1]. Further observe that $\mathrm{Aut}(-A + I_q)$ is isomorphic to the subgroup of $\mathrm{Aut}(S + I_{q+1})$ comprised of elements such that the left and right components fix the first row and column respectively of $S + I_{q+1}$.

The *expanded design* of a $\{\pm 1\}$-matrix H is the block matrix $E_H = \begin{bmatrix} H & -H \\ -H & H \end{bmatrix}$. We will require the following, which is a special case of [7, Theorem 2.6].

Theorem 3.11. *Let $E_{S+I_{q+1}}$ be the expanded design of $S + I_{q+1}$. Then $\mathrm{Aut}(S + I_{q+1}) \cong \mathrm{PAut}(E_{S+I_{q+1}})$.*

In particular, elements of $\mathrm{Aut}(S+I_{q+1})$ with left component fixing the first row of $S+I_{q+1}$, correspond to elements of $\mathrm{PAut}(E_{S+I_{q+1}})$ with left component fixing the first row of $E_{S+I_{q+1}}$. De Launey and Stafford [8, Section 2] show that $\mathrm{PAut}(E_{S+I_{q+1}})$ acts transitively on rows of $E_{S+I_{q+1}}$, and so the stabilizer of the first row of $E_{S+I_{q+1}}$ in $\mathrm{PAut}(E_{S+I_{q+1}})$ is of index at least $2(q+1)$, by the Orbit-Stabilizer Theorem. Thus $\mathrm{Aut}(-A+I_q)$ is isomorphic to a subgroup of index at least $2(q+1)$ in $\mathrm{Aut}(S + I_{q+1})$.

Finally, we prove the following.

Theorem 3.12. *For all $q = p^m \equiv 1 \mod 4$ with p a prime, $\mathrm{PAut}(\mathcal{P}_2(q))$ is a group of order $mq(q-1)/2$, generated by the pairs of permutation matrices of Lemma 3.9.*

Proof. It remains only to show that the group generated by the pairs of permutation matrices of Lemma 3.9 is in fact all of $\mathrm{PAut}(\mathcal{P}_2(q))$. Lemma 3.10 gives that $\mathrm{PAut}(\mathcal{P}_2(q)) \cong$

$\mathrm{PAut}(-A+I_q) \leq \mathrm{Aut}(-A+I_q) \cong G \leq \mathrm{Aut}(S+I_{q+1}) \cong \Gamma\mathrm{L}(2,q)/Q$, where G is the subgroup of $\mathrm{Aut}(S+I_{q+1})$ stabilizing the first row and column. The group $\Gamma\mathrm{L}(2,q)/Q$ is of order $2mq(q^2-1)$. As G is of index least $2(q+1)$ in $\mathrm{Aut}(S+I_{q+1})$, we know that $|\mathrm{Aut}(-A+I_q)| \leq mq(q-1)$. Finally, since $\mathrm{PAut}(-A+I_q)$ is of index at least 2 in $\mathrm{Aut}(-A+I_q)$, we get that $|\mathrm{PAut}(-A+I_q)| \leq mq(q-1)/2$. □

3.4 Examples from $\mathcal{P}_2(q)$

Here we list the codes $\mathbb{F}_p$ constructed from orbit matrices of Paley type II Hadamard matrix, up to order $2(q+1) = 228$. As before, here p is a prime not dividing q.

The examined Hadamard matrices and their permutation automorphism groups do not satisfy conditions from Theorem 2.7. For the examples from Table 3, p divides $n(= 2(q+1))$ but the divisibility conditions for orbit lengths are not satisfied. The codes spanned by the non-fixed parts of the orbit matrices are not self-orthogonal, but their dual codes are self-orthogonal.

Remark 3.13. Some of the best known codes from Table 3 are optimal and some of them are near-optimal. The optimal codes are $[8,6,2]_5$, $[8,6,2]_3$, $[8,2,6]_3$, $[16,10,4]_3$ and $[20,8,9]_3$, and the near-optimal codes are $[16,10,4]_5$, $[16,6,6]_3$, $[28,16,7]_3$, $[20,12,5]_3$ and $[44,20,15]_3$. Additionally, the constructed linear codes with parameters $[8,2,6]_3$ and $[8,2,4]_5$ are quasi-cyclic of degree 4, and the code with parameters $[14,6,4]_5$ is a quasi-cyclic code of degree 2.

$2(q+1)$	$G \leq \mathrm{PAut}(\mathcal{P}_2(q))$	C	$\mathrm{Dual}(C)$	$\lvert\mathrm{Aut}(C)\rvert$
36	Z_4	$[8,6,2]_3$ *	$[8,2,6]_3$ * SO	768
36	Z_2	$[16,10,4]_3$ *	$[16,6,6]_3$ SO	1024
60	Z_7	$[8,6,2]_5$ *	$[8,2,4]_5$ SO	18432
60	Z_2	$[28,16,7]_3$ *	$[28,12,9]_3$ SO	112
60	Z_2	$[28,16,7]_5$	$[28,12,10]_5$ SO	224
84	Z_4	$[20,12,5]_3$	$[20,8,9]_3$ * SO	160
84	Z_2	$[40,22,9]_3$ *	$[40,18,12]_3$ SO	320
100	Z_2	$[42,28,6]_5$	$[42,14,6]_5$ SO	2688
100	Z_2	$[48,26,6]_5$	$[48,22,8]_5$ SO	768
100	Z_3	$[32,18,4]_5$	$[32,14,8]_5$ SO	1024
100	Z_7	$[14,8,2]_5$	$[14,6,4]_5$ SO	$2^{13} \cdot 3^2 \cdot 5^1 \cdot 7^1$
100	Z_4	$[24,14,4]_5$	$[24,10,4]_5$ SO	12288
100	Z_6	$[16,10,2]_5$	$[16,6,4]_5$ SO	$2^{19} \cdot 3^2$
108	Z_2	$[52,28,10]_3$	$[52,24,12]_3$ SO	208
180	Z_4	$[44,24,11]_3$ *	$[44,20,15]_3$ * SO	176
180	Z_4	$[44,24,10]_5$	$[44,20,14]_5$ SO	352
180	Z_{11}	$[16,10,4]_5$	$[16,6,7]_5$ SO	256
204	Z_5	$[40,22,8]_3$	$[40,18,12]_3$ SO	160
220	Z_9	$[24,14,6]_5$	$[24,10,8]_5$ SO	768
220	Z_6	$[36,20,9]_5$	$[36,16,10]_5$ SO	288
228	Z_8	$[28,16,6]_3$	$[28,12,9]_3$ SO	672
228	Z_7	$[32,18,7]_3$	$[32,14,9]_3$ SO	128
228	Z_4	$[56,30,12]_3$	$[56,26,12]_3$ SO	224

Table 3: Codes constructed from non-fixed parts of orbit matrices

4 Codes from orbit matrices of regular Hadamard matrices

In this section we construct codes from orbit matrices of regular Hadamard matrices of order 100. A regular Hadamard matrix of order 100 corresponds to a symmetric design with parameters (100,45,20), and vice versa (see [21]). We construct four symmetric (100,45,20) designs that are not isomorphic to any of the previously known designs with these parameters, and then use the associated regular Hadamard matrices to obtain self-orthogonal codes. The designs are constructed using orbit matrices of symmetric designs. We briefly describe the construction of the designs. For further details on this construction the reader is referred to [3, 5, 18].

All known symmetric (100,45,20) designs are the design given in [17], the designs corresponding to Bush-type Hadamard matrices of order 100 presented in [3, 11, 19], and the designs corresponding to strongly regular graphs with parameters (100,45,20,20) and (100,44,18,20) (see [20]). We construct four symmetric (100,45,20) designs admitting an automorphism group isomorphic to the dihedral group $D_{10} \cong Z_5 : Z_2$ acting with ten fixed points (and blocks) and 18 orbits of length 5, with the orbit matrix given below (first ten columns and rows correspond to the fixed points and blocks, respectively).

$$\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 5 & 5 & 5 & 5 & 5 & 5 & 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 0 & 5 & 0 & 5 & 5 & 0 & 0 & 5 & 5 & 0 & 5 & 0 & 5 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 5 & 5 & 0 & 0 & 5 & 0 & 0 & 5 & 5 & 5 & 5 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 0 & 5 & 0 & 5 & 5 & 0 & 0 & 5 & 5 & 0 & 5 & 0 & 5 & 5 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 0 & 5 & 0 & 0 & 0 & 5 & 5 & 0 & 5 & 0 & 5 & 5 & 0 & 0 & 5 & 5 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 5 & 5 & 0 & 0 & 5 & 0 & 0 & 5 & 5 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 0 & 0 & 0 & 5 & 0 & 5 & 0 & 5 & 5 & 0 & 0 & 5 & 5 & 0 & 5 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 0 & 5 & 0 & 5 & 0 & 0 & 0 & 5 & 5 & 0 & 5 & 0 & 5 & 5 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 5 & 5 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 5 & 5 & 0 & 0 & 5 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 0 & 5 & 0 & 5 & 5 & 0 & 0 & 0 & 5 & 0 & 5 & 0 & 5 & 5 & 0 & 0 & 5 \\
1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 2 & 2 & 3 & 3 & 2 & 3 & 2 & 3 \\
1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 2 & 2 & 3 & 3 & 3 & 3 & 2 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 2 & 2 & 4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 3 & 2 & 3 & 2 & 3 & 3 \\
1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 2 & 2 & 2 & 4 & 2 & 2 & 2 & 2 & 2 & 3 & 2 & 3 & 0 & 2 & 2 & 3 & 3 & 2 \\
1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 2 & 2 & 2 & 4 & 2 & 2 & 2 & 2 & 3 & 3 & 2 & 2 & 0 & 2 & 2 & 3 & 3 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 2 & 2 & 2 & 2 & 2 & 4 & 2 & 2 & 2 & 2 & 3 & 3 & 2 & 2 & 0 & 3 & 2 & 3 \\
1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 4 & 2 & 2 & 3 & 3 & 2 & 3 & 2 & 3 & 0 & 2 & 2 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 4 & 2 & 2 & 3 & 3 & 3 & 3 & 2 & 2 & 0 & 2 \\
1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 4 & 3 & 2 & 3 & 2 & 3 & 3 & 2 & 2 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 3 & 3 & 2 & 2 & 3 & 2 & 3 & 2 & 4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 3 & 0 & 3 & 3 & 2 & 2 & 2 & 2 & 3 & 2 & 4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 3 & 3 & 0 & 2 & 3 & 2 & 3 & 2 & 2 & 2 & 2 & 4 & 2 & 2 & 2 & 2 & 2 & 2 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 2 & 3 & 2 & 0 & 3 & 3 & 2 & 2 & 3 & 2 & 2 & 2 & 4 & 2 & 2 & 2 & 2 & 2 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 2 & 2 & 3 & 3 & 0 & 3 & 3 & 2 & 2 & 2 & 2 & 2 & 2 & 4 & 2 & 2 & 2 & 2 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 3 & 2 & 2 & 3 & 3 & 0 & 2 & 3 & 2 & 2 & 2 & 2 & 2 & 2 & 4 & 2 & 2 & 2 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 2 & 2 & 3 & 2 & 3 & 2 & 0 & 3 & 3 & 2 & 2 & 2 & 2 & 2 & 2 & 4 & 2 & 2 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 3 & 2 & 2 & 2 & 2 & 3 & 3 & 0 & 3 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 4 & 2 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 2 & 3 & 2 & 3 & 2 & 2 & 3 & 3 & 0 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 4
\end{bmatrix}$$

Note that the above given orbit matrix is an orbit matrix of a 2-design, i.e. an orbit matrix in the sense of the definition that can be found in [5]. To construct symmetric

(100,45,20) designs from the orbit matrix we have to determine exactly which points from each point orbit are incident with a chosen representative of a block orbit, having in mind the action of the group D_{10} on the point and block orbits (see [3, 5, 18]). This step of the construction is usually called indexing. Since the indexing of the part of an orbit matrix corresponding to fixed blocks or fixed points is a trivial task, for each representative B_i of a block orbit $\mathcal{B}_i$ of length 5 we have to determine set of points from point orbits of length 5 belonging to the representative B_i. This set of points is called an index set. We can assume that the generators of D_{10} act on the set of 5 points as permutations $(0, 1, 2, 3, 4)$ and $(0)(1, 4)(2, 3)$. Further, as representatives of the block orbits of order 5 we chose blocks fixed by the permutation which acts as $(0)(1, 4)(2, 3)$ on each point orbit of length 5. Therefore, the index sets – numbered from 0 to 5 – which could occur in the designs are among the following:
$0 = \emptyset$, $1 = \{1, 4\}$, $2 = \{2, 3\}$, $3 = \{0, 1, 4\}$, $4 = \{0, 2, 3\}$ $5 = \{0, 1, 2, 3, 4\}$.

Indexing of the given orbit matrix with the presumed automorphism group D_{10} lead to exactly four mutually non-isomorphic designs, which we denote by $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{D}_3$, and $\mathcal{D}_4$. The design $\mathcal{D}_4$ is the dual design of $\mathcal{D}_1$, and $\mathcal{D}_3$ is the dual of $\mathcal{D}_2$. The full automorphism group of any of these designs is isomorphic to $Z_5 : Z_4$.

We write down parts of the base blocks for the designs $\mathcal{D}_1$ and $\mathcal{D}_2$ in terms of the index sets defined above, corresponding to the 18×18 lower-right part of the orbit matrix. The other blocks of designs can be obtained by acting on the representatives by the group generated by the cyclic permutation that on each orbit of length 5 act as $(0, 1, 2, 3, 4)$.

$\mathcal{D}_1$

5 1 1 1 1 2 2 2 2 0 1 2 3 3 2 4 1 4
2 5 2 1 1 1 2 2 1 2 0 1 1 4 3 3 4 2
2 1 5 1 2 2 1 2 1 1 2 0 4 1 3 2 4 3
2 2 2 5 1 1 1 1 2 4 2 3 0 1 2 4 3 1
2 2 1 2 5 2 1 1 1 4 3 2 2 0 1 1 3 4
1 2 1 2 1 5 1 2 2 1 4 4 1 2 0 3 2 3
1 1 2 2 2 2 5 1 1 3 4 1 3 2 4 0 1 2
1 1 1 2 2 1 2 5 2 2 3 3 4 4 1 2 0 1
1 2 2 1 2 1 2 1 5 3 1 4 2 3 4 1 2 0
0 3 4 1 1 4 2 3 2 5 2 2 2 2 1 1 1 1
4 0 3 3 2 1 1 2 4 1 5 1 2 2 2 1 1 2
3 4 0 2 3 1 4 2 1 1 2 5 2 1 1 2 1 2
2 4 1 0 3 4 2 1 3 1 1 1 5 2 2 2 2 1
2 1 4 4 0 3 3 1 2 1 1 2 1 5 1 2 2 2
3 2 2 3 4 0 1 4 1 2 1 2 1 2 5 2 1 1
1 2 3 1 4 2 0 3 4 2 2 1 1 1 1 5 2 2
4 1 1 2 2 3 4 0 3 2 2 2 1 1 2 1 5 1
1 3 2 4 1 2 3 4 0 2 1 1 2 1 2 1 2 5

$\mathcal{D}_2$

5 1 1 1 1 2 2 2 2 0 1 2 3 4 2 3 1 4
2 5 1 2 1 2 1 2 1 2 0 1 2 4 3 3 4 1
2 2 5 1 1 1 1 2 2 1 2 0 4 1 4 2 3 3
2 1 2 5 2 2 1 1 1 4 1 3 0 1 2 4 3 2
2 2 2 1 5 1 2 1 1 3 3 2 2 0 1 1 4 4
1 1 2 1 2 5 2 2 1 1 4 3 1 2 0 4 2 3
1 2 2 2 1 1 5 1 2 4 4 1 3 2 3 0 1 2
1 1 1 2 2 1 2 5 2 2 3 4 4 3 1 2 0 1
1 2 1 2 2 2 1 1 5 3 2 4 1 3 4 1 2 0
0 3 4 1 2 4 1 3 2 5 2 2 2 2 1 1 1 1
4 0 3 4 2 1 1 2 3 1 5 2 1 2 1 2 1 2
3 4 0 2 3 2 4 1 1 1 1 5 2 2 2 2 1 1
2 3 1 0 3 4 2 1 4 1 2 1 5 1 1 2 2 2
1 1 4 4 0 3 3 2 2 1 1 1 2 5 2 1 2 2
3 2 1 3 4 0 2 4 1 2 2 1 2 1 5 1 1 2
2 2 3 1 4 1 0 3 4 2 1 1 1 2 2 5 2 1
4 1 2 2 1 3 4 0 3 2 2 2 1 1 2 1 5 1
1 4 2 3 1 2 3 4 0 2 1 2 1 1 1 2 2 5

These four symmetric (100,45,20) designs are not isomorphic to the previously known designs with the same parameters. From these four symmetric designs we produce four regular Hadamard matrices, build the corresponding orbit matrices and construct codes from the orbit matrices. The results are presented in Tables 4 and 5. The self-orthogonal

code with parameters $[18, 8, 8]_5$ is constructed from the orbit matrix that satisfies the conditions of Theorem 2.7.

Remark 4.1. One of the obtained codes is optimal and some of them are near-optimal. The optimal code is $[18, 9, 6]_3$, and the codes $[18, 8, 8]_5$, $[18, 10, 6]_5$ and $[28, 25, 2]_5$ are near-optimal.

$\mathcal{D}$	$G \leq \mathrm{Aut}(\mathcal{D})$	C	Dual(C)	$\lvert\mathrm{Aut}(C)\rvert$
$\mathcal{D}_1$	$\mathbb{Z}_2$	$[36, 25, 6]_5$	$[36, 11, 15]_5$	16
$\mathcal{D}_2$	$\mathbb{Z}_2$	$[36, 25, 6]_5$	$[36, 11, 12]_5$	16
$\mathcal{D}_1$	$\mathbb{Z}_2$	$[36, 28, 4]_7$	$[36, 8, 19]_7$ SO	12
$\mathcal{D}_1$	$\mathbb{Z}_5$	$[18, 9, 6]_3$ $*$	$[18, 9, 6]_3$ $*$	288
$\mathcal{D}_1$	$\mathbb{Z}_5$	$[18, 8, 8]_5$ $*$ SO	$[18, 10, 6]_5$ $*$	1152
$\mathcal{D}_1$	$\mathbb{Z}_5$	$[18, 9, 6]_7$	$[18, 9, 6]_7$	864

Table 4: Codes constructed from non-fixed parts of orbit matrices

Design	$H \leq Aut\mathcal{D}$	C	Dual(C)	$\lvert Aut(C)\rvert$
$\mathcal{D}_1$	$\mathbb{Z}_2$	$[28, 25, 2]_5$	$[28, 3, 10]_5$	$2^{24} \cdot 3^{13} \cdot 5^3 \cdot 7^3$
$\mathcal{D}_1$	$\mathbb{Z}_2$	$[28, 20, 1]_7$	$[28, 8, 12]_7$ SO	15552

Table 5: Codes constructed from fixed parts of orbit matrices

5 Codes over $\mathbb{Z}_4$

In the same way that linear codes are defined over finite fields they can be defined over finite rings. In this case, codes are modules instead of vector spaces. The most notable codes over rings are codes over $\mathbb{Z}_4$. For more information on codes over rings we refer the reader to [10, 16].

Theorems 2.6 and 2.7 and Corollary 2.8 hold true if we replace the prime power q with a non-negative integer $m \geq 2$, and the field $\mathbb{F}_q$ by the ring $\mathbb{Z}_m$. In this section we give information on $\mathbb{Z}_4$ linear codes constructed from orbit matrices of the Hadamard matrices that we take into consideration in this paper.

According to [1], a quaternary linear code C ($\mathbb{Z}_4$-code) with parameters $[n, 4^{k_1}2^{k_2}, d]$ (where d is the Lee weight) is called good if $d > d'$, where d' is the minimum distance of the best known binary linear code of length $2n$, and dimension $2k_1 + k_2$, i.e., if the Gray image of C has a larger minimum distance than the comparable binary linear code. Similarly, a quaternary code will be called decent if its Gray image has the same parameters as the best known binary code (i.e., if $d = d'$). In tables in this section $*$ denotes that the $\mathbb{Z}_4$-code is decent, and MW, MLW and MEW stand for the minimum weight, minimum Lee weight and minimum Euclidean weight, respectively. The Gray images of the constructed codes are denoted by C'.

In Table 6 we list codes over $\mathbb{Z}_4$ constructed from orbit matrices of Paley type I Hadamard matrices. The quaternary code $((26, 4^1 2^{25}))$ is a cyclic code whose dual code is self-orthogonal.

C	MW, MEW, MLW	C'	Dual (C)	MW, MEW, MLW	Dual(C')
$((14, 4^1 2^7))$	2,8,4	$[28, 9, 4]_2$	$((14, 4^6 2^7))$ $*$	2,4,4	$[28, 19, 4]_2$
$((10, 4^1 2^5))$	2,8,4	$[20, 7, 4]_2$	$((10, 4^4 2^5))$ $*$	2,4,4	$[20, 13, 4]_2$
$((26, 4^1 2^{13}))$	5,20,10	$[52, 15, 17]_2$	$((26, 4^{12} 2^{13}))$	2,8,4	$[52, 37, 6]_2$
$((26, 4^1 2^{25}))$	1,4,2	$[52, 27, 2]_2$	$((26, 4^0 2^{25}))$	2,8,4	$[52, 25, 4]_2$
$((38, 4^1 2^{19}))$	6,24,12	$[76, 21, 12]_2$	$((38, 4^{18} 2^{19}))$	2,4,4	$[76, 55, 4]_2$
$((18, 4^1 2^9))$	4,16,8	$[36, 11, 8]_2$	$((18, 4^8 2^9))$	2,4,4	$[36, 25, 5]_2$
$((22, 4^1 2^{11}))$	6,22,12	$[44, 13, 12]_2$	$((22, 4^{10} 2^{11}))$	2,8,4	$[44, 31, 4]_2$

Table 6: Codes over $\mathbb{Z}_4$ constructed from non-fixed parts of orbit matrices of Paley type I Hadamard matrices

In Table 7 we list codes over $\mathbb{Z}_4$ constructed from orbit matrices of Paley type II Hadamard matrices. All these $\mathbb{Z}_4$-codes are self-dual. The Gray image of a $\mathbb{Z}_4$-code can be linear or non-linear and self-dual or not self-dual (see [10]). The corresponding Gray images of self-dual $\mathbb{Z}_4$-codes presented in Table 7 are self-dual linear codes. Moreover, all $\mathbb{Z}_4$-codes presented in Table 7 are cyclic. A self-dual $\mathbb{Z}_4$-code is of type II if the Euclidean weight of every codeword is a multiple of 8. A self-dual $\mathbb{Z}_4$ linear code is of type I if the Euclidean weight of some codeword is not a multiple of 8. The $\mathbb{Z}_4$-codes $((8, 4^1 2^6))$ and $((16, 4^1 2^{14}))$ presented in Table 7 are extremal type II $\mathbb{Z}_4$-codes. We refer the reader to [16] for more information.

C	MW, MEW, MLW	Type	C'
$((8, 4^0 2^8))$	1,4,2	I	$[16, 8, 2]_2$
$((16, 4^0 2^{16}))$	1,4,2	I	$[32, 16, 2]_2$
$((28, 4^0 2^{28}))$	1,4,2	I	$[56, 28, 2]_2$
$((8, 4^1 2^6))$	2,8,4	II	$[16, 8, 4]_2$
$((20, 4^0 2^{20}))$	1,4,2	I	$[40, 20, 2]_2$
$((40, 4^0 2^{40}))$	1,4,2	I	$[80, 40, 2]_2$
$((52, 4^0 2^{52}))$	1,4,2	I	$[104, 52, 2]_2$
$((44, 4^0 2^{44}))$	1,4,2	I	$[88, 44, 2]_2$
$((16, 4^1 2^{14}))$	2,8,4	II	$[32, 16, 4]_2$
$((40, 4^1 2^{38}))$	2,8,4	II	$[80, 40, 4]_2$
$((100, 4^0 2^{100}))$	1,4,2	II	$[200, 100, 2]_2$
$((24, 4^1 2^{22}))$	2,8,4	II	$[48, 24, 4]_2$
$((36, 4^0 2^{36}))$	1,4,2	I	$[72, 36, 2]_2$
$((32, 4^1 2^{30}))$	2,8,4	II	$[64, 32, 4]_2$
$((56, 4^0 2^{56}))$	1,4,2	I	$[112, 56, 2]_2$

Table 7: Self-dual codes over $\mathbb{Z}_4$ constructed from non-fixed parts of orbit matrices of Paley type II Hadamard matrices

In Table 8 we list codes over $\mathbb{Z}_4$ constructed from orbit matrices of the regular Hadamard matrices corresponding to the four symmetric $(100, 45, 20)$ designs constructed

from Section 4. The codes $((36, 4^0 2^{36}))$ and $((28, 4^1 2^{26}))$ are self-dual type I cyclic codes over $\mathbb{Z}_4$ whose Gray images are self-dual codes. The Gray image of the $((18, 4^1 2^8))$ $\mathbb{Z}_4$-code is self-orthogonal code. The dual code of this self-orthogonal code is optimal.

C	MW, MEW, MLW	C'	Dual (C)	MW, MEW, MLW	C'
$((36, 4^0 2^{36}))$	1,4,2	$[72, 36, 2]_2$	$((36, 4^0 2^{36}))$	1,4,2	$[72, 36, 2]_2$
$((18, 4^1 2^8))$	4,16,8	$[36, 10, 8]_2$ SO	$((18, 4^9 2^8))$ $*$	2,4,4	$[36, 26, 4]_2$
$((28, 4^1 2^{26}))$	$[56, 28, 4]_2$	2,8,4	$((28, 4^1 2^{26}))$	2,8,4	$[56, 28, 4]_2$

Table 8: Codes over $\mathbb{Z}_4$ constructed from orbit matrices of regular Hadamard matrices

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

References

[1] N. Aydin, T. Asamov, A Database of Z_4 Codes, J. Comb. Inf. Syst. Sci. 34 (2009), 1–12.

[2] W. Bosma, J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, 1994. http://magma.maths.usyd.edu.au/magma.

[3] D. Crnković, D. Held, Some new Bush-type Hadamard matrices of order 100 and infinite classes of symmetric designs, J. Combin. Math. Combin. Comput. 47 (2003), 155–164.

[4] D. Crnković, B. G. Rodrigues, S. Rukavina, L. Simčić, Self-orthogonal codes from orbit matrices of 2-designs, Adv. Math. Commun. 7 (2013), 161-174.

[5] D. Crnković, S. Rukavina, Construction of block designs admitting an Abelian automorphism group, Metrika 62 (2005), 175-183.

[6] W. de Launey, D. L. Flannery, *Algebraic design theory*, Math. Surveys Monogr., 175, American Mathematical Society, Providence, RI, 2011.

[7] W. de Launey, R. M. Stafford, On cocyclic weighing matrices and the regular group actions of certain Paley matrices, Discrete Appl. Math. 102, no. 1-2, (2000), 63–101, Coding, cryptography and computer security (Lethbridge, AB, 1998).

[8] W. de Launey, R. M. Stafford, On the automorphisms of Paley's type II Hadamard matrix, Discrete Math. 308, no. 13, (2008), 2910–2924.

[9] P. Dembowski, Verallgemeinerungen von Transitivitatsklassen endlicher projektiver Ebenen, Math. Z. 69 (1958), 59–89.

[10] S. T. Dougherty, Algebraic coding theory over finite commutative rings, SpringerBriefs in Mathematics, Springer-Verlag, 2017.

[11] A. Golemac, T. Vučičić, New $(100, 45, 20)$ symmetric designs and Bush-type Hadamard matrices of order 100, Discrete Math. 245 (2002), 263–272.

[12] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, `http://www.codetables.de`.

[13] M. Hall, Jr., Note on the Mathieu Group M_{12}, Arch. Math. 13 (1962), 334–340.

[14] M. Harada, A. Munemasa, On the classification of self-dual $[20, 10, 9]$ codes over GF(7), Finite Fields Appl. 42 (2016), 57–66.

[15] M. Harada, V. Tonchev, Self-orthogonal codes from symmetric designs with fixed-point-free automorphisms, The 2000 Com^{2}MaC Conference on Association Schemes, Codes and Designs (Pohang), Discrete Math. 264 (2003), 81–90.

[16] W. C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.

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

[18] Z. Janko, Coset enumeration in groups and constructions of symmetric designs, Combinatorics 90 (Gaeta, 1990), Ann. Discrete Math. 52 (1992), 275-277.

[19] Z. Janko, H. Kharaghani, V. D. Tonchev, Bush-type Hadamard matrices and symmetric designs, J. Combin. Des. 9 (2001), 72–78.

[20] L. K. Jørgensen, M. H. Klin, Switching of edges in strongly regular graphs. I.: A family of partial difference sets on 100 vertices, Electr. J. Combin. 10 (2003), R17.

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

[22] W. Kantor, Automorphism groups of Hadamard matrices, J. Combinatorial Theory 6, (1969) 279–281.

[23] H. Kharaghani, B. Tayfeh-Rezaie, A Hadamard matrix of order 428, J. Combin. Des. 13 (2005), 435-440.

[24] A. Munemasa, H. Tamura, The codes and the lattices of Hadamard matrices, Eur. J. Comb. 33 (2012), 519–533.