Self-orthogonal codes constructed from weakly self-orthogonal designs invariant under an action of $M_{11}$

Vedrana Mikulić Crnković1 · Ivona Traunkar1

Received: 21 October 2020 / Revised: 10 December 2020 / Accepted: 19 December 2020 / Published online: 1 February 2021
© The Author(s), under exclusive licence to Springer-Verlag GmbH, DE part of Springer Nature 2021

Abstract
In this paper we generalize the construction of binary self-orthogonal codes obtained from weakly self-orthogonal designs described in Tonchev (J Combinat Theory Ser A 52:197-205, 1989) in order to obtain self-orthogonal codes over an arbitrary field. We extend construction self-orthogonal codes from orbit matrices of self-orthogonal designs and weakly self-orthogonal 1-designs such that block size is odd and block intersection numbers are even described in Crnković (Adv Math Commun 12:607–628, 2018). Also, we generalize mentioned construction in order to obtain self-orthogonal codes over an arbitrary field. We construct weakly self-orthogonal designs invariant under an action of Mathieu group $M_{11}$ and, from them, binary self-orthogonal codes.

Keywords  Mathieu group · Design · Orbit matrix · Linear code · Weakly self-orthogonal design · Self-orthogonal codes

1 Introduction

Codes constructed from block designs ([1,2,13]) and from orbit matrices ([4,8–11]) have been extensively studied. In [12], Tonchev described some extensions of incidence matrices of a block design which define self-orthogonal binary codes and in [5] authors study similar extensions of orbit matrices and submatrices of orbit matrices of 1-design in order to construct binary self-orthogonal codes from the simple group $He$. In [7] authors construct self-dual codes over finite fields by extending incidence matrices and orbit matrices of a block designs. In [3] authors proved that all $G$-invariant
binary self-orthogonal codes are subcodes of the dual code of the code spanned by the sets of fixed points of involutions of $G$ and they classify all $M_{11}$-invariant binary self-dual codes.

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a $t$-$(v, k, \lambda)$ design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely $k$ points, and every $t$ distinct points are together incident with precisely $\lambda$ blocks. An incidence matrix of a $t$-$(v, k, \lambda)$ design $\mathcal{D}$ with $b$ blocks is a $b \times v$ matrix $M = [m_{i,j}]$, where $m_{i,j} = 1$ if point $P_j$ is incident with block $B_i$, and 0 otherwise. A $t$-$(v, k, \lambda)$ design is called weakly self-orthogonal if all the block intersection numbers have the same parity. A design is self-orthogonal if it is weakly self-orthogonal and if the block intersection numbers and the block size are even numbers.

An isomorphism from one design to other is a bijective mapping of points to points and blocks to blocks which preserves incidence. An isomorphism from a design $\mathcal{D}$ onto itself is called an automorphism of $\mathcal{D}$. The set of all automorphisms of $\mathcal{D}$ forms its full automorphism group denoted by $\text{Aut}(\mathcal{D})$.

The code $C_{\mathbb{F}}(\mathcal{D})$ of the design $\mathcal{D}$ over the finite field $\mathbb{F}$ is the space spanned by the incidence vectors of the blocks over $\mathbb{F}$. A code $C$ over field of order $q$, length $n$, dimension $k$ is $[n, k]_q$ code. If $q = 2$ and minimum distance $d$, we denote code $C$ by $[n, k, d]$. The dual code $C^\perp$ is the orthogonal under the standard inner product, i.e. $C^\perp = \{v \in \mathbb{F}^n \mid v \cdot c = 0 \text{ for all } c \in C\}$. A code $C$ is self-orthogonal if $C \subseteq C^\perp$. If $\mathcal{D}$ is a self-orthogonal design then the binary code of the design $\mathcal{D}$ is self-orthogonal. The incidence matrix $M$ of a weakly self-orthogonal design can be extended in a certain way in order to span self-orthogonal code. The $i$-th row of the matrix $M$ will be denoted by $M[i]$. The all-one vector will be denoted by $1$, and is the constant vector with all coordinate entries equal to 1. Two linear codes are equivalent if they can be obtained from one another by multiplication of the coordinate positions by non-zero field elements or by permuting the coordinate positions. An automorphism of a code $C$ is an isomorphism from $C$ to $C$. The full automorphism group will be denoted by $\text{Aut}(C)$. If code $C_{\mathbb{F}}(\mathcal{D})$ is a linear code of a design $\mathcal{D}$ over a finite field $\mathbb{F}$, then the full automorphism group of $\mathcal{D}$ is contained in the full automorphism group of code $C_{\mathbb{F}}(\mathcal{D})$.

Designs are obtained from transitive permutation representations of Mathieu group $M_{11}$. $M_{11}$ is simple group of order 7920 which has 39 non-equivalent transitive permutation representations. Among others, lattice of $M_{11}$ is consisted of 1 subgroup of index 22, 1 subgroup of index 55, 1 subgroup of index 66, 3 subgroups of index 110, 2 subgroups of index 132, 1 subgroup of index 144 and 1 subgroup of index 165. Using mentioned subgroups we obtained transitive permutation representations of $M_{11}$ on 22, 55, 66, 110, 132, 144 and 165 points.

In Sect. 2, we generalize the construction (in [12]) of binary self-orthogonal codes using incidence matrix of weakly self-orthogonal design to obtain self-orthogonal codes over an arbitrary finite field. In Sect. 3, we extend the construction (in [5]) of binary self-orthogonal codes using orbit matrices of self-orthogonal designs and weakly self-orthogonal designs such that block size is even and block intersection numbers are odd to the construction from general weakly self-orthogonal designs. Also, we generalize mentioned construction in order to obtain self-orthogonal codes over an arbitrary finite field.
Finally, in Sect. 4 we give tables of constructed optimal, near-optimal and best known binary codes obtained from weakly self-orthogonal designs invariant under an action of $M_{11}$, constructed using construction described in [6].

2 Self-orthogonal codes obtained from WSO designs

Let $\mathcal{D}$ be weakly self-orthogonal design and let $M$ be its $b \times v$ incidence matrix. Using suitable extension of $M$ one can obtain self-orthogonal binary code $C$.

**Theorem 1** Let $\mathcal{D}$ be weakly self-orthogonal design and let $M$ be its $b \times v$ incidence matrix.

1. If $\mathcal{D}$ is a self-orthogonal design, than $C(\mathcal{D})$ is a binary self-orthogonal code.
2. If $\mathcal{D}$ is such that $k$ is even and the block intersection numbers are odd, then the matrix $[I_b, M, 1]$, generates a binary self-orthogonal code.
3. If $\mathcal{D}$ is such that $k$ is odd and the block intersection numbers are even, then the matrix $[I_b, M]$, generates a binary self-orthogonal code.
4. If $\mathcal{D}$ is such that $k$ is odd and the block intersection numbers are odd, then the matrix $[[M, 1]]$, generates a binary self-orthogonal code.

**Proof** [12].

Previous theorem can be generalized to obtain self-orthogonal codes over finite field $\mathbb{F}_q$, where $q$ is prime power.

**Theorem 2** Let $q$ be prime power and $\mathbb{F}_q$ a finite field of order $q$. Let $\mathcal{D}$ be 1 – (v, k, r) design and let $M$ be its $b \times v$ incidence matrix. Let $\mathcal{D}$ be such that $k \equiv a (\text{mod } q)$ and $|B_i \cap B_j| \equiv d (\text{mod } q)$, for all $i, j \in \{1, \ldots, b\}$, $i \neq j$, where $B_i$ and $B_j$ are two blocks of the design $\mathcal{D}$.

1. If $a = d = 0$, than $M$ generates a self-orthogonal code over $\mathbb{F}_q$.
2. If $a = 0$ and $d \neq 0$, then the matrix $[\sqrt{d} \cdot I_b, M, \sqrt{-d} \cdot 1]$ generates a $b$-dimensional self-orthogonal code over $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if $-d$ is quadratic residue modulo $q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise.
3. If $a \neq 0$ and $d = 0$, then the matrix $[\sqrt{-a} \cdot I_b, M]$ generates a $b$-dimensional self-orthogonal code over $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if $-a$ is quadratic residue modulo $q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise. If $b = v$, obtained code is self-dual.
4. If $a \neq 0$ and $d \neq 0$, there are two cases:
   (a) if $a = d$, then the matrix $[M, \sqrt{-a} \cdot 1]$ generates a self-orthogonal code over $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if $-a$ is quadratic residue modulo $q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise, and
   (b) if $a \neq d$, then the matrix $[\sqrt{d - a} \cdot I_b, M, \sqrt{-d} \cdot 1]$ generates a $b$-dimensional self-orthogonal code over $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if $-d$ is quadratic residue modulo $q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise.

**Proof** 1. Since $a = 0$, it follows that

$$M[i] \cdot M[i] = k \equiv a (\text{mod } q) \equiv 0 (\text{mod } q),$$
and since \( d = 0 \) it follows that
\[
M[i] \cdot M[j] = |B_i \cap B_j| \equiv d \pmod{q} \equiv 0 \pmod{q},
\]
for all \( i, j \in \{1, \ldots, b\}, \ i \neq j \). We conclude that \( M \) generates a self-orthogonal code over \( \mathbb{F}_q \).

2. Let \( A = [\sqrt{d} \cdot I_b, M, \sqrt{-d} \cdot 1] \). Then
\[
A[i] \cdot A[i] = d + k - d \equiv 0 \pmod{q}
\]
and
\[
A[i] \cdot A[j] = |B_i \cap B_j| - d \equiv d - d \pmod{q} \equiv 0 \pmod{q},
\]
for all \( i, j \in \{1, \ldots, b\}, \ i \neq j \). We conclude that \( A \) generates a self-orthogonal code over \( \mathbb{F} \), where \( \mathbb{F} = \mathbb{F}_q \) if \(-d\) is quadratic residue modulo \( q \), and \( \mathbb{F} = \mathbb{F}_{q^2} \) otherwise. ¹

3. Let \( A = [\sqrt{-a} \cdot I_b, M] \). Then
\[
A[i] \cdot A[i] = -a + k \equiv 0 \pmod{q}
\]
and
\[
A[i] \cdot A[j] = |B_i \cap B_j| \equiv 0 \pmod{q},
\]
for all \( i, j \in \{1, \ldots, b\}, \ i \neq j \). We conclude that \( A \) generates a \( b \)-dimensional self-orthogonal code over \( \mathbb{F} \), where \( \mathbb{F} = \mathbb{F}_q \) if \(-d\) is quadratic residue modulo \( q \), and \( \mathbb{F} = \mathbb{F}_{q^2} \) otherwise. If \( b = v \), dimension of a code is half of its length, so the code is self-dual.

4. (a) Let \( A = [M, \sqrt{-a} \cdot 1] \). Then
\[
A[i] \cdot A[i] = k - a \equiv 0 \pmod{q}
\]
and
\[
A[i] \cdot A[j] = |B_i \cap B_j| - a \equiv 0 \pmod{q},
\]
for all \( i, j \in \{1, \ldots, b\}, \ i \neq j \). We conclude that \( A \) generates a self-orthogonal code over \( \mathbb{F} \), where \( \mathbb{F} = \mathbb{F}_q \) if \(-d\) is quadratic residue modulo \( q \), and \( \mathbb{F} = \mathbb{F}_{q^2} \) otherwise.

(b) Let \( A = [\sqrt{d - a} \cdot I_b, M, \sqrt{-d} \cdot 1] \). Then
\[
A[i] \cdot A[i] = d - a + k - d \equiv 0 \pmod{q}
\]

¹ Elements which are equal to 0 in \( \mathbb{F}_q \) are also equal to 0 in \( \mathbb{F}_{q^2} \), since elements of \( \mathbb{F}_q \) are polynomials in \( \mathbb{F}_{q^2} \) of degree at most 1 with coefficients in \( \mathbb{F}_q \).
and

\[ A[i] \cdot A[j] = |B_i \cap B_j| - d \equiv 0 \pmod{q}, \]

for all \( i, j \in \{1, \ldots, b\}, i \neq j \). We conclude that \( A \) generates a \( b \)-dimensional self-orthogonal code over \( \mathbb{F} \), where \( \mathbb{F} = \mathbb{F}_q \) if \( -d \) is quadratic residue modulo \( q \), and \( \mathbb{F} = \mathbb{F}_{q^2} \) otherwise.

\[ \square \]

### 3 Codes from orbit matrices of weakly self-orthogonal designs

**Remark 3** Let \( D \) be \( 1-(v, k, r) \) design and \( G \) be an automorphism group of the design. Let \( v_1 = |V_1|, \ldots, v_n = |V_n| \) be the sizes of point orbits and \( b_1 = |B_1|, \ldots, b_m = |B_m| \) be the sizes of block orbits under the action of the group \( G \). We define an orbit matrix under the action of \( G \) as an \( m \times n \) matrix:

\[
\begin{bmatrix}
a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\
a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{m,1} & a_{m,2} & \cdots & a_{m,n}
\end{bmatrix},
\]

where \( a_{i,j} \) is the number of points of the orbit \( V_j \) incident with a block of the orbit \( B_i \).

It is easy to see that the orbit matrix is well defined and that \( k = \sum_{j=1}^{n} a_{i,j} \).

For \( x \in B_s \), by counting the incidence pairs \( (P, x') \) such that \( x' \in B_t \) and \( P \) is incident with the block \( x \), we obtain \( \sum_{x' \in B_t} |x \cap x'| = \sum_{j=1}^{n} b_{t} \frac{w}{v_j} a_{s,j} a_{t,j} \).

**Remark 4** Let \( D \) be \( 1-(v, k, r) \) design such that \( k \equiv a \pmod{q} \) and \( |B_i \cap B_j| \equiv d \pmod{q} \), for all \( i, j \in \{1, \ldots, b\}, i \neq j \), where \( B_i \) and \( B_j \) are two blocks of the design \( D \). Let \( G \) be an automorphism group of the design which acts on \( D \) with \( n \) point orbits of length \( w \) and block orbits of length \( b_1, b_2, \ldots, b_m \), and let \( O \) be an orbit matrix of a design \( D \) under the action of the group \( G \). From previous remark, for \( x \in B_s \) and \( s \neq t \) one concludes that

\[
\frac{b_{t}}{w} O[s] \cdot O[t] = \sum_{j=1}^{n} \frac{b_{t}}{w} a_{s,j} a_{t,j} \\
= \sum_{x' \in B_t} |x \cap x'|.
\]

It follows that

\[
\frac{b_{t}}{w} O[s] \cdot O[t] \equiv b_{t} d \pmod{q}.
\]
Similar, for \( x \in B_s \) one can conclude that

\[
\frac{b_t}{w} O[s] \cdot O[s] = \sum_{x' \in B_s} |x \cap x'| \\
= |x \cap x| + \sum_{x' \in B_s, x \neq x'} |x \cap x'|.
\]

It follows that

\[
\frac{b_s}{w} O[s] \cdot O[s] \equiv a + (b_s - 1)d \pmod{q}.
\]

Let \( D \) be \( 1 - (v, k, r) \) design and \( G \) an automorphism group of \( D \) acting with \( f_1 \) fixed points and \( n \) point orbits of length \( q > 1 \), and with \( f_2 \) fixed blocks and \( m \) block orbits of length \( q \). We define matrices \( OM1 \) and \( OM2 \) to be, respectively, the matrices

\[
\begin{bmatrix}
  a_{1,1} & a_{1,2} & \cdots & a_{1,f_1} \\
  a_{2,1} & a_{2,2} & \cdots & a_{2,f_1} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{f_1,1} & a_{f_1,2} & \cdots & a_{f_1,f_1}
\end{bmatrix}
\]

and

\[
\begin{bmatrix}
  a_{f_2+1,f_1+1} & a_{f_2+1,f_1+2} & \cdots & a_{f_2+1,f_1+n} \\
  a_{f_2+2,f_1+1} & a_{f_2+2,f_1+2} & \cdots & a_{f_2+2,f_1+n} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{f_2+m,f_1+1} & a_{f_2+m,f_1+2} & \cdots & a_{f_2+m,f_1+n}
\end{bmatrix},
\]

where the columns 1, 2, \ldots, \( f_1 \) correspond to the fixed points and the rows 1, 2, \ldots, \( f_2 \) correspond to the fixed blocks.

**Remark 5**

a) If \( B_1 \) and \( B_2 \) are blocks fixed under the action of group \( G \) on the design, then \( B_1, B_2 \) and \( B_1 \cap B_2 \) are unions of some \( G \)-orbits of the point set.

b) Let \( B_t \) and \( B_s \) be block orbits of size \( q \) under the action of the group \( G \) on the design. It follows from Remark 3 that

\[
\sum_{x' \in B_t} |x \cap x'| = \frac{f_1}{v_j} b_j a_{s,j} a_{t,j} + \sum_{j=f_1+1}^{f_1+n} \frac{b_j}{v_j} a_{s,j} a_{t,j} \\
= q \sum_{j=1}^{f_1} a_{s,j} a_{t,j} + \sum_{j=f_1+1}^{f_1+n} a_{s,j} a_{t,j}.
\]
3.1 Codes from orbit matrices of self-orthogonal 1-designs

**Theorem 6** Let $\mathcal{D}$ be a self-orthogonal 1-design and $G$ be an automorphism group of the design which acts on $\mathcal{D}$ with $n$ point orbits of length $w$ and block orbits of length $b_1, b_2, \ldots, b_m$ such that $b_i = 2^u \cdot b_i'$, $w = 2^u \cdot w'$, $0 \leq u, 2 \nmid b_i'$ and $2 \nmid w'$, for $i \in \{1, \ldots, m\}$. Then the binary code spanned by the rows of orbit matrix of the design $\mathcal{D}$ (under the action of the group $G$) is a self-orthogonal code of length $\frac{v \cdot w}{w}$.

**Proof** In [5]. $\square$

Using the following theorem, one can use orbit matrices of a self-orthogonal design to construct self-orthogonal codes over $\mathbb{F}_q$, where $q$ is prime power.

**Theorem 7** Let $q$ be prime power and $\mathbb{F}_q$ a finite field of order $q$. Let $\mathcal{D}$ be a 1–$(v, k, r)$ design such that $k \equiv 0 \pmod{q}$ and $|B_i \cap B_j| \equiv 0 \pmod{q}$, for all $i, j \in \{1, \ldots, b\}$, $i \neq j$, where $B_i$ and $B_j$ are two blocks of the design $\mathcal{D}$, and let $G$ be an automorphism group of the design which acts on $\mathcal{D}$ with $n$ point orbits of length $w$ and $m$ block orbits of length $w$. Then the binary linear code spanned by the rows of orbit matrix of the design $\mathcal{D}$ (under the action of the group $G$) is a self-orthogonal code over $\mathbb{F}_q$ of length $\frac{v \cdot w}{w}$ with dimension equal to $\text{rank}(O)$.

**Proof** Let $O$ be the orbit matrix of a design $\mathcal{D}$ under the action of $G$. From Remark 4 it follows that $O[s] \cdot O[t] \equiv 0 \pmod{q}$, and $O[s] \cdot O[s] \equiv 0 \pmod{q}$, for all $s, t \in \{1, \ldots, m\}$. $\square$

**Theorem 8** Let $\mathcal{D}$ be a self-orthogonal 1–$(v, k, r)$ design and $G$ be an automorphism group of $\mathcal{D}$ acting with $f_1$ fixed points and $n$ point orbits of length 2, and with $f_2$ fixed blocks and $m$ block orbits of length 2. Then

1. The binary linear code spanned by the matrix $OM_1$ is a binary self-orthogonal code of length $f_1$ and dimension $\text{rank}(OM_1)$;
2. The binary linear code spanned by the matrix $OM_2$ is a binary self-orthogonal code of length $n$ and dimension $\text{rank}(OM_2)$.

**Proof** In [5]. $\square$

We generalize previous theorem to obtain self-orthogonal codes over $\mathbb{F}_q$, where $q$ is a prime power.

**Theorem 9** Let $q$ be prime power and $\mathbb{F}_q$ a finite field of order $q$. Let $\mathcal{D}$ be a 1–$(v, k, r)$ design such that $k \equiv 0 \pmod{q}$ and $|B_i \cap B_j| \equiv 0 \pmod{q}$, for all $i, j \in \{1, \ldots, b\}$, $i \neq j$, where $B_i$ and $B_j$ are two blocks of the design $\mathcal{D}$, and let $G$ be an automorphism group of the design which acts on $\mathcal{D}$ with $f_1$ fixed points and $n$ point orbits of length $q$, and with $f_2$ fixed blocks and $m$ block orbits of length $q$. Then

1. the linear code spanned by the matrix $OM_1$ is a self-orthogonal $[f_1, \text{rank}(OM_1)]$ code over the field $\mathbb{F}_q$.
2. the linear code spanned by the matrix $OM_2$ is a self-orthogonal $[n, \text{rank}(OM_2)]$ code over the field $\mathbb{F}_q$. $\square$
1. Since \( k \equiv 0 \pmod{q} \), each block contains \( q \cdot \alpha \) fixed points and since \( |B_i \cap B_j| \equiv 0 \pmod{q} \), for all \( i, j \in \{1, \ldots, b\}, i \neq j \), intersection of every two blocks contains \( q \cdot \beta \) fixed points. Therefore, it follows that the matrix \( OM1 \) spans a self-orthogonal code over the field \( \mathbb{F}_q \).

2. From Remark 5, for \( s \neq t \), since \( B_t \) is block orbit of size \( q \), it follows that

\[
\sum_{x' \in B_t} |x \cap x'| \equiv 0 \pmod{q},
\]

and for \( s = t \) it follows that

\[
\sum_{x' \in B_s} |x \cap x'| = |x \cap x| + \sum_{x' \in B_s, x \neq x'} |x \cap x'| \equiv 0 + (q - 1)0 \pmod{q}.
\]

We conclude that \( OM2[s] \cdot OM2[t] \equiv 0 \pmod{q} \), for \( s \neq t \) and \( OM2[s] \cdot OM2[s] \equiv 0 \pmod{q} \) and that the binary code spanned by the matrix \( OM2 \) is self-orthogonal over the field \( \mathbb{F}_q \). □

### 3.2 Codes from orbit matrices of extended weakly self-orthogonal 1-designs with \( k \) even and odd block intersection numbers

**Theorem 10** Let \( \mathcal{D} \) be a weakly self-orthogonal 1-design such that \( k \) is even and the block intersection numbers are odd, and let \( G \) be an automorphism group of the design which acts on \( \mathcal{D} \) with \( n \) point orbits of length \( w \) and block orbits of length \( b_1, b_2, \ldots, b_m \) such that \( b_i = 2^o \cdot b'_i, \ w = 2^u \cdot w' \), \( o \leq u \), \( 2 \nmid b'_i \) and \( 2 \nmid w' \) for \( i \in \{1, \ldots, m\} \). Let \( O \) be the orbit matrix of \( \mathcal{D} \) under action of the group \( G \).

a) If \( o = u = 0 \), then the binary linear code spanned by the rows of the matrix \( [I_m, O, I] \) is a self-orthogonal code of the length \( m + \frac{w}{w} + 1 \) and dimension \( m \).

b) If \( o \geq 1 \) and \( o = u \) then the binary linear code spanned by the rows of the matrix \( [I_m, O] \) is a self-orthogonal code of the length \( m + \frac{w}{w} \) and dimension \( m \). If \( m = n \), the obtained code is self-dual.

c) If \( o < u \), then binary linear code spanned by the rows of the matrix \( O \) is a self-orthogonal code of the length \( \frac{w}{w} \) and dimension \( \text{rank}(O) \).

**Proof**

a) Since \( w, b_1, \ldots, b_m \) are all odd numbers, it follows from Remark 4 that

\[
O[s] \cdot O[t] \equiv 1 \pmod{2}, \quad O[s] \cdot O[s] \equiv 0 \pmod{2},
\]

for all \( s, t \in \{1, \ldots, m\}, \ s \neq t \).

b) Since \( w, b_1, \ldots, b_m \) are all even numbers and \( \frac{b_t}{w} = \frac{2^o \cdot b'_t}{2^u \cdot w'} = \frac{b'_t}{w'} \), for every \( t \in \{1, \ldots, m\} \), it follows from Remark 4 that

\[
O[s] \cdot O[t] \equiv 0 \pmod{2}, \quad O[s] \cdot O[s] \equiv 1 \pmod{2},
\]

for all \( s, t \in \{1, \ldots, m\} \).
c) Since \( o < u \) and since \( \frac{b_t}{w} O[s] \cdot O[t] = \frac{b'_t}{2w-\nu w'} O[s] \cdot O[t] \) is a positive integer from Remark 4, it follows that \( 2 \mid O[s] \cdot O[t] \), for all \( s, t \in \{1, \ldots, m\} \). \( \square \)

One can generalize previous theorem to construct a self-orthogonal code over \( \mathbb{F}_q \), where \( q \) is a prime power. The following theorem describes the construction.

**Theorem 11** Let \( q \) be prime power and \( \mathbb{F}_q \) a finite field of order \( q \). Let \( \mathcal{D} \) be a \( (v, k, r) \) design such that \( k \equiv 0(\text{mod } q) \) and \( |B_i \cap B_j| \equiv d(\text{mod } q) \), for all \( i, j \in \{1, \ldots, b\}, \ i \neq j \), where \( B_i \) and \( B_j \) are two blocks of the design \( \mathcal{D} \), and let \( G \) be an automorphism group of the design which acts on \( \mathcal{D} \) with \( n \) point orbits of length \( w \) and \( m \) block orbits of length \( w \) and let \( O \) be the orbit matrix of \( \mathcal{D} \) under action of the group \( G \).

a) If \( q \mid w \), then linear code spanned by the rows of the matrix \( A = [\sqrt{-d} I_m, O] \) is a self-orthogonal \([m + n, m] \) code over the field \( \mathbb{F} \), where \( \mathbb{F} = \mathbb{F}_q \) if \( d \) is square root in \( \mathbb{F}_q \), and \( \mathbb{F} = \mathbb{F}_{q^2} \) otherwise. If \( m = n \), the obtained code is self-dual.

b) If \( q \not| \ w - 1 \), then linear code spanned by the rows of the matrix \( A = [\sqrt{wd} I_m, O, \sqrt{-wd} I] \) is a self-orthogonal \([m + n + 1, m] \) code over the field \( \mathbb{F} \), where \( \mathbb{F} = \mathbb{F}_q \) if \( wd \) is square root in \( \mathbb{F}_q \), and \( \mathbb{F} = \mathbb{F}_{q^2} \) otherwise.

c) If \( q \not| \ w \) and \( q \not| \ w - 1 \), then linear code spanned by the rows of the matrix \( A = [\sqrt{wd} - (w - 1)d I_m, O, \sqrt{-wd} I] \) is a self-orthogonal \([m + n + 1, m] \) code over the field \( \mathbb{F} \), where \( \mathbb{F} = \mathbb{F}_q \) if \( -wd \) is square root in \( \mathbb{F}_q \), and \( \mathbb{F} = \mathbb{F}_{q^2} \) otherwise.

**Proof** It follows from Remark 4 that \( O[s] \cdot O[t] \equiv wd(\text{mod } q) \), for \( s \neq t \) and \( O[s] \cdot O[s] \equiv (w - 1)d(\text{mod } q) \).

a) If \( q \mid w \), then \( A[s] \cdot A[t] = O[s] \cdot O[t] \equiv 0(\text{mod } q) \) and \( A[s] \cdot A[s] = -d + O[s] \cdot O[s] \equiv 0(\text{mod } q) \).

b) If \( q \mid w - 1 \), then \( A[s] \cdot A[t] = O[s] \cdot O[t] - wd \equiv 0(\text{mod } q) \) and \( A[s] \cdot A[s] = wd + O[s] \cdot O[s] - wd \equiv 0(\text{mod } q) \).

c) If \( q \not| \ w \) and \( q \not| \ w - 1 \), then \( A[s] \cdot A[t] = O[s] \cdot O[t] - wd \equiv 0(\text{mod } q) \) and \( A[s] \cdot A[s] = wd - (w - 1)d + O[s] \cdot O[s] - wd \equiv 0(\text{mod } q) \). \( \square \)

**Theorem 12** Let \( \mathcal{D} \) be a weakly self-orthogonal \( (v, k, r) \) design such that \( k \) is even and block intersection numbers are odd. Let \( G \) be an automorphism group of \( \mathcal{D} \) acting with \( f_1 \) fixed points and \( n \) point orbits of length 2, and with \( f_2 \) fixed blocks and \( m \) block orbits of length 2. Then

1. the binary linear code spanned by the matrix \( [I_{f_2}, OM1, I] \) is a self-orthogonal code of length \( f_2 + f_1 + 1 \) and dimension \( f_2 \).
2. the binary linear code spanned by the matrix \( [I_m, OM2] \) is a self-orthogonal code of length \( m + n \) and dimension \( m \). If \( m = n \), the obtained code is self-dual.

**Proof** 1. Since \( k \) is even, each block contains even number of fixed points and since block intersection numbers are odd, intersection of every two blocks contains odd number of fixed points. Therefore, it follows that the matrix \( [I_{f_2}, OM1, I] \) spans a binary self-orthogonal code.
2. For $s \neq t$, since $B_i$ is block orbit of size 2, it follows from Remark 5 that
\[
\sum_{x' \in B_i} |x \cap x'| \equiv 2 \cdot 1 \pmod{2} \equiv 0 \pmod{2},
\]
and for $s = t$,
\[
\sum_{x' \in B_i} |x \cap x'| = |x \cap x| + \sum_{x' \in B_i, x \neq x'} |x \cap x'| \equiv 0 + 1 \pmod{2}.
\]

We conclude that $\sum_{j=f_1+1}^{f_1+n} a_{s,j} a_{t,j} \equiv 0 \pmod{2}$, for $s \neq t$ and
\[
\sum_{j=f_1+1}^{f_1+n} a_{s,j} a_{s,j} \equiv 1 \pmod{2}
\]
and that the binary code spanned by the matrix $[I_m, OM2]$ is self-orthogonal. If $m = n$, dimension of the code is half of its length, so the code is self-dual. \hfill \Box

We generalize previous theorem to obtain self-orthogonal codes over $\mathbb{F}_q$, where $q$ is a prime power.

**Theorem 13** Let $q$ be prime power and $\mathbb{F}_q$ a finite field of order $q$. Let $\mathcal{D}$ be a $(v, k, r)$ design such that $k \equiv 0 \pmod{q}$ and $|B_i \cap B_j| \equiv d \pmod{q}$, for all $i, j \in \{1, \ldots, b\}$, $i \neq j$, where $B_i$ and $B_j$ are two blocks of the design $\mathcal{D}$, and let $G$ be an automorphism group of the design which acts on $\mathcal{D}$ with $f_1$ fixed points and $n$ point orbits of length $q$, and with $f_2$ fixed blocks and $m$ block orbits of length $q$. Then

1. linear code spanned by the matrix $[\sqrt{-d} \cdot I_{f_2}, OM1, \sqrt{-d} \cdot I]$ is a self-orthogonal $[f_2 + f_1 + 1, f_2]$ code over the field $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if $d$ is square root in $\mathbb{F}_q$, and $\mathbb{F} = \mathbb{F}_q^2$ otherwise.

2. linear code spanned by the matrix $[\sqrt{-q-1}d \cdot I_m, OM2]$ is a self-orthogonal $[m+n, m]$ code over the field $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if $d$ is square root in $\mathbb{F}_q$, and $\mathbb{F} = \mathbb{F}_q^2$ otherwise. If $m = n$, the obtained code is self-dual.

**Proof** 1. Since $k \equiv 0 \pmod{q}$, each block contains $q \cdot \alpha$ fixed points and since $|B_i \cap B_j| \equiv d \pmod{q}$, for all $i, j \in \{1, \ldots, b\}$, $i \neq j$, intersection of every two blocks contains $q \cdot \beta + d$ fixed points. Therefore, it follows that the matrix $[\sqrt{-d} \cdot I_m, OM1, \sqrt{-d} \cdot I]$ spans a self-orthogonal code of length $f_2 + f_1 + 1$ over the field $\mathbb{F}$.

2. For $s \neq t$, since $B_i$ is block orbit of size $q$, it follows from Remark 5 that
\[
\sum_{x' \in B_i} |x \cap x'| \equiv qd \pmod{q} \equiv 0 \pmod{q},
\]
and if $s = t$ it follows that
\[
\sum_{x' \in B_i} |x \cap x'| = |x \cap x| + \sum_{x' \in B_i, x \neq x'} |x \cap x'| \equiv 0 + (q - 1)d \pmod{q}.
\]
We conclude that $OM2[s] \cdot OM2[t] \equiv 0 (\text{mod } q)$, for $s \neq t$ and $OM2[s] \cdot OM2[s] \equiv (q - 1)d (\text{mod } q)$ and that the binary code spanned by the matrix $[\sqrt{(q - 1)d} \cdot I_m, OM2]$ is self-orthogonal over the field $\mathbb{F}$.

\[ \square \]

### 3.3 Codes from orbit matrices of extended weakly self-orthogonal 1-designs with $k$ odd and even block intersection numbers

**Theorem 14** Let $\mathcal{D}$ be a weakly self-orthogonal 1-design such that $k$ is odd and the block intersection numbers are even and $G$ be an automorphism group of the design which acts on $\mathcal{D}$ with $n$ point orbits of length $w$ and block orbits $b_1, b_2, \ldots, b_m$ such that $b_i = 2^o \cdot b'_i$, $w = 2^u \cdot w'$, $o \leq u$, $2 \not| b'_i$ and $2 \not| w'$, for $i \in \{1, \ldots, m\}$. Let $O$ be the orbit matrix of $\mathcal{D}$ under action of the group $G$.

a) If $o = u$, then the binary linear code spanned by the rows of matrix $[I_m, O]$ is a self-orthogonal code of length $m + \frac{w}{w'}$ and dimension $m$. If $m = n$, the obtained code is self-dual.

b) If $o < u$, then the binary linear code spanned by the rows of matrix $O$ is a self-orthogonal code of length $\frac{w}{w'}$ and dimension $\text{rank}(O)$.

**Proof** In [5].

One can generalize previous theorem to construct a self-orthogonal code over $\mathbb{F}_q$, where $q$ is a prime power. The following theorem describes the construction.

**Theorem 15** Let $q$ be prime power and $\mathbb{F}_q$ a finite field of order $q$. Let $\mathcal{D}$ be $1-(v, k, r)$ design such that $k \equiv a (\text{mod } q)$ and $|B_i \cap B_j| \equiv 0 (\text{mod } q)$, for all $i, j \in \{1, \ldots, b\}$, $i \neq j$, where $B_i$ and $B_j$ are two blocks of the design $\mathcal{D}$, and let $G$ be an automorphism group of the design which acts on $\mathcal{D}$ with $n$ point orbits of length $w$ and $m$ block orbits of length $w$. Then the linear code spanned by the rows of matrix $A = [\sqrt{-a}I_m, O]$, where $O$ is the orbit matrix of the design $\mathcal{D}$ (under the action of the group $G$), is a self-orthogonal $[m + n, m]$ code over $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if $a$ is a square root modulo $q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise. If $m = n$, the obtained code is self-dual.

**Proof** From Remark 4 it follows that $O[s] \cdot O[t] \equiv 0 (\text{mod } q)$, and $O[s] \cdot O[s] \equiv a (\text{mod } q)$, so the rows of $A = [\sqrt{-a}I_m, O]$ generates self-orthogonal code. If $m = n$, the dimension of the code is half of its length, so the code is self-dual.

\[ \square \]

**Theorem 16** Let $\mathcal{D}$ be a weakly self-orthogonal $1-(v, k, r)$ design such that $k$ is odd and block intersection numbers are even. Let $G$ be an automorphism group of $\mathcal{D}$ acting with $f_1$ fixed points and $n$ point orbits of length 2, and with $f_2$ fixed blocks and $m$ block orbits of length 2. Then

1. the binary linear code spanned by the matrix $[I_{f_2}, OM1]$ is a binary self-orthogonal code of length $f_2 + f_1$ and dimension $f_2$;
2. the binary linear code spanned by the matrix $[I_m, OM2]$ is a self-orthogonal code of length $m + n$ and dimension $m$.

**Proof** In [5].

\[ \square \]
We generalize previous theorem to obtain self-orthogonal codes over \( \mathbb{F}_q \), where \( q \) is a prime power.

**Theorem 17** Let \( q \) be prime power and \( \mathbb{F}_q \) a finite field of order \( q \). Let \( D \) be an \( 1-(v,k,r) \) design such that \( k \equiv a \pmod{q} \) and \( |B_i \cap B_j| \equiv 0 \pmod{q} \), for all \( i, j \in \{1, \ldots, b\} \), \( i \neq j \), where \( B_i \) and \( B_j \) are two blocks of the design \( D \), and let \( G \) be an automorphism group of the design which acts on \( D \) with \( f_1 \) fixed points and \( n \) point orbits of length \( q \), and with \( f_2 \) fixed blocks and \( m \) block orbits of length \( q \). Then

1. the linear code spanned by the matrix \( [\sqrt{-a} \cdot I_2, OM] \) is a self-orthogonal \([f_2 + f_1, f_2]\) code over the field \( \mathbb{F} \), where \( \mathbb{F} = \mathbb{F}_q \) if \( a \) is square root in \( \mathbb{F}_q \), and \( \mathbb{F} = \mathbb{F}_q \) otherwise.
2. the linear code spanned by the matrix \( [\sqrt{-a} \cdot I_m, OM] \) is a self-orthogonal \([m + n, m]\) code over the field \( \mathbb{F} \), where \( \mathbb{F} = \mathbb{F}_q \) if \( a \) is square root in \( \mathbb{F}_q \), and \( \mathbb{F} = \mathbb{F}_q \) otherwise. If \( m = n \), the obtained code is self-dual.

**Proof** 1. Since \( k \equiv a \pmod{q} \), each block contains \( q \cdot \alpha + a \) fixed points and since \( |B_i \cap B_j| \equiv 0 \pmod{q} \), for all \( i, j \in \{1, \ldots, b\} \), \( i \neq j \), intersection of every two blocks contains \( q \cdot \beta \) fixed points. Therefore, it follows that the matrix \( [\sqrt{-a} \cdot I_m, OM] \) spans a self-orthogonal code of length \( f_2 + f_1 + 1 \) over the field \( \mathbb{F} \).

2. For \( s \neq t \), since \( B_i \) is block orbit of size \( q \), it follows from Remark 5 that

\[
\sum_{x' \in B_i} |x \cap x'| \equiv 0 \pmod{q},
\]

and for \( s = t \) it follows that

\[
\sum_{x' \in B_i} |x \cap x'| = |x \cap x| + \sum_{x' \in B_i, x \neq x'} |x \cap x'| \equiv a + 0 \pmod{q}.
\]

We conclude that \( OM_2[s] \cdot OM_2[t] \equiv 0 \pmod{q} \), for \( s \neq t \) and \( OM_2[s] \cdot OM_2[s] \equiv a \pmod{q} \) and that the binary code spanned by the matrix \( [\sqrt{-a} \cdot I_m, OM] \) is self-orthogonal over the field \( \mathbb{F} \).

\[ \square \]

### 3.4 Codes from orbit matrices of extended weakly self-orthogonal 1-designs with \( k \) odd and odd block intersection numbers

**Theorem 18** Let \( D \) be a weakly self-orthogonal 1-design such that \( k \) is odd and the block intersection numbers are odd and \( G \) be an automorphism group of the design which acts on \( D \) with \( n \) point orbits of length \( w \) and block orbits of length \( b_1, b_2, \ldots, b_m \) such that \( b_i = 2^u \cdot b'_i, w = 2^u \cdot w', o \leq u, 2 \nmid b'_i \) and \( 2 \nmid w' \), for \( i \in \{1, \ldots, m\} \). Let \( O \) be the orbit matrix of \( D \) under action of the group \( G \).

a) If \( o = u = 0 \), then the binary linear code spanned by the rows of the matrix \( [O, I] \) is a self-orthogonal code of the length \( \frac{v}{w} + 1 \) and dimension \( \text{rank}(O) \).

b) Otherwise, the binary linear code spanned by the rows of the matrix \( O \) is a self-orthogonal code of the length \( \frac{v}{w} \) and dimension \( \text{rank}(O) \).
Proof a) If \( o = u = 0 \), it follows from Remark 4 that
\[
\frac{b_t}{w} O[s] \cdot O[t] \equiv 1 \pmod{2}
\]
and
\[
\frac{b_s}{w} O[s] \cdot O[s] \equiv 1 \pmod{2}
\]
for all \( s, t \in \{1, \ldots, m\} \). Since \( w, b_1, \ldots, b_s \) are odd numbers, it follows that \( O[s] \cdot O[t] \equiv 1 \pmod{2} \) and \( O[s] \cdot O[s] \equiv 1 \pmod{2} \).

b) If \( o = u > 1 \), it follows Remark 4 that
\[
\frac{b'_t}{w'} O[s] \cdot O[t] \equiv 0 \pmod{2}
\]
for all \( s, t \in \{1, \ldots, m\} \). Since \( w', b'_1, \ldots, b'_s \) are odd numbers, it follows that \( O[s] \cdot O[t] \equiv 0 \pmod{2} \) and \( O[s] \cdot O[s] \equiv 0 \pmod{2} \).

If \( 1 < o < u \), it follows Remark 4 that
\[
\frac{b'_s}{2^{u-o} \cdot w'} O[s] \cdot O[t] \equiv 0 \pmod{2}
\]
for all \( s, t \in \{1, \ldots, m\} \) and since \( \frac{b'_s}{2^{u-o} \cdot w'} O[s] \cdot O[t] \) has to be a positive integer, it follows that \( O[s] \cdot O[t] \equiv 0 \pmod{2} \) and \( O[s] \cdot O[s] \equiv 0 \pmod{2} \).

\( \square \)

One can generalize previous theorem to construct a self-orthogonal code over \( \mathbb{F}_q \), where \( q \) is a prime power. The following theorem describes the construction.

**Theorem 19** Let \( q \) be prime power and \( \mathbb{F}_q \) a finite field of order \( q \). Let \( D \) be a \((v, k, r)\) design such that \( k \equiv a \pmod{q} \) and \(|B_i \cap B_j| \equiv d \pmod{q} \), for all \( i, j \in \{1, \ldots, b\}, i \neq j \), where \( B_i \) and \( B_j \) are two blocks of the design \( D \), and let \( G \) be an automorphism group of the design which acts on \( D \) with \( n \) point orbits of length \( w \) and \( m \) block orbits of length \( w' \) and let \( O \) be the orbit matrix of \( D \) under action of the group \( G \).

- If \( a = d \) we differ two cases.
  a) If \( q \mid w \), then linear code spanned by the rows of the matrix \( O \) is a self-orthogonal \([m, \text{rank}(O)]\) code over the field \( \mathbb{F}_q \).
  b) If \( q \nmid w \), then linear code spanned by the rows of the matrix \( A = [O, \sqrt{-wdI}] \)
    is a self-orthogonal \([m + 1, \text{rank}(O)]\) code over the field \( \mathbb{F} \), where \( \mathbb{F} = \mathbb{F}_q \) if
    \(-a \) is square root in \( \mathbb{F}_q \), and \( \mathbb{F} = \mathbb{F}_q^2 \) otherwise.

- If \( a \neq d \), we differ three cases.
  a) If \( q \mid w \), then linear code spanned by the rows of the matrix \( A = [\sqrt{d - aI_m}, O] \)
    is a self-orthogonal \([m + n, m] \) code over the field \( \mathbb{F} \), where
\( \mathbb{F} = \mathbb{F}_q \) if \( d - a \) is square root in \( \mathbb{F}_q \), and \( \mathbb{F} = \mathbb{F}_{q^2} \) otherwise. If \( m = n \), the obtained code is self-dual.

b) If \( q \mid w - 1 \), then linear code spanned by the rows of the matrix \( A = [\sqrt{wd - aI_m}, O, \sqrt{-dw}I] \) is a self-orthogonal \([m + n + 1, m]\) code over the field \( \mathbb{F} \), where \( \mathbb{F} = \mathbb{F}_q \) if \( wd \) is square root in \( \mathbb{F}_q \), and \( \mathbb{F} = \mathbb{F}_{q^2} \) otherwise.

c) If \( q \not\mid w \) and \( q \not\mid w - 1 \), then binary linear code spanned by the rows of the matrix \( A = [\sqrt{d - aI_m}, O, \sqrt{-wd}I] \) is a self-orthogonal \([m + n + 1, m]\) code over the field \( \mathbb{F} \), where \( \mathbb{F} = \mathbb{F}_q \) if \( wd \) is square root in \( \mathbb{F}_q \), and \( \mathbb{F} = \mathbb{F}_{q^2} \) otherwise.

**Proof** – If \( a = d \), it follows form Remark 4 that \( O[s] \cdot O[t] \equiv dw \pmod{q} \), for \( s, t \in \{1, \ldots, m\} \). It is now easy to see that \( O \) generates self-orthogonal code if \( q \mid w \), and that \( A = [O, \sqrt{-dw}I] \) generates self-orthogonal code otherwise.

- If \( a \neq d \), it follows from Remark 4 that \( O[s] \cdot O[t] \equiv dw \pmod{q} \), for \( s \neq t \) and \( O[s] \cdot O[t] \equiv a - d + wd \pmod{q} \).

  a) If \( q \mid w \), then \( O[s] \cdot O[t] \equiv 0 \pmod{q} \), and \( O[s] \cdot O[t] \equiv a - d \pmod{q} \). The matrix \( [\sqrt{d - aI_m}, O] \) generates self-orthogonal \([m + n, m]\) code. If \( m = n \), dimension of the code is half of its length, so the code is self-dual.

  b) If \( q \mid w - 1 \), then \( O[s] \cdot O[t] \equiv wd \pmod{q} \), and \( O[s] \cdot O[t] \equiv a \pmod{q} \). The matrix \( [\sqrt{wd - aI_m}, O, \sqrt{-wd}I] \) generates self-orthogonal \([m + n + 1, m]\) code.

  c) If \( q \not\mid w \) and \( q \not\mid w - 1 \), then \( O[s] \cdot O[t] \equiv wd \pmod{q} \), and \( O[s] \cdot O[t] \equiv a - d + wd \pmod{q} \). The matrix \( [\sqrt{d - aI_m}, O, \sqrt{-wd}I] \) generates self-orthogonal \([m + n + 1, m]\) code. \( \Box \)

**Theorem 20** Let \( \mathcal{D} \) be a weakly self-orthogonal \( 1 - (v, k, r) \) design such that \( k \) is odd and block intersection numbers are odd. Let \( G \) be an automorphism group of \( \mathcal{D} \) acting with \( f_1 \) fixed points and \( n \) point orbits of length 2, and with \( f_2 \) fixed blocks and \( m \) block orbits of length 2. Then

1. the binary linear code spanned by the matrix \([OM1, I]\) is a self-orthogonal code of length \( f_1 + 1 \) and dimension \( \text{rank}(OM1) \),
2. the binary linear code spanned by the matrix \( OM2 \) is a self-orthogonal code of length \( n \) and dimension \( \text{rank}(OM2) \).

**Proof** 1. Since \( k \) is odd, each block contains odd number of fixed points and since block intersection numbers are odd, intersection of every two blocks contains odd number of fixed points. Therefore, it follows that the matrix \([OM1, I]\) spans a binary self-orthogonal code.

2. Let \( \mathcal{B}_s \) and \( \mathcal{B}_t \) be block orbits of size 2 under the action of the group \( G \) on the design. For \( s \neq t \), since \( \mathcal{B}_t \) is block orbit of size 2, it follows from Remark 5 that

\[
\sum_{x' \in \mathcal{B}_t} |x \cap x'| \equiv 2 \pmod{2} \equiv 0 \pmod{2},
\]
and for \( s = t \), it follows that
\[
\sum_{x' \in B_s} |x \cap x'| = |x \cap x| + \sum_{x' \in B_s, x \neq x'} |x \cap x'| \equiv 1 + 1 \pmod{2}.
\]

We conclude that \( \sum_{j = f_1 + 1}^{f_1 + n} a_i \alpha a_{i,j} \equiv 0 \pmod{2} \), for \( s \neq t \) and \( \sum_{j = f_1 + 1}^{f_1 + n} a_i \alpha a_{s,j} \equiv 0 \pmod{2} \) and that the binary code spanned by the matrix \( OM_2 \) is self-orthogonal.

\[\square\]

We generalize previous theorem to obtain self-orthogonal codes over \( \mathbb{F}_q \), where \( q \) is a prime power.

**Theorem 21** Let \( q \) be prime power and \( \mathbb{F}_q \) a finite field of order \( q \). Let \( \mathcal{D} \) be \( 1 - (v, k, r) \) design such that \( k \equiv a \pmod{q} \) and \(|B_i \cap B_j| \equiv d \pmod{q} \), for all \( i, j \in \{1, \ldots, b\}, i \neq j \), where \( B_i \) and \( B_j \) are two blocks of the design \( \mathcal{D} \), and let \( G \) be an automorphism group of the design which acts on \( \mathcal{D} \) with \( f_1 \) fixed points and \( n \) point orbits of length \( q \), and with \( f_2 \) fixed blocks and \( m \) block orbits of length \( q \).

Then

- If \( a = q \), we differ two cases.
  
  1. the linear code spanned by the matrix \( [OM_1, \sqrt{-a}I] \) is a self-orthogonal \([f_1 + 1, \text{rank}(OM1)]\) code over the field \( \mathbb{F} = \mathbb{F}_q \) if \( a \) is square root in \( \mathbb{F}_q \) and \( \mathbb{F} = \mathbb{F}_{q^2} \) otherwise.
  
  2. the linear code spanned by the matrix \( OM_2 \) is a self-orthogonal \([n, \text{rank}(OM2)]\) code of length over the field \( \mathbb{F}_q \).

- If \( a \neq q \), we differ two cases.
  
  1. the linear code spanned by the matrix \( [\sqrt{a - d} \cdot I_{f_2}, OM_1, \sqrt{-a}I] \) is a self-orthogonal \([f_2 + f_1 + 1, f_2]\) code over the field \( \mathbb{F} = \mathbb{F}_q \) if \( d \) is square root in \( \mathbb{F}_q \), and \( \mathbb{F} = \mathbb{F}_{q^2} \) otherwise.

  2. the linear code spanned by the matrix \( [\sqrt{a - d} \cdot I_m, OM_2] \) is a self-orthogonal \([m + n, m]\) code over the field \( \mathbb{F} = \mathbb{F}_q \) if \( d \) is square root in \( \mathbb{F}_q \), and \( \mathbb{F} = \mathbb{F}_{q^2} \) otherwise. If \( m = n \), the obtained code is self-dual.

**Proof** 1. Since \( k \equiv a \pmod{q} \), each block contains \( q \cdot \alpha + a \) fixed points and since \(|B_i \cap B_j| \equiv d \pmod{q} \), for all \( i, j \in \{1, \ldots, b\}, i \neq j \), intersection of every two blocks contains \( q \cdot \beta + d \) fixed points. Therefore, if \( a = d \), it follows that the matrix \( [OM_1, \sqrt{-a}I] \) spans a self-orthogonal \([f_1 + 1, \text{rank}(OM1)]\) code over the field \( \mathbb{F} \), and if \( a \neq d \), it follows that the matrix \( [\sqrt{d - a} \cdot I_{f_2}, OM_1, \sqrt{-a}I] \) spans a self-orthogonal \([f_2 + f_1 + 1, f_2]\) code over the field \( \mathbb{F} \).

2. For \( s \neq t \), since \( B_t \) is block orbit of size \( q \), it follows from Remark 5 that
\[
\sum_{x' \in B_t} |x \cap x'| \equiv qd \pmod{q} \equiv 0 \pmod{q}.
\]
and for $s = t$ it follows that

$$
\sum_{x' \in B_s} |x \cap x'| = |x \cap x| + \sum_{x' \in B_s, x' \neq x'} |x \cap x'| \equiv a + (q - 1)d \pmod{q}.
$$

It follows that $OM_2[s] \cdot OM_2[t] \equiv 0 \pmod{q}$, for $s \neq t$ and $OM_2[s] \cdot OM_2[s] \equiv a - d \pmod{q}$. If $a = d$, then the code spanned by the matrix $OM_2$ is self-orthogonal $[n, \text{rank}(OM_2)]$ code over $\mathbb{F}_q$, and if $a \neq d$, it follows that the code spanned by the matrix $[\sqrt{d - a \cdot I_m}, OM_2]$ is self-orthogonal $[nm + n, n]$ code over the field $\mathbb{F}$. If $m = n$, dimension of the code is half of its length, so the code is self-dual. 

\[\Box\]

### 4 Results

**Theorem 22** Let $G$ be a finite permutation group acting transitively on the set $\Omega$ of size $n$. Let $\alpha \in \Omega$ and $\Delta = \bigcup_{i=1}^{s} \delta_i G_\alpha$, where $\delta_1, \ldots, \delta_s \in \Omega$ are representatives of distinct $G_\alpha$-orbits. If $\Delta \neq \Omega$ and

$$
B = \{ \Delta g \mid g \in G \},
$$

then $D = (\Omega, B)$ is $1 - (n, |\Delta|, \frac{|G_\alpha|}{|G_\alpha| \sum_{i=1}^{n} |\alpha G_{\delta_i}|})$ design with $\frac{m|G_\alpha|}{|G_\alpha|}$ blocks.

**Proof** In [6]. \[\Box\]

Using this construction, we constructed 178 pairwise non-isomorphic weakly self-orthogonal 1-designs on 22, 55, 66, 110, 132, 144 and 165 points invariant under an action of $M_{11}$. Precisely, 4 designs on 22 points, 2 designs on 55 points, 6 designs on 66 points, 41 designs on 110 points, 76 designs on 132 points, 26 designs on 144 points and 20 designs on 165 points.

Using constructed designs, we obtained at least 217 non-equivalent binary self-orthogonal codes. We present tables with optimal, near-optimal and best known obtained codes. Optimal codes are denoted with $\ast$, best known codes are denoted with $\ast\ast$, and near-optimal codes are denoted with $\dagger$.

Tables will be ordered by four cases of weakly self-orthogonal designs.

Case 1. Codes obtained from self-orthogonal designs.
Case 2. Codes obtained from weakly self-orthogonal designs such that block sizes are even and block intersection numbers are odd.
Case 3. Codes obtained from weakly self-orthogonal designs such that block sizes are odd and block intersection numbers are even.
Case 4. Codes obtained from weakly self-orthogonal designs such that block sizes are odd and block intersection numbers are odd.

Using Theorems 6, 10, 14 and 18, we constructed binary self-orthogonal codes from the orbit matrices of the non-trivial weakly self-orthogonal 1-designs on less than 165 points (including). In order to construct the orbit matrices we determined orbits of all cyclic subgroups of prime order of the group $M_{11}$ acting with orbits of the same length.
Table 1  Non-trivial binary pairwise non-equivalent self-orthogonal codes obtained from the orbit matrices of the non-trivial self-orthogonal 1-designs

| C                  | AutC or #AutC                   | Design          | Theorem |
|--------------------|---------------------------------|-----------------|---------|
| [10, 4, 4]*        | $Z_2 \times (E_24 : S_5)$       | 1 – (110, 72, 36) | 6 (Case 1) |
| [12, 5, 4]*        | $(E_{25} : A_6) : (Z_2 \times Z_2)$ | 1 – (132, 40, 40) | 6 (Case 1) |
| [12, 5, 4]*        | $E_{24} : S_5$                  | 1 – (132, 46, 46) | 6 (Case 1) |
| [15, 4, 8]*        | $A_8$                           | 1 – (165, 48, 48) | 6 (Case 1) |
| [31, 15, 8]*       | $PSL(5, 2)$                     | 1 – (165, 116, 116) | 10 (Case 2) |
| [12, 6, 4]*        | $E_{25} : S_6$                  | 1 – (66, 21, 21) | 14 (Case 3) |
| [24, 12, 8]*       | $M_{24}$                        | 1 – (132, 27, 27) | 14 (Case 3) |
| [96, 48, 16] **    | $D_{12}$                        | 1 – (144, 23, 23) | 14 (Case 3) |
| [16, 5, 8]*        | $E_{24} : A_8$                  | 1 – (165, 109, 109) | 18 (Case 4) |

Table 2  Non-trivial binary pairwise non-equivalent self-orthogonal codes obtained from the orbit matrices of the non-trivial self-orthogonal 1-designs

| C                  | AutC or #AutC                   | Design          | Theorem |
|--------------------|---------------------------------|-----------------|---------|
| [6, 2, 4]*         | $Z_2 \times S_4$               | 1 – (22, 10, 10) | 8 (Case 1) |
| [6, 3, 2]+         | $Z_2 \times S_4$               | 1 – (22, 2, 1)  | 8 (Case 1) |
| [10, 3, 4]+        | $Z_2 \times S_4 \times S_4$    | 1 – (66, 46, 46) | 8 (Case 1) |
| [14, 6, 4]+        | $Z_2 \times (E_{26} : S_7)$    | 1 – (110, 72, 72) | 8 (Case 1) |
| [12, 3, 6]*        | $(((Z_2 \times (E_{24} : Z_2)) : Z_2) : Z_2)$ | 1 – (132, 66, 6) | 8 (Case 1) |
| [12, 2, 8]*        | $(((Z_2 \times (E_{24} : Z_2)) : Z_2) : Z_2)$ | 1 – (132, 100, 100) | 8 (Case 1) |
| [64, 4, 32]+       | 1139927356332115625068462080   | 1 – (132, 55, 5) | 16 (Case 3) |

Optimal, near-optimal and best known codes constructed using Theorems 6,10,14 and 18 are shown in Table 1.

Using Theorem 8 and Theorem 16, we constructed binary self-orthogonal codes from the orbit matrices of the non-trivial weakly self-orthogonal 1-designs on less than 165 points (including). In order to construct the orbit matrices we determined orbits of cyclic subgroup $Z_2$ of the group $M_{11}$ acting with orbits of lengths 1 and 2. Optimal, near-optimal and best known codes constructed using Theorems 8 and 16 are shown in Table 2.

References

1. Assmus, E.F., Key, J.D.: Designs and their codes. Cambridge University Press, Cambridge (1992)
2. Baartmans, A., Landjev, I., Tonchev, V.D.: On the binary codes of Steiner triple systems. Des. Codes Cryptogr. 8, 29–43 (1996)
3. Chigira, N., Harada, M., Kitazume, M.: Permutation groups and binary selforthogonal codes. J. Algebra 309, 610–621 (2007)
4. Crnković, D., Egan, R., Švob, A.: Constructing self-orthogonal and Hermitian self-orthogonal codes via weighing matrices and orbit matrices. Finite Fields Appl. 55, 64–77 (2019)
5. Crnković, D., Mikulić Crnković, V., Rodrigues, B.G.: On self-orthogonal designs and codes related to Held’s simple group. Adv. Math. Commun. 12, 607–628 (2018)
6. Crnković, D., Mikulić Crnković, V., Švob, A.: On some transitive combinatorial structures constructed from the unitary group $U(3, 3)$. J. Statist. Plann. Inference 144, 19–40 (2014)
7. Crnković, D., Mostarac, N.: Self-dual codes from orbit matrices and quotient matrices of combinatorial designs. Dis. Math. 341, 3331–3343 (2018)
8. Crnković, D., Rodrigues, B.G., Simčić, L., Rukavina, S.: Self-orthogonal codes from orbit matrices of 2-designs. Adv. Math. Commun. 7, 161–174 (2013)
9. Crnković, D., Rukavina, S.: Self-dual codes from extended orbit matrices of symmetric designs. Des. Codes Cryptogr. 79, 113–120 (2016)
10. Crnković, D., Dumičić Danilović, D., Rukavina, S.: On symmetric (78,22,6) designs and related self-orthogonal codes. Util. Math. 109, 227–253 (2018)
11. Harada, M., Tonchev, V.D.: Self-orthogonal codes from symmetric designs with fixed-point-free automorphisms. Dis. Math. 264, 81–90 (2003)
12. Tonchev, V.: Self-orthogonal designs and extremal doubly-even codes. J. Combin. Theory, Ser A 52, 197–205 (1989)
13. Tonchev, V.D.: Quantum codes from finite geometry and combinatorial designs. Finite Groups Vertex Oper Algebras Combinat Res Inst Math Sci 1656, 44–54 (2009)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.