On some self-orthogonal codes from M_{11}

Ivona Novak
(inovak@math.uniri.hr)
joint work with Vedrana Mikulić Crnković
(vmikulic@math.uniri.hr)

Department of Mathematics, University of Rijeka

Finite Geometry & Friends,
A Brussels Summer School on Finite Geometry

This work has been supported by Croatian Science Foundation under the project 6732 and by the University of Rijeka under the project number uniri-prirod-18-111-1249.

Weakly self-orthogonal designs from M_{11}

Codes from M_{11}

Codes from orbit matrices of weakly q-self-orthogonal 1-designs

V. Tonchev, Self-Orthogonal Designs and Extremal Doubtly-Even Codes, Journal of Combinatorial Theory, Series A 52, 197-205 (1989).

D. Crnković, V. Mikulić Crnković, A. Svob, On some transitive combinatorial structures constructed from the unitary group $U(3,3)$, J. Statist. Plann. Inference 144 (2014), 19-40.

D. Crnković, V. Mikulić Crnković, B.G. Rodrigues, On self-orthogonal designs and codes related to Held's simple group, Advances in Mathematics of Communications 607-628 (2018).

UNIVERSITY OF RIJEKA
DEPARTMENT OF MATHEMATICS

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. Subgroup of M_{11} with largest index has index 3960.

Using mentioned subgroups we obtained transitive permutation representations of M_{11} on $22, 55, 66, 110, 132, 144$ and 165 points.

Weakly self-orthogonal designs

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 called a $t-(v,k,\lambda)$ design, if $\mathcal{P}$ contains v points, every block $B \in \mathcal{B}$ is incident with k points, and every t distinct points are incident with λ blocks.

The incidence matrix of a design is a $b \times v$ matrix $[m_{ij}]$ where b and v are the numbers of blocks and points respectively, such that $m_{ij} = 1$ if the point P_j and the block B_i are incident, and $m_{ij} = 0$ otherwise.

A design is weakly q-self-orthogonal if all the block intersection numbers gives the same residue modulo q.
A weakly q-self-orthogonal design is q-self-orthogonal if the block intersection numbers and the block sizes are multiples of q.

Specially, weakly 2-self-orthogonal design is called weakly self-orthogonal design, and 2-self-orthogonal design is called self-orthogonal.

UNIVERSITY OF RIJEKA
DEPARTMENT OF MATHEMATICS

Construction

Theorem ([2])

Let G be a finite permutation group acting transitively on the sets Ω_1 and Ω_2 of size m and n, respectively. Let $\alpha \in \Omega_1$ and $\Delta_2 = \bigcup_{i=1}^{s} \delta_i G_\alpha$, where $\delta_i, \ldots, \delta_s \in \Omega_2$ are representatives of distinct G_α-orbits. If $\Delta_2 \neq \Omega_2$ and

$$\mathcal{B} = \{\Delta_2 g \mid g \in G\},$$

then $\mathcal{D} = (\Omega_2, \mathcal{B})$ is $1 - (n, |\Delta_2|, \frac{|G_\alpha|}{|G_{\Delta_2}|} \sum_{i=1}^{n} |\alpha G_{\delta_i}|)$ design with $\frac{m \cdot |G_\alpha|}{|G_{\Delta_2}|}$ blocks.

Using mentioned construction for transitive permutation representations of M_{11}, we constructed 169 non-isomorphic weakly self-orthogonal designs:

- 6 designs on 66 points,
- 41 designs on 110 points,
- 76 designs on 132 points,
- 26 designs on 144 points,
- 20 designs on 165 points.

Two of constructed designs are 2-designs: $2 - (144, 66, 30)$ and its complement.

Codes from weakly self-orthogonal designs

Theorem ([1])

Let $\mathcal{D}$ be weakly self-orthogonal design and let M be it's $b \times v$ incidence matrix.

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

Codes from weakly q-self-orthogonal designs

Theorem

Let q be prime power and $\mathbb{F}_q$ a finite field of order q. Let $\mathcal{D}$ be a weakly q-self-orthogonal 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 a design $\mathcal{D}$. Let M be it's $b \times v$ incidence matrix.

- *If $\mathcal{D}$ is q self-orthogonal design, then M generates a self-orthogonal code over $\mathbb{F}_q$.*
- *If $a = 0$ and $d \neq 0$, then the matrix $[\sqrt{d} \cdot I_b, M, \sqrt{-d} \cdot \mathbf{1}]$ generates a self-orthogonal code over $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if $-d$ is a square in $\mathbb{F}_q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise.*
- *If $a \neq 0$ and $d = 0$, then the matrix $[M, \sqrt{-a} \cdot I_b]$ generates a self-orthogonal code over $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if $-a$ is a square in $\mathbb{F}_q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise.*
- *If $a \neq 0$ and $d \neq 0$, there are two cases:*
  1. *if $a = d$, then the matrix $[M, \sqrt{-d} \cdot \mathbf{1}]$ generates a self-orthogonal code over $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if $-a$ is a square in $\mathbb{F}_q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise, and*
  2. *if $a \neq d$, then the matrix $[\sqrt{d - a} \cdot I_b, M, \sqrt{-d} \cdot \mathbf{1}]$ generates a self-orthogonal code over $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if $-d$ is a square in $\mathbb{F}_q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise.*

Some results...

From permutation representations of M_{11} on less than 165 points (inclusive), from incidence matrices of weakly self-orthogonal designs we constructed at least 70 non-equivalent non-trivial binary self-orthogonal codes:

- 6 codes from M_{11} on 66 points,
- 14 or more codes from M_{11} on 110 points,
- 37 or more codes from M_{11} on 132 points,
- 3 or more codes from M_{11} on 144 points,
- 10 or more codes from M_{11} on 165 points.

Orbit matrices

Let $\mathcal{D}$ be a $1-(v,k,\lambda)$ design and G be an automorphism group of the design. Let $v_1 = |\mathcal{V}_1|, \dots, v_n = |\mathcal{V}_n|$ be the sizes of point orbits and $b_1 = |\mathcal{B}_1|, \dots, b_m = |\mathcal{B}_m|$ be the sizes of block orbits under the action of the group G. We define an orbit matrix as $m \times n$ matrix:

$$O = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix},$$

where a_{ij} is the number of points of the orbit $\mathcal{V}_j$ incident with a block of the orbit $\mathcal{B}_i$. It is easy to see that the matrix is well-defined and that $k = \sum_{j=1}^{n} a_{ij}$.

For $x \in \mathcal{B}_s$, by counting the incidence pairs (P, x') such that $x' \in \mathcal{B}_t$ and P is incident with the block x, we obtain

$$\sum_{x' \in \mathcal{B}_t} |x \cap x'| = \sum_{j=1}^{m} \frac{b_t}{v_j} a_{sj} a_{tj}.$$

UNIVERSITY OF RIJEKA
DEPARTMENT OF MATHEMATICS

Let $\mathcal{D}$ be a weakly q-self-orthogonal design such that

$$k \equiv a \pmod{q}$$

and

$$|B_i \cap B_j| \equiv d \pmod{q},$$

for all $i, j \in \{1, \dots, b\}$, $i \neq j$, where B_i and B_j are two blocks of a design $\mathcal{D}$.
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 $b_1, b_2, \dots, b_m$, and let O be an orbit matrix of a design $\mathcal{D}$ under the action of a group G.
For $x \in \mathcal{B}_s$ and $s \neq t$ it follows that

$$\frac{b_t}{w} O[s] \cdot O[t] \equiv b_t d \pmod{q}, \qquad (1)$$

$$\frac{b_s}{w} O[s] \cdot O[s] \equiv a + (b_s - 1)d \pmod{q}. \qquad (2)$$

Codes from orbit matrices of q-self-orthogonal 1-designs

Theorem ([3])

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 $b_i = 2^o \cdot b_i'$, $w = 2^u \cdot w'$, $o \leqslant u, 2 \nmid b_i', w'$, 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 $\frac{v}{w}$.

Theorem

Let q be prime power and $\mathbb{F}_q$ a finite field of order p.
Let $\mathcal{D}$ be a q self-orthogonal 1-design 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 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 $\frac{v}{w}$.

UNIVERSITY OF RIJEKA
DEPARTMENT OF MATHEMATICS

Case 2

Theorem

Let $\mathcal{D}$ be a weakly self-orthogonal 1-design such that k is even and the block intersection numbers are odd 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 $b_1, b_2, \dots, b_m$ such that $b_i = 2^o \cdot b_i'$, $w = 2^u \cdot w'$, $o \leqslant u, 2 \nmid b_i', w'$ for $i \in \{1, \dots, m\}$. Let O be the orbit matrix of $\mathcal{D}$ under action of a group G.

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

b) *If $o \geqslant 1$ and $o = u$ then the binary linear code spanned by the rows of the matrix $[I_m, O, \mathbf{1}]$ is a self-orthogonal code of the length $m + \frac{v}{w} + 1$.*

b) *If $o < u$, then binary linear code spanned by the rows of the matrix O is a self-orthogonal code of the length $\frac{v}{w}$.*

Case 2 (over $\mathbb{F}_q$)

Theorem

Let q be prime power and $\mathbb{F}_q$ a finite field of order p.
Let $\mathcal{D}$ be a weakly q-self-orthogonal 1-design such that $k \equiv 0 \pmod{q}$ and $|B_i \cap B_j| \equiv d \pmod{q}$, for all $i, j \in \{1, \dots, b\}$, $i \neq j$, where B_i and B_j are two blocks of a 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 a group G.

a) *If $p \mid w$, then linear code spanned by the rows of the matrix $[\sqrt{-d} I_m, O]$ is a self-orthogonal code over the field $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if d is a square in $\mathbb{F}_q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise.*
b) *If $p \mid w - 1$, then linear code spanned by the rows of the matrix $[\sqrt{wd} I_m, O, \sqrt{-wd}\mathbf{1}]$ is a self-orthogonal code over the field $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if wd is a square in $\mathbb{F}_q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise.*
c) *If $p \nmid w$ and $p \nmid w - 1$, then linear code spanned by the rows of the matrix $[\sqrt{wd - (w-1)d} I_m, O, \sqrt{-wd}\mathbf{1}]$ is a self-orthogonal code over the field $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if $-wd$ is a square in $\mathbb{F}_q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise.*

UNIVERSITY OF RIJEKA
DEPARTMENT OF MATHEMATICS

Case 3

Theorem ([3])

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 $b_1, b_2, \dots, b_m$ such that $b_i = 2^o \cdot b_i',\ w = 2^u \cdot w',\ o \leqslant u, 2 \nmid b_i', w'$, for $i \in \{1, \dots, m\}$. Let O be the orbit matrix of $\mathcal{D}$ under action of a group G.

a) *If $o = u$, then he binary linear code spanned by the rows of matrix $[I_m, O]$ is a self-orthogonal code of length $m + \frac{v}{w}$.*
b) *If $o < u$, then he binary linear code spanned by the rows of matrix O is a self-orthogonal code of length $\frac{v}{w}$.*

Theorem

Let q be prime power and $\mathbb{F}_q$ a finite field of order p.
Let $\mathcal{D}$ be a weakly q-self-orthogonal design such that $k \equiv a \pmod{q}$ and block intersection numbers are multiples of q, 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 $[\sqrt{-a} I_m, O]$, where O is orbit matrix of the design $\mathcal{D}$ (under the action of the group G), is a self-orthogonal code over $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if a is a square in $\mathbb{F}_q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise.

Case 4

Theorem

Let $\mathcal{D}$ 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 $\mathcal{D}$ with n point orbits of length w and block orbits of length $b_1, b_2, \ldots, b_m$ such that $b_i = 2^o \cdot b_i'$, $w = 2^u \cdot w'$, $o \leqslant u, 2 \nmid b_i', w'$, for $i \in \{1, \ldots, m\}$. Let O be the orbit matrix of $\mathcal{D}$ under action of a group G.

a) *If $o = u = 0$, then the binary linear code spanned by the rows of the matrix $[O, \mathbf{1}]$ is a self-orthogonal code of the length $\frac{v}{w} + 1$.*
b) *Otherwise, the binary linear code spanned by the rows of the matrix O is a self-orthogonal code of the length $\frac{v}{w}$.*

UNIVERSITY OF RIJEKA
DEPARTMENT OF MATHEMATICS

Theorem

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 $k \equiv a \pmod{q}$ and $|B_i \cap B_j| \equiv d \pmod{q}$, for all $i,j \in \{1,\dots,b\}$, $i \neq j$, where B_i and B_j are two blocks of a 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 a group G.

- *If $a = d$ we differ two cases.*
  a) *If $p \mid w$, then linear code spanned by the rows of the matrix O is a self-orthogonal code over the field $\mathbb{F}_q$.*
  b) *If $p \nmid w$, then linear code spanned by the rows of the matrix $[\sqrt{-a}I_m, O]$ is a self-orthogonal 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 $p \mid w$, then linear code spanned by the rows of the matrix $[\sqrt{d-a}I_m, O]$ is a self-orthogonal 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.*
  b) *If $p \mid w-1$, then linear code spanned by the rows of the matrix $[\sqrt{wd-a}I_m, O, \sqrt{-wd}\mathbf{1}]$ is a self-orthogonal 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 $p \nmid w$ and $p \nmid w-1$, then binary linear code spanned by the rows of the matrix $[\sqrt{d-a}I_m, O, \sqrt{-wd}\mathbf{1}]$ is a self-orthogonal 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.*

Some results...

From permutation representations of M_{11} on less than 165 points (inclusive), from orbit matrices we constructed at least 87 non-equivalent non-trivial binary self-orthogonal codes:

- 2 codes from M_{11} on 66 points,
- 22 codes from M_{11} on 110 points,
- 21 codes from M_{11} on 132 points,
- 24 or more codes from M_{11} on 144 points,
- 18 or more codes from M_{11} on 165 points.

8 of constructed codes are optimal: $[10, 4, 4], [12, 5, 4](2), [12, 6, 4], [12, 11, 2], [16, 5, 8], [24, 12, 8], [31, 15, 8]$ and one of them is best known: $[96, 48, 16]$.

UNIVERSITY OF RIJEKA
DEPARTMENT OF MATHEMATICS

Thank you for your attention!