SELF-ORTHOGONAL DESIGNS AND CODES FROM HELD'S GROUP

UNIVERSITY OF RIJEKA DEPARTMENT OF MATHEMATICS

DEAN CRNKOVIĆ, **VEDRANA MIKULIĆ CRNKOVIĆ**, AND BERNARDO G. RODRIGUES

UNIVERSITY OF RIJEKA DEPARTMENT OF MATHEMATICS

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

THE INTRODUCTION

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,λ) **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 λ blocks.

A t-(v,k,λ) 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.

Let $\mathcal{D}$ be a 1-design and G be an automorphism group of the design acting on the set of points with the orbits $\mathcal{V}_1, \ldots, \mathcal{V}_n$ and on the set of blocks with the orbits $\mathcal{B}_1, \ldots, \mathcal{B}_m$. Denote by $a_{i,j}$ the number of points of the orbit $\mathcal{V}_j$ incident with a block of the orbit $\mathcal{B}_i$. The **orbit matrix** of the design $\mathcal{D}$ is the matrix

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

The **code** $C(\mathcal{D})$ **of the design** $\mathcal{D}$ over the finite field $\mathbf{F}$ is the space spanned by the incidence vectors of the blocks over $\mathbf{F}$.

If $\mathcal{D}$ is a self-orthogonal design, then $C_{\mathbb{F}_2}(\mathcal{D})$ is self-orthogonal code. If $\mathcal{D}$ is such that k is odd and the block intersection numbers are even, then the matrix $[I_b, M]$, where M is the incidence matrix of $\mathcal{D}$, generate a binary self-orthogonal code. If $\mathcal{D}$ is such that k is odd and the block intersection numbers are odd, then the matrix $[M, \mathbf{1}]$ generate a binary self-orthogonal code. If $\mathcal{D}$ is such that k is even and the block intersection numbers are odd, then the matrix $[I_b, M, \mathbf{1}]$ generate a binary self-orthogonal code.

CODES FROM ORBIT MATRICES

There exists a cyclic subgroup G of order 3 of the group He acting on the set $\{1,2,\ldots,2058\}$ with orbits of length 3, a cyclic subgroup G of order 7 of the group He acting on the set $\{1,2,\ldots,2058\}$ with orbits of length 7, a cyclic subgroup G of order 7 of the group He acting on the set $\{1,2,\ldots,8330\}$ with orbits of length 7 and a cyclic subgroup G of order 17 of the group He acting on the set $\{1,2,\ldots,8330\}$ with orbits of length 17.

Self-orthogonal codes constructed from orbit matrices of self-orthogonal 1-designs invariant under the action of He

$[294,111]$	$[294,110]$	$[980,47]$	$[980,46]$
$[294,10]$	$[294,6]$	$[980,41]$	$[980,40]$
$[294,93]$	$[294,98]$	$[980,44]$	$[980,43]$
$[294,101]$	$[294,105]$	$[980,3]$	$[980,4]$
$[294,18]$	$[294,13]$	$[980,6]$	$[980,7]$
$[686,261]$	$[686,260]$	$[2380,111]$	$[2380,110]$
$[686,18]$	$[686,17]$	$[2380,99]$	$[2380,98]$
$[686,227]$	$[686,226]$	$[2380,105]$	$[2380,104]$
$[686,243]$	$[686,244]$	$[2380,6]$	$[2380,7]$
$[686,34]$	$[686,35]$	$[2380,12]$	$[2380,13]$
$[294,104]$	$[294,105]$	$[490,43]$	$[490,44]$
$[294,7]$	$[294,6]$	$[490,4]$	$[490,3]$
$[294,98]$	$[294,99]$	$[490,40]$	$[490,41]$
$[294,13]$	$[294,12]$	$[490,7]$	$[490,6]$
$[294,111]$	$[294,110]$	$[490,47]$	$[490,46]$
$[686,243]$	$[686,244]$	$[1190,101]$	$[1190,102]$
$[686,18]$	$[686,17]$	$[1190,10]$	$[1190,9]$
$[686,226]$	$[686,227]$	$[1190,92]$	$[1190,93]$
$[686,35]$	$[686,34]$	$[1190,19]$	$[1190,18]$
$[686,261]$	$[686,260]$	$[1190,111]$	$[1190,110]$

We constructed weakly self-orthogonal 1-designs invariant under the action of He such that k is odd and the block intersection numbers are even.

From the orbit matrices of the extension of those 1-designs we constructed: 6 self-orthogonal binary codes with parameters $[980,490]$, 6 self-orthogonal binary codes with parameters $[2380,1190]$, 4 self-orthogonal binary codes with parameters $[1484,294]$, 4 self-orthogonal binary codes with parameters $[612,122]$.

THE CONSTRUCTIONS

D. Crnković, V. Mikulić Crnković: Unitals, projective planes and other combinatorial structures constructed from the unitary groups $U(3,q)$, $q = 3,4,5,7$, Ars Combin. 110 (2013), pp. 3-13

- Let G be a finite permutation group acting primitively 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 $\delta_1, \ldots, \delta_s \in \Omega_2$ are representatives of distinct G_α-orbits. If $\Delta_2 \neq \Omega_2$ and $\mathcal{B} = \{\Delta_2 g : g \in G\}$, then $(\Omega_2, \mathcal{B})$ is a $1-(n, |\Delta_2|, \sum_{i=1}^{s} |\alpha G_{\delta_i}|)$ design with m blocks, and G acts as an automorphism group, primitively on points and blocks of the design.

D. Crnković, V. Mikulić Crnković, B. G. Rodrigues: On self-orthogonal designs and codes related to Held's simple group, submitted

- Let $\mathcal{D}$ be a self-orthogonal 1-(v,k,r) design and G be an automorphism group of the design acting on $\mathcal{D}$ with n point orbits of length w and block orbits of lengths $b_1, \ldots, b_m$ such that $\frac{b_i}{w}$ is odd number for $i \in \{1, \ldots, m\}$. Then the binary linear code generated by the orbit matrix of the design $\mathcal{D}$ (under the action of the group G) is a self-orthogonal code of length $\frac{v}{w}$.
- Let $\mathcal{D}$ be a weakly self-orthogonal 1-(v,k,r) design such that k is odd and the block intersection numbers are even. 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 lengths $b_1, \ldots, b_m$ such that $\frac{b_i}{w}$ is odd number for $i \in \{1, \ldots, m\}$. Let the matrix A be the orbit matrix of the design under that action. Then the matrix $[I_m, A]$ generates a binary self-orthogonal linear code of length $m + \frac{v}{w}$.

1-DESIGNS CONSTRUCTED FROM THE SIMPLE GROUP He

- Let G be the sporadic simple group He, and Ω the primitive G-set of size 2058 defined by the action on the cosets of $S_4(4){:}2$. Let $\omega \in \Omega$, and $\Delta = \bigcup_{j=1}^{l} \Omega_{i_j}$, $1 \leq l \leq 4$, be a union of $(S_4(4){:}2)$-orbits. Let $\mathcal{B} = \{\Delta^g : g \in G\}$, and $\mathcal{D}_k = (\Omega, \mathcal{B})$ with $k = |\Delta|$. Further, define the sets M and N such that $M = \{136, 137, 561, 562\}$ and $N = \{272, 273, 425, 426, 697, 698\}$. Then the following hold:
(a) $\mathcal{D}_k$ is a primitive symmetric 1-$(2058, |\Delta|, |\Delta|)$ design.
(b) If $k \in M$ then $\mathrm{Aut}\mathcal{D}_k \cong \mathrm{He}$, and if $k \in N$ then $\mathrm{Aut}\mathcal{D}_k \cong \mathrm{He}{:}2$.
(c) If k is even then $\mathcal{D}_k$ and $\bar{\mathcal{D}}_k$ are self-orthogonal designs.
- Let Δ be a union of some $2^2 {}^{\cdot} L_3(4){:}S_3$-orbits of the set $\{1, \ldots, 8330\}$ such that $1 < |\Delta| \leq 4165$. Then $\mathcal{B} = \{\Delta^g : g \in G\}$ is a set of blocks of a symmetric design $\mathcal{D}'_{|\Delta|}$ with parameters 1-$(8330, |\Delta|, |\Delta|)$ having He acting primitively as the automorphism group. Up to isomorphism, there are 46 symmetric 1-designs on 8330 points admitting He as a primitive automorphism group. Of these 30 have $\mathrm{He} : 2$ acting as the full automorphism group and 16 have He acting as the full automorphism group.
- Let Δ be a union of some S_1-orbits on the set $\{1, \ldots, 2058\}$ such that $1 < |\Delta| \leq 1028$ and $S_1 \cong 2^2 {}^{\cdot} L_3(4){:}S_3$. Then $\mathcal{B} = \{\Delta^g : g \in G\}$ is a set of blocks of a 1-design $\mathcal{D}''_{|\Delta|}$ on 2058 points with $b = 8330$ admitting He as a primitive automorphism group. Up to isomorphism, there are nine 1-designs on 2058 points with 8330 blocks having He acting primitively as automorphism group. Three of these have He:2 acting as the full automorphism group and six have He acting as the full automorphism group.

Weakly self-orthogonal 1-designs invariant under the action of the group He

$\mathcal{S}$	Aut$\mathcal{S}$	$\mathcal{S}$	Aut$\mathcal{S}$	$\mathcal{S}$	Aut$\mathcal{S}$	$\mathcal{S}$	Aut$\mathcal{S}$
1-$(2058, 426, 426)$	He:2	1-$(8330, 1450, 1450)$	He:2	1-$(2058, 840, 3400)$	He	1-$(8330, 1681, 1681)$	He:2
1-$(2058, 562, 562)$	He	1-$(8330, 3130, 3130)$	He:2	1-$(2058, 882, 3570)$	He	1-$(8330, 1449, 1449)$	He:2
1-$(2058, 698, 698)$	He:2	1-$(8330, 1666, 1666)$	He	1-$(2058, 336, 1360)$	He:2	1-$(8330, 3129, 3129)$	He:2
1-$(2058, 562, 562)$	He	1-$(8330, 2904, 2904)$	He	1-$(2058, 378, 1530)$	He:2		
1-$(2058, 272, 272)$	He:2	1-$(8330, 1680, 1680)$	He:2	1-$(2058, 42, 170)$	He:2		

SELF-ORTHOGONAL CODES CONSTRUCTED FROM THE SIMPLE GROUP He

- Let C_k and $\bar{C}_k$ denote the binary codes defined by the row span of the incidence matrices of $\mathcal{D}_k$ (respectively $\bar{\mathcal{D}}_k$). Then the following hold:
(i) If k is odd then $C_k = \bar{C}_k = V_{2058}(\mathbf{F}_2)$.
(ii) If $k \in \{136, 272, 1360, 1496, 1632\}$ then $\bar{C}_k = C_k \oplus \mathbf{1}$ is a decomposable self-orthogonal code.
- Let C'_k and $\bar{C}'_k$ denote the binary codes of length 8330 defined by the row span of the incidence matrices of $\mathcal{D}'_k$ (respectively $\bar{\mathcal{D}}'_k$). If $k \in \{1450, 1666, 1680, 2904, 3130\}$, then C'_k and $\bar{C}'_k$ are self-orthogonal codes invariant under the action of He.
- Let C''_k and $\bar{C}''_k$ denote the binary codes of length 2058 defined by the row span of the incidence matrices of $\mathcal{D}''_i$ with blocks of size k (respectively $\bar{\mathcal{D}}''_i$). Then the following hold:
(i) If k is odd, then $C''_k = \bar{C}''_k = V_{2058}(\mathbf{F}_2)$.
(ii) If k is even, then C''_k and $\bar{C}''_k$ are non-trivial self-orthogonal codes.
(iii) If k is even, then ${C''_k}^t$ and ${\bar{C}''_k}{}^t$ (codes of the dual designs and their complementary designs) are self-orthogonal codes of length 8330.

Binary self-orthogonal codes invariant under the action of the group He

C	$\bar{C}$	C'	$\bar{C}'$	C''	$\bar{C}''$	C''^t	$\bar{C}''^t$
$[2058,783]$	$[2058,782]$	$[8330,783]$	$[8330,782]$	$[2058,731]$	$[2058,732]$	$[8330,731]$	$[8330,732]$
$[2058,52]$	$[2058,51]$	$[8330,681]$	$[8330,680]$	$[2058,52]$	$[2058,51]$	$[8330,52]$	$[8330,51]$
$[2058,681]$	$[2058,680]$	$[8330,732]$	$[8330,731]$	$[2058,680]$	$[2058,681]$	$[8330,680]$	$[8330,681]$
$[2058,731]$	$[2058,732]$	$[8330,51]$	$[8330,52]$	$[2058,103]$	$[2058,102]$	$[8330,103]$	$[8330,102]$
$[2058,102]$	$[2058,103]$	$[8330,102]$	$[8330,103]$	$[2058,783]$	$[2058,782]$	$[8330,783]$	$[8330,782]$

Moreover, from the extended matrices we constructed 3 binary self-orthogonal codes of the length 16660 and 2 binary self-orthogonal of the length 10388.