On self-orthogonal binary codes invariant under the action of the Held group

Vedrana Mikulić Crnković
(vmikulic@math.uniri.hr)

(joint work with D. Crnković and B. G. Rodrigues)

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

November 5, 2015

Introduction

- Group action
- Held group
- Designs
- Codes
- The construction

Results

- Symmetric designs on 2058 points
- Binary codes from the symmetric designs on 2058 points
- Symmetric designs on 8330 points
- Binary codes from the symmetric designs on 8330 points
- Non-symmetric designs on 2058 points
- Binary codes from the non-symmetric designs on 2058 points

Group action

A group G acts on a set S if there exists function $f : G \times S \to S$ such that

1. $f(e, x) = x, \ \forall x \in S,$
2. $f(g_1, f(g_2, x)) = f(g_1 g_2, x), \ \forall x \in S, \ \forall g_1, \ g_2 \in G.$

Denote the described action by $xg, \ x \in S, \ g \in G.$

The set $G_x = \{g \in G \mid xg = x\}$ is a group called stabilizer of the element $x \in S$.

Primitive action

The action of the group G on the set S induces the equivalence relation on the set S: $x \sim y \Leftrightarrow (\exists g \in G) xg = y$. The equivalence classes are orbits of the action. If group G act on the set S in one orbit then the action is transitive.
If G acts on the set S transitively and if each stabilizer is a maximal subgroup of G then the action is primitive.

Example

If G acts on $S = \{1, 2, 3, ..., n\}$ then there exists homomorphism $f : G \rightarrow S_n$. If the action is primitive then the stabilizers of the elements of S are maximal subgroups of the group $\mathrm{Im} f$ of index n (permutation representation of the group G of degree n).

Held group He is a sporadic simple group of order 4030387200 discover by Dieter Held in 1970's.

No.	Max. sub.	Deg.	No.	Max. sub.	Deg.
S_1	$\mathcal{S}_4(4):2$	2058	S_7	$3^{\cdot} S_7$	266560
S_2	$2^2{}^{\cdot}L_3(4){:}S_3$	8330	S_8	$7_+^{1+2}{:}(3\times S_3)$	652800
S_3	$2^6{:}3^{\cdot} S_6$	29155	S_9	$S_4\times L_3(2)$	999600
S_4	$2^6{:}3^{\cdot} S_6$	29155	S_{10}	$7{:}3\times L_3(2)$	1142400
S_5	$2^{1+6}{:}L_3(2)$	187425	S_{11}	$5^2{:}4A_4$	3358656
S_6	$7^2{:}L_2(7)$	244800			

Table : Maximal subgroups of He

- The full automorphism group of Held group is isomorphic to $\mathrm{He}:2$.
- The only primitive groups of degree 2058 are isomorphic to $\mathrm{He}:2$ or He (except A_{2058} and S_{2058}).

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.

- The complement of $\mathcal{D}$ is the structure $\bar{\mathcal{D}} = (\mathcal{P}, \mathcal{B}, \bar{\mathcal{I}})$, where $\bar{\mathcal{I}} = \mathcal{P} \times \mathcal{B} - \mathcal{I}$.
- The dual structure of $\mathcal{D}$ is $\mathcal{D}^t = (\mathcal{B}, \mathcal{P}, \mathcal{I}^t)$, where $(B, P) \in \mathcal{I}^t$ if and only if $(P, B) \in \mathcal{I}$.
- The design is symmetric if it has the same number of points and blocks.

A t-(v, k, λ) design is 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 $\mathrm{Aut}(\mathcal{D})$.

The full automorphism group of a design is isomorphic to the full automorphism groups of its complementary design and its dual design.

Codes will be linear codes, i.e. subspaces of the ambient vector space. A code C over a field of order 2, of length n and dimension k is denoted by $[n, k]$.
A generator matrix for the code is a $k \times n$ matrix made up of a basis for C.

Two linear codes are isomorphic if they can be obtained from one another 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 $\mathrm{Aut}(C)$.

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 $\mathbb{F}$.
The full automorphism group of $\mathcal{D}$ is contained in the full automorphism group of $C_{\mathbb{F}}(\mathcal{D})$.

The dual code $C^{\perp}$ is the orthogonal under the standard inner product $(,)$, i.e. $C^{\perp} = \{v \in \mathbb{F}^n | (v, c) = 0 \text{ for all } c \in C\}$.
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 such that k is odd and the block intersection numbers are even can be extend to the generating matrix (I_b, M) of the self-orthogonal code.

D. Crnković, VMC: 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

Theorem

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 $\delta_1, ..., \delta_s \in \Omega_2$ 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.

If Ω_1=Ω_2 then the constructed design is symmetric.

- Maximal subgroup S_1 of the permutation representation of the group He on 2058 points (i.e. S_1 is the stabilizer) acts on the set $\{1, 2, ..., 2058\}$ in 5 orbits Ω_1, Ω_2, Ω_3, Ω_4, Ω_5 with subdegrees 1, 136, 136, 425, and 1360, respectively.
- The two orbits of length 136 are interchanged by the involutory outer automorphism of the group He and all other orbits are invariant under the action of the involutory outer automorphism.

Orbits	Parameters	Full Automorphism Group
Ω_1,Ω_4	1-(2058, 426, 426)	He:2
Ω_1,Ω_4,Ω_2	1-(2058, 562, 562)	He
Ω_1,Ω_4,Ω_2,Ω_3	1-(2058, 698, 698)	He:2
Ω_1,Ω_4,Ω_3	1-(2058, 562, 562)	He
Ω_1,Ω_2	1-(2058, 137, 137)	He
Ω_1,Ω_2,Ω_3	1-(2058, 273, 273)	He:2
Ω_1,Ω_3	1-(2058, 137, 137)	He
Ω_4	1-(2058, 425, 425)	He:2
Ω_4,Ω_2	1-(2058, 561, 561)	He
Ω_4,Ω_2,Ω_3	1-(2058, 697, 697)	He:2
Ω_4,Ω_3	1-(2058, 561, 561)	He
Ω_2	1-(2058, 136, 136)	He
Ω_2,Ω_3	1-(2058, 272, 272)	He:2
Ω_3	1-(2058, 136, 136)	He

- The permutation representation of the group He on 2058 points acts primitively on the constructed designs.
- The permutation representation of the group He on 2058 points acts flag-transitive on the design with parameters 1-$(2058, 272, 272)$.
- All designs with even block sizes are self-orthogonal.

- If k is odd then the binary code of the constructed designs with blocks of size k is trivial.
- If k is even then the binary code of the constructed designs with blocks of size k are self-orthogonal.

k	C_k	$\mathrm{Aut}(C_k)$	$\bar{C}_k$	$\mathrm{Aut}(\bar{C}_k)$	E_k
426	$[2058, 783]$	$\mathrm{He}:2$	$[2058, 782]$	$\mathrm{He}:2$	$[2058, 782]$
562	$[2058, 52]$	He	$[2058, 51]$	He	$[2058, 51]$
698	$[2058, 681]$	$\mathrm{He}:2$	$[2058, 680]$	$\mathrm{He}:2$	$[2058, 680]$
136	$[2058, 731]$	He	$[2058, 732]$	He	$[2058, 731]$
272	$[2058, 102]$	$\mathrm{He}:2$	$[2058, 103]$	$\mathrm{He}:2$	$[2058, 102]$

Table : Non-trivial binary codes constructed from the pairwise non-isomorphic symmetric 1-designs on 2058 points

- The group He acts primitively on the coordinate positions (i.e. the set $\{1, 2, ..., 2058\}$).

- Maximal subgroup S_2 of the permutation representation of the group He on 8330 points (i.e. S_2 is the stabilizer) acts on the set $\{1, 2, ..., 8330\}$ in 7 orbits with subdegrees 1, 105, 1344, 840, 720, 840 and 4480 respectively.
- The two orbits of length 840 are interchanged by the outer automorphism of the group He, and all other orbits are invariant under the action of the involutory outer automorphism.

- There are, up to isomorphism, 46 symmetric 1-designs on 8330 points admitting He as a primitive automorphism group.
- 30 of them have $\mathrm{He}:2$ as the full automorphism group and 16 have He as the full automorphism group.
- 5 of them are self-orthogonal designs, and 3 designs are weakly self-orthogonal such that k is odd and the block intersection numbers are even.

- We constructed, up to isomorphism, 52 non-trivial binary codes of length 8330. 5 of them are self-orthogonal.

k	C'_k	$\bar{C}'_k$	E'_k
106	[8330, 7055]	[8330, 7054]	[8330, 7054]
1450	[8330, 783]	[8330, 782]	[8330, 782]
2290	[8330, 1972]	[8330, 1971]	[8330, 1971]
3010	[8330, 7004]	[8330, 7003]	[8330, 7003]
3850	[8330, 4353]	[8330, 4352]	[8330, 4352]
3130	[8330, 681]	[8330, 680]	[8330, 680]
2170	[8330, 4455]	[8330, 4454]	[8330, 4454]
946	[8330, 4404]	[8330, 4403]	[8330, 4403]
1666	[8330, 732]	[8330, 731]	[8330, 731]
2506	[8330, 1921]	[8330, 1920]	[8330, 1920]
1786	[8330, 6953]	[8330, 6952]	[8330, 6952]
826	[8330, 2023]	[8330, 2022]	[8330, 2022]
1345	[8330, 2058]	[8330, 2058]	[8330, 2057]
2185	[8330, 3978]	[8330, 3978]	[8330, 3977]
3745	[8330, 6410]	[8330, 6410]	[8330, 6409]
1344	[8330, 6272]	[8330, 6273]	[8330, 6272]
2184	[8330, 5083]	[8330, 5084]	[8330, 5083]
2904	[8330, 51]	[8330, 52]	[8330, 51]
3744	[8330, 2702]	[8330, 2703]	[8330, 2702]
3024	[8330, 6374]	[8330, 6375]	[8330, 6374]
2064	[8330, 2600]	[8330, 2601]	[8330, 2600]
840	[8330, 2651]	[8330, 2652]	[8330, 2651]
1560	[8330, 6323]	[8330, 6324]	[8330, 6323]
2400	[8330, 5134]	[8330, 5135]	[8330, 5134]
1680	[8330, 102]	[8330, 103]	[8330, 102]
720	[8330, 5032]	[8330, 5033]	[8330, 5032]

- The permutation representation of the group He on 8330 points acts primitively on the coordinate positions of the code and it is contained in the full automorphism groups of the constructed codes which are primitive groups of degree 8330. 16 codes have the full automorphism group that does not contain the full automorphism group of the permutation representation of the group He on 8330.
- If k is even then the binary code of the constructed designs with blocks of size k is contained in the binary code of the complementary design (with blocks of size $8330 - k$) or vice versa.
- If k is odd then the binary code of the constructed designs with blocks of size k is equal to the binary code of the complementary design (with blocks of size $8330 - k$).
- We also constructed 3 binary self-orthogonal codes of length 16660.

- Maximal subgroup S_2 of the permutation representation of the group He on 2058 points acts on the set $\{1, 2, ..., 2058\}$ in 5 orbits Δ_1, Δ_2, Δ_3, Δ_4, and Δ_5 with subdegrees 21, 21, 336, 840, and 840 respectively.
- The outer automorphism of the group He interchanges the orbits of the length 21 and the orbits of the length 840.

Orbits	Parameters	Full Automorphism Group
Δ_5	1-(2058, 840, 3400)	He
Δ_5,Δ_2	1-(2058, 861, 3485)	He
Δ_5,Δ_2,Δ_1	1-(2058, 882, 3570)	He
Δ_5,Δ_1	1-(2058, 861, 3485)	He
Δ_4	1-(2058, 840, 3400)	He
Δ_4,Δ_2	1-(2058, 861, 3485)	He
Δ_4,Δ_2,Δ_1	1-(2058, 882, 3570)	He
Δ_4,Δ_1	1-(2058, 861, 3485)	He
Δ_3	1-(2058, 336, 1360)	He:2
Δ_3,Δ_2	1-(2058, 357, 1445)	He
Δ_3,Δ_2,Δ_1	1-(2058, 378, 1530)	He:2
Δ_3,Δ_1	1-(2058, 357, 1445)	He
Δ_2	1-(2058, 21, 85)	He
Δ_2,Δ_1	1-(2058, 42, 170)	He:2
Δ_1	1-(2058, 21, 85)	He

Table : 1-designs on 2058 points and 8330 blocks

- The permutation representation of the group He on 2058 points acts primitively on the points of the constructed designs and the permutation representation of the group He on 8330 points acts primitively on the blocks of the constructed designs.
- All designs with even block sizes are self-orthogonal.
- Among 9 dual designs, there are 5 self-orthogonal designs (the ones with even block sizes) and 2 weakly self-orthogonal designs such that k is odd and the block intersection numbers are even.

- If k is odd then the binary code of the constructed designs with blocks of size k is trivial.
- If k is even then the binary code of the constructed designs with blocks of size k and the binary code of the dual designs are self-orthogonal.

k	C_k''	Aut(C_k'')	$\bar{C}_k''$	Aut($\bar{C}_k''$)	E_k''
840	$[2058, 731]$	He	$[2058, 732]$	He	$[2058, 731]$
882	$[2058, 52]$	He	$[2058, 51]$	He	$[2058, 51]$
336	$[2058, 680]$	He:2	$[2058, 681]$	He:2	$[2058, 680]$
378	$[2058, 103]$	He:2	$[2058, 102]$	He:2	$[2058, 102]$
42	$[2058, 783]$	He:2	$[2058, 782]$	He:2	$[2058, 782]$

Table : Non-trivial binary codes constructed from the pairwise non-isomorphic 1-designs on 2058 points and 8330 blocks and their duals

- We also constructed 2 self-orthogonal codes of length 10388 (codes of the weakly self-orthogonal designs).
- The group He acts primitively on the coordinate positions.

UNIVERSITY OF RIJEKA
DEPARTMENT OF MATHEMATICS

Thank you for your attention.