On self-orthogonal codes generated by orbit matrices of 1-designs

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

(joint work with D. Crnković)

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

April 7, 2016

UNIVERSITY OF RIJEKA
DEPARTMENT OF MATHEMATICS

Introduction
- Group action
- Designs
- The construction
- Codes
- Codes from weakly self-orthogonal 1-designs

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

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 $x \in S$. The set $xG = \{xg \mid g \in G\}$ is orbit of the element x.

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.
- Dual of a 1-design is a 1-design.

Examples of 1-designs

- $t-$designs (2-designs, duals of 2-designs, symmetric designs)
- regular graphs (strongly regular graphs)

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.

Groups and designs

An automorphism group A of a $1-$design $\mathcal{D}$ act on the set of points $\mathcal{P}$ and on the set of blocks $\mathcal{B}$.
Denote the orbits on the point set by $\mathcal{P}_1, \ldots, \mathcal{P}_m$ and the orbits on the block set by $\mathcal{B}_1, \ldots, \mathcal{B}_n$ and by $\gamma_{i,j}$ number of points in the orbit $\mathcal{P}_i$ that are contain in every block in the orbit $\mathcal{B}_j$.
The orbit matrix of the design $\mathcal{D}$ (under the action of the group A) is

$$\begin{array}{c|cccc} & \omega_1 & \omega_2 & \ldots & \omega_m \\ \hline \Omega_1 & \gamma_{1,1} & \gamma_{2,1} & \cdots & \gamma_{m,1} \\ \Omega_2 & \gamma_{1,2} & \gamma_{2,2} & \cdots & \gamma_{m,2} \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ \Omega_n & \gamma_{1,n} & \gamma_{2,n} & \cdots & \gamma_{m,n} \end{array}$$

where $\Omega_i = |\mathcal{B}_i|,\ i \in \{1, \ldots, n\}$, and $\omega_j = |\mathcal{P}_j|,\ j \in \{1, \ldots, m\}$.

UNIVERSITY OF RIJEKA
DEPARTMENT OF MATHEMATICS

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 $\Omega_1 = \Omega_2$ then the constructed design is symmetric.

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

By using this construction we obtained the following pairwise non-isomorphic self-orthogonal 1-designs:

Parameters	Full Automorphism Group
1-(2058, 426, 426)	$\mathrm{He}{:}2$
1-(2058, 562, 562)	He
1-(2058, 698, 698)	$\mathrm{He}{:}2$
1-(2058, 562, 562)	He
1-(2058, 272, 272)	$\mathrm{He}{:}2$
1-(8330, 1450, 1450)	$\mathrm{He}{:}2$
1-(8330, 3130, 3130)	$\mathrm{He}{:}2$
1-(8330, 1666, 1666)	He
1-(8330, 2904, 2904)	He
1-(8330, 1680, 1680)	$\mathrm{He}{:}2$
1-(2058, 840, 3400)	He
1-(2058, 882, 3570)	He
1-(2058, 336, 1360)	$\mathrm{He}{:}2$
1-(2058, 378, 1530)	$\mathrm{He}{:}2$
1-(2058, 42, 170)	$\mathrm{He}{:}2$

We also constructed weakly self-orthogonal 1-designs such that k is odd and the block intersection numbers are even:

Parameters	Full Automorphism Group
1-(8330, 1681, 1681)	He:2
1-(8330, 1449, 1449)	He:2
1-(8330, 3129, 3129)	He:2

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 whose rows generate all the elements of C.

The dual code $C^\perp$ is the orthogonal complement 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 $C \subseteq C^\perp$.

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 $C_{\mathbb{F}}(\mathcal{D})$.

Codes constructed from block designs have been extensively studied.

- E. F. Assmus Jnr, J. D. Key, Designs and their codes, Cambridge University Press, Cambridge, 1992.
- A. Baartmans, I. Landjev, V. D. Tonchev, On the binary codes of Steiner triple systems, Des. Codes Cryptogr. 8 (1996), 29–43.
- V. D. Tonchev, Quantum Codes from Finite Geometry and Combinatorial Designs, Finite Groups, Vertex Operator Algebras, and Combinatorics, Research Institute for Mathematical Sciences 1656, (2009) 44-54.

V. Tonchev, Self-orthogonal designs and extremal doubly-even codes, J. Combin. Theory, A 52 (1989), 197-205.

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

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

k	C_k	$\bar{C}_k$
426	$[2058, 783]$	$[2058, 782]$
562	$[2058, 52]$	$[2058, 51]$
698	$[2058, 681]$	$[2058, 680]$
136	$[2058, 731]$	$[2058, 732]$
272	$[2058, 102]$	$[2058, 103]$
1450	$[8330, 783]$	$[8330, 782]$
3130	$[8330, 681]$	$[8330, 680]$
1666	$[8330, 732]$	$[8330, 731]$
2904	$[8330, 51]$	$[8330, 52]$
1680	$[8330, 102]$	$[8330, 103]$
840	$[2058, 731]$	$[2058, 732]$
882	$[2058, 52]$	$[2058, 51]$
336	$[2058, 680]$	$[2058, 681]$
378	$[2058, 103]$	$[2058, 102]$
42	$[2058, 783]$	$[2058, 782]$

We also constructed 3 binary self-orthogonal codes of length 16660.

Theorem [M. Harada, V. D. Tonchev]

Let $\mathcal{D}$ be a 2-(v, k, λ) design with a fixed-point-free and fixed-block-free automorphism ϕ of order q, where q is prime. Further, let M be the orbit matrix induced by the action of the group $G = \langle \phi \rangle$ on the design $\mathcal{D}$. If p is a prime dividing r and λ then the orbit matrix M generates a self-orthogonal code of length $b|q$ over $\mathbf{F}_p$.

Theorem [V. D. Tonchev]

If G is a cyclic group of a prime order p that does not fix any point or block and $p|(r-\lambda)$, then the rows of the orbit matrix M generate a self-orthogonal code over $\mathbf{F}_p$.

Theorem [D. Crnković, L. Simčić]

Let $\mathcal{D}$ be a 2-(v,k,λ) design with an automorphism group G which acts on $\mathcal{D}$ with f fixed points, h fixed blocks, $\frac{v-f}{w}$ point orbits of length w and $\frac{b-h}{w}$ block orbits of length w. If a prime p divides w and $r-\lambda$, then the columns of the non-fixed part of the orbit matrix M for the automorphism group G generate a self-orthogonal code of length $\frac{b-h}{p}$ over $\mathbf{F}_p$.

Theorem [D. Crnković]

Let Γ be a srg(v, k, λ, μ) with an automorphism group G which acts on the set of vertices of Γ with $\frac{v}{w}$ orbits of length w. Let R be the row orbit matrix of the graph Γ with respect to G. If q is a prime dividing k, λ and μ, then the matrix R generates a self-orthogonal code of length $\frac{v}{w}$ over $\mathbf{F}_q$.

Let $\mathcal{D}$ be a self-orthogonal 1-design and G be an automorphism group of the design which acts on $\mathcal{D}$ with point orbits of length w. The binary code generate by the orbit matrix of the design $\mathcal{D}$ (under the action of the group G) is a self-orthogonal code of length $\frac{v}{w}$.

Example

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

Self-orthogonal codes constructed from an orbit matrix of self-orthogonal 1-designs constructed from He

$[294, 111]$	$[294, 110]$
$[294, 10]$	$[294, 6]$
$[294, 93]$	$[294, 98]$
$[294, 101]$	$[294, 6]$
$[294, 18]$	$[294, 98]$
$[686, 261]$	$[686, 260]$
$[686, 18]$	$[686, 17]$
$[686, 227]$	$[686, 226]$
$[686, 243]$	$[686, 244]$
$[686, 34]$	$[686, 35]$
$[294, 104]$	$[294, 105]$
$[294, 7]$	$[294, 6]$
$[294, 98]$	$[294, 99]$
$[294, 13]$	$[294, 12]$
$[294, 111]$	$[294, 110]$
$[686, 243]$	$[686, 244]$
$[686, 18]$	$[686, 17]$
$[686, 226]$	$[686, 227]$
$[686, 35]$	$[686, 34]$
$[686, 261]$	$[686, 260]$

[980, 47]	[980, 46]
[980, 41]	[980, 40]
[980, 44]	[980, 43]
[980, 3]	[980, 4]
[980, 6]	[980, 7]
[2380, 261]	[2380, 260]
[2380, 18]	[2380, 17]
[2380, 227]	[2380, 226]
[2380, 243]	[2380, 244]
[2380, 34]	[2380, 35]

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 point orbits of length w.
Consider the following matrix:

$$
\begin{array}{c|cccccccc}
 & & & & & \omega_1 & \omega_2 & \dots & \omega_m \\
\hline
\Omega_1 & 1 & 0 & \dots & 0 & \gamma_{1,1} & \gamma_{2,1} & \dots & \gamma_{m,1} \\
\Omega_2 & 0 & 1 & \dots & 0 & \gamma_{1,2} & \gamma_{2,2} & \dots & \gamma_{m,2} \\
\vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\
\Omega_n & 0 & 0 & \dots & 1 & \gamma_{1,n} & \gamma_{2,n} & \dots & \gamma_{m,n}
\end{array}
$$

The binary code generated by defined orbit matrix generate is a self-orthogonal code of length $\frac{v}{w}$.

We constructed 3 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 constracted 6 self-orthogonal codes with parameters $[980, 490]$ and 6 self-orthogonal codes with parameters $[2380, 1190]$.

Thank you for your attention.