WEAKLY SELF-ORTHOGONAL DESIGNS AND RELATED LINEAR CODES

UNIVERSITY OF RIJEKA
DEPARTMENT OF MATHEMATICS

VEDRANA MIKULIĆ CRNKOVIĆ AND IVONA TRAUNKAR

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

INTRODUCTION

A t-design is **weakly p-self-orthogonal** if all the block intersection numbers gives the same residue modulo p. A design is **self-orthogonal** if the block intersection numbers and the block size are even numbers.

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 $C\subseteq C^{\perp}$, **self-dual** if $C=C^{\perp}$ and **LCD** if $C\cap C^{\perp}=\mathbf{0}$.

We will denote $b\times v$ incidence matrix of a design by M. A finite field will be of order q, where $q=p^n$ and p is prime.

ORBIT MATRIX

Let $\mathcal{D}$ be 1-design and G be an automorphism group of $\mathcal{D}$. Let $v_1=|\mathcal{V}_1|,\ldots,v_n=|\mathcal{V}_n|$ be the sizes of point orbits and $b_1=|\mathcal{B}_1|,\ldots,b_m=|\mathcal{B}_m|$ be the sizes of block orbits under the action of the group G. We define an orbit matrix under the action of G as $m\times n$ matrix $O=[a_{i,j}]$, where $a_{i,j}$ is the number of points of the orbit $\mathcal{V}_j$ incident with a block of the orbit $\mathcal{B}_i$.

Let $\mathcal{D}$ be $1-(v,k,r)$ design and G an automorphism group of $\mathcal{D}$ 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. We define matrices: $OM1=[a_{i,j}]$, $i\in\{1,...,f_2\}$, $j\in\{1,...,f_1\}$ and $OM2=[a_{i,j}]$, $i\in\{f_2+1,...,f_2+m\}$, $j\in\{f_1+1,...,f_1+n\}$, where the columns $1,\ldots,f_1$ correspond to the fixed points and the rows $1,\ldots,f_2$ correspond to the fixed blocks.

SELF-ORTHOGONAL CODES FROM WSO DESIGNS

Let $\mathcal{D}$ be such that $k\equiv a \pmod p$ and $|B_i\cap B_j|\equiv d \pmod p$, 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 $[\sqrt{d}\cdot I_b, M, \sqrt{-d}\cdot\mathbf{1}]$ generates a b-dimensional self-orthogonal code over $\mathbb{F}$, where $\mathbb{F}=\mathbb{F}_q$ if d and $-d$ are squares in $\mathbb{F}_q$, 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 square in $\mathbb{F}_q$, and $\mathbb{F}=\mathbb{F}_{q^2}$ otherwise.
4. if $a=d\neq 0$ then the matrix $[M,\sqrt{-a}\cdot\mathbf{1}]$ generates a self-orthogonal code over $\mathbb{F}$, where $\mathbb{F}=\mathbb{F}_q$ if $-a$ is square in $\mathbb{F}_q$, and $\mathbb{F}=\mathbb{F}_{q^2}$ otherwise, and
5. if $a\neq 0$, $d\neq 0$, $a\neq d$, then the matrix $[\sqrt{d-a}\cdot I_b, M, \sqrt{-d}\cdot\mathbf{1}]$ generates a b-dimensional self-orthogonal code over $\mathbb{F}$, where $\mathbb{F}=\mathbb{F}_q$ if $d-a$ and $-d$ are squares in $\mathbb{F}_q$, and $\mathbb{F}=\mathbb{F}_{q^2}$ otherwise.

LCD CODES FROM WSO DESIGNS

Let $\mathcal{D}$ be such that $k\equiv a \pmod p$ and $|B_i\cap B_j|\equiv d \pmod p$, 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 $a=d=0$ then the matrix $[\mathbf{M}, x\mathbf{I}_b]$ for $x\neq 0$, and the matrix $[\mathbf{M}, x\mathbf{I}_b, y\mathbf{1}]$ for $y\neq 0$ and $x^2+by^2\neq 0$, generate an LCD code over the field $\mathbb{F}_q$.
2. If $a=d\neq 0$ then the matrix $[\mathbf{M}, x\mathbf{I}_b]$ for $x\neq 0$ and $x^2+ba\neq 0$, and the matrix $[\mathbf{M}, x\mathbf{I}_b, y\mathbf{1}]$ for $x\neq 0$ and $by^2+x^2+bd\neq 0$, generate an LCD code over the field $\mathbb{F}_q$.
3. If $a=0$ and $d\neq 0$ then the matrix $\mathbf{M}$ for $(b-1)d\neq 0$ and if $\mathbf{M}$ is of full rank, the matrix $[\mathbf{M}, y\mathbf{1}]$ for $by^2+(b-1)d\neq 0$ and if $\mathbf{M}$ is of full rank, the matrix $[\mathbf{M}, x\mathbf{I}_b]$ for $x-d\neq 0$ and $x^2+(b-1)d\neq 0$, and the matrix $[\mathbf{M}, x\mathbf{I}_b, y\mathbf{1}]$ for $x^2-d\neq 0$ and $by^2+x^2+(b-1)d\neq 0$ generate an LCD code over the field $\mathbb{F}_q$.
4. If $a\neq 0$ and $d=0$ then the matrix $\mathbf{M}$ if $\mathbf{M}$ is of full rank, the matrix $[\mathbf{M}, y\mathbf{1}]$ for $by^2+a\neq 0$ and if $\mathbf{M}$ is of full rank, the matrix $[\mathbf{M}, x\mathbf{I}_b]$ for $x^2+a\neq 0$, and the matrix $[\mathbf{M}, x\mathbf{I}_b, y\mathbf{1}]$ for $x^2+a\neq 0$ and $by^2+x^2+a\neq 0$, generate an LCD code over the field $\mathbb{F}_q$.
5. If $a\neq 0$, $d\neq 0$, $a\neq d$ then the matrix $\mathbf{M}$ for $a+(b-1)d\neq 0$ and if $\mathbf{M}$ is of full rank, the matrix $[\mathbf{M}, x\mathbf{I}_b]$ for $x^2-d+a\neq 0$ and $x^2+a+(b-1)d\neq 0$, the matrix $[\mathbf{M}, y\mathbf{1}]$ for $by^2+a+(b-1)d\neq$ and if $\mathbf{M}$ is of full rank, and the matrix $[\mathbf{M}, x\mathbf{I}_b, y\mathbf{1}]$ for $x^2-d+a\neq 0$ and $by^2+x^2+a+(b-1)d\neq 0$ generate an LCD code over $\mathbb{F}_q$.

SELF-ORTHOGONAL CODES FROM ORBIT MATRIX OF WSO DESIGNS

Let $\mathcal{D}$ be a $1-(v,k,r)$ design and $|B_i\cap B_j|=s$, for all $i,j\in\{1,\ldots,b\}$, $i\neq j$, where B_i and B_j two blocks of the design $\mathcal{D}$.

Let $k\equiv 0 \pmod p$, $s\equiv 0 \pmod p$, and let G be an automorphism group of $\mathcal{D}$ with n point orbits of length w and m block orbits of length w. Then linear code spanned by the rows of orbit matrix of the design $\mathcal{D}$ is a self-orthogonal code over $\mathbb{F}_q$ of length $\frac{v}{w}$ with dimension equal to $\operatorname{rank}(O)$.

Let $k\equiv 0 \pmod p$, $s\equiv 0 \pmod p$, 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 linear code spanned by the matrix $OM1$ is a self-orthogonal $[f_1,\operatorname{rank}(OM1)]$ code over $\mathbb{F}_q$ and the linear code spanned by the matrix $OM2$ is a self-orthogonal $[n,\operatorname{rank}(OM2)]$ code over $\mathbb{F}_q$.

Let $k\equiv 0 \pmod p$ and $s\equiv d \pmod p$, 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. If $p\mid w$, then linear code spanned by the rows of the matrix $[\sqrt{d}\cdot I_m, O]$ is a self-orthogonal $[m+n,m]$ code over $\mathbb{F}$, where $\mathbb{F}=\mathbb{F}_q$ if d is square root in $\mathbb{F}_q$, and $\mathbb{F}=\mathbb{F}_{q^2}$ otherwise. If $p\mid w-1$, then linear code spanned by the rows of the matrix $[\sqrt{wd}\cdot I_m, O, \sqrt{-wd}\cdot\mathbf{1}]$ is a self-orthogonal $[m+n+1,m]$ code over $\mathbb{F}$, where $\mathbb{F}=\mathbb{F}_q$ if wd and $-wd$ are square roots in $\mathbb{F}_q$, and $\mathbb{F}=\mathbb{F}_{q^2}$ otherwise. If $p\nmid w$ and $p\nmid w-1$, then linear code spanned by the rows of the matrix $[\sqrt{d}\cdot I_m, O, \sqrt{-wd}\cdot\mathbf{1}]$ is a self-orthogonal $[m+n+1,m]$ code over $\mathbb{F}$, where $\mathbb{F}=\mathbb{F}_q$ if d and $-wd$ are square roots in $\mathbb{F}_q$, and $\mathbb{F}=\mathbb{F}_{q^2}$ otherwise.

Let $k\equiv 0 \pmod p$, $s\equiv d \pmod p$, and let G be an automorphism group of $\mathcal{D}$ 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 linear code spanned by the matrix $[\sqrt{d}\cdot I_{f_2}, OM1, \sqrt{-d}\cdot\mathbf{1}]$ is a self-orthogonal $[f_2+f_1+1,f_2]$ code $\mathbb{F}$ ($\mathbb{F}=\mathbb{F}_q$ if d and $-d$ are square roots in $\mathbb{F}_q$, and $\mathbb{F}=\mathbb{F}_{q^2}$ otherwise), and linear code spanned by the matrix $[\sqrt{d}\cdot I_m, OM2]$ is a self-orthogonal $[m+n,m]$ code over $\mathbb{F}$ (where $\mathbb{F}=\mathbb{F}_q$ if d is square root in $\mathbb{F}_q$, and $\mathbb{F}=\mathbb{F}_{q^2}$ otherwise).

Let $k\equiv a \pmod p$ and $s\equiv 0 \pmod p$, and let G be an automorphism group of $\mathcal{D}$ with n point orbits of length w and m block orbits of length w. Then the linear code spanned by the rows of matrix $[\sqrt{-a}\cdot I_m, O]$, where O is the orbit matrix of the design $\mathcal{D}$ is a self-orthogonal $[m+n,m]$ code over $\mathbb{F}$, where $\mathbb{F}=\mathbb{F}_q$ if $-a$ is a square rootin $\mathbb{F}_q$,, and $\mathbb{F}=\mathbb{F}_{q^2}$ otherwise.

Let $k\equiv a \pmod q$, $s\equiv 0 \pmod q$, and let G be an automorphism group of $\mathcal{D}$ 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 linear code spanned by the matrix $[\sqrt{-a}\cdot I_{f_2}, OM1]$ is a self-orthogonal $[f_2+f_1,f_2]$ code over $\mathbb{F}$ ($\mathbb{F}=\mathbb{F}_q$ if $-a$ is square root in $\mathbb{F}_q$, and $\mathbb{F}=\mathbb{F}_{q^2}$ otherwise) and linear code spanned by the matrix $[\sqrt{-a}\cdot I_m, OM2]$ is a self-orthogonal $[m+n,m]$ code $\mathbb{F}$ ($\mathbb{F}=\mathbb{F}_q$ if $-a$ is square root in $\mathbb{F}_q$, and $\mathbb{F}=\mathbb{F}_{q^2}$ otherwise).

Let $k\equiv a \pmod p$ and $s\equiv d \pmod p$, for all $i,j\in\{1,\ldots,b\}$, $i\neq j$, 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. If $a=d$ and $p\mid w$, then linear code spanned by the rows of the matrix O is a self-orthogonal $[m,\operatorname{rank}(O)]$ code over the field $\mathbb{F}_q$. If $a=d$ and $p\nmid w$, then linear code spanned by the rows of the matrix $[O,\sqrt{-wd}\cdot\mathbf{1}]$ is a self-orthogonal $[m+1,\operatorname{rank}(O)]$ 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. If $a\neq d$ and $p\mid w$, then linear code spanned by the rows of the matrix $[\sqrt{d-a}\cdot I_m, O]$ 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 $a\neq d$ and $p\mid w-1$, then linear code spanned by the rows of the matrix $[\sqrt{wd-a}\cdot I_m, O, \sqrt{-dw}\cdot\mathbf{1}]$ is a self-orthogonal $[m+n+1,m]$ code over the field $\mathbb{F}$, where $\mathbb{F}=\mathbb{F}_q$ if $-wd$ and $wd-a$ are square roots in $\mathbb{F}_q$, and $\mathbb{F}=\mathbb{F}_{q^2}$ otherwise. If $a\neq d$ and $p\nmid w$ and $p\nmid w-1$, then binary linear code spanned by the rows of the matrix $[\sqrt{d-a}\cdot I_m, O, \sqrt{-wd}\cdot\mathbf{1}]$ is a self-orthogonal $[m+n+1,m]$ code over the field $\mathbb{F}$, where $\mathbb{F}=\mathbb{F}_q$ if $d-a$ and $-wd$ are square roots in $\mathbb{F}_q$, and $\mathbb{F}=\mathbb{F}_{q^2}$ otherwise.

Let $k\equiv a \pmod p$, $s\equiv d \pmod p$, and let G be an automorphism group of $\mathcal{D}$ 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. If $a=d$, then linear code spanned by the matrix $[OM1,\sqrt{-a}\cdot\mathbf{1}]$ is a self-orthogonal $[f_1+1,\operatorname{rank}(OM1)]$ code over $\mathbb{F}$ ($\mathbb{F}=\mathbb{F}_q$ if $-a$ is square root in $\mathbb{F}_q$, and $\mathbb{F}=\mathbb{F}_{q^2}$ otherwise) and linear code spanned by the matrix $OM2$ is a self-orthogonal $[n,\operatorname{rank}(OM2)]$ code of length over $\mathbb{F}_q$. If $a\neq d$ then linear code spanned by the matrix $[\sqrt{d-a}\cdot I_{f_2}, OM1, \sqrt{-d}\cdot\mathbf{1}]$ is a self-orthogonal $[f_2+f_1+1,f_2]$ code over $\mathbb{F}$ ($\mathbb{F}=\mathbb{F}_q$ if $d-a$ and $-d$ are square roots in $\mathbb{F}_q$, and $\mathbb{F}=\mathbb{F}_{q^2}$ otherwise) and linear code spanned by the matrix $[\sqrt{a-d}\cdot I_m, OM2]$ is a self-orthogonal $[m+n,m]$ code over $\mathbb{F}$ ($\mathbb{F}=\mathbb{F}_q$ if $a-d$ is square root in $\mathbb{F}_q$, and $\mathbb{F}=\mathbb{F}_{q^2}$ otherwise).

BIBLIOGRAPHY

D. Crnković, V. Mikulić Crnković, B. G. Rodrigues, On self-orthogonal designs and codes related to Held's simple group, Adv. Math. Commun. 12 (2018)
V. Mikulić Crnković, I. Traunkar, Self-orthogonal codes constructed from weakly self-orthogonal designs invariant under an action of M_{11}, AAECC (2021)
V. Tonchev, Self-Orthogonal Designs and Extremal Doubtly-Even Codes, Journal of Combinatorial Theory, Series A 52 (1989)