# Construction of self-orthogonal linear codes from orbit matrices of combinatorial structures

Sanja Rukavina
sanjar@math.uniri.hr

Department of Mathematics
University of Rijeka, Croatia

8th PhD Summer School in Discrete Mathematics
Rogla, Slovenia, 1-7 July 2018

UNIVERSITY OF RIJEKA
DEPARTMENT OF MATHEMATICS

hrzz
Hrvatska zaklada za znanost

Supported by CSF under the project 1637.

# Codes

Let $\mathbf{F}_q$ be the finite field of order $q$. A **linear code** of **length** $n$ is a subspace of the vector space $\mathbf{F}_q^n$. A $k$-dimensional subspace of $\mathbf{F}_q^n$ is called a linear $[n, k]$ code over $\mathbf{F}_q$.

For $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \mathbf{F}_q^n$ the number $d(x, y) = |\{i \,|1 \leq i \leq n, \, x_i \neq y_i\}|$ is called a Hamming distance. A **minimum distance** of a code $C$ is $d = min\{d(x, y) \,|x, y \in C, x \neq y\}$.
A linear $[n, k, d]$ code is a linear $[n, k]$ code with minimum distance $d$.

The **dual** code $C^\perp$ is the orthogonal complement under the standard inner product $(,)$. A code $C$ is **self-orthogonal** if $C \subseteq C^\perp$ and **self-dual** if $C = C^\perp$.

# Designs

A $t-(v,k,\lambda)$ **design** is a finite incidence structure $\mathcal{D}=(\mathcal{P},\mathcal{B},\mathcal{I})$ satisfying the following requirements:

1. $|\mathcal{P}|=v$,
2. every element of $\mathcal{B}$ is incident with exactly $k$ elements of $\mathcal{P}$,
3. every $t$ elements of $\mathcal{P}$ are incident with exactly $\lambda$ elements of $\mathcal{B}$.

Every element of $\mathcal{P}$ is incident with exactly $r$ elements of $\mathcal{B}$. The number of blocks is denoted by $b$.
If $|\mathcal{P}|=|\mathcal{B}|$ (or equivalently $k=r$) then the design is called **symmetric**.

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

# Tactical decomposition

Let $A$ be the incidence matrix of a design $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$. A **decomposition** of $A$ is any partition $B_1, \ldots, B_s$ of the columns of $A$ (blocks of $\mathcal{D}$) and a partition $P_1, \ldots, P_t$ of the rows of $A$ (points of $\mathcal{D}$).

For $i \leq s$, $j \leq t$ define

$$\alpha_{ij} = |\{P \in P_i |\ P\mathcal{I}x\}|, \text{ for } x \in B_j \text{ arbitrarily chosen,}$$
$$\beta_{ij} = |\{x \in B_j |\ P\mathcal{I}x\}|, \text{ for } P \in P_i \text{ arbitrarily chosen.}$$

We say that a decomposition is **tactical** if the $\alpha_{ij}$ and $\beta_{ij}$ are well defined (independent from the choice of $x \in B_j$ and $P \in P_i$, respectively).

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ be a 2-$(v, k, \lambda)$ design and $G \leq \mathrm{Aut}(\mathcal{D})$. We denote the $G-$orbits of points by $\mathcal{P}_1, \ldots, \mathcal{P}_m$, $G-$orbits of blocks by $\mathcal{B}_1, \ldots, \mathcal{B}_n$, and put $|\mathcal{P}_i| = \nu_i$, $|\mathcal{B}_j| = \beta_j$, $i = 1, \ldots, m$, $j = 1, \ldots, n$.

The **group action** of $G$ induces a **tactical decomposition of** $\mathcal{D}$. Denote by $a_{ij}$ the number of blocks of $\mathcal{B}_j$ which are incident with a representative of the point orbit $\mathcal{P}_i$. The number $a_{ij}$ does not depend on the choice of a point $P \in \mathcal{P}_i$, and the following equalities hold:

$$\sum_{j=1}^{n} a_{ij} = r \,, \tag{1}$$

$$\sum_{j=1}^{n} \frac{\nu_t}{\beta_j} a_{sj} \; a_{tj} = \lambda \nu_t + \delta_{st}(r - \lambda) \,. \tag{2}$$

## Definition

A $(m \times n)$-matrix $M = (a_{ij})$ with entries satisfying conditions (1) and (2) is called a point orbit matrix for the parameters $2-(v,k,\lambda)$ and orbit lengths distributions $(\nu_1,\dots,\nu_m)$ and $(\beta_1,\dots,\beta_n)$.

Orbit matrices are often used in construction of designs with a presumed automorphism group. Construction of designs admitting an action of the presumed automorphism group consists of two steps:

1. Construction of orbit matrices for the given automorphism group,
2. Construction of block designs for the obtained orbit matrices.

# (7,3,1)

Incidence matrix for the symmetric (7,3,1) design

$$\left(\begin{array}{c|ccc|ccc} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ \hline 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right)$$

Corresponding orbit matrix for $Z_3$

| | 1 | 3 | 3 |
|---|---|---|---|
| 1 | 0 | 3 | 0 |
| 3 | 1 | 1 | 1 |
| 3 | 0 | 1 | 2 |

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.
- I. Bouyukliev, V. Fack, J. Winne, 2-$(31, 15, 7)$, 2-$(35, 17, 8)$ and 2-$(36, 15, 6)$ designs with automorphisms of odd prime order, and their related Hadamard matrices and codes, Des. Codes Cryptogr., **51** (2009), no. 2, 105–122.
- 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.
- ...

# Codes from orbit matrices of block designs

## Theorem [M. Harada, V. D. Tonchev, 2003]

Let $\mathcal{D}$ be a 2-$(v,k,\lambda)$ design with a **fixed-point-free** and **fixed-block-free automorphism** $\phi$ 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 $\lambda$ then the **orbit matrix** $M$ generates a **self-orthogonal code** of length $b|q$ over $\mathbf{F}_p$.

Harada and Tonchev classified all codes over $\mathbf{F}_3$ and $\mathbf{F}_7$ derived from symmetric 2-$(v,k,\lambda)$ designs with fixed-point-free automorphisms of order $p$ for the parameters $(v,k,\lambda,p)$=(27, 14, 7, 3), (40, 27, 18, 5) and (45, 12, 3, 5).

**Theorem** [D. Crnković, D. Dumičić Danilović, SR]

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a 2-$(v, k, \lambda)$ design admitting an automorphism group $G$ acting on $\mathcal{P}$ with $f$ fixed points and $\frac{v-f}{w}$ orbits of length $w$, and acting on $\mathcal{B}$ with $h$ fixed blocks and $\frac{b-h}{w}$ orbits of length $w$. Let $p$ be a prime number such that $p|w$ and $p|(r-\lambda)$. The code spanned by the rows corresponding to the nonfixed part of the point orbit matrix $A$ of $\mathcal{D}$ with respect to $G$ is a self-orthogonal code of length $\frac{b-h}{w}$ over $F_q$ with respect to the ordinary inner product, where $q = p^{\overline{n}}$ and $\overline{n}$ is a positive integer.

**Theorem** [D. Crnković, D. Dumičić Danilović, SR]

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a 2-$(v, k, \lambda)$ design admitting an automorphism group $G$ acting on $\mathcal{P}$ with $f$ fixed points and $\frac{v-f}{w}$ orbits of length $w$, and on $\mathcal{B}$ with $h$ fixed blocks and $\frac{b-h}{w}$ orbits of length $w$. Let $p$ be a prime number such that $p|w$, $p|r$ and $p|\lambda$. The code spanned by the rows corresponding to the fixed part of the point orbit matrix $A$ of $\mathcal{D}$ with respect to $G$ is a self-orthogonal code of length $h$ over $F_q$ with respect to the ordinary inner product, where $q = p^{\overline{n}}$ and $\overline{n}$ is a positive integer.

# Strongly regular graphs

A graph is **regular** if all the vertices have the same valency; a regular graph is **strongly regular** of type $(v, k, \lambda, \mu)$ if it has $v$ vertices, valency $k$, and if any two adjacent vertices are together adjacent to $\lambda$ vertices, while any two non-adjacent vertices are together adjacent to $\mu$ vertices.
A strongly regular graph of type $(v, k, \lambda, \mu)$ is denoted by $\mathrm{srg}(v, k, \lambda, \mu)$.

# OM of strongly regular graphs

M. Behbahani and C. Lam have studied orbit matrices of strongly regular graphs that admit an automorphism group of prime order.

M. BEHBAHANI, C. LAM, Strongly regular graphs with non-trivial automorphisms, *Discrete Math.*, 311 (2011), 132-144

Let $\Gamma$ be a srg$(v, k, \lambda, \mu)$ and $A$ be its adjacency matrix. Suppose an automorphism group $G$ of $\Gamma$ partitions the set of vertices $V$ into $t$ orbits $O_1, \ldots, O_t$, with sizes $n_1, \ldots, n_t$, respectively. The orbits divide $A$ into submatrices $[A_{ij}]$, where $A_{ij}$ is the adjacency matrix of vertices in $O_i$ versus those in $O_j$. We define matrices $C = [c_{ij}]$ and $R = [r_{ij}]$, $1 \leq i, j \leq t$, such that

$$c_{ij} = \text{column sum of } A_{ij},$$
$$r_{ij} = \text{row sum of } A_{ij}.$$

$R$ is related to $C$ by $r_{ij} n_i = c_{ij} n_j$. Since the adjacency matrix is symmetric, $R = C^T$. The matrix $R$ is the row orbit matrix of the graph $\Gamma$ with respect to $G$, and the matrix $C$ is the column orbit matrix of the graph $\Gamma$ with respect to $G$.

# srg(10,3,0,1)

$$\left[\begin{array}{c|ccc|ccc|ccc}
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ \hline
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ \hline
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ \hline
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0
\end{array}\right]$$

$$R = \begin{bmatrix} 0 & 0 & 3 & 0 \\ 0 & 0 & 1 & 2 \\ 1 & 1 & 0 & 1 \\ 0 & 2 & 1 & 0 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 \\ 3 & 1 & 0 & 1 \\ 0 & 2 & 1 & 0 \end{bmatrix}$$

## Definition

A $(t \times t)$-matrix $R = [r_{ij}]$ with entries satisfying conditions

$$\sum_{j=1}^{t} r_{ij} = \sum_{i=1}^{t} \frac{n_i}{n_j} r_{ij} = k \tag{3}$$

$$\sum_{s=1}^{t} \frac{n_s}{n_j} r_{si} r_{sj} = \delta_{ij}(k-\mu) + \mu n_i + (\lambda - \mu) r_{ji} \tag{4}$$

is called a **row orbit matrix** for a strongly regular graph with parameters $(v, k, \lambda, \mu)$ and orbit lengths distribution $(n_1, \dots, n_t)$. A $(t \times t)$-matrix $C = [c_{ij}]$ with entries satisfying conditions

$$\sum_{i=1}^{t} c_{ij} = \sum_{j=1}^{t} \frac{n_j}{n_i} c_{ij} = k \tag{5}$$

$$\sum_{s=1}^{t} \frac{n_s}{n_j} c_{is} c_{js} = \delta_{ij}(k-\mu) + \mu n_i + (\lambda - \mu) c_{ij} \tag{6}$$

is called a **column orbit matrix** for a strongly regular graph with parameters $(v, k, \lambda, \mu)$ and orbit lengths distribution $(n_1, \dots, n_t)$.

If all orbits have the same length $w$, *i.e.* $n_i = w$ for $i = 1, \dots, t$, then $C = R$, and the following holds

$$\sum_{s=1}^{t} r_{is} r_{js} = \delta_{ij}(k-\mu) + \mu w + (\lambda - \mu) r_{ij}.$$

- Let us suppose that the group $Z_4$ acts on the vertices of an srg(40,12,2,4) with ten orbits of length 4.
- 39 matrices $C_1 - C_{39}$ for the parameters $(40, 12, 2, 4)$ and orbit lengths distribution $(4, 4, 4, 4, 4, 4, 4, 4, 4, 4)$ are given.
- Only five of them are induced by an action of $Z_4$ on some of the strongly regular (40,12,2,4) graphs constructed by Spence (E. Spence, The strongly regular (40,12,2,4) graphs, Electron. J. Combin., 7 (2000), #22, pp. 4.)

**Theorem [ D. Crnković, M. Maksimović, B. G. Rodrigues, SR, 2016]**

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

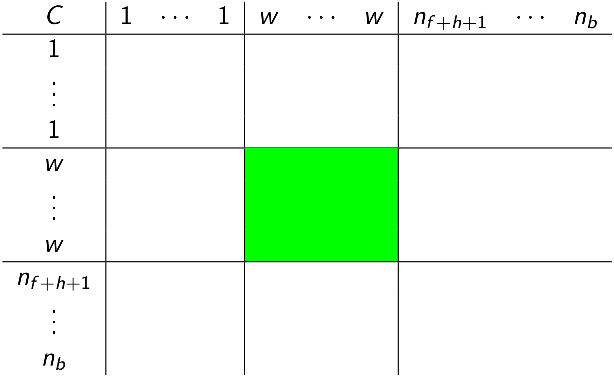
## Theorem [ D. Crnković, M. Maksimović, SR, 2018]

Let $\Gamma$ be a SRG$(v, k, \lambda, \mu)$ having an automorphism group $G$ which acts on the set of vertices of $\Gamma$ with $b$ orbits of lengths $n_1, \dots, n_b$, respectively, with $f$ fixed vertices, and the other $b - f$ orbits of lengths $n_{f+1}, \dots, n_b$ divisible by $p$, where $p$ is a prime dividing $k$, $\lambda$ and $\mu$. Let $C$ be the column orbit matrix of the graph $\Gamma$ with respect to $G$. If $q$ is a prime power such that $q = p^n$, then the code spanned by the rows of the fixed part of the matrix $C$ is a self-orthogonal code of length $f$ over $F_q$.

| $C$ | $1$ | $\cdots$ | $1$ | $n_{f+1}$ | $\cdots$ | $n_b$ |
|---|---|---|---|---|---|---|
| $1$ | | | | | | |
| $\vdots$ | | | | | | |
| $1$ | | | | | | |
| $n_{f+1}$ | | | | | | |
| $\vdots$ | | | | | | |
| $n_b$ | | | | | | |

## Theorem [ D. Crnković, M. Maksimović, SR, 2018]

Let $\Gamma$ be a SRG$(v, k, \lambda, \mu)$ having an automorphism group $G$ which acts on the set of vertices of $\Gamma$ with $b$ orbits of lengths $n_1, \ldots, n_b$, respectively, such that there are $f$ fixed vertices, $h$ orbits of length $w$, and $b - f - h$ orbits of lengths $n_{f+h+1}, \ldots, n_b$. Further, let $pw|n_s$ if $w < n_s$, and $pn_s|w$ if $n_s < w$, for $s = f + h + 1, \ldots, b$, where $p$ is a prime number dividing $k$, $\lambda$, $\mu$ and $w$. Let $C$ be the column orbit matrix of the graph $\Gamma$ with respect to $G$. If $q$ is a prime power such that $q = p^n$, then the code over $F_q$ spanned by the part of the matrix $C$ (rows and columns) determined by the orbits of length $w$ is a self-orthogonal code of length $h$.



| $C$ | 1 ··· 1 | 2 ··· 2 | 4 ··· 4 |
|---|---|---|---|
| 1 ⋮ 1 | | | |
| 2 ⋮ 2 | | | |
| 4 ⋮ 4 | | | |

| $C$ | 1 ··· 1 | 2 ··· 2 | 4 ··· 4 |
|---|---|---|---|
| 1 ⋮ 1 | | | |
| 2 ⋮ 2 | | | |
| 4 ⋮ 4 | | | |

| $C$ | 1 ··· 1 | 2 ··· 2 | 4 ··· 4 |
|---|---|---|---|
| 1 ⋮ 1 | | | |
| 2 ⋮ 2 | | | |
| 4 ⋮ 4 | | | |

## Theorem [ D. Crnković, M. Maksimović, SR, 2018]

Let $\Gamma$ be a SRG$(v, k, \lambda, \mu)$ with an automorphism group $G$ which acts on the set of vertices of $\Gamma$ with $b$ orbits of lengths $n_1, \dots, n_b$, respectively, and $w = max\{n_1, \dots, n_b\}$. Further, let $p$ be a prime dividing $k$, $\lambda$, $\mu$ and $w$, and let $pn_s|w$ if $n_s \neq w$. Let $C$ be the column orbit matrix of the graph $\Gamma$ with respect to $G$. If $q$ is a prime power such that $q = p^n$, then the code over $F_q$ spanned by the rows of $C$ corresponding to the orbits of length $w$ is a self-orthogonal code of length $b$.

| $C$ | $n_1$ | $\cdots$ | $n_{i_1}$ | $n_{i_1+1}$ | $\cdots$ | $n_{i_2}$ | $\cdots$ | $w$ | $\cdots$ | $w$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $n_1$ | | | | | | | | | | |
| $\vdots$ | | | | | | | | | | |
| $n_{i_1}$ | | | | | | | | | | |
| $n_{i_1+1}$ | | | | | | | | | | |
| $\vdots$ | | | | | | | | | | |
| $n_{i_2}$ | | | | | | | | | | |
| $\vdots$ | | | | | | | | | | |
| $w$ | | | | | | | | | | |
| $\vdots$ | | | | | | | | | | |
| $w$ | | | | | | | | | | |

## Theorem [ D. Crnković, M. Maksimović, SR, 2018]

Let $\Gamma$ be a SRG$(v, k, \lambda, \mu)$ with an automorphism group $G$ which acts on the set of vertices of $\Gamma$ with $b$ orbits of lengths $n_1, \ldots, n_b$, respectively, and $w = min\{n_1, \ldots, n_b\}$. Further, let $p$ be a prime dividing $k$, $\lambda$, $\mu$ and $w$, and let $pw | n_s$ if $n_s \neq w$. Let $R$ be the row orbit matrix of the graph $\Gamma$ with respect to $G$. If $q$ is a prime power such that $q = p^n$, then the code over $F_q$ spanned by the rows of $R$ corresponding to the orbits of length $w$ is a self-orthogonal code of length $b$.

| $R$ | $w$ | $\cdots$ | $w$ | $n_{i_1+1}$ | $\cdots$ | $n_{i_2}$ | $\cdots$ | $n_{i_l+1}$ | $\cdots$ | $n_b$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $w$ | | | | | | | | | | |
| $\vdots$ | | | | | | | | | | |
| $w$ | | | | | | | | | | |
| $n_{i_1+1}$ | | | | | | | | | | |
| $\vdots$ | | | | | | | | | | |
| $n_{i_2}$ | | | | | | | | | | |
| $\vdots$ | | | | | | | | | | |
| $n_{i_l+1}$ | | | | | | | | | | |
| $\vdots$ | | | | | | | | | | |
| $n_b$ | | | | | | | | | | |

# Self-dual codes from extended orbit matrices of symmetric designs

In the sequel we will study codes spanned by orbit matrices for a symmetric $(v, k, \lambda)$ design and orbit lengths distribution $(\Omega, \dots, \Omega)$, where $\Omega = \frac{v}{t}$. We follow the ideas presented in:

- E. Lander, Symmetric designs: an algebraic approach, Cambridge University Press, Cambridge (1983).
- R. M. Wilson, Codes and modules associated with designs and $t$-uniform hypergraphs, in: D. Crnković, V. Tonchev, (eds.) Information security, coding theory and related combinatorics, pp. 404–436. NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur. 29 IOS, Amsterdam (2011).

(Lander and Wilson have considered codes from incidence matrices of symmetric designs.)

## Theorem

Let $p$ be a prime. Suppose that $C$ is the code over $\mathbf{F}_p$ spanned by the incidence matrix of a symmetric $(v,k,\lambda)$ design.

1. If $p \mid (k-\lambda)$, then $dim(C) \leq \frac{1}{2}(v+1)$.
2. If $p \nmid (k-\lambda)$ and $p \mid k$, then $dim(C) = v-1$.
3. If $p \nmid (k-\lambda)$ and $p \nmid k$, then $dim(C) = v$.

## Theorem [D. Crnković, SR, 2016]

Let a group $G$ acts on a symmetric $(v,k,\lambda)$ design $\mathcal{D}$ with $t = \frac{v}{\Omega}$ orbits of length $\Omega$, on the set of points and the set of blocks, and let $M$ be an orbit matrix of $\mathcal{D}$ induced by the action of $G$. Let $p$ be a prime. Suppose that $C$ is the code over $\mathbf{F}_p$ spanned by the rows of $M$.

1. If $p \mid (k-\lambda)$, then $dim(C) \leq \frac{1}{2}(t+1)$.
2. If $p \nmid (k-\lambda)$ and $p \mid k$, then $dim(C) = t-1$.
3. If $p \nmid (k-\lambda)$ and $p \nmid k$, then $dim(C) = t$.

Let a group $G$ acts on a symmetric $(v, k, \lambda)$ design with $t = \frac{v}{\Omega}$ orbits of length $\Omega$ on the set of points and set of blocks.

## Theorem (HT)

Let $\mathcal{D}$ be a symmetric $(v, k, \lambda)$ design admitting an automorphism group $G$ that acts on the sets of points and blocks with $t = \frac{v}{\Omega}$ orbits of length $\Omega$. Further, let $M$ be the orbit matrix induced by the action of the group $G$ on the design $\mathcal{D}$. If $p$ is a prime dividing $k$ and $\lambda$, then the rows of the matrix $M$ span a self-orthogonal code of length $t$ over $\mathbf{F}_p$.

Let $V$ be a vector space of finite dimension $n$ over a field $\mathbf{F}$, let $b : V \times V \to \mathbf{F}$ be a symmetric bilinear form, i.e. a scalar product, and $(e_1, \ldots, e_n)$ be a basis of $V$. The bilinear form $b$ gives rise to a matrix $B = [b_{ij}]$, with

$$b_{ij} = b(e_i, e_j).$$

The matrix $B$ determines $b$ completely. If we represent vectors $x$ and $y$ by the row vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, then

$$b(x, y) = xBy^T.$$

Since the bilinear form $b$ is symmetric, $B$ is a symmetric matrix.

A bilinear form $b$ is nondegenerate if and only if its matrix $B$ is nonsingular.

We may use a symmetric nonsingular matrix $U$ over a field $\mathbf{F}_p$ to introduce a scalar product $\langle \cdot, \cdot \rangle_U$ for row vectors in $\mathbf{F}_p^n$, namely

$$\langle a, c \rangle_U = aUc^\top.$$

For a linear $p$-ary code $C \subset F_p^n$, the $U$-dual code of $C$ is

$$C^U = \{a \in \mathbf{F}_p^n : \langle a, c \rangle_U = 0 \quad \text{for all} \quad c \in C\}.$$

We call $C$ **self-$U$-dual**, or **self-dual with respect to $U$**, when $C = C^U$.

Let a group $G$ acts on a symmetric $(v, k, \lambda)$ design $\mathcal{D}$ with $t = \frac{v}{\Omega}$ orbits of length $\Omega$, on the set of points and the set of blocks, and let $M$ be the corresponding orbit matrix.

If $p$ divides $k - \lambda$, but does not divide $k$, we use a different code. Define the extended orbit matrix

$$M^{ext} = \left[ \begin{array}{ccc|c} & & & 1 \\ & M & & \vdots \\ & & & 1 \\ \hline \lambda\Omega & \cdots & \lambda\Omega & k \end{array} \right],$$

and denote by $C^{ext}$ the extended code spanned by $M^{ext}$.

Define the symmetric bilinear form $\psi$ by

$$\psi(\bar{x}, \bar{y}) = x_1 y_1 + \ldots + x_t y_t - \lambda\Omega x_{t+1} y_{t+1},$$

for $\bar{x} = (x_1, \ldots, x_{t+1})$ and $\bar{y} = (y_1, \ldots, y_{t+1})$. Since $p \mid n$ and $p \nmid k$, it follows that $p \nmid \Omega$ and $p \nmid \lambda$. Hence $\psi$ is a nondegenerate form on $\mathbf{F}_p$. The extended code $C^{ext}$ over $\mathbf{F}_p$ is self-orthogonal (or totally isotropic) with respect to $\psi$.

The matrix of the bilinear form $\psi$ is the $(t+1) \times (t+1)$ matrix

$$\Psi = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & -\lambda\Omega \end{bmatrix}.$$

**Theorem** [D. Crnković, SR, 2016]

Let $\mathcal{D}$ be a symmetric $(v, k, \lambda)$ design admitting an automorphism group $G$ that acts on the set of points and the set of blocks with $t = \frac{v}{\Omega}$ orbits of length $\Omega$. Further, let $M$ be the orbit matrix induced by the action of the group $G$ on the design $\mathcal{D}$, and $C^{ext}$ be the corresponding extended code over $F_p$. If a prime $p$ divides $(k - \lambda)$, but $p^2 \nmid (k - \lambda)$ and $p \nmid k$, then $C^{ext}$ is **self-dual with respect to** $\psi$.

If $p^2 \mid (k - \lambda)$ we use a chain of codes to obtain a self-dual code from an orbit matrix.

Given an $m \times n$ integer matrix $A$, denote by $row_{\mathbf{F}}(A)$ the linear code over the field $\mathbf{F}$ spanned by the rows of $A$. By $row_p(A)$ we denote the $p$-ary linear code spanned by the rows of $A$.
For a given matrix $A$, we define, for any prime $p$ and nonnegative integer $i$,

$$\mathcal{M}_i(A) = \{x \in \mathbb{Z}^n : p^i x \in row_{\mathbb{Z}}(A)\}.$$

We have $\mathcal{M}_0(A) = row_{\mathbb{Z}}(A)$ and

$$\mathcal{M}_0(A) \subseteq \mathcal{M}_1(A) \subseteq \mathcal{M}_2(A) \subseteq \dots .$$

Let

$$C_i(A) = \pi_p(\mathcal{M}_i(A))$$

where $\pi_p$ is the homomorphism (projection) from $\mathbb{Z}^n$ onto $\mathbf{F}_p^n$ given by reading all coordinates modulo $p$. Then each $C_i(A)$ is a $p$-ary linear code of length $n$, $C_0(A) = row_p(A)$, and

$$C_0(A) \subseteq C_1(A) \subseteq C_2(A) \subseteq \dots .$$

## Theorem

Suppose $A$ is an $n \times n$ integer matrix such that $AUA^T = p^e V$ for some integer $e$, where $U$ and $V$ are square matrices with determinants relatively prime to $p$. Then $C_e(A) = \mathbf{F}_p^n$ and

$$C_j(A)^U = C_{e-j-1}(A), \quad \text{for} \quad j = 0, 1, \dots, e-1.$$

In particular, if $e = 2f + 1$, then $C_f(A)$ is a self-$U$-dual $p$-ary code of length $n$.

In the next theorem the previous result is used to associate a self-dual code to an orbit matrix of a symmetric design.

## Theorem [D. Crnković, SR, 2016]

Let $\mathcal{D}$ be a symmetric $(v, k, \lambda)$ design admitting an automorphism group $G$ that acts on the set of points and the set of blocks with $t = \frac{v}{\Omega}$ orbits of length $\Omega$. Suppose that $n = k - \lambda$ is exactly divisible by an odd power of a prime $p$ and $\lambda$ is exactly divisible by an even power of $p$, *e.g.* $n = p^e n_0$, $\lambda = p^{2a}\lambda_0$ where $e$ is odd, $a \geq 0$, and $(n_0, p) = (\lambda_0, p) = 1$. If $p \nmid \Omega$, then there exists a self-dual $p$-ary code of length $t + 1$ with respect to the scalar product corresponding to $U = diag(1, \ldots, 1, -\lambda_0\Omega)$.

If $\lambda$ is exactly divisible by an odd power of $p$, we apply the above case to the complement of the given symmetric design, which is a symmetric $(v, k', \lambda')$ design, where $k' = v - k$ and $\lambda' = v - 2k + \lambda$.

## Theorem [D. Crnković, SR, 2016]

Let $\mathcal{D}$ be a symmetric $(v, k, \lambda)$ design admitting an automorphism group $G$ that acts on the set of points and the set of blocks with $t = \frac{v}{\Omega}$ orbits of length $\Omega$. Suppose that $n = k - \lambda$ is exactly divisible by an odd power of a prime $p$ and $\lambda$ is also exactly divisible by an odd power of $p$, *e.g.* $n = p^e n_0$, $\lambda = p^{2a+1}\lambda_0$ where $e$ is odd, $a \geq 0$, and $(n_0, p) = (\lambda_0, p) = 1$. If $p \nmid \Omega$, then there exists a self-dual $p$-ary code of length $t + 1$ with respect to the scalar product corresponding to $U = diag(1, \ldots, 1, \lambda_0 n_0 \Omega)$.

# Divisible designs

An incidence structure with $v$ points, $b$ blocks and constant block size $k$ in which every point appears in exactly $r$ blocks is a **(group) divisible design** (GDD) with parameters $(v, b, r, k, \lambda_1, \lambda_2, m, n)$ whenever the point set can be partitioned into $m$ classes of size $n$, such that two points from the same class appear together in exactly $\lambda_1$ blocks, and two points from different classes appear together in exactly $\lambda_2$ blocks.

The following holds:

$$v = mn,\ bk = vr,\ (n-1)\lambda_1 + n(m-1)\lambda_2 = r(k-1),\ rk \geq v\lambda_2.$$

If $n \neq 1$ and $\lambda_1 \neq \lambda_2$, then a divisible design is called **proper**.

# Symmetric divisible designs

A GDD is called a **symmetric** GDD (SGDD) if $v = b$ (or, equivalently, $r = k$). It is then denoted by $D(v, k, \lambda_1, \lambda_2, m, n)$ and it follows that:

$$v = mn, \quad (n-1)\lambda_1 + n(m-1)\lambda_2 = k(k-1), \ k^2 \geq v\lambda_2.$$

A SGDD $D$ is said to have the **dual property** if the dual of $D$ (that is, the design with the transposed incidence matrix) is again a divisible design with the same parameters as $D$. This means that blocks of $D$ can be divided into sets $S_1, ..., S_m$, each set containing $n$ blocks, such that any two blocks belonging to the same set intersect in $\lambda_1$ points, and any two blocks belonging to different sets intersect in $\lambda_2$ points.

The point and the block partition from the definition of a SGDD with the dual property give us a partition (which will be called the **canonical partition**) of the incidence matrix

$$N = \begin{bmatrix} A_{11} & \cdots & A_{1m} \\ \vdots & \ddots & \vdots \\ A_{m1} & \cdots & A_{mm} \end{bmatrix},$$

where $A_{ij}$'s are square submatrices of order $n$.

$$
\left[\begin{array}{cccc|cccc|cccc|cccc}
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\
\hline
0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\
\hline
0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
\hline
0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0
\end{array}\right]
$$

(16,7,2,3,4,4) SGDD
(D. Crnković, H. Kharaghani, Divisible design digraphs, in: Algebraic Design Theory and Hadamard Matrices, (C. J. Colbourn, Ed.), Springer Proc. Math. Stat., Vol. 133, Springer, New York, 2015, 43-60.)

# Quotient matrices

We say that an $m \times m$ matrix $R = [r_{ij}]$ is a **quotient matrix** of a SGDD with the dual property if every element $r_{ij}$ is equal to the row sum of the block $A_{ij}$ of the canonical partition. If we denote the classes of points from the definition of a divisible design by $T_1, \dots, T_m$, and classes of blocks by $S_1, \dots, S_m$, then this means that each point of $T_i$ appears in exactly $r_{ij}$ blocks of $S_j$ and each block of $S_j$ contains exactly $r_{ij}$ points of $T_i$.

$$\begin{bmatrix} 1 & 2 & 2 & 2 \\ 2 & 1 & 2 & 2 \\ 2 & 2 & 1 & 2 \\ 2 & 2 & 2 & 1 \end{bmatrix}$$

# Codes from quotient matrices of SGDDs with the dual property

**Theorem** [D. Crnković, N. Mostarac, SR, 2016]

Let $D(v, k, \lambda_1, \lambda_2, m, n)$ be a *SGDD* with the dual property, and let $N$ be the incidence matrix of $D$. If $p$ is a prime such that $p \mid \lambda_1$, $p \mid k$ and $p \mid \lambda_2$, then the rows of $N$ span a self-orthogonal code of length $v$ over $\mathbb{F}_p$.

**Theorem** [D. Crnković, N. Mostarac, SR, 2016]

Let $D(v, k, \lambda_1, \lambda_2, m, n)$ be a *SGDD* with the dual property, and let $R$ be the quotient matrix of $D$. If $p$ is a prime such that $p \nmid (k^2 - v\lambda_2)$ and $p \nmid k$, then the linear code over $\mathbb{F}_p$ spanned by the rows of $R$ has dimension $m$.

**Theorem** [D. Crnković, N. Mostarac, SR, 2016]

Let $D(v, k, \lambda_1, \lambda_2, m, n)$ be a *SGDD* with the dual property and $R$ be the quotient matrix of $D$. If $p$ is a prime such that $p \nmid (k^2 - v\lambda_2)$ and $p \mid k$, then the linear code over $\mathbb{F}_p$ spanned by the rows of $R$ has dimension $m - 1$.

**Theorem** [D. Crnković, N. Mostarac, SR, 2016]

Let $D(v, k, \lambda_1, \lambda_2, m, n)$ be a *SGDD* with the dual property and let $R$ be the quotient matrix of $D$. If $p$ is a prime such that $p \mid (k^2 - v\lambda_2)$ and $p \mid n\lambda_2$, then the rows of $R$ span a self-orthogonal code of length $m$ over $\mathbb{F}_p$.

# Codes from extended quotient matrices

Let $D(v, k, \lambda_1, \lambda_2, m, n)$ be a *SGDD* with the dual property, and let $R$ be the quotient matrix of $D$. If a prime $p$ does not divide $n\lambda_2$, we can use a slightly different code then the one spanned by the quotient matrix $R$.

We define the extended quotient matrix

$$R^{ext} = \left[\begin{array}{ccc|c} & & & 1 \\ & R & & \vdots \\ & & & 1 \\ \hline n\lambda_2 & \cdots & n\lambda_2 & k \end{array}\right]$$

and the extended code $C^{ext}$ over $\mathbb{F}_p$ spanned by the rows of $R^{ext}$.

For $x = (x_1, \dots, x_{m+1})$ and $y = (y_1, \dots, y_{m+1})$ we define the scalar product $\psi$ by

$$\psi(x, y) = x_1 y_1 + \dots + x_m y_m - n\lambda_2 x_{m+1} y_{m+1}.$$

We know that $p \nmid n\lambda_2$, hence $\psi$ is a nondegenerate form on $\mathbb{F}_p$ (its matrix is non-singular).
If $x$ and $y$ are rows of the matrix $R^{ext}$, then

$$\psi(x, y) \in \{0, k^2 - v\lambda_2, -n\lambda_2(k^2 - v\lambda_2)\}.$$

Thus the extended code $C^{ext}$ over $\mathbb{F}_p$ is *self-orthogonal with respect to* $\psi$ if $p \mid (k^2 - v\lambda_2)$.

The matrix of the bilinear form $\psi$ will be denoted by $\Psi$.

**Theorem** [D. Crnković, N. Mostarac, SR, 2016]

Let $D(v, k, \lambda_1, \lambda_2, m, n)$ be a *SGDD* with the dual property, $R$ be the quotient matrix of $D$, and $C$ be the code over $\mathbb{F}_p$ spanned by the rows of $R$. If $p$ is a prime such that $p \mid (k^2 - v\lambda_2)$, then $dim(C) \leq \frac{m+1}{2}$.

- If $p \mid n\lambda_2$ then $C$ is self-orthogonal, hence $dim(C) \leq \frac{m}{2}$.
- If $p \nmid n\lambda_2$ then $C^{ext}$ is self-orthogonal with respect to $\psi$, $dim(C^{ext}) \leq \frac{m+1}{2}$, $dim(C) = dim(C^{ext})$ and $R$ and $R^{ext}$ have the same rank over $\mathbb{F}_p$.

**Theorem** [D. Crnković, N. Mostarac, SR, 2016]

Let $D(v, k, \lambda_1, \lambda_2, m, n)$ be a *SGDD* with the dual property, $R$ be the quotient matrix of $D$, and let $C^{ext}$ be the corresponding extended code over $\mathbb{F}p$. If $p$ is a prime such that $p \nmid n\lambda_2$, $p \mid (k^2 - v\lambda_2)$, but $p^2 \nmid (k^2 - v\lambda_2)$, then $C^{ext}$ is self-dual with respect to $\psi$.

- The inequality $dim(C^{ext}) \leq \frac{1}{2}(m+1)$ follows from the fact that $C^{ext}$ is self-orthogonal.
- In order to prove that $\frac{1}{2}(m+1) \leq dim(C^{ext})$, we have to show that $R^{ext}$ has $\mathbb{F}_p$-rank at least $\frac{1}{2}(m+1)$. (use of the Smith normal form)

If $p^2 \mid (k^2 - v\lambda_2)$ we can use a chain of codes to obtain a self-dual code from a quotient matrix.

**Theorem** [D. Crnković, N. Mostarac, SR, 2016]

Let $D(v, k, \lambda_1, \lambda_2, m, n)$ be a *SGDD* with the dual property. Suppose that $k^2 - v\lambda_2$ is exactly divisible by an odd power of a prime $p$ and $\lambda_2$ is exactly divisible by an even power of $p$, e.g. $k^2 - v\lambda_2 = p^e n_0$, $\lambda_2 = p^{2a}\lambda_0$, where $e$ is odd, $a \geq 0$ and $(n_o, p) = (\lambda_0, p) = 1$. If $p \nmid n$ then there exists a self-dual $p$-ary code of length $m + 1$ with respect to the scalar product corresponding to $U = diag(1, ..., 1, -n\lambda_0)$.

$$R_1^{ext} = \left[\begin{array}{ccc|c} & & & p^a \\ & R_1 & & \vdots \\ & & & p^a \\ \hline p^a n\lambda_0 & \cdots & p^a n\lambda_0 & k \end{array}\right].$$