



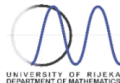
Orbit matrices of symmetric designs and related self-dual codes

(a joint work with Dean Crnković)

Sanja Rukavina
sanjar@math.uniri.hr

Department of Mathematics
University of Rijeka, Croatia

Symmetries and Covers of Discrete Objects
14 - 19 February 2016, Queenstown, New Zealand



Supported by CSF under the project 1637.

Orbit matrices
of symmetric
designs and
related
self-dual codes

Introduction

Orbit matrices
of symmetric
designs

Codes from
orbit matrices
of symmetric
designs

Self-dual
codes from
extended orbit
matrices



Orbit matrices
of symmetric
designs and
related
self-dual codes

Introduction

Orbit matrices
of symmetric
designs

Codes from
orbit matrices
of symmetric
designs

Self-dual
codes from
extended orbit
matrices

1 Introduction

Orbit matrices of symmetric designs

2 Codes from orbit matrices of symmetric designs

3 Self-dual codes from extended orbit matrices

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

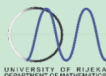
- 1 $|\mathcal{P}| = v$,
- 2 every element of \mathcal{B} is incident with exactly k elements of \mathcal{P} ,
- 3 every t elements of \mathcal{P} are incident with exactly λ elements of \mathcal{B} .

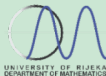
Every element of \mathcal{P} is incident with exactly r elements of \mathcal{B} .

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 $b \times v$ matrix $[m_{ij}]$ where b and v are the numbers of blocks and points respectively, such that $m_{ij} = 1$ if the point P_j and the block x_i are incident, and $m_{ij} = 0$ otherwise.



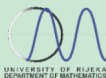


Let A be the incidence matrix of a design $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$. A **decomposition** of A is any partition B_1, \dots, B_s of the rows of A (blocks of \mathcal{D}) and a partition P_1, \dots, P_t of the columns of A (points of \mathcal{D}).

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

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

We say that a decomposition is **tactical** if the α_{ij} and β_{ij} are well defined (independent from the choice of $x \in B_i$ and $P \in P_j$, respectively).



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 a group called the full automorphism group of \mathcal{D} and is denoted by $Aut(\mathcal{D})$.

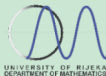
Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a symmetric (v, k, λ) design and $G \leq Aut(\mathcal{D})$. The group action of G produces the same number of point and block orbits. We denote that number by t , the G -orbits of points by $\mathcal{P}_1, \dots, \mathcal{P}_t$, G -orbits of blocks by $\mathcal{B}_1, \dots, \mathcal{B}_t$, and put $|\mathcal{P}_r| = \omega_r$, $|\mathcal{B}_i| = \Omega_i$, $1 \leq i, r \leq t$.

The **group action** of G induces a **tactical decomposition** of the incidence matrix of \mathcal{D} . Denote by γ_{ij} the number of points of \mathcal{P}_j incident with a representative of the block orbit \mathcal{B}_i . For these numbers the following equalities hold:

$$\sum_{j=1}^t \gamma_{ij} = k, \quad (1)$$

$$\sum_{i=1}^t \frac{\Omega_i}{\omega_j} \gamma_{ij} \gamma_{is} = \lambda \omega_s + \delta_{js} \cdot n, \quad (2)$$

where $n = k - \lambda$ is the order of the symmetric design \mathcal{D} .



Orbit matrices
of symmetric
designs and
related
self-dual codes

Introduction
Orbit matrices
of symmetric
designs

Codes from
orbit matrices
of symmetric
designs

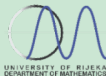
Self-dual
codes from
extended orbit
matrices

Definition 1

A $(t \times t)$ -matrix $M = (\gamma_{ij})$ with entries satisfying conditions (1) and (2) is called an **orbit matrix** for the parameters (v, k, λ) and orbit lengths distributions $(\omega_1, \dots, \omega_t)$, $(\Omega_1, \dots, \Omega_t)$.

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.



Codes from orbit matrices of symmetric designs

Orbit matrices
of symmetric
designs and
related
self-dual codes

Introduction

Orbit matrices
of symmetric
designs

Codes from
orbit matrices
of symmetric
designs

Self-dual
codes from
extended orbit
matrices

Theorem 1 [M. Harada, V. D. Tonchev, 2003]

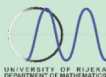
Let \mathcal{D} be a 2 - (v, k, λ) design with a **fixed-point-free** and **fixed-block-free automorphism** ϕ of order q , where q is prime. Further, let M be the orbit matrix induced by the action of the group $G = \langle \phi \rangle$ on the design \mathcal{D} . If p is a prime dividing r and λ then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

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

Theorem 1a

Let \mathcal{D} be a symmetric (v, k, λ) design admitting an automorphism group G that acts on the sets of points and blocks with $t = \frac{v}{\Omega}$ orbits of length Ω . 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 λ , then the rows of the matrix M span a self-orthogonal code of length t over \mathbf{F}_p .

Self-dual codes from extended orbit matrices



Orbit matrices
of symmetric
designs and
related
self-dual codes

Introduction

Orbit matrices
of symmetric
designs

Codes from
orbit matrices
of symmetric
designs

Self-dual
codes from
extended orbit
matrices

In the sequel we will study codes spanned by orbit matrices for a symmetric (v, k, λ) design and orbit lengths distribution (Ω, \dots, Ω) , 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 2

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, λ) 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 3 [D. Crnković, SR]

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

Theorem 1a

Let \mathcal{D} be a symmetric (v, k, λ) design admitting an automorphism group G that acts on the sets of points and blocks with $t = \frac{v}{\Omega}$ orbits of length Ω . 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 λ , 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 $b : V \times V \rightarrow \mathbf{F}$ be a symmetric bilinear form, i.e. a scalar product, and (e_1, \dots, 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 $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$, 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

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

For a linear p -ary code $C \subset \mathbf{F}_p^n$, the U -dual code of C is

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

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, λ) design \mathcal{D} with $t = \frac{v}{\Omega}$ orbits of length Ω , 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

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

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

Define the symmetric bilinear form ψ by

$$\psi(\bar{x}, \bar{y}) = x_1y_1 + \dots + x_t y_t - \lambda \Omega x_{t+1} y_{t+1},$$

for $\bar{x} = (x_1, \dots, x_{t+1})$ and $\bar{y} = (y_1, \dots, y_{t+1})$. Since $p \mid n$ and $p \nmid k$, it follows that $p \nmid \Omega$ and $p \nmid \lambda$. Hence ψ 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 ψ .

The matrix of the bilinear form ψ 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 4 [D. Crnković, SR]

Let \mathcal{D} be a symmetric (v, k, λ) 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 Ω . 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 ψ** .

Theorem 5

If there exists a self-dual p -ary code of length n with respect to a nondegenerate scalar product ψ , where p is an odd prime, then $(-1)^{\frac{n}{2}} \det(\psi)$ is a square in \mathbf{F}_p .

A direct consequence of Theorems 4 and 5 is the following theorem.

Theorem 6

Let \mathcal{D} be a symmetric (v, k, λ) 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 Ω . If an odd prime p divides $(k - \lambda)$, but $p^2 \nmid (k - \lambda)$ and $p \nmid k$, then $-\lambda\Omega(-1)^{\frac{t+1}{2}}$ is a square in \mathbf{F}_p .

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 $\text{row}_{\mathbf{F}}(A)$ the linear code over the field \mathbf{F} spanned by the rows of A . By $\text{row}_p(A)$ 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 ,

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

We have $\mathcal{M}_0(A) = \text{row}_{\mathbb{Z}}(A)$ 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 π_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 , $C_0(A) = \text{row}_p(A)$, and

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

Theorem 7

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

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

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 above result is used to associate a self-dual code to an orbit matrix of a symmetric design.

Theorem 8 [D. Crnković, SR]

Let \mathcal{D} be a symmetric (v, k, λ) 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 Ω . Suppose that $n = k - \lambda$ is exactly divisible by an odd power of a prime p and λ 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 $U = \text{diag}(1, \dots, 1, -\lambda_0 \Omega)$.

If λ 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', λ') design, where $k' = v - k$ and $\lambda' = v - 2k + \lambda$.

Theorem 9

Let \mathcal{D} be a symmetric (v, k, λ) 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 Ω . Suppose that $n = k - \lambda$ is exactly divisible by an odd power of a prime p and λ 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 $U = \text{diag}(1, \dots, 1, \lambda_0 n_0 \Omega)$.

As a consequence of Theorems 5, 8 and 9, we have

Theorem 10

Let \mathcal{D} be a symmetric (v, k, λ) 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 Ω . Suppose that p is an odd prime such that $n = p^e n_0$ and $\lambda = p^b \lambda_0$, where $(n_0, p) = (\lambda_0, p) = 1$, and $p \nmid \Omega$. Then

- $-(-1)^{(t+1)/2} \lambda_0 \Omega$ is a square (mod p) if b is even,
- $(-1)^{(t+1)/2} n_0 \lambda_0 \Omega$ is a square (mod p) if b is odd.

Similarly ...

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 λ_1 blocks, and two points from different classes appear together in exactly λ_2 blocks.

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

Theorem

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

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 λ_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 $(n_0, p) = (\lambda_0, p) = 1$. 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 $U = \text{diag}(1, \dots, 1, -n\lambda_0)$.



UNIVERSITY OF RIJEKA
DEPARTMENT OF MATHEMATICS

Orbit matrices
of symmetric
designs and
related
self-dual codes

Introduction

Orbit matrices
of symmetric
designs

Codes from
orbit matrices
of symmetric
designs

Self-dual
codes from
extended orbit
matrices

Thank you for your attention!