Self-dual codes from orbit matrices and quotient matrices of combinatorial designs

Nina Mostarac (nmavrovic@math.uniri.hr)
Dean Crnković (deanc@math.uniri.hr)

Department of Mathematics, University of Rijeka, Croatia

Supported by CSF, Grant 1637

Graphs, groups, and more: celebrating Brian Alspach's 80th and Dragan Marušič's 65th birthdays, Koper, Slovenia

June 1, 2018

Content

Content

Codes

Definition 1

Let p be a prime power. A p-ary linear code C of **length** n and **dimension** k is a k-dimensional subspace of the vector space $(\mathbb{F}_p)^n$.

- Notation: $[n, k]_p$ code or $[n, k]$ code

Definition 2

A **generating matrix** of a linear $[n, k]$ code is a $k \times n$ matrix whose rows are the basis vectors of the code.

Self-dual codes

Definition 3

Let $C \subseteq \mathbb{F}_p^n$ be a linear code. Its dual code is the code $C^\perp = \{x \in \mathbb{F}_p^n | x \cdot c = 0, \ \forall c \in C\}$, where $\cdot$ is the standard inner product. The code C is called self-orthogonal if $C \subseteq C^\perp$, and C is called self-dual if $C = C^\perp$.

Proposition 4

Let G be a generating matrix of a linear $[n, k, d]$ code C.

1. C is **self-orthogonal** $\Leftrightarrow GG^T = 0$.
2. C is **self-dual** $\Leftrightarrow$ it is self-orthogonal and $k = \dfrac{n}{2}$.

Self-dual codes

Definition 5

We may use a symmetric nonsingular matrix U over the field $\mathbb{F}_p$ to define a scalar product $\langle \cdot, \cdot \rangle_U$ for row vectors in $\mathbb{F}_p^n$: $\langle a, c \rangle_U = aUc^T$.
The U-dual code of a linear code C is the code

$$C^U = \{a \in \mathbb{F}_p^n \mid \langle a, c \rangle_U = 0, \ \forall c \in C\}.$$

A code C is called self-U-dual, or self-dual with respect to U, if $C = C^U$.

Content

Block designs

Definition 6

A **block design** or a $2-(v,k,\lambda)$ **design** is a finite incidence structure $\mathcal{D}=(\mathcal{P},\mathcal{B},\mathcal{I})$ such that $|\mathcal{P}|=v$, each block is incident with exactly k points and each pair of points is incident with exactly λ blocks.
If $v=b$, we say that a block design is **symmetric**.

Orbit matrices of block designs

- Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a 2-(v, k, λ) design and let $G \leq Aut(\mathcal{D})$.
- Denote with $P_1, ..., P_n$ G-orbits of points, and with $B_1, ..., B_m$ G-orbits of blocks and let $|P_i| = \omega_i$, $|B_j| = \Omega_j$, $1 \leq i \leq n$, $1 \leq j \leq m$.
- For $x \in \mathcal{B}$ and $Q \in \mathcal{P}$ we introduce the notation: $\langle x \rangle = \{R \in \mathcal{P} | (R, x) \in I\}$, $\langle Q \rangle = \{y \in \mathcal{B} | (Q, y) \in I\}$.
- Let $Q \in P_i$, $x \in B_j$. We will denote:

$$\Gamma_{ij} = |\langle Q \rangle \cap B_j|, \quad \gamma_{ij} = |\langle x \rangle \cap P_i|.$$

It holds: $\sum_{j=1}^{m} \Gamma_{ij} = r, \ \forall i \in \{1, ..., n\}, \qquad \sum_{i=1}^{n} \gamma_{ij} = k, \ \forall j \in \{1, ..., m\}.$

Definition 7

Matrices $S = [\Gamma_{ij}]$ and $R = [\gamma_{ij}]$ are called point and block orbit matrix of the design $\mathcal{D}$ induced by the action of the group G.

Lemma 8

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a block design, $G \leq Aut(\mathcal{D})$, and let ω_i, Ω_j, γ_{ij}, Γ_{ij} be defined as before. The following equations hold:

a) $\Omega_j \gamma_{ij} = \omega_i \Gamma_{ij}$;

b) $\sum_{j=1}^{m} \Gamma_{ij}\gamma_{sj} = \lambda\omega_s + \delta_{is} \cdot (r - \lambda), \ \ i, s \in \{1, ..., n\}$.

Proposition 9

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a block design, $G \leq Aut(\mathcal{D})$, and let ω_i, Ω_j, γ_{ij}, Γ_{ij} be defined as before. The following equations hold:

1. $\sum_{i=1}^{n} \gamma_{ij} = k$;
2. $\sum_{j=1}^{m} \frac{\Omega_j}{\omega_i} \gamma_{ij}\gamma_{sj} = \lambda\omega_s + \delta_{is} \cdot (r - \lambda)$.

Content

SGDD

Definition 10

A (group) divisible design (GDD) with parameters $(v, b, r, k, \lambda_1, \lambda_2, m, n)$ is an incidence structure with v points, b blocks and constant block size k in which every point appears in exactly r blocks and whose 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,
- two points from different classes appear together in exactly λ_2 blocks.

For the parameters of a GDD it holds:

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

SGDD

Definition 11

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

Definition 12

A SGDD $\mathcal{D}$ is said to have the dual property if the dual of $\mathcal{D}$ is again a divisible design with the same parameters as $\mathcal{D}$.

Quotient matrices of SGDDs with the dual property

The point and the block partition from the definition of a SGDD with the dual property give us a canonical partition of the incidence matrix:

$$N = \begin{bmatrix} A_{11} & \cdots & A_{1m} \\ \vdots & \ddots & \vdots \\ A_{m1} & \cdots & A_{mm} \end{bmatrix}, \text{ where } A_{ij}\text{'s are square submatrices of order } n.$$

$$\Rightarrow NN^T = \begin{bmatrix} B_{11} & \cdots & B_{1m} \\ \vdots & \ddots & \vdots \\ B_{m1} & \cdots & B_{mm} \end{bmatrix}, \ B_{ij} = [(k-\lambda_1)I_n + (\lambda_1 - \lambda_2)J_n]\delta_{ij} + \lambda_2 J_n$$

Quotient matrices of SGDDs with the dual property

Remark 1

Each block A_{ij} has constant row (and block) sum.

Definition 13

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 above canonical partition.

It holds: $RR^T = (k^2 - v\lambda_2)I_m + n\lambda_2 J_m.$

Content

Wilson describes the following result of Blokhuis and Calderbank:

Theorem 4.1

Let $\mathcal{D}$ be a 2-(v, k, λ) design and p an odd prime which exactly divides $r - \lambda$ (that is $p|(r-\lambda)$, but $p^2 \nmid (r-\lambda)$). Suppose that $|S \cap T| \equiv k (mod\ p)$ for every two blocks S and T of the design and that v is odd. Then:

1. *if $k \not\equiv 0 (mod\ p)$, then there exists a self-dual p-ary code of length $v+1$ with respect to $U = diag(1, ..., 1, -k)$;*
2. *if $k \equiv 0 (mod\ p)$, then there exists a self-dual p-ary code of length $v+1$ with respect to $U' = diag(1, ..., 1, -v)$.*

Sketch of the proof:

Let N be a $v \times b$ incidence matrix for $\mathcal{D}$.

$$M = \left[\begin{array}{c|c} N^T & \begin{array}{c} 1 \\ \vdots \\ 1 \end{array} \end{array} \right], \quad M' = \left[\begin{array}{c|c} N^T & \begin{array}{c} 0 \\ \vdots \\ 0 \end{array} \\ \hline 1 \ \cdots \ 1 & 1 \end{array} \right] \ldots$$

Theorem 4.2 (Crnković, Mostarac)

Let $\mathcal{D}$ be a 2-(v,k,λ) design, $G \leq Aut(\mathcal{D})$, and let ω_i, Ω_j, γ_{ij}, Γ_{ij} be defined as before. Let p be a prime such that $p|(r-\lambda)$, and $p \nmid \Omega_1, ..., \Omega_m, \omega_1, ..., \omega_n$. Then the following holds:

1. *if $p \nmid \lambda$ then there exists a self-orthogonal p-ary code of length $m+1$ with respect to $U = diag(\Omega_1, ..., \Omega_m, -\lambda)$;*
2. *if $p|\lambda$ and $p \nmid b$ then there exists a self-orthogonal p-ary code of length $m+1$ with respect to $V = diag(\Omega_1, ..., \Omega_m, -b)$.*

Sketch of the proof:

Let R be a block orbit matrix for $\mathcal{D}$ induced by the action of G.

$$M = \left[\begin{array}{c|c} & \omega_1 \\ & \omega_2 \\ R & \vdots \\ & \omega_n \end{array}\right] \quad \text{and} \quad M' = \left[\begin{array}{ccc|c} & & & 0 \\ & R & & \vdots \\ & & & 0 \\ \hline 1 & \cdots & 1 & 1 \end{array}\right] \ldots$$

□

Self-orthogonal codes from orbit matrices of block designs

Theorem 4.3 (Crnković, Mostarac)

Let $\mathcal{D}$ be a 2-(v, k, λ) design which admits an automorphism group G acting on $\mathcal{D}$ with all orbits of the same size w, and let R be an orbit matrix induced by the action of the group G on the design $\mathcal{D}$. If all the block intersection numbers of the design (including k) are divisible by p, where p is a prime, then the matrix R^T spans a self-orthogonal code of length $\frac{v}{w}$ over $\mathbb{F}_p$.

Theorem 4.4 (Crnković, Mostarac)

Let $\mathcal{D}$ be a 2-(v, k, λ) design which admits an automorphism group G acting on $\mathcal{D}$ with all orbits of the same length q, and let R be an orbit matrix induced by the action of the group G on $\mathcal{D}$. Let p be a prime such that $p|(r-\lambda)$ but $p^2 \nmid (r-\lambda)$, and $p \nmid q$. If the number of point orbits n is odd, and all the block intersection numbers of $\mathcal{D}$ (including k) are congruent modulo p, then:

1. *if $p \nmid k$ then there exists a self-dual p-ary code of length $n+1$ with respect to $U = diag(q, ..., q, -k)$;*
2. *if $p|k$ then there exists a self-dual p-ary code of length $n+1$ with respect to $V = diag(1, ..., 1, -n)$.*

Sketch of the proof:

$$M = \left[\begin{array}{c|c} R^T & \begin{array}{c} q \\ \vdots \\ q \end{array} \end{array} \right] \text{ and } M' = \left[\begin{array}{ccc|c} & R^T & & \begin{array}{c} 0 \\ \vdots \\ 0 \end{array} \\ \hline 1 & \cdots & 1 & 1 \end{array} \right] \ldots$$

Codes from symmetric block designs

- Assmus, Mezzaroba and Salwach used incidence matrices of symmetric designs to obtain **self-dual codes.**

Theorem 4.5 (E. F. Assmus, Jr., J. A. Mezzaroba, C. J. Salwach)

Let p be a prime and $\mathcal{D}$ a ***symmetric*** *(v,k,λ)-design with an incidence matrix M.*

1. *If $p|k$ and $p|\lambda$, then the rows of M span a* ***self-orthogonal*** *code over $\mathbb{F}_p$.*
2. *Let $p|(k-\lambda)$ and $p\nmid k$, and let a $v\times(v+1)$ matrix G be defined as follows:*

$$G = \left[\begin{array}{c|c} \sqrt{-k} & \\ \vdots & M \\ \sqrt{-k} & \end{array}\right].$$

   If $-k$ is a quadratic residue mod p let $\mathbb{F}=\mathbb{F}_p$, if not let $\mathbb{F}=\mathbb{F}_{p^2}$. Then the rows of G span a ***self-orthogonal*** *code over $\mathbb{F}$, and if $p^2\nmid(k-\lambda)$ the code is* ***self-dual****.*
3. *If $p|\lambda$ and $p|(k+1)$, then the rows of a $v\times 2v$ matrix G span a* ***self-dual*** *$[2v,v]$ code over $\mathbb{F}_p$, where $G=\left[\begin{array}{c|c} I & M\end{array}\right]$.*
4. *If $p=2$, λ is odd, and k even, then the rows of a $(v+1)\times(2v+2)$ matrix G span a* ***self-dual*** *$[2v+2,v+1]$ code over $\mathbb{F}_2$, where G is defined as:*

$$G = \left[\begin{array}{c|cccc} & 0 & 1 & \cdots & 1 \\ & 1 & & & \\ I & \vdots & & M & \\ & 1 & & & \end{array}\right].$$

Codes from symmetric designs

- Instead of using incidence matrices of symmetric designs we will use **orbit matrices** of **symmetric designs** to obtain self-dual codes.
- We will assume an automorphism group of a symmetric design that acts on the set of points and on the set of blocks with all the orbits of the same lenght.

Theorem 4.6 (Crnković, Mostarac)

Let $\mathcal{D}$ be a symmetric (v,k,λ)-design which admits the automorphism group G that acts on the set of points and on the set of blocks with $t = \frac{v}{\Omega}$ orbits of length Ω. Let R be the ***orbit matrix*** *of the design $\mathcal{D}$ induced by the action of the group G, and p a prime.*

1. *If $p|k$ and $p|\lambda$, then the rows of R span a self-orthogonal code of length t over $\mathbb{F}_p$.*
2. *Let $p|(k-\lambda)$, $p \nmid k\Omega$, and let a $t \times (t+1)$ matrix G be defined as:*

$$G = \begin{bmatrix} \sqrt{-k\Omega} & \\ \vdots & R \\ \sqrt{-k\Omega} & \end{bmatrix}.$$

If $-k\Omega$ is a quadratic residue modulo p, then let $\mathbb{F} = \mathbb{F}_p$, otherwise let $\mathbb{F} = \mathbb{F}_{p^2}$. Then the rows of G span a ***self-orthogonal*** *code over $\mathbb{F}$. Furthermore, if $p^2 \nmid (k-\lambda)$, this code is a self-dual $[t+1, \frac{t+1}{2}]$ code.*

Codes from symmetric designs

Theorem 4.6 continued.

3. If $p|\lambda$ and $p|(k+1)$, then the rows of a $t \times 2t$ matrix $G = \begin{bmatrix} I & & R \end{bmatrix}$ G span a self-dual $[2t, t]$ code over $\mathbb{F}_p$.
4. If $p = 2$, λ is odd, k is even, and Ω odd, then the rows of a $(t+1) \times (2t+2)$ matrix G span a self-dual $[2t+2, t+1]$ code over $\mathbb{F}_2$, where G is defined as:

$$G = \begin{bmatrix} & 0 & 1 & \cdots & 1 \\ & 1 & & & \\ I & \vdots & & R & \\ & 1 & & & \end{bmatrix}.$$

□

Codes from SGDDs with the dual property

- We will also use **quotient matrices** of SGDDs with the dual property to obtain **self-dual codes**.

Theorem 4.7 (Crnković, Mostarac)

Let $D = (v, k, \lambda_1, \lambda_2, m, n)$ be a SGDD with the dual property, with the ***quotient matrix*** *R, and let p be a prime.*

1. *If $p \mid (k^2 - v\lambda_2)$ and $p \mid n\lambda_2$, then the rows of R span a self-orthogonal code of lenght m over $\mathbb{F}_p$.*
2. *Let $p|(k^2 - v\lambda_2)$, $p \nmid n\lambda_2$, and let an $m \times (m+1)$ matrix G be equal to:*

$$G = \begin{bmatrix} \sqrt{-n\lambda_2} & & \\ \vdots & & R \\ \sqrt{-n\lambda_2} & & \end{bmatrix}.$$

If $-n\lambda_2$ is a quadratic residue modulo p, then let $\mathbb{F} = \mathbb{F}_p$, otherwise let $\mathbb{F} = \mathbb{F}_{p^2}$. Then the rows of G span a ***self-orthogonal*** *code over $\mathbb{F}$. Furthermore, if $p^2 \nmid (k^2 - v\lambda_2)$ and $p \nmid k$, then this code is a self-dual $[m+1, \frac{m+1}{2}]$ code.*

Codes from SGDDs with the dual property

Theorem 4.7 continued.

3. If $p|n\lambda_2$ and $p|(k^2+1)$, then the rows of an $m \times 2m$ matrix G span a self-dual $[2m, m]$ code over $\mathbb{F}_p$, where $G = \begin{bmatrix} I & R \end{bmatrix}$.
4. If $p = 2$, k is even, and m, n and λ_2 are odd, then the rows of an $(m+1) \times (2m+2)$ matrix G span a self-dual $[2m+2, m+1]$ code over $\mathbb{F}_2$, where G is defined as:

$$G = \begin{bmatrix} & 0 & 1 & \cdots & 1 \\ & 1 & & & \\ I & \vdots & & R & \\ & 1 & & & \end{bmatrix}.$$

□

Thank you for your attention! ;)