Using groups to construct combinatorial structures and codes

Ronan Egan
Joint work with Dean Crnković and Andrea Švob

SVEUČILIŠTE U RIJECI
ODJEL ZA MATEMATIKU

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

Block designs

A 2-(v, k, λ) design is a finite incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$, where $\mathcal{P}$ and $\mathcal{B}$ are disjoint sets and $I \subseteq \mathcal{P} \times \mathcal{B}$ with the following properties:

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

Block designs

A 2-(v, k, λ) design is a finite incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$, where $\mathcal{P}$ and $\mathcal{B}$ are disjoint sets and $I \subseteq \mathcal{P} \times \mathcal{B}$ with the following properties:

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

An automorphism of a block design $\mathcal{D}$ is determined by its action on the set of points or the set of blocks. The set of all automorphisms of $\mathcal{D}$ is denoted $\mathrm{Aut}(\mathcal{D})$.

Orbit structures

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ be a 2-(v, k, λ) design and $G \leq \mathrm{Aut}(\mathcal{D})$. Denote the G-orbits of points by $\mathcal{P}_1, \ldots, \mathcal{P}_n$, the G-orbits of blocks by $\mathcal{B}_1, \ldots, \mathcal{B}_m$, and put $|\mathcal{P}_r| = \omega_r$ and $|\mathcal{B}_i| = \Omega_i$, for $1 \leq r \leq n$, $1 \leq i \leq m$.

Orbit structures

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ be a 2-(v, k, λ) design and $G \leq \mathrm{Aut}(\mathcal{D})$. Denote the G-orbits of points by $\mathcal{P}_1, \ldots, \mathcal{P}_n$, the G-orbits of blocks by $\mathcal{B}_1, \ldots, \mathcal{B}_m$, and put $|\mathcal{P}_r| = \omega_r$ and $|\mathcal{B}_i| = \Omega_i$, for $1 \leq r \leq n$, $1 \leq i \leq m$.

For $x \in \mathcal{B}$ and $P \in \mathcal{P}$, let $\langle x \rangle = \{Q \in \mathcal{P} \mid (Q, x) \in I\}$ and $\langle P \rangle = \{y \in \mathcal{B} \mid (P, y) \in I\}$.

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ be a 2-(v, k, λ) design and $G \leq \mathrm{Aut}(\mathcal{D})$. Denote the G-orbits of points by $\mathcal{P}_1, \ldots, \mathcal{P}_n$, the G-orbits of blocks by $\mathcal{B}_1, \ldots, \mathcal{B}_m$, and put $|\mathcal{P}_r| = \omega_r$ and $|\mathcal{B}_i| = \Omega_i$, for $1 \leq r \leq n$, $1 \leq i \leq m$.

For $x \in \mathcal{B}$ and $P \in \mathcal{P}$, let $\langle x \rangle = \{Q \in \mathcal{P} \mid (Q, x) \in I\}$ and $\langle P \rangle = \{y \in \mathcal{B} \mid (P, y) \in I\}$.

Let $x \in \mathcal{B}_i$ and $P \in \mathcal{P}_r$, and $g \in G$. Then define $\gamma_{ir} = |\langle x \rangle \cap \mathcal{P}_r| = |\langle x \rangle g \cap \mathcal{P}_r g| = |\langle xg \rangle \cap \mathcal{P}_r|$. Similarly let $\Gamma_{ir} = |\langle P \rangle \cap \mathcal{B}_r|$.

Orbit structures

The $(m \times n)$ matrix $[\gamma_{ir}]$ is called the orbit structure for parameters (v, k, λ) and orbit distribution $(\omega_1, \ldots, \omega_n),\ (\Omega_1, \ldots, \Omega_m)$.

The set of indices of points of the orbit $\mathcal{P}_r$ indicating which points of $\mathcal{P}_r$ are incident with the representative of the block orbit $\mathcal{B}_i$ is called the index set for the position (i, r) of the orbit structure.

Constructing designs with presumed automorphism group

Construction of block designs admitting an action of the presumed automorphism group consists of two basic steps:

1. Construction of orbit structures for the given automorphism group.
2. Construction of block designs for the orbit structures obtained in this way. This step is often called an indexing of orbit structures.

Example

Construction of a symmetric $(66, 26, 10)$ design $\mathcal{D}$ admitting the automorphism group $\mathbb{Z}_{55}$.

Example

Construction of a symmetric $(66, 26, 10)$ design $\mathcal{D}$ admitting the automorphism group $\mathbb{Z}_{55}$.

The only possible orbit distribution for $\mathbb{Z}_{55}$ is $(11, 55)$. The resulting orbit structure is

$$\begin{array}{c|cc} OS & 11 & 55 \\ \hline 11 & 1 & 25 \\ 55 & 5 & 21 \end{array}.$$

There are $\binom{55}{25}$ ways to index position $(1, 2)$. To simplify the problem, we consider the subgroup $\mathbb{Z}_{11}$.

$OS1$	11	11	11	11	11	11
11	1	5	5	5	5	5
11	5	5	5	5	5	1
11	5	5	5	5	1	5
11	5	5	5	1	5	5
11	5	5	1	5	5	5
11	5	1	5	5	5	5

.

$$\begin{array}{c|cccccc} OS1 & 11 & 11 & 11 & 11 & 11 & 11 \\ \hline 11 & 1 & 5 & 5 & 5 & 5 & 5 \\ 11 & 5 & 5 & 5 & 5 & 5 & 1 \\ 11 & 5 & 5 & 5 & 5 & 1 & 5 \\ 11 & 5 & 5 & 5 & 1 & 5 & 5 \\ 11 & 5 & 5 & 1 & 5 & 5 & 5 \\ 11 & 5 & 1 & 5 & 5 & 5 & 5 \end{array}.$$

Possible index sets are the 1-subsets and 5-subsets of $\{0, 1, \ldots, 10\}$. Labeled with the integers from 0-472, the only design up to isomorphism is

$$\begin{bmatrix} 0 & 280 & 280 & 280 & 280 & 280 \\ 20 & 20 & 450 & 450 & 20 & 5 \\ 20 & 450 & 450 & 20 & 5 & 20 \\ 20 & 450 & 20 & 5 & 20 & 450 \\ 20 & 20 & 5 & 20 & 450 & 450 \\ 20 & 5 & 20 & 450 & 450 & 20 \end{bmatrix}.$$

Some outcomes

- There are at least 413 symmetric $(78, 22, 6)$ designs; Crnković, Dumičić Danilović, Rukavina.
- There are exactly 4285 symmetric $(45, 12, 3)$ designs that admit nontrivial automorphisms; Crnković, Dumičić Danilović, Rukavina.
- A construction of Menon designs with parameters $(784, 378, 182)$ and $(900, 435, 210)$; Crnković.

Linear codes

A q-ary *linear code* C of dimension k for a prime power q, is a k-dimensional subspace of a vector space $\mathbb{F}_q^n$. Elements of C are called codewords.

Let $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n) \in \mathbb{F}_q^n$. The *Hamming distance* between words x and y is the number $d(x, y) = |\{i : x_i \neq y_i\}|$. The *minimum distance* of the code C is defined by $d = \min\{d(x, y) : x, y \in C,\ x \neq y\}$. The *weight* of a codeword x is $w(x) = d(x, 0) = |\{i : x_i \neq 0\}|$. For a linear code, $d = \min\{w(x) : x \in C, x \neq 0\}$.

For such code we write $[n, k, d]_q$ linear code.

Linear codes

The *dual* code $C^\perp$ is the orthogonal complement under the standard inner product $\langle \cdot\,, \cdot \rangle$, i.e. $C^\perp = \{v \in \mathbb{F}_q^n | \langle v, c \rangle = 0 \text{ for all } c \in C\}$.

Linear codes

The *dual* code $C^{\perp}$ is the orthogonal complement under the standard inner product $\langle \cdot\,, \cdot \rangle$, i.e. $C^{\perp} = \{v \in \mathbb{F}_q^n | \langle v, c \rangle = 0 \text{ for all } c \in C\}$.

Analogously, the *Hermitian dual* code C^H is the orthogonal complement under the Hermitian inner product, $\langle x\,, y \rangle_H = \sum_{i=1}^{n} x_i y_i^*$ where $a^* = a^{-1}$ for all $a \in \mathbb{F}_q \setminus \{0\}$ and $0^* = 0$.

The *dual* code $C^\perp$ is the orthogonal complement under the standard inner product $\langle \cdot\,,\cdot \rangle$, i.e. $C^\perp = \{v \in \mathbb{F}_q^n | \langle v, c\rangle = 0 \text{ for all } c \in C\}$.

Analogously, the *Hermitian dual* code C^H is the orthogonal complement under the Hermitian inner product, $\langle x\,, y\rangle_H = \sum_{i=1}^n x_i y_i^*$ where $a^* = a^{-1}$ for all $a \in \mathbb{F}_q \setminus \{0\}$ and $0^* = 0$.

A code C is *self-orthogonal* if $C \subseteq C^\perp$ and *self-dual* if $C = C^\perp$. It is *Hermitian self-orthogonal* if $C \subseteq C^H$ and *Hermitian self-dual* if $C = C^H$.

Combinatorial structures

Let W be an $n \times n$ matrix with entries in $\{0, \pm 1\}$. If $WW^{\top} = mI_n$ over the integers, W is a *weighing matrix* $\mathrm{W}(n, m)$. If $m = n$, W is a *Hadamard matrix* $\mathrm{H}(n)$.

Let W be an $n \times n$ matrix with entries in $\{0, \pm 1\}$. If $WW^\top = mI_n$ over the integers, W is a *weighing matrix* $\mathrm{W}(n, m)$. If $m = n$, W is a *Hadamard matrix* $\mathrm{H}(n)$.

Let $\zeta_k = e^{2\pi i/k}$. An $n \times n$ matrix with entries in $\{0\} \cup \langle \zeta_k \rangle$ such that $WW^* = mI_n$ where $[W_{ij}]^* = [W_{ji}^*]$, is a *complex generalized weighing matrix* $\mathrm{CGW}(n, m, k)$.

Combinatorial structures

Let W be an $n \times n$ matrix with entries in $\{0, \pm 1\}$. If $WW^\top = mI_n$ over the integers, W is a *weighing matrix* $\mathrm{W}(n, m)$. If $m = n$, W is a *Hadamard matrix* $\mathrm{H}(n)$.

Let $\zeta_k = e^{2\pi i/k}$. An $n \times n$ matrix with entries in $\{0\} \cup \langle \zeta_k \rangle$ such that $WW^* = mI_n$ where $[W_{ij}]^* = [W_{ji}^*]$, is a *complex generalized weighing matrix* $\mathrm{CGW}(n, m, k)$.

If W has entries in $\mathbb{F}_q$ and $WW^* = mI_n$, then we call W a $\mathbb{F}_q$*-weighing matrix* $\mathrm{W}(n, m; \mathbb{F}_q)$.

Combinatorial structures

A graph $\mathcal{G}$ is strongly regular of type (v, k, λ, μ) if it has v vertices, each of degree k, such that any two adjacent (non-adjacent) vertices are both adjacent to λ (μ) common vertices.

A graph $\mathcal{G}$ is strongly regular of type (v, k, λ, μ) if it has v vertices, each of degree k, such that any two adjacent (non-adjacent) vertices are both adjacent to λ (μ) common vertices.

Let A be the adjacency matrix of $\mathcal{G}$.

- The *Seidel matrix* of $\mathcal{G}$ is $S = J - I - 2A$.
- The *Laplacian matrix* of $\mathcal{G}$ is $L = kI - A$.
- The *signless Laplacian matrix* of $\mathcal{G}$ is $L = kI + A$.

$$M^2_{i,j} = \begin{cases} \alpha, & i = j \\ \beta, & v_i \sim v_j, \\ \pi, & v_i \nsim v_j \end{cases} \qquad M \in \{S, L, |L|\}.$$

Orbit matrices

Let M be an $n \times n$ matrix with entries in some set X. A *permutation automorphism* of M is a pair of $n \times n$ permutation matrices (P, Q) such that $PMQ^\top = M$. The set of all such pairs form the *permutation automorphism group* of M, denoted $\mathrm{PAut}(M)$ under the composition $(P_1, Q_1)(P_2, Q_2) = (P_1 P_2, Q_1 Q_2)$. Any permutation automorphism group $G \leq \mathrm{PAut}(M)$ acts on rows and columns of M.

Orbit matrices

Let M be an $n \times n$ matrix with entries in some set X. A *permutation automorphism* of M is a pair of $n \times n$ permutation matrices (P, Q) such that $PMQ^\top = M$. The set of all such pairs form the *permutation automorphism group* of M, denoted $\mathrm{PAut}(M)$ under the composition $(P_1, Q_1)(P_2, Q_2) = (P_1 P_2, Q_1 Q_2)$. Any permutation automorphism group $G \leq \mathrm{PAut}(M)$ acts on rows and columns of M.

Let G be a permutation automorphism group of an integer matrix $M = [m_{ij}]$, acting in t orbits on the set of rows and the set of columns of M. Denote the G-orbits on rows and columns of M by $\mathcal{R}_1, \ldots, \mathcal{R}_t$ and $\mathcal{C}_1, \ldots, \mathcal{C}_t$, respectively, and put $|\mathcal{R}_i| = \Omega_i$ and $|\mathcal{C}_i| = \omega_i$, $i = 1, \ldots, t$.

Orbit matrices

Let M_{ij} be the submatrix of M consisting of the rows belonging to the row orbit $\mathcal{R}_i$ and the column belonging to $\mathcal{C}_j$. We denote by Γ_{ij} and γ_{ij} the sum of a row and column of M_{ij}, respectively.

The $t \times t$ matrix $R = [\Gamma_{ij}]$ is called a *row orbit matrix* of M with respect to G. The $t \times t$ matrix $C = [\gamma_{ij}]$ is called a *column orbit matrix* of M with respect to G.

When M is an $\mathbb{F}_q$-matrix, orbit sizes Ω_i and ω_i will often be associated with their value modulo the characteristic of $\mathbb{F}_q$.

Orthogonality

Lemma

Let G be a permutation automorphism group of a weighing matrix $W = [w_{ij}]$ of order n and weight m, and let $\mathcal{R}_1, \ldots, \mathcal{R}_t$ and $\mathcal{C}_1, \ldots, \mathcal{C}_t$ be the G-orbits on the rows and columns of the matrix W, respectively. Then

$$\sum_{j=1}^{t} \Gamma_{ij}\gamma_{sj} = \delta_{is} m,$$

where δ_{is} is the Kronecker delta.

Orthogonality

Theorem

Let G be a permutation automorphism group of a weighing matrix W of order n and weight m, and let $\mathcal{R}_1, \dots, \mathcal{R}_t$ and $\mathcal{C}_1, \dots, \mathcal{C}_t$ be the G-orbits on the rows and columns of the matrix W, respectively. Then

$$\sum_{j=1}^{t} \frac{\Omega_s}{\omega_j} \Gamma_{ij} \Gamma_{sj} = \delta_{is} m,$$

where δ_{is} is the Kronecker delta.

Orthogonality for weighing matrices

Theorem

Let W be a $\mathrm{W}(n, m)$ and G be a permutation automorphism group of W acting with all orbits of the same length w. Further, let R be the row orbit matrix of W with respect to G. If p is a prime dividing m, and $q = p^r$ is a prime power, then the linear code spanned by the matrix R over the field $\mathbb{F}_q$ is a self-orthogonal code of length t.

Orthogonality for weighing matrices

Theorem

Let W be a $\mathrm{W}(n,m)$, G be a permutation automorphism group of W, and R the corresponding row orbit matrix. Further, let ω_j, $j = 1, \ldots, t$, be the lengths of the G-orbits on columns of W, and $w \in \{\omega_j |\ j = 1, \ldots, t\}$. Let $q = p^r$ be a prime power, where p is a prime dividing m, and let the lengths of the column G-orbits of H have a property that $p\omega_j | w$ if $\omega_j < w$, and $pw | \omega_j$ if $w < \omega_j$. Then the submatrix of R corresponding to row orbits and column orbits of length w spans a self-orthogonal code over $\mathbb{F}_q$.

Orthogonality for weighing matrices

The submatrix of an orbit matrix R corresponding to the fixed rows and fixed columns is called the fixed part of the orbit matrix R. The submatrix of R corresponding to the orbits of rows and columns of lengths greater than 1 is called the non-fixed part of the orbit matrix R.

Corollary

Let W be a $\mathrm{W}(n, m)$, G be a permutation automorphism group of W, and R the corresponding row orbit matrix. Further, let ω_j, $j = 1, \ldots, t$, be the lengths of the G-orbits on columns of W, and p be a prime that divides ω_j if $\omega_j > 1$. Then the rows of the fixed part of R span a self-orthogonal code over the field $\mathbb{F}_q$, where $q = p^r$.

Codes from symmetric conference matrices

q	$G \leq \mathrm{PAut}(W)$	C	$\mathrm{Dual}(C)$	$\lvert\mathrm{Aut}(C)\rvert$
25	Z_2	$[10,6,4]_5$ *	$[10,4,6]_5$ *	480
25	Z_2	$[12,5,6]_5$ *	$[12,7,4]_5$ *	576
25	Z_3	$[8,3,4]_5$	$[8,5,2]_5$	1536
81	Z_2	$[36,10,16]_3$ *	$[36,26,6]_3$ *	2880
81	Z_2	$[40,8,20]_3$	$[40,32,4]_3$	640
81	Z_3	$[27,5,15]_3$	$[27,22,3]_3$	2592
81	Z_4	$[20,4,10]_3$	$[20,16,2]_3$	8
81	Z_4	$[16,6,6]_3$	$[16,10,4]_3$ *	64
81	Z_4	$[18,6,8]_3$	$[18,12,4]_3$ *	48
81	Z_6	$[13,2,7]_3$	$[13,11,2]_3$ *	207360
81	Z_8	$[10,2,5]_3$	$[10,8,2]_3$ *	115200
125	Z_2	$[62,14,31]_5$ *	$[62,48,8]_5$*	1488
125	Z_3	$[40,11,20]_5$ *	$[40,29,6]_5$	480
125	Z_5	$[25,4,19]_5$ *	$[25,21,4]_5$ *	4800
125	Z_{10}	$[12,2,9]_5$	$[12,10,2]_5$ *	41472
125	Z_{15}	$[8,2,6]_5$ *	$[8,6,2]_5$ *	512

Table: Self-orthogonal codes constructed from non-fixed parts of orbit matrices

Codes from orbit matrices of an $\mathbb{F}_4$-weighing matrix

We obtain a $\mathrm{W}(72, 72; \mathbb{F}_4)$ from a $\mathrm{CGW}(72, 72, 3)$ and construct orbit matrices.

$G \leq \mathrm{PAut}(W)$	C	$\mathrm{Dual}(C)$	$\lvert\mathrm{Aut}(C)\rvert$
Z_2	$[12, 3, 8]*$	$[12, 9, 2]$	$2^9 \cdot 3^3 \cdot 5^1$
Z_2	$[30, 6, 16]$	$[30, 24, 3]$	$2^5 \cdot 3^4 \cdot 5^2$
Z_2	$[34, 8, 8]$	$[34, 26, 2]$	2304
Z_2	$[24, 6, 8]$	$[24, 18, 2]$	$2^{19} \cdot 3^4$
Z_4	$[14, 3, 4]$	$[14, 11, 2]$	$2^{10} \cdot 3^4 \cdot 5^1$
Z_4	$[10, 2, 8]*$	$[10, 8, 2]*$	5760

Table: Hermitian self-orthogonal codes over $\mathbb{F}_4$ constructed from fixed and non-fixed parts of orbit matrices

Codes from orbit matrices of Seidel matrices

Let $\mathcal{G}$ be a strongly regular graph with parameters (136,72,36,40).

$G \leq \mathrm{PAut}(\mathcal{G})$	C	$\mathrm{Dual}(C)$
Z_3	$[8, 2, 6]_3*$	$[8, 6, 2]_3*$
Z_3	$[36, 14, 12]_3$	$[36, 22, 6]_3$
Z_3	$[28, 7, 12]_3$	$[28, 21, 4]_3*$
Z_3	$[10, 4, 6]_3*$	$[10, 6, 4]_3*$
Z_3	$[42, 15, 12]_3$	$[42, 27, 4]_3$
Z_3	$[45, 15, 12]_3$	$[45, 30, 4]_3$

Table: Self-orthogonal codes constructed from orbit matrices of Seidel matrix of $\mathcal{G}$

Codes from orbit matrices of Laplacian matrices

Let $\mathcal{G}$ be a strongly regular graph with parameters (280,135,70,60).

$G \leq \mathrm{PAut}(\mathcal{G})$	C	$\mathrm{Dual}(C)$
Z_2	$[40, 14, 8]_2$	$[40, 26, 4]_2$
Z_2	$[14, 7, 4]_2*$	$[14, 7, 4]_2*$
Z_2	$[133, 27, 24]_2$	$[133, 106, 6]_2$
Z_2	$[12, 2, 6]_2$	$[12, 10, 2]_2*$
Z_2	$[134, 30, 24]_2$	$[134, 104, 5]_2$
Z_5	$[56, 10, 16]_2$	$[56, 46, 2]_2$
Z_7	$[40, 8, 8]_2$	$[40, 32, 2]_2$
Z_4	$[16, 6, 6]_2*$	$[16, 10, 4]_2*$
Z_4	$[48, 8, 16]_2$	$[48, 40, 4]_2*$
Z_4	$[18, 3, 6]_2$	$[18, 15, 2]_2*$
Z_4	$[61, 13, 16]_2$	$[61, 48, 4]_2$
Z_4	$[18, 4, 8]_2*$	$[18, 14, 2]_2*$
Z_7	$[40, 6, 14]_5$	$[40, 34, 2]_5$
Z_5	$[56, 8, 20]_5$	$[56, 48, 2]_5$
Z_5	$[54, 8, 20]_5$	$[56, 48, 2]_5$

Table: Self-orthogonal codes constructed from orbit matrices of Laplace matrix of $\mathcal{G}$