Codes constructed from orbit matrices of block designs

Loredana Simčić (Faculty of Engineering, University of Rijeka, Croatia)

Dean Crnković (Department of Mathematics, University of Rijeka, Croatia)

2014 PhD Summer School in Discrete Mathematics and SYGN IV

July 2, 2014

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST IN ŠPORT

Basic definitions

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 λ elements of $\mathcal{B}$.

If $|\mathcal{P}|=|\mathcal{B}|$ then the design is called symmetric.

A 2-(v,k,λ) design is called a block design.

In a 2-(v,k,λ) design every point is incident with exactly $r=\dfrac{\lambda(v-1)}{k-1}$ blocks, and r is called the replication number of a design.

The number of blocks is denoted by b.

The number $n=r-\lambda$ is called the order of the design.

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a 2-(v, k, λ) design and $G \leq \mathrm{Aut}(\mathcal{D})$.

Denote the G-orbits of points by $\mathcal{P}_1, \ldots, \mathcal{P}_n$, G-orbits of blocks by $\mathcal{B}_1, \ldots, \mathcal{B}_m$, and put $|\mathcal{P}_j| = \omega_j$, $|\mathcal{B}_i| = \Omega_i$, $1 \leq j \leq n$, $1 \leq i \leq m$.

Denote by γ_{ij} the number of points of $\mathcal{P}_j$ incident with a representative of the block orbit $\mathcal{B}_i$.

For those numbers the following equalities hold:

$$\sum_{j=1}^{n} \gamma_{ij} = k \tag{1}$$

$$\sum_{i=1}^{m} \frac{\Omega_i}{\omega_j} \gamma_{ij}\gamma_{is} = \lambda\omega_s + \delta_{js} \cdot (r - \lambda). \tag{2}$$

Definition

A $(m \times n)$-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 $(\omega_1, \ldots, \omega_n)$, $(\Omega_1, \ldots, \Omega_m)$.

Given an orbit matrix M the rows and columns that correspond to non-fixed blocks and non-fixed points form a submatrix called the non-fixed part of the orbit matrix M.

Example

$\mathbb{Z}_2$ acting on 2-$(10, 4, 2)$ design

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

$$\left[\begin{array}{ccccccc}
0 & 0 & 0 & 0 & 2 & 2 & 0 \\
0 & 0 & 0 & 0 & 2 & 0 & 2 \\
0 & 0 & 0 & 0 & 0 & 2 & 2 \\ \hline
1 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1
\end{array}\right]$$

Linear codes

Let $\mathbb{F}_q$ be the finite field of order q.

A linear code of length n is a subspace of the vector space $\mathbb{F}_q^n$.

A k-dimensional subspace of $\mathbb{F}_q^n$ is called a linear $[n, k]_q$ code over $\mathbb{F}_q$.

A linear $[n, k, d]_q$ code is a linear $[n, k]_q$ code with minimum distance d.

An automorphism of a code is any permutation of the coordinate positions that maps codewords to codewords.

Two codes are equivalent if one of the codes can be obtained from the other by permuting the coordinates and multiplying some coordinate position with a nonzero element of the field.

For a linear code $C \subseteq \mathbb{F}_q^n$, we define its dual code $C^\perp \subseteq \mathbb{F}_q^n$ by

$$C^\perp = \{x \in \mathbb{F}_q^n \mid \langle x, y \rangle = 0, \forall y \in C\}.$$

A code C is self-orthogonal if $C \subseteq C^\perp$, and self-dual if $C = C^\perp$.

Codes from orbit matrices of block designs

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 $\mathbb{F}_p$.

Theorem 2

Let G be an automorphism group of a symmetric (v, k, λ) design $\mathcal{D}$. If G is a cyclic group of prime order p and $p|(r - \lambda)$, then the rows of the non-fixed part of the orbit matrix generate a self-orthogonal code of length $\frac{v-f}{p}$ over $\mathbb{F}_p$, where f is the number of fixed points.

Theorem 3

Let $\mathcal{D}$ be a 2-(v, k, λ) design with an automorphism group G. Further, let G act on the set of points $\mathcal{P}$ with f fixed points and $\frac{v-f}{w}$ orbits of length w, and on the set of blocks $\mathcal{B}$ with h fixed blocks and $\frac{b-h}{w}$ orbits of length w. If a prime power p divides w and $r - \lambda$, then the columns of the non-fixed part of the orbit matrix M for the automorphism group G generate a self-orthogonal code of length $\frac{b-h}{w}$ over $\mathbb{F}_p$.

Results

Ternary self-orthogonal codes from the 2-$(15, 3, 1)$ designs

- 80 2-$(15, 3, 1)$ designs
- possibilities for $\mathbb{Z}_3$ acting on the 2-$(15, 3, 1)$ designs:
  - fixed point free and with two fixed blocks (four orbit matrices)
  - fixed point free and with five fixed blocks (one orbit matrix)
  - with three fixed points and five fixed blocks (one orbit matrix)
  - with three fixed points and two fixed blocks (four orbit matrices)

no.	parameters	$\lvert\mathrm{Aut}(C)\rvert$	0	3	6	9
1	$[11, 4, 3]_3$	8	1	2	38	40
2	$[11, 4, 6]_3$	24	1		42	38
3	$[10, 4, 6]_3$	120	1		60	20

Self-orthogonal codes over $GF(5)$ from the 2-$(45, 5, 1)$ designs

- possibilities for $\mathbb{Z}_5$ acting on the 2-$(45, 5, 1)$ design (V. Krčadinac, PhD Thesis)
  - fixed point free and with four fixed blocks (574985 orbit matrices);
  - with five fixed points and four fixed blocks (one orbit matrix);
  - fixed point free and with nine fixed blocks (11 orbit matrices);
  - with five fixed points and nine fixed blocks (one orbit matrix).

parameters	$\lvert\mathrm{Aut}(C)\rvert$	no	parameters	$\lvert\mathrm{Aut}(C)\rvert$	no	parameters	$\lvert\mathrm{Aut}(C)\rvert$	no
$[19, 7, 4]_5$	32	1		1	141		3	17
	16	1	$[19, 8, 4]_5$	16	21		2	29040
$[19, 7, 6]_5$	32	3		8	59		1	284126
	16	4		4	260	$[19, 8, 7]_5$	6	1
	8	16		2	664		4	38
	4	27		1	117		3	13
	2	35	$[19, 8, 5]_5$	16	1		2	4755
	1	20		8	1		1	164151
$[19, 7, 7]_5$	8	7		6	1	$[19, 8, 8]_5$	6	1
	4	27		4	257		4	5
	2	40		2	1611		3	9
	1	32		1	10865		2	203
$[19, 7, 8]_5$	8	6	$[19, 8, 6]_5$	8	31		1	40859
	4	18		6	3			
	2	89		4	1889			

no.	parameters	$\lvert\mathrm{Aut}(C)\rvert$	0	8	10	11
1	$[18, 8, 8]_5$	16	1	792	5544	13824
2	$[18, 7, 8]_5$	8	1	228	776	3200
3	$[18, 8, 8]_5$	2	1	792	5544	13824
4	$[18, 8, 8]_5$	1	1	792	5544	13824
5	$[18, 8, 8]_5$	1	1	792	5544	13824

12	13	14	15	16	17	18
35616	48384	95040	83520	70416	30024	7464
7168	8512	20160	17248	13440	5512	1880
35616	48384	95040	83520	70416	30024	7464
35616	48384	95040	83520	70416	30024	7464
35616	48384	95040	83520	70416	30024	7464

no.	parameters	$\lvert\mathrm{Aut}(C)\rvert$
1	$[18, 9, 6]_5$	8
2	$[18, 9, 6]_5$	2
3	$[18, 9, 6]_5$	2
4	$[18, 9, 6]_5$	2
5	$[18, 9, 6]_5$	2
6	$[18, 9, 6]_5$	1
7	$[18, 9, 6]_5$	1
8	$[18, 9, 6]_5$	1
9	$[18, 9, 6]_5$	1

Binary self-orthogonal codes from the 2-$(64, 8, 1)$ designs

- orbit length distributions for $\mathbb{Z}_2 \times \mathbb{Z}_2$ acting on the 2-$(64, 8, 1)$ design:

1. $(4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4)$,
   $(2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4)$
2. $(4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4)$,
   $(1, 1, 1, 1, 1, 1, 1, 1, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4)$
3. $(2, 2, 2, 2, 2, 2, 2, 2, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4)$,
   $(1, 1, 1, 1, 1, 1, 1, 1, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4)$
4. $(1, 1, 1, 1, 1, 1, 1, 1, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4)$,
   $(1, 1, 1, 1, 1, 1, 1, 1, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4)$
5. $(2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4)$,
   $(1, 1, 1, 1, 1, 1, 1, 1, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4)$

- one orbit matrix for orbit length distributions
$(4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4)$,
$(1,1,1,1,1,1,1,1,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4)$

- one orbit matrix for orbit length distributions
$(1,1,1,1,1,1,1,1,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4)$,
$(1,1,1,1,1,1,1,1,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4)$

parameters	$\lvert\mathrm{Aut}(C)\rvert$	0	8	16
$[16,5,8]_2$	322560	1	30	1

no.	parameters	$\lvert\mathrm{Aut}(C)\rvert$	0	4	6	8	10	12	16
1	$[16,8,4]_2$	5160960	1	28	0	198	0	28	1
2	$[16,8,4]_2$	3612672	1	28	0	198	0	28	1
3	$[16,8,4]_2$	73728	1	12	64	102	64	12	1