Legendre pairs, balanced incomplete block designs and codes

Daniel Šanko
daniel.sanko@math.uniri.hr

(Joint work with Dean Crnković and Andrea Švob)

This work was supported by the Croatian Science Foundation under the project number HRZZ-IP-2022-10–4571 .

Faculty of Mathematics - University of Rijeka

May 26, 2025.

Content

1. Preliminaries
2. Construction
3. Results

Legendre pairs

- **Introduction:** Legendre pairs were introduced in 2001 by J. Seberry and her students

Legendre pairs

- **Introduction:** Legendre pairs were introduced in 2001 by J. Seberry and her students
- **Motivation:** The primary goal was to develop new constructions for Hadamard matrices

$LP(\ell)$

Definition

Let ℓ be an odd positive integer. Two sequences $A = [a_1, \ldots, a_\ell]$ and $B = [b_1, \ldots, b_\ell]$ of length ℓ with $a_i, b_i \in \{-1, +1\}$ and

$$\sum_{i=1}^{\ell} a_i = \sum_{i=1}^{\ell} b_i = \pm 1,$$

form a **Legendre pair** if

$$PAF(A, s) + PAF(B, s) = -2, \quad \text{for } s = 1, \ldots, \frac{\ell - 1}{2}.$$

$LP(\ell)$

Definition

Let ℓ be an odd positive integer. Two sequences $A = [a_1, \ldots, a_\ell]$ and $B = [b_1, \ldots, b_\ell]$ of length ℓ with $a_i, b_i \in \{-1, +1\}$ and

$$\sum_{i=1}^{\ell} a_i = \sum_{i=1}^{\ell} b_i = \pm 1,$$

form a **Legendre pair** if

$$PAF(A, s) + PAF(B, s) = -2, \quad \text{for } s = 1, \ldots, \frac{\ell - 1}{2}.$$

For a sequence $A = [a_1, \ldots, a_\ell]$ with $a_i \in \{-1, +1\}$, the **PAF** at shift s is defined as

$$PAF(A, s) = \sum_{i=1}^{\ell} a_i a_{i+s \mod \ell}, \quad s = 0, \ldots, \ell - 1.$$

Equivalence

Transformations that preserve equivalence[1]:

[1] R. J. Fletcher, M. Gysin, and J. Seberry, "Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices," *Australasian Journal of Combinatorics*, vol. 23, pp. 75–86, 2001.

Equivalence

Transformations that preserve equivalence[1]:

- **Exchange:**

$$(A, B) \sim (B, A)$$

[1] R. J. Fletcher, M. Gysin, and J. Seberry, "Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices," *Australasian Journal of Combinatorics*, vol. 23, pp. 75–86, 2001.

Equivalence

Transformations that preserve equivalence[1]:

- **Exchange:**

$$(A, B) \sim (B, A)$$

- **Cyclic shift:**

$$(A, B) \sim (C(A), C(B)) \sim (C(A), B) \sim (A, C(B))$$

[1] R. J. Fletcher, M. Gysin, and J. Seberry, "Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices," *Australasian Journal of Combinatorics*, vol. 23, pp. 75–86, 2001.

Equivalence

Transformations that preserve equivalence[1]:

- **Exchange:**

$$(A, B) \sim (B, A)$$

- **Cyclic shift:**

$$(A, B) \sim (C(A), C(B)) \sim (C(A), B) \sim (A, C(B))$$

- **Reversal:**

$$(A, B) \sim (R(A), R(B)) \sim (R(A), B) \sim (A, R(B))$$

[1] R. J. Fletcher, M. Gysin, and J. Seberry, "Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices," *Australasian Journal of Combinatorics*, vol. 23, pp. 75–86, 2001.

Equivalence

Transformations that preserve equivalence[1]:

- **Exchange:**
$$(A, B) \sim (B, A)$$

- **Cyclic shift:**
$$(A, B) \sim (C(A), C(B)) \sim (C(A), B) \sim (A, C(B))$$

- **Reversal:**
$$(A, B) \sim (R(A), R(B)) \sim (R(A), B) \sim (A, R(B))$$

- **Decimation:**
$$(A, B) \sim (d_k(A), d_k(B)), \ k \in \mathbb{Z}_\ell^\times = \{j \in \mathbb{Z}_\ell | \gcd(j, \ell) = 1\}$$

[1] R. J. Fletcher, M. Gysin, and J. Seberry, "Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices," *Australasian Journal of Combinatorics*, vol. 23, pp. 75–86, 2001.

BIBDs

Incidence structure $\mathcal{D}$ is an ordered triple $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, where $\mathcal{P}$ is a non empty set of elements called points, $\mathcal{B}$ is a collection of subsets of $\mathcal{P}$ called blocks, and $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$.

Definition

Let v, k, λ be positive integers. Incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is called a $t - (v, k, \lambda)$ **design** if

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

Linear codes

Definition

A **linear code** C of length n and dimension k over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$.

- Binary ($q = 2$), Ternary ($q = 3$)
- Code size: q^k
- Codewords: vectors in the code

Distance

Let $x = (x_1, \ldots, x_n),\ y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$

- **Hamming Distance:** $d(x, y) = |\{i : x_i \neq y_i\}|$
- **Minimum Distance:** $d = \min\{d(x, y) : x, y \in C, x \neq y\}$
- **Weight:** $w(x) = d(x, 0) = |\{i : x_i \neq 0\}|$

Structure

- **Cyclic code:** invariant under full shifts
- **Quasi-cyclic:** invariant under shifts of ℓ positions

The **dual** code $C^\perp$ of the code C is $C^\perp = \left\{x \in \mathbb{F}_q^n : x \cdot c = 0, \forall c \in C\right\}$

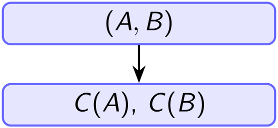
- **Self-orthogonal:** $C \subseteq C^\perp$
- **Self-dual:** $C = C^\perp$

Construction

(A, B)

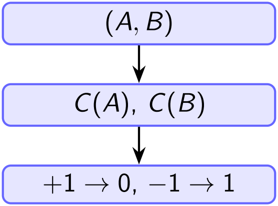
$$A = [+, +, -, -, +],\ B = [+, -, +, +, -]$$

Construction



$$C(A) = \begin{bmatrix} + & + & - & - & + \\ + & + & + & - & - \\ - & + & + & + & - \\ - & - & + & + & + \\ + & - & - & + & + \end{bmatrix},\ C(B) = \begin{bmatrix} + & - & + & + & - \\ - & + & - & + & + \\ + & - & + & - & + \\ + & + & - & + & - \\ - & + & + & - & + \end{bmatrix}$$

Construction



$$C(A) = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix},\ C(B) = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Construction

(A, B)

↓

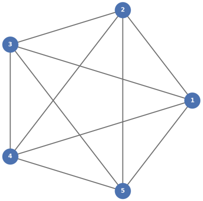
$C(A),\ C(B)$

↓

$+1 \to 0,\ -1 \to 1$

↓

$M = [C(A) \mid C(B)]$



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

Construction

$$b = \frac{v\,r}{k}$$

$$r = \frac{\lambda(v-1)}{(k-1)}$$

(A, B)

↓

$C(A),\ C(B)$

↓

$+1 \to 0,\ -1 \to 1$

↓

$M = [C(A) \mid C(B)]$

↓

2-design

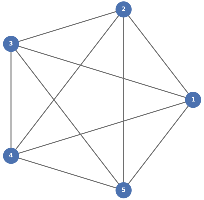
$v = \ell$

$b = 2\ell$

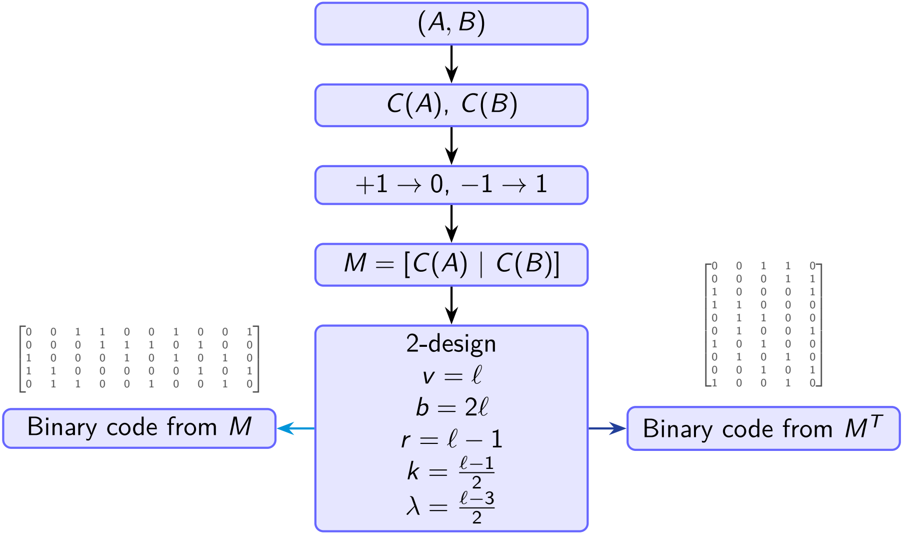
$r = \ell - 1$

$k = \frac{\ell-1}{2}$

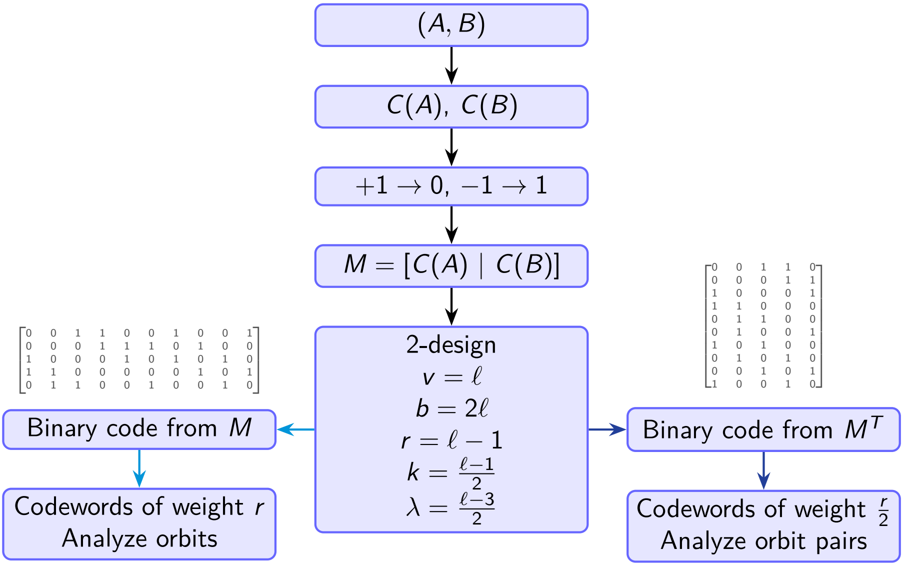
$\lambda = \frac{\ell-3}{2}$



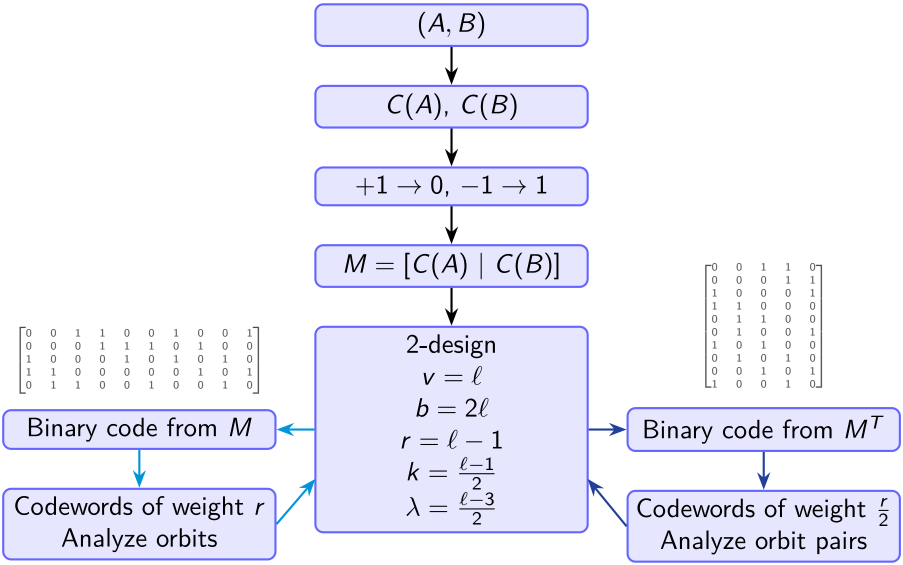
Construction



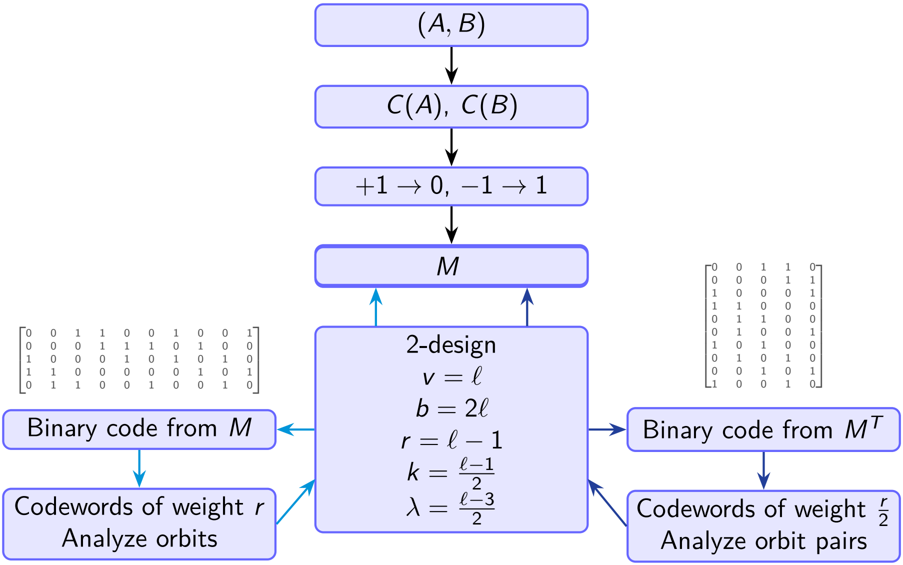
Construction



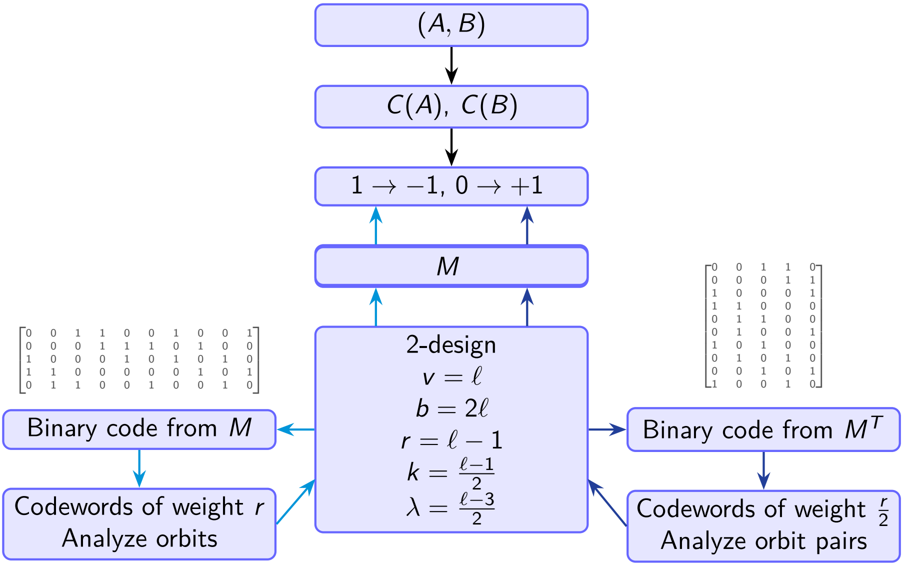
Construction



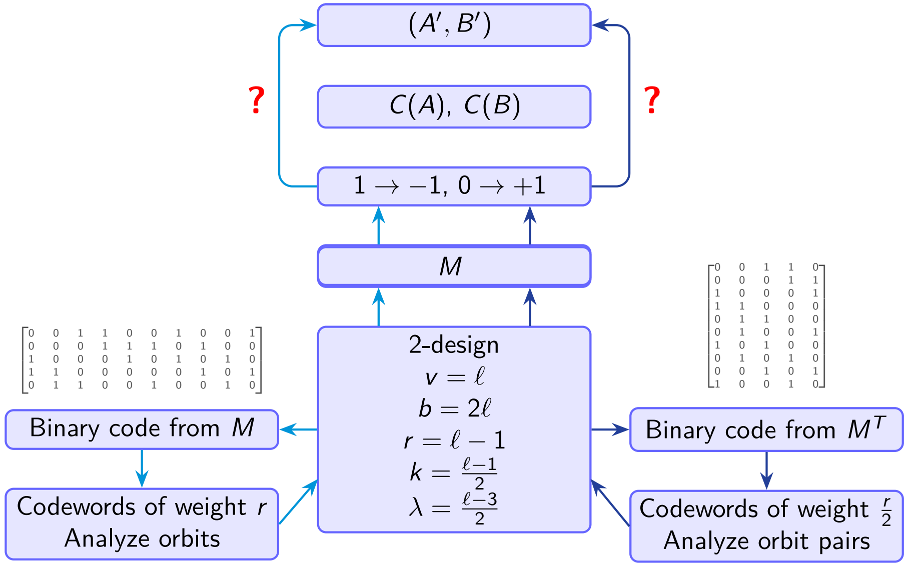
Construction



Construction



Construction



Results: first case

ℓ	Design	Aut	Order	Code	Aut	Order	# Designs	# New Designs	Aut	Order	# LP
5	2-(5,2,1)	S_5	120	[10,4,4]	S_5	120	1	0	/	/	1
7	2-(7,3,2)	F_7	42	[14,7,4]	$\mathrm{PSL}(2,7) \wr C_2$	56448	7	0	/	/	1
9	2-(9,4,3)	C_9	9	[18,8,4]	D_9	18	2	0	/	/	1
11	2-(11,5,4)	F_{11}	110	[22,11,6]	$M_{22} \cdot C_2$	887040	11	1	C_{11}	11	2
13	2-(13,6,5)	F_{13}	156	[26,12,8]	F_{13}	156	1	0	/	/	1
15	2-(15,7,6)	C_{15}	15	[30,13,6]	$D_5 \times S_4$	240	10	1 1	$C_5 \times S_3$ C_{15}	30 15	2
17	2-(17,8,7)	F_{17}	272	[34,16,6]	$C_{17}^2 \cdot C_8^2 \cdot C_2$	36992	17	0	/	/	1
19	2-(19,9,8)	F_{19}	342	[38,19,8]	F_{19}	342	7	1	$C_{19} \rtimes C_3$	57	2
21	2-(21,10,9)	C_{21}	21	[42,20,8]	C_{21}	21	1	0	/	/	1
23	2-(23,11,10)	F_{23}	506	[46,23,8]	$M_{23} \wr C_2$	$\approx 2 \cdot 10^{14}$	23	0	/	/	1
25	2-(25,12,11)	C_{25}	25	[50,24,10]	C_{25}	25	1	0	/	/	1
27	2-(27,13,12)	C_{27}	27	[54,27,8]	D_{27}	54	14	6	C_{27}	27	7
29	2-(29,14,13)	F_{29}	812	[58,28,12]	F_{29}	812	1	0	/	/	1
31	2-(31,15,14)	F_{31}	930	[62,31,8]	$(C_{31} \rtimes C_{15}) \wr C_2$	432450	496	2 1	$C_{31} \rtimes C_5$ $D_{31} \rtimes C_5$	155 310	4

Results: second case

ℓ	Design	Aut	Order	Code	Aut	Order	# Designs	# New Designs	Aut	Order	# LP
5	2-(5,2,1)	S_5	120	[5,4,2]	S_5	120	1	0	/	/	1
7	2-(7,3,2)	F_7	42	[7,7,1]	S_7	5040	1	0	/	/	1
9	2-(9,4,3)	C_9	9	[9,8,2]	S_9	362880	6	0	/	/	1
11	2-(11,5,4)	F_{11}	110	[11,11,1]	S_{11}	39916800	11	1	C_{11}	11	2
13	2-(13,6,5)	F_{13}	156	[13,12,2]	S_{13}	$\approx 6 \cdot 10^9$	21	1 2	C_{13} $C_{13} \rtimes C_3$	13 39	4
15	2-(15,7,6)	C_{15}	15	[15,13,2]	$A_5^3 \cdot A_4 \cdot C_2^2$	10368000	21	1 1 1	C_{15} $C_5 \times S_3$ $S_3 \times F_5$	15 30 120	3
17	2-(17,8,7)	F_{17}	272	[17,16,2]	S_{17}	$\approx 356 \cdot 10^{12}$	161	10	C_{17}	17	7
19	2-(19,9,8)	F_{19}	342	[19,19,1]	S_{19}	$\approx 12 \cdot 10^{16}$	223	11 4	C_{19} $C_{19} \rtimes C_3$	19 57	9
21	2-(21,10,9)	C_{21}	21	[21,20,2]	S_{21}	$\approx 51 \cdot 10^{18}$	492	40	C_{21}	21	22
23	2-(23,11,10)	F_{23}	506	[23,23,1]	S_{23}	$\approx 26 \cdot 10^{21}$	1167	53	C_{23}	23	28
25	2-(25,12,11)	C_{25}	25	[25,24,2]	S_{25}	$\approx 155 \cdot 10^{23}$	1660	82	C_{25}	25	46
27	2-(27,13,12)	C_{27}	27	[27,27,1]	S_{27}	$\approx 109 \cdot 10^{26}$	?	?	?	?	?
29	2-(29,14,13)	F_{29}	812	[29,28,2]	S_{29}	$\approx 88 \cdot 10^{29}$	?	?	?	?	?
31	2-(31,15,14)	F_{31}	930	[31,31,1]	S_{31}	$\approx 82 \cdot 10^{32}$	?	?	?	?	?

Results: LP

ℓ	N_{LP}	results from 2001[2]
5	1	1
7	1	1
9	1	1
11	2	2
13	4	4
15	3	8
17	7	8
19	9	9
21	22	22
23	28	28
25	46	46
27	?	102
29	?	139
31	?	201

[2] R. J. Fletcher, M. Gysin, and J. Seberry, "Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices," *Australasian Journal of Combinatorics*, vol. 23, pp. 75–86, 2001.

Work in progress...

Theorem

Let $\mathcal{D}$ be a $t-(v,k,\lambda)$ BIBD corresponding to a $LP(\ell)$. Then the cyclic group $G \cong C_v$ is a subgroup of Aut($\mathcal{D}$). Let H be a subgroup of G and M be a point orbit matrix with respect to the group H. Then the matrix M spans a quasi-cyclic self-orthogonal code C of length $\frac{2v}{|H|}$ over the field $GF(p^n)$, where p is a prime dividing $2k$ and λ.

Similar results for periodic Golay pairs can be found in D. Crnković, D. Dumičić Danilović, R. Egan, A. Švob, Periodic Golay pairs and pairwise balanced designs, J. Algebraic Combin. 55 (2022), 245-257

Work in progress...

Theorem

Let $\mathcal{D}$ be a $t-(v,k,\lambda)$ BIBD corresponding to a $LP(\ell)$. Then the cyclic group $G \cong C_v$ is a subgroup of Aut($\mathcal{D}$). Let H be a subgroup of G and M be a point orbit matrix with respect to the group H. Then the matrix M spans a quasi-cyclic self-orthogonal code C of length $\frac{2v}{|H|}$ over the field $GF(p^n)$, where p is a prime dividing $|H|$ and $2k-\lambda$.

Similar results for periodic Golay pairs can be found in D. Crnković, D. Dumičić Danilović, R. Egan, A. Švob, Periodic Golay pairs and pairwise balanced designs, J. Algebraic Combin. 55 (2022), 245-257

Thank you for your attention!