Recent results on incidence matrices of designs

Alfred Wassermann

Department of Mathematics, Universität Bayreuth, Germany

Workshop on convolutional codes
Universität Zürich
June 8, 2023

Combinatorial designs

t-(v, k, λ) design $\mathcal{D} = (V, \mathcal{B})$

- V: set of v points
- $\mathcal{B}$: set of k-subsets (blocks) of V
- $\mathcal{D} = (V, \mathcal{B})$ is called a t-(v, k, λ) design on V if

  each t-subset of V is contained in exactly λ blocks.

2-$(6, 3, 2)$ design:

0,1,2
0,1,4
0,2,5
0,3,4
0,3,5
1,2,3
1,3,5
1,4,5
2,3,4
2,4,5

$\#\mathcal{B} = 10$, $r = 5$

Replication number

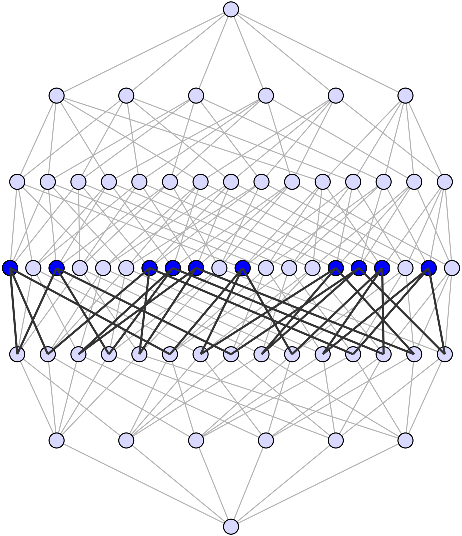
- $\mathcal{D}$ is also s-(v, k, λ_s) design for

$$\lambda_s = \lambda \binom{v-s}{t-s} / \binom{k-s}{t-s}, s = 0, \ldots, t$$

- $b := \#\mathcal{B} = \lambda_0$
- every point $P \in V$ appears in $r := \lambda_1$ blocks: replication number

Subset lattice

$V = \{0, 1, 2, 3, 4, 5\}$



2-$(6, 3, 2)$ design:

0,1,2
0,1,4
0,2,5
0,3,4
0,3,5
1,2,3
1,3,5
1,4,5
2,3,4
2,4,5

Incidence matrix

The $(v \times b)$-matrix N with

$$N_{ij} = \begin{cases} 1, & \text{if } i \in B_j \\ 0, & \text{otherwise} \end{cases}$$

is the point/block incidence matrix of the Design $\mathcal{D}$.

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

2-(v, k, λ) design

Bose (1949):

$$N \cdot N^\top = (r - \lambda) \cdot I + \lambda \cdot J$$

- $(NN^\top)_{ij} = \begin{cases} r, & i = j \\ \lambda, & i \neq j \end{cases}$
- $NN^\top$ has Eigenvalues $(r - \lambda) + \lambda v = rk$ and $(r - \lambda) + 0$ over $\mathbb{Q}$
- $\Rightarrow NN^\top$ has rank v over $\mathbb{Q}$
- $\Rightarrow N$ has rank v

Theorem (Fisher's inequality (1930))

$$b \geq v$$

p-rank of N

2-(v,k,λ) design

Definition

The rank of N over $\mathbb{F}_p$ is called p-rank of N (also p-rank of $\mathcal{D}$)

Theorem (Hamada)

Let $\mathcal{D}$ be a 2-(v,k,λ) design with replication number r and p prime.

- *If p does not divide $r(r-\lambda)$, then $\text{rank}_p N = v$.*
- *If p divides r but does not divide $r-\lambda$, then $\text{rank}_p N \geq v-1$.*
- *If $\text{rank}_p N < v-1$, then p divides $r-\lambda$.*

Majority logic decoding and designs

Rudolph (1967), Ng (1970)

- Given: 2-(v, k, λ) design $\mathcal{D} = (V, \mathcal{B})$ with incidence matrix N
- Take $N^\top$ as parity check matrix of a code
- $C_\mathcal{D} \leq \mathbb{F}_p^v$: p-ary linear code of length v having parity-check matrix $H_\mathcal{D} := N^\top$

Example

	0, 1, 2, 3, 4, 5
0,1,2	1, 1, 1, 0, 0, 0
0,1,4	1, 1, 0, 0, 1, 0
0,2,5	1, 0, 1, 0, 0, 1
0,3,4	1, 0, 0, 1, 1, 0
0,3,5	1, 0, 0, 1, 0, 1
1,2,3	0, 1, 1, 1, 0, 0
1,3,5	0, 1, 0, 1, 0, 1
1,4,5	0, 1, 0, 0, 1, 1
2,3,4	0, 0, 1, 1, 1, 0
2,4,5	0, 0, 1, 0, 1, 1

Majority logic decoding

- r equations for each coordinate
- Each error spoils at most λ of these equations
- Decoding correct if

$$\#\text{errors} \cdot \lambda < (r + \lambda)/2$$

Linear code $C_{\mathcal{D}}$:

- Length: v
- Dimension: $\dim C_{\mathcal{D}} = v - \text{rank}_p N$
- Majority logic decodes at least $\lfloor \frac{r+\lambda-1}{2\lambda} \rfloor$ errors
- Complexity $\approx$ #equations, i.e. r

Drawback:

For most designs, $C_{\mathcal{D}}$ will have dimension 0 or 1.

Challenge:

Search for designs with low p-rank!

Classical / geometric designs

- $2 \leq k < v$, $\mathcal{V} = \mathbb{F}_q^v$
- Classical / geometric design, Bose (1939)

$$\mathcal{G} = (\begin{bmatrix}\mathcal{V}\\1\end{bmatrix}_q, \begin{bmatrix}\mathcal{V}\\k\end{bmatrix}_q)$$

- $\begin{bmatrix}\mathcal{V}\\k\end{bmatrix}_q$: set of all k-dimensional subspaces of $\mathcal{V}$ (k-subspaces)
- Gaussian coefficient:

$$\#\begin{bmatrix}\mathcal{V}\\m\end{bmatrix}_q = \begin{bmatrix}v\\m\end{bmatrix}_q = \frac{(q^v-1)(q^{v-1}-1)\cdots(q^{v-m+1})}{(q^m-1)(q^{m-1}-1)\cdots(q-1)}$$

- $\mathcal{G}$: combinatorial design with parameters

$$2\text{-}(\begin{bmatrix}v\\1\end{bmatrix}_q, \begin{bmatrix}k\\1\end{bmatrix}_q, \begin{bmatrix}v-2\\k-2\end{bmatrix}_q)$$

p-rank of classical designs

Theorem (Hamada (1973))

- *The p-rank of $\mathcal{G}$ is*

$$\sum_{s_0} \cdots \sum_{s_{f-1}} \prod_{j=0}^{f-1} \sum_{i=0}^{L(s_{j+1},s_j)} (-1)^i \binom{v}{i} \binom{v-1+s_{j+1}p-s_j-ip}{v-1}$$

- $s_f = s_0$
- $k \leq s_j \leq v$ *and* $0 \leq s_{j+1}p - s_j \leq v(p-1)$
- $L(s_{j+1}, s_j) = \lfloor (s_{j+1}p - s_j)/p \rfloor$

Hamada's conjecture (1973)

Among the designs with the same parameters as the classical designs, the classical designs have minimal p-rank.

Codes from classical designs

projective case:

- Projective Geometry codes
- $p = 2$: subcodes of punctured Reed-Muller codes

affine case:

- Euclidean Geometry codes
- $p = 2$: Reed-Muller codes

- Assmus, Key (1992): Designs and their codes
- Since Rudolph (1967), codes from incidence matrices of various structures in finite geometry have been studied.

Subspace designs

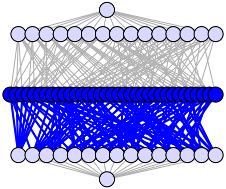
Subspace designs

q-analogs of designs

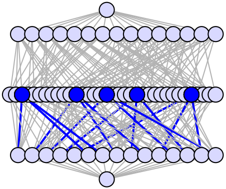
A pair $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ is called t-$(v, k, \lambda)_q$ subspace design if

- $\mathcal{V} = \mathbb{F}_q^v$
- $\begin{bmatrix}\mathcal{V}\\1\end{bmatrix}_q$: points, $\mathcal{B} \subseteq \begin{bmatrix}\mathcal{V}\\k\end{bmatrix}_q$: blocks

  each t-subspace of $\mathcal{V}$ is contained in exactly λ blocks.
- $\mathcal{B} = \begin{bmatrix}\mathcal{V}\\k\end{bmatrix}_q$: complete design



1-$(4, 2, 7)_2$ design



1-$(4, 2, 1)_2$ design

History of subspace designs

- Introduced by Ray-Chaudhuri, Cameron, Delsarte in the 1970s
- Thomas (1987):
  2-$(v, 3, 7)_2$ for $v \geq 7$ and $\pm 1 \equiv v \pmod 6$
- Suzuki (1989):
  2-$(v, 3, q^2 + q + 1)_q$ for $v \geq 7$ and $\pm 1 \equiv v \pmod 6$
- Nontrivial q-Steiner systems (i.e. $\lambda = 1$):
  Braun, Etzion, Östergård, Vardy, W. (2013)
- Many sporadic examples found by computer, see
  Greferath, Pavčević, Silberstein, Vázquez-Castro:
  Network Coding and Subspace Designs (2018)
- Keevash et al (2023): q-Steiner systems asymptotically exist for all t.

Designs: necessary conditions

t-$(v,k,\lambda)_q$ design $\mathcal{D}$ for $q \geq 1$

- $\mathcal{D}$ is also s-$(v,k,\lambda_s)_q$ design for

$$\lambda_s = \lambda \begin{bmatrix} v-s \\ t-s \end{bmatrix}_q \Big/ \begin{bmatrix} k-s \\ t-s \end{bmatrix}_q$$

- Necessary conditions:

$$\lambda_s \in \mathbb{Z} \text{ for } 0 \leq s \leq t$$

- λ_1: replication number
- λ_0: number of blocks
- Bose's equation holds, too:

$$N \cdot N^\top = (r - \lambda) \cdot I + \lambda \cdot J$$

Subspace designs $\rightarrow$ combinatorial designs

Complete design

- Blocks are the set of all k-subspaces
- $\lambda_{\max} = \begin{bmatrix} v-t \\ k-t \end{bmatrix}_q$

Combinatorial design parameters

- A 2-$(v, k, \lambda)_q$ subspace design is a

$$2\text{-}(\begin{bmatrix} v \\ 1 \end{bmatrix}_q, \begin{bmatrix} k \\ 1 \end{bmatrix}_q, \lambda)$$

  combinatorial design
- The classical / geometric designs are a special case of subspace designs: namely the complete subspace designs 2-$(v, k, \lambda_{\max})_q$

Classical designs vs. subspace designs
part I

classical design $\mathcal{G}$

- 2-$(v, k, \lambda_{\max})_q$
- incidence matrix $H_\mathcal{G}$

subspace design $\mathcal{D}$

- 2-$(v, k, \lambda)_q$
- incidence matrix $H_\mathcal{D}$

Observation:

The rows of $H_\mathcal{D}$ are a subset of the rows of $H_\mathcal{G}$

$$\Longrightarrow$$

$$\mathrm{rank}_p\,\mathcal{D} \leq \mathrm{rank}_p\,\mathcal{G} \quad \text{and} \quad C_\mathcal{D} \geq C_\mathcal{G}$$

Conjecture:

$$C_\mathcal{D} = C_\mathcal{G}$$

Classical designs vs. subspace designs

part II: majority logic decoding

- $r_{\mathcal{D}} = \lambda \frac{\begin{bmatrix} v-1 \\ 1 \end{bmatrix}_q}{\begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q}$ $\qquad r_{\mathcal{G}} = \lambda_{\max} \frac{\begin{bmatrix} v-1 \\ 1 \end{bmatrix}_q}{\begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q} = \begin{bmatrix} v-2 \\ k-2 \end{bmatrix}_q \frac{\begin{bmatrix} v-1 \\ 1 \end{bmatrix}_q}{\begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q}$

Dela Cruz, W. (2021):

- Length of $C_{\mathcal{D}}$, $C_{\mathcal{G}}$: $\begin{bmatrix} v \\ 1 \end{bmatrix}_q$
- Dimension: $\dim C_{\mathcal{D}} \geq \dim C_{\mathcal{G}}$
- Majority logic decoding is correct if $\qquad$ ($\#\text{err} \cdot \lambda < (r + \lambda)/2$)

$$\#\text{errors} \leq \left\lfloor \frac{\begin{bmatrix} v-1 \\ 1 \end{bmatrix}_q}{2\begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q} \right\rfloor$$

  i.e. the number of correctable errors is independent from λ.
- #equations: $r_{\mathcal{D}} + 1 \leq r_{\mathcal{G}} + 1$
- For $v \to \infty$, the Suzuki family $2\text{-}(v, 3, q^2 + q + 1)_q$ gives an exponential improvement in the # equations compared to the geometric designs

LDPC codes

Gallager (1963)

- LDPC code: "sparse matrix of parity check equations"
- Gallager's bit-flipping algorithm:

  > *[...] the decoder computes all the parity-checks and then changes any digit that is contained in more than some fixed number of unsatisfied parity-check equations. Using these new values, the parity checks are recomputed, and the process is repeated until the parity-check equations are all satisfied.*

- Majority logic decoding – alternative view:
  - For each coordinate, $0 \leq i < n$, set a counting variable $f_i \leftarrow 0$.
  - For each parity-check equation:
    if equation h is unsatisfied:
    $f_i \leftarrow f_i + 1$ for all i in the supp(h)
  - Flip entry if $f_i > (r + \lambda)/2$
- Majority logic decoding is a single step in the bit-flipping algorithm with specific treshold.
- Soft-decision variants: Kolesnik (1971), Bossert et. al. (2009)

LDPC codes

From Kou, Lin, Fossorier (2001): Decoding codes from geometric designs

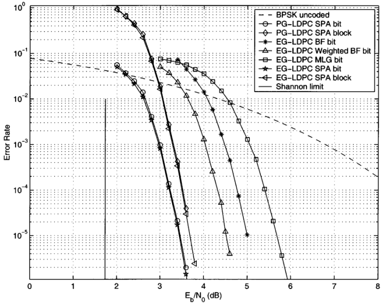


Fig. 3. Bit- and block-error probabilities of the type-I 2-D (1023, 781) EG-LDPC code and (1057, 813) PG-LDPC code based on different decoding algorithms.

Open

Performance of bit-flipping and sum-product algorithm on parity-check matrices from subspace designs?

Finite classical polar spaces

Finite classical polar spaces

Geometries associated with the non-degenerate sesquilinear and non-singular quadratic forms over a finite field.

- $\mathrm{PG}(v-1,q)$: projective space of $\mathbb{F}_q^v$
- Polar space $\mathcal{Q}$ in $\mathrm{PG}(v-1,q)$ consists of the

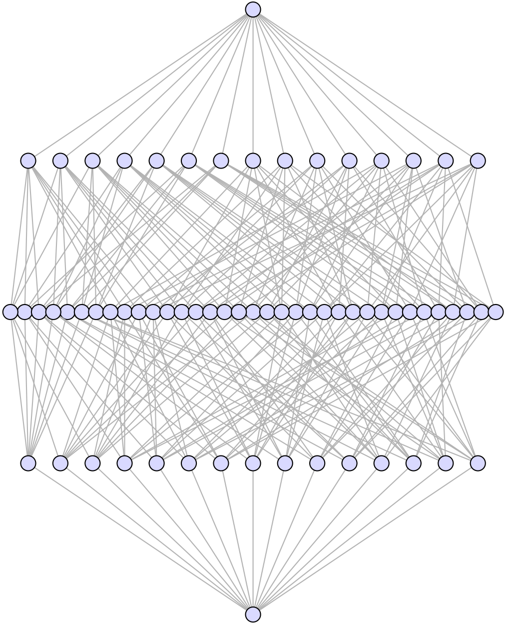
  projective subspaces of $\mathrm{PG}(v-1,q)$ that are
  - totally isotropic with relation to a given non-degenerate sesquilinear form or
  - totally singular with relation to a given non-singular quadratic form

Example

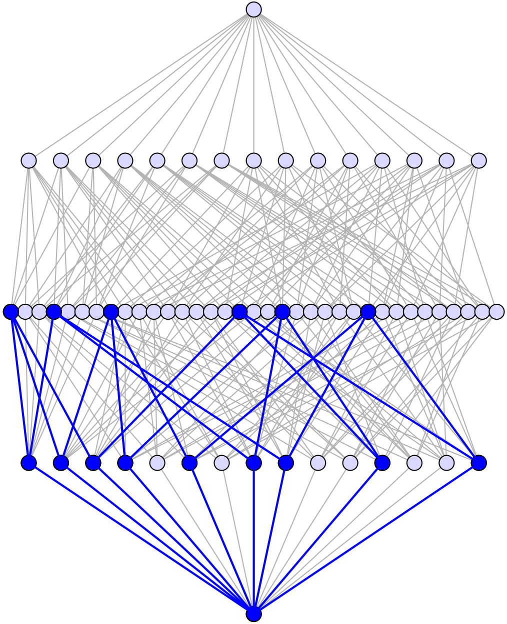
Hyperbolic quadric $\Omega^+(2r,q) \subset \mathrm{PG}(2r-1,q)$, $r \geq 1$:

$$x_0 x_r + \ldots + x_{r-1} x_{2r-1} = 0$$

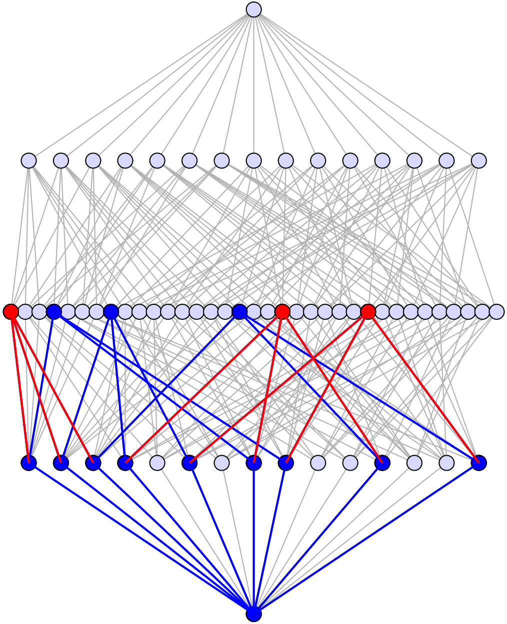
$\Omega^+(4,2)$ embedded in $PG(3,2)$ ($\mathbb{F}_2^4$)



$\Omega^+(4,2)$ embedded in $PG(3,2)$ ($\mathbb{F}_2^4$)



$\Omega^+(4,2)$ embedded in $PG(3,2)$ $(\mathbb{F}_2^4)$



Finite classical polar spaces

generators

- $\mathcal{Q}$ polar space in $\mathrm{PG}(v-1,q)$, v minimal
- A subspace of maximum dimension r in a polar space $\mathcal{Q}$: generator
- r: rank of $\mathcal{Q}$

Finite classical polar spaces

name	symbol $\mathcal{Q}$	type Q	ϵ	alternative symbols	
symplectic	$Sp(2r,q)$	Sp	0	C_r	$W_{2r-1}(q)$
Hermitian	$U(2r,q)$	U	$-1/2$	${}^2A_{2r-1}$	$H_{2r-1}(q)$
Hermitian	$U(2r+1,q)$	U^+	$1/2$	${}^2A_{2r}$	$H_{2r}(q)$
hyperbolic	$\Omega^+(2r,q)$	Ω^+	-1	D_r	$Q^+_{2r-1}(q)$
parabolic	$\Omega(2r+1,q)$	Ω	0	B_r	$Q_{2r}(q)$
elliptic	$\Omega^-(2r+2,q)$	Ω^-	1	${}^2D_{r+1}$	$Q^-_{2r+1}(q)$

Counting

Lemma (Brouwer, Cohen, Neumaier, Distance regular graphs)

- *The number of k-dimensional subspaces of $\mathcal{Q}$ is equal to*

$$\begin{bmatrix} r \\ k \end{bmatrix}_Q = \begin{bmatrix} r \\ k \end{bmatrix}_q \cdot \prod_{i=r-k+1}^{r} (q^{i+\epsilon} + 1).$$

- *The number of k-dimensional subspaces of $\mathcal{Q}$ containing a fixed u-dimensional subspace is*

$$\begin{bmatrix} r-u \\ k-u \end{bmatrix}_Q = \begin{bmatrix} r-u \\ k-u \end{bmatrix}_q \cdot \prod_{i=r-k+1}^{r-u} (q^{i+\epsilon} + 1).$$

Designs in finite classical polar spaces

Definition

- finite polar space $\mathcal{Q}$ of rank r
- set of $\mathcal{B}$ of k-dimensional subspaces in $\mathcal{Q}$ (blocks)
- $\mathcal{D} = (\mathcal{Q}, \mathcal{B})$ is called a t-$(r, k, \lambda)_Q$-design if

  each t-dimensional subspace of $\mathcal{Q}$ is contained in exactly λ blocks

(Here, dimensions are vector space dimensions)

Designs in polar spaces as combinatorial designs

2-designs in polar spaces

- fail to be combinatorial designs (in general)
- are (combinatorial) 1-designs and 2-packings, i.e. possess a replication number
- are candidates for codes with majority logic decoder

Connection to rank metric codes

Kerdock sets

- Hyperbolic quadric $\Omega^+_{2r}(q) \subset \mathbb{F}_q^{2r}$

$$x_0x_r + \ldots + x_{r-1}x_{2r-1} = 0 \iff x \cdot \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \cdot x^\top = 0$$

- Lift matrices $\mathbb{F}_q^{r\times r} \ni A \mapsto (I \mid A) \in \begin{bmatrix} \mathbb{F}_q^{2r} \\ r \end{bmatrix}_q$:

$$\begin{aligned} 0 &= (I \mid A) \cdot \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \cdot (I \mid A)^\top \\ &= (I \mid A) \cdot (A \mid I)^\top = A^\top + A \\ &\Leftrightarrow\ A^\top = -A \end{aligned}$$

- Elements of Ω^+ correspond to (skew) symmetric matrices
- …it follows:

  Kerdock sets (of matrices) in coding theory are 1-$(2r, r, 1)_{\Omega^+}$ designs, i.e. spreads in Ω^+

Steiner systems
of generators

Theorem (K.-U. Schmidt, Ch. Weiß (2022))

Suppose there exists a t-$(r, r, 1)_Q$ *Steiner system with* $t \in \{2, \dots, r-1\}$. *Then one of the following holds*

- $t = 2$ *and* $Q = U(q)$ *or* $Q = \Omega^-(q)$ *for odd* r.
- $t = r - 1$ *and* $Q = U^-(q)$ *or* $Q = \Omega^-(q)$ *for* $q \neq 2$, *or* $Q = \Omega^+(q)$.

Well known

In $\Omega^+(2r, q)$ there always exists the Latin-Greek halving, i.e. a

$$(r-1)\text{-}(r, r, 1)_{\Omega^+} \text{ design}$$

Necessary conditions

Lemma

Let $\mathcal{D}$ be a t-$(r,k,\lambda)_Q$ design.
Then for each $s \in \{0,\ldots,t\}$, $\mathcal{D}$ is an s-$(r,k,\lambda_s)_Q$ design with

$$\lambda_s = \lambda \cdot \frac{\begin{bmatrix} r-s \\ t-s \end{bmatrix}_Q}{\begin{bmatrix} k-s \\ t-s \end{bmatrix}_q} = \lambda \cdot \frac{\begin{bmatrix} r-s \\ t-s \end{bmatrix}_q}{\begin{bmatrix} k-s \\ t-s \end{bmatrix}_q} \cdot \prod_{i=r-t+1}^{r-s} (q^{i+\epsilon}+1).$$

In particular, the number of blocks of $\mathcal{D}$ is given by λ_0 and the replication number by λ_1.

Incidence matrix

2-$(r,k,\lambda)_Q$

N: point / block incidence matrix

$$(NN^\top)_{ij} = \begin{cases} \lambda_1, & i = j \\ \lambda, & i \neq j,\ P_i, P_j \text{ collinear} \\ 0, & i \neq j,\ P_i, P_j \text{ non-collinear} \end{cases}$$

Collinearity graph

Lemma

Let A be the adjacency matrix of the collinearity graph (a strongly regular graph) of the polar space $\mathcal{Q}$.
The eigenvalues of A are

$$\theta_0 = q \cdot \begin{bmatrix} r-1 \\ 1 \end{bmatrix}_{\mathcal{Q}}, \qquad \theta_1 = q^{r-1} - 1, \qquad \theta_2 = -(q^{r+\epsilon-1} + 1),$$

with multiplicities

$$\begin{aligned} m_0 &= 1, \\ m_1 &= q^{\epsilon+1} \cdot \frac{q^{r+\epsilon-1}+1}{q^\epsilon+1} \cdot \begin{bmatrix} r \\ 1 \end{bmatrix}_q \quad \textit{and} \\ m_2 &= q \cdot \frac{q^{r+\epsilon}+1}{q^\epsilon+1} \cdot \begin{bmatrix} r-1 \\ 1 \end{bmatrix}_q. \end{aligned}$$

Bose's equation

for designs in polar spaces

Theorem

The eigenvalues μ_i of

$$NN^\top = \lambda_1 I + \lambda A$$

are

$$\mu_i = \lambda_1 + \lambda\theta_i$$

with multiplicities m_i, $i = 0, 1, 2$.

- Since $\lambda, \lambda_1 > 0$ also $\mu_0, \mu_1 > 0$
- $\mu_2 = 0$ iff $t = 2$ and $k = r$, independent from λ
- If $\mu_2 = 0$, the rank of the matrices $NN^\top$ and N over $\mathbb{Q}$ is equal to $1 + m_1$
- In all other cases the matrix N has full rank
- Fisher's inequality is not true in all cases

Computer search

Previous results

- First nontrivial 2-designs [De Bruyn, Vanhove (2012, unpublished)]:
  - $\Omega(7,3)$: $2\text{-}(3,3,2)_\Omega$
  - $\Omega^-(8,2)$: $2\text{-}(3,3,2)_{\Omega^-}$
- Lansdown (2020):
  - $\Omega(7,5)$: $2\text{-}(3,3,3)_\Omega$
  - $\Omega(7,7)$: $2\text{-}(3,3,4)_\Omega$
  - $\Omega(7,11)$: $2\text{-}(3,3,6)_\Omega$
- Found as m-ovoids in the dual polar space with $m = \lambda_{\max}/2$ (hemisystems)

$2\text{-}(r, k, \lambda)_{\Omega^-}$

$q = 2$

r	k	Δ_λ	$\lambda_{\max}$	$\nexists\lambda$	$\exists\lambda$
3	3	1	5	1	2 (De Bruyn, Vanhove)
4	**3**	3	27		6, 9, 12
4	4	1	45	1	9, 11, 12, 14, 15, 16, 18, 19, 21
5	5	1	765	1	240, 245, 275, 280, 315, 360

$q = 3$

r	k	Δ_λ	$\lambda_{\max}$	$\nexists\lambda$	$\exists\lambda$
3	3	1	10	?	2, 5

$2\text{-}(r, k, \lambda)_\Omega$

$q = 2$

r	k	Δ_λ	$\lambda_{\max}$	$\nexists\lambda$	$\exists\lambda$
3	3	1	3	1	-
4	**3**	1	15		6, 7
4	4	1	15	1	5, 6, 7
5	5	1	135	1	21, 24, 27, 29, 30, 32, 33, 35, 36, 39, 40, 42, 45, 47, 48, 50, 51, 52, 53, 54, 55, 56, 57, 58, 60, 61, 62, 63, 64, 65, 66

$q = 3$

r	k	Δ_λ	$\lambda_{\max}$	$\nexists\lambda$	$\exists\lambda$
3	3	1	4	1	2 (De Bruyn, Vanhove)
4	4	1	40		8, 20

$2\text{-}(r, k, \lambda)_{\Omega^+}$

Latin-Greek halvings (i.e. $\lambda = \lambda_{\max}/2$) are marked with *.

$q = 2$

r	k	Δ_λ	$\lambda_{\max}$	$\nexists\lambda$	$\exists\lambda$
3	3	1	2	-	1^*
4	**3**	3	9		3
4	4	1	6	1,2	3^*
5	5	1	30	1	6, 8, 10, 12, 14, 15^*
6	6	1	270	1	40, 45, 48, 50, 51, 53, 54, 56, 57, 58, 60, 62, 63, 64, 65, 66, 67, 69, 70, 72, 74, 75, 77, 78, 79, 80, 81, 84, 85, 86, 87, 88, 90, 91, 93, 94, 95, 96, 98, 99, 100, 102, 103, 104, 105, 107, 108, 109, 110, 111, 112, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 132, 133, 134, 135^*

2-$(r, k, \lambda)_{\Omega^+}$

$q = 3$

r	k	Δ_λ	$\lambda_{\max}$	$\nexists\lambda$	$\exists\lambda$
3	3	1	2	-	1*
4	4	1	8	1	4*
5	5	1	80		8, 16, 32, 40*

$2\text{-}(r, k, \lambda)_{Sp}$

For $q = 2$: $\Omega(2r + 1, q) = Sp(2r, q)$

$q = 3$

r	k	Δ_λ	$\lambda_{\max}$	$\nexists\lambda$	$\exists\lambda$
3	3	1	4	1, 2	- (2 by De Bruyn, Vanhove)
4	4	1	40		20
5	5	1	1120		

Back to combinatorial designs

Higher incidence matrices

- $\mathcal{D}$: t-(v,k,λ) design for $t \geq 2$
- The number of blocks which contain a given i-set of points and are disjoint to a given j-set of points is equal to

$$\lambda_{i,j} = \lambda \frac{\binom{v-i-j}{k-j}}{\binom{v-t}{k-t}}$$

- $N^{(e)}$ is the incidence matrix between all e-subsets and design blocks ($e \leq t$), i.e.

$$N^{(e)}_{E,B} = \begin{cases} 1, & E \subset B \\ 0, & \text{else} \end{cases}$$

- $W^{(xy)}$ is the incidence matrix between all x-subsets and all y-subsets, i.e.

$$W^{(xy)}_{X,Y} = \begin{cases} 1, & X \subset Y \\ 0, & \text{else} \end{cases}$$

Wilson's theorem

Theorem (Wilson (1982))

For $e + f \leq t$:

$$N^{(e)} \left(N^{(f)}\right)^\top = \sum_{i=0}^{\min\{e,f\}} \lambda_{e+f-i,\, i} \left(W^{(ie)}\right)^\top W^{(if)}$$

$$W^{(ie)}\, N^{(e)} = \binom{k-i}{e-i} N^{(i)} \qquad \text{for } 0 \leq i \leq e \leq k\,.$$

Corollary

Let $2s \leq t$ and $v \geq k + s$. Then

$$b \geq \binom{v}{s}\,.$$

Tactical decomposition matrix

- $(V, \mathcal{B})$: 2-(v, k, λ) design invariant under group G.
- The action of G partitions
  - V into orbits $\mathcal{P}_1, \ldots, \mathcal{P}_m$
  - $\mathcal{B}$ into orbits $\mathcal{B}_1, \ldots, \mathcal{B}_n$.
- For $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$ let $N_{i,j}$ be the submatrix of N whose
  - rows are assigned to the elements $\mathcal{P}_i$
  - whose columns to the elements of $\mathcal{B}_j$.

  $N_{i,j}$ has a constant number of ones in each row and a constant number of ones in each column.
- Such a decomposition of N into submatrices $N_{i,j}$ is called tactical.
- Replace for all i, j the submatrix $N_{i,j}$ by the number of ones in each row: $(m \times n)$-matrix ρ
- Replace the submatrix $N_{i,j}$ by the number of ones in each column: $(m \times n)$-matrix κ.
- The matrices ρ and κ are both called tactical decomposition matrix.

Example

2-$(6,3,2)$ design

$$G = \langle (0,1)(2,4) \rangle$$

$$N = \left(\begin{array}{cc|cc|cc|cc|c|c} 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ \hline 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right)$$

$$\rho = \begin{pmatrix} 2 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 2 & 2 & 1 & 0 \\ 0 & 2 & 0 & 2 & 0 & 1 \end{pmatrix} \quad \kappa = \begin{pmatrix} 2 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 2 & 2 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Dembowski (1958)

For ρ and κ and $P = \mathrm{diag}(\#\mathcal{P}_i)$ and $B = \mathrm{diag}(\#\mathcal{B}_i)$ holds:

$$P \cdot \rho = \kappa \cdot B$$
$$\rho \cdot (1, \ldots, 1)^\top = (\lambda_1, \ldots, \lambda_1)^\top$$
$$(1, \ldots, 1) \cdot \kappa = (k, \ldots, k)$$
$$\rho \cdot \kappa^\top = (\lambda_1 - \lambda) \cdot I + \lambda \cdot P \cdot J$$

For $G = \mathrm{Id}$ the last equation reduces to Bose's equation, i.e. $\rho = \kappa = N$

Algorithmic use

Janko and Tran Van Trung (1985) and many follow-ups:

1. construct (all non-isomorphic) tactical decomposition matrices of a design using these equations
2. Extend the tactical decomposition matrices to incidence matrices of designs

Combining Wilson and Dembowski?

Wilson, $t \geq 2$:

$$N^{(e)}\,(N^{(f)})^\top = \sum_{i=0}^{\min\{e,f\}} \lambda_{e+f-i,\,i}(W^{(ie)})^\top W^{(if)}$$

Dembowski, $t = 2$, group G:

$$\rho \cdot \kappa^\top = (\lambda_1 - \lambda) \cdot I + \lambda \cdot P \cdot J$$

Bose: N	Dembowski: ρ, κ
Wilson: $N^{(e)}$	$\rho^{(e)}, \kappa^{(f)}$?

Higher tactical decomposition matrices

Kiermaier, W.: Higher incidence matrices and tactical decomposition matrices (2023)

Let G be a group acting on V and $\mathcal{D} = (V, \mathcal{B})$ be a t-(v, k, λ) design

- $R^{(x,y)}$: Tactical decomposition of $W^{(xy)}$ w.r.t. action of G, row sums
- $K^{(x,y)}$: Tactical decomposition of $W^{(xy)}$ w.r.t. action of G, column sums
- $\rho^{(e)}$: Tactical decomposition of $N^{(e)}$ w.r.t. action of G, row sums
- $\kappa^{(e)}$: Tactical decomposition of $N^{(e)}$ w.r.t. action of G, column sums

Higher tactical decomposition matrices

Equations

Theorem (Kiermaier, W. (2023))

Let G be a group acting on V and $\mathcal{D} = (V, \mathcal{B})$ be a t-(v, k, λ) design. For $e + f \leq t$:

$$\rho^{(e)} \left(\kappa^{(f)}\right)^\top = \sum_{j=0}^{\min(e,f)} \lambda_{e+f-j,\,j} \left(K^{(je)}\right)^\top R^{(jf)}$$

Let x, y be non-negative integers with $x \leq y \leq k$. Then

$$R^{(xy)}\,\rho^{(y)} = \binom{k-x}{y-x}\rho^{(x)} \qquad \text{and} \qquad K^{(xy)}\,\kappa^{(y)} = \binom{k-x}{y-x}\kappa^{(x)}$$

Higher tactical decomposition matrices

Fisher's equation, Block's theorem

Theorem (Kiermaier, W. (2023))

Let G be a group acting on V and $\mathcal{D} = (V, \mathcal{B})$ be a t-(v, k, λ) design.

$$\#\mathcal{B}^G \geq \#\binom{V}{s}^G$$

for all $s \in \{0, \ldots, \lfloor t/2 \rfloor\}$, i.e.

Number of block orbits is at least as large as the overall number of s-orbits

All theorems have a q-analog version for subspace designs

Overview

N

- Bose
- Fisher: $b \geq v$
- q

ρ, κ

- Dembowski
- Block: $\#\mathcal{B}^G \geq \#V^G$
- q: Krčadinac et al

$N^{(e)}$

- Wilson
- RayChaudhuri, Wilson: $b \geq \binom{v}{s}$
- q: Suzuki, Cameron

$\rho^{(e)}, \kappa^{(f)}$

- ✔
- $\#\mathcal{B}^G \geq \#\binom{V}{s}^G$ ✔
- q ✔

Open questions

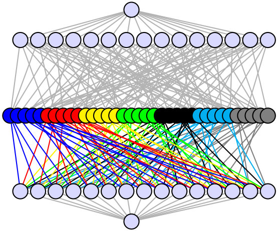
Subspace designs, designs in polar spaces

- $C_{\mathcal{D}} = C_{\mathcal{G}}$?
- Study codes from designs in polar spaces
- Performance of soft-decision decoding algorithms?
- Performance for LDCP decoding
- More constructions

Higher tactical decomposition matrices

- Algorithmic use
- Relation to the work of Krčadinac, Nakić, Pavčević (2014): (complicated) equations on N for $t \geq 2$

The end



Thank you for listening !