New 2-designs in polar spaces

Alfred Wassermann

Department of Mathematics, Universität Bayreuth, Germany

Coding theory and cryptography 2022
– Zürich – July 15, 2022

joint work with
Michael Kiermaier (Bayreuth), Kai-Uwe Schmidt (Paderborn)

Combinatorial Designs

Combinatorial designs

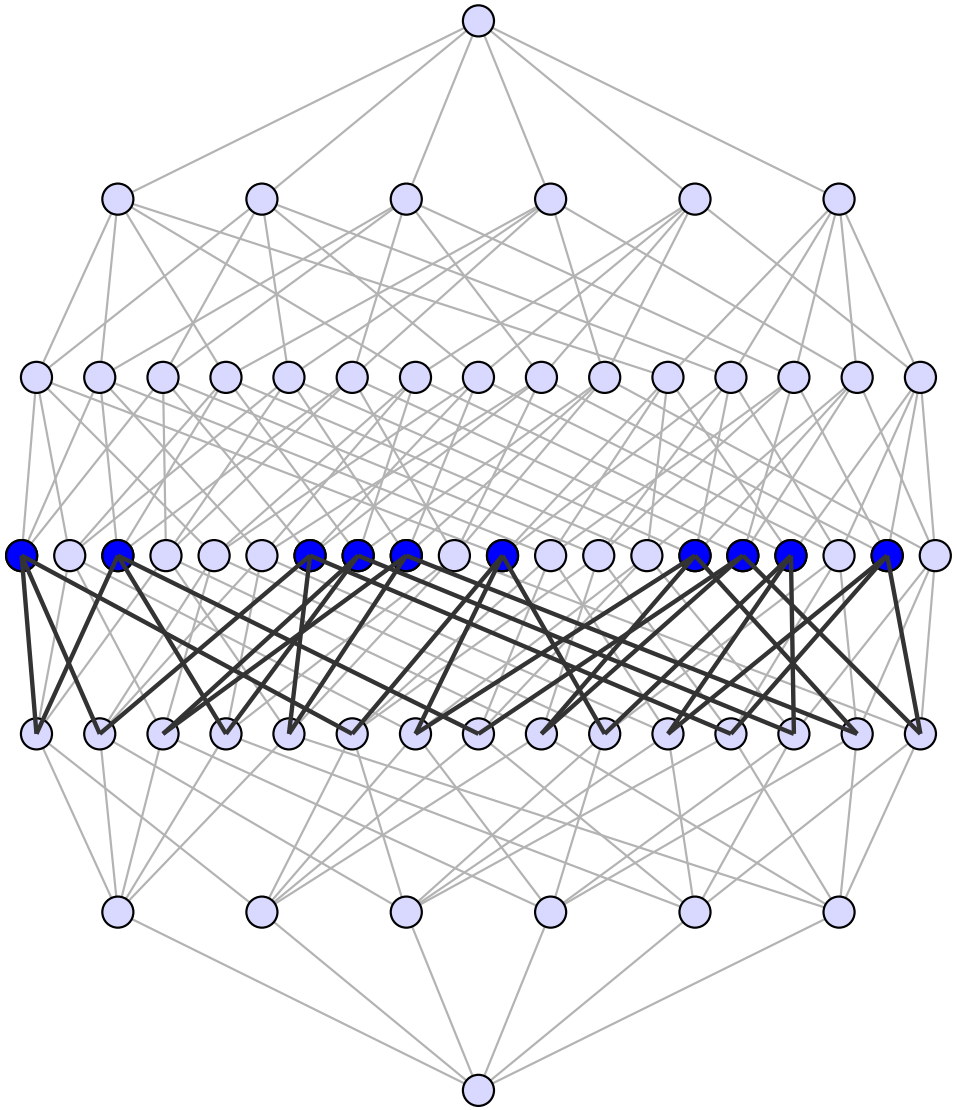
t-(v, k, λ) design $\mathcal{D} = (V, \mathcal{B})$

- V: set of v points
- $\mathcal{B}$: collection 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.

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

Necessary conditions

t-(v,k,λ) design $\mathcal{D}$

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

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

- Necessary conditions:

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

- λ_1: replication number
- λ_0: number of blocks

Symmetry

combinatorial designs

- Two designs $(V, \mathcal{B})$, $(V, \mathcal{B}')$ are considered to be isomorphic if there is a permutation $\pi \in S_V$ such that

$$\pi\mathcal{B} = \mathcal{B}'$$

- A permutation $\pi \in S_V$ is called automorphism of the design $(V, \mathcal{B})$ if

$$\pi\mathcal{B} = \mathcal{B}$$

- S_V is the symmetric group acting on the set V

Computer construction

Kramer-Mesner method

Search for t-(v, k, λ) design:

- Choose subgroup G of S_V as possible automorphism group
- Partition the t- and k-subsets of V into orbits under the action of G
- Combine some of these orbits to t-(v, k, λ) designs, i.e.
  - Compute $M_{t,k}^G$: incidence matrix of orbits
  - Solve the integer linear program:

$$M_{t,k}^G \cdot x = \begin{pmatrix} \lambda \\ \vdots \\ \lambda \end{pmatrix},$$

    where x is a $\{0, 1\}$-vector.
- Good candidates for groups: $(\mathbb{Z}_v, +)$ together with $(\mathbb{Z}_v^*, \cdot)$

q-analogs

q-analogs of combinatorial structures

The q-analog of a combinatorial structure over sets is defined by replacing

- (sub)sets by (sub)spaces and
- cardinalities by dimensions.
- $\mathcal{V}$: vector space of dimension v over $\mathbb{F}_q$
- $\begin{bmatrix} \mathcal{V} \\ k \end{bmatrix}_q$: set of all k-dimensional subspaces of $\mathcal{V}$

Vector space $\mathcal{V} = \mathbb{F}_q^v$

- $\begin{bmatrix} \mathcal{V} \\ k \end{bmatrix}_q$: set of all k-dimensional subspaces of $\mathcal{V}$
- Points of $\mathcal{V}$: one-dimensional subspaces of $\mathcal{V}$, i.e. elements of $\begin{bmatrix} \mathcal{V} \\ 1 \end{bmatrix}_q$
- $\# \begin{bmatrix} \mathcal{V} \\ k \end{bmatrix}_q = \begin{bmatrix} v \\ k \end{bmatrix}_q$ with Gaussian coefficients

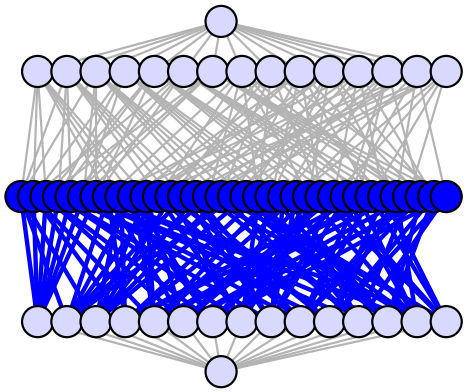
$$\begin{bmatrix} v \\ k \end{bmatrix}_q = \frac{(q^v - 1)(q^{v-1} - 1) \cdots (q^{v-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}$$

- Subspaces can be uniquely described by their row reduced echelon form

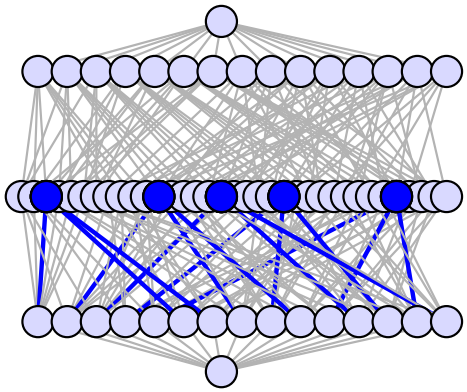
Subspace designs

q-analogs of designs

- $\mathcal{V} = \mathbb{F}_q^v$
- $\mathcal{B} \subseteq \begin{bmatrix} \mathcal{V} \\ k \end{bmatrix}_q$: blocks
- $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ is called t-$(v, k, \lambda)_q$ subspace design if
  each t-subspace of $\mathcal{V}$ is contained in exactly λ blocks.



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



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

$\mathcal{B} = \begin{bmatrix} \mathcal{V} \\ k \end{bmatrix}_q$: complete design

Related parameters

t-$(v,k,\lambda)_q$ subspace design

- Necessary conditions: $\lambda_s = \begin{bmatrix} v-s \\ t-s \end{bmatrix}_q / \begin{bmatrix} k-s \\ t-s \end{bmatrix}_q \in \mathbb{Z}$, $0 \leq s \leq t$
- Number of blocks: λ_0
- Replication number: λ_1
- Complete design: $\lambda_{\max} = \begin{bmatrix} v-t \\ k-t \end{bmatrix}_q$

Connections to Coding Theory

- Random Network Coding, Kötter, Kschischang (2008)
- Majority logic decoding, Romar dela Cruz, W. (2021)

  p-rank of incidence matrix is small – Hamada's formula

Designs in 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

Finite classical polar spaces

Sesquilinear and quadratic forms

- Elliptic quadric $Q^-(2n+1,q) \subset \mathrm{PG}(2n+1,q)$, $n \geq 1$:

$$x_0x_n + \ldots + x_{n-1}x_{2n-1} + f(x_{2n}, x_{2n+1}) = 0,$$

f irreducible quadratic polynomial

- Parabolic quadric $Q(2n,q) \subset \mathrm{PG}(2n,q)$, $n \geq 1$:

$$x_0x_n + \ldots + x_{n-1}x_{2n-1} + x_{2n}^2 = 0,$$

- Hyperbolic quadric $Q^+(2n+1,q) \subset \mathrm{PG}(2n+1,q)$, $n \geq 0$:

$$x_0x_{n+1} + \ldots + x_nx_{2n+1} = 0,$$

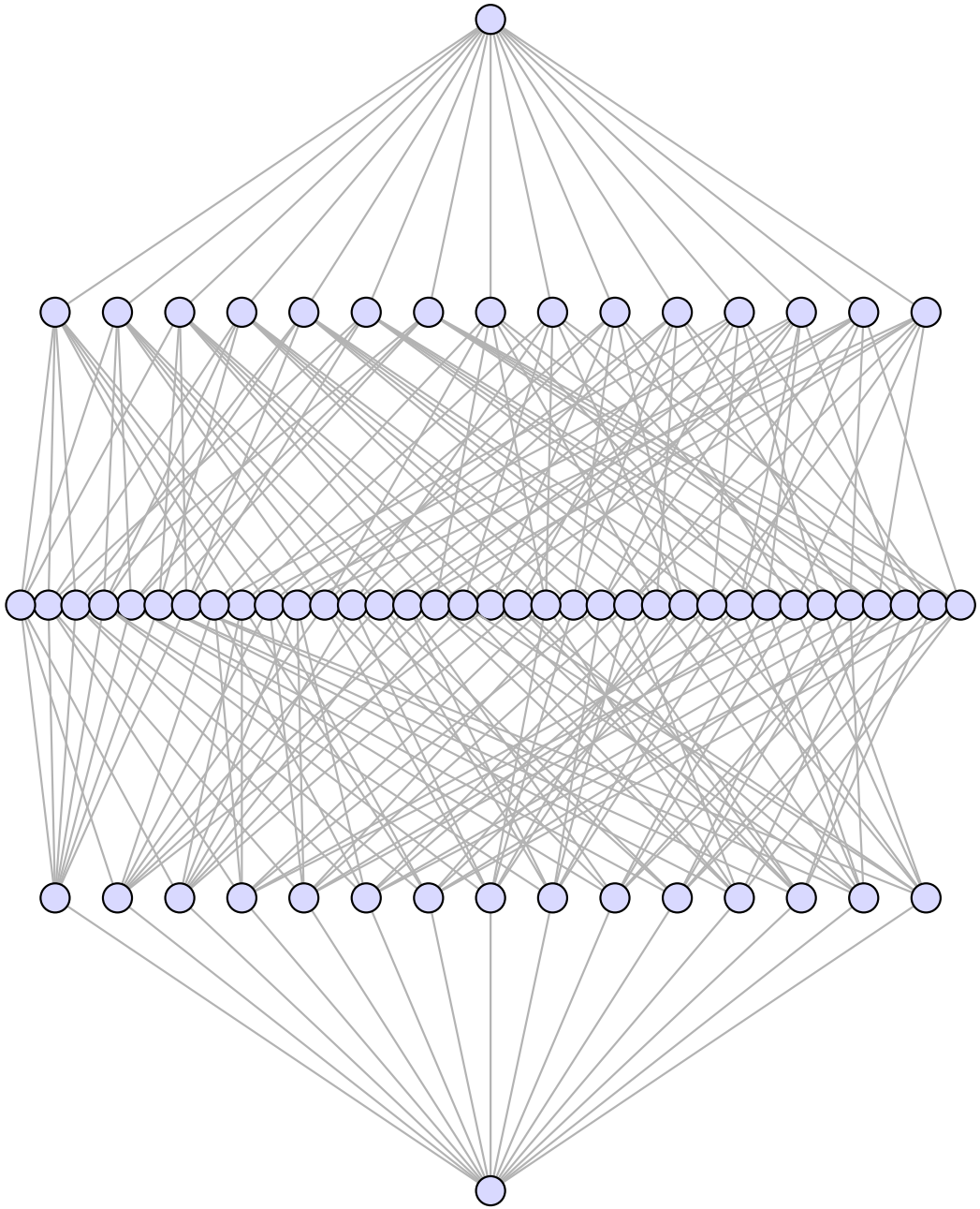
- Symplectic polar space $W(2n+1,q) \subset \mathrm{PG}(2n+1,q)$, $n \geq 0$:

$$x_0y_1 - x_1y_0 + \ldots + x_{2n}y_{2n+1} - x_{2n+1}y_{2n} = 0,$$

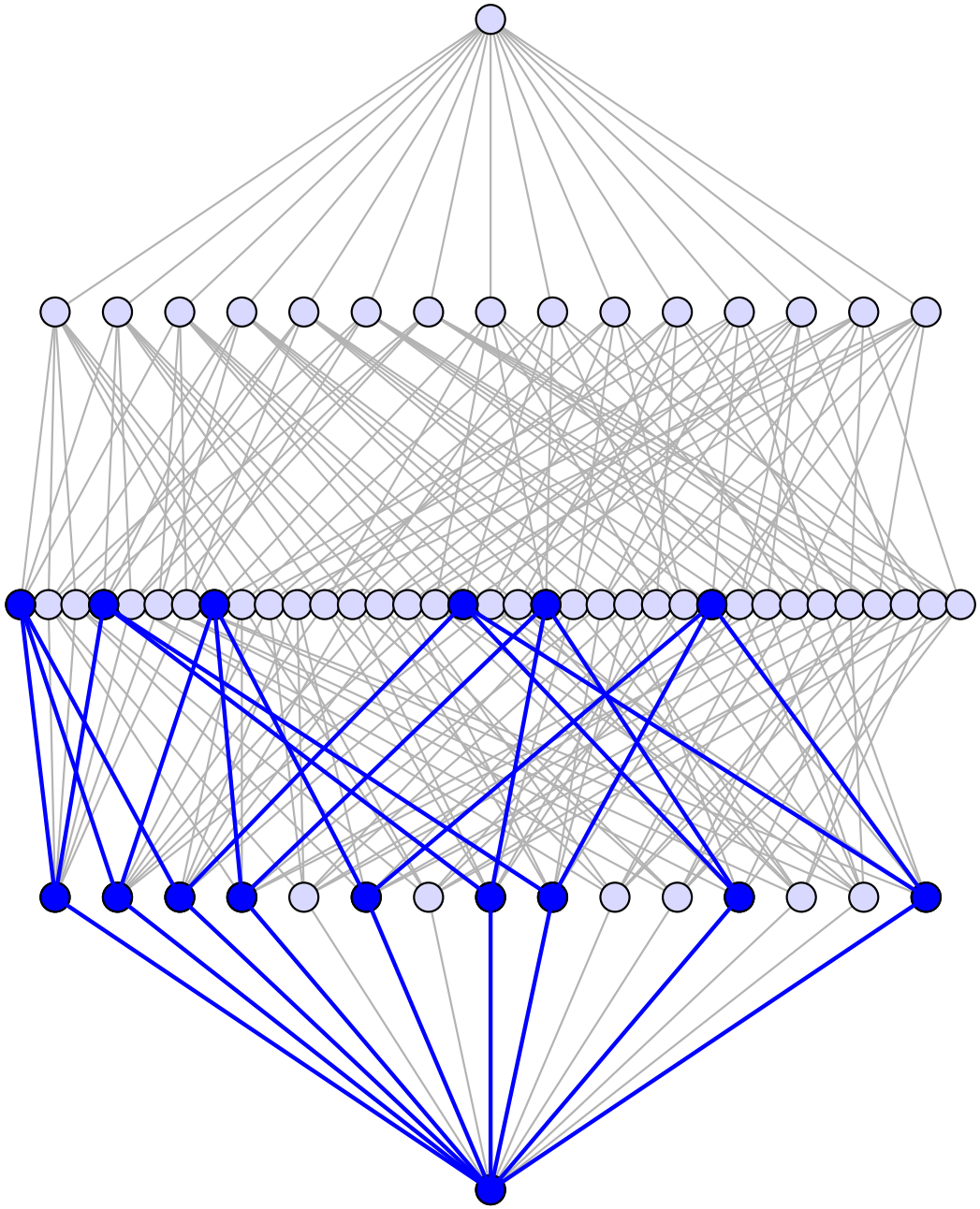
- Hermitian variety $H(n,q^2) \subset \mathrm{PG}(n,q^2)$, $n \geq 1$:

$$x_0^{q+1} + \ldots + x_n^{q+1} = 0$$

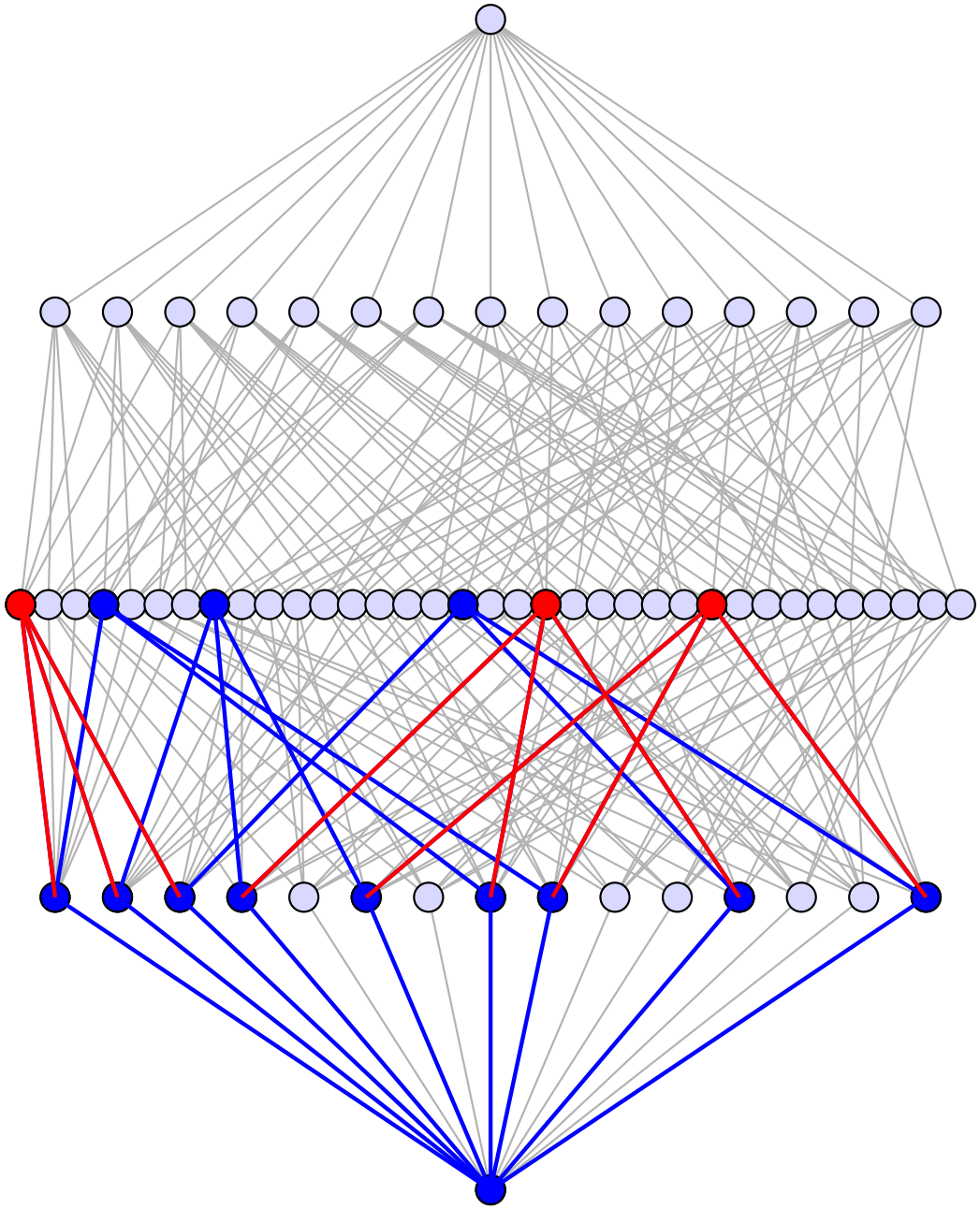
$Q^+(3,2)$ embedded in $PG(3,2)$ $(\mathbb{F}_2^4)$



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



$Q^+(3,2)$ 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
- $\begin{bmatrix} v \\ k \end{bmatrix}_{\mathcal{Q}}$: number of k-dimensional subspaces in $\mathcal{Q}$,
  see Brouwer, Cohen, Neumaier, Distance regular graphs
- A subspace of maximum dimension r in a polar space $\mathcal{Q}$:
  generator
- r: rank of $\mathcal{Q}$

Designs in finite classical polar spaces

Definition

- finite polar space $\mathcal{Q} \subset \mathrm{PG}(v-1, q)$, v minimal
- family $\mathcal{B}$ of k-dimensional subspaces in $\mathcal{Q}$ (blocks)
- $\mathcal{D} = (\mathcal{Q}, \mathcal{B})$ is called a t-$(v, k, \lambda)_{\mathcal{Q}}$-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

Related parameters

Easy counting gives:

- Necessary conditions:

$$\lambda_s = \lambda \frac{\begin{bmatrix} v \\ t \end{bmatrix}_{\mathcal{Q}} \begin{bmatrix} k \\ s \end{bmatrix}_q}{\begin{bmatrix} v \\ s \end{bmatrix}_{\mathcal{Q}} \begin{bmatrix} k \\ t \end{bmatrix}_q} \in \mathbb{Z},\ 0 \leq s \leq t$$

- Number of blocks: λ_0
- Replication number: λ_1
- The complete design consisting of all generators of $\mathcal{Q}$ is a design for

$$\lambda_{\max} = \frac{\begin{bmatrix} v \\ k \end{bmatrix}_{\mathcal{Q}} \begin{bmatrix} k \\ t \end{bmatrix}_q}{\begin{bmatrix} v \\ t \end{bmatrix}_{\mathcal{Q}}}$$

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 Coding Theory

Kerdock sets

- Hyperbolic quadric $Q^+(2n+1,q) \subset \mathbb{F}_q^{2n+2}$

$$x_0x_{n+1} + \ldots + x_nx_{2n+1} = 0 \iff x \cdot \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \cdot x^\top = 0$$

- Lift matrices $\mathbb{F}_q^{(n+1)\times(n+1)} \ni A \mapsto (I \mid A) \in \begin{bmatrix} \mathbb{F}_q^{2n+2} \\ n+1 \end{bmatrix}_q$:

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

- Elements of Q^+ correspond to (skew) symmetric matrices
- . . . it follows:

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

Finite Geometry

- Let $\mathcal{Q}$ be a polar space in dimension v and rank r
- 1-$(v, r, 1)_{\mathcal{Q}}$ designs are also known as spreads
- t-$(v, r, m)_{\mathcal{Q}}$ designs are also known as

  m-regular systems with regard to $(t-1)$-spaces [Segre (1965)]

  Here, $m = \lambda$, see further Cossidente, Marino, Pavese, Smaldore (2021)
- Apparantly, t-(v, k, λ) designs have not yet been studied for

$$k < r$$

Known designs I

- Let $\mathcal{Q}$ be a polar space in dimension v and rank r
- Complete designs in $\mathcal{Q}$ are designs for all t
- In $\mathcal{Q} = Q^+$ the set of generators partitions always in two classes (latins and greeks):
  $(r-1)$-$(v, r, 1)_{\mathcal{Q}}$ designs
- Spreads in $\mathcal{Q}$:
  1-$(v, r, 1)_{\mathcal{Q}}$ designs [see De Beule, Klein, Metsch (2010)]
- λ-regular systems with regard to 0-spaces:
  1-$(v, r, \lambda)_{\mathcal{Q}}$ designs [see Cossidente, et. al (2021)]

Known designs II

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

Nonexistence results I

Steiner systems, i.e. $\lambda = 1$

- Let $\mathcal{Q}$ be a polar space in dimension v and rank r
- There are no 2-$(v, r, 1)_{\mathcal{Q}}$ designs
  - in $Q(6, q)$ [Payne and Thas]
  - in $W(5, q)$ [Thomas]
  - in $Q^-(7, q)$ [Panigraphi]
  - in $Q^+(4n + 3, q)$

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

$\mathcal{Q}$ finite classical polar space.
There are no Steiner systems t-$(v, r, 1)_{\mathcal{Q}}$ for $2 \leq t \leq r - 2$ beside trivial cases.

Nonexistence results II

$t = r - 1$

- Let $\mathcal{Q}$ be a polar space of type
$$Q(2r, q),\ W(2r-1, q) \text{ or } H(2r-1, q^2)$$
of rank $r \geq 3$ and dimension v.
- Nontrivial $(r-1)$-$(v, r, \lambda)_{\mathcal{Q}}$ design
$\Rightarrow\ \lambda = (q+1)/2 = \lambda_{\max}/2$.
- [Bamberg, Lansdown, Lee (2021)]

New computer constructions

Symmetry

The ambient groups of symmetry are

- orthogonal groups
- unitary groups
- symplectic groups

Computer search

- Kramer-Mesner method
- Prescribed automorphism groups: cyclic subgroups or their normalizers
- Promising groups: not yet clear
- Search method based on lattice basis reduction [solvediophant, see W. (IWOCA 2021)]
- Kiermaier, Schmidt, W. (2022+, in preparation)

Results Q^-

2-designs for $q = 2$:

space	k	$\lambda_{\max}$	$\nexists\lambda$	$\exists\lambda$
$Q^-(7,2)$	3	5	1	2 (De Bruyn, Vanhove)
$Q^-(9,2)$	3	27		6, 9, 12, $\Delta_\lambda = 3$
$Q^-(9,2)$	4	45	1	9, 11, 12, 14, 15, 16, 18, 19, 21
$Q^-(11,2)$	5	765	1	240, 245, 275, 280, 315, 360

2-designs for $q = 3$:

space	$\lambda_{\max}$	$\nexists\lambda$	$\exists\lambda$
$Q^-(7,3)$	10	1	2, 5

Results Q

2-designs for $q = 2$:

space	k	$\lambda_{\max}$	$\nexists\lambda$	$\exists\lambda$
$Q(6,2)$	3	3	1	-
$Q(8,2)$	3	15		6, 7
$Q(8,2)$	4	15	1	5, 6, 7
$Q(10,2)$	5	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

2-designs for $q = 3$:

space	$\lambda_{\max}$	$\nexists\lambda$	$\exists\lambda$
$Q(6,3)$	4	1	2 (De Bruyn, Vanhove)
$Q(8,3)$	40	1	8, 20

Results Q^+

2-designs for $q = 2$:

space	k	$\lambda_{\max}$	$\nexists\lambda$	$\exists\lambda$
$Q^+(5,2)$	3	2	-	1*
$Q^+(7,2)$	3	9		3, $\Delta_\lambda = 3$
$Q^+(7,2)$	4	6	1,2	3*
$Q^+(9,2)$	5	30	1	6, 8, 10, 12, 14, 15*
$Q^+(11,2)$	6	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-designs for $q = 3$:

space	$\lambda_{\max}$	$\nexists\lambda$	$\exists\lambda$
$Q^+(5,3)$	2	-	1*
$Q^+(7,3)$	8	1	4*
$Q^+(9,3)$	80	1	8, 16, 32, 40*

Results W

2-designs for $q = 2$:

$Q(2n, 2) = W(2n - 1, 2)$

2-designs for $q = 3$:

space	λ_{max}	$\nexists\lambda$	$\exists\lambda$
$W(5, 3)$	4	1, 2	- (2 shown by De Bruyn, Vanhove)
$W(7, 3)$	40	1	20
$W(9, 3)$	1120	1	

Open questions

- More structural results
- More examples
- Infinite series
- Large sets of designs. Partial results available: hemisystems are "halvings"
- Properties of resulting codes, e.g. p-ranks

Thank you for listening and

congratulations to Joachim!