Linear Codes from q-analogues in Design Theory

Alfred Wassermann

Department of Mathematics, Universität Bayreuth, Germany

Combinatorial Designs and Codes — Rijeka — July 15, 2021

Outline

Combinatorial designs

- $0 \leq t \leq k \leq v$: integers
- λ: non-negative integer
- 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.

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

- $\#\mathcal{B} = \lambda \binom{v}{t} / \binom{k}{t}$
- every point $P \in V$ appears in $r = \lambda \binom{v-1}{t-1} / \binom{k-1}{t-1}$ blocks
- r is called replication number
- we will just consider simple designs

Majority logic decoding and designs

Rudolph (1967), Ng (1970)

- Based on Reed (1954): First non-trivial majority logic decoding scheme
- Given: 2-(v, k, λ) design $\mathcal{D} = (V, \mathcal{B})$ with $V = \{0, 1, \ldots, v-1\}$
- Characteristic vectors of $\mathcal{B}$ are the rows of a $\#\mathcal{B} \times v$ incidence matrix $H_{\mathcal{D}}$ between blocks and points of $\mathcal{D}$
- Code $C_{\mathcal{D}} \leq \mathbb{F}_p^v$: p-ary linear code of length v having parity-check matrix $H_{\mathcal{D}}$

Majority logic decoding and designs

Task

- Sent: $c = (c_0, c_1, \ldots, c_{v-1}) \in C_{\mathcal{D}}$
- $H_{\mathcal{D}} \cdot (c_0, c_1, \ldots, c_{v-1})^\top = 0$
- Error: $e = (e_0, e_1, \ldots, e_{v-1})$
- Received:

$$y = (y_0, y_1, \ldots, y_{v-1}) = c + e \mod p$$

- Decode y, i.e. find c

Decode y_0:

- Assume point 0 to be in design blocks B_0, ..., B_{r-1},
- corresponding to rows h_0, ..., h_{r-1} of $H_{\mathcal{D}}$
- $0 = \sum_{j=0}^{v-1} h_{ij} c_j$ for $0 \leq i < r$
- $c_0 = -h_{i0}^{-1} \sum_{j=1}^{v-1} h_{ij} c_j$ for $0 \leq i < r$

Decoding y_0

- $r+1$ equations give $r+1$ estimates for c_0:

$$c_0^{(0)} = -h_{00}^{-1} \sum_{j=1}^{v-1} h_{0j} \cdot y_j \pmod p$$

$$c_0^{(1)} = -h_{10}^{-1} \sum_{j=1}^{v-1} h_{1j} \cdot y_j \pmod p$$

$$\vdots$$

$$c_0^{(r-1)} = -h_{(r-1)0}^{-1} \sum_{j=1}^{v-1} h_{(r-1)j} \cdot y_j \pmod p$$

$$c_0^{(r)} = y_0 \qquad \text{(counted } \lambda \text{ times)}$$

- Majority decision: $c_0^{(0)}, \ldots, c_0^{(r)} \to c_0$
- Each error spoils at most λ equations (for c_0)
- Requirement: $\#\text{errors} \cdot \lambda < (r+\lambda)/2$

Majority logic decoding

Remarks

- To be precise: One-step majority logic decoding
- In most cases, more than $\lfloor \frac{r+\lambda-1}{2\lambda} \rfloor$ errors can be corrected
- t-designs for $t > 2$: error analysis by Rahman, Blake (1975)
- $\lambda = 1$: orthogonal check equations

Applications

- Circuit is very easy to realize
- Still interesting: e.g. for nano-structure storage
- Hardware implemention: only cyclic designs are interesting

Connections

Majority logic decodable codes with orthogonal check equations are closely connected to

- Linear locally repairable codes, Huang et. al. (2015)
- Private information retrieval (PIR) codes, Fazeli, Vardy, Yaakobi (2015)

Performance of this decoder

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

- Length: v
- Dimension: $\dim C_{\mathcal{D}} = v - \mathrm{rank}_p\, H_{\mathcal{D}}$
- Majority logic decodes at least $\lfloor \frac{r+\lambda-1}{2\lambda} \rfloor$ errors
- #equations: $r+1$

Drawback:

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

Theorem (Hamada)

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

- *If $\mathrm{rank}_p\, H_{\mathcal{D}} < v-1$, then p divides $r-\lambda$.*

Classical / geometric designs

Finite geometry

- prime power q
- $\mathcal{V} = \mathbb{F}_q^v$
- $\begin{bmatrix}\mathcal{V}\\ m\end{bmatrix}_q$: set of all m-dimensional subspaces of $\mathcal{V}$ (m-subspaces)
- Gaussian coefficient:

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

Designs from projective geometry

- Let $q = p^f$ and $2 \leq k < v$
- $\mathcal{V} = \mathbb{F}_q^v$
- Classical / geometric design $\mathcal{G} = (V, \mathcal{B})$ [Bose (1939)]:
  - $V = \begin{bmatrix} \mathcal{V} \\ 1 \end{bmatrix}_q$
  - $\mathcal{B} = \begin{bmatrix} \mathcal{V} \\ k \end{bmatrix}_q$, i.e. all k-subspaces in $\mathcal{V}$
  - $\mathcal{G}$: combinatorial design with parameters

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

  - $\lambda = \begin{bmatrix} v-2 \\ k-2 \end{bmatrix}_q, \quad r = \lambda \frac{\begin{bmatrix} v-1 \\ 1 \end{bmatrix}_q}{\begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q}$
- Most interesting for majority logic decoding:

$$t = k = 2 \qquad (\Rightarrow \lambda = 1, \text{ i.e. orthogonal checks})$$

- Suggested by Rudolph (1967)

p-rank of classical designs

Theorem (Hamada (1973))

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

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

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

Hamada conjecture

Conjecture: Hamada (1973)

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

Tonchev (1986)

There are other designs having the same p-rank as the classical designs.

The codes

Codes from classical designs

affine case:

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

projective case:

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

- Incidence matrices in affine spaces give closely related codes
- Since Rudolph (1967), codes from incidence matrices of various structures in finite geometry have been studied.
- Assmus / Key: Designs and their codes (1992)
- See e.g. Lavrauw, Storme, Van de Voorde (2008)

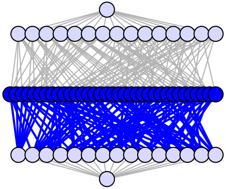
Subspace designs

Subspace designs

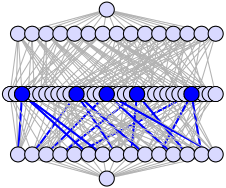
q-analogs of designs

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

- $\mathcal{V} = \mathbb{F}_q^v$
- $\mathcal{B} \subseteq \begin{bmatrix}\mathcal{V}\\k\end{bmatrix}_q$: blocks, $\begin{bmatrix}\mathcal{V}\\1\end{bmatrix}_q$: points
- every t-dimensional subspace $T \in \begin{bmatrix}\mathcal{V}\\t\end{bmatrix}_q$ is contained in exactly λ blocks of $\mathcal{B}$
- $\mathcal{B} = \begin{bmatrix}\mathcal{V}\\k\end{bmatrix}_q$: complete design



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



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

History of subspace designs

- Introduced by Ray-Chaudhuri, Cameron, Delsarte in the early 1970s
- First nontrivial subspace design for $t \geq 2$:
  Thomas (1987)
- Many computer constructions:
  Braun, Kerber, Laue (2005)
- Nontrivial q-Steiner systems (i.e. $\lambda = 1$):
  Braun, Etzion, Östergård, Vardy, W. (2013)
- Recent survey:
  Greferath, Pavčević, Silberstein, Vázquez-Castro:
  Network Coding and Subspace Designs (2018)

Necessary conditions

- Necessary conditions for t-$(v, k, \lambda)_q$:

$$\lambda_i = \lambda \frac{\begin{bmatrix} v-i \\ t-i \end{bmatrix}_q}{\begin{bmatrix} k-i \\ t-i \end{bmatrix}_q} \in \mathbb{Z} \qquad \text{for } i = 0, \ldots, t$$

- $\#\mathcal{B} = \lambda_0 = \lambda \frac{\begin{bmatrix} v \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q}$
- $r = \lambda_1 = \lambda \frac{\begin{bmatrix} v-1 \\ 1 \end{bmatrix}_q}{\begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q}$
- Complete design: $\lambda_{\max} = \begin{bmatrix} v-t \\ k-t \end{bmatrix}_q$

Known subspace designs

families

- 1-$(v, k, 1)_q$ with $k \mid v$: spreads
- 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 $\pm 1 \equiv v \pmod 6$

Known subspace designs

computer constructions

Braun, Kerber, Laue (2005), S. Braun (2010)

t-$(v,k,\lambda)_q$	G	$\lambda_{\max}$	λ
3-$(8,4,\lambda)_2$	$\langle\sigma,\phi^2\rangle$	31	11, 15
2-$(10,3,\lambda)_2$	$\langle\sigma,\phi\rangle$	255	15, 30, 45, 60, 75, 90, 105, 120
2-$(9,4,\lambda)_2$	$\langle\sigma,\phi\rangle$	2667	21, 63, 84, 126, 147, 189, 210, 252, 273, 315, 336, 378, 399, 441, 462, 504, 525, 567, 576, 588, 630, 651, 693, 714, 756, 777, 819, 840, 882, 903, 945, 966, 1008, 1029, 1071, 1092, 1134, 1155, 1197, 1218, 1260, 1281, 1323
2-$(9,3,\lambda)_2$	$\langle\sigma,\phi^3\rangle$	127	21, 22, 42, 43, 63
2-$(8,4,\lambda)_2$	$\langle\sigma,\phi^2\rangle$	651	21, 35, 56, 70, 91, 105, 126, 140, 161, 175, 196, 210, 231, 245, 266, 280, 301, 315
2-$(8,3,\lambda)_2$	$\langle\sigma\rangle$	63	21
2-$(7,3,\lambda)_2$	$\langle\sigma\rangle$	31	3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
2-$(6,3,\lambda)_2$	$\langle\sigma^7\rangle$	15	3, 6

σ: Singer cycle, ϕ: Frobenius automorphism

Subspace designs $\to$ combinatorial designs

Three types:

$$2\text{-}(v,k,\lambda)_q \to \begin{cases} 2\text{-}(\begin{bmatrix} v \\ 1 \end{bmatrix}_q, \begin{bmatrix} k \\ 1 \end{bmatrix}_q, \lambda) & \text{projective case} \\ 2\text{-}(q^{v-1}, q^{k-1}, \lambda) & \text{affine case} \\ 3\text{-}(q^v, q^k, \lambda), & q = 2 \quad (*) \end{cases}$$

$(*)$: Etzion, Vardy (2011), Dela Cruz, W. (2021)

Resulting codes

- All three types of combinatorial designs give majority logic decodable codes
- Here, we'll focus on the projective case

Subspace designs → combinatorial designs

projective case

- A $2\text{-}(v, k, \lambda)_q$ 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 the complete subspace designs, i.e. have maximum possible λ, $\lambda_{\max}$

Subspace designs vs. classical designs

part I

classical design $\mathcal{G}$

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

subspace design $\mathcal{D}$

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

Observation:

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

$$\Longrightarrow$$

$$\operatorname{rank}_p H_{\mathcal{D}} \leq \operatorname{rank}_p H_{\mathcal{G}} \quad \text{and} \quad C_{\mathcal{D}} \geq C_{\mathcal{G}}$$

So far: $C_{\mathcal{D}} = C_{\mathcal{G}}$ for all tested examples (which are few)

Subspace designs vs. classical designs

part II

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

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 decodes at least

$$\lfloor \frac{r_{\mathcal{D}} + \lambda - 1}{2\lambda} \rfloor = \lfloor \frac{r_{\mathcal{G}} + \lambda_{\max} - 1}{2\lambda_{\max}} \rfloor$$

  errors
- # equations: $r_{\mathcal{D}} + 1 \leq r_{\mathcal{G}} + 1$
- Suzuki family 2-$(v, 3, q^2 + q + 1)_q$ gives an exponential improvement in the # equations compared to the geometric designs

Subspace designs decoders for $q = 2$

part I

v	k	λ_{known}	$\lambda_{\min}$	$\lambda_{\max}$	r	$(n, \text{dim}, l)_2$	$r_{\max}/r$
3	2	1	1	1	3	(7, 3, 1)	
4	2	1	1	1	7	(15, 4, 3)	
4	3	3	3	3	7	(15, 10, 1)	
5	2	1	1	1	15	(31, 5, 7)	
5	3	7	7	7	35	(31, 15, 2)	
5	4	7	7	7	15	(31, 25, 1)	
6	2	1	1	1	31	(63, 6, 15)	
6	3	3	3	15	31	(63, 21, 5)	5.0
7	2	1	1	1	63	(127, 7, 31)	
7	3	3	1	31	63	(127, 28, 10)	10.3
7	4	15	5	155	135	(127, 63, 4)	10.3
7	5	155	155	155	651	(127, 98, 2)	
7	6	31	31	31	63	(127, 119, 1)	
8	2	1	1	1	127	(255, 8, 63)	
8	3	21	21	63	889	(255, 36, 21)	3.0
8	4	7	7	651	127	(255, 92, 9)	93.0
8	5	465	465	1395	3937	(255, 162, 4)	3.0

Subspace designs decoders for $q = 2$

part II

v	k	λ_{known}	$\lambda_{\min}$	$\lambda_{\max}$	r	$(n, \text{dim}, l)_2$	$r_{\max}/r$
9	2	1	1	1	255	(511, 9, 127)	
9	3	7	1	127	595	(511, 45, 42)	18.1
9	4	21	7	2667	765	(511, 129, 18)	127.0
9	5	93	31	11811	1581	(511, 255, 8)	127.0
9	6	651	93	11811	5355	(511, 381, 4)	18.1
10	2	1	1	1	511	(1023, 10, 255)	
10	3	15	3	255	2555	(1023, 55, 85)	17.0
10	4	595	5	10795	43435	(1023, 175, 36)	18.1
10	5	765	15	97155	26061	(1023, 385, 17)	127.0
10	6	11067	93	200787	182427	(1023, 637, 8)	18.1
10	7	5715	1143	97155	46355	(1023, 847, 4)	17.0
11	2	1	1	1	1023	(2047, 11, 511)	
11	3	7	7	511	2387	(2047, 66, 170)	73.0
11	8	10795	10795	788035	86955	(2047, 1815, 4)	73.0
12	2	1	1	1	2047	(4095, 12, 1023)	
13	2	1	1	1	4095	(8191, 13, 2047)	
13	3	1	1	2047	1365	(8191, 91, 682)	2047.0
13	10	24893	24893	50955971	199485	(8191, 7813, 4)	2047.0

Codes from subspace designs

Summary

Subspace designs with small λ have small decoders (i.e. few equations) without losing error correction capability compared to codes from classical designs

Can we do better?

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

Sufficient for majority logic decoding:

Incidence matrix between blocks / points of combinatorial structure with

- constant replication number of the points
- every pair of points appears in at most λ blocks

Desirable:

- Blocks are subspaces of $\mathbb{F}_q^v$ $\rightarrow$ submatrix of $H_{\mathcal{G}}$ $\rightarrow$ Hamada formula is involved
- Cyclic structure

More q-analogues

Candidates

1. q-analogues of group divisible designs
2. lifted MRD codes
3. designs in classical polar spaces

q-analogues of group divisible designs

A q-analog of a group divisible design (q-GDD) with parameters $(v, g, k, \lambda)_q$ is a triple $(\mathcal{V}, \mathcal{G}, \mathcal{B})$, where

- $\mathcal{G}$ is a partition of $\begin{bmatrix}\mathcal{V}\\1\end{bmatrix}_q$ into g-subspaces
  (g-spread, the groups, $\#\mathcal{G} > 1$)
- $\mathcal{B}$ is a family of k-subspaces (blocks) of $\mathcal{V}$ such that
  every 2-dimensional subspace $L \in \begin{bmatrix}\mathcal{V}\\2\end{bmatrix}_q$ occurs in exactly λ blocks or one spread element, but not both.

Remarks

- Introduced in Buratti, Kiermaier, Kurz, Nakić, W. (2019)
- Blocks B are scattered subspaces with respect to spread $\mathcal{G}$

Replication number

- $r = \lambda \frac{\begin{bmatrix}v-1\\1\end{bmatrix}_q - \begin{bmatrix}g-1\\1\end{bmatrix}_q}{\begin{bmatrix}k-1\\1\end{bmatrix}_q}$

q-analogues of group divisible designs

Improved decoders

Using constructions from Buratti, Kiermaier, Kurz, Nakić, W. (2019):

$\mathcal{D}$	r	q-GDD	r	$[n, \dim, \ell]_2$
$2\text{-}(6,3,3)_2$	31	$(6,2,3,2)_2$	20	$[63,21,5]_2$
$2\text{-}(8,3,21)_2$	889	$(8,2,3,2)_2$	84	$[255,36,21]_2$
$2\text{-}(9,3,7)_2$	595	$(9,3,3,2)_2$	168	$[511,45,42]_2$
$2\text{-}(10,3,15)_2$	2555	$(10,2,3,14)_2$	2380	$[1023,55,85]_2$

Burst error correction?

Errors in the same spread elements are treated independently

Lifted MRD codes

Rank distance codes – MRD codes

- $\mathbb{F}_q^{k\times m}$, $k \leq m$
- Rank distance: for $A, B \in \mathbb{F}_q^{k\times m}$: $d_r(A,B) = \mathrm{rank}(A-B)$
- Rank metric code: $\mathcal{C} \subseteq (\mathbb{F}_q^{k\times m}, d_r)$
- $d_r(\mathcal{C}) = \min\{d_r(A,B) \mid A \neq B \in \mathcal{C}\}$

- Singleton bound: $\#\mathcal{C} \leq q^{m(k-d_r+1)}$
- Equality can always be attained (Gabidulin codes): Maximum rank distance codes – MRD codes
- Delsarte (1978), Gabidulin (1985)

Lifted MRD codes

subspace codes

Kötter, Kschischang (2008):

- $\mathcal{C}_r \subseteq (\mathbb{F}_q^{k\times m}, d_r)$ MRD code
- $v = k + m$, $\mathcal{V} = \mathbb{F}_q^v$
- $A \in \mathcal{C}_r$: $\langle (I \mid A) \rangle$, row space
- Subspace code $\mathcal{C} = \{\langle (I \mid A)\rangle \leq \mathcal{V} \mid A \in \mathcal{C}_r\}$
- $\#\mathcal{C} = q^{m(k-d_r+1)}$
- Subspace distance: $d_s(\mathcal{C}) = 2d_r(\mathcal{C}_r)$

Lifted $(k \times m, d_r)$ MRD code $\mathcal{C}$

transversal design

Etzion, Silberstein (2013):

- Define $S := \langle (0 \mid I) \rangle$
- Each $(k - d_r + 1)$-subspace of $\mathcal{V}$, disjoint from S, is contained in exactly one codeword of $\mathcal{C}$
- Let $0 \leq i \leq k - d_r - 1$. Each $(k - d_r - i)$-subspace of $\mathcal{V}$, disjoint from S, is contained in exactly $q^{m(i+1)}$ codewords of $\mathcal{C}$
- The codewords of $\mathcal{C}$ form the blocks of a transversal design $\mathrm{TD}_\lambda(\begin{bmatrix} k \\ 1 \end{bmatrix}_q, q^m)$ with $\lambda = q^{m(k-d_r-1)}$
- $r = q^{m(k-d_r)}$
- $\rightarrow$ take incidence matrix of TD as parity-check matrix
- See also Lavauzelle (2018): TDs as PIR codes

Bounds on the rank of $H_\mathcal{C}$

- Etzion, Silberstein (2013):
  $q^m \le \operatorname{rank}_2 H_\mathcal{C} \le \begin{bmatrix} k \\ 1 \end{bmatrix}_q (q^m - 1) + 1$ if q even.
- Kiermaier, Kurz, W. (2021+):
  $$\operatorname{rank}_p H_\mathcal{C} \le \underbrace{\operatorname{rank} H_\mathcal{G}}_{\text{Hamada formula}} - \begin{bmatrix} m \\ 1 \end{bmatrix}_q$$

Example:

- $\mathbb{F}_2^{3\times 4}$: $k = 3, m = 4$ with $d_r = 2$.
- $\mathrm{TD}_1(7, 16)$, $n = 112 \to$ orthogonal checks
- Etzion, Silberstein (2013): $16 \le \operatorname{rank}_2 H_\mathcal{C} \le 106$
- Kiermaier, Kurz, W. (2021+):
  - Bound: $\operatorname{rank}_2 H_\mathcal{C} \le 84$
  - Computer enumeration: there are 33 MRD codes
  - Rank spectrum: $68 \le \operatorname{rank}_2 H_\mathcal{C} \le 83$
  - Rank 68: $[112, 44, 24]_2$ code
    - Meets known lower bound
    - One-step majority logic decoding corrects 8 errors

Designs in polar spaces

Finite classical polar spaces

type	v	rank
$Q^-(2n+1,q)$	$2n+2$	n
$Q(2n,q)$	$2n+1$	n
$Q^+(2n+1,q)$	$2n+2$	$n+1$
$W(2n+1,q)$	$2n+2$	$n+1$
$H(2n,q^2)$	$n+1$	n
$H(2n+1,q^2)$	$n+2$	$n+1$

Definition

A family of generators (subspaces of maximal rank k) in a finite polar space $\mathcal{Q}$ is called t-design if there exists a positive integer λ such that every t-dimensional subspace of $\mathcal{Q}$ is contained in exactly λ blocks. (Dimensions are vector space dimensions)

Designs in polar spaces

Known results

- Segre (1967): λ-regular system with regard to $t-1$-spaces
- Trivial designs in Q^+ for all t: latins and greeks
- First nontrivial 2-design:
  $Q(6,3)$, $\lambda = 2$ [De Bruyn and Vanhove (2013)]
- Lansdown (2020): more examples for $q = 3, 5$
- See also Cossidente, Marino, Pavese, Smaldore (2021)

Kiermaier, Schmidt, W. (2021+)

- $\lambda_i = \lambda \frac{\begin{bmatrix} n \\ t \end{bmatrix}_Q \begin{bmatrix} k \\ i \end{bmatrix}_q}{\begin{bmatrix} n \\ i \end{bmatrix}_Q \begin{bmatrix} k \\ t \end{bmatrix}_q}$
- $r = \lambda_1$
- ≥ 100 computer constructions for $q = 2, 3$ and $t = 2$

2-designs in polar spaces

Codes from designs in polar spaces

First observations

- Design blocks are subspaces in an ambient vector space $\mathcal{V}$
- Hamada formula somehow involved in rank $H_{\mathcal{D}}$

Examples

$\mathcal{D}$: $(v,k,\lambda)_{\mathcal{Q}}$	rank$_{H_{\mathcal{D}}}$	$[n,k,d]_2$	r	ℓ
$(6,3,1)_{Q+}$	11	$[35,24,4]_2$	3	1
$(8,4,3)_{Q+}$	43	$[135,92]_2$	15	2
$(10,5,6)_{Q+}$	187	$[527,340]_2$	54	4
$(11,5,21)_{Q}$	517	$[1023,506]_2$	357	8
$(8,4,5)_{W}$	135	$[255,120]_2$	45	4
$(8,3,2)_{Q-}$	84	$[119,35,24]_2$	18	4
$(10,4,9)_{Q-}$	330	$[495,165]_2$	153	8

Open questions

Subspace designs, q-GDDs

- Does $\dim C_{\mathcal{D}} = \dim C_{\mathcal{G}}$ always hold?

Lifted MRD codes

- Role of d_r for rank $H_{\mathcal{C}}$? (e.g. 83 vs. 84)

Designs in polar spaces

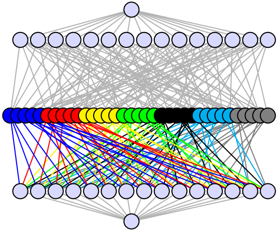
- Bounds for rank $H_{\mathcal{D}}$?

Applications

- Efficient error detection? (resolvable configurations?)
- Only information bits need to be decoded. Can this be exploited?

Summary

q-analogues of design configurations enable the use of the Hamada formula and lead to interesting linear codes



Thank you for listening !

Example

$\mathbb{F}_2^{2\times 2}$: $k = m = 2$ with $d_r = 2$.

$\mathcal{C} = \{\langle\binom{1000}{0100}\rangle, \langle\binom{1010}{0101}\rangle, \langle\binom{1011}{0110}\rangle, \langle\binom{1001}{0111}\rangle\}$ lifted MRD code

$\langle\binom{1000}{0100}\rangle = \{(10|00), (01|00), (11|00)\}$

	$\begin{bmatrix}\mathcal{V}\\1\end{bmatrix}_2 \setminus \begin{bmatrix}S\\1\end{bmatrix}_2$											
	10				01				11			
	00	10	01	11	00	10	01	11	00	10	01	11
$\langle\binom{1000}{0100}\rangle$	1				1				1			
$\langle\binom{1010}{0101}\rangle$		1					1					1
$\langle\binom{1011}{0110}\rangle$				1		1					1	
$\langle\binom{1001}{0111}\rangle$			1					1		1		