Intersection numbers for q-analogs of designs

Michael Kiermaier

Institut für Mathematik
Universität Bayreuth

Conference on Random network codes
and Designs over GF(q)
September 18, 2013
Ghent University

joint work with Mario Pavčević

Notation

- prime power q
- v-dim. $\mathbb{F}_q$-vector space V
- Grassmannian $\left[{V \atop k}\right]_q$: set of all k-dim. subspaces of V.
- Gaussian Binomial coefficient

$$\begin{bmatrix} v \\ k \end{bmatrix}_q := \# \begin{bmatrix} V \\ k \end{bmatrix}_q = \frac{(q^v - 1)(q^{v-1} - 1) \cdot \ldots \cdot (q^{v-k+1} - 1)}{(q-1)(q^2-1) \cdot \ldots \cdot (q^k - 1)}$$

Example

How many 2-dimensional subspaces has $\mathbb{F}_2^4$?
Answer ($v = 4$, $k = 2$, $q = 2$):

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_2 = \frac{(2^4 - 1)(2^3 - 1)}{(2^1 - 1)(2^2 - 1)} = \frac{15 \cdot 7}{1 \cdot 3} = 35$$

Definition

$D \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$ is t-$(v, k, \lambda)_q$ design (q-analog of a design)
if
every $T \in \begin{bmatrix} V \\ t \end{bmatrix}_q$ is contained in exactly λ blocks (elements of D).

Connection to network coding

- Of particular interest: Case $\lambda = 1$ (Steiner System)
- Steiner Systems and *perfect* constant dimension codes are the same:

$$t\text{-}(v, k, 1)_q \text{ Steiner System}$$
$$=$$
$$\text{perfect } (v, 2 \cdot (k - t + 1); k)_q \text{ constant dimension code}$$

Existence of Steiner systems

- $t = 1$ (Spreads):
  $1\text{-}(v, k, 1)_q$ Steiner System exists $\iff$ k divides v
- Braun, Etzion, Östergård, Vardy, Wassermann 2013:
  $$2\text{-}(13, 3, 1)_2 \text{ exists!}$$
- No further Steiner system known.
- Smallest open case:
  $2\text{-}(7, 3, 1)_q$ (q-analog of the Fano plane)
  Existence open for any prime power q.

Lemma

Let D be a t-$(v, k, \lambda)_q$ design and $i \in \{0, \dots, t\}$.
Then D is also an i-$(v, k, \lambda_i)_q$ design with

$$\lambda_i = \frac{\begin{bmatrix} v-i \\ t-i \end{bmatrix}_q}{\begin{bmatrix} k-i \\ t-i \end{bmatrix}_q} \cdot \lambda.$$

In particular, $\#D = \lambda_0$.

Example

For a 2-$(7, 3, 1)_2$ design (2-analog of the Fano plane):

$$\lambda_2 = 1, \quad \lambda_1 = 21, \quad \lambda_0 = 381$$

Corollary: Integrality conditions

If a t-$(v, k, \lambda)_q$ design exists, then $\lambda_0, \lambda_1, \dots, \lambda_t \in \mathbb{Z}$.

Example

- Famous classical Steiner system: 5-$(24, 8, 1)$ Witt design
- Is there a q-analog of the Witt design,
  i.e. a 5-$(24, 8, 1)_q$ design (q some prime power)?

$$\lambda_2 = \frac{\begin{bmatrix}22\\3\end{bmatrix}_q}{\begin{bmatrix}6\\3\end{bmatrix}_q} = \frac{(q^{22}-1)(q^{21}-1)(q^{20}-1)}{(q^6-1)(q^5-1)(q^4-1)}$$

$$= \frac{\Phi_{22}(q)\Phi_{21}(q)\Phi_{20}(q)\Phi_{11}(q)\Phi_{10}(q)\Phi_7(q)}{\Phi_6(q)}$$

  where Φ_n the n-th cyclotomic polynomial.
- Known: If a/b is not the power of a prime, then
  $\gcd(\Phi_a(x), \Phi_b(x)) = 1$ for all $x \in \mathbb{Z}$.
  $\implies \lambda_2 \notin \mathbb{Z}$ for all prime powers q.
- Integrality conditions:
  There is no q-analog of the Witt design!

Intersection numbers

- Mendelsohn 1971, Alltop 1975:
  Intersection numbers for t-designs
- Useful tool for construction, classification and non-existence proofs of classical designs.
- Goal: Generalize intersection numbers to q-analogs of designs.

Definition

- In the following: D a t-$(v, k, \lambda)_q$ design, S a subspace of V, $s = \dim(S)$
- The i-th intersection number of S in D is

$$\alpha_i = \alpha_i(S) = \#\{B \in D \mid \dim(B \cap S) = i\}.$$

- The intersection vector of S in D is

$$(\alpha_0(S), \alpha_1(S), \ldots, \alpha_k(S))$$

Theorem (q-analog of Mendelsohn equations 1971)

For $i \in \{0, \dots, t\}$

$$\sum_{j=i}^{s} \begin{bmatrix} j \\ i \end{bmatrix}_q \alpha_j = \begin{bmatrix} s \\ i \end{bmatrix}_q \lambda_i$$

Proof.

Double count

$$X = \left\{ (I, B) \in \begin{bmatrix} V \\ i \end{bmatrix}_q \times D \mid I \leq B \cap S \right\}$$

- $\left[\begin{smallmatrix} s \\ i \end{smallmatrix}\right]_q$ possibilities for I.
  For each I, λ_i blocks B with $I \leq B$.
  $\implies \#X = \left[\begin{smallmatrix} s \\ i \end{smallmatrix}\right]_q \lambda_i$.
- For fixed block B, there are $\left[\begin{smallmatrix} \dim(B \cap S) \\ i \end{smallmatrix}\right]_q$ suitable I.
  $\implies \#X = \sum_{j=i}^{s} \left[\begin{smallmatrix} j \\ i \end{smallmatrix}\right]_q \alpha_j$.

□

Theorem (q-analog of Köhler equations 1988)

For $i \in \{0, \ldots, t\}$

$$\alpha_i = \begin{bmatrix} s \\ i \end{bmatrix}_q \sum_{j=i}^{t} (-1)^{j-i} q^{\binom{j-i}{2}} \begin{bmatrix} s-i \\ j-i \end{bmatrix}_q \lambda_j + (-1)^{t+1-i} q^{\binom{t+1-i}{2}} \sum_{j=t+1}^{s} \begin{bmatrix} j \\ i \end{bmatrix}_q \begin{bmatrix} j-i-1 \\ t-i \end{bmatrix}_q \alpha_j.$$

(Parameterization of $\alpha_0, \alpha_1 \ldots, \alpha_t$ by $\alpha_{t+1}, \alpha_{t+2}, \ldots, \alpha_k$)

History

- For classical designs by Köhler in 1988, long and complicated induction proof.
- Simpler proof by de Vroedt in 1991.
- Can be simplified further! Idea: Apply Gauss reduction to the Mendelsohn equations.

Proof

- Read Mendelsohn equations as linear equation system on the intersection vector:

$$\left(\begin{array}{ccccc|ccc} \begin{bmatrix}0\\0\end{bmatrix} & \begin{bmatrix}1\\0\end{bmatrix} & \begin{bmatrix}2\\0\end{bmatrix} & \cdots & \begin{bmatrix}t\\0\end{bmatrix} & \begin{bmatrix}t+1\\0\end{bmatrix} & \cdots & \begin{bmatrix}k\\0\end{bmatrix} \\ 0 & \begin{bmatrix}1\\1\end{bmatrix} & \begin{bmatrix}2\\1\end{bmatrix} & \cdots & \begin{bmatrix}t\\1\end{bmatrix} & \begin{bmatrix}t+1\\1\end{bmatrix} & \cdots & \begin{bmatrix}k\\1\end{bmatrix} \\ 0 & 0 & \begin{bmatrix}2\\2\end{bmatrix} & \cdots & \begin{bmatrix}t\\2\end{bmatrix} & \begin{bmatrix}t+1\\2\end{bmatrix} & \cdots & \begin{bmatrix}k\\2\end{bmatrix} \\ \vdots & & \ddots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & \begin{bmatrix}t\\t\end{bmatrix} & \begin{bmatrix}t+1\\t\end{bmatrix} & \cdots & \begin{bmatrix}k\\t\end{bmatrix} \end{array}\right) \begin{pmatrix}\alpha_0\\ \alpha_1\\ \alpha_2\\ \vdots\\ \alpha_k\end{pmatrix} = \begin{pmatrix}\begin{bmatrix}s\\0\end{bmatrix}\lambda_0\\ \begin{bmatrix}s\\1\end{bmatrix}\lambda_1\\ \begin{bmatrix}s\\2\end{bmatrix}\lambda_2\\ \vdots\\ \begin{bmatrix}s\\t\end{bmatrix}\lambda_t\end{pmatrix}$$

- Has the form

$$(P_q \mid A) \cdot \mathbf{x} = \mathbf{b}$$

where $P_q = \left(\begin{bmatrix}i\\j\end{bmatrix}_q\right)_{i,j}$ is upper q-Pascal matrix.

- Known: P_q invertible with $P_q^{-1} = \left((-1)^{j-i} q^{\binom{j-i}{2}} \begin{bmatrix}j\\i\end{bmatrix}_q\right)_{i,j}$.

Proof (cont.)

- Left multiplication of

$$(P_q \mid A) \cdot \mathbf{x} = \mathbf{b}$$

with P_q^{-1} yields

$$(I \mid P_q^{-1} A) \cdot \mathbf{x} = P_q^{-1} \mathbf{b}.$$

- Rows evaluate to the Köhler equations.
Use the q-binomial identity

$$\sum_{j=0}^{t} (-1)^j q^{\binom{j}{2}} \begin{bmatrix} n \\ j \end{bmatrix}_q = (-1)^t q^{\binom{t+1}{2}} \begin{bmatrix} n-1 \\ t \end{bmatrix}_q .$$

to compute $P_q^{-1} A$ and $P_q^{-1} \mathbf{b}$. □

Corollary

Intersection vector is uniquely determined for $\dim(S) \leq t$ and $\dim(S) \geq v - t$.

In the following

Determine the ”intersection structure” of a 2-$(7, 3, 1)_2$ design (2-analog of the Fano plane).
Parameters:

$$v = 7, \quad k = 3, \quad t = 2, \quad \lambda = 1, \quad q = 2$$

$$\lambda_0 = 381, \quad \lambda_1 = 21, \quad \lambda_2 = 1.$$

Example

- Köhler equations for $s = 4$:

$$\begin{aligned}\alpha_0 &= 136 - 8\alpha_3\\ \alpha_1 &= 210 + 14\alpha_3\\ \alpha_2 &= 35 - 7\alpha_3\end{aligned}$$

- $\alpha_3 \in \{0, 1\}$
  Otherwise, S contains two blocks B_1, B_2.
  By the dimension formula

$$\begin{aligned}\dim(B_1 \cap B_2) &= \dim(B_1) + \dim(B_2) - \dim(\underbrace{B_1 + B_2}_{\leq S})\\ &\geq 3 + 3 - 4 = 2. \quad \text{Contradiction.}\end{aligned}$$

- $\implies$ Two possible intersection vectors:
  $(136, 210, 35, 0)$ and $(128, 224, 28, 1)$.

Example (cont.)

- Distribution of the 4-dim subspaces S to the two intersection numbers? (total: $\begin{bmatrix} 7 \\ 4 \end{bmatrix}_2 = 11811$ subspaces S)
- Double counting:
  $(136, 210, 35, 0)$ occurs 6096 times,
  $(128, 224, 28, 1)$ occurs 5715 times.

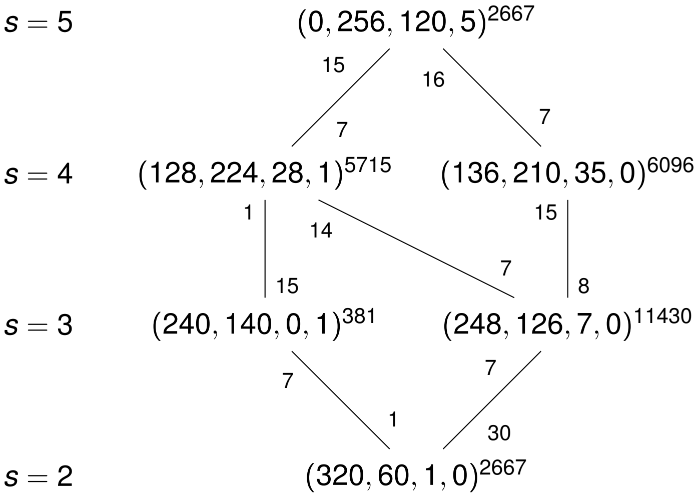
- Similarly, compute the intersection vectors for all possible values of s.

s	intersection vector	frequency
7	$(0, 0, 0, 381)$	1
6	$(0, 0, 336, 45)$	127
5	$(0, 256, 120, 5)$	2667
4	$(128, 224, 28, 1)$	5715
4	$(136, 210, 35, 0)$	6096
3	$(240, 140, 0, 1)$	381
3	$(248, 126, 7, 0)$	11430
2	$(320, 60, 1, 0)$	2667
1	$(360, 21, 0, 0)$	127
0	$(381, 0, 0, 0)$	1

- How do the different S relate to each other?

Theorem

The "intersection structure" of a 2-analog of the Fano plane is



Intersection vectors for arbitrary q

s	intersection vector				frequency
7	$(0,$	$0,$	$0,$	$\Phi_6\Phi_7)$	1
6	$(0,$	$0,$	$q^4\Phi_3\Phi_6,$	$\Phi_2\Phi_4\Phi_6)$	Φ_7
5	$(0,$	$q^8,$	$q^3\Phi_2\Phi_4,$	$\Phi_4)$	$\Phi_3\Phi_6\Phi_7$
4	$(q^7\Phi_1,$	$q^5\Phi_3,$	$q^2\Phi_3,$	$1)$	$\Phi_2\Phi_4\Phi_6\Phi_7$
4	$(q^3(q^5-q^4+1),$	$q\Phi_1\Phi_2\Phi_3\Phi_4,$	$\Phi_3\Phi_4,$	$0)$	$q^4\Phi_6\Phi_7$
3	$(q^4\Phi_4\Phi_2\Phi_1,$	$q^2\Phi_3\Phi_4,$	$0,$	$1)$	$\Phi_6\Phi_7$
3	$(q^3(q^5-q+1),$	$q(q^3+q-1)\Phi_3,$	$\Phi_3,$	$0)$	$q\Phi_2\Phi_4\Phi_6\Phi_7$
2	$(q^6\Phi_4,$	$q^2\Phi_2\Phi_4,$	$1,$	$0)$	$\Phi_3\Phi_6\Phi_7$
1	$(q^3\Phi_2\Phi_4\Phi_6,$	$\Phi_3\Phi_6,$	$0,$	$0)$	Φ_7
0	$(\Phi_6\Phi_7,$	$0,$	$0,$	$0)$	1

Comment

Applying this method to $2\text{-}(9,3,1)_q$ or $2\text{-}(13,3,1)_q$,
we don't end up with a unique intersection vector distribution.

Theorem

If there exists a $2\text{-}(7,3,1)_q$ *design,*
then there exist designs with the parameters

- $2\text{-}(7,3,q^4)_q$
- $2\text{-}(7,3,q^3+q^2+q+1)_q$
- $2\text{-}(7,3,q^4+q^3+q^2+q)_q$

Comment

A $2\text{-}(7,3,16)_2$ design does exist.

Open problems

- Use the Köhler equations for a nonexistence proof.
- Use the intersection structure
  to show the nonexistence / construct a $2\text{-}(7, 3, 1)_2$.