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 $\binom{V}{k}_q$: set of all $k$-dim. subspaces of $V$.
- Gaussian Binomial coefficient

\[
\binom{v}{k}_q := \# \binom{V}{k}_q = \frac{(q^v - 1)(q^{v-1} - 1) \ldots (q^{v-k+1} - 1)}{(q - 1)(q^2 - 1) \ldots (q^k - 1)}
\]

Example

How many 2-dimensional subspaces has $\mathbb{F}_2^4$?

Answer ($v = 4$, $k = 2$, $q = 2$):

\[
\binom{4}{2}_2 = \frac{(2^4 - 1)(2^3 - 1)}{(2^1 - 1)(2^2 - 1)} = \frac{15 \cdot 7}{1 \cdot 3} = 35
\]
Definition

$D \subseteq \binom{V}{k}_q$ is $t-(v, k, \lambda)_q$ design ($q$-analog of a design) if every $T \in \binom{V}{t}_q$ is contained in exactly $\lambda$ 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:

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

- $t = 1$ (Spreads):
  - $1-(v, k, 1)_q$ Steiner System exists $\iff k$ divides $v$

- Braun, Etzion, Östergård, Vardy, Wassermann 2013:
  - $2-(13, 3, 1)_2$ exists!

- No further Steiner system known.

- Smallest open case:
  - $2-(7, 3, 1)_q$ (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 $i \in \{0, \ldots, t\}$. Then $D$ is also an $i-(v, k, \lambda_i)_q$ design with

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

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 $\lambda_0, \lambda_1, \ldots, \lambda_t \in \mathbb{Z}$. 
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)?

$$
\lambda_2 = \frac{\binom{22}{3}_q}{\binom{6}{3}_q} = \frac{(q^{22} - 1)(q^{21} - 1)(q^{20} - 1)}{(q^{6} - 1)(q^{5} - 1)(q^{4} - 1)} = \frac{\Phi_{22}(q)\Phi_{21}(q)\Phi_{20}(q)\Phi_{11}(q)\Phi_{10}(q)\Phi_{7}(q)}{\Phi_{6}(q)}
$$

where $\Phi_n$ 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 $x \in \mathbb{Z}$.

  $$\implies \lambda_2 \notin \mathbb{Z} \text{ for all prime powers } q.$$  

- 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 \( i \in \{0, \ldots, t\} \)
\[
\sum_{j=i}^{s} \binom{j}{i} q^{\alpha_j} = \binom{s}{i} q^{\lambda_i}
\]

Proof.
Double count
\[
X = \left\{ (I, B) \in \binom{V}{i} q \times D \mid I \leq B \cap S \right\}
\]

▷ \( \binom{s}{i} q \) possibilities for \( I \).
For each \( I \), \( \lambda_i \) blocks \( B \) with \( I \leq B \).
\[\implies \#X = \binom{s}{i} q^{\lambda_i}.\]

▷ For fixed block \( B \), there are \( \binom{\dim(B \cap S)}{i} q \) suitable \( I \).
\[\implies \#X = \sum_{j=i}^{s} \binom{j}{i} q^{\alpha_j}.\]
Theorem \((q\text{-analog of Köhler equations 1988})\)

For \(i \in \{0, \ldots, t\}\)

\[
\alpha_i = \binom{s}{i}_q \sum_{j=i}^{t} (-1)^{j-i} q^{\binom{j-i}{2}} \binom{s-i}{j-i}_q \lambda_j 
+ (-1)^{t+1-i} q^{\binom{t+1-i}{2}} \sum_{j=t+1}^{s} \binom{j}{i}_q \binom{j-i-1}{t-i}_q \alpha_j.
\]

(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:

\[
\begin{pmatrix}
0 & 1 & 2 & \ldots & t & t+1 & \ldots & k \\
0 & 1 & 2 & \ldots & t & t+1 & \ldots & k \\
0 & 0 & 1 & \ldots & t & t+1 & \ldots & k \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \ldots & 0 & t & t+1 & \ldots & k
\end{pmatrix}
\begin{pmatrix}
\alpha_0 \\
\alpha_1 \\
\alpha_2 \\
\vdots \\
\alpha_k
\end{pmatrix} =
\begin{pmatrix}
\lambda_0 \\
\lambda_1 \\
\lambda_2 \\
\vdots \\
\lambda_t
\end{pmatrix}
\]

- Has the form

\[(P_q \mid A) \cdot x = b\]

where \(P_q = \binom{i}{j}_q\) is upper \(q\)-Pascal matrix.

- Known: \(P_q\) invertible with \(P_q^{-1} = \binom{j-i}{j}_q \binom{i}{j}_q\).
Proof (cont.)

- Left multiplication of

\[(P_q | A) \cdot x = b\]

with \(P_q^{-1}\) yields

\[(I | P_q^{-1} A) \cdot x = P_q^{-1} b.\]

- Rows evaluate to the Köhler equations.

Use the \(q\)-binomial identity

\[
\sum_{j=0}^{t} (-1)^j q^{(j)} \binom{n}{j} q = (-1)^t q^{t+1} \binom{n-1}{t} q.
\]

to compute \(P_q^{-1} A\) and \(P_q^{-1} b.\) □
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 $s = 4$:
  \[
  \begin{align*}
  \alpha_0 &= 136 - 8\alpha_3 \\
  \alpha_1 &= 210 + 14\alpha_3 \\
  \alpha_2 &= 35 - 7\alpha_3 \\
  \end{align*}
  \]

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

  By the dimension formula

  \[
  \dim(B_1 \cap B_2) = \dim(B_1) + \dim(B_2) - \dim(B_1 + B_2) \leq S
  \]

  \[
  \geq 3 + 3 - 4 = 2. \quad \text{Contradiction.}
  \]

- $\implies$ 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: $\binom{7}{4}_2 = 11811$ 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 $s$.

<table>
<thead>
<tr>
<th>$s$</th>
<th>Intersection vector</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>$(0, 0, 0, 381)$</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>$(0, 0, 336, 45)$</td>
<td>127</td>
</tr>
<tr>
<td>5</td>
<td>$(0, 256, 120, 5)$</td>
<td>2667</td>
</tr>
<tr>
<td>4</td>
<td>$(128, 224, 28, 1)$</td>
<td>5715</td>
</tr>
<tr>
<td>4</td>
<td>$(136, 210, 35, 0)$</td>
<td>6096</td>
</tr>
<tr>
<td>3</td>
<td>$(240, 140, 0, 1)$</td>
<td>381</td>
</tr>
<tr>
<td>3</td>
<td>$(248, 126, 7, 0)$</td>
<td>11430</td>
</tr>
<tr>
<td>2</td>
<td>$(320, 60, 1, 0)$</td>
<td>2667</td>
</tr>
<tr>
<td>1</td>
<td>$(360, 21, 0, 0)$</td>
<td>127</td>
</tr>
<tr>
<td>0</td>
<td>$(381, 0, 0, 0)$</td>
<td>1</td>
</tr>
</tbody>
</table>

How do the different $S$ relate to each other?
Theorem

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

\[
\begin{align*}
    s = 5 & \quad (0, 256, 120, 5)^{2667} \\
    & \quad 15 \quad 16 \\
    & \quad 7 \quad 7 \\
    s = 4 & \quad (128, 224, 28, 1)^{5715} \quad (136, 210, 35, 0)^{6096} \\
    & \quad 1 \quad 14 \quad 15 \\
    & \quad 15 \quad 7 \quad 8 \\
    s = 3 & \quad (240, 140, 0, 1)^{381} \quad (248, 126, 7, 0)^{11430} \\
    & \quad 7 \quad 1 \quad 30 \\
    s = 2 & \quad (320, 60, 1, 0)^{2667}
\end{align*}
\]
Intersection vectors for arbitrary $q$

<table>
<thead>
<tr>
<th>$s$</th>
<th>intersection vector</th>
<th>frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>(0, 0, 0, $\Phi_6\Phi_7$)</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>(0, 0, $q^4\Phi_3\Phi_6$, $\Phi_2\Phi_4\Phi_6$)</td>
<td>$\Phi_7$</td>
</tr>
<tr>
<td>5</td>
<td>(0, $q^8$, $q^3\Phi_2\Phi_4$, $\Phi_4$)</td>
<td>$\Phi_3\Phi_6\Phi_7$</td>
</tr>
<tr>
<td>4</td>
<td>($q^7\Phi_1$, $q^5\Phi_3$, $q^2\Phi_3$, 1)</td>
<td>$\Phi_2\Phi_4\Phi_6\Phi_7$</td>
</tr>
<tr>
<td>4</td>
<td>($q^3(q^5 - q^4 + 1)$, $q\Phi_1\Phi_2\Phi_3\Phi_4$, $\Phi_3\Phi_4$, 0)</td>
<td>$q^4\Phi_6\Phi_7$</td>
</tr>
<tr>
<td>3</td>
<td>($q^4\Phi_4\Phi_2\Phi_1$, $q^2\Phi_3\Phi_4$, 0, 1)</td>
<td>$\Phi_6\Phi_7$</td>
</tr>
<tr>
<td>3</td>
<td>($q^3(q^5 - q + 1)$, $q(q^3 + q - 1)\Phi_3$, $\Phi_3$, 0)</td>
<td>$q\Phi_2\Phi_4\Phi_6\Phi_7$</td>
</tr>
<tr>
<td>2</td>
<td>($q^6\Phi_4$, $q^2\Phi_2\Phi_4$, 1, 0)</td>
<td>$\Phi_3\Phi_6\Phi_7$</td>
</tr>
<tr>
<td>1</td>
<td>($q^3\Phi_2\Phi_4\Phi_6$, $\Phi_3\Phi_6$, 0, 0)</td>
<td>$\Phi_7$</td>
</tr>
<tr>
<td>0</td>
<td>($\Phi_6\Phi_7$, 0, 0, 0)</td>
<td>1</td>
</tr>
</tbody>
</table>

Comment

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

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

- $2-(7,3,q^4)_q$
- $2-(7,3,q^3 + q^2 + q + 1)_q$
- $2-(7,3,q^4 + q^3 + q^2 + q)_q$

Comment

A $2-(7,3,16)_2$ design does exist.
Open problems

- Use the Köhler equations for a nonexistence proof.
- Use the intersection structure to show the nonexistence / construct a 2-(7, 3, 1)₂.