New subspace designs from large set recursion

Michael Kiermaier

Institut für Mathematik
Universität Bayreuth

Combinatorics 2014
June 5, 2014
Hotel Serapo, Gaeta

joint work with Michael Braun, Axel Kohnert and Reinhard Laue

Subsets

For V a set of cardinality v:

- $\binom{V}{k} :=$ set of all k-element subsets of V.
- binomial coefficient:

$$\#\binom{V}{k} = \binom{v}{k} = \frac{v \cdot (v-1) \cdot \ldots \cdot (v-k+1)}{1 \cdot 2 \cdot \ldots \cdot k}$$

Subspaces

For V an $\mathbb{F}_q$-vector space of dimension v:

- Graßmannian $\begin{bmatrix} V \\ k \end{bmatrix}_q$: set of all k-dim. subspaces of V.
- Gaussian Binomial coefficient

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

Observation

- Looks quite similar!
- $\lim_{q \to 1} \begin{bmatrix} v \\ k \end{bmatrix}_q = \binom{v}{k}$

Connection

Replace notions from set theory by vector space counterparts.

$$\begin{aligned} \text{set} &\longleftrightarrow \mathbb{F}_q\text{-vector space} \\ \text{cardinality} &\longleftrightarrow \text{dimension} \\ \text{binomial coefficient} &\longleftrightarrow \text{Gaussian binomial coefficient} \\ 1 &\longleftarrow q \end{aligned}$$

q-analogs in combinatorics

More precisely:

- subset lattice $\longleftrightarrow$ subspace lattice
- subspace lattice: *q-analog* of subset lattice.
- subset lattice: subspace lattice over "$\mathbb{F}_1$".

Definition (block design)

Let V be a v-element set.
$D \subseteq \binom{V}{k}$ is called a t-(v, k, λ) (block) design
if each $T \in \binom{V}{t}$ is contained in exactly λ elements of D.

Question

q-analog of a block design?

Definition (subspace design)

Let V be a v-dimensional $\mathbb{F}_q$ vector space.
$D \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$ is called a t-$(v, k, \lambda)_q$ (subspace) design
if each $T \in \begin{bmatrix} V \\ t \end{bmatrix}_q$ is contained in exactly λ elements of D.

Definition (block design)

Let V be a v-element set.

$D \subseteq \binom{V}{k}$ is called a t-(v, k, λ) (block) design

if each $T \in \binom{V}{t}$ is contained in exactly λ elements of D.

Question

q-analog of a block design?

Definition (subspace design)

Let V be a v-dimensional $\mathbb{F}_q$ vector space.

$D \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$ is called a t-$(v, k, \lambda)_q$ (subspace) design

if each $T \in \begin{bmatrix} V \\ t \end{bmatrix}_q$ is contained in exactly λ elements of D.

Definition (block design)

Let V be a v-element set.
$D \subseteq \binom{V}{k}$ is called a t-(v, k, λ) (block) design
if each $T \in \binom{V}{t}$ is contained in exactly λ elements of D.

Question

q-analog of a block design?

Definition (subspace design)

Let V be a v-dimensional $\mathbb{F}_q$ vector space.
$D \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$ is called a t-$(v, k, \lambda)_q$ (subspace) design
if each $T \in \begin{bmatrix} V \\ t \end{bmatrix}_q$ is contained in exactly λ elements of D.

Example

- 1-$(4, 2, 1)_2$ design
- Take row spaces of

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

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

- Geometrically: a *spread*
  5 lines in $\mathrm{PG}(3, 2)$ covering each point exactly once.

Representation of subspaces

$$\begin{bmatrix} V \\ k \end{bmatrix}_q \overset{\text{1-to-1}}{\longleftrightarrow} \textit{reduced row echelon forms (rref)} \text{ in } \mathbb{F}_q^{k \times v}$$

History of subspace designs

- First reference: P. Cameron 1974
- First nontrivial subspace designs with $t \geq 2$:
  S. Thomas 1987
- First Steiner system ($\lambda = 1$) with $t \geq 2$:
  M. Braun, T. Etzion, P. Östergård, A. Vardy, A. Wassermann 2013
- Only known infinite nontrivial families with $t \geq 2$:
  - $2\text{-}(v, 3, q^2 + q + 1)_q$ for $v \geq 7$, $\gcd(v, 6) = 1$
    (S. Thomas 1987; Suzuki 1990, 1992)
  - $2\text{-}(m\ell, 3, q^3 \frac{q^{\ell-5}-1}{q-1})_q$
    for $m \geq 3$, $\ell \geq 7$ and $\ell \equiv 5 \mod 6(q-1)$
    (T. Itoh 1998)

Goal

Construction of new infinite families!

Definition

Fix a parameter set t-$(v, k, \lambda)_q$.

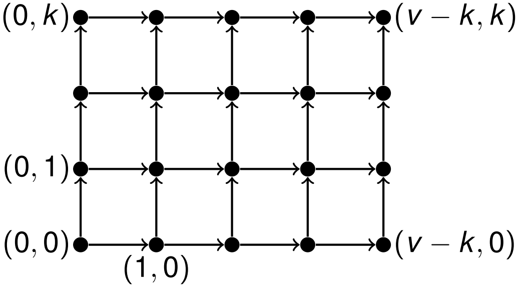
A large set $\mathrm{LS}_q[N](t, k, v)$

is a partition of $\begin{bmatrix} V \\ k \end{bmatrix}_q$ into N t-$(v, k, \lambda)_q$ designs.

Remarks

- $\lambda = \begin{bmatrix} v-t \\ k-t \end{bmatrix}_q / N$ is determined by N, v, k, t, q.
- Only known nontrivial large sets with $t \geq 2$:
  - $\mathrm{LS}_2[3](2, 3, 8)$ (M. Braun; A. Kohnert; P. Östergård; A. Wassermann 2014)
  - $\mathrm{LS}_3[2](2, 3, 6), \mathrm{LS}_5[2](2, 3, 6)$ (new)
- For large sets of *ordinary* block designs:
  Powerful recursion methods!
  (Khosrovshahi, Ajoodani-Namini 1991)
- Adjust those recursion methods to subspace designs!

Definition (Directed grid graph)

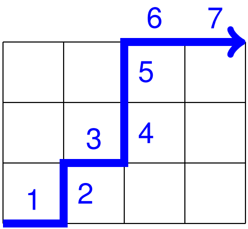


Bijection

$$\text{paths from } (0,0) \text{ to } (v-k,k) \overset{\text{1-to-1}}{\longleftrightarrow} k\text{-subsets } K \text{ of } V$$
$$\text{vertical step} \longleftrightarrow \text{element in } K$$
$$\text{horizontal step} \longleftrightarrow \text{element not in } K$$

Example

$V = \{1, 2, 3, 4, 5, 6, 7\}$.



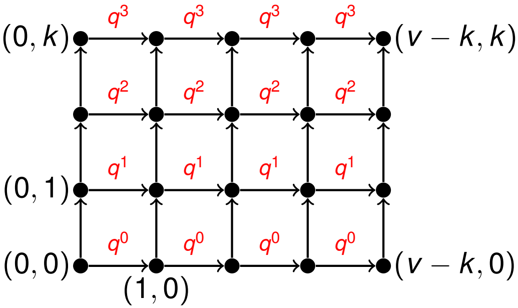
vertical steps: 2, 4, 5 $\rightsquigarrow$ $\{2, 4, 5\} \in \binom{V}{3}$

Question

Is there a q-analog of this bijection?

- Wanted: paths in some graph $\overset{\text{1-to-1}}{\longleftrightarrow}$ $\begin{bmatrix} V \\ k \end{bmatrix}_q$
- As good: paths in some graph $\overset{\text{1-to-1}}{\longleftrightarrow}$ rref in $\mathbb{F}_q^{k\times v}$

Definition (Directed q-grid multigraph)



Bijection

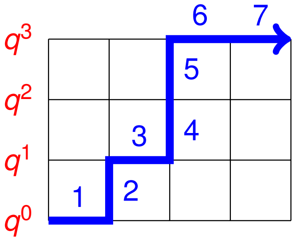
$$k\text{-subspaces } K \text{ of } V \overset{\text{1-to-1}}{\longleftrightarrow} \text{paths from } (0,0) \text{ to } (v-k,k)$$

$$\text{vertical step} \longleftrightarrow \text{pivot column}$$

$$\text{horizontal step} \longleftrightarrow \text{non-pivot column}$$

Example

$V = \mathbb{F}_q^7$



$$\rightsquigarrow \quad \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix}$$

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

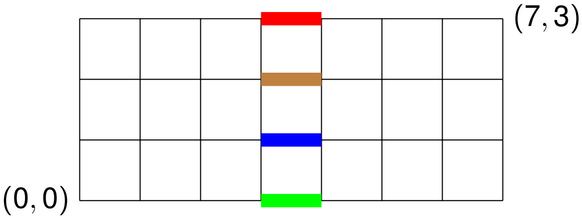
$$\begin{matrix} q^0 & & q^1 & & & q^3 & q^3 \end{matrix}$$

Partitions

Partition of the set of paths from $(0,0)$ to $(v-k,k)$ yields

- partition of $\begin{bmatrix} V \\ k \end{bmatrix}_q$
- identity for Gaussian binomial coefficients
- ... including bijective proof.
- New large sets from old ones!

Example



Partition of paths from $(0,0)$ to $(7,3)$ into 4 parts.

- Blue part $\longleftrightarrow \left(\begin{array}{ccccccccccc} \multicolumn{5}{c}{1 \times 4 \text{ rref}} & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & \multicolumn{6}{c}{} \\ 0 & 0 & 0 & 0 & 0 & \multicolumn{6}{c}{2 \times 5 \text{ rref}} \end{array} \right)$
- Number of such rref: $\begin{bmatrix} 4 \\ 1 \end{bmatrix}_q \cdot \begin{bmatrix} 5 \\ 2 \end{bmatrix}_q \cdot q \cdot q^3$
- $\leadsto$ identity

$$\begin{bmatrix} 6 \\ 3 \end{bmatrix}_q + q^4 \begin{bmatrix} 5 \\ 2 \end{bmatrix}_q \begin{bmatrix} 4 \\ 1 \end{bmatrix}_q + q^8 \begin{bmatrix} 4 \\ 1 \end{bmatrix}_q \begin{bmatrix} 5 \\ 2 \end{bmatrix}_q + q^{12} \begin{bmatrix} 6 \\ 3 \end{bmatrix}_q = \begin{bmatrix} 10 \\ 3 \end{bmatrix}_q$$

Example

$$\begin{bmatrix}6\\3\end{bmatrix}_q + q^4 \begin{bmatrix}5\\2\end{bmatrix}_q \begin{bmatrix}4\\1\end{bmatrix}_q + q^8 \begin{bmatrix}4\\1\end{bmatrix}_q \begin{bmatrix}5\\2\end{bmatrix}_q + q^{12} \begin{bmatrix}6\\3\end{bmatrix}_q$$

Theorem (very informal version)

We may „plug in" suitable large sets into the identity!

Example (cont.)

- Computer search: $\exists\, \mathrm{LS}_q[2](2,3,6)$ for $q \in \{3,5\}$.
- *Derived large sets*: $\exists\, \mathrm{LS}_q[2](1,2,5)$, $\quad \exists\, \mathrm{LS}_q[2](0,1,4)$

$$\implies \mathrm{LS}_q[2](2,3,6) \cup \mathrm{LS}_q[2](1,2,5) * \mathrm{LS}_q[2](0,1,4)$$
$$\cup\, \mathrm{LS}_q[2](0,1,4) * \mathrm{LS}_q[2](1,2,5) \cup \mathrm{LS}_q[2](2,3,6)$$

is a $\mathrm{LS}_q[2](\mathbf{??},3,10)$

Example (cont.)

$$\underbrace{\mathrm{LS}_q[2](\mathbf{2},3,6)}_{t=2} \cup \underbrace{\mathrm{LS}_q[2](\mathbf{1},2,5) * \mathrm{LS}_q[2](\mathbf{0},1,4)}_{t=1+\mathbf{1}+0}$$
$$\cup \underbrace{\mathrm{LS}_q[2](\mathbf{0},1,4) * \mathrm{LS}_q[2](\mathbf{1},2,5)}_{t=0+\mathbf{1}+1} \cup \underbrace{\mathrm{LS}_q[2](\mathbf{2},3,6)}_{t=2}$$

is a $\mathrm{LS}_q[2](\mathbf{2},3,10)$

- $\implies \exists\, \mathrm{LS}_q[2](2,3,10)$ for $q \in \{3,5\}$
- $\implies \exists 2\text{-}(10,3,1640)_3$ and $2\text{-}(10,3,48828)_5$ designs
- number of blocks: 238247460880 and 208628946735352

Idea

Iterate these methods!

$\rightsquigarrow$ infinite families of large sets
$\rightsquigarrow$ infinite families of subspace designs

Theorem

- $\exists\, \mathrm{LS}_q[2](2, 2^s - 1, v)$
  for $q \in \{3, 5\}$, $s \geq 1$, $v \equiv 2 \mod 4$, $v > 2^s$.
- $\exists\, \mathrm{LS}_2[3](2, k, v)$
  for $k \in \{5, 11, 17\}$, $v \equiv 4 \mod 12$, $v > k$.
- *If* $p = 2 \cdot 3^a + 1$ *is prime and* $\exists\, \mathrm{LS}_2[3](2, k, p + 1)$,
  then $\exists\, \mathrm{LS}_2[3](2, p + 1 - k, n(p - 1) + 2)$ *for all* $n \geq 2$.
- *etc.*

Open questions

- Find new starting points for the recursion.
  Candidates:
  - $\mathrm{LS}_2[3](2,4,8)$ (Smallest open case for $q = 2$, $N = 3$)
  - Anything with $t \geq 2$, $N \geq 4$.
  - $\mathrm{LS}_q[2](2,3,6)$, $q \geq 7$ odd
    (known for $q \in \{3,5\}$, invariant under Singer^2)
  - harder: $\mathrm{LS}_q[q^2+1](2,3,6)$, q unrestricted
- When does $\mathrm{LS}_q[N](1,k,v)$ exist? (includes parallelisms)
  Necessary conditions: $k \mid v$ and $N \mid \begin{bmatrix} v-1 \\ k-1 \end{bmatrix}_q$
  Z. Baranyai 1975: Sufficient for $q = 1$.