

Recursive construction of subspace designs

Michael Kiermaier

Institut für Mathematik
Universität Bayreuth

ALCOMA 2015
Mar 20, 2015
Kloster Banz, Germany

joint work with Michael Braun, Axel Kohnert and Reinhard Laue

Definition (block design)

Let V be a v -element set.

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

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

q -analog in combinatorics:

Replace subset lattice by subspace lattice!

Definition (subspace design)

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

$D \subseteq \left[\begin{smallmatrix} V \\ k \end{smallmatrix} \right]_q$ is a t - $(v, k, \lambda)_q$ (subspace) design

if each $T \in \left[\begin{smallmatrix} V \\ t \end{smallmatrix} \right]_q$ is contained in exactly λ elements of D .

Definition (block design)

Let V be a v -element set.

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

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

q -analog in combinatorics:

Replace subset lattice by subspace lattice!

Definition (subspace design)

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

$D \subseteq \left[\begin{smallmatrix} V \\ k \end{smallmatrix} \right]_q$ is a t - $(v, k, \lambda)_q$ (subspace) design

if each $T \in \left[\begin{smallmatrix} V \\ t \end{smallmatrix} \right]_q$ is contained in exactly λ elements of D .

Definition (block design)

Let V be a v -element set.

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

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

q -analog in combinatorics:

Replace subset lattice by subspace lattice!

Definition (subspace design)

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

$D \subseteq \left[\begin{smallmatrix} V \\ k \end{smallmatrix} \right]_q$ is a t - $(v, k, \lambda)_q$ (subspace) design

if each $T \in \left[\begin{smallmatrix} V \\ t \end{smallmatrix} \right]_q$ is contained in exactly λ elements of D .

Infinite families

Only known infinite nontrivial families with $t \geq 2$:

- ▶ $2-(v, 3, q^2 + q + 1)_q$ for $v \geq 7$, $\gcd(v, 6) = 1$
(S. Thomas 1987; Suzuki 1990, 1992)
- ▶ $2-(m\ell, 3, q^3 \frac{q^{\ell-5}-1}{q-1})_q$
for $m \geq 3$, $\ell \geq 7$ and $\ell \equiv 5 \pmod{6(q-1)}$
(T. Itoh 1998)

Goal

Construction of new infinite families!

Definition

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

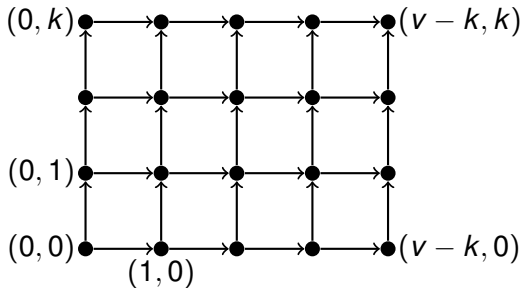
A **large set** $LS_q[N](t, k, v)$

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 $t \geq 2$:
 - ▶ $LS_3[2](2, 3, 6)$ (M. Braun 2005)
 - ▶ $LS_2[3](2, 3, 8)$ (M. Braun; A. Kohnert; P. Östergård; A. Wassermann 2014)
 - ▶ $LS_5[2](2, 3, 6)$ (new, computer construction)
- ▶ 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

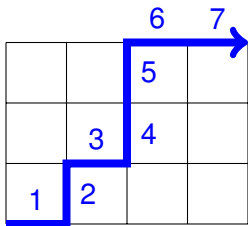
paths from $(0, 0)$ to $(v - k, k) \xleftrightarrow{1\text{-to-}1} k\text{-subsets } K \text{ of } V$

vertical step \longleftrightarrow element in K

horizontal step \longleftrightarrow element not in K

Example

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



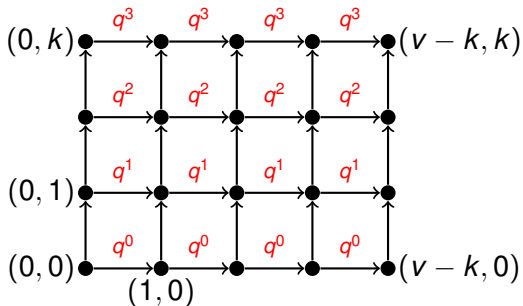
vertical steps: 2, 4, 5 \rightsquigarrow $\{2, 4, 5\} \in \binom{V}{3}$

Question

Is there a q -analog of this bijection?

- ▶ Wanted: paths in some graph $\xleftrightarrow{1\text{-to-1}} [k]_q$
- ▶ As good: paths in some graph $\xleftrightarrow{1\text{-to-1}} \text{rref in } \mathbb{F}_q^{k \times v}$

Definition (Directed q -grid multigraph)



Bijection

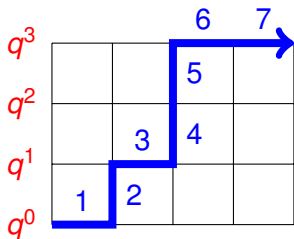
k -subspaces K of $V \xleftrightarrow{1\text{-to-1}}$ paths from $(0, 0)$ to $(v - k, k)$

vertical step \longleftrightarrow pivot column

horizontal step \longleftrightarrow non-pivot column

Example

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



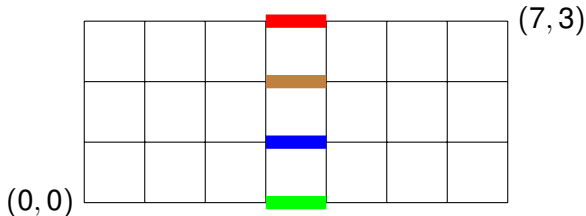
$$\rightsquigarrow \begin{matrix} & \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \\ \begin{matrix} q^0 \\ q^1 \\ q^3 \\ q^3 \end{matrix} & \begin{pmatrix} 0 & \mathbf{1} & * & 0 & 0 & * & * \\ 0 & 0 & 0 & \mathbf{1} & 0 & * & * \\ 0 & 0 & 0 & 0 & \mathbf{1} & * & * \end{pmatrix} \end{matrix}$$

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
$$\begin{pmatrix} 1 \times 4 \text{ rref} & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & & \\ 0 & 0 & 0 & 0 & 0 & 2 \times 5 \text{ rref} & \end{pmatrix}$$

► Number of such rref: $\begin{bmatrix} 4 \\ 1 \end{bmatrix}_q \cdot \begin{bmatrix} 5 \\ 2 \end{bmatrix}_q \cdot q \cdot q^3$

► \rightsquigarrow 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

$$\begin{bmatrix} 10 \\ 3 \end{bmatrix}_q = \begin{bmatrix} 3 \\ 0 \end{bmatrix}_q \begin{bmatrix} 6 \\ 3 \end{bmatrix}_q + q^4 \begin{bmatrix} 4 \\ 1 \end{bmatrix}_q \begin{bmatrix} 5 \\ 2 \end{bmatrix}_q + q^8 \begin{bmatrix} 5 \\ 2 \end{bmatrix}_q \begin{bmatrix} 4 \\ 1 \end{bmatrix}_q + q^{12} \begin{bmatrix} 6 \\ 3 \end{bmatrix}_q \begin{bmatrix} 3 \\ 0 \end{bmatrix}_q$$

► Blue part \longleftrightarrow $\begin{pmatrix} 1 \times 4 \text{ rref} & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & & \\ 0 & 0 & 0 & 0 & 0 & 2 \times 5 \text{ rref} & \end{pmatrix}$

► Describe this set of subspaces as **join** $\begin{bmatrix} \mathbb{F}_q^4 \\ 1 \end{bmatrix}_q * \begin{bmatrix} \mathbb{F}_q^5 \\ 2 \end{bmatrix}_q$.

► Simplified notation: $\begin{bmatrix} 4 \\ 1 \end{bmatrix} * \begin{bmatrix} 5 \\ 2 \end{bmatrix}$.

\rightsquigarrow Disjoint union of joins

$$\begin{bmatrix} 10 \\ 3 \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \end{bmatrix} * \begin{bmatrix} 6 \\ 3 \end{bmatrix} \uplus \begin{bmatrix} 4 \\ 1 \end{bmatrix} * \begin{bmatrix} 5 \\ 2 \end{bmatrix} \uplus \begin{bmatrix} 5 \\ 2 \end{bmatrix} * \begin{bmatrix} 4 \\ 1 \end{bmatrix} \uplus \begin{bmatrix} 6 \\ 3 \end{bmatrix} * \begin{bmatrix} 3 \\ 0 \end{bmatrix}$$

Definition

- ▶ Let $\mathcal{B}_1, \mathcal{B}_2 \subseteq \binom{V}{k}_q$.
- ▶ \mathcal{B}_1 and \mathcal{B}_2 **t -equivalent** if for all $T \in \binom{V}{t}_q$

$$\#\{\mathbf{B} \in \mathcal{B}_1 \mid T \subseteq \mathbf{B}\} = \#\{\mathbf{B} \in \mathcal{B}_2 \mid T \subseteq \mathbf{B}\}$$

Example

$q = 1, t = 2, k = 3$.

$$\mathcal{B}_1 = \{\{1, 2, 4\}, \{1, 3, 6\}, \{2, 5, 6\}, \{3, 4, 5\}\}$$

$$\mathcal{B}_2 = \{\{1, 2, 6\}, \{1, 3, 4\}, \{2, 4, 5\}, \{3, 5, 6\}\}$$

- ▶ $T = \{1, 4\} \implies \lambda(T, \mathcal{B}_1) = \lambda(T, \mathcal{B}_2) = 1$
- ▶ $T = \{2, 3\} \implies \lambda(T, \mathcal{B}_1) = \lambda(T, \mathcal{B}_2) = 0$
- ▶ ... Check all T ...
- ▶ $\implies \mathcal{B}_1$ and \mathcal{B}_2 are 2-equivalent.

Definition

- ▶ Let $\mathcal{B}_1, \mathcal{B}_2 \subseteq \binom{V}{k}_q$.
- ▶ \mathcal{B}_1 and \mathcal{B}_2 **t -equivalent** if for all $T \in \binom{V}{t}_q$

$$\#\{B \in \mathcal{B}_1 \mid T \subseteq B\} = \#\{B \in \mathcal{B}_2 \mid T \subseteq B\}$$

Example

$q = 1, t = 2, k = 3$.

$$\mathcal{B}_1 = \{\{1, 2, 4\}, \{1, 3, 6\}, \{2, 5, 6\}, \{3, 4, 5\}\}$$

$$\mathcal{B}_2 = \{\{1, 2, 6\}, \{1, 3, 4\}, \{2, 4, 5\}, \{3, 5, 6\}\}$$

- ▶ $T = \{1, 4\} \implies \lambda(T, \mathcal{B}_1) = \lambda(T, \mathcal{B}_2) = 1$
- ▶ $T = \{2, 3\} \implies \lambda(T, \mathcal{B}_1) = \lambda(T, \mathcal{B}_2) = 0$
- ▶ ... Check all T ...
- ▶ $\implies \mathcal{B}_1$ and \mathcal{B}_2 are 2-equivalent.

Definition

- ▶ Let $\mathcal{B}_1, \mathcal{B}_2 \subseteq \binom{V}{k}_q$.
- ▶ \mathcal{B}_1 and \mathcal{B}_2 **t -equivalent** if for all $T \in \binom{V}{t}_q$

$$\#\{B \in \mathcal{B}_1 \mid T \subseteq B\} = \#\{B \in \mathcal{B}_2 \mid T \subseteq B\}$$

Example

$q = 1, t = 2, k = 3$.

$$\mathcal{B}_1 = \{\{1, 2, 4\}, \{1, 3, 6\}, \{2, 5, 6\}, \{3, 4, 5\}\}$$

$$\mathcal{B}_2 = \{\{1, 2, 6\}, \{1, 3, 4\}, \{2, 4, 5\}, \{3, 5, 6\}\}$$

- ▶ $T = \{1, 4\} \implies \lambda(T, \mathcal{B}_1) = \lambda(T, \mathcal{B}_2) = 1$
- ▶ $T = \{2, 3\} \implies \lambda(T, \mathcal{B}_1) = \lambda(T, \mathcal{B}_2) = 0$
- ▶ ... Check all T ...
- ▶ $\implies \mathcal{B}_1$ and \mathcal{B}_2 are 2-equivalent.

Definition

- ▶ Let $\mathcal{B}_1, \mathcal{B}_2 \subseteq \binom{V}{k}_q$.
- ▶ \mathcal{B}_1 and \mathcal{B}_2 **t -equivalent** if for all $T \in \binom{V}{t}_q$

$$\#\{B \in \mathcal{B}_1 \mid T \subseteq B\} = \#\{B \in \mathcal{B}_2 \mid T \subseteq B\}$$

Example

$q = 1, t = 2, k = 3$.

$$\mathcal{B}_1 = \{\{1, 2, 4\}, \{1, 3, 6\}, \{2, 5, 6\}, \{3, 4, 5\}\}$$

$$\mathcal{B}_2 = \{\{1, 2, 6\}, \{1, 3, 4\}, \{2, 4, 5\}, \{3, 5, 6\}\}$$

- ▶ $T = \{1, 4\} \implies \lambda(T, \mathcal{B}_1) = \lambda(T, \mathcal{B}_2) = 1$
- ▶ $T = \{2, 3\} \implies \lambda(T, \mathcal{B}_1) = \lambda(T, \mathcal{B}_2) = 0$
- ▶ ... Check all T ...
- ▶ $\implies \mathcal{B}_1$ and \mathcal{B}_2 are 2-equivalent.

Definition

- ▶ Let $\mathcal{B}_1, \mathcal{B}_2 \subseteq \binom{V}{k}_q$.
- ▶ \mathcal{B}_1 and \mathcal{B}_2 **t -equivalent** if for all $T \in \binom{V}{t}_q$

$$\#\{B \in \mathcal{B}_1 \mid T \subseteq B\} = \#\{B \in \mathcal{B}_2 \mid T \subseteq B\}$$

Example

$q = 1, t = 2, k = 3$.

$$\mathcal{B}_1 = \{\{1, 2, 4\}, \{1, 3, 6\}, \{2, 5, 6\}, \{3, 4, 5\}\}$$

$$\mathcal{B}_2 = \{\{1, 2, 6\}, \{1, 3, 4\}, \{2, 4, 5\}, \{3, 5, 6\}\}$$

- ▶ $T = \{1, 4\} \implies \lambda(T, \mathcal{B}_1) = \lambda(T, \mathcal{B}_2) = 1$
- ▶ $T = \{2, 3\} \implies \lambda(T, \mathcal{B}_1) = \lambda(T, \mathcal{B}_2) = 0$
- ▶ ... Check all T ...
- ▶ $\implies \mathcal{B}_1$ and \mathcal{B}_2 are 2-equivalent.

Definition

- ▶ Let $\mathcal{B} \subseteq \binom{V}{k}_q$
- ▶ For $t \geq 0$: \mathcal{B} is (N, t) -partitionable : \iff
 \exists partition $\{\mathcal{B}_1, \dots, \mathcal{B}_N\}$ of \mathcal{B} s.t. all \mathcal{B}_i are t -equivalent.
- ▶ Always: \mathcal{B} is $(N, -1)$ -partitionable.

Lemma

$$\exists \text{LS}_q[N](t, k, v) \iff \binom{v}{k} \text{ is } (N, t)\text{-partitionable.}$$

Application for $q \in \{3, 5\}$

- ▶ $\exists \text{LS}_q[2](2, 3, 6) \implies \binom{6}{3}$ is $(2, 2)$ -partitionable
- ▶ *Derived large set*: $\exists \text{LS}_q[2](1, 2, 5) \implies \binom{5}{2}$ is $(2, 1)$ -part.
- ▶ *Derived large set*: $\exists \text{LS}_q[2](0, 1, 4) \implies \binom{4}{1}$ is $(2, 0)$ -part.

Rules to create (N, t) -partitionable sets:

Proposition

The disjoint union of (N, t) -partitionable sets is (N, t) -partitionable.

Basic Lemma

- ▶ Let \mathcal{B}_1 be (N, t_1) -partitionable
- ▶ Let \mathcal{B}_2 be (N, t_2) -partitionable

The join $\mathcal{B}_1 * \mathcal{B}_2$ is $(N, t_1 + t_2 + 1)$ -partitionable.

Example

$$\begin{aligned} \begin{bmatrix} 10 \\ 3 \end{bmatrix} &= \\ \begin{bmatrix} 3 \\ 0 \end{bmatrix} * \begin{bmatrix} 6 \\ 3 \end{bmatrix} \uplus \begin{bmatrix} 4 \\ 1 \end{bmatrix} * \begin{bmatrix} 5 \\ 2 \end{bmatrix} \uplus \begin{bmatrix} 5 \\ 2 \end{bmatrix} * \begin{bmatrix} 4 \\ 1 \end{bmatrix} \uplus \begin{bmatrix} 6 \\ 3 \end{bmatrix} * \begin{bmatrix} 3 \\ 0 \end{bmatrix} \\ \underbrace{(2, -1) \quad (2, 2)} & \quad \underbrace{(2, 0) \quad (2, 1)} & \quad \underbrace{(2, 1) \quad (2, 0)} & \quad \underbrace{(2, 2) \quad (2, -1)} \\ \underbrace{(2, -1 + 2 + 1)} & \quad \underbrace{(2, 0 + 1 + 1)} & \quad \underbrace{(2, 1 + 0 + 1)} & \quad \underbrace{(2, 2 - 1 + 1)} \\ & = (2, 2) & = (2, 2) & = (2, 2) \\ \underbrace{\hspace{15em}} & \\ & (2, 2)\text{-partitionable} \end{aligned}$$

$$\Rightarrow \begin{bmatrix} 10 \\ 3 \end{bmatrix} \text{ is } (2, 2)\text{-partitionable} \quad \Rightarrow \exists \text{LS}_q[2](2, 3, 10)$$

Example (cont.)

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

Theorem

Let $q \in \{3, 5\}$.

There exists an $LS_q[2](2, k, v)$ for all

- ▶ $v \equiv 2 \pmod{4}$ with $v \geq 6$
- ▶ $k \equiv 3 \pmod{4}$ with $3 \leq k \leq v - 3$.

From $LS_2[3](2, 3, 8)$:

Theorem? (work in progress!)

There exists an $LS_2[3](2, k, v)$ for all

- ▶ $v \equiv 2 \pmod{6}$ with $v \geq 8$
- ▶ $k \equiv 3, 5 \pmod{6}$ with $3 \leq k \leq v - 3$.

Open questions

- ▶ Construct $LS_q[2](2, 3, 6)$, $q \geq 7$ odd.
(known for $q \in \{3, 5\}$, invariant under Singer²)
- ▶ Construct $LS_2[3](2, 4, 8)$
(Smallest open case for $q = 2$, $N = 3$)
- ▶ When does $LS_q[N](1, k, v)$ 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 $q = 1$.