Construction of new large sets of designs over the binary field

Alfred Wassermann

Department of Mathematics, Universität Bayreuth, Germany

joint work with Michael Kiermaier and Reinhard Laue

DARNEC ’15
Istanbul

Outline

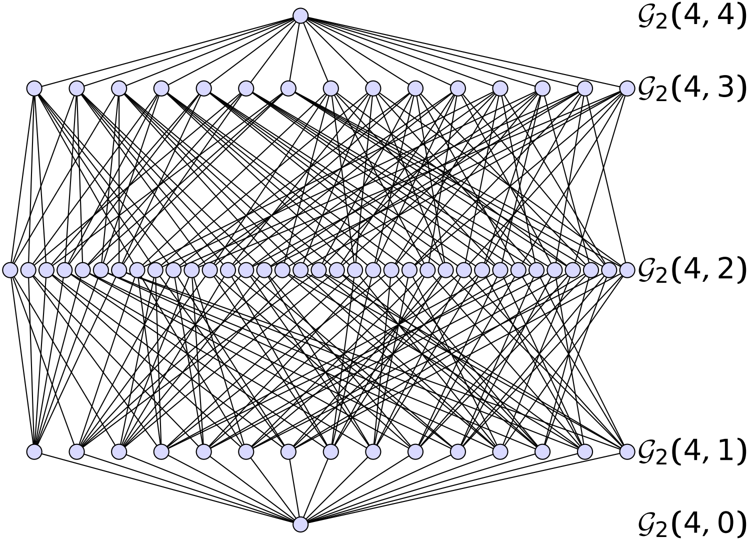
- Designs over finite fields
- Computer construction
- Infinite series of large sets

Designs over finite fields

Subspaces

- vector space $\mathcal{V} = \mathbb{F}_q^v$
- Grassmannian: $\mathcal{G}_q(v, k) := \{U \le \mathbb{F}_q^v : \dim U = k\}$

Subspace lattice of $\mathbb{F}_2^4$



Subspace lattice

- Gaussian coefficient:

$$\begin{bmatrix} v \\ k \end{bmatrix}_q = \frac{(q^v - 1)(q^{v-1} - 1)\cdots(q^{v-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1)\cdots(q - 1)}$$

- $|\mathcal{G}_q(v,k)| = \begin{bmatrix} v \\ k \end{bmatrix}_q$

Designs over finite fields

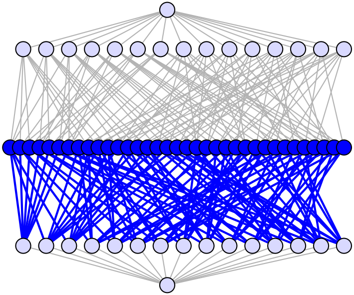
- Cameron (1974), Delsarte (1976)
- $\mathcal{B} \subseteq \mathcal{G}_q(v, k)$: set of k-subspaces (blocks)
- $(\mathbb{F}_q^v, \mathcal{B})$: t-$(v, k, \lambda; q)$ design over $\mathbb{F}_q$

  each t-subspace of $\mathbb{F}_q^v$ is contained in exactly λ blocks of $\mathcal{B}$

- $\mathcal{B}$ set: simple design
- $\mathcal{B}$ multiset: non-simple design

Designs over finite fields

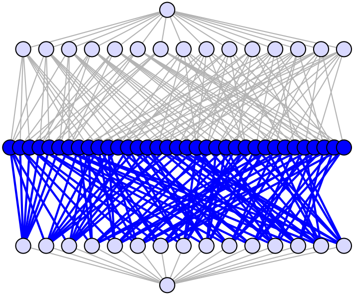
- $\mathcal{B} = \mathcal{G}_q(v,k)$ is a t-$(v,k,\begin{bmatrix} v-t \\ k-t \end{bmatrix}_q;q)$ design: trivial design



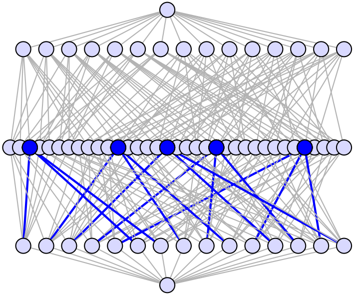
trivial 1-$(4,2,7;2)$ design

Designs over finite fields

- $\mathcal{B} = \mathcal{G}_q(v,k)$ is a t-$(v,k,\left[\begin{smallmatrix} v-t \\ k-t \end{smallmatrix}\right]_q;q)$ design: trivial design



trivial 1-$(4,2,7;2)$ design



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

t-$(v, k, \lambda; q)$ designs

- $|\mathcal{B}| = \lambda \frac{\begin{bmatrix} v \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q}$
- Necessary conditions:

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

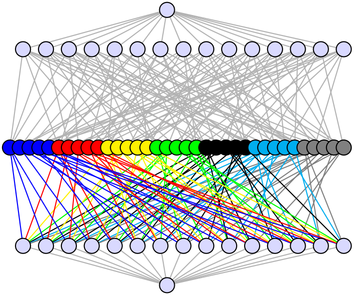
Related designs

t-$(v, k, \lambda; q)$ design $\rightarrow$

- dual design: t-$(v, v-k, \lambda; q)$
- derived design: $(t-1)$-$(v-1, k-1, \lambda; q)$
- residual design: $(t-1)$-$(v-1, k, \mu; q)$, where $\mu = \lambda \cdot \begin{bmatrix} v-k \\ 1 \end{bmatrix}_q / \begin{bmatrix} k-t+1 \\ 1 \end{bmatrix}_q$

Large sets of q-analogs of designs

- $\mathcal{G}_q(v,k)$ is a t-$(v,k,\begin{bmatrix}v-t\\k-t\end{bmatrix}_q;q)$ design
- Large set $LS_q[N](t,k,v)$:
  partition of $\mathcal{G}_q(v,k)$ into N disjoint t-$(v,k,\lambda;q)$ designs



$LS_2[7](1,2,4)$

- Necessary: $N \cdot \lambda = \begin{bmatrix}v-t\\k-t\end{bmatrix}_q$

Automorphisms

Designs over finite fields:

- $GL(v, q) = \{M \in \mathbb{F}_q^{v \times v} : M \text{ invertible}\}$
- $\sigma \in GL(v, q)$ automorphism: $\mathcal{B}^\sigma = \mathcal{B}$

Automorphisms of designs over finite fields

- Singer cycle:
  - take $v \in \mathbb{F}_q^v$ as an element of $\mathbb{F}_{q^v}$
  - $(\mathbb{F}_{q^v} \setminus \{0\}, \cdot)$ is a cyclic group G of order $q^v - 1$, i.e.
  - $G = \langle \sigma \rangle$
  - $G \leq GL(v, q)$ is called *Singer cycle*
- Frobenius automorphism:
  - $\phi : \mathbb{F}_{q^v} \to \mathbb{F}_{q^v}$, $U \mapsto U^q$
  - $|\langle \phi \rangle| = v$
- $|\langle \sigma, \phi \rangle| = v \cdot (q^v - 1)$

Computer construction

Brute force approach for construction

- incidence matrix between t-subset and k-subsets:

$$M_{t,k} = (m_{i,j}), \text{ where } m_{i,j} = \begin{cases} 1 & \text{if } T_i \subset K_j \\ 0 & \text{else} \end{cases}$$

- solve

$$M_{t,k} \cdot x = \begin{pmatrix} \lambda \\ \lambda \\ \vdots \\ \lambda \end{pmatrix} \quad \text{for 0/1-vector } x$$

Designs with prescribed automorphism group

Construction of designs with prescribed automorphism group

- choose group G acting on $\mathcal{V}$, i.e. $G \leq S_v$
- search for t-designs $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ having G as a group of automorphisms,
  i.e. for all

$$g \in G \text{ and } K \in \mathcal{B} \Longrightarrow K^g \in \mathcal{B}.$$

- construct $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ as

union of orbits of G on k-subsets.

The method of Kramer and Mesner

Definition

- $K \subset \mathcal{V}$ and $|K| = k$: $K^G := \{K^g \mid g \in G\}$
- $T \subset \mathcal{V}$ and $|T| = t$: $T^G := \{T^g \mid g \in G\}$
- Let
$$K_1^G \cup K_2^G \cup \ldots \cup K_n^G \subseteq \binom{\mathcal{V}}{k}$$
and
$$T_1^G \cup T_2^G \cup \ldots \cup T_m^G = \binom{\mathcal{V}}{t}$$
-
$$M_{t,k}^G = (m_{i,j}) \text{ where } m_{i,j} := |\{K \in K_j^G \mid T_i \subset K\}|$$

The method of Kramer and Mesner

Theorem (Kramer and Mesner, 1976)

The union of orbits corresponding to the 1*s in a* $\{0,1\}$ *vector which solves*

$$M_{t,k}^{G} \cdot x = \begin{pmatrix} \lambda \\ \lambda \\ \vdots \\ \lambda \end{pmatrix}$$

is a t*-*(v,k,λ) *design having* G *as an automorphism group.*

Known large sets for $t \geq 2$

- $LS_2[3](2, 3, 8)$: Braun, Kohnert, Östergård, W. (2014)
  - Three disjoint 2-$(8, 3, 21; 2)$ designs
  - Group: $\langle\sigma\rangle$ in $GL(8, 2)$ of order 255
- $LS_3[2](2, 3, 6)$: Braun (2005)
  - Two disjoint 2-$(6, 3, 20; 3)$ designs
- $LS_5[2](2, 3, 6)$: Braun, Kiermaier, Kohnert, Laue (2014)
  - Two disjoint 2-$(6, 3, 78; 5)$ designs

A new large set

- $LS_2[3](2,4,8)$
  - Three disjoint 2-$(8,4,217;2)$ designs
  - Group: $\langle \sigma^5, \phi^2 \rangle$ in $GL(8,2)$ of order 204

Related large sets

Theorem (Kiermaier, Laue 2015)

- *derived large set:*

$$LS_q[N](t,k,v) \quad \rightarrow \quad LS_q[N](t-1,k-1,v-1)$$

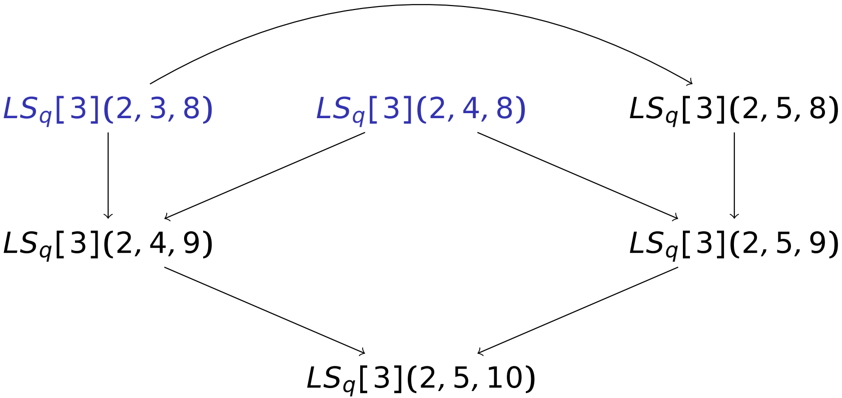
- *q-analog of Van Trung, Van Leyenhorst, Driessen:*

$$LS_q[N](t,k-1,v-1) \quad \text{and} \quad LS_q[N](t,k,v-1)$$

$$\longrightarrow$$

$$LS_q[N](t,k,v)$$

Related large sets



Admissibility and realizability of $LS_2[3](2, k, v)$

																		v
-																		6
-																		7
3	4																	8
-	4																	9
-	-	5																10
-	-	-																11
-	-	-	-															12
-	-	-	-															13
3	4	5	-	-														14
-	4	5	-	-														15
-	-	5	-	-	-													16
-	-	-	-	-	-													17
-	-	-	-	-	-	-												18
-	-	-	-	-	-	-												19
3	4	5	?	?	?	9	10											20
-	4	5	?	?	?	?	10											21
-	-	5	?	?	?	?	?	11										22
-	-	-	?	?	?	?	?	?										23
-	-	-	-	?	?	?	?	?	?									24
-	-	-	-	-	?	?	?	?	?									25
3	4	5	-	-	-	9	10	11	?	?								26
-	4	5	-	-	-	-	10	11	?	?								27
-	-	5	-	-	-	-	-	11	?	?	?							28
-	-	-	-	-	-	-	-	-	?	?	?							29
-	-	-	-	-	-	-	-	-	-	?	?	?						30
-	-	-	-	-	-	-	-	-	-	-	?	?						31
3	4	5	-	-	-	9	10	11	-	-	-	15	16					32
-	4	5	-	-	-	-	10	11	-	-	-	-	16					33
-	-	5	-	-	-	-	-	11	-	-	-	-	-	17				34
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-				35
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-			36
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-			37
3	4	5	?	?	?	9	10	11	?	?	?	15	16	17	-	-		38
-	4	5	?	?	?	?	10	11	?	?	?	?	16	17	-	-		39
-	-	5	?	?	?	?	?	11	?	?	?	?	?	17	-	-	-	40

Open problems

Thank you for listening !