Construction of q-analogs of combinatorial designs

Stefanie Braun

University of Bayreuth

ALCOMA'10 Thurnau

13. April 2010

q-Analogs of Combinatorial Designs

Definition

q-analog of $t-(n,k,\lambda)$-design

q-Analogs of Combinatorial Designs

Definition

q-analog of $t-(n,k,\lambda)$-design

$$\Longleftrightarrow$$

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

q-Analogs of Combinatorial Designs

Definition

q-analog of $t-(n,k,\lambda)$-design

$$\Longleftrightarrow$$

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

$$\Longleftrightarrow$$

design of finite fields

q-Analogs of Combinatorial Designs

Definition

q-analog of $t-(n,k,\lambda)$-design

$$\Longleftrightarrow$$

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

$$\Longleftrightarrow$$

design of finite fields

$$\Longleftrightarrow$$

$$\mathcal{B} \subseteq \begin{bmatrix} GF(q)^n \\ k \end{bmatrix}_q : |\{K \in \mathcal{B} \mid T \leq K\}| = \lambda \quad \forall\ T \in \begin{bmatrix} GF(q)^n \\ t \end{bmatrix}_q$$

History of Designs over Finite Fields

- S. Thomas (1987):

  $2-(n,3,7;2)$-designs $\forall\ n \geq 7 \in \mathbb{N}$ with $n \equiv \pm 1 \bmod 6$

History of Designs over Finite Fields

- S. Thomas (1987):

  $$2-(n,3,7;2)\text{-designs } \forall\ n \geq 7 \in \mathbb{N} \text{ with } n \equiv \pm 1 \bmod 6$$

- H. Suzuki (1992):

  $$2-(n,3,q^2+q+1;q)\text{-design } \forall\ n \geq 7 \text{ with } n \equiv \pm 1 \bmod 6$$
  and q prime

- M. Miyakawa, A. Munemasa and S. Yoshiara (1995):

  classification of $2-(7,3,\lambda;q)$-designs for $q = 2, 3$ with small λ

- T. Itoh (1998):

  $$2-(ml,3,q^3(q^{l-5}/(q-1);q)\text{-designs for any } m \geq 3$$
  which admits the action of $SL(m,q^l)$

History of Designs over Finite Fields

- S. Thomas (1987):

  $$2-(n,3,7;2)\text{-designs } \forall\ n \geq 7 \in \mathbb{N} \text{ with } n \equiv \pm 1 \bmod 6$$

- H. Suzuki (1992):

  $$2-(n,3,q^2+q+1;q)\text{-design } \forall\ n \geq 7 \text{ with } n \equiv \pm 1 \bmod 6$$
  and q prime

- M. Miyakawa, A. Munemasa and S. Yoshiara (1995):

  classification of $2-(7,3,\lambda;q)$-designs for $q=2,3$ with small λ

- T. Itoh (1998):

  $$2-(ml,3,q^3(q^{l-5}/(q-1);q)\text{-designs for any } m \geq 3$$
  which admits the action of $SL(m,q^l)$

- M. Braun (2005):

  $$3-(8,4,11,2)\text{-design}$$

q-Steiner Systems and Network Codes

Definition

A $t-(n, k, 1; q)$*-design is called a q-Steiner system.*

q-Steiner Systems and Network Codes

Definition

A $t-(n,k,1;q)$-design is called a q-Steiner system.

Etzion and Schwartz gave necessary conditions for the existence of such structures and presented connections between Steiner systems and q-Steiner systems in 2002.

q-Steiner Systems and Network Codes

Definition

A $t-(n,k,1;q)$-design is called a q-Steiner system.

Etzion and Schwartz gave necessary conditions for the existence of such structures and presented connections between Steiner systems and q-Steiner systems in 2002.
Anyway till this day no q-Steiner system has been found yet!

q-Steiner Systems and Network Codes

Definition

A $t-(n,k,1;q)$-design is called a q-Steiner system.

Etzion and Schwartz gave necessary conditions for the existence of such structures and presented connections between Steiner systems and q-Steiner systems in 2002.
Anyway till this day no q-Steiner system has been found yet!

Application of q-analogs of designs:
$\Rightarrow$ NETWORK CODING!

q-Steiner Systems and Network Codes

Definition

A $t-(n,k,1;q)$-design is called a q-Steiner system.

Etzion and Schwartz gave necessary conditions for the existence of such structures and presented connections between Steiner systems and q-Steiner systems in 2002.
Anyway till this day no q-Steiner system has been found yet!

Application of q-analogs of designs:
$\Rightarrow$ NETWORK CODING!

- Error-correcting network code = a set of k-subspaces in $GF(q)^n$ such that each t-subspace is in at most 1 k-subspace

q-Steiner Systems and Network Codes

Definition

A $t-(n,k,1;q)$-design is called a q-Steiner system.

Etzion and Schwartz gave necessary conditions for the existence of such structures and presented connections between Steiner systems and q-Steiner systems in 2002.
Anyway till this day no q-Steiner system has been found yet!

Application of q-analogs of designs:
$\Rightarrow$ NETWORK CODING!

- Error-correcting network code = a set of k-subspaces in $GF(q)^n$ such that each t-subspace is in at most 1 k-subspace
- Perfect code = a set of k-subspaces in $GF(q)^n$ such that each t-subspace is in exactly 1 k-subspace

Construction

$\mathcal{M}$:= incidence matrix between k-subspaces and t-subspaces of $GF(q)^n$

$$\mathcal{M}_{T,K} := \begin{cases} 1 & \text{if } t\text{-subspace } T \leq k\text{-subspace } K \\ 0 & \text{else} \end{cases} .$$

Construction

$\mathcal{M} :=$ incidence matrix between k-subspaces and t-subspaces of $GF(q)^n$

$$\mathcal{M}_{T,K} := \begin{cases} 1 & \text{if } t\text{-subspace } T \leq k\text{-subspace } K \\ 0 & \text{else} \end{cases} .$$

Solve the diophantine system of equations

$$\mathcal{M} \cdot \vec{x} = \begin{pmatrix} \lambda \\ \vdots \\ \lambda \end{pmatrix}$$

$\Rightarrow$ 0/1-solution $\vec{x} = t - (n, k, \lambda; q)$-design

Construction

$\mathcal{M}$:= incidence matrix between k-subspaces and t-subspaces of $GF(q)^n$

$$\mathcal{M}_{T,K} := \begin{cases} 1 & \text{if } t\text{-subspace } T \leq k\text{-subspace } K \\ 0 & \text{else} \end{cases} .$$

Solve the diophantine system of equations

$$\mathcal{M} \cdot \vec{x} = \begin{pmatrix} \lambda \\ \vdots \\ \lambda \end{pmatrix}$$

$\Rightarrow$ 0/1-solution $\vec{x} = t - (n, k, \lambda; q)$-design

PROBLEM: Size of $\mathcal{M}$ grows too fast for increasing parameters!

Construction – Kramer-Mesner method

Prescribing a group G of automorphisms of the design reduces the size of $\mathcal{M}$

$\Rightarrow$ shrinked Kramer-Mesner matrix $\mathcal{M}^G :=$ incidence matrix between the G-orbits of k-subspaces and the G-orbits of t-subspaces of $GF(q)^n$

Construction – Kramer-Mesner method

Prescribing a group G of automorphisms of the design reduces the size of $\mathcal{M}$

$\Rightarrow$ shrinked Kramer-Mesner matrix $\mathcal{M}^G :=$ incidence matrix between the G-orbits of k-subspaces and the G-orbits of t-subspaces of $GF(q)^n$

Solve the new diophantine system of equations

$$\mathcal{M}^G \cdot \vec{x} = \begin{pmatrix} \lambda \\ \vdots \\ \lambda \end{pmatrix}$$

$\Rightarrow$ 0/1-solution $\vec{x} = t - (n, k, \lambda; q)$-design

Existing Implementation

Implementation with Double Cosets for the construction of $G \backslash\!\backslash \begin{bmatrix} GF(q)^n \\ k \end{bmatrix}_q$

Transform the problem of constructing $G \backslash\!\backslash \begin{bmatrix} GF(q)^n \\ k \end{bmatrix}_q$ into a double coset problem:

$$G \backslash\!\backslash \begin{bmatrix} GF(q)^n \\ k \end{bmatrix}_q \twoheadrightarrow G \backslash GL(n,q) / GL(n,q)_{\langle e_1,\ldots,e_k \rangle}$$

Existing Implementation

Implementation with Double Cosets for the construction of $G\backslash\!\!\backslash \begin{bmatrix} GF(q)^n \\ k \end{bmatrix}_q$

Transform the problem of constructing $G\backslash\!\!\backslash \begin{bmatrix} GF(q)^n \\ k \end{bmatrix}_q$ into a double coset problem:

$$G\backslash\!\!\backslash \begin{bmatrix} GF(q)^n \\ k \end{bmatrix}_q \twoheadrightarrow G\backslash GL(n,q)/GL(n,q)_{\langle e_1,\ldots,e_k\rangle}$$

PROBLEM: Works just a for a few selected groups

New Implementation

- Schreier-Sims algorithm for $G \leq GL(n, q)$
- Direct construction of $G \backslash\!\backslash \begin{bmatrix} GF(q)^n \\ k \end{bmatrix}_q$ via the laddergame

Schreier-Sims Algorithm for Matrix Groups

- compute a base and strong generating set (BSGS) of $G \leq GL(n, q)$

Schreier-Sims Algorithm for Matrix Groups

- compute a base and strong generating set (BSGS) of $G \leq GL(n, q)$
- G operates on the set of standard basis vectors of $GF(q)^n$

Schreier-Sims Algorithm for Matrix Groups

- compute a base and strong generating set (BSGS) of $G \leq GL(n, q)$
- G operates on the set of standard basis vectors of $GF(q)^n$
- stabilizer chain of G in terms of the base

$$G = G_1 \geq G_2 \geq \cdots \geq G_n = 1$$

Schreier-Sims Algorithm for Matrix Groups

- compute a base and strong generating set (BSGS) of $G \leq GL(n, q)$
- G operates on the set of standard basis vectors of $GF(q)^n$
- stabilizer chain of G in terms of the base

$$G = G_1 \geq G_2 \geq \cdots \geq G_n = 1$$

- transversal chain of G

$$T_1 \geq T_2 \geq \cdots \geq T_n \;, \quad T_i \in \mathcal{T}(G_i / G_{i+1})$$

Schreier-Sims Algorithm for Matrix Groups

- compute a base and strong generating set (BSGS) of $G \leq GL(n,q)$
- G operates on the set of standard basis vectors of $GF(q)^n$
- stabilizer chain of G in terms of the base

$$G = G_1 \geq G_2 \geq \cdots \geq G_n = 1$$

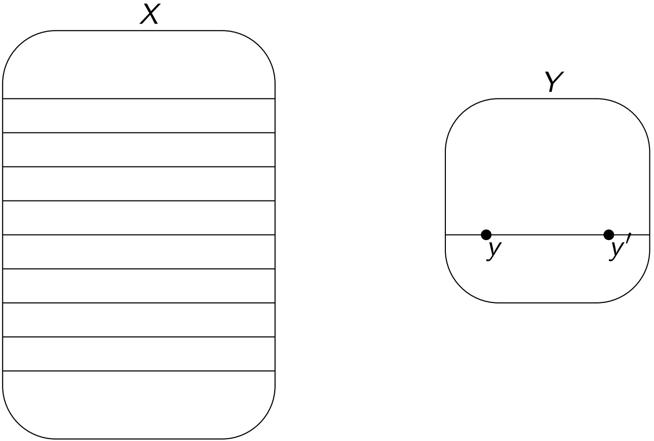
- transversal chain of G

$$T_1 \geq T_2 \geq \cdots \geq T_n\ , \quad T_i \in \mathcal{T}(G_i/G_{i+1})$$

$\Rightarrow$ $T_{i_{(i=1,\dots,n)}}$ as Input for Construction of $G \backslash\!\!\backslash \begin{bmatrix} GF(q)^n \\ k \end{bmatrix}_q$

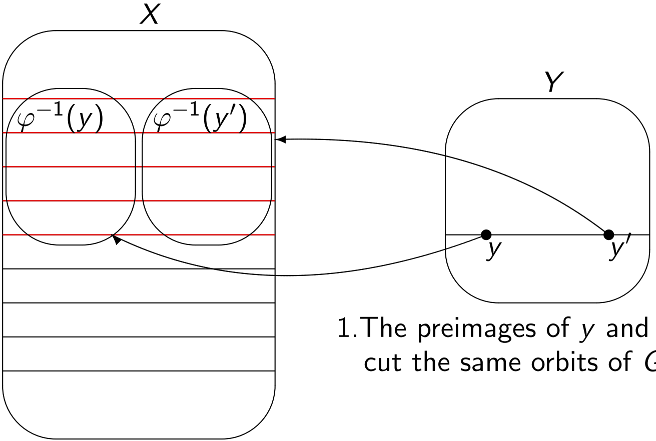
Homomorphism Principle

$\varphi : X \to Y$ is a surjective G-homomorphism



Homomorphism Principle

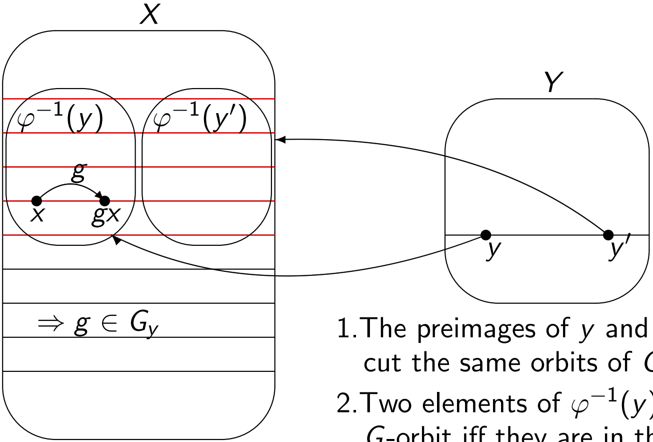
$\varphi : X \to Y$ is a surjective G-homomorphism



1. The preimages of y and y' cut the same orbits of G in X

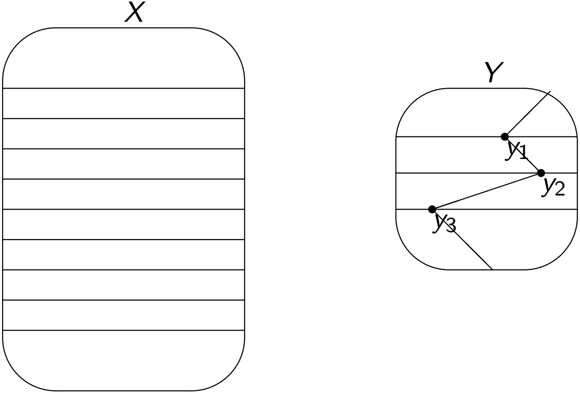
Homomorphism Principle

$\varphi : X \to Y$ is a surjective G-homomorphism

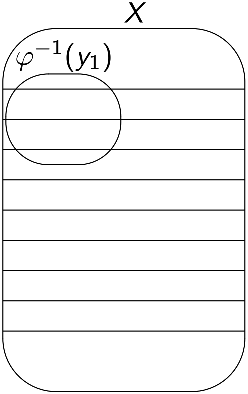


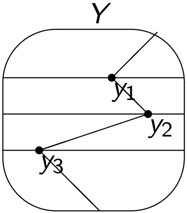
1. The preimages of y and y' cut the same orbits of G in X
2. Two elements of $\varphi^{-1}(y)$ are in the same G-orbit iff they are in the same orbit under G_y

1.case: get $G \backslash\backslash X$ from $G \backslash\backslash Y$ by splitting orbits

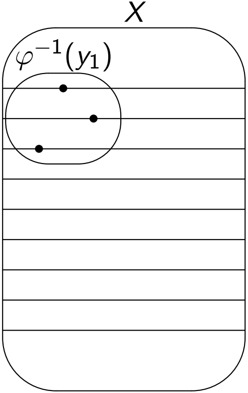


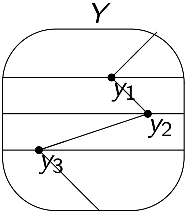
1.case: get $G\backslash\!\backslash X$ from $G\backslash\!\backslash Y$ by splitting orbits



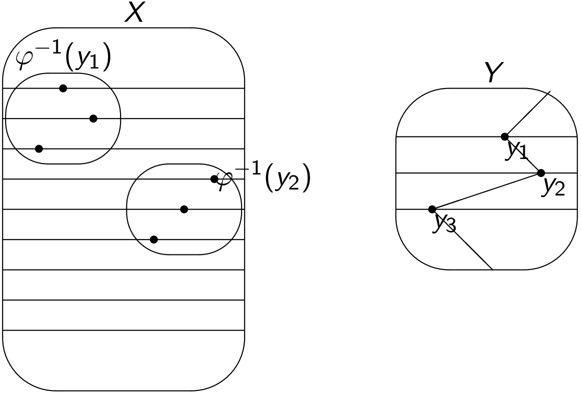


1.case: get $G\sslash X$ from $G\sslash Y$ by splitting orbits

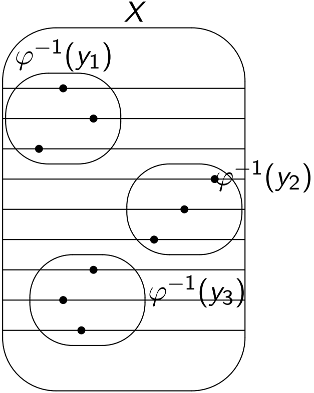


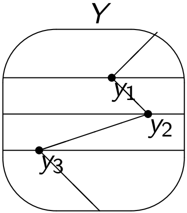


1.case: get $G\backslash\!\!\backslash X$ from $G\backslash\!\!\backslash Y$ by splitting orbits

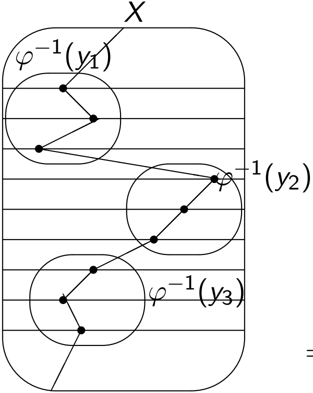


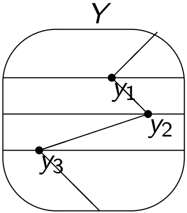
1.case: get $G \sslash X$ from $G \sslash Y$ by splitting orbits





1.case: get $G \backslash\backslash X$ from $G \backslash\backslash Y$ by splitting orbits





$$\Rightarrow \bigcup_i (G_{y_i} \backslash\backslash \varphi^{-1}(y_i)) \in \mathcal{T}(G \backslash\backslash X)$$

2.case: get $G \backslash\backslash Y$ from $G \backslash\backslash X$ by fusing orbits

Laddergame

$Y_i := \{y \leq GF(q)^n \mid dim(y) = i\}$

$X_i := \{(y, t) \mid y \in Y_{i-1}, t \in Y_1, t \nsubseteq y\}$

Laddergame

$Y_i := \{y \leq GF(q)^n \mid dim(y) = i\}$

$X_i := \{(y, t) \mid y \in Y_{i-1}, t \in Y_1, t \not\subseteq y\}$

- Downstep – Splitting orbits

$$\varphi_i : X_i \longrightarrow Y_{i-1},\ (y, t) \mapsto y$$

Laddergame

$Y_i := \{y \leq GF(q)^n \mid dim(y) = i\}$

$X_i := \{(y, t) \mid y \in Y_{i-1}, t \in Y_1, t \nsubseteq y\}$

- Downstep – Splitting orbits

$$\varphi_i : X_i \longrightarrow Y_{i-1},\ (y, t) \mapsto y$$

$$G \backslash\!\backslash Y_{i-1}$$

Laddergame

$Y_i := \{y \leq GF(q)^n \mid dim(y) = i\}$

$X_i := \{(y, t) \mid y \in Y_{i-1}, t \in Y_1, t \nsubseteq y\}$

- Downstep – Splitting orbits

$$\varphi_i : X_i \longrightarrow Y_{i-1},\ (y, t) \mapsto y$$

$$G \backslash\!\backslash Y_{i-1} \Rightarrow G \backslash\!\backslash X_i$$

Laddergame

$Y_i := \{y \leq GF(q)^n \mid dim(y) = i\}$

$X_i := \{(y, t) \mid y \in Y_{i-1}, t \in Y_1, t \not\subseteq y\}$

- Downstep – Splitting orbits

$$\varphi_i : X_i \to Y_{i-1},\, (y, t) \mapsto y$$

$$G \backslash\backslash Y_{i-1} \Rightarrow G \backslash\backslash X_i$$

- Upstep – Fusing orbits

$$\delta_i : X_i \to Y_i,\, (y, t) \mapsto \langle y \cup t \rangle$$

Laddergame

$Y_i := \{y \leq GF(q)^n \mid dim(y) = i\}$

$X_i := \{(y, t) \mid y \in Y_{i-1}, t \in Y_1, t \nsubseteq y\}$

- Downstep – Splitting orbits

$$\varphi_i : X_i \longrightarrow Y_{i-1},\ (y, t) \mapsto y$$

$$G \backslash\!\backslash Y_{i-1} \Rightarrow G \backslash\!\backslash X_i$$

- Upstep – Fusing orbits

$$\delta_i : X_i \longrightarrow Y_i,\ (y, t) \mapsto \langle y \cup t \rangle$$

$$G \backslash\!\backslash X_i$$

Laddergame

$Y_i := \{y \leq GF(q)^n \mid dim(y) = i\}$

$X_i := \{(y,t) \mid y \in Y_{i-1}, t \in Y_1, t \nsubseteq y\}$

- Downstep – Splitting orbits

$$\varphi_i : X_i \to Y_{i-1},\ (y,t) \mapsto y$$

$$G \backslash\!\backslash Y_{i-1} \Rightarrow G \backslash\!\backslash X_i$$

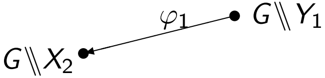
- Upstep – Fusing orbits

$$\delta_i : X_i \to Y_i,\ (y,t) \mapsto \langle y \cup t \rangle$$

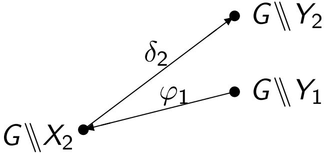
$$G \backslash\!\backslash X_i \Rightarrow G \backslash\!\backslash Y_i$$

- $G \mathbin{\!/\mkern-5mu/\!} Y_1$

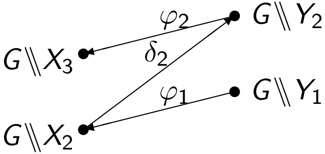
Laddergame



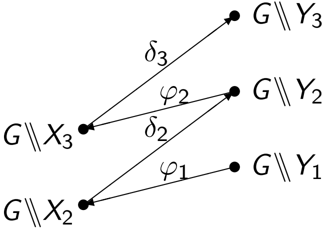
Laddergame



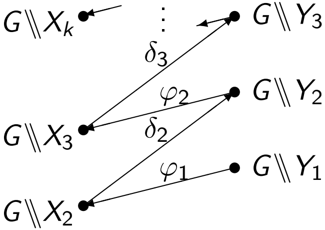
Laddergame



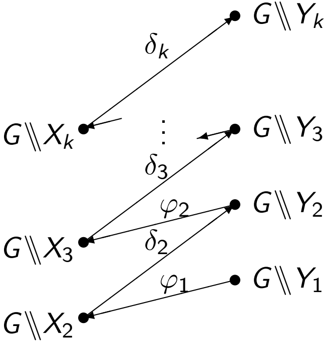
Laddergame



Laddergame



Laddergame



$G \mathbin{/\!/} Y_k$
δ_k
$G \mathbin{/\!/} X_k$
$G \mathbin{/\!/} Y_3$
δ_3
φ_2
$G \mathbin{/\!/} Y_2$
$G \mathbin{/\!/} X_3$
δ_2
φ_1
$G \mathbin{/\!/} Y_1$
$G \mathbin{/\!/} X_2$

New Results

parameters	$\|G\|$	dim $\mathcal{M}_{t,k}^{G}$	λ
$2-(6,3,\lambda;3)$	336	93×234	16
$2-(8,4,\lambda;2)$	1020	15×217	$35, 56, 70, 105, 126, 161,$ $176, 196, 245, 266, 280, 315$
$2-(9,3,\lambda;2)$	1533	31×529	$21, 22, 42, 43, 63$
$2-(9,4,\lambda;2)$	4599	11×725	$21, 63, 84, 126, 147, 189, 210,$ $252, 273, 315, 336, 378, 399, 462$ $504, 525, 567, 588, 651, 693$ $714, 756, 777, 840, 882, 903$ $945, 966, 1008, 1029, 1071, 1092$ $1134, 1155, 1197, 1218, 1281, 1323$

Open Problems

- q-Steiner systems ?
- Designs with $t > 3$?

Open Problems

- q-Steiner systems ?
- Designs with $t > 3$?

Thank you very much for your attention!

References

M. Braun, A. Kerber, R. Laue: *Systematic construction of q-analogs of designs*, Designs, Codes and Cryptography, 34(1): 55–70, 2005.

G. Butler: *The Schreier Algorithm for Matrix Groups*, SYMSAC '76, 167–170, 1976

T.Etzion, M. Schwartz: *Codes and Anticodes in the Grassmann Graph*, Journal of Combinatorial Theory, A 97: 27–42, 2002

A. Kohnert, S. Kurz: *Construction of Large Constant Dimension Codes With a Prescribed Minimus Distance*, Lecture Notes in Computer Science, 31–42, 2008

E. S. Kramer, D. M. Mesner: *t-Designs on Hypergraphs*, Discrete Mathematics 15: 263–296, 1976

R. Laue: *Construction of Combinatorial Objects – A Tutorial*, Bayreuther Mathematische Schriften 43: 53–96, 1993

S. Thomas: *Designs over Finite Fields*, Geom. Ded. 24: 237–242, 1987