Construction of $q$-analogs of combinatorial designs

Stefanie Braun

University of Bayreuth

ALCOMA’10 Thurnau

13. April 2010
Definition

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

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

$\iff$

$t - (n, k, \lambda; q)$-design
**q-Analogs of Combinatorial Designs**

**Definition**

Let $q$ be a positive integer. A $q$-analog of a $t-(n, k, \lambda)$-design is defined as follows:

$$
q\text{-analog of } t - (n, k, \lambda)\text{-design} \iff t - (n, k, \lambda; q)\text{-design} \iff \text{design of finite fields}
$$
Definition

\[ q\text{-analog of } t - (n, k, \lambda)\text{-design} \]

\[ \iff \]

\[ t - (n, k, \lambda; q)\text{-design} \]

\[ \iff \]

\[ \text{design of finite fields} \]

\[ \iff \]

\[ \mathcal{B} \subseteq \left[ \begin{array}{c} GF(q)^n \\ k \end{array} \right]_q : \left| \{ K \in \mathcal{B} \mid T \leq K \} \right| = \lambda \quad \forall \ T \in \left[ \begin{array}{c} GF(q)^n \\ t \end{array} \right]_q \]
History of Designs over Finite Fields

- S. Thomas (1987):
  
  \(2 - (n, 3, 7; 2)\)-designs \(\forall n \geq 7 \in \mathbb{N}\) with \(n \equiv \pm 1 \mod 6\)
History of Designs over Finite Fields

- **S. Thomas (1987):**
  \[ 2 - (n, 3, 7; 2)\text{-designs } \forall n \geq 7 \in \mathbb{N} \text{ with } n \equiv \pm 1 \mod 6 \]

- **H. Suzuki (1992):**
  \[ 2 - (n, 3, q^2 + q + 1; q)\text{-design } \forall n \geq 7 \text{ with } n \equiv \pm 1 \mod 6 \]
  \text{ and } q \text{ prime}

- **M. Miyakawa, A. Munemasa and S. Yoshiara (1995):**
  classification of \[ 2 - (7, 3, \lambda; q)\text{-designs for } q = 2, 3 \text{ with small } \lambda \]

- **T. Itoh (1998):**
  \[ 2 - (ml, 3, q^3(q^{l-5}/(q - 1); q)\text{-designs for any } m \geq 3 \]
  \text{ which admits the action of } SL(m, q^l) \]
History of Designs over Finite Fields

- S. Thomas (1987):
  \[ 2 - (n, 3, 7; 2) \text{-designs } \forall \ n \geq 7 \in \mathbb{N} \text{ with } n \equiv \pm 1 \mod 6 \]

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

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

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

- M. Braun (2005):
  \[ 3 - (8, 4, 11, 2) \text{-design} \]
A $t-(n, k, 1; q)$-design is called a $q$-Steiner system.
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.
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:

⇒ NETWORK CODING!
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

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

\[ M_{T,K} := \begin{cases} 
1 & \text{if } t\text{-subspace } T \leq k\text{-subspace } K \\
0 & \text{else} 
\end{cases} \]
\[ M := \text{incidence matrix between } k\text{-subspaces and } t\text{-subspaces of } GF(q)^n \]

\[ M_{T,K} := \begin{cases} 
1 & \text{if } t\text{-subspace } T \leq k\text{-subspace } K \\
0 & \text{else} 
\end{cases} \]

Solve the diophantine system of equations

\[ M \cdot \vec{x} = \begin{pmatrix} 
\lambda \\
\vdots \\
\lambda 
\end{pmatrix} \]

\[ \Rightarrow \text{0/1-solution } \vec{x} = t - (n, k, \lambda; q)\text{-design} \]
\[ M := \text{incidence matrix between } k\text{-subspaces and } t\text{-subspaces of } GF(q)^n \]

\[ M_{T,K} := \begin{cases} 1 & \text{if } t\text{-subspace } T \leq k\text{-subspace } K \\ 0 & \text{else} \end{cases} \]

Solve the diophantine system of equations

\[
M \cdot \vec{x} = \begin{pmatrix} \lambda \\ \vdots \\ \lambda \end{pmatrix}
\]

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

\text{PROBLEM: Size of } M \text{ grows too fast for increasing parameters!}
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 $GF(q)^n$
Prescribing a group $G$ of automorphisms of the design reduces the size of $\mathcal{M}$

$\Rightarrow$ shrunked 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 \( G \backslash \left[ \frac{GF(q)^n}{k} \right]_q \)

Transform the problem of constructing \( G \backslash \left[ \frac{GF(q)^n}{k} \right]_q \) into a double coset problem:

\[
G \backslash \left[ \frac{GF(q)^n}{k} \right]_q \rightarrow G \backslash GL(n, q)/GL(n, q)\langle e_1, \ldots, e_k \rangle
\]
Implementation with Double Cosets for the construction of $ G \sslash \left[ GF(q)^n \right]_q \\

Transform the problem of constructing $ G \sslash \left[ GF(q)^n \right]_q $ into a double coset problem:

$$ G \sslash \left[ GF(q)^n \right]_q \rightarrow G \backslash GL(n, q)/GL(n, q)_{\langle e_1, \ldots, e_k \rangle} $$

PROBLEM: Works just a for a few selected groups
New Implementation

- Schreier-Sims algorithm for $G \leq GL(n, q)$
- Direct construction of $G \backslash \left[ GF(q)^n \right]_k$ via the laddergame
compute a base and strong generating set (BSGS) of $G \leq GL(n, q)$.
compute a base and strong generating set (BSGS) of $G \leq GL(n, q)$

$G$ operates on the set of standard basis vectors of $GF(q)^n$
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

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

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

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

$\Rightarrow T_{i(i=1,\ldots,n)}$ as Input for Construction of $G\ \left[\begin{array}{c} GF(q)^n \\ k \end{array}\right]_q$
Homomorphism Principle

\[ \varphi : X \rightarrow Y \] 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 \( G \).
Homomorphism Principle

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

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

\( \varphi : X \rightarrow Y \) 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 $G\parallel X$ from $G\parallel Y$ by splitting orbits

\[ \phi^{-1}(y_1) \cup \phi^{-1}(y_2) \cup \phi^{-1}(y_3) \in T(G\parallel X) \]
1. case: get $G \parallel X$ from $G \parallel Y$ by splitting orbits

$X$

$\varphi^{-1}(y_1)$

$Y$

$y_1 - y_2 - y_3$
1. case: get $G\parallel X$ from $G\parallel Y$ by splitting orbits

$\varphi^{-1}(y_1)$
1. case: get $G\backslash\!\!\!\backslash X$ from $G\backslash\!\!\!\backslash Y$ by splitting orbits

\[ \varphi^{-1}(y_1) \subseteq X \]
\[ \varphi^{-1}(y_2) \subseteq X \]
\[ \varphi^{-1}(y_3) \subseteq X \]

\[ \varphi^{-1}(y_1) \cap \varphi^{-1}(y_2) \cap \varphi^{-1}(y_3) \subseteq X \]

\[ \bigcup_i (G y_i) \subseteq T(G X) \]

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

$X$

$\varphi^{-1}(y_1)$

$\varphi^{-1}(y_3)$

$\varphi^{-1}(y_2)$

$Y$

$y_1$

$y_2$

$y_3$

$\varphi^{-1}(y_1) \cup \varphi^{-1}(y_2) \cup \varphi^{-1}(y_3) \in T(G \parallel X)$
1. case: get $G \parallel X$ from $G \parallel Y$ by splitting orbits

\[ \varphi^{-1}(y_1) \]
\[ \varphi^{-1}(y_2) \]
\[ \varphi^{-1}(y_3) \]

\[ \Rightarrow \bigcup_{i} (G_{y_i} \parallel \varphi^{-1}(y_i)) \in \mathcal{T}(G \parallel X) \]

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

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

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

\[ Y_i := \{ y \leq GF(q)^n \mid \text{dim}(y) = i \} \]
\[ X_i := \{ (y, t) \mid y \in Y_{i-1}, t \in Y_1, t \not\in y \} \]

- Downstep – Splitting orbits

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

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

\[ X_i := \{(y, t) \mid y \in Y_{i-1}, t \in Y_1, t \not\subset y\} \]

- **Downstep – Splitting orbits**

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

\[ G \backslash Y_{i-1} \]
Laddergame

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

\[ X_i := \{(y, t) \mid y \in Y_{i-1}, t \in Y_1, t \notin y\} \]

- **Downstep – Splitting orbits**

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

\[ G \backslash Y_{i-1} \Rightarrow G \backslash X_i \]
\(Y_i := \{ y \leq GF(q)^n \mid \text{dim}(y) = i \}\)

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

- **Downstep – Splitting orbits**

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

  \[G\backslash Y_{i-1} \Rightarrow G\backslash X_i\]

- **Upstep – Fusing orbits**

  \(\delta_i : X_i \rightarrow Y_i, (y, t) \mapsto \langle y \cup t \rangle\)
Ladder Game

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

\[ X_i := \{(y, t) \mid y \in Y_{i-1}, t \in Y_1, t \notin y\} \]

- **Downstep – Splitting orbits**

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

\[ G \backslash Y_{i-1} \Rightarrow G \backslash X_i \]

- **Upstep – Fusing orbits**

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

\[ G \backslash X_i \]
Laddergame

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

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

- **Downstep – Splitting orbits**

\[ \varphi_i : X_i \rightarrow Y_{i-1}, \ (y, t) \mapsto y \]

\[ G \backslash Y_{i-1} \Rightarrow G \backslash X_i \]

- **Upstep – Fusing orbits**

\[ \delta_i : X_i \rightarrow Y_i, \ (y, t) \mapsto \langle y \cup t \rangle \]

\[ G \backslash X_i \Rightarrow G \backslash Y_i \]
• $G \parallel Y_1$
Laddergame
Laddergame
Laddergame
Laddergame
Laddersgame
### New Results

| parameters | $|G|$ | $\dim \mathcal{M}_{t,k}^G$ | $\lambda$ |
|------------|------|-----------------|--------|
| $2 - (6, 3, \lambda; 3)$ | 336 | $93 \times 234$ | 16 |
| $2 - (8, 4, \lambda; 2)$ | 1020 | $15 \times 217$ | 35, 56, 70, 105, 126, 161, 176, 196, 245, 266, 280, 315 |
| $2 - (9, 3, \lambda; 2)$ | 1533 | $31 \times 529$ | 21, 22, 42, 43, 63 |
| $2 - (9, 4, \lambda; 2)$ | 4599 | $11 \times 725$ | 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 $t > 3$ ?

Thank you very much for your attention!
Open Problems

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

Thank you very much for your attention!


