Derived designs of $q$-Fano planes and $q$-analogs of group divisible designs

Michael Kiermaier

Institut für Mathematik
Universität Bayreuth

Academy Contact Forum
“Coding Theory and Cryptography VIII”
September 27, 2019
Brussels, Belgium
What is this?

- Most frequent image in discrete math.
- Fano plane.
What is special about it?

- Smallest projective plane.
- Smallest non-trivial Steiner triple system.
Outline

Block designs and their \( q \)-analogs

Derived \( q \)-Fano planes and \( \alpha \)-points

\( q \)-analogs of group divisible designs
Outline

Block designs and their $q$-analsogs

Derived $q$-Fano planes and $\alpha$-points

$q$-analogs of group divisible designs
Subset lattice

- Let $V$ be a $\nu$-element set.
- $(\binom{V}{k}) :=$ Set of all $k$-subsets of $V$.
- $#(\binom{V}{k}) = (\binom{\nu}{k})$.
- Subsets of $V$ form a distributive lattice (wrt. $\subseteq$).

Definition

$D \subseteq (\binom{V}{k})$ is a $t-(\nu, k, \lambda)$ (block) design if each $T \in (\binom{V}{t})$ is contained in exactly $\lambda$ blocks (elements of $D$).

- If $\lambda = 1$: $D$ Steiner system
- If $\lambda = 1$, $t = 2$ and $k = 3$: $D$ Steiner triple system $STS(\nu)$
Example

\[ V = \{1, 2, 3, 4, 5, 6, 7\} \]
\[ D = \{\{1, 2, 7\}, \{1, 3, 6\}, \{1, 4, 5\}, \{2, 3, 5\}, \]
\[ \{2, 4, 6\}, \{3, 4, 7\}, \{5, 6, 7\}\} \]

Fano plane \(D\) is a 2-(7, 3, 1) design, i.e an STS(7).
Lemma
Let $D$ be a $t$-$\left(v, k, \lambda\right)$ design and $i, j \in \{0, \ldots, t\}$ with $i + j \leq t$. Then for all $I \in \binom{V}{i}$ and $J \in \binom{V}{v-j}$ with $I \subseteq J$

$$\lambda_{i,j} := \#\{B \in D \mid I \subseteq B \subseteq J\} = \lambda \cdot \frac{\binom{v-i-j}{k-i}}{\binom{v-t}{k-t}}.$$ 

In particular, $\#D = \lambda_{0,0}$. 

Example
Fano plane STS(7) ($v = 7, k = 3, t = 2, \lambda = 1$):

$$\lambda_{0,0} = 7 \quad \lambda_{1,0} = 3 \quad \lambda_{0,1} = 4 \quad \lambda_{2,0} = 1 \quad \lambda_{1,1} = 2 \quad \lambda_{0,2} = 2$$
Corollary: Integrality conditions
If a $t-(v, k, \lambda)$ design exists, then all $\lambda_{i,j} \in \mathbb{Z}$.

Sufficient to check: $\lambda_i := \lambda_{i,0} \in \mathbb{Z}$ (Parameters admissible)

Lemma
STS$(v)$ admissible $\iff v \equiv 1, 3 \pmod{6}$.

STS$(v)$ for small $v$

- STS$(3) = \{ V \}$ exists trivially.
- Smallest non-trivial Steiner triple system: Fano plane STS$(7)$.
- Next admissible case: STS$(9)$ exists (affine plane of order 3).

Theorem (Kirkman 1847)
All admissible STS$(v)$ do exist.
Subspace lattice

- Let $V$ be a $v$-dimensional $\mathbb{F}_q$ vector space.
- Grassmannian $\left[ \begin{array}{c} V \\ k \end{array} \right]_q := \text{Set of all } k\text{-dim. subspaces of } V$.
- Gaussian Binomial coefficient
  \[
  \# \left[ \begin{array}{c} V \\ k \end{array} \right]_q = \left[ \begin{array}{c} V \\ k \end{array} \right]_q = \frac{(q^v - 1)(q^{v-1} - 1) \cdots (q^{v-k+1} - 1)}{(q - 1)(q^2 - 1) \cdots (q^k - 1)}
  \]
- Subspaces of $V$ form a modular lattice (wrt. $\subseteq$).
- Subspace lattice of $V = \text{projective geometry } \text{PG}(v - 1, q)$
  - Elements of $\left[ \begin{array}{c} V \\ 1 \end{array} \right]_q$ are points.
  - Elements of $\left[ \begin{array}{c} V \\ 2 \end{array} \right]_q$ are lines.
  - Elements of $\left[ \begin{array}{c} V \\ 3 \end{array} \right]_q$ are planes.
  - Elements of $\left[ \begin{array}{c} V \\ v-1 \end{array} \right]_q$ are hyperplanes.
- Fano plane is the projective geometry $\text{PG}(2, 2)$. 
**$q$-analogs in combinatorics**

Replace subset lattice by subspace lattice!

<table>
<thead>
<tr>
<th>orig.</th>
<th>$q$-analog</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\nu$-element set $V$</td>
<td>$\nu$-dim. $\mathbb{F}_q$ vector space $V$</td>
</tr>
<tr>
<td>${V \choose k}$</td>
<td>$[V \choose k]_q$</td>
</tr>
<tr>
<td>${V \choose k}$</td>
<td>$[V \choose k]_q$</td>
</tr>
</tbody>
</table>

- **cardinality**
- **dimension**

- $\cap$  
- $\cap$

- $\cup$  
- $+$

- The subset lattice corresponds to $q = 1$.

- Sometimes: Unary field $\mathbb{F}_1$. 
Definition (block design, stated again)
Let $V$ be a $v$-element set.  
$D \subseteq \binom{V}{k}$ is a $t-(v, k, \lambda)$ (block) design 
if each $T \in \binom{V}{t}$ is contained in exactly $\lambda$ elements of $D$.

$q$-analog of a design?

Definition (subspace design)
Let $V$ be a $v$-dimensional $\mathbb{F}_q$ vector space.  
$D \subseteq [V]_k$ is a $t-(v, k, \lambda)_q$ (subspace) design 
if each $T \in [V]_t$ is contained in exactly $\lambda$ elements of $D$.

- If $\lambda = 1$: $D$ $q$-Steiner system
- If $\lambda = 1$, $t = 2$, $k = 3$: $D$ $q$-Steiner triple system $STS_q(v)$
- Geometrically:
  $STS_q(v)$ is a set of planes in $PG(v - 1, q)$
  covering each line exactly once.
Lemma
Let $D$ be a $t-$$(v, k, \lambda)_q$ design and $i, j \in \{0, \ldots, t\}$ with $i + j \leq t$. Then for all $I \in \left[V_i\right]_q$ and $J \in \left[V_{v-j}\right]_q$ with $I \subseteq J$

$$\lambda_{i,j} := \#\{B \in D \mid I \subseteq B \subseteq J\} = \lambda \frac{\left[V_{v-j}\right]_q}{\left[k-i\right]_q}.$$

In particular, $\#D = \lambda_{0,0}$.

Corollary: Integrality conditions
If a $t-$$(v, k, \lambda)_q$ design exists, then all $\lambda_{i,j} \in \mathbb{Z}$.

Sufficient to check: $\lambda_i := \lambda_{i,0} \in \mathbb{Z}$ (Parameters admissible)
Lemma
\(\text{STS}_q(\nu)\) admissible \(\iff\ \nu \equiv 1, 3 \pmod{6} \).

\(\text{STS}_q(\nu)\) for small \(\nu\)

- \(\nu = 3\): \(\text{STS}_q(3) = \{V\}\) exists trivially.
- \(\nu = 7\): \(q\)-analog of the Fano plane \(\text{STS}_q(7)\). Existence undecided for every field order \(q\).

Most important open problem in \(q\)-analogs of designs.

- \(\nu = 9\): \(\text{STS}_q(9)\): existence open for every \(q\).
- \(\nu = 13\): Only known non-trivial \(q\)-STS: \(\text{STS}_2(13)\) exists (Braun, Etzion, Östergård, Vardy, Wassermann 2013)
Status of the binary $q$-analog of the Fano plane.

\[ \lambda_{0,0} = 381 \]
\[ \lambda_{1,0} = 21 \]
\[ \lambda_{0,1} = 45 \]
\[ \lambda_{1,1} = 5 \]
\[ \lambda_{0,2} = 5 \]
\[ \lambda_{2,0} = 1 \]

- \text{STS}_2(7) consists of $\lambda_{0,0} = 381$ blocks (out of $\left[\binom{7}{3}\right]_2 = 11811$ planes).
- Huge search space ($\binom{11811}{381}$ has 730 digits).
- Heinlein, MK, Kurz, Wassermann 2019: Best known \textit{packing} has size 333.
- Braun, MK, Nakić 2016; MK, Kurz, Wassermann 2018: \text{STS}_2(7) has at most 2 automorphisms.
For general $q$:

\[(q^2 - q + 1)[\frac{7}{1}]_q\]

\[
\begin{array}{c}
q^4 + q^2 + 1 \\
1 \\
1
\end{array}
\quad
\begin{array}{c}
(q^3 + 1)(q^2 + 1) \\
q^2 + 1 \\
q^2 + 1
\end{array}
\]

Theme for remainder of the talk

» Let $D$ be a $\text{STS}_q(7)$.

» Fix a point $P$.

» What can be said about the “local” point of view of $D$ from $P$?
Outline

Block designs and their $q$-analogs

Derived $q$-Fano planes and $\alpha$-points

$q$-analogs of group divisible designs
Let $P$ be a point.

For $t-(v, k, \lambda)_q$ design $D$:

Derived design in $P$:

$$\{ B/P \mid B \in D \text{ with } P \subseteq B \} \subseteq V/P$$

is $(t - 1)-(v - 1, k - 1, \lambda)_q$ design.

For $STS_q(7)$:

Derived design is $1-(6, 2, 1)_q$ design.

That is a set of $\lambda_{1,0} = q^4 + q^2 + 1$ lines in $PG(5, q)$ covering all points exactly once.

In other words:

The derived design of $STS_q(7)$ in a point $P$ is a line spread of $PG(5, q)$.
Spread $S$ called geometric if for all distinct $L_1, L_2 \in S$:
\[ \{ L \in S \mid L \subseteq L_1 + L_2 \} \]
is spread of the solid $L_1 + L_2$.

$P$ is called $\alpha$-point of $\text{STS}_q(7)$ if the derived design in $P$ is a geometric spread.

S. Thomas 1996: There exists a non-$\alpha$-point.

O. Heden, P. Sissokho 2016: For $q = 2$:
Each hyperplane contains non-$\alpha$-point.

Goal: Investigate Heden-Sissokho result for general $q$!
Assume that $H$ is hyperplane containing only $\alpha$-points.

Fix a poor solid $S$ in $H$ (not containing any block).

Let $\mathcal{F} = \{ F \in \binom{H}{5} \mid S \subseteq F \}$. We have $\#\mathcal{F} = q + 1$.

For $F \in \mathcal{F}$, let

$$\mathcal{L}_F := \{ B \cap S \mid B \in D \text{ and } B + S = F \}.$$ 

Dimension formula:
$$\dim(B \cap S) = \dim(B) + \dim(S) - \dim(F) = 3 + 4 - 5 = 2.$$ 
So $\mathcal{L}_F$ is a set of lines in $S$.

Lemma $\mathcal{L}_F$ is a line spread of $S$.

Conclusion

$\mathcal{L} := \biguplus_{F \in \mathcal{F}} \mathcal{L}_F$ is a set of $(q + 1)(q^2 + 1)$ lines in $\text{PG}(3, q)$ admitting a partition into $q + 1$ line spreads.
Lemma
For each point $P$ in $S$, the $q + 1$ lines in $\mathcal{L}$ passing through $P$ span only a plane $E_P$.
(In other words, the lines form a pencil in $E_P$ through $P$.)

Corollary
$([S^1]_q, \mathcal{L})$ is a generalized quadrangle.

Classification
Classification of projective generalized quadrangles:
(F. Buekenhout, C. Lefèvre 1974)
$\implies ([S^1]_q, \mathcal{L})$ is symplectic generalized quadrangle $W(q)$. 
By property of $\mathcal{L}$:
The lines of $W(q)$ admit a partition into $q + 1$ line spreads.

Equivalently: The points of the parabolic quadric $Q(4, q)$ admit a partition into ovoids.

Not possible for even $q$.
  - Payne, Thas: Finite generalized quadrangles, 3.4.1(i)

Not possible for prime $q$.
  - Ball, Govaerts, Storme 2006:
    Each ovoid in $Q(4, q)$ is an elliptic quadric.
    Any two of them have non-trivial intersection.

**Theorem**
Let $q$ be prime or even and $D$ a $\text{STS}_q(7)$.
Then each hyperplane contains a non-$\alpha$-point of $D$.

**Research problem**
Investigate the remaining $q$ (i.e. $q$ a proper odd prime power).
Outline

Block designs and their $q$-analogs

Derived $q$-Fano planes and $\alpha$-points

$q$-analogs of group divisible designs
Definition (Classical group divisible design)
Let $V$ be a finite set of size $v$.
$(G, B)$ is a $(v, k, \lambda, g)$ group divisible design (gdd), if

1. $G \subseteq \binom{V}{g}$ is a partition of $V$.
2. $B \subseteq \binom{V}{k}$
3. such that each $T \in \binom{V}{2}$ is either contained in a group, or in exactly $\lambda$ blocks.
Example
A $(6, 3, 1, 2)$-gdd. (So: $v = 6$, $k = 3$, $\lambda = 1$, $g = 2$)

$V = \{1, 2, 3, 4, 5, 6\}$
$G = \{\{1, 2\}, \{3, 4\}, \{5, 6\}\}$
$B = \{\{1, 3, 6\}, \{1, 4, 5\}, \{2, 3, 5\}, \{2, 4, 6\}\}$
Definition (\(q\)-analog of group divisible design)

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

\((\mathcal{G}, \mathcal{B})\) is a \((v, k, \lambda, g)_q\) group divisible design (gdd), if

\(\mathcal{G} \subseteq \binom{V}{g}_q\) is a spread of \(V\).

\(\mathcal{B} \subseteq \binom{V}{k}_q\)

such that each \(T \in \binom{V}{2}_q\) is either contained in a group, or in exactly \(\lambda\) blocks.
Lemma
Let $D$ be a $2-(v, k, 1)_q$ Steiner system on $V$ and $P \in \binom{V}{1}_q$. Projection mod $P$ is

$$
\pi : \text{PG}(V) \to \text{PG}(V / P), \quad U \mapsto (U + P) / P
$$

Set

$$
\mathcal{G} := \{ \pi(B) \mid B \in D \text{ and } P \subseteq B \}
$$
$$
\mathcal{B} := \{ \pi(B) \mid B \in D \text{ and } P \not\subseteq B \}
$$

Then $(\mathcal{G}, \mathcal{B})$ is a $(v - 1, k, q^2, k - 1)_q$-gdd.

Application to $q$-Fano plane
Existence of $\text{STS}_q(7) \implies$ Existence of $(6, 3, q^2, 2)_q$-gdd
Admissibility of the parameters

1. Spread $\mathcal{G}$ exists $\iff g \mid v$

2. For all blocks $B \in \mathcal{B}$ and $G \in \mathcal{G}$:
   \[ \dim(B \cap G) \leq 1 \quad (B \text{ scattered wrt } \mathcal{G}) \implies k \leq v - g \]

3. Double count incidences $(B, T)$ with $B \in \mathcal{B}$ and $T \in \binom{B}{2} q$
   \[ \implies \#\mathcal{B} = \lambda \cdot \frac{\binom{v}{2} q - \binom{v}{1} q / \binom{g}{1} q \cdot \binom{g}{2} q}{\binom{k}{2} q} \in \mathbb{Z} \]

4. Fix $P \in \binom{V}{1} q$, let $r = \#\{B \in \mathcal{B} \mid P \subseteq B\}$ replication number.
   Double count incid. $(B, T)$ with $B \in \mathcal{B}$, $T \in \binom{B}{2} q$, $P \subseteq T$
   \[ \implies r = \lambda \cdot \frac{\binom{v-1}{1} q - \binom{g-1}{1} q}{\binom{k-1}{1} q} \in \mathbb{Z} \]

1. – 4. are counterparts of conditions for classical gdds.
New admissibility condition (no classical counterpart):

**Lemma**

$q^{k-g} \mid \lambda$

**Proof.**

- Let $P$ be a point.
- There is a unique $G \in \mathcal{G}$ passing through $P$.
- Let $G'$ be image of $G$ mod $P$.
- Points outside of $G'$ are covered $\lambda$ times by the images of the blocks ($k-1$-subspaces).
- $\quad \iff \lambda$-fold repetition of the complement of $G'$ is $q^{k-2}$-divisible.
- $\quad \iff \lambda$-fold repetition of $G'$ is $q^{k-2}$-divisible.
- $G'$ is exactly $q^{g-2}$-divisible, so $q^{k-g} \mid \lambda$. 

□
Lemma
Let $G \subseteq \left[ \begin{array}{c} V \\ g \end{array} \right]_q$ be spread, $G$ subgroup of $\Gamma L(v, q)_G$.
If action of $G$ on $\left[ \begin{array}{c} V \\ 2 \end{array} \right]_q \setminus \bigcup_{U \in G} \left[ \begin{array}{c} U \\ 2 \end{array} \right]_q$ is transitive
$\implies$ For any union $\mathcal{B}$ of $G$-orbits on the scattered $k$-subspaces
$(G, \mathcal{B})$ is a $(v, k, \lambda, g)_q$-gdd (with suitable $\lambda$).

Proof.
Use transitivity.

Remark on the principle
- Powerful construction method for classical designs.
- Does not work for subspace designs (lack of suitable groups).
Now:

- $v = g \cdot s$
- $V = (\mathbb{F}_{q^g})^s$
- $G = \begin{bmatrix} V \\ 1 \end{bmatrix}_{q^g}$ Desarguesian $(g - 1)$-spread.
- $\forall U \leq \mathbb{F}_q V : \dim_{\mathbb{F}_{q^g}} \langle U \rangle_{\mathbb{F}_{q^g}} \leq \dim_{\mathbb{F}_q}(U)$.

   In case of equality: $U$ fat

- Let $\mathcal{F}_k$ be set of fat $k$-subspaces.
- Lines covered by elements of $G = \text{non-fat 2-subspaces}$.

**Lemma**

Action of $\text{SL}(s, q^g)/(\mathbb{F}_q^\times \cap \text{SL}(s, q))$ on $\mathcal{F}_k$

- for $k < s$: is transitive
- for $k = s$: $\frac{q^g - 1}{q - 1}$ orbits of equal length
Theorem
Let $g \geq 2$ and $s \geq 3$.

- **Case** $k \in \{3, \ldots, s-1\}$:
  
  $(G, F_k)$ is $(gs, k, \lambda, g)_q$-gdd with

  \[
  \lambda = q^{(g-1)((k^2)-1)} \prod_{i=2}^{k-1} \frac{q^{g(s-i)} - 1}{q^{k-i} - 1}.
  \]

- **Case** $k = s$:
  
  For all $\alpha \in \{1, \ldots, \frac{q^g-1}{q-1}\}$ and any union $B$ of $\alpha$ orbits of the action of $\text{SL}(s, q^g)/(\mathbb{F}_q^* \cap \text{SL}(s, q))$ on $F_s$:

  $(G, F_k)$ is a $(gs, s, \lambda, g)_q$-gdd with

  \[
  \lambda = \alpha q^{(g-1)((k^2)-1)} \prod_{i=2}^{s-2} \frac{q^{g_i} - 1}{q^i - 1}.
  \]
Remark

- Theorem with $g = 2$, $k = s = 3$, $\alpha = 1$:
  $\exists (6, 3, q^2, 2)q \text{ gdds}$
- We have seen: gdds with these parameters would arise from $q$-analog of the Fano plane $\text{STS}_q(7)$.
- First $(6, 3, q^2, 2)q$-gdds constructed by Etzion, Hooker 2018.
- If $\text{STS}_q(7)$ exists $\implies (6, 3, q^2, 2)q$-gdds exist for non-Desarguesian spreads, too. ($\alpha$-points!)
  Found computationally for $q = 2$.

Conclusion for binary $q$-analog of the Fano plane

- $\text{STS}_2(7)$ cannot look too nice.
  (at most 2 automorphisms; result on $\alpha$-points)
  $\leadsto$ Might be seen as sign for non-existence.
- So far, all “local” investigations lead to consistent answers.
  $\leadsto$ Might be seen as sign for existence.
Open problems

▶ Further investigate $\alpha$-points.
▶ Computational evidence:

▶ For the Desarguesian spread:
  \[(6, 3, \lambda, 2)_2 \text{ exists } \iff \lambda \in \{2, 4, 6, 8, 10, 12\}\]

▶ For the 131,043 non-Desarguesian spreads:
  \[(6, 3, \lambda, 2)_2 \text{ exists only for } \lambda \in \{4, 8, 12\}\]

Explain this!

▶ For any of the 8 solid spreads in $\text{PG}(7, 2)$:
  No \((8, 4, 7, 4)_2\) does exist. Explanation?
Invitation!
Conference ALCOMA 20
(Algebraic Combinatorics and Applications)

▶ 2020-3-29 – 2020-4-4
▶ Kloster Banz, Lichtenfels, Germany
▶ https://alcoma20.uni-bayreuth.de/

Photo from Wikipedia, © Reinhold Möller