Subspace codes and q-analogs of designs

Michael Kiermaier

Institut für Mathematik
Universität Bayreuth
Germany

January 19, 2022
Universität Bayreuth

Outline

Outline

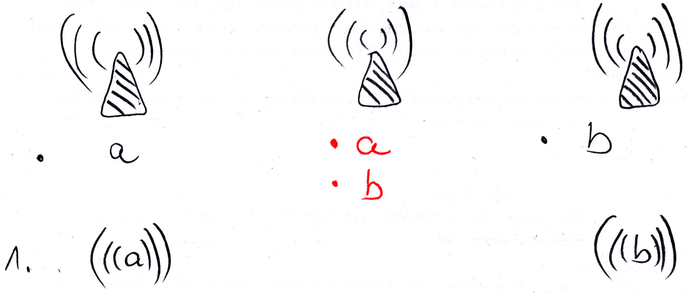
Example

3 time units needed.

Example

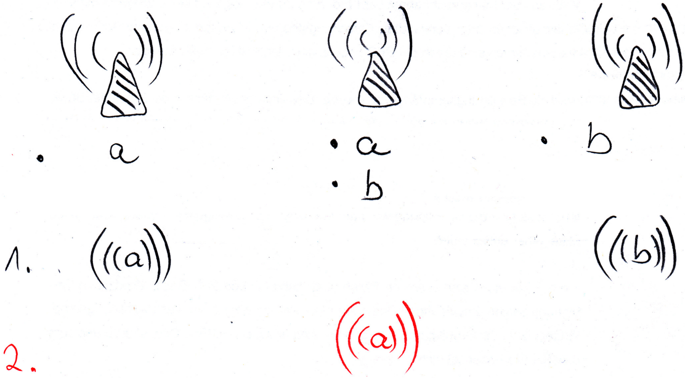
3 time units needed.

Example



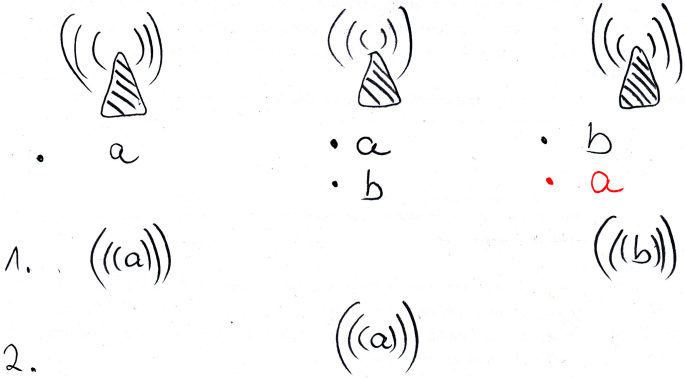
3 time units needed.

Example



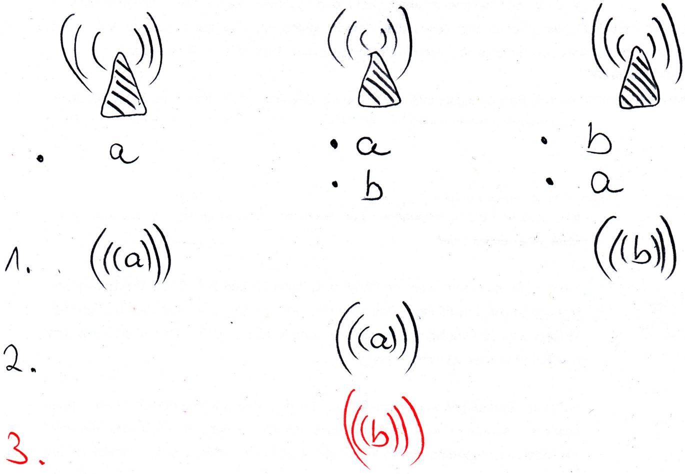
3 time units needed.

Example



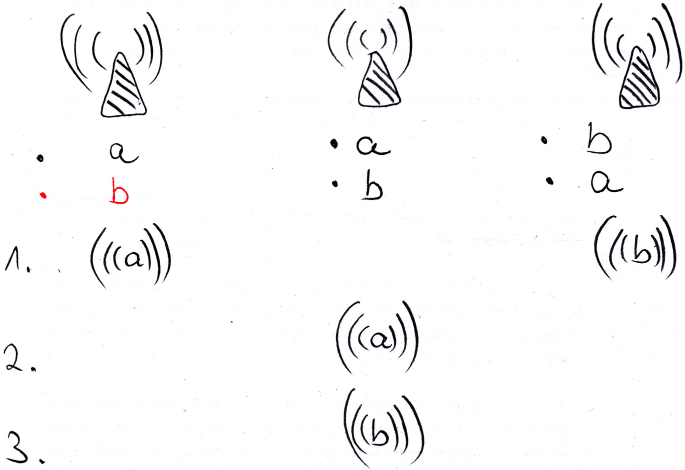
3 time units needed.

Example



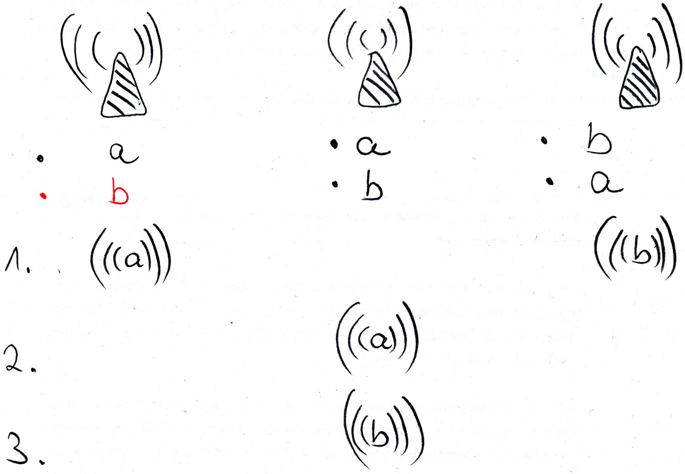
3 time units needed.

Example



3 time units needed.

Example

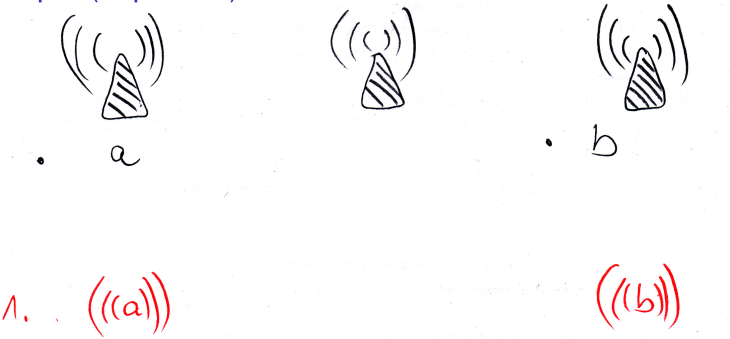


3 time units needed.

Example (improved)

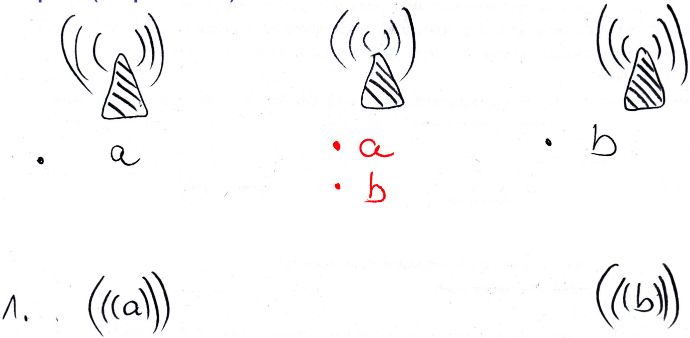
Improvement to 2 time units!

Example (improved)



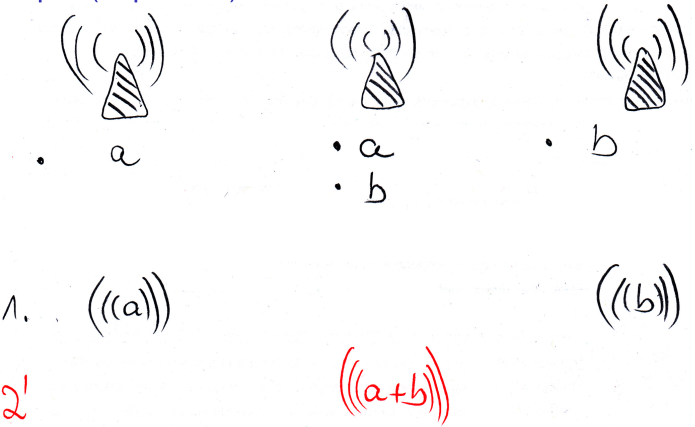
Improvement to 2 time units!

Example (improved)



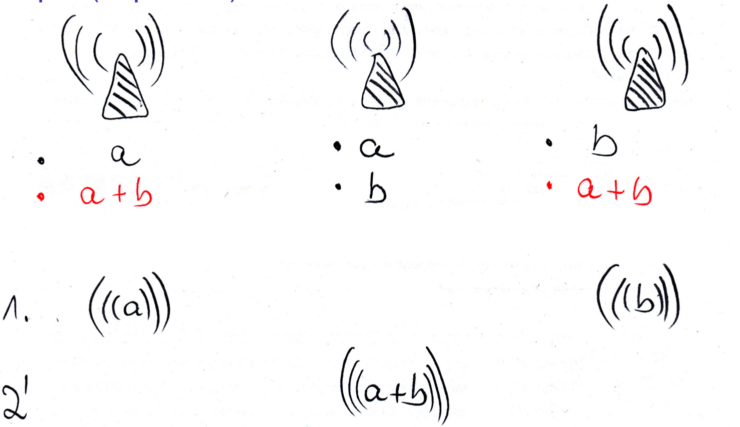
Improvement to 2 time units!

Example (improved)



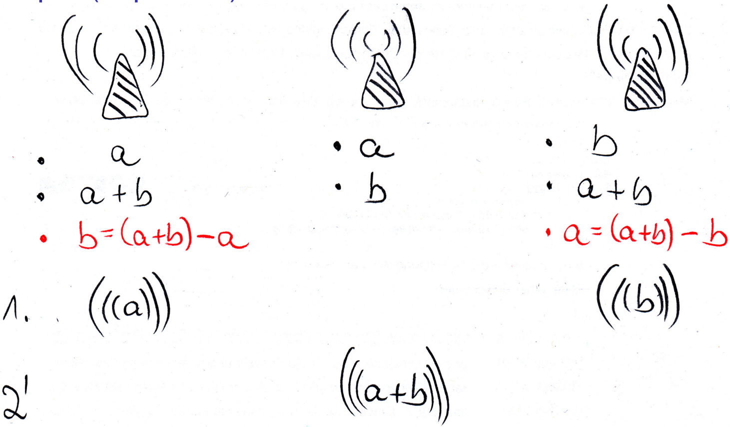
Improvement to 2 time units!

Example (improved)



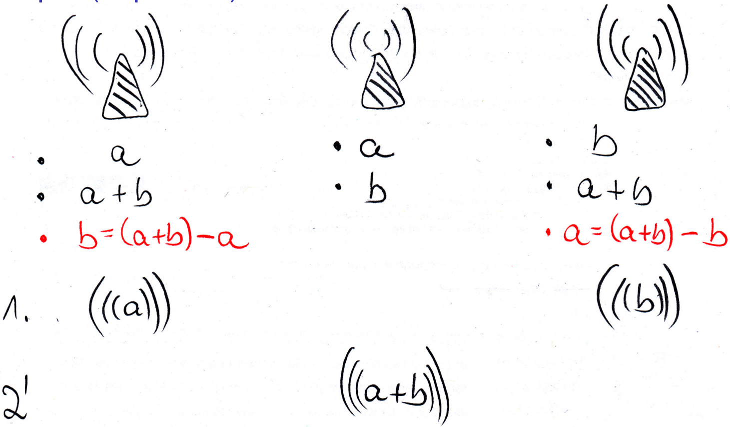
Improvement to 2 time units!

Example (improved)



Improvement to 2 time units!

Example (improved)



Improvement to 2 time units!

Subspace codes

- Given: Communication network
  with several senders and receivers.
  (internet broadcasting, cloud storage, ...)
- From example:
  For optimal transmission times, consider sending linear combinations of messages.
- Error correction in such networks?
- Electrical engineers Kötter and Kschischang in 2008:
  Definition of suitable error correcting codes
  for network coding.
- Interesting mathematical objects on its own.
- Interconnections to several established fields of research.
- Interpretation: q-analog (or geometrization) of classical binary block codes.

Fixed notation

- q prime power
- V an $\mathbb{F}_q$-vector space of dimension v.
- $\mathcal{L}(V)$ lattice of all subspaces of V.
- Grassmannian $\begin{bmatrix} V \\ k \end{bmatrix}_q :=$ Set of all k-dim. subspaces of V.
  Reminder: $\#\begin{bmatrix} V \\ k \end{bmatrix}_q = \begin{bmatrix} v \\ k \end{bmatrix}_q$ Gaussian binomial coefficient.

Projective geometry

- Subspace lattice $\mathcal{L}(V)$
  $=$ finite projective geometry $\mathrm{PG}(V) \cong \mathrm{PG}(v-1, q)$
  - Elements of $\begin{bmatrix} V \\ 1 \end{bmatrix}_q$ are points.
  - Elements of $\begin{bmatrix} V \\ 2 \end{bmatrix}_q$ are lines.
  - Elements of $\begin{bmatrix} V \\ 3 \end{bmatrix}_q$ are planes.
  - Elements of $\begin{bmatrix} V \\ 4 \end{bmatrix}_q$ are solids.
  - Elements of $\begin{bmatrix} V \\ v-1 \end{bmatrix}_q$ are hyperplanes.

Definition (Kötter, Kschischang 2008)

- subspace distance on $\mathcal{L}(V)$:
  $d(A, B) = \dim(A + B) - \dim(A \cap B) =$
  $\dim(A) + \dim(B) - 2\dim(A \cap B)$
- $C \subseteq \mathcal{L}(V)$ subspace code.
  Its elements are the codewords or blocks of C.
- $d(C) = \min\{d(A, B) \mid A \neq B \in C\}$
  (minimum) subspace distance of C.
- Abbreviation: C is $(v, \#C, d(C))_q$-subspace code.
- Important special case $C \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$
  $\Longrightarrow$ C constant dimension (subspace-)code,
  abbreviated C $(v, \#C, d(C); k)_q$ CDC.
- We want: $\#C$ large, $d(C)$ large
- Let $A_q(v, d; k)$ maximum size M of $(v, M, d; k)_q$ CDC.

Research goals

- Find lower bounds for $A_q(v, d; k)$ by constructing good codes.
- Find upper bounds for $A_q(v, d; k)$.
- Determine exact values of $A_q(v, d; k)$.
- Classify all optimal CDCs.
- (Find efficient decoding algorithms.)

Outline

Subspace codes and partial spreads

- For $\dim(A) = \dim(B) = k$ we have $d(A, B) = 2(k - \dim(A \cap B))$.
  $\implies$ minimum distance $d(C) = 2\delta$ of CDC C is even.
- With $t := k - \delta + 1$:
  $C \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$ CDC with $d(C) \geq 2\delta$
  $\iff$ every t-subspace of V
  is contained in at most one codeword.
- Therefore: $C \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$ is $(v, M, 2k; k)_q$ CDC
  $\iff$ Each point of $\mathrm{PG}(V)$
  is contained in at most one codeword.
- In finite geometry, these objects are known as partial $(k-1)$-spreads.

Spreads

- Partial $(k-1)$-spread covering all points of $\mathrm{PG}(V)$ is called $(k-1)$-spread.
- Known: $(k-1)$-spread exists $\iff k \mid v$.
- $\implies$ For $k \mid v$ we have $A_q(v, 2k; k) = \begin{bmatrix} v \\ 1 \end{bmatrix}_q / \begin{bmatrix} k \\ 1 \end{bmatrix}_q = \frac{q^v - 1}{q^k - 1}$.
- Maximum size $A_q(v, 2k; k)$ of partial spreads studied since the 1970s, not known in general.
- Recent strong result (Năstase, Sissokho 2017):

  Write $v = tk + r$ with remainder $r \in \{0, \ldots, k-1\}$. Then

$$A_q(v, 2k; k) = \frac{q^v - q^{k+r}}{q^k - 1} + 1$$

  whenever $k > \begin{bmatrix} r \\ 1 \end{bmatrix}_q$.

Holes

- Let S be a partial $(k-1)$-spread.
- Let P be its set of holes (points not covered by S).
- Observation:
  P defines an $\mathbb{F}_q$-linear code C of effective length $\#P$,
  C is q^{k-1}-divisible (all Hamming weights divisible by q^{k-1}).
- K., Kurz 2018: Classification of the effective lengths of Δ-divisible $\mathbb{F}_q$-linear codes where Δ power of q.
- Result of Năstase and Sissokho follows as a corollary!

Improvement of the Johnson bound

- Xia, Fu 2009: Important recursive bound for CDCs (Johnson bound)

$$A_q(v,d;k) \le \left\lfloor \frac{(q^v-1)A_q(v-1,d;k-1)}{q^k-1} \right\rfloor$$

- Idea: Fix a point P and consider the image in V/P.
- K., Kurz 2018: Improvement of the Johnson bound.
- Idea:
  - Suitable notion of "holes" (with multiplicities!) of a CDC.
  - Holes yield a divisible code, apply characterization of effective lengths.
- Example: best known bound $A_2(9,6;4) \le 1158$ improved to $A_2(9,6;4) \le 1156$.

Outline

The case $A_q(6,4;3)$

- Smallest case not covered by results on partial spreads: $v = 6$, $k = 3$, $d = 4$.
- Geometrically: Set of planes in $\mathrm{PG}(\mathbb{F}_q^6)$ intersecting pairwise at most in a point.
- Best known upper bound: $A_q(6,4;3) \leq (q^3+1)^2$. (Johnson bound + result on partial spreads)

Computer classification for $q = 2$

- In binary case $q = 2$: $A_2(6,4;3) \leq 81$.
- Best known construction $\rightsquigarrow A_2(6,4;3) \geq 77$.
- Goal: Classify all CDCs of maximum size for $q = 2$.
- Huge search space: There are $\begin{bmatrix}6\\3\end{bmatrix}_2 = 1395$ planes,

$$\binom{1395}{77} = \text{129-digit number}.$$

- Intermediate classification steps needed.

9-configurations

- 9-configuration = set of 9 planes of subspace distance ≥ 4, passing through a common point.
- Lemma: If $\#C \geq 73$ then C contains a 9-configuration.
- 9-configurations $\hat{=}$ partial line spreads in $\mathrm{PG}(\mathbb{F}_2^5)$.
- Soicher 2000: 4 isomorphism types.

17-configurations

- 17-configuration = set of 17 planes of subspace distance ≥ 4 containing two 9-configurations.
- Lemma: If $\#C \geq 74$ then C contains a 17-configuration.
- Computer classification of 17-configurations:
  - Compute all extensions of the 4 types of 9-configurations.
  - Filter out isomorphic copies.
  - Result: 12770 isomorphism types of 17-configurations.
- For each of the 12770 17-configurations, compute all extensions to $(6, M, 4; 3)_2$ CDCs with $M \geq 77$.

Result of the classification:

Theorem (Honold, K., Kurz 2015)

- $A_2(6,4;3) = 77$
- 5 PGL-isomorphism types of $(6,77,4;3)_2$ CDCs.

Analysis of the computer result

- The most symmetric $(6,77,4;3)_2$-code shows a clear construction principle.
- This construction generalizes to all values of q.

Theorem (Honold, K., Kurz 2015)

For all q,

$$q^6 + 2q^2 + 2q + 1 \leq A_q(6,4;3) \leq q^6 + 2q^3 + 1.$$

Next open case for $q = 2$ is $333 \leq A_2(7,4;3) \leq 381$.
$\rightsquigarrow$ q-analog of the Fano plane.

Outline

Outline

Subset lattice

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

Definition

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

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

Subset lattice

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

Definition

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

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

Subset lattice

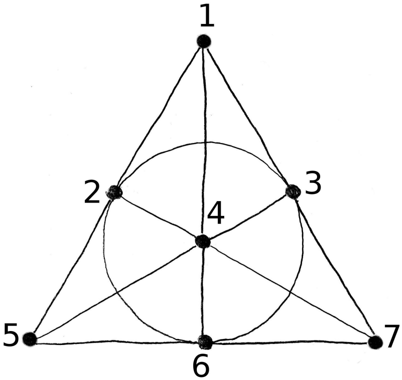
- Let V be a v-element set.
- $\binom{V}{k} :=$ Set of all k-subsets of V.
- $\#\binom{V}{k} = \binom{v}{k}$.
- Subsets of V form a distributive lattice (wrt. $\subseteq$).

Definition

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

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

Example (Fano plane $\mathrm{PG}(2,2)$)



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

Fano plane D is a 2-$(7,3,1)$ design, i.e an $\mathrm{STS}(7)$.

Idea of q-analogs in combinatorics

Replace subset lattice by subspace lattice!

Dictionary

original	q-analog
subset lattice	subspace lattice
v-element set V	v-dim. $\mathbb{F}_q$ vector space V
$\binom{V}{k}$	$\begin{bmatrix} V \\ k \end{bmatrix}_q$
$\binom{v}{k}$	$\begin{bmatrix} v \\ k \end{bmatrix}_q$
cardinality	dimension
$\cap$	$\cap$
$\cup$	$+$
$q = 1$	q proper prime power
"$\mathbb{F}_1$"	$\mathbb{F}_q$

Definition (block design, stated again)

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 of a design?

Definition (subspace design)

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

- If $\lambda = 1$: D q-Steiner system
- If $\lambda = 1$, $t = 2$, $k = 3$: D q-Steiner triple system $\mathrm{STS}_q(v)$
- Geometrically:
  $\mathrm{STS}_q(v)$ is a set of planes in $\mathrm{PG}(v - 1, q)$
  covering each line exactly once.

Remarks

- First definition of subspace designs by P. Cameron, 1972.

  "Several people have observed that the concept of a t-design can be generalised as follows. [...]"
- $1\text{-}(v, k, 1)_q$ designs $\quad \hat{=} \quad$ $(k-1)$-spreads in $\mathrm{PG}(v-1, q)$
- First construction of non-trivial subspace designs with $t \geq 2$ by S. Thomas in 1987.
- subspace codes $=$ q-analog of binary block codes,
  CDCs $=$ q-analog of binary constant weight codes.

Existence of subspace designs

- Fazeli, Lovett, Vardy 2014 (non-constructive proof):
  Non-trivial subspace designs exist for all t.
- Still not too many concrete constructions are known.

Known infinite series of subspace designs with $t \geq 2$

- Thomas 1987; Suzuki 1990 and 1992:
  $2\text{-}(v, 3, q^2 + q + 1; q)$ for all q and $v \equiv \pm 1 \pmod 6$, $v \geq 7$.
- A series by Itoh 1998.
- Braun, K., Kohnert, Laue 2017: $2\text{-}(v, k, \begin{bmatrix} v-2 \\ k-2 \end{bmatrix}_q / 2)_q$
  for $q \in \{3, 5\}$, $v \equiv 2 \pmod 4$, $v \geq 6$, $k \equiv 3 \pmod 4$,
  $3 \leq k \leq v - 3$.
- K., Laue, Wassermann 2018: $2\text{-}(v, k, \begin{bmatrix} v-2 \\ k-2 \end{bmatrix}_q / 3)_2$
  for $v \geq 8$, $2 \leq (v \bmod 6) < (k \bmod 6) \leq 5$.
- Braun, K., Laue 2019: $2\text{-}(8, 4, \frac{(q^6-1)(q^3-1)}{(q^2-1)(q-1)})_q$ for all q.

Subspace designs with $t \geq 3$

- $t = 3$: Only two subspace designs known.
- $t \geq 4$: no subspace design known.

Subspace designs and subspace codes

- Let $C \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$ and $t = k - \delta + 1$.
- Remember: C is $(v, \#C, 2\delta)_q$ CDC
$\Leftrightarrow$ each $T \in \begin{bmatrix} V \\ t \end{bmatrix}_q$ is contained in at most 1 element of C.
- By definition: C is t-$(v, k, \lambda)_q$ subspace design
$\Leftrightarrow$ each $T \in \begin{bmatrix} V \\ t \end{bmatrix}_q$ is contained in exactly λ elements of C.
- Therefore:
C is both $(v, \#C, 2\delta)_q$ CDC and t-$(v, k, \lambda)_q$ design
$\iff$ C is a Steiner system
($\iff$ C is a diameter perfect CDC)

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 $I \in \begin{bmatrix} V \\ i \end{bmatrix}_q$ and $J \in \begin{bmatrix} V \\ v-j \end{bmatrix}_q$ with $I \subseteq J$

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

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)

Corollary

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

$\mathrm{STS}_q(v)$ for small admissible v

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

  Most important open problem in q-analogs of designs.
- $v = 9$
  existence open for every q.
- $v = 13$
  $\mathrm{STS}_2(13)$ exists (Braun, Etzion, Östergård, Vardy, Wassermann 2013)

  Only known non-trivial q-Steiner system with $t \geq 2$!

Status of $STS_q(7)$

- A $STS_q(7)$ is a set of planes in $PG(\mathbb{F}_2^7)$ covering each line exactly once.
- A $STS_q(7)$ has size $\lambda_{0,0} = q^8 + q^6 + q^5 + q^4 + q^3 + q^2 + 1$.
  - binary: 381
  - ternary: 7651
- $STS_q(7)$ exists if and only if $A_q(7, 4; 3) = q^8 + q^6 + q^5 + q^4 + q^3 + q^2 + 1$.
- Question for its existence first stated in 1972.
- Still open for every q.
- Largest known subspace codes:
  - binary: 333 (Heinlein, K., Kurz, Wassermann 2019)
  - ternary: 6978 (Honold, K. 2016 + extension by D. Heinlein)

q-Pascal triangle for $\mathrm{STS}_q(7)$ D

$$\lambda_{0,0} = q^8 + q^6 + q^5 + q^4 + q^3 + q^2 + 1$$

$$\lambda_{1,0} = q^4 + q^2 + 1 \qquad \lambda_{0,1} = q^5 + q^3 + q^2 + 1$$

$$\lambda_{2,0} = 1 \qquad \lambda_{1,1} = q^2 + 1 \qquad \lambda_{0,2} = q^2 + 1$$

- Each point P is contained in $\lambda_{1,0} = q^4 + q^2 + 1$ blocks.
- $\rightsquigarrow$ derived design wrt P (“local point of view from P”)

$$\mathrm{Der}_P(D) = \{B/P \mid B \in D \text{ with } P \subseteq B\} \subseteq V/P$$

- In general: $\mathrm{Der}_P(D)$ is $(t-1)$-$(v-1, k-1, \lambda)_q$ design.
- $\implies$ $\mathrm{Der}_P(\mathrm{STS}_q(7))$ is 1-$(6, 2, 1)_q$ design.
  $=$ set of lines in $\mathrm{PG}(5, q)$ covering each point exactly once.
- In other words: $\mathrm{Der}(\mathrm{STS}_q(7))$ is a line spread of $\mathrm{PG}(5, q)$.

Outline

α-points

- spread $\mathcal{S}$ called geometric if for all distinct $L_1, L_2 \in \mathcal{S}$: $\{L \in \mathcal{S} \mid L \subseteq L_1 + L_2\}$ is spread of the solid $L_1 + L_2$.
- P is called α-point of $\mathrm{STS}_q(7)$ if the derived design in P is a geometric spread.
- S. Thomas 1996: There exists a non-α-point.
- O. Heden, P. Sissokho 2016: For $q = 2$: Each hyperplane contains non-α-point.
- Goal: Investigate Heden-Sissokho result for general q!

- Assume that H is hyperplane containing only α-points.
- Fix a poor solid S in H (not containing any block).
- Let $\mathcal{F} = \{F \in \begin{bmatrix} H \\ 5 \end{bmatrix}_q \mid S \subseteq F\}$.
  We have $\#\mathcal{F} = q + 1$.
- For $F \in \mathcal{F}$, let

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

- Lemma
  - $\mathcal{L}_F$ is a line spread of S.
  - The sets $\mathcal{L}_F$ with $F \in \mathcal{F}$ are pairwise disjoint.

Conclusion

$\mathcal{L} := \biguplus_{F \in \mathcal{F}} \mathcal{L}_F$ is a set of $(q+1)(q^2+1)$ lines in $\mathrm{PG}(3, q)$ 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.)

Lemma

$(\begin{bmatrix} S \\ 1 \end{bmatrix}_q, \mathcal{L})$ is a projective generalized quadrangle of order (q, q).

Classification

Classification of projective generalized quadrangles:
(F. Buekenhout, C. Lefèvre 1974)
$\Longrightarrow$ $(\begin{bmatrix} S \\ 1 \end{bmatrix}_q, \mathcal{L})$ is symplectic generalized quadrangle $W(q)$.

Implication

- 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 (K., submitted)

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

Outline

Automorphisms

- Fundamental theorem of projective geometry:
  For $v \geq 3$, $\mathrm{Aut}(\mathcal{L}(V)) = \mathrm{P\Gamma L}(V)$.
- Let $D \subseteq \mathcal{L}(V)$, define linear automorphism group as

$$\mathrm{Aut}(D) = \{\varphi \in \mathrm{PGL}(V) \mid \varphi(D) = D\}$$

  ($\mathrm{Aut}(D)$ = stabilizer of D in $\mathrm{PGL}(V)$.)

Automorphisms of $\mathrm{STS}_2(7)$

- Goal Investigate possible automorphisms of $\mathrm{STS}_2(7)$.
- Here: $\mathrm{PGL}(V) = \mathrm{GL}(V)$.

Automorphisms of order 3

- Case study: Automorphisms of an $\mathrm{STS}_2(7)$ of order 3.
- Elements of order 3 in $\mathrm{GL}(v, 2)$ are represented by

$$A_{v,f} := \begin{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} & & & \\ & \ddots & & \\ & & \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} & \\ & & & I_f \end{pmatrix}$$

with $f \in \{0, \ldots, v-1\}$, $v - f$ even.

Example

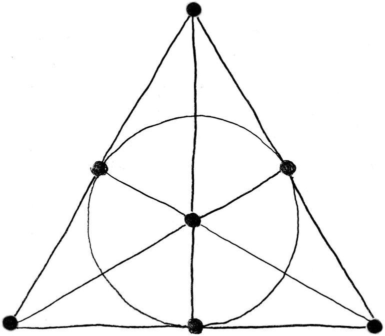
Elements of order 3 in $\mathrm{GL}(7,2)$ up to conjugates:

$$A_{7,1} = \begin{pmatrix} 1 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & 1 & 1 & & & \\ & & 1 & 0 & & & \\ & & & & 1 & 1 & \\ & & & & 1 & 0 & \\ & & & & & & 1 \end{pmatrix} \qquad A_{7,3} = \begin{pmatrix} 1 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & 1 & 1 & & & \\ & & 1 & 0 & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & 1 \end{pmatrix}$$

$$A_{7,5} = \begin{pmatrix} 1 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & 1 & & & & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & 1 \end{pmatrix}$$

Example $(\mathrm{GL}(3,2))$

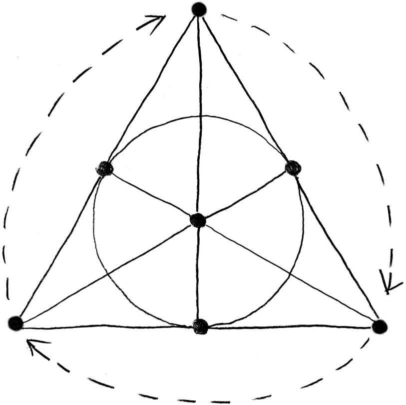
Single element type of order 3: $A_{3,1} = \begin{pmatrix} 1 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}$



- 1 fixed point
- 2 orbits of size 3 falling into:
  - 1 orbit line
  - 1 orbit triangle

Example ($GL(3,2)$)

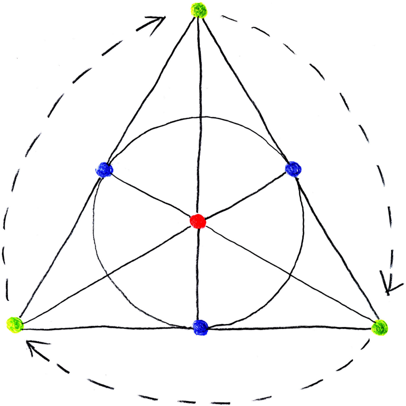
Single element type of order 3: $A_{3,1} = \begin{pmatrix} 1 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}$



- 1 fixed point
- 2 orbits of size 3 falling into:
  - 1 orbit line
  - 1 orbit triangle

Example $(\mathrm{GL}(3,2))$

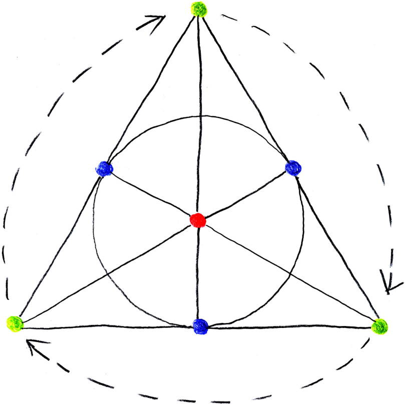
Single element type of order 3: $A_{3,1} = \begin{pmatrix} 1 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}$



- 1 fixed point
- 2 orbits of size 3 falling into:
  - 1 orbit line
  - 1 orbit triangle

Example ($GL(3,2)$)

Single element type of order 3: $A_{3,1} = \begin{pmatrix} 1 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}$



- 1 fixed point
- 2 orbits of size 3 falling into:
  - 1 orbit line
  - 1 orbit triangle

Action of $A_{v,f}$ on the point set $\begin{bmatrix} V \\ 1 \end{bmatrix}_q$

- $2^f - 1$ fixed points
  (points of the form $\langle(0,\ldots,0,*,\ldots,*)\rangle$)
- $\dfrac{2^{v-f}-1}{3}$ orbit lines
  (points of the form $\langle(*,\ldots,*,0,\ldots,0)\rangle$)
- $\dfrac{(2^{v-f}-1)(2^f-1)}{3}$ orbit triangles

Example

v	f	fixed points	orbit triangles	orbit lines
3	1	1	1	1
7	1	1	21	21
7	3	7	35	5
7	5	31	31	1

Fixed planes

- Let $G = \langle A_{v,f} \rangle$
- Let $E \in \begin{bmatrix} V \\ 3 \end{bmatrix}_q$ be a fixed plane (i.e. $E^G = E$)
- Then $G|_E$ is well-defined
- $\#G|_E \in \{1, 3\}$
- $\#G|_E = 1 \implies E$ has 7 fixed points (type 7)
- $\#G|_E = 3 \implies$
  E has 1 fixed point, 1 orbit line and 1 orbit triangle (type 1)

Counting fixed planes

How many fixed planes of type 1 and 7?

- Type 7:
  3-subspaces of the f-dim space of fixed points.
  $\rightsquigarrow \begin{bmatrix} f \\ 3 \end{bmatrix}_2$
- Type 1:
  Uniquely spanned by an orbit triangle.
  $\rightsquigarrow \#\text{orbit triangles} = \dfrac{(2^f - 1)(2^{v-f} - 1)}{3}$

Example

v	f	#f.p.	#o.t. = #T1	#o.l.	#T7
3	1	1	1	1	0
7	1	1	21	21	0
7	3	7	35	5	1
7	5	31	31	1	155

Fixed blocks

- Let D be a G-invariant $\mathrm{STS}_2(v)$.
- $\mathcal{F}_1 :=$ set of fixed blocks of D of type 1
  $\mathcal{F}_7 :=$ set of fixed blocks of D of type 7

Double count $\quad X = \{(L, B) \mid L \text{ orbit line}, B \in \mathcal{F}_1, L < B\}$.

1. $\#X = \#\mathcal{F}_1 \cdot 1$
2.
   - Let L be an orbit line.
   - D Steiner system $\implies \exists$ unique $B \in D$ with $L < B$.
   - For all $g \in G$: $B^g > L^g = L$.
   - Uniqueness of $B \implies B$ is fixed block.
   - B contains orbit line $L \implies B$ of type 1.

   So: $\#X = \#(\text{orbit lines}) \cdot 1$.

$$\implies \quad \#\mathcal{F}_1 = \#\text{orbit lines} = \frac{2^{v-f} - 1}{3}$$

$$\text{Similarly:} \quad \#\mathcal{F}_7 = \frac{(2^f - 1)(2^{f-1} - 1)}{21}$$

Example

v	f	#f.p.	$\#\text{o.l.} = \#\mathcal{F}_1$	$\#\text{o.t.} = \#\text{T1}$	#T7	$\#\mathcal{F}_7$
7	1	1	21	21	0	0
7	3	7	5	35	1	1
7	5	31	1	31	155	$155/7$

Conclusion

- $\#\mathcal{F}_7$ must be integral
  $\Longrightarrow$ The group $\langle A_{7,5} \rangle$ is not possible!
- For $f = 3$, the T7-plane is contained in D.
- For $f = 1$, all 21 T1-planes are contained in D.

Example

v	f	$\#$f.p.	$\#$o.l. $= \#\mathcal{F}_1$	$\#$o.t. $= \#$T1	$\#$T7	$\#\mathcal{F}_7$
7	1	1	21	21	0	0
7	3	7	5	35	1	1
7	5	31	1	31	155	$155/7$

Conclusion

- $\#\mathcal{F}_7$ must be integral
  $\Longrightarrow$ The group $\langle A_{7,5} \rangle$ is not possible!
- For $f = 3$, the T7-plane is contained in D.
- For $f = 1$, all 21 T1-planes are contained in D.

Example

v	f	#f.p.	$\#$o.l. $= \#\mathcal{F}_1$	$\#$o.t. $= \#$T1	$\#$T7	$\#\mathcal{F}_7$
7	1	1	21	21	0	0
7	3	7	5	35	1	1
7	5	31	1	31	155	$155/7$

Conclusion

- $\#\mathcal{F}_7$ must be integral
  $\Longrightarrow$ The group $\langle A_{7,5} \rangle$ is not possible!
- For $f = 3$, the T7-plane is contained in D.
- For $f = 1$, all 21 T1-planes are contained in D.

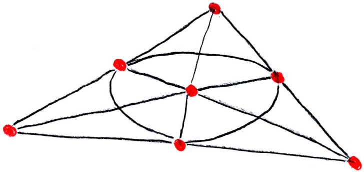
Example

v	f	#f.p.	$\#$o.l. $= \#\mathcal{F}_1$	$\#$o.t. $= \#$T1	$\#$T7	$\#\mathcal{F}_7$
7	1	1	21	21	0	0
7	3	7	5	35	1	1
7	5	31	1	31	155	$155/7$

Conclusion

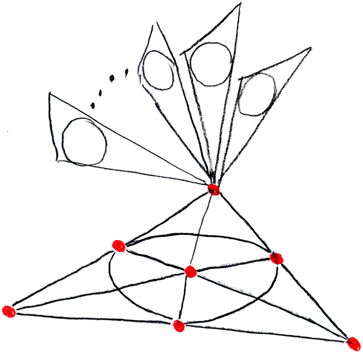
- $\#\mathcal{F}_7$ must be integral
  $\implies$ The group $\langle A_{7,5} \rangle$ is not possible!
- For $f = 3$, the T7-plane is contained in D.
- For $f = 1$, all 21 T1-planes are contained in D.

The case $v = 7$, $f = 3$



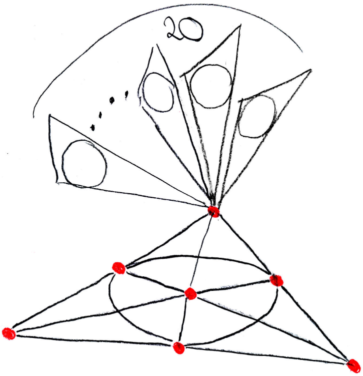
- $\#\mathcal{F}_7 = 1$. Let B be this block and $P \in \begin{bmatrix} B \\ 1 \end{bmatrix}_q$. $\implies$ P fixed.
- Through P: The block B and $\lambda_1 - 1 = 20$ others.
- Orbit lengths 1 or 3 $\implies \geq 2$ fixed blocks among them!
- In total: At least 14 fixed blocks different from B.
- But $\#\mathcal{F}_1 = 5$. Contradiction!

The case $v = 7$, $f = 3$



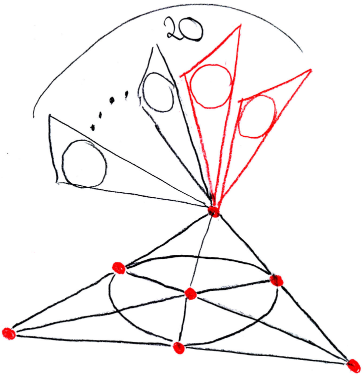
- $\#\mathcal{F}_7 = 1$. Let B be this block and $P \in \begin{bmatrix} B \\ 1 \end{bmatrix}_q$. $\implies$ P fixed.
- Through P: The block B and $\lambda_1 - 1 = 20$ others.
- Orbit lengths 1 or 3 $\implies \geq 2$ fixed blocks among them!
- In total: At least 14 fixed blocks different from B.
- But $\#\mathcal{F}_1 = 5$. Contradiction!

The case $v = 7$, $f = 3$



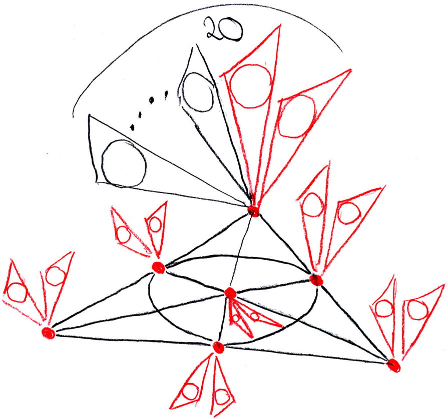
- $\#\mathcal{F}_7 = 1$. Let B be this block and $P \in \begin{bmatrix} B \\ 1 \end{bmatrix}_q$. $\implies$ P fixed.
- Through P: The block B and $\lambda_1 - 1 = 20$ others.
- Orbit lengths 1 or 3 $\implies \geq 2$ fixed blocks among them!
- In total: At least 14 fixed blocks different from B.
- But $\#\mathcal{F}_1 = 5$. Contradiction!

The case $v = 7$, $f = 3$



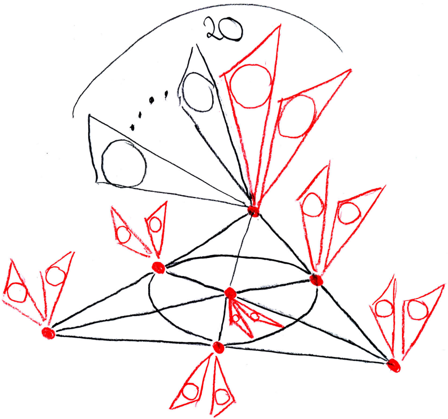
- $\#\mathcal{F}_7 = 1$. Let B be this block and $P \in \begin{bmatrix} B \\ 1 \end{bmatrix}_q$. $\implies$ P fixed.
- Through P: The block B and $\lambda_1 - 1 = 20$ others.
- Orbit lengths 1 or 3 $\implies \geq 2$ fixed blocks among them!
- In total: At least 14 fixed blocks different from B.
- But $\#\mathcal{F}_1 = 5$. Contradiction!

The case $v = 7$, $f = 3$



- $\#\mathcal{F}_7 = 1$. Let B be this block and $P \in \begin{bmatrix} B \\ 1 \end{bmatrix}_q$. $\implies$ P fixed.
- Through P: The block B and $\lambda_1 - 1 = 20$ others.
- Orbit lengths 1 or 3 $\implies \geq 2$ fixed blocks among them!
- In total: At least 14 fixed blocks different from B.
- But $\#\mathcal{F}_1 = 5$. Contradiction!

The case $v = 7$, $f = 3$



- $\#\mathcal{F}_7 = 1$. Let B be this block and $P \in \begin{bmatrix} B \\ 1 \end{bmatrix}_q$. $\implies$ P fixed.
- Through P: The block B and $\lambda_1 - 1 = 20$ others.
- Orbit lengths 1 or 3 $\implies \geq 2$ fixed blocks among them!
- In total: At least 14 fixed blocks different from B.
- But $\#\mathcal{F}_1 = 5$. Contradiction!

The case $v = 7$, $f = 1$

- We didn't find a theoretic argument to exclude $G = \langle A_{7,1} \rangle$.
- We know: D contains the set $\mathcal{S}$ of 21 T1-blocks.
  They all pass through $P = \langle (0, 0, 0, 0, 0, 0, 1) \rangle$.
  In $V/P \cong \mathrm{PG}(5, 2)$, they form a Desarguesian line spread.
- Problem: Out of 3720 orbits of length 3, select 120 such that together with $\mathcal{S}$, they form an $\mathrm{STS}_2(7)$.
  Huge search space!
- Normalizer $N(G)$ of order 362880 acts on the search space.
- Orderly generation (wrt $N(G)$) to reduce the number of cases.
- Parallel computation on the Bayreuth Linux cluster.
- Finally: There is no G-invariant $\mathrm{STS}_2(7)$.

Theorem (Braun, K., Nakič 2016 and K., Kurz, Wassermann 2018)

The automorphism group of a binary q-analog of the Fano plane is

- *trivial or*
- *of order* 2 *and conjugate to*

$$\left\langle \begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & 0 & 1 & & & \\ & & 1 & 0 & & & \\ & & & & 0 & 1 & \\ & & & & 1 & 0 & \\ & & & & & & 1 \end{pmatrix} \right\rangle .$$

Implications of our results on the existence of a $\mathsf{STS}_2(7)$

- Won't be very symmetric.
- Many "natural" approaches for the construction won't work.
- Still: Vast part of the search space remains untouched.
- Further theoretical insight is needed
  to reduce the complexity to a computationally feasible level.
- Problem is still wide open!

Things I didn't talk about

- rank metric codes, MRD codes, lifted MRD codes
  + connections to finite semifields, translation planes . . .
- mixed dimension subspace codes
- vector space partitions
- and others

Thank you!

Slides can be found at
`https://mathe2.uni-bayreuth.de/michaelk/`