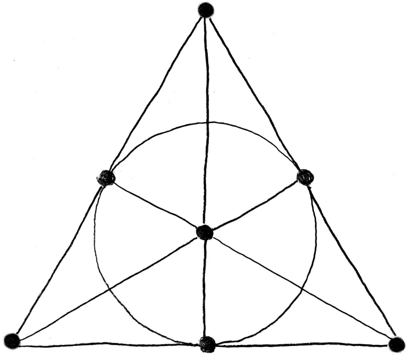
On q-analogs of the Fano plane

Michael Kiermaier

Institut für Mathematik
Universität Bayreuth

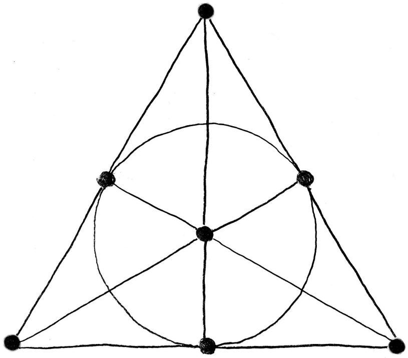
Network Coding and Designs
April 4, 2016
Dubrovnik, Hrvatska

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

Outline

Subset lattice

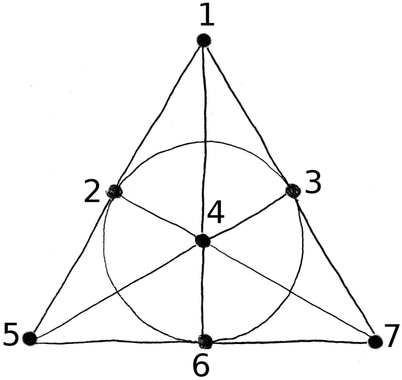
- Let V be a v-element set.
- $\binom{V}{k} :=$ Set of all k-subsets of V.
- $\#\binom{V}{k} = \binom{v}{k}$.
- Subsets of V form a distributive lattice (wrt. $\subseteq$).

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)

Example



$$
\begin{aligned}
V &= \{1,2,3,4,5,6,7\} \\
D &= \{\{1,2,5\},\{1,4,6\},\{1,3,7\},\{2,3,6\}, \\
&\qquad \{2,4,7\},\{3,4,5\},\{5,6,7\}\}
\end{aligned}
$$

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

Lemma

Let D be a t-(v, k, λ) design and $i \in \{0, \ldots, t\}$.
Then D is also an i-(v, k, λ_i) design with

$$\lambda_i = \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}} \cdot \lambda.$$

In particular, $\#D = \lambda_0$.

Example

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

$$\lambda_2 = 1, \quad \lambda_1 = 3, \quad \lambda_0 = 7$$

Corollary: Integrality conditions

If a t-(v, k, λ) design exists, then

$$\lambda_0, \lambda_1, \ldots, \lambda_t \in \mathbb{Z} \qquad \text{(Parameters are admissible)}$$

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 $\begin{bmatrix} V \\ k \end{bmatrix}_q :=$ Set of all k-dim. subspaces of V.
- Gaussian Binomial coefficient

$$\#\begin{bmatrix} V \\ k \end{bmatrix}_q = \begin{bmatrix} v \\ k \end{bmatrix}_q = \frac{(q^v - 1)(q^{v-1} - 1) \cdot \ldots \cdot (q^{v-k+1} - 1)}{(q-1)(q^2-1) \cdot \ldots \cdot (q^k - 1)}$$

- Subspaces of V form a modular lattice (wrt. $\subseteq$).
- Subspace lattice of V = projective geometry $\mathrm{PG}(v-1, q)$
  - 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 $\begin{bmatrix} V \\ v-1 \end{bmatrix}_q$ are hyperplanes.
- Fano plane is the projective geometry $\mathrm{PG}(2, 2)$.

q-analogs in combinatorics

Replace subset lattice by subspace lattice!

orig.	q-analog
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
$\cap$	$\cap$
$\cup$	$+$

- The subset lattice corresponds to $q = 1$.
- Sometimes: Unary field $\mathbb{F}_1$.

Definition (block design)

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.

Lemma

Let D be a t-$(v, k, \lambda)_q$ design and $i \in \{0, \ldots, t\}$.
Then D is also an i-$(v, k, \lambda_i)_q$ design with

$$\lambda_i = \frac{\begin{bmatrix} v-i \\ t-i \end{bmatrix}_q}{\begin{bmatrix} k-i \\ t-i \end{bmatrix}_q} \cdot \lambda.$$

In particular, $\#D = \lambda_0$.

Corollary: Integrality conditions

If a t-$(v, k, \lambda)_q$ design exists, then

$$\lambda_0, \lambda_1, \ldots, \lambda_t \in \mathbb{Z} \qquad \text{(Parameters are admissible)}$$

Lemma

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

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

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

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

Focus on binary q-analog of the Fano plane $\mathrm{STS}_2(7)$.

$$\lambda_2 = 1, \quad \lambda_1 = 21, \quad \lambda_0 = 381$$

- $\mathrm{STS}_2(7)$ consists of $\lambda_0 = 381$ blocks (out of $\begin{bmatrix}7\\3\end{bmatrix}_2 = 11811$ planes).
- Huge search space ($\binom{11811}{381}$ has 730 digits).

Need additional properties!

- Through each point P there are $\lambda_1 = 21$ blocks.
  Image in $V/P \cong \mathrm{PG}(5,2)$ is a line spread.
  Mateva, Topalova 2009: $\exists$ 131044 types of spreads.
  Problem still way too big.
- More refined information by intersection numbers (joint work with Mario Pavčević.)

Outline

Definition

- In the following: D a t-$(v, k, \lambda)_q$ design, S a subspace of V, $s = \dim(S)$
- The i-th intersection number of S in D is

$$\alpha_i = \alpha_i(S) = \#\{B \in D \mid \dim(B \cap S) = i\}.$$

- The intersection vector of S in D is

$$(\alpha_0(S), \alpha_1(S), \ldots, \alpha_k(S))$$

Theorem (q-analog of Mendelsohn equations 1971)

For $i \in \{0, \dots, t\}$

$$\sum_{j=i}^{s} \begin{bmatrix} j \\ i \end{bmatrix}_q \alpha_j = \begin{bmatrix} s \\ i \end{bmatrix}_q \lambda_i$$

(Linear system of equations for the intersection vector)

Proof.

Double count

$$X = \left\{ (I, B) \in \begin{bmatrix} V \\ i \end{bmatrix}_q \times D \mid I \leq B \cap S \right\}$$

- $\begin{bmatrix} s \\ i \end{bmatrix}_q$ possibilities for I.
  For each I, λ_i blocks B with $I \leq B$.
  $\implies \#X = \begin{bmatrix} s \\ i \end{bmatrix}_q \lambda_i$.
- For fixed block B, there are $\begin{bmatrix} \dim(B \cap S) \\ i \end{bmatrix}_q$ suitable I.
  $\implies \#X = \sum_{j=i}^{s} \begin{bmatrix} j \\ i \end{bmatrix}_q \alpha_j$.

Theorem (q-analog of Köhler equations 1988)

For $i \in \{0, \ldots, t\}$

$$\alpha_i = \begin{bmatrix} s \\ i \end{bmatrix}_q \sum_{j=i}^{t} (-1)^{j-i} q^{\binom{j-i}{2}} \begin{bmatrix} s-i \\ j-i \end{bmatrix}_q \lambda_j$$
$$+ (-1)^{t+1-i} q^{\binom{t+1-i}{2}} \sum_{j=t+1}^{s} \begin{bmatrix} j \\ i \end{bmatrix}_q \begin{bmatrix} j-i-1 \\ t-i \end{bmatrix}_q \alpha_j.$$

(Parameterization of $\alpha_0, \alpha_1 \ldots, \alpha_t$ by $\alpha_{t+1}, \alpha_{t+2}, \ldots, \alpha_k$)

History

- For classical designs by Köhler in 1988, long and complicated induction proof.
- Simpler proof by de Vroedt in 1991.
- Can be simplified further!
  Idea: Apply Gauss reduction to the Mendelsohn equations.
  Works in the q-analog situation, too.

Corollary

Intersection vector is uniquely determined for $\dim(S) \leq t$ and $\dim(S) \geq v - t$.

Example

Köhler equations for $\mathrm{STS}_2(7)$ with $s = 4$.

$$\alpha_0 = 136 - 8\alpha_3$$
$$\alpha_1 = 210 + 14\alpha_3$$
$$\alpha_2 = 35 - 7\alpha_3$$

$\alpha_3 \in \{0, 1\}$, since otherwise

- S contains two blocks B_1, B_2.
- By the dimension formula, $\dim(B_1 \cap B_2) \geq 2$. Contradiction.

$\Longrightarrow$ Two possible intersection vectors:

$$(136, 210, 35, 0) \quad \text{and} \quad (128, 224, 28, 1)$$

Example (cont.)

- Distribution of the 4-dim subspaces S to the two intersection numbers? (total: $\begin{bmatrix}7\\4\end{bmatrix}_2 = 11811$ subspaces S)
- Double counting:
  $(136, 210, 35, 0)$ occurs 6096 times,
  $(128, 224, 28, 1)$ occurs 5715 times.

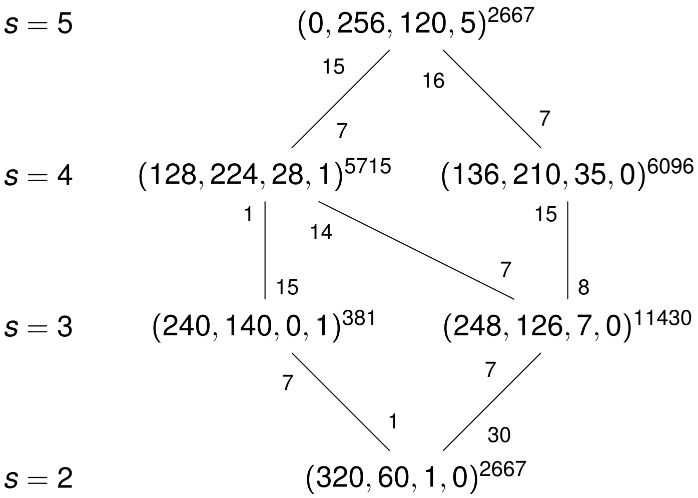
- Similarly, compute the intersection vectors for all possible values of s.

s	intersection vector	frequency
7	$(0, 0, 0, 381)$	1
6	$(0, 0, 336, 45)$	127
5	$(0, 256, 120, 5)$	2667
4	$(128, 224, 28, 1)$	5715
4	$(136, 210, 35, 0)$	6096
3	$(240, 140, 0, 1)$	381
3	$(248, 126, 7, 0)$	11430
2	$(320, 60, 1, 0)$	2667
1	$(360, 21, 0, 0)$	127
0	$(381, 0, 0, 0)$	1

- How do the different S relate to each other?

Theorem (K., Pavčević 2015)

The "intersection structure" of a 2-analog of the Fano plane is



Outline

Block designs and their q-analogs

Intersection numbers

Prescribed automorphisms

Subspace codes

Fundamental theorem of projective geometry

For $v \geq 3$, the automorphism group of the subspace lattice of V is $\mathrm{P\Gamma L}(v, q)$.

For $q = 2$, simply $\mathrm{P\Gamma L}(v, 2) = \mathrm{GL}(v, 2)$.

Idea

- Pick some subgroup $G < \mathrm{GL}(7, 2)$.
- Focus on G-invariant q-analogs of the Fano plane.
  $\rightsquigarrow$ problem gets much smaller.
- If lucky: Find one!
- Otherwise: Systematically narrow down the possible automorphism groups.

Observation

- Conjugate subgroups G yield isomorphic designs.
- $\implies$ Only the conjugation type of G matters.

Theorem (Braun, K., Nakić 2016)

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

- 1 *or*
- 2 *(1 remaining type) or*
- 3 *(2 remaining types) or*
- 4 *(1 remaining type)*

Progress

(joint work with Sascha Kurz and Alfred Wassermann)

- Parallel computing: Order 4 not possible.
- Theory and parallel computing: Order 3 not possible.

Theorem (Braun, K., Nakić 2016)

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

- 1 *or*
- 2 *(1 remaining type) or*
- 3 *(2 remaining types) or*
- 4 *(1 remaining type)*

Progress

(joint work with Sascha Kurz and Alfred Wassermann)

- Parallel computing: Order 4 not possible.
- Theory and parallel computing: Order 3 not possible.

Theorem (Braun, K., Nakić 2016)

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

- 1 *or*
- 2 *(1 remaining type) or*
- 3 *(2 remaining types) or*
- ~~4 *(1 remaining type)*~~

Progress

(joint work with Sascha Kurz and Alfred Wassermann)

- Parallel computing: Order 4 not possible.
- Theory and parallel computing: Order 3 not possible.

Theorem (Braun, K., Nakić 2016)

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

- 1 *or*
- 2 *(1 remaining type) or*
- ~~3 *(2 remaining types*~~*) or*
- ~~4 *(1 remaining type)*~~

Progress

(joint work with Sascha Kurz and Alfred Wassermann)

- Parallel computing: Order 4 not possible.
- Theory and parallel computing: Order 3 not possible.

Lemma

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.*

Proof.

Let $A \in \mathrm{GL}(v, 2)$ of order 3.

$\implies A^3 = I_v$.

$\implies m_A \mid X^3 - 1 = (X^2 + X + 1)(X - 1)$.

Enumerate the possible rational normal forms. $\square$

Example

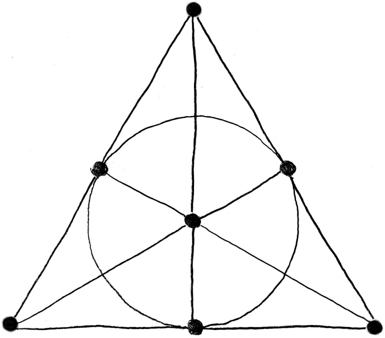
Types of elements of order 3 in $\mathrm{GL}(7,2)$:

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

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

Example (GL(3, 2))

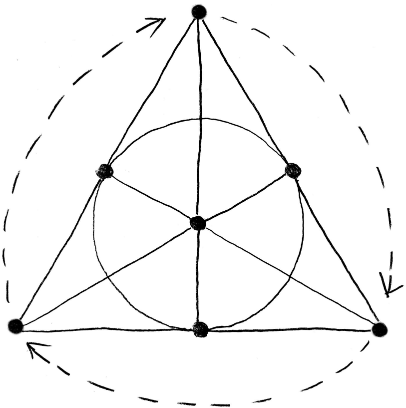
Single element type of order 3: $\quad A_{3,1} = \begin{pmatrix} 1 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}$



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

Example (GL(3, 2))

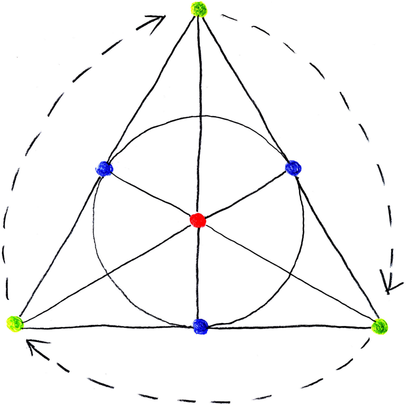
Single element type of order 3: $A_{3,1} = \begin{pmatrix} 1 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}$



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

Example (GL(3, 2))

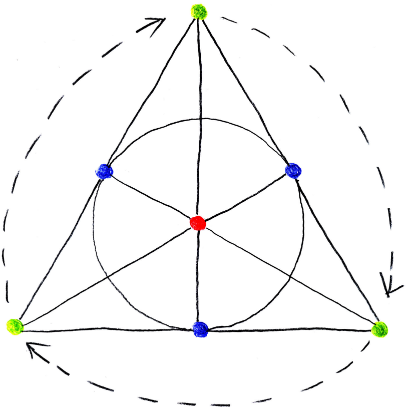
Single element type of order 3: $A_{3,1} = \begin{pmatrix} 1 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}$



- 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.
  $\rightsquigarrow$ $\#$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.	$\#$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.

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.

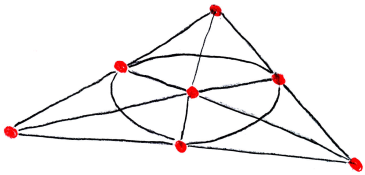
Example

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

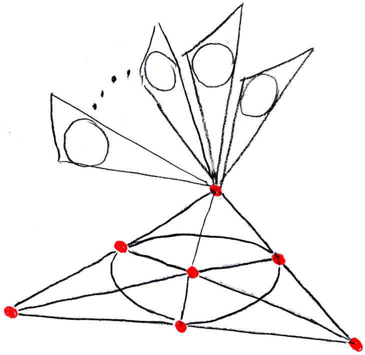
- $\#\mathcal{F}_7$ must be integral
  $\Longrightarrow$ The group $\langle A_{7,5} \rangle$ is not possible!
- For $f = 3$, the T7-plane is contained in D.
- For $f = 1$, all 21 T1-planes are contained in D.

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



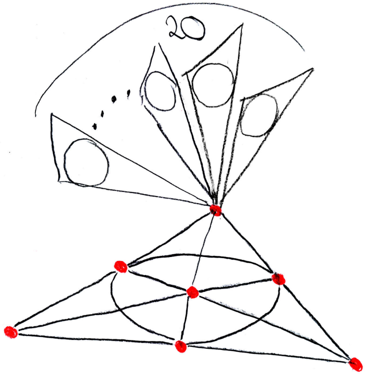
- $\#\mathcal{F}_7 = 1$
- $\lambda_1 = 21$
- Orbit lengths 1 or 3 $\implies$ at least 2 fixed blocks!
- In total: At least 14 fixed blocks.
- But $\#\mathcal{F}_1 = 5$. Contradiction!

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



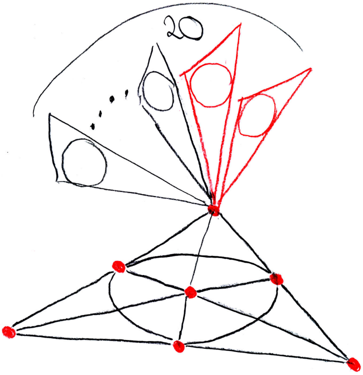
- $\#\mathcal{F}_7 = 1$
- $\lambda_1 = 21$
- Orbit lengths 1 or 3 $\implies$ at least 2 fixed blocks!
- In total: At least 14 fixed blocks.
- But $\#\mathcal{F}_1 = 5$. Contradiction!

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



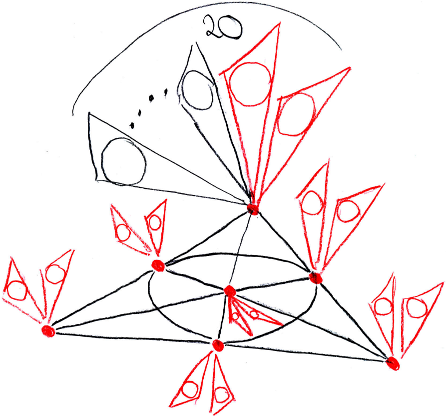
- $\#\mathcal{F}_7 = 1$
- $\lambda_1 = 21$
- Orbit lengths 1 or 3 $\implies$ at least 2 fixed blocks!
- In total: At least 14 fixed blocks.
- But $\#\mathcal{F}_1 = 5$. Contradiction!

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



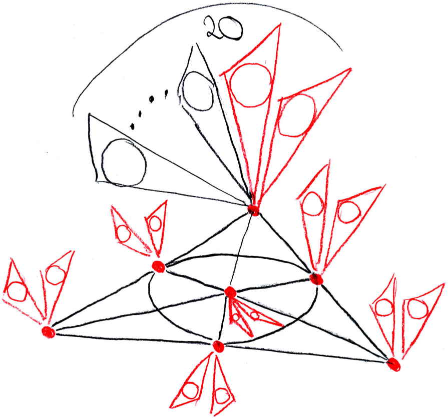
- $\#\mathcal{F}_7 = 1$
- $\lambda_1 = 21$
- Orbit lengths 1 or 3 $\implies$ at least 2 fixed blocks!
- In total: At least 14 fixed blocks.
- But $\#\mathcal{F}_1 = 5$. Contradiction!

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



- $\#\mathcal{F}_7 = 1$
- $\lambda_1 = 21$
- Orbit lengths 1 or 3 $\implies$ at least 2 fixed blocks!
- In total: At least 14 fixed blocks.
- But $\#\mathcal{F}_1 = 5$. Contradiction!

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



- $\#\mathcal{F}_7 = 1$
- $\lambda_1 = 21$
- Orbit lengths 1 or 3 $\implies$ at least 2 fixed blocks!
- In total: At least 14 fixed blocks.
- 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 (K., Kurz, Wassermann)

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 on the existence of a $STS_2(7)$

- 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!

Outline

Definition (Steiner system)

$D \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$ is a t-$(v, k, 1)_q$ Steiner system

if each $T \in \begin{bmatrix} V \\ t \end{bmatrix}_q$ is contained in exactly one element of D.

Definition ((constant dimension) subspace code)

$C \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$ is a $(v, 2(k - t + 1); k)_q$ subspace code

if each $T \in \begin{bmatrix} V \\ t \end{bmatrix}_q$ is contained in at most one element of C.

- q-Fano setting: $(7, 4; 3)_q$ subspace code C.
- For $q = 2$:
  - $\#C \leq 381$
  - $\#C = 381 \iff C$ is a $\mathrm{STS}_2(7)$
- Find maximum size $A_q(7, 4; 3)$ of $(7, 4; 3)_q$ subspace code!

History

- Silberstein 2008: $A_2(7,4;3) \geq 289$
  Based on lifted rank metric codes.
- Vardy 2008: $A_2(7,4;3) \geq 294$
- Kohnert, Kurz 2008: $A_2(7,4;3) \geq 304$
  Prescribe group of order 21
- Braun, Reichelt 2012: $A_2(7,4;3) \geq 329$
  Prescribe group of order 15, modify large solutions.
- Liu, Honold 2014; Honold, K. 2015:
  explicit construction of $\#C = 329$
  expurgation and augmentation of the lifted Gabidulin code

  Also: $A_3(7,4;3) \geq 6977$ for $q = 3$
  ($\mathrm{STS}_3(7)$ would have size 7651.)

Recent approach

joint work with Daniel Heinlein, Sascha Kurz and Alfred Wassermann.

- Systematically check $G < \mathrm{GL}(7,2)$ for admitting large G-invariant codes.
- Found $\#G = 64$ admitting $\#C = 319$.
- ... having a subgroup of order 32 admitting $\#C = 327$.
- ... having a subgroup of order 16 admitting $\#C = 329$.
- ... having a subgroup of order 4 admitting

$$\#C = 333.$$

- Code provided at subspacecodes.uni-bayreuth.de

Thank you!