2-arcs of maximal size in projective and affine Hjelmslev planes over $\mathbb{Z}_{25}$

Michael Kiermaier

Institut für Mathematik
Universität Bayreuth

ALCOMA 2010, Thurnau

joint work with Matthias Koch, Sascha Kurz
supported by DFG grant WA 1666/4-1

Outline

1. Introduction
2. Computations
   - Approach 1: Via factor plane
   - Approach 2: Via affine subplane
3. Conclusion

Definition of a *2-arc*

Given

- Some geometry $\mathfrak{G}$
  (consisting of points, lines, incidence relation).
- $\mathfrak{k}$ a set of points in $\mathfrak{G}$.

Definition

- $\mathfrak{k}$ is a 2-arc, if
  $\#(L \cap \mathfrak{k}) \leq 2$ for each line L in $\mathfrak{G}$.
- Maximum possible size of a 2-arc: $n_2(\mathfrak{G})$.

Goal

For interesting finite geometries $\mathfrak{G}$, determine $n_2(\mathfrak{G})$.

Definition of a *2-arc*

Given

- Some geometry $\mathfrak{G}$
  (consisting of points, lines, incidence relation).
- $\mathfrak{k}$ a set of points in $\mathfrak{G}$.

Definition

- $\mathfrak{k}$ is a 2-arc, if
  $\#(L \cap \mathfrak{k}) \leq 2$ for each line L in $\mathfrak{G}$.
- Maximum possible size of a 2-arc: $n_2(\mathfrak{G})$.

Goal

For interesting finite geometries $\mathfrak{G}$, determine $n_2(\mathfrak{G})$.

Recall

Projective plane $\mathrm{PG}(2, \mathbb{F}_q)$ over the finite field $\mathbb{F}_q$:

- Points: one-dimensional linear subspaces of $\mathbb{F}_q^3$.
- Lines: two-dimensional linear subspaces of $\mathbb{F}_q^3$.
- Incidence given by subset relation.

Ovals and hyperovals

- If q odd: $n_2(\mathrm{PG}(2, \mathbb{F}_q)) = q + 1$, such arcs are called ovals.
- If q even: $n_2(\mathrm{PG}(2, \mathbb{F}_q)) = q + 2$, such arcs are called hyperovals.

Connection to coding theory

Ovals and hyperovals give MDS-codes.

Recall

Projective plane $\mathrm{PG}(2, \mathbb{F}_q)$ over the finite field $\mathbb{F}_q$:

- Points: one-dimensional linear subspaces of $\mathbb{F}_q^3$.
- Lines: two-dimensional linear subspaces of $\mathbb{F}_q^3$.
- Incidence given by subset relation.

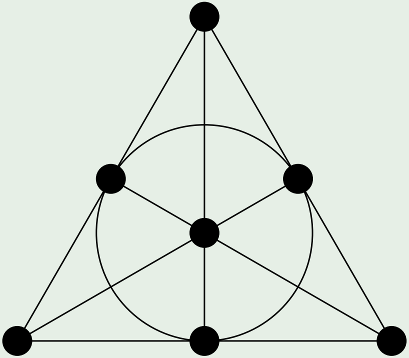
Ovals and hyperovals

- If q odd: $n_2(\mathrm{PG}(2, \mathbb{F}_q)) = q + 1$, such arcs are called ovals.
- If q even: $n_2(\mathrm{PG}(2, \mathbb{F}_q)) = q + 2$, such arcs are called hyperovals.

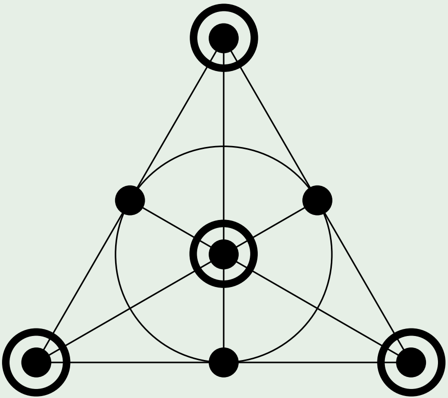
Connection to coding theory

Ovals and hyperovals give MDS-codes.

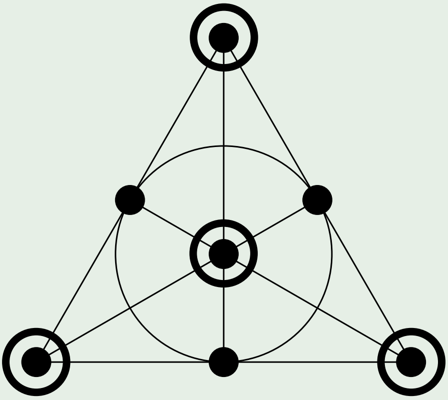
Example (The Fano plane PG$(2, \mathbb{F}_2)$)



Example (The Fano plane PG$(2, \mathbb{F}_2)$)



Example (The Fano plane $\mathrm{PG}(2, \mathbb{F}_2)$)



$$n_2(\mathrm{PG}(2, \mathbb{F}_2)) = 4$$

Characterization of finite fields

A finite field is a finite ring R with exactly 2 left ideals.
Of course: These ideals are $\{0\}$ and R.

Generalization:

Definition

A finite ring R with exactly 3 left ideals is called
finite chain ring of composition length 2 (CR2).

Example

$\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$, left-ideals are $\{0\}$, $\{0, 2\}$ and $\{0, 1, 2, 3\}$.

Properties of CR2-rings

- Left-ideals: $\{0\} \lneq N \lneq R$
- $N = \mathrm{rad}(R)$, so N both-sided ideal and $R/N \cong \mathbb{F}_q$.

Characterization of finite fields

A finite field is a finite ring R with exactly 2 left ideals.
Of course: These ideals are $\{0\}$ and R.

Generalization:

Definition

A finite ring R with exactly 3 left ideals is called
finite chain ring of composition length 2 (CR2).

Example

$\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$, left-ideals are $\{0\}$, $\{0,2\}$ and $\{0,1,2,3\}$.

Properties of CR2-rings

- Left-ideals: $\{0\} \lneq N \lneq R$
- $N = \mathrm{rad}(R)$, so N both-sided ideal and $R/N \cong \mathbb{F}_q$.

Characterization of finite fields

A finite field is a finite ring R with exactly 2 left ideals.
Of course: These ideals are $\{0\}$ and R.

Generalization:

Definition

A finite ring R with exactly 3 left ideals is called
finite chain ring of composition length 2 (CR2).

Example

$\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$, left-ideals are $\{0\}$, $\{0, 2\}$ and $\{0, 1, 2, 3\}$.

Properties of CR2-rings

- Left-ideals: $\{0\} \lneq N \lneq R$
- $N = \mathrm{rad}(R)$, so N both-sided ideal and $R/N \cong \mathbb{F}_q$.

Theorem

Let R be a CR2-ring, $N = \operatorname{rad}(R)$ with $R/N \cong \mathbb{F}_q$ and $q = p^r$, p prime. Then $\#R = q^2$ and either

- $\operatorname{char}(R) = p^2$ *and* $R \cong \operatorname{GR}(q^2, p^2)$
  (Galois ring of order q^2 and characteristic p^2)
  or
- $\operatorname{char}(R) = p$ *and there is a unique* $\sigma \in \operatorname{Aut}(\mathbb{F}_q)$ *s.t.*
  $R \cong \mathbb{F}_q[X, \sigma]/(X^2)$
  (σ-duals over $\mathbb{F}_q$)

Smallest CR2-rings

q	R		
	Galois ring	σ-duals over $\mathbb{F}_q$	
2	$\mathbb{Z}_4$	$\mathbb{F}_2[X]/(X^2)$	
3	$\mathbb{Z}_9$	$\mathbb{F}_3[X]/(X^2)$	
4	$\mathrm{GR}(16, 4)$	$\mathbb{F}_4[X]/(X^2)$	$\mathbb{F}_4[X, a \mapsto a^2]/(X^2)$
5	$\mathbb{Z}_{25}$	$\mathbb{F}_5[X]/(X^2)$	

Abbreviations

- $\mathbb{G}_4 := \mathrm{GR}(16, 4)$
- $\mathbb{S}_q := \mathbb{F}_q[X]/(X^2)$
- $\mathbb{T}_4 := \mathbb{F}_4[X, a \mapsto a^2]/(X^2)$ (non-commutative!)

Definition

Let R be a CR2-ring. Projective Hjelmslev plane $\mathrm{PHG}(2, R)$ over R:

- Points: Free submodules of R_R^3 of rank 1.
- Lines: Free submodules of R_R^3 of rank 2.
- Incidence given by subset relation.

Two different lines may meet in more than one point!

Goal

Find $n_2(R) := n_2(PHG(2, R))$ for CR2-rings R.

Definition

Let R be a CR2-ring. Projective Hjelmslev plane $\mathrm{PHG}(2, R)$ over R:

- Points: Free submodules of R_R^3 of rank 1.
- Lines: Free submodules of R_R^3 of rank 2.
- Incidence given by subset relation.

Two different lines may meet in more than one point!

Goal

Find $n_2(R) := n_2(PHG(2, R))$ for CR2-rings R.

Definition

Let R be a CR2-ring. Projective Hjelmslev plane $\mathrm{PHG}(2, R)$ over R:

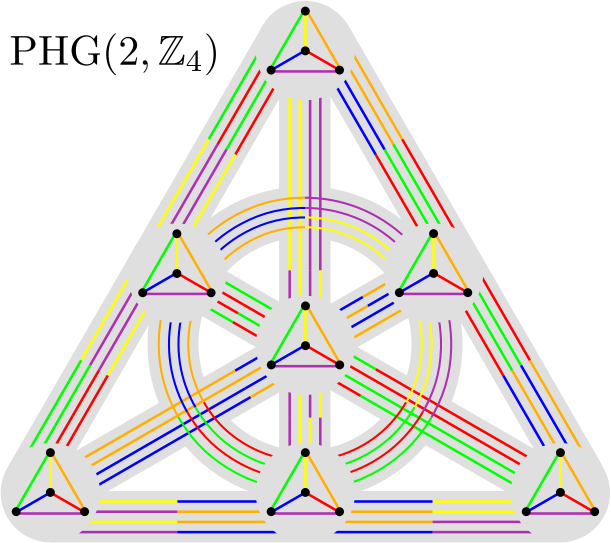
- Points: Free submodules of R_R^3 of rank 1.
- Lines: Free submodules of R_R^3 of rank 2.
- Incidence given by subset relation.

Two different lines may meet in more than one point!

Goal

Find $n_2(R) := n_2(PHG(2, R))$ for CR2-rings R.

$\mathrm{PHG}(2, \mathbb{Z}_4)$



Previous results (Thomas Honold, Ivan Landjev, M.K.)

$n_2(R)$		R: Galois ring	R: σ-duals
q	even	q^2+q+1	$q^2+2 \leq \cdot \leq q^2+q$
	odd	$\cdot \leq q^2$	q^2

Previous results for small q

q	2		3		4			5	
R	$\mathbb{Z}_4$	$\mathbb{S}_2$	$\mathbb{Z}_9$	$\mathbb{S}_3$	$\mathbb{G}_4$	$\mathbb{S}_4$	$\mathbb{T}_4$	$\mathbb{Z}_{25}$	$\mathbb{S}_5$
$n_2(R)$	7	6	**9**	9	21	**18**	**18**	**21** $-$ **25**	25

Aim

Computationally attack smallest open case $R = \mathbb{Z}_{25}$!

Previous results (Thomas Honold, Ivan Landjev, M.K.)

$n_2(R)$		R	
		Galois ring	σ-duals
q	even	q^2+q+1	$q^2+2 \leq \cdot \leq q^2+q$
	odd	$\cdot \leq q^2$	q^2

Previous results for small q

q	2		3		4			5	
R	$\mathbb{Z}_4$	$\mathbb{S}_2$	$\mathbb{Z}_9$	$\mathbb{S}_3$	$\mathbb{G}_4$	$\mathbb{S}_4$	$\mathbb{T}_4$	$\mathbb{Z}_{25}$	$\mathbb{S}_5$
$n_2(R)$	7	6	**9**	9	21	**18**	**18**	**21** – **25**	25

Aim

Computationally attack smallest open case $R = \mathbb{Z}_{25}$!

Previous results (Thomas Honold, Ivan Landjev, M.K.)

$n_2(R)$		R	
		Galois ring	σ-duals
q	even	q^2+q+1	$q^2+2 \leq \cdot \leq q^2+q$
	odd	$\cdot \leq q^2$	q^2

Previous results for small q

q	2		3		4			5	
R	$\mathbb{Z}_4$	$\mathbb{S}_2$	$\mathbb{Z}_9$	$\mathbb{S}_3$	$\mathbb{G}_4$	$\mathbb{S}_4$	$\mathbb{T}_4$	$\mathbb{Z}_{25}$	$\mathbb{S}_5$
$n_2(R)$	7	6	**9**	9	21	**18**	**18**	**21** – **25**	25

Aim

Computationally attack smallest open case $R = \mathbb{Z}_{25}$!

Size of problem

- Number of points in $\mathrm{PHG}(2, \mathbb{Z}_{25})$ is 775.

$$\binom{775}{22} = 24166244646934786007388621053037746466588 00.$$

Huge search space!

- Collineation group $\mathrm{PGL}(3, \mathbb{Z}_{25})$ has size 145312500000.

Conclusion

Advanced search methods are needed.

Size of problem

- Number of points in $\mathrm{PHG}(2, \mathbb{Z}_{25})$ is 775.

$$\binom{775}{22} = 24166244646934786007388621053037746466658800.$$

  Huge search space!

- Collineation group $\mathrm{PGL}(3, \mathbb{Z}_{25})$ has size 145312500000.

Conclusion

Advanced search methods are needed.

Size of problem

- Number of points in $\mathrm{PHG}(2, \mathbb{Z}_{25})$ is 775.

$$\binom{775}{22} =$$
$$24166244646934786007388621053037746466588 00.$$

Huge search space!

- Collineation group $\mathrm{PGL}(3, \mathbb{Z}_{25})$ has size 145312500000.

Conclusion

Advanced search methods are needed.

Homomorphisms

- Ring homomorphism

$$\phi : \mathbb{Z}_{25} \to \mathbb{F}_5, \quad a \mapsto a \pmod 5$$

  extends to
  $\phi : \mathrm{PHG}(2, \mathbb{Z}_{25}) \to \mathrm{PG}(2, \mathbb{F}_5)$ (collineation) and
  $\phi : \mathrm{PGL}(3, \mathbb{Z}_{25}) \to \mathrm{PGL}(3, \mathbb{F}_5)$ (group homomorphism).
- Together: ϕ is homomorphism of group actions!

Idea

First do computations in $\mathrm{PG}(2, \mathbb{F}_5)$,
then compute preimages under ϕ.

Homomorphisms

- Ring homomorphism

$$\phi : \mathbb{Z}_{25} \to \mathbb{F}_5, \quad a \mapsto a \pmod 5$$

  extends to
  $\phi : \mathrm{PHG}(2, \mathbb{Z}_{25}) \to \mathrm{PG}(2, \mathbb{F}_5)$ (collineation) and
  $\phi : \mathrm{PGL}(3, \mathbb{Z}_{25}) \to \mathrm{PGL}(3, \mathbb{F}_5)$ (group homomorphism).
- Together: ϕ is homomorphism of group actions!

Idea

First do computations in $\mathrm{PG}(2, \mathbb{F}_5)$,
then compute preimages under ϕ.

Homomorphisms

- Ring homomorphism

$$\phi : \mathbb{Z}_{25} \to \mathbb{F}_5, \quad a \mapsto a \pmod 5$$

  extends to
  $\phi : \mathrm{PHG}(2, \mathbb{Z}_{25}) \to \mathrm{PG}(2, \mathbb{F}_5)$ (collineation) and
  $\phi : \mathrm{PGL}(3, \mathbb{Z}_{25}) \to \mathrm{PGL}(3, \mathbb{F}_5)$ (group homomorphism).
- Together: ϕ is homomorphism of group actions!

Idea

First do computations in $\mathrm{PG}(2, \mathbb{F}_5)$,
then compute preimages under ϕ.

Homomorphism Principle

To compute $\mathrm{PGL}(2, \mathbb{Z}_{25})$-representatives of a $(n, 2)$-arcs in $\mathrm{PHG}(2, \mathbb{Z}_{25})$:

- Step 1:
  Compute set X of $\mathrm{PG}(2, \mathbb{F}_5)$-representatives of possible ϕ-images.
- Step 2:
  For each $x \in X$:
  Compute representatives of $\phi^{-1}(x)$ with respect to action of $\phi^{-1}(\mathrm{PG}(2, \mathbb{F}_5)_x)$ on $\mathrm{PHG}(2, \mathbb{Z}_{25})$.

Remarks

- Step 2 much harder than Step 1.
- Small X will reduce running time of Step 2.
  Find as many restrictions on the ϕ-images as possible!

Homomorphism Principle

To compute $\mathrm{PGL}(2, \mathbb{Z}_{25})$-representatives of a $(n, 2)$-arcs in $\mathrm{PHG}(2, \mathbb{Z}_{25})$:

- Step 1:
  Compute set X of $\mathrm{PG}(2, \mathbb{F}_5)$-representatives of possible ϕ-images.
- Step 2:
  For each $x \in X$:
  Compute representatives of $\phi^{-1}(x)$ with respect to action of $\phi^{-1}(\mathrm{PG}(2, \mathbb{F}_5)_x)$ on $\mathrm{PHG}(2, \mathbb{Z}_{25})$.

Remarks

- Step 2 much harder than Step 1.
- Small X will reduce running time of Step 2.
  Find as many restrictions on the ϕ-images as possible!

Restrictions

- ϕ-image is exactly the distribution of points to the point classes.
- Geometric considerations give very hard restrictions.
- For $(22, 2)$-arcs we get $|X| = 4$, can be done by hand by combinatorial and geometric reasoning.

Implementation

- In C++.
- Further methods: Backtrack search, Ladder game, forbidden substructurs.

Results

- In 8.5 hours: There is no $(22, 2)$-arc.
- In 13.5 hours: The already known $(21, 1)$-arc is unique.

Restrictions

- ϕ-image is exactly the distribution of points to the point classes.
- Geometric considerations give very hard restrictions.
- For $(22, 2)$-arcs we get $|X| = 4$, can be done by hand by combinatorial and geometric reasoning.

Implementation

- In C++.
- Further methods: Backtrack search, Ladder game, forbidden substructurs.

Results

- In 8.5 hours: There is no $(22, 2)$-arc.
- In 13.5 hours: The already known $(21, 1)$-arc is unique.

Restrictions

- ϕ-image is exactly the distribution of points to the point classes.
- Geometric considerations give very hard restrictions.
- For $(22, 2)$-arcs we get $|X| = 4$, can be done by hand by combinatorial and geometric reasoning.

Implementation

- In C++.
- Further methods: Backtrack search, Ladder game, forbidden substructurs.

Results

- In 8.5 hours: There is no $(22, 2)$-arc.
- In 13.5 hours: The already known $(21, 1)$-arc is unique.

Second approach

Computational nonexistence/uniqueness proof:

Delicate matter.

Double-check result by completely independent approach.

Lemma

Let $\mathfrak{K}$ be a 2-arc in $\mathrm{PHG}(2, \mathbb{Z}_{25})$ *intersecting each point class in at most 2 points.*
Then there is a line class containing at most 2 points of $\mathfrak{K}$.

Idea

- Large 2-arcs fulfill requirement of the Lemma.
- So: Removing the line class of the Lemma: $(n, 2)$-arc yields $(\geq n - 2, 2)$-arc in the affine Hjelmslev plane $\mathrm{AHG}(2, \mathbb{Z}_{25})$.
- Classify all $(20, 2)$ and $(19, 2)$-arcs in $\mathrm{AHG}(2, \mathbb{Z}_{25})$. Problem size is reduced, because:
  - $\mathrm{AHG}(2, \mathbb{Z}_{25})$ has 150 points less then $\mathrm{PHG}(2, \mathbb{Z}_{25})$,
  - Arc size is reduced by 2.
- Easy: Check results for extendibility in $\mathrm{PHG}(2, \mathbb{Z}_{25})$.

Lemma

Let $\mathfrak{K}$ be a 2-arc in $\mathrm{PHG}(2, \mathbb{Z}_{25})$ *intersecting each point class in at most 2 points.*
Then there is a line class containing at most 2 points of $\mathfrak{K}$.

Idea

- Large 2-arcs fulfill requirement of the Lemma.
- So: Removing the line class of the Lemma:
  $(n, 2)$-arc yields $(\geq n - 2, 2)$-arc in the affine Hjelmslev plane $\mathrm{AHG}(2, \mathbb{Z}_{25})$.
- Classify all $(20, 2)$ and $(19, 2)$-arcs in $\mathrm{AHG}(2, \mathbb{Z}_{25})$.
  Problem size is reduced, because:
  - $\mathrm{AHG}(2, \mathbb{Z}_{25})$ has 150 points less then $\mathrm{PHG}(2, \mathbb{Z}_{25})$,
  - Arc size is reduced by 2.
- Easy: Check results for extendibility in $\mathrm{PHG}(2, \mathbb{Z}_{25})$.

Implementation

- Fast canonizer.
- Backtrack search combined with orderly generation on the first few levels.
- On leaf nodes of backtrack search:
  Formulate problem as linear program,
  get solutions from CPLEX.

Results

- Exactly the same results as with the first approach.
- Number and isomorphism type of extendible 2-arcs in $\mathrm{AHG}(2, \mathbb{Z}_{25})$
  perfectly match the affine reductions of the known $(21, 2)$-arc.

Implementation

- Fast canonizer.
- Backtrack search combined with orderly generation on the first few levels.
- On leaf nodes of backtrack search:
  Formulate problem as linear program,
  get solutions from CPLEX.

Results

- Exactly the same results as with the first approach.
- Number and isomorphism type of extendible 2-arcs in $\mathrm{AHG}(2, \mathbb{Z}_{25})$
  perfectly match the affine reductions of the known $(21, 2)$-arc.

Updated table

q	2		3		4			5	
R	$\mathbb{Z}_4$	$\mathbb{S}_2$	$\mathbb{Z}_9$	$\mathbb{S}_3$	$\mathbb{G}_4$	$\mathbb{S}_4$	$\mathbb{T}_4$	$\mathbb{Z}_{25}$	$\mathbb{S}_5$
$n_2(R)$	7	6	9	9	21	18	18	**21**	25

Surprise

"Exotic" ring $\mathbb{S}_5$ admits much larger 2-arc than its brother $\mathbb{Z}_{25}$!

Updated table

q	2		3		4			5	
R	$\mathbb{Z}_4$	$\mathbb{S}_2$	$\mathbb{Z}_9$	$\mathbb{S}_3$	$\mathbb{G}_4$	$\mathbb{S}_4$	$\mathbb{T}_4$	$\mathbb{Z}_{25}$	$\mathbb{S}_5$
$n_2(R)$	7	6	9	9	21	18	18	**21**	25

Surprise

"Exotic" ring $\mathbb{S}_5$ admits much larger 2-arc than its brother $\mathbb{Z}_{25}$!

Open questions

- Understand $n_2(\mathbb{Z}_{25}) < 25$ without use of computer.
- Construct the unique $(21, 2)$-arc by hand.
- New smallest open case: $n_2(\mathbb{Z}_{49})$.
- Find reasonable lower bound on $n_2(R)$ for q odd, R Galois ring.
- Holds $n_2(\mathbb{Z}_{q^2}) < q^2$ for all odd $q \geq 5$?