New 2-arcs in projective Hjelmslev planes

Michael Kiermaier

Institut für Mathematik
Universität Bayreuth

Sixth International Workshop on Optimal Codes And Related Topics

Outline

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

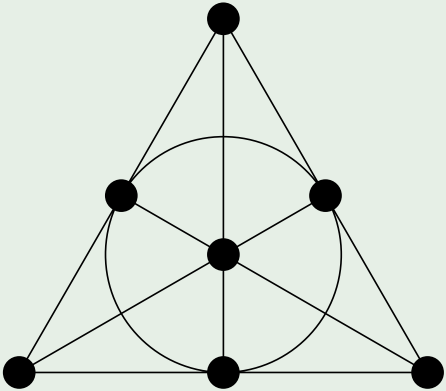
Ovals and hyperovals

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

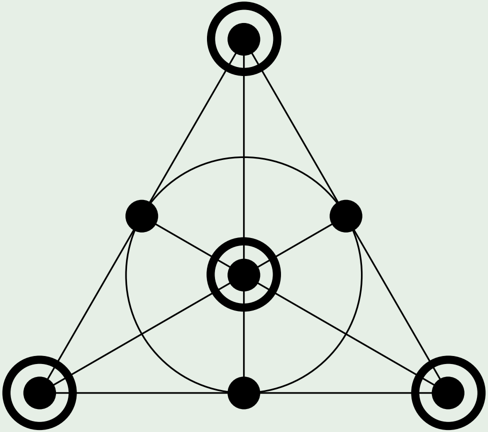
Connection to coding theory

Ovals and hyperovals give MDS-codes.

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



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



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 $R/N \cong \mathbb{F}_q$.

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

Theorem

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

- $\mathrm{char}(R) = p^2$ *and* $R \cong \mathrm{GR}(q^2, p^2)$
  (Galois ring of order q^2 and characteristic p^2)
  or
- $\mathrm{char}(R) = p$ *and there is a unique* $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$ *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.

Previous results (Thomas Honold, Ivan Landjev)

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

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	$20-25$	$18-25$

With Matthias Koch (proceedings): $n_2(\mathbb{Z}_{25}) \geq 21$, $n_2(\mathbb{S}_5) \geq 22$.
Shortly later, different search method: $n_2(\mathbb{S}_5) = 25$.

Previous results (Thomas Honold, Ivan Landjev)

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

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	$20-25$	$18-25$

With Matthias Koch (proceedings): $n_2(\mathbb{Z}_{25}) \geq 21$, $n_2(\mathbb{S}_5) \geq 22$.
Shortly later, different search method: $n_2(\mathbb{S}_5) = 25$.

Previous results (Thomas Honold, Ivan Landjev)

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

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	$21-25$	$22-25$

With Matthias Koch (proceedings): $n_2(\mathbb{Z}_{25}) \geq 21$, $n_2(\mathbb{S}_5) \geq 22$.

Shortly later, different search method: $n_2(\mathbb{S}_5) = 25$.

Previous results (Thomas Honold, Ivan Landjev)

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

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

With Matthias Koch (proceedings): $n_2(\mathbb{Z}_{25}) \geq 21$, $n_2(\mathbb{S}_5) \geq 22$.
Shortly later, different search method: $n_2(\mathbb{S}_5) = 25$.

Theorem (joint work with Thomas Honold)

For every prime power q end every ring R of σ-duals over $\mathbb{F}_q$, there is a $(q^2, 2)$-arc in $\mathrm{PHG}(2, R)$.

Sketch of proof

- Work in *affine* Hjelmslev plane $\mathrm{AHG}(2, R) \subset \mathrm{PHG}(2, R)$.
- Write $R = \mathbb{F}_q[X; x \mapsto x^{p^i}]/(X^2)$.
  $(q = p^r; i \in \{0, \ldots, r-1\})$.
- Identify R^2 with $S = \mathbb{F}_{q^2}[X; x \mapsto x^{p^i}]/(X^2)$.
- Write points of arc as $t + f(t)X$ with $t \in \mathbb{F}_{q^2}$, $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$.
  $(\Rightarrow$ in each point neighbor class: 1 point of the arc).
- Question: What are good maps f?

Theorem (joint work with Thomas Honold)

For every prime power q end every ring R of σ-duals over $\mathbb{F}_q$, there is a $(q^2, 2)$-arc in $\mathrm{PHG}(2, R)$.

Sketch of proof

- Work in *affine* Hjelmslev plane $\mathrm{AHG}(2, R) \subset \mathrm{PHG}(2, R)$.
- Write $R = \mathbb{F}_q[X; x \mapsto x^{p^i}]/(X^2)$.
  $(q = p^r; i \in \{0, \ldots, r-1\})$.
- Identify R^2 with $S = \mathbb{F}_{q^2}[X; x \mapsto x^{p^i}]/(X^2)$.
- Write points of arc as $t + f(t)X$ with $t \in \mathbb{F}_{q^2}$, $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$.
  ($\Rightarrow$ in each point neighbor class: 1 point of the arc).
- Question: What are good maps f?

Theorem (joint work with Thomas Honold)

For every prime power q end every ring R of σ-duals over $\mathbb{F}_q$, there is a $(q^2, 2)$-arc in $\mathrm{PHG}(2, R)$.

Sketch of proof

- Work in *affine* Hjelmslev plane $\mathrm{AHG}(2, R) \subset \mathrm{PHG}(2, R)$.
- Write $R = \mathbb{F}_q[X; x \mapsto x^{p^i}]/(X^2)$.
  $(q = p^r; i \in \{0, \ldots, r - 1\})$.
- Identify R^2 with $S = \mathbb{F}_{q^2}[X; x \mapsto x^{p^i}]/(X^2)$.
- Write points of arc as $t + f(t)X$ with $t \in \mathbb{F}_{q^2}$, $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$.
  ($\Rightarrow$ in each point neighbor class: 1 point of the arc).
- Question: What are good maps f?

Theorem (joint work with Thomas Honold)

For every prime power q end every ring R of σ-duals over $\mathbb{F}_q$, there is a $(q^2, 2)$-arc in $\mathrm{PHG}(2, R)$.

Sketch of proof

- Work in *affine* Hjelmslev plane $\mathrm{AHG}(2, R) \subset \mathrm{PHG}(2, R)$.
- Write $R = \mathbb{F}_q[X; x \mapsto x^{p^i}]/(X^2)$.
  $(q = p^r; i \in \{0, \ldots, r-1\})$.
- Identify R^2 with $S = \mathbb{F}_{q^2}[X; x \mapsto x^{p^i}]/(X^2)$.
- Write points of arc as $t + f(t)X$ with $t \in \mathbb{F}_{q^2}$, $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$.
  ($\Rightarrow$ in each point neighbor class: 1 point of the arc).
- Question: What are good maps f?

Theorem (joint work with Thomas Honold)

For every prime power q end every ring R of σ-duals over $\mathbb{F}_q$, there is a $(q^2, 2)$-arc in $\mathrm{PHG}(2, R)$.

Sketch of proof

- Work in *affine* Hjelmslev plane $\mathrm{AHG}(2, R) \subset \mathrm{PHG}(2, R)$.
- Write $R = \mathbb{F}_q[X; x \mapsto x^{p^i}]/(X^2)$.
  $(q = p^r; i \in \{0, \ldots, r-1\})$.
- Identify R^2 with $S = \mathbb{F}_{q^2}[X; x \mapsto x^{p^i}]/(X^2)$.
- Write points of arc as $t + f(t)X$ with $t \in \mathbb{F}_{q^2}$, $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$.
  ($\Rightarrow$ in each point neighbor class: 1 point of the arc).
- Question: What are good maps f?

Theorem (joint work with Thomas Honold)

For every prime power q end every ring R of σ-duals over $\mathbb{F}_q$, there is a $(q^2, 2)$-arc in $\mathrm{PHG}(2, R)$.

Sketch of proof

- Work in *affine* Hjelmslev plane $\mathrm{AHG}(2, R) \subset \mathrm{PHG}(2, R)$.
- Write $R = \mathbb{F}_q[X; x \mapsto x^{p^i}]/(X^2)$.
  $(q = p^r; i \in \{0, \ldots, r-1\})$.
- Identify R^2 with $S = \mathbb{F}_{q^2}[X; x \mapsto x^{p^i}]/(X^2)$.
- Write points of arc as $t + f(t)X$ with $t \in \mathbb{F}_{q^2}$, $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$.
  ($\Rightarrow$ in each point neighbor class: 1 point of the arc).
- Question: What are good maps f?

Sketch of proof, continued

- Take $f(t) = \beta(t^{p^i}, t^{p^i})$, where β is $\mathbb{F}_q$-bilinear form of $\mathbb{F}_{q^2}$, then: f yields 2-arc $\Longleftrightarrow f(u)/u \notin \mathbb{F}_q$ for all $u \in \mathbb{F}_{q^2}^\times$.
- $\beta(x, y) = (xy)^q + Axy$ with suitable parameter A works if not $p = 2$ and $i = r - 1$.
- $\beta(x, y) = x^q y + Axy$ with suitable $A \in \mathbb{F}_q$ works it not $i = 0$.

Sketch of proof, continued

- Take $f(t) = \beta(t^{p^i}, t^{p^i})$, where β is $\mathbb{F}_q$-bilinear form of $\mathbb{F}_{q^2}$, then: f yields 2-arc $\iff f(u)/u \notin \mathbb{F}_q$ for all $u \in \mathbb{F}_{q^2}^\times$.
- $\beta(x, y) = (xy)^q + Axy$ with suitable parameter A works if not $p = 2$ and $i = r - 1$.
- $\beta(x, y) = x^q y + Axy$ with suitable $A \in \mathbb{F}_q$ works it not $i = 0$.

Sketch of proof, continued

- Take $f(t) = \beta(t^{p^i}, t^{p^i})$, where β is $\mathbb{F}_q$-bilinear form of $\mathbb{F}_{q^2}$, then: f yields 2-arc $\iff f(u)/u \notin \mathbb{F}_q$ for all $u \in \mathbb{F}_{q^2}^\times$.
- $\beta(x, y) = (xy)^q + Axy$ with suitable parameter A works if not $p = 2$ and $i = r - 1$.
- $\beta(x, y) = x^q y + Axy$ with suitable $A \in \mathbb{F}_q$ works it not $i = 0$.

Codes

Apply *generalized Gray map* to the 2-arcs:
$\rightsquigarrow$ linear $[q^3, 6, q^3 - q^2 - q]$-code over $\mathbb{F}_q$.

Numerical values

q	Code	distance-optimal?
2	$[8, 6, 2]_2$	optimal
3	$[27, 6, 15]_3$	optimal
4	$[64, 6, 44]_4$	optimal
5	$[125, 6, 95]_5$	best known
7	$[343, 6, 287]_7$	?

Updated table

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

Open questions & future research

- For q even: Investigate extendibility of new 2-arcs. Can we always get $(q+2, 2)$-arcs?
- Computationally determine the exact value of $n_2(\mathbb{Z}_{25})$.
- Find reasonable lower bound for q odd, R Galois ring.

Updated table

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

Open questions & future research

- For q even: Investigate extendibility of new 2-arcs. Can we always get $(q+2,2)$-arcs?
- Computationally determine the exact value of $n_2(\mathbb{Z}_{25})$.
- Find reasonable lower bound for q odd, R Galois ring.

Updated table

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

Open questions & future research

- For q even: Investigate extendibility of new 2-arcs. Can we always get $(q+2, 2)$-arcs?
- Computationally determine the exact value of $n_2(\mathbb{Z}_{25})$.
- Find reasonable lower bound for q odd, R Galois ring.

Updated table

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

Open questions & future research

- For q even: Investigate extendibility of new 2-arcs. Can we always get $(q+2, 2)$-arcs?
- Computationally determine the exact value of $n_2(\mathbb{Z}_{25})$.
- Find reasonable lower bound for q odd, R Galois ring.