ARCS AND BLOCKING SETS IN HJELMSLEV PLANES OVER FINITE CHAIN RINGS

Ivan Landjev

New Bulgarian University

– ALCOMA 2010, Schloss Thurnau, 11.-18.04.2010 –

Outline of the talk

1. Finite chain rings and modules over finite chain rings

2. Projective and affine Hjelmslev planes

3. Arcs in $\mathrm{PHG}(R_R^3)$

    (i) General upper bounds
    (ii) Arcs with $n = 2$ in $\mathrm{PHG}(R_R^3)$
    (iii) Constructions for general n
    (iv) Dual constructions

4. Blocking Sets

    (i) General results on blocking sets in $\mathrm{PHG}(R_R^3)$
    (ii) Rédei type blocking sets in $\mathrm{PHG}(R_R^3)$

1. Finite chain rings and modules over finite chain rings

1.1. Finite chain rings

Definition. A ring (associative, $1 \neq 0$, ring homomorphisms preserving 1) is called a **left (right) chain ring** if the lattice of its left (right) ideals forms a chain.

A. Nechaev, Mat. Sbornik **20**(1973), 364–382.

Example. Chain Rings with q^2 Elements

$$\boxed{R\colon |R| = q^2,\ R/\operatorname{rad} R \cong \mathbb{F}_q}$$

$$\boxed{R > \operatorname{rad} R > (0)}$$

R. Raghavendran, Compositio Mathematica **21** (1969), 195–229.

A.Cronheim, Geom. Dedicata **7**(1978), 287–302.

If $q = p^r$ there exist $r+1$ isomorphism classes of such rings:

- σ-dual numbers over $\mathbb{F}_q$, $\forall \sigma \in \operatorname{Aut}\mathbb{F}_q$: $R_\sigma = \mathbb{F}_q \oplus \mathbb{F}_q t$; addition – componentwise, multiplication –

  $(x_0 + x_1 t)(y_0 + y_1 t) = x_0 y_0 + (x_0 y_1 + x_1 \sigma(y_0))t$;

  Also: $R_\sigma = \mathbb{F}_q[t;\sigma]/(X^2)$.

- the Galois ring $\mathrm{GR}(q^2, p^2) = \mathbb{Z}_{p^2}[X]/\left(f(X)\right)$, $f(X)$ is monic of degree r, irreducible mod p.

1.2. Modules over finite chain rings

Theorem. Let R be a finite chain ring of nilpotency index m. For any finite module ${}_RM$ there exists a uniquely determined partition $\lambda = (\lambda_1 \ldots, \lambda_k) \vdash \log_q |M|$ into parts $\lambda_i \le m$ such that

$${}_RM \cong R/(\operatorname{rad} R)^{\lambda_1} \oplus \ldots \oplus R/(\operatorname{rad} R)^{\lambda_k}.$$

The partition λ is called the **shape** of ${}_RM$.

The number k is called the **rank** of ${}_RM$.

2. Projective and affine Hjelmslev spaces

2.1. Definitions

- $M = R_R^k$; $M^* := M \setminus M\theta$;
- $\mathcal{P} = \{xR \mid x \in M^*\}$;
- $\mathcal{L} = \{xR + yR \mid x, y \text{ linearly independent}\}$;
- $I \subseteq \mathcal{P} \times \mathcal{L}$ – incidence relation;
- $\bigcirc$ - **neighbour relation**:

  (N1) $X \bigcirc Y$ if $\exists s, t \in \mathcal{L}$: $X, Y I s, X, Y I t$;

  (N2) $s \bigcirc t$ if $\forall X\, I\, s\; \exists Y\, I\, t$: $X \bigcirc Y$ and $\forall Y\, I\, t\; \exists X\, I\, s$: $Y \bigcirc X$.

Definition. The incidence structure $\Pi = (\mathcal{P}, \mathcal{L}, I)$ with neighbour relation $\bigcirc$ is called the (**right**) **projective Hjelmslev geometry** over the chain ring R.

Notation: $\mathrm{PHG}(R_R^k)$

Theorem. (**Kreuzer**) For every Desarguesian Hjelmslev space Π of dimension at least 3, having on each line at least 5 points no two of which are neighbours, there exists a Hjelmslev module M over a chain ring R such that $\mathrm{PHG}(M_R)$ is isomorphic to Π.

A. Kreuzer, Resultate der Mathematik, **12** (1987), 148–156.

A. Kreuzer, *Projektive Hjelmslev-Räume*, PhD Thesis, Technische Universität München, 1988.

F.D. Veldkamp, Handbook of Incidence Geometry, 1995, 1033–1084.

2.2. The structure of $\mathrm{PHG}(R_R^k)$

$\mathcal{P}'$ – the set of all neighbour classes on points

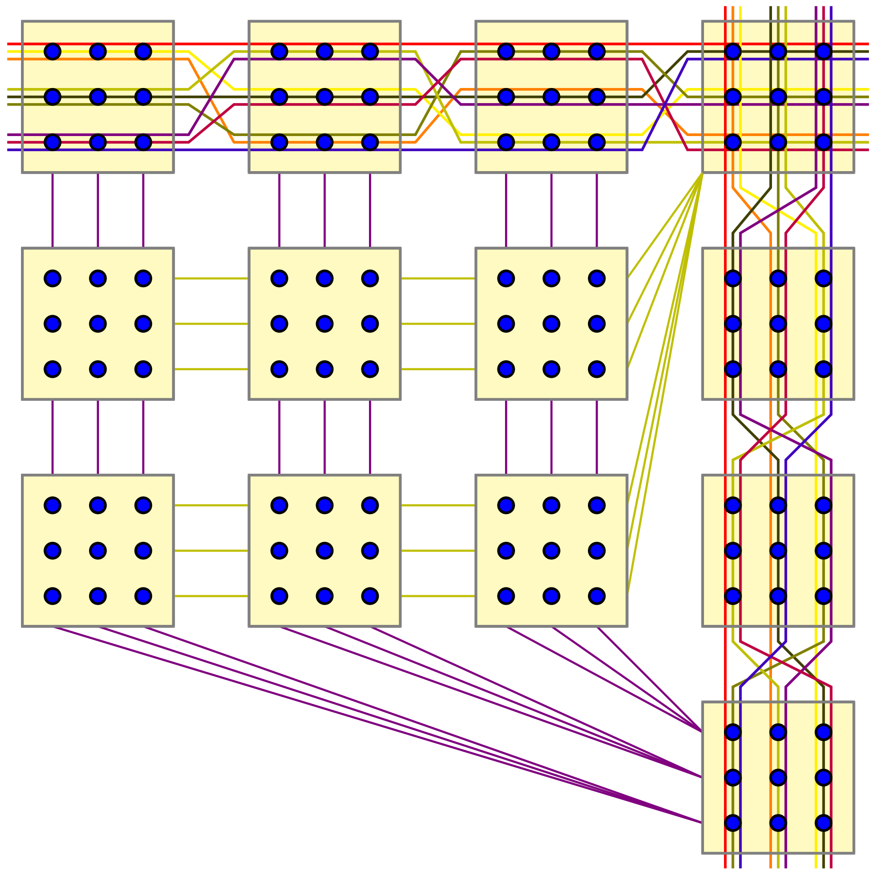
$\mathcal{L}'$ – the set of all neighbour classes on lines

$I' \subseteq \mathcal{P}' \times \mathcal{L}'$ – incidence relation defined by

$$[P]I'[l] \Leftrightarrow \exists P_0 \in [P], \exists l_0 \in [l], P_0 I l_0.$$

Theorem. $(\mathcal{P}', \mathcal{L}', I') \cong \mathrm{PG}(k-1, q)$.

$\mathrm{PHG}(\mathbb{Z}_9^3)$



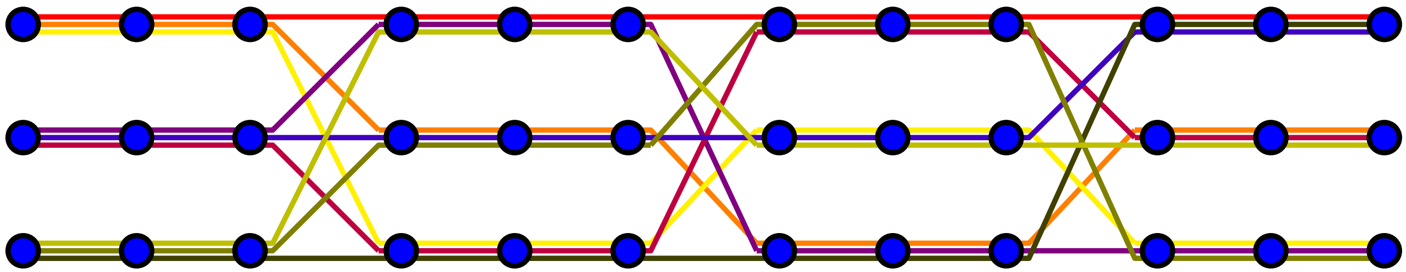
$\mathcal{S}_0$ – a subspace with $\dim \mathcal{S}_0 = s - 1$

$\mathfrak{P} = \{\mathcal{S} \cap [X] \mid X \circ \mathcal{S}_0, \mathcal{S} \in [\mathcal{S}_0]\}$

$\mathfrak{L}$ – the set of all lines incident with at least one point from $[\mathcal{S}_0]$;

$\mathfrak{I} \subseteq \mathfrak{P} \times \mathcal{L}(\mathcal{S}_0)$

Theorem. $(\mathfrak{P}, \mathfrak{L}, \mathfrak{I})$ can be imbedded isomorphically into $\mathrm{PG}(k-1, q)$. The missing part contains the points of a $(k-s-1)$-projective geometry.

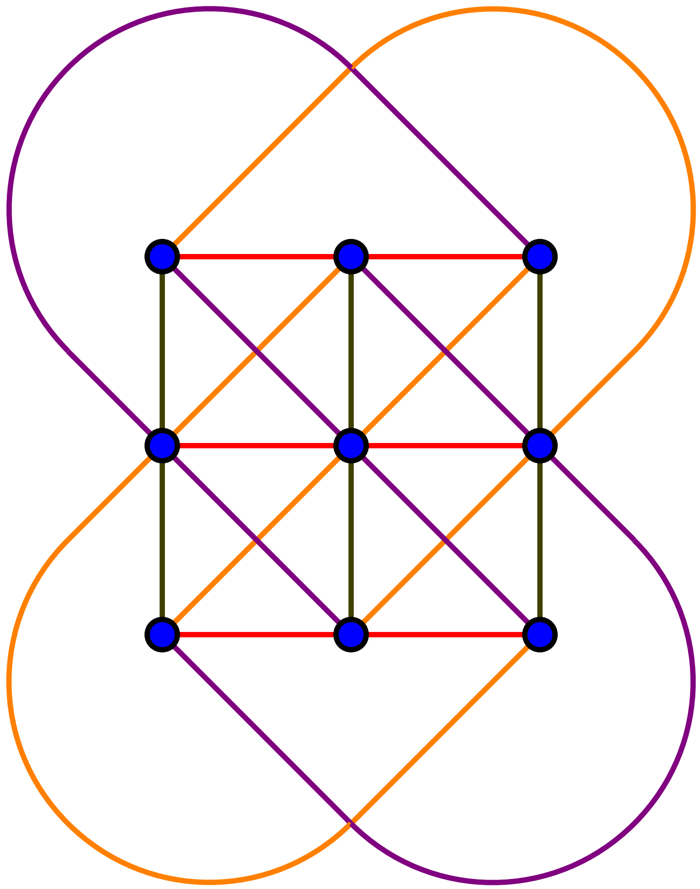


In particular, if we take $\mathcal{S}_0$ to be a point, we get

Theorem. $(\mathfrak{P}, \mathfrak{L}, \mathfrak{I}) \cong \mathrm{AG}(k-1, q)$.

B. Artmann, Math. Z. **112**(1969), 163–180.

D. Drake, J. Comb. Th. (A) **9**(1970), 267-288.



2.3. Combinatorics in $\mathrm{PHG}(R_R^k)$

$[P]$ – all neighbours to P;

$[l]$ – all neighbours to l;

$\mathcal{P}'$ – the set of all neighbour classes of points;

$\mathcal{L}'$ – the set of all neighbour classes of lines.

Gaussian coefficients

$$\begin{bmatrix} k \\ s \end{bmatrix}_q = \frac{(q^k - 1) \ldots (q^{k-s+1} - 1)}{(q^s - 1) \ldots (q - 1)}.$$

Theorem. Let $\Pi = \mathrm{PHG}(R_R^k)$, $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$.

(i) The number of subspaces of dimension s is $q^{s(k-s)} \begin{bmatrix} k \\ s \end{bmatrix}_q$, in particular, Π has $q^{k-1} \cdot \frac{q^k-1}{q-1}$ points (hyperplanes) and $q^{2(k-2)} \cdot \frac{(q^k-1)(q^{k-1}-1)}{(q^2-1)(q-1)}$ lines.

(ii) Every subspace of dimension $s-1$ is contained in exactly $q^{(t-s)(k-t)} \begin{bmatrix} k-s \\ t-s \end{bmatrix}_q$ subspaces of dimension $t-1$, $0 \leq s \leq k$.

(iii) Every point (hyperplane) has q^{k-1} neighbours;

(iv) Given a point P and a subspace $\mathcal{S}$ containing P there exist q^{s-1} points in $\mathcal{S}$ that are neighbours to P.

Theorem. Let $\Pi = \mathrm{PHG}(R_R^3)$, $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$.

(i) The number of points (lines) in Π is $q^2(q^2+q+1)$.

(ii) Every line (point) is incident with exactly $q(q+1)$ lines (points).

(iii) Every point (line) has q^2 neighbours.

(iv) Given a point P and a line L incident P there exist q points on L that are neighbours to P. Dually, there exist q points through P that are neighbours to L.

2.4. Arcs and blocking sets in $\mathrm{PHG}(R_R^3)$

Let Π be $\mathrm{PG}(k-1,q)$ or $\mathrm{PHG}(R_R^k)$.

Definition. A **multiset** in $\Pi = (\mathcal{P}, \mathcal{L}, I)$ is defined as a mapping

$$\mathfrak{K} : \mathcal{P} \to \mathbb{N}_0.$$

Definition. (n,w)-**multiarc** in Π: a multiset $\mathfrak{K}$ with

1) $\mathfrak{K}(\mathcal{P}) = n$;

2) for every hyperplane H: $\mathfrak{K}(H) \leq w$;

3) there exists a hyperplane H_0: $\mathfrak{K}(H_0) = w$.

Definition. (n, w)-**blocking multiset** in Π (or (n, w)-**minihyper**): a multiset $\mathfrak{K}$ with

1) $\mathfrak{K}(\mathcal{P}) = n$;

2) for every hyperplane H: $\mathfrak{K}(H) \geq w$;

3) there exists a hyperplane H_0: $\mathfrak{K}(H_0) = w$.

Definition.

$$\mathrm{m}_n(R_R^3) := \text{maximal size } k \text{ of a } (k, n) - \text{arc in } \mathrm{PHG}(R_R^3)$$

3. Arcs in $\mathrm{PHG}(R_R^3)$

3.1. General bounds on arcs

Theorem. $\mathcal{K}$: (n, w)-arc in $\mathrm{PHG}(R_R^3)$

Let $u = \mathcal{K}([x])$ for some class $[x]$.

Let u_i, $i = 1, \ldots, q+1$, be the maximum number of points on a line from the i-th parallel class in the affine plane defined on $[x]$. Then

$$k \leq q(q+1)n - q \sum_{i=1}^{q+1} u_i + u.$$

Corollary.

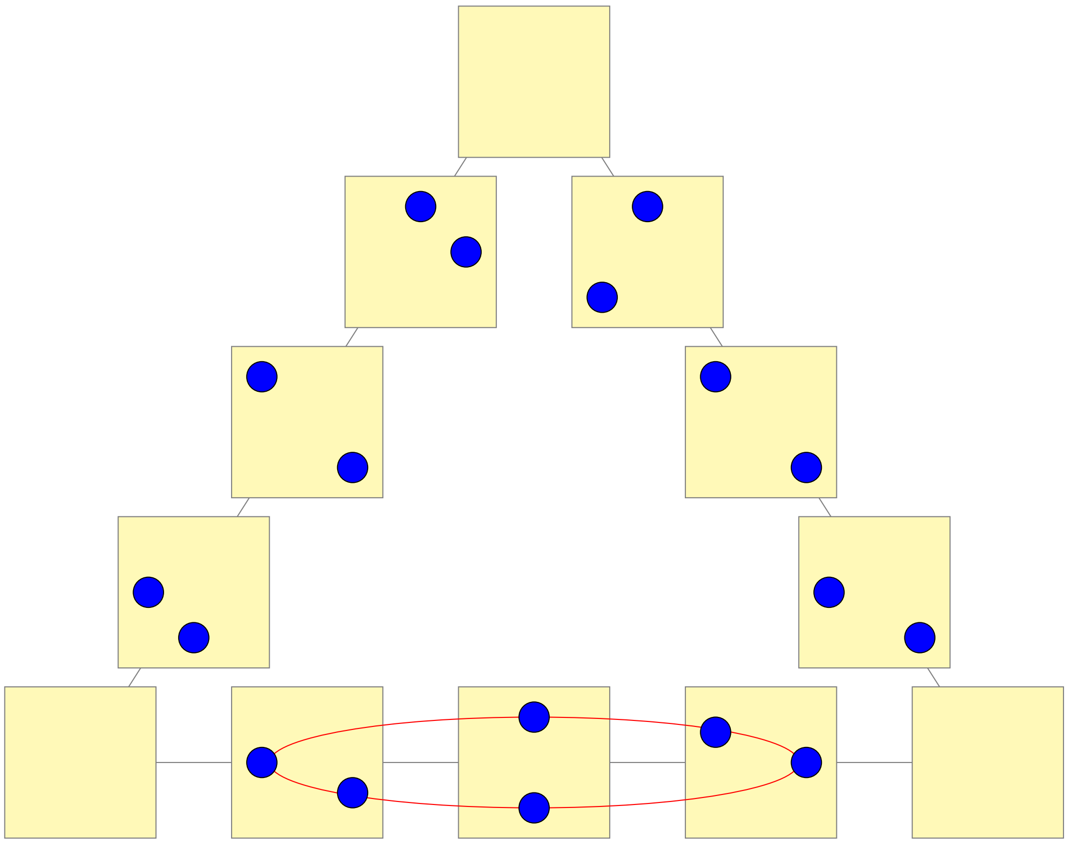
$$m_n(R_R^3) \le \max_{1\le u\le \min\{\mu_n(q),q^2\}} \min\{u(q^2+q+1), \\ q^2(n-1)+q(n-u)+u, q(q+1)(n-\lceil u/q\rceil)+u\}.$$

Corollary.

$$m_2(R_R^3) \le \begin{cases} q^2+q+1 & \text{for } q \text{ even,} \\ q^2 & \text{for } q \text{ odd.} \end{cases}$$

3.2. Arcs with $n = 2$ in $\mathrm{PHG}(R_R^3)$

- $R = \mathbb{Z}_4$: $\exists$ $(7, 2)$-arc;
- $R = \mathbb{F}_2[X]/(X^2)$: $\nexists$ $(7, 2)$-arc, $\exists$ $(6, 2)$-arc;
- $R = \mathbb{Z}_9$: $\exists$ $(9, 2)$-arc;
- $R = \mathbb{F}_3[X]/(X^2)$: $\exists$ $(9, 2)$-arc;
- $R = \mathrm{GR}(4^2, 2^2) = \mathbb{Z}_4[X]/(X^2 + X + 1)$: $\exists$ $(21, 2)$-arc
- $R = \mathbb{F}_4[X]/(X^2)$: $\exists$ $(18, 2)$-arc the nonempty neighbour classes lie on a Hermitian curve in $(\mathcal{P}', \mathcal{L}', I') \cong \mathrm{PG}(2, 4)$;
- $R = \mathbb{F}_5[X]/(X^2)$: $\exists$ $(25, 2)$-arc;
- $R = \mathbb{Z}_{25}$: $\exists$ $(21, 2)$-arc.



Construction of Hyperovals for Chain Rings R with $\operatorname{char} R = 4$

- $\mathbb{G} = \mathrm{GR}(q^2, p^2)$, $q = p^r$
- $\mathbb{G}_f = \mathrm{GR}(q^{2f}, p^2)$, $f \in \mathbb{N}$
- $\mathrm{PHG}(\mathbb{G}_{f_\mathbb{G}}) = \mathrm{PHG}(\mathbb{G}^f)$
- $\mathbb{G}_f$ contains a unique cyclic subgroup $T_f^* = \langle \eta \rangle$ of order $q^f - 1$, **the group of Teichmüller units**
- $T_f = \{x \in \mathbb{G}_f \mid x^{q^f} = x\} = T_f^* \cup \{0\}$

Definition. The set

$$\mathfrak{T}_f = \{\mathbb{G}\eta^j \mid 0 \leq j < (q^f - 1)/(q - 1)\}$$

in $\mathrm{PHG}(\mathbb{G}_f/\mathbb{G})$ is called the **Teichmüller set** of $\mathbb{G}_f$.

Theorem. Let $\mathbb{G} = \mathrm{GR}(q^2, p^2)$ be a Galois ring of characteristic p^2 and $f \geq 3$ be an integer.

(i) If every prime divisor of f is greater than p, then no three points from the Teichmüller set $\mathfrak{T}_f$ in $\mathrm{PHG}(\mathbb{G}_f/\mathbb{G})$ are collinear.

(ii) If f is even, $\mathfrak{T}_f$ contains three collinear points.

Theorem. If R is a Galois ring with $\mathrm{char}\, R = 4$ then $m_2(R_R^3) = q^2 + q + 1$.

Theorem. Let R be a chain ring with $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$, q even, which contains a subring isomorphic to the residue field $\mathbb{F}_q$. Then $m_2(R_R^3) \leq q^2 + q$.

Proof.

b_2 – number of 2-lines that meet the "Baer" subplane in 2 points

Count the flags (x, L), where x is a point from the hyperoval and L – a line from the subplane:

$$2b_2 = 3t + (q^2 + q + 1 - t) \cdot 1 = 2t + q^2 + q + 1.$$

Theorem. (Honold, Kiermaier) Let R be a chain ring with $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$, $q = p^m$ odd, which contains a subring isomorphic to the residue field $\mathbb{F}_q$. Then $m_2(R_R^3) = q^2$.

q – even	$\mathrm{char}\, R = 2$	$q^2 + 2 \leq \mathrm{m}_n(R_R^3) \leq q^2 + q$
	$\mathrm{char}\, R = 4$	$\mathrm{m}_n(R_R^3) = q^2 + q + 1$
q – odd	$\mathrm{char}\, R = p$	$\mathrm{m}_n(R_R^3) = q^2$
	$\mathrm{char}\, R = p^2$	$??? \leq \mathrm{m}_n(R_R^3) \leq q^2$

Problems for arcs with $n = 2$ in projective Hjelmslev planes

(1) Are the hyperovals obtained from the Teichmüller sets unique?

(2) What is the maximum size of an $(n, 2)$-arc in $\mathrm{PHG}(R_R^3)$, when $\operatorname{char} R = 2$?

(3) What is the maximum size of an $(n, 2)$-arc in $\mathrm{PHG}(R_R^3)$, for $\operatorname{char} R = p^2$ odd?

(4) Construct $(n, 2)$-arcs in $\mathrm{PHG}(R_R^3)$, $\operatorname{char} R = p^2$ odd, with $\approx Cq^2$ points (preferably for some constant C close to 1).

3.3. Constructions for General n

- for $q^2 \leq n \leq q^2 + q$: $\mathrm{m}_n(R) = q(q+1)n - q^3$.
- for $n = q^2 - 1$: $\exists$ $(q^4 - q^2 - q, q^2 - 1)$-arc for all R.

  We conjecture $\mathrm{m}_n(R) = q^4 - q^2 - q$.
- for $q^2 - q \leq n \leq q^2 - 2$: $\exists$ $(q^2 n - 2q, n)$-arcs for every R.
- for $n < 2q$ no statisfactory general constructions are known except for the case $n = 2$.

3.4. The Dual Construction in $\mathrm{PHG}(R^3_R)$

- $\Pi = \mathrm{PHG}(R^k_R)$, R – a chain ring of nilpotency index 2
- $\mathfrak{K}$: (n, w)-arc in Π

Definition. The **type** of a hyperplane H is the triple $(a_0(H), a_1(H), a_2(H))$:

$$\begin{aligned} a_0(H) &= \sum_{x : x \notin [H]} \mathfrak{K}(x), \quad a_1(H) = \sum_{x : x \in [H] \setminus H} \mathfrak{K}(x), \\ a_2(H) &= \sum_{x : x \in H} \mathfrak{K}(x). \end{aligned}$$

For $\boldsymbol{a} = (a_0, a_1, a_2) \in \mathbb{N}_0 \times \mathbb{N}_0 \times \mathbb{N}_0$. define

$$A_{\boldsymbol{a}} = |\{H \mid H \in \mathcal{H}, H \text{ has type } \boldsymbol{a}\}|,$$

where $\mathcal{H}$ is the set of all hyperplanes.

Definition. The sequence

$$\{A_{\boldsymbol{a}} \mid \boldsymbol{a} \in \mathbb{N}_0 \times \mathbb{N}_0 \times \mathbb{N}_0\}$$

is called the **spectrum** of $\mathfrak{K}$.

The **set of intersection numbers** of $\mathfrak{K}$ is

$$W(\mathfrak{K}) = \{\boldsymbol{a} \mid \boldsymbol{a} \in \mathbb{N}_0 \times \mathbb{N}_0 \times \mathbb{N}_0, A_{\boldsymbol{a}} > 0\}.$$

- $\tau : W(\mathfrak{K}) \rightarrow \mathbb{N}_0$ – an arbitrary function
- Define

$$\mathfrak{K}^\tau : \left\{ \begin{array}{ccc} \mathcal{H} & \rightarrow & \mathbb{N}_0 \\ H & \rightarrow & \tau(\boldsymbol{a}(H)) \end{array} \right. .$$

- We call $\mathfrak{K}^\tau$ the τ-dual to $\mathfrak{K}$
- **Note:** $\mathfrak{K}^\tau$ is a multi-arc in $\mathrm{PHG}({}_R R^k)$.
- **Parameters:**

$$\begin{aligned} n' &= \sum_{\boldsymbol{a} \in W} \tau(\boldsymbol{a}) A_{\boldsymbol{a}}, \\ w' &= \max_{x \in \mathcal{P}} \mathfrak{K}^\tau(x) = \max_{x \in \mathcal{P}} \sum_{H : x \in H} \mathfrak{K}^\tau(H). \end{aligned}$$

Let

$$\tau(\boldsymbol{a}) = \alpha + \beta a_1 + \gamma a_2,$$

where α, β, γ are chosen in such way that $\tau(\boldsymbol{a})$ are non-negative integers for all $\boldsymbol{a} \in W(\mathfrak{K})$.

$$\mathfrak{K}^{\tau}(H) = \alpha + \beta\mathfrak{K}([H]) + (\gamma - \beta)\mathfrak{K}(H).$$

Theorem. Let $\mathfrak{K}$ be a (n, w)-arc in $\mathrm{PHG}(R_R^k)$, where R is a chain ring with $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Let $\alpha, \beta, \gamma \in \mathbb{Q}$ be such that $\alpha + \beta a_1 + \gamma a_2 \in \mathbb{N}_0$ for all $\boldsymbol{a} = (a_0, a_1, a_2) \in W$. For any hyperplane H of type $\boldsymbol{a} = (a_0, a_1, a_2)$, let

$$\tau(H) = \tau(\boldsymbol{a}(H)) = \alpha + \beta a_1 + \gamma a_2.$$

Then the type of an arbitrary hyperplane $x^* = \boldsymbol{x}R \in \mathcal{P}$ in the dual geometry is $\boldsymbol{b} = (b_0, b_1, b_2)$, where

$$
\begin{aligned}
b_0 &= \alpha q^{2k-2} + \beta n q^{2k-4}(q-1) + \gamma n q^{2k-4} \\
&\quad -\Big(\beta q^{2k-4}(q-1) + \gamma q^{2k-4}\Big)\mathfrak{K}([x]),
\end{aligned}
$$

$$
\begin{aligned}
b_1 &= \alpha q^{k-2}(q^{k-1}-1) + \beta n q^{k-3}(q^{k-2}-1)(q-1) + \gamma n q^{k-3}(q^{k-2}-1) \\
&\quad +\Big(\beta q^{k-3}(q^k - 2q^{k-1} + q^{k-2} - 1) + \gamma q^{k-3}(q^{k-1} - q^{k-2} + 1)\Big)\mathfrak{K}([x]) \\
&\quad -(\gamma - \beta) q^{2k-4}\mathfrak{K}(x),
\end{aligned}
$$

$$
\begin{aligned}
b_2 &= \alpha q^{k-2} \cdot \frac{q^{k-1}-1}{q-1} + \beta n q^{k-3}(q^{k-2}-1) + \gamma n q^{k-3} \cdot \frac{q^{k-2}-1}{q-1} \\
&\quad +\Big(\beta q^{k-3}(q^{k-1} - q^{k-2} + 1) + \gamma q^{k-3}(q^{k-2} - 1)\Big)\mathfrak{K}([x]) \\
&\quad +(\gamma - \beta) q^{2k-4}\mathfrak{K}(x).
\end{aligned}
$$

Example 1. The hyperoval in $\mathrm{PHG}(R_R^3)$, $R = \mathrm{GR}(q^2, 2^2)$, $q = 2^r$

• We take $\tau\colon (q^2, q+1, 0) \mapsto 1$, $(q^2, q-1, 2) \mapsto 0$, so that $\mathfrak{K}^\tau$ consists of the 0-lines of the hyperoval $\mathfrak{K}$, taken with multiplicity 1. The mapping τ is realized by the choice of coefficients

$$\alpha = 0, \beta = \frac{1}{q+1}, \gamma = -\frac{q-1}{2(q+1)},$$

• We have $n = q^2 + q + 1$ and $\mathfrak{K}([x]) = 1$ for all x.

• The possible types of lines in the dual plane:

$$
\begin{aligned}
b_0 &= \frac{q^4 - q^3}{2}, \\
b_1 &= \frac{q^3 - q^2 - q}{2} + \frac{1}{2} q^2 \mathfrak{K}(x), \\
b_2 &= \frac{q^2}{2} - \frac{1}{2} q^2 \mathfrak{K}(x).
\end{aligned}
$$

• The dual arc is a $((q^4 - q)/2, q^2/2)$-arc with two intersection numbers 0 and $q^2/2$. Moreover, every neighbour class of points contains exactly $(q^2 - q)/2$ points.

• It can be checked that the dual arcs are optimal , i.e.

$$\mathrm{m}_{q^2/2}(R_R^3) = \frac{q^4 - q}{2},$$

where $R = \mathrm{GR}(q^2, q)$ with $q = 2^r$.

• In particular, there exists a $(126, 8)$-**arc** in the Hjelmslev plane over $\mathrm{GR}(4^2, 2^2)$.

Example 2. The "Baer" subplane

- $|R| = q^2 = p^{2r}$, $R/\operatorname{rad} R \cong \mathbb{F}_{p^r}$, $\operatorname{char} R = p$
- there exists a "Baer" subplane: $(q^2+q+1, q+1)$-arc
- $W = \{(q^2, 0, q+1), (q^2, q, 1)\}$:

$$\alpha = 0, \beta = -\frac{1}{q(q+1)}, \gamma = \frac{1}{q+1}.$$

- The dual arc has the same parameters.

Example 3.

• A $(q(q^2+q+1), q)$-arc consisting of q^2+q+1 line segments, one segment in each neighbour class of points, and the segments have all possible directions.

$$W = \left\{(q^3, q^2, q), (q^3, q^2-q, 2q)\right\}.$$

• We have line types $(q^3, q^2-\varepsilon q, q+\varepsilon q)$, where $\varepsilon = 0$ or 1, and $\mathfrak{K}([x]) = q$ for all classes of points $[x]$.

• Take $\tau \colon W \to \mathbb{N}_0$ as $(q^3, q^2, q) \mapsto 0$, $(q^3, q^2-q, 2q) \mapsto 1$ or, equivalently,

$$\alpha = 0, \;\; \beta = -\frac{1}{q(q+1)}, \;\; \gamma = \frac{1}{q+1}.$$

• The dual arc has the same parameters.

Values of $m_n(R_R^3)$ for Hjelmslev planes of order $q^2 = 4$ and $q^2 = 9$

n/R	$\mathbb{Z}_4$	$\mathbb{F}_2[X]/(X^2)$	$\mathbb{Z}_9$	$\mathbb{F}_3[X]/(X^2)$
2	7	6	9	9
3	10	10	19	18
4			30	30
5			39	38
6			49	50
7			60	60
8			69	69

4. Blocking Sets in $\mathrm{PHG}(R_R^3)$

4.1. General results

Theorem. R finite chain ring with $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. The minimal size of a (k, n)-blocking set in $\mathrm{PHG}(R_R^3)$ is $nq^{m-1}(q+1)$.

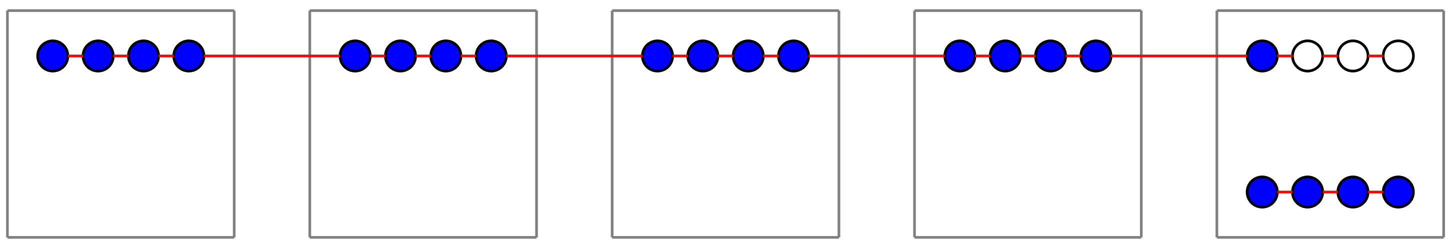
Corollary. The minimal size of blocking set is $q^{m-1}(q+1)$ and in case of equality it contains the points of a line.

Blocking Sets with $k = q^2 + q + 1$

(1) a subplane $\cong \mathrm{PG}(2, q)$

(2) Lines: ℓ_0, ℓ_1 with $\ell_0 \circ \ell_1$; $X \in \ell \setminus \ell_0$.

$$\mathfrak{K}(P) = \begin{cases} 1 & \text{if } P \in (\ell_0 \setminus [X]) \cup \{X\} \text{ or } P \in \ell_1 \cap [X] \\ 0 & \text{otherwise.} \end{cases}$$



Theorem.

Let $\mathfrak{K}$ be an irreducible $(q^2+q+1,1)$-blocking set in $\mathrm{PHG}(R_R^3)$, $|R|=q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Then either

(1) $\operatorname{Supp}\mathfrak{K}$ is a projective plane of order q, or else

(2) $\mathfrak{K}$ is a blocking set of the type (2).

If $R=\mathrm{GR}(q^2,p^2)$, then $\mathfrak{K}$ is of the type (2).

4.2. Rédei-type Blocking Sets in $\mathrm{PHG}(R^3_R)$

$$\Gamma = \{\gamma_0 = 0, \gamma_1 = 1, \gamma_2, \dots, \gamma_{q-1}\}$$

$\gamma_i \not\equiv \gamma_j \pmod{\operatorname{rad} R}$

$[Z = 0]$ – the line class at infinity.

$[Z = 0] = \{aX + bY + Z = 0 \mid a, b \in \operatorname{rad} R\}$.

All points incident with lines in this class: (x, y, z) with $z \in \operatorname{rad} R$.

All points outside this class: $(x, y, 1)$, $x, y \in R$.

The points of $\mathrm{AHG}(R_R^2)$: (x, y), where $x, y \in R$.

The lines of $\mathrm{AHG}(R_R^2)$:

- $Y = aX + b$, $a, b \in R$;

- $X = cY + d$, $d \in R$, $c \in \mathrm{rad}\, R$.

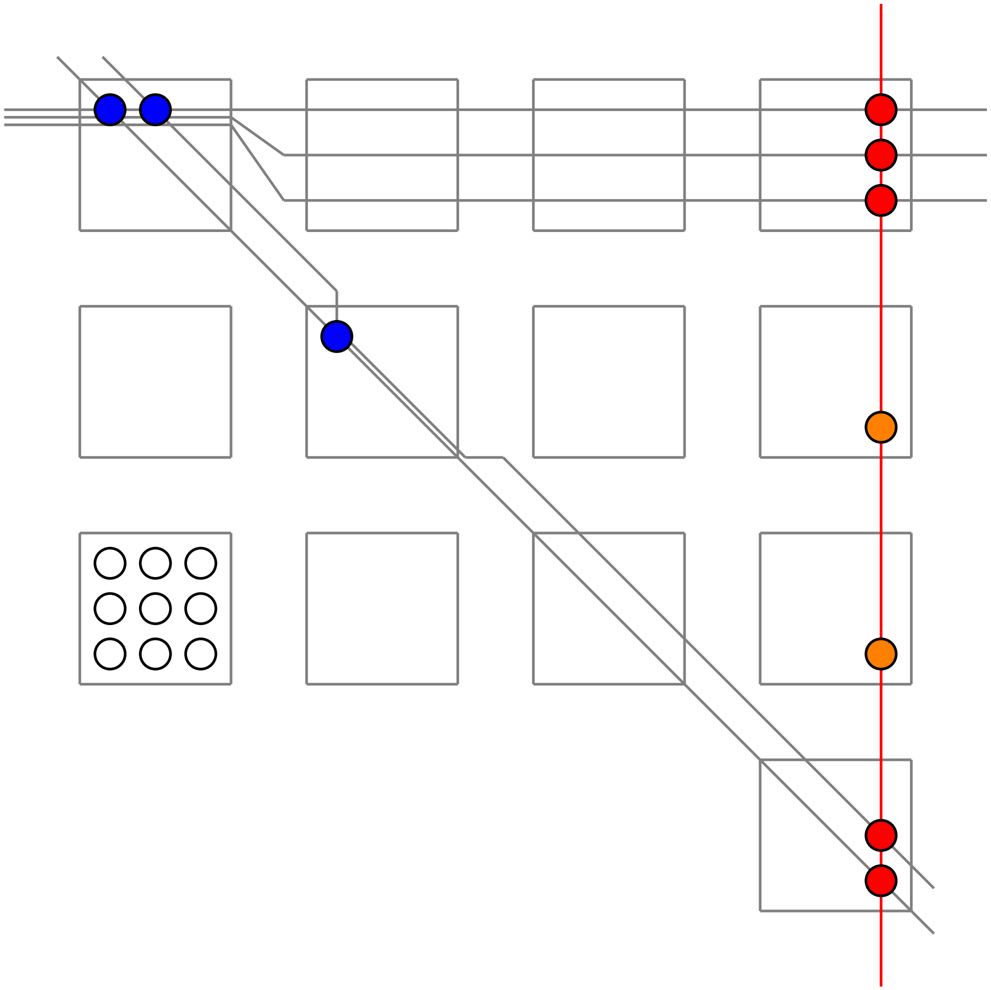
Definition. We say that a line of the first type has slope a . A line with equation $X = cY + d$ is said to have slope ∞_j, if $c = \theta\gamma_j$, $j = 0, 1, \ldots, q-1$.

Lemma. A line ℓ through $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ in $\mathrm{AHG}(R_R^2)$ has slope a, $a \in R^*$, if the line in $\mathrm{PHG}(R_R^3)$ through $(x_1, y_1, 1)$ and $(x_2, y_2, 1)$ meets $Z = 0$ in $(1, a, 0)$. Similarly, a line ℓ through P and Q has slope ∞_j if it meets $Z = 0$ in $(\theta\gamma_j, 1, 0)$.

Definition. (a) (resp. (∞_j)) will denote the infinite point from $Z = 0$ of the lines with slope a (resp. ∞_j).

Definition. Let U be a set of q^2 points in $\mathrm{AHG}(R_R^2)$. We say that the infinite point (a) is determined by U if there exist different points $P, Q \in U$ such that P, Q and (a) are collinear in $\mathrm{PHG}(R_R^3)$.

Theorem. Let U be a set of q^2 points in $\mathrm{AHG}(R_R^2)$. Denote by D the set of infinite points determined by U and by $D^{(1)}$ the set of neighbour classes in the infinite line class containing points from D. If $|D| < q^2 + q$ then there exists an irreducible blocking set in $\mathrm{PHG}(R_R^3)$ of size $q^2 + q + 1 + |D| - |D^{(1)}|$ that contains U. In particular, if D contains representatives from all neighbour classes on the infinite line, then $B = U \cup D$ is an irreducible blocking set of size $q^2 + |D|$ in $\mathrm{PHG}(R_R^3)$.



Definition. A blocking set of size $q^2 + u$ is said to be of Rédei type if there exists a line ℓ with $|B \cap \ell| = u$ and $|B \cap [\ell]| = u$.

We are interested in sets U that are obtained in the form

$$U = \{(x, f(x)) \mid x \in R\}$$

for some suitably chosen function $f\colon R \to R$. Let $P = (x, f(x))$ and $Q = (y, f(y))$ be two different points from U. We have the following possibilities:

1) if $x - y \notin \operatorname{rad} R$ then P and Q determine the point (a), where

$$(a) = (f(x) - f(y))(x - y)^{-1}.$$

2) if $x - y \in \operatorname{rad} R \setminus (0)$, and $f(x) - f(y) \notin \operatorname{rad} R$ the points P and Q determine the point (∞_i) if

$$(x - y)(f(x) - f(y))^{-1} = \theta\gamma_i, \gamma_i \in \Gamma.$$

3) if $x - y \in \operatorname{rad} R \setminus (0)$, and $f(x) - f(y) \in \operatorname{rad} R$, say $x - y = a\theta$, $a \neq 0$, $f(x) - f(y) = b\theta$, $a, b \in \Gamma$, the points P and Q determine all points (c) with $c \in ba^{-1} + \operatorname{rad} R$.

Example 1.

$$f : a + \theta b \to b + \theta a.$$

over R_σ : $q+1$ directions;

over $\mathrm{GR}(q^2, p^2)$: $q^2 - q + 2$ directions.

Example 2.

Theorem. Let $R = \mathrm{GR}(q^2, p^2)$, $q = p^m$, p odd. The set $U = \{(x, f(x) \mid x \in S\}$, where the function is defined by

$$f(x) = \begin{cases} (a_0, a_1) & \text{if } a_0 \text{ is a square in } \mathbb{F}_q, \\ (-a_0, -a_1) & \text{if } a_0 \text{ is a non-square in } \mathbb{F}_q. \end{cases}$$

$$\frac{q^2}{2} + \frac{3}{2}q$$

directions in $\mathrm{AHG}(R_R^2)$.

In particular, there exists a Rédei type blocking set in $\mathrm{PHG}(R_R^3)$ of size

$$\frac{3}{2}q^2 + 2q - \frac{1}{2}.$$

Example 3.

Let $R = \mathrm{GR}(q^2, p^2)$, $q = p^s$, p a prime,

Set $\Gamma(R) = \{\alpha \in R \mid \alpha^q = \alpha\}$.

$\alpha = a_0 + a_1 p$, $a_i \in \Gamma(R)$

$\mathrm{Aut}\, R$ is cyclic of order s:

$$\sigma(\alpha) = a_0^{p^i} + a_1^{p^i} p, \quad i = 0, \ldots, s-1.$$

$S = \mathrm{GR}(q^{2m}, p^2)$.

$\mathrm{Aut}(S:R)$ is cyclic of order m and is generated by

$$\sigma_0(\alpha) = a_0^q + a_1^q p.$$

The trace function $\mathrm{Tr}_{S:R} : S \to R$ is defined by

$$\mathrm{Tr}_{S:R}(x) = \sum_{\sigma \in \mathrm{Aut}(S:R)} \sigma(x).$$

Properties:

(1) for all $\alpha \in S$ and for all $a \in R$: $\mathrm{Tr}_{S:R}(a\alpha) = a\,\mathrm{Tr}_{S:R}(\alpha)$;

(2) for all $\alpha, \beta \in S$: $\mathrm{Tr}_{S:R}(\alpha + \beta) = \mathrm{Tr}_{S:R}(\alpha) + \mathrm{Tr}_{S:R}(\beta)$;

(3) for all $c \in \mathrm{rad}\, S$, $\mathrm{Tr}\,_{S:R}(c) \in \mathrm{rad}\, R$;

(4) for every $b \in R$, the equation $\mathrm{Tr}\,_{S:R}(x) = b$ has exactly $|S|/|R| = q^{2(m-1)}$ solutions.

Let $R = \mathrm{GR}(q^2, p^2)$ and $S = \mathrm{GR}(q^{2m}, p^2)$, i.e. $S = R[X]/(g(X))$

where g is a monic polynomial of degree m which is irreducible modulo p.

Define

$$f(x) = \mathrm{Tr}\,_{S:R}(x)$$

Theorem. Let $R = \mathrm{GR}(q^2, p^2)$ and let S be an extension of R of degree m. The set $U = \{(x, f(x)) \mid x \in S\}$ defined by the function $f(x) = \mathrm{Tr}_{S:R}(x)$ determines

$$\frac{q^m - 1}{q - 1} q^m$$

directions in $\mathrm{AHG}(S_S^2)$. There exists a Rédei type blocking set in $\mathrm{PHG}(S_S^3)$ of size

$$q^{2m} + q^m + 1 + \frac{q^m - 1}{q - 1} q^m - q^{m-1}.$$