ARCS AND BLOCKING SETS IN HJELMSLEV PLANES OVER FINITE CHAIN RINGS

Ivan Landjev

New Bulgarian University

Outline of the talk

1. Finite chain rings and modules over finite chain rings

2. Projective and affine Hjelmslev planes

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

4. Blocking Sets
   (i) General results on blocking sets in $\mathrm{PHG}(R^3_R)$
   (ii) Rédei type blocking sets in $\mathrm{PHG}(R^3_R)$
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.

Example. Chain Rings with $q^2$ Elements

\[
R : |R| = q^2, \ R/\text{rad} \ R \cong \mathbb{F}_q
\]

\[
R > \text{rad} \ R > (0)
\]


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

- $\sigma$-dual numbers over $\mathbb{F}_q$, $\forall \sigma \in \text{Aut} \mathbb{F}_q$: $R_\sigma = \mathbb{F}_q \oplus \mathbb{F}_q t$; 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 $\text{GR}(q^2, p^2) = \mathbb{Z}_p^2[X]/(f(X))$, $f(X)$ 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 $R M$ there exists a uniquely determined partition $\lambda = (\lambda_1 \ldots, \lambda_k) \vdash \log_q |M|$ into parts $\lambda_i \leq m$ such that

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

The partition $\lambda$ is called the **shape** of $R M$.

The number $k$ is called the **rank** of $R M$. 

2. Projective and affine Hjelmslev spaces

2.1. Definitions

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

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

(N2) $s \circ t$ if $\forall X I s \exists Y I t : X \circ Y$ and $\forall Y I t \exists X I s : Y \circ X$. 
**Definition.** The incidence structure $\Pi = (\mathcal{P}, \mathcal{L}, I)$ with neighbour relation $\oslash$ is called the (right) **projective Hjelmslev geometry** over the chain ring $R$.

Notation: $\text{PHG}(R^k_R)$

**Theorem.** (Kreuzer) For every Desarguesian Hjelmslev space $\Pi$ 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 $\text{PHG}(M_R)$ is isomorphic to $\Pi$.


2.2. The structure of $\text{PHG}(R^k_R)$

$\mathcal{P'}$ – 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

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

**Theorem.** $(\mathcal{P'}, \mathcal{L'}, I') \cong \text{PG}(k - 1, q)$. 
$\text{PHG}(\mathbb{Z}_9^3)$
$S_0$ – a subspace with $\dim S_0 = s - 1$

$\mathcal{P} = \{S \cap [X] \mid X \supset S_0, S \in [S_0]\}$

$\mathcal{L}$ – the set of all lines incident with at least one point from $[S_0]$;

$\mathcal{I} \subseteq \mathcal{P} \times \mathcal{L}(S_0)$

**Theorem.** $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ can be imbedded isomorphically into $\text{PG}(k - 1, q)$. The missing part contains the points of a $(k - s - 1)$-projective geometry.
In particular, if we take $S_0$ to be a point, we get

**Theorem.** $(\mathcal{P}, \mathcal{L}, \mathcal{I}) \cong \text{AG}(k - 1, q)$.


2.3. Combinatorics in PHG($R^k_R$)

$[P]$ – 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 $\Pi = \text{PHG}(R^k_R)$, $|R| = q^2$, $R/\text{rad} \, R \cong \mathbb{F}_q$.

(i) The number of subspaces of dimension $s$ is $q^{s(k-s)} \binom{k}{s}_q$, in particular, $\Pi$ 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 $q^{(t-s)(k-t)} \binom{k-s}{t-s}_q$ 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 $S$ containing $P$ there exist $q^{s-1}$ points in $S$ that are neighbours to $P$. 
**Theorem.** Let $\Pi = \text{PHG}(R^3_R)$, $|R| = q^2$, $R/\text{rad } R \cong \mathbb{F}_q$.

(i) The number of points (lines) in $\Pi$ 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 $\text{PHG}(R^3_R)$

Let $\Pi$ be $\text{PG}(k-1, q)$ or $\text{PHG}(R^k_R)$.

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

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

**Definition.** $(n, w)$-multi\_arc in $\Pi$: a multiset $\mathcal{K}$ with

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

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

3) there exists a hyperplane $H_0$: $\mathcal{K}(H_0) = w$. 
**Definition.** \((n, w)\)-blocking multiset in \(\Pi\) (or \((n, w)\)-minihyper): a multiset \(\mathcal{K}\) with

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

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

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

**Definition.**

\[
m_n(R^3_R) := \text{maximal size } k \text{ of a } (k, n) - \text{arc in PHG}(R^3_R)
\]
3. Arcs in \( \text{PHG}(R^3_R) \)

3.1. General bounds on arcs

**Theorem.** \( \mathcal{K} \): \((n, w)\)-arc in \( \text{PHG}(R^3_R) \)

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.

\[ m_n(R^3_R) \leq \max_{1 \leq u \leq \min\{\mu_n(q), q^2\}} \min\{u(q^2 + q + 1), q^2(n - 1) + q(n - u) + u, q(q + 1)(n - \lceil u/q \rceil) + u\}. \]

Corollary.

\[ m_2(R^3_R) \leq \begin{cases} \qquad q^2 + q + 1 & \text{for } q \text{ even,} \\ \qquad q^2 & \text{for } q \text{ odd.} \end{cases} \]
3.2. Arcs with \( n = 2 \) in \( \text{PHG}(R^3_R) \)

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

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

**Definition.** The set

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

in $\text{PHG}(G_f/G)$ is called the **Teichmüller set** of $G_f$. 

---

- ALCOMA 2010, Schloss Thurnau, 11.-18.04.2010 - 23
Theorem. Let $\mathbb{G} = GR(q^2, p^2)$ 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 $\mathcal{T}_f$ in $PHG(\mathbb{G}_f/\mathbb{G})$ are collinear.

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

Theorem. If $R$ is a Galois ring with char $R = 4$ then $m_2(R_R^3) = q^2 + q + 1$. 
Theorem. Let $R$ be a chain ring with $|R| = q^2$, $R/\text{rad } R \cong \mathbb{F}_q$, $q$ even, which contains a subring isomorphic to the residue field $\mathbb{F}_q$. Then $m_2(R^3_R) \leq q^2 + q$.

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 $|R| = q^2$, $R/\text{rad } R \cong \mathbb{F}_q$, $q = p^m$ odd, which contains a subring isomorphic to the residue field $\mathbb{F}_q$. Then $m_2(R^3_R) = q^2$. 

---

<table>
<thead>
<tr>
<th>$q$ - even</th>
<th>char $R = 2$</th>
<th>$q^2 + 2 \leq m_n(R_R^3) \leq q^2 + q$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>char $R = 4$</td>
<td>$m_n(R_R^3) = q^2 + q + 1$</td>
</tr>
<tr>
<td>$q$ - odd</td>
<td>char $R = p$</td>
<td>$m_n(R_R^3) = q^2$</td>
</tr>
<tr>
<td></td>
<td>char $R = p^2$</td>
<td>$??\leq m_n(R_R^3) \leq q^2$</td>
</tr>
</tbody>
</table>
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 $\text{PHG}(R^3_R)$, when $\text{char } R = 2$?

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

(4) Construct $(n, 2)$-arcs in $\text{PHG}(R^3_R)$, 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 $q^2 \leq n \leq q^2 + q$: $m_n(R) = q(q + 1)n - q^3$.

- for $n = q^2 - 1$: $\exists (q^4 - q^2 - q, q^2 - 1)$-arc for all $R$.
  We conjecture $m_n(R) = q^4 - q^2 - q$.

- for $q^2 - q \leq n \leq q^2 - 2$: $\exists (q^2n - 2q, n)$-arcs for every $R$.

- for $n < 2q$ no satisfactory general constructions are known except for the case $n = 2$. 
3.4. The Dual Construction in $\text{PHG}(R_R^3)$

- $\Pi = \text{PHG}(R_R^k)$, $R$ – a chain ring of nilpotency index 2

- $\mathcal{K}$: $(n, w)$-arc in $\Pi$

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

\[
\begin{align*}
a_0(H) &= \sum_{x : x \notin [H]} \mathcal{K}(x), \\
a_1(H) &= \sum_{x : x \in [H] \setminus H} \mathcal{K}(x), \\
a_2(H) &= \sum_{x : x \in H} \mathcal{K}(x).
\end{align*}
\]
For \( \mathbf{a} = (a_0, a_1, a_2) \in \mathbb{N}_0 \times \mathbb{N}_0 \times \mathbb{N}_0 \). define

\[
A_{\mathbf{a}} = |\{H \mid H \in \mathcal{H}, H \text{ has type } \mathbf{a}\}|
\]

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

**Definition.** The sequence

\[
\{A_{\mathbf{a}} \mid \mathbf{a} \in \mathbb{N}_0 \times \mathbb{N}_0 \times \mathbb{N}_0\}
\]

is called the **spectrum** of \( \mathcal{K} \).

The **set of intersection numbers** of \( \mathcal{K} \) is

\[
W(\mathcal{K}) = \{\mathbf{a} \mid \mathbf{a} \in \mathbb{N}_0 \times \mathbb{N}_0 \times \mathbb{N}_0, A_{\mathbf{a}} > 0\}.
\]
• \( \tau : W(\mathcal{R}) \rightarrow \mathbb{N}_0 \) – an arbitrary function

• Define

\[
\mathcal{R}^\tau : \begin{cases} 
H & \rightarrow \mathbb{N}_0 \\
H & \rightarrow \tau(a(H)) \end{cases}
\]

• We call \( \mathcal{R}^\tau \) the \( \tau \)-dual to \( \mathcal{R} \)

• **Note:** \( \mathcal{R}^\tau \) is a multi-arc in \( \text{PHG}(\text{R} \text{R}^k) \).

• **Parameters:**

\[
n' = \sum_{a \in W} \tau(a) A_a,
\]

\[
w' = \max_{x \in \mathcal{P}} \mathcal{R}^\tau(x) = \max_{x \in \mathcal{P}} \sum_{H : x \in H} \mathcal{R}^\tau(H).
\]
Let
\[ \tau(a) = \alpha + \beta a_1 + \gamma a_2, \]
where \( \alpha, \beta, \gamma \) are chosen in such way that \( \tau(a) \) are non-negative integers for all \( a \in W(\mathcal{R}) \).

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

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

Then the type of an arbitrary hyperplane $x^* = xR \in \mathcal{P}$ in the dual geometry is $b = (b_0, b_1, b_2)$, where
\[ b_0 = \alpha q^{2k-2} + \beta n q^{2k-4} (q - 1) + \gamma n q^{2k-4} - \left( \beta q^{2k-4}(q - 1) + \gamma q^{2k-4} \right) \mathcal{R}([x]), \]

\[ b_1 = \alpha q^{k-2} (q^{k-1} - 1) + \beta n q^{k-3} (q^{k-2} - 1)(q - 1) + \gamma n q^{k-3} (q^{k-2} - 1) + \left( \beta q^{k-3}(q - 2q^{k-1} + q^{k-2} - 1) + \gamma q^{k-3}(q^{k-1} - q^{k-2} + 1) \right) \mathcal{R}([x]) \]

\[ - (\gamma - \beta) q^{2k-4} \mathcal{R}(x), \]

\[ b_2 = \alpha q^{k-2} \cdot \frac{q^{k-1} - 1}{q - 1} + \beta n q^{k-3} (q^{k-2} - 1) + \gamma n q^{k-3} \cdot \frac{q^{k-2} - 1}{q - 1} + \left( \beta q^{k-3}(q^{k-1} - q^{k-2} + 1) + \gamma q^{k-3}(q^{k-2} - 1) \right) \mathcal{R}([x]) \]

\[ + (\gamma - \beta) q^{2k-4} \mathcal{R}(x). \]
Example 1. The hyperoval in $\text{PHG}(R^3_R)$, $R = \text{GR}(q^2, 2^2)$, $q = 2^r$

- We take $\tau: (q^2, q + 1, 0) \mapsto 1$, $(q^2, q - 1, 2) \mapsto 0$, so that $\mathcal{K}^\tau$ consists of the 0-lines of the hyperoval $\mathcal{K}$, taken with multiplicity 1. The mapping $\tau$ 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 $\mathcal{K}([x]) = 1$ for all $x$. 
• The possible types of lines in the dual plane:

\[
\begin{align*}
    b_0 &= \frac{q^4 - q^3}{2}, \\
    b_1 &= \frac{q^3 - q^2 - q}{2} + \frac{1}{2}q^2K(x), \\
    b_2 &= \frac{q^2}{2} - \frac{1}{2}q^2K(x).
\end{align*}
\]

• 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.

\[ m_{q^2/2}(R^3_R) = \frac{q^4 - q}{2}, \]

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

• In particular, there exists a \((126, 8)\)-arc in the Hjelmslev plane over \( \text{GR}(4^2, 2^2) \).
Example 2. The “Baer” subplane

- $|R| = q^2 = p^{2r}$, $R/\text{rad } R \cong \mathbb{F}_{p^r}$, 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.

\[
W = \{(q^3, q^2, q), (q^3, q^2 - q, 2q)\}.
\]

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

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

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

- The dual arc has the same parameters.
Values of $m_n(R^3_R)$ for Hjelmslev planes of order $q^2 = 4$ and $q^2 = 9$

<table>
<thead>
<tr>
<th>$n/R$</th>
<th>$\mathbb{Z}_4$</th>
<th>$\mathbb{F}_2[X]/(X^2)$</th>
<th>$\mathbb{Z}_9$</th>
<th>$\mathbb{F}_3[X]/(X^2)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>7</td>
<td>6</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>10</td>
<td>19</td>
<td>18</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>39</td>
<td>38</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td>49</td>
<td>50</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td>69</td>
<td>69</td>
</tr>
</tbody>
</table>
4. Blocking Sets in \( \text{PHG}(R^3_R) \)

4.1. General results

**Theorem.** \( R \) finite chain ring with \( |R| = q^m \), \( R/\text{rad } R \cong \mathbb{F}_q \). The minimal size of a \((k, n)\)-blocking set in \( \text{PHG}(R^3_R) \) 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 $\cong \text{PG}(2, q)$

(2) Lines: $\ell_0$, $\ell_1$ with $\ell_0 \cap \ell_1$, $X \in \ell \setminus \ell_0$.

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

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

(1) $\text{Supp } \mathcal{R}$ is a projective plane of order $q$, or else

(2) $\mathcal{R}$ is a blocking set of the type (2).

If $R = \text{GR}(q^2, p^2)$, then $\mathcal{R}$ is of the type (2).
4.2. Rédei-type Blocking Sets in $\text{PHG}(R^3_R)$

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

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

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

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

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

All points outside this class: $(x, y, 1)$, $x, y \in R$. 
The points of \( \text{AHG}(R^2_R) \): \((x, y)\), where \( x, y \in R \).

The lines of \( \text{AHG}(R^2_R) \):

- \( Y = aX + b, \ a, b \in R \);
- \( X = cY + d, \ d \in R, \ c \in \text{rad} \ R \).

**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 \( \infty_j \), if \( c = \theta \gamma_j, \ j = 0, 1, \ldots, q - 1 \).

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

**Definition.** \((a)\) (resp. \((\infty_j)\)) will denote the infinite point from \( Z = 0 \) of the lines with slope \( a \) (resp. \( \infty_j \)).
Definition. Let $U$ be a set of $q^2$ points in $AHG(R_R^2)$. 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 $PHG(R_R^3)$.

Theorem. Let $U$ be a set of $q^2$ points in $AHG(R_R^2)$. 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 $PHG(R_R^3)$ 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 $PHG(R_R^3)$. 
**Definition.** A blocking set of size $q^2 + u$ is said to be of Rédei type if there exists a line $\ell$ 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 $f : R \to R$. Let $P = (x, f(x))$ and $Q = (y, f(y))$ be two different points from $U$. We have the following possibilities:
1) if \( x - y \not\in \text{rad} \, R \) then \( P \) and \( Q \) determine the point \((a)\), where

\[
(a) = (f(x) - f(y))(x - y)^{-1}.
\]

2) if \( x - y \in \text{rad} \, R \setminus \{0\} \), and \( f(x) - f(y) \not\in \text{rad} \, R \) the points \( P \) and \( Q \) determine the point \((\infty_i)\) if

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

3) if \( x - y \in \text{rad} \, R \setminus \{0\} \), and \( f(x) - f(y) \in \text{rad} \, R \), 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 \( c \in ba^{-1} + \text{rad} \, R \).
Example 1.

\[ f : a + \theta b \to b + \theta a. \]

over \( R_\sigma : q + 1 \) directions;

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

Theorem. Let $R = GR(q^2, p^2)$, $q = p^m$, $p$ 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 $AHG(R^2_R)$.

In particular, there exists a Rédei type blocking set in $PHG(R^3_R)$ of size

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

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

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

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

\( \text{Aut} \, R \) is cyclic of order \( s \):

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

\( S = \text{GR}(q^{2m}, p^2) \).
Aut(S : R) is cyclic of order m and is generated by

\[ \sigma_0(\alpha) = a_0^q + a_1^q \beta. \]

The trace function \( \text{Tr}_{S:R} : S \rightarrow R \) is defined by

\[ \text{Tr}_{S:R}(x) = \sum_{\sigma \in \text{Aut}(S:R)} \sigma(x). \]

Properties:

1. for all \( \alpha \in S \) and for all \( a \in R \): \( \text{Tr}_{S:R}(a\alpha) = a \text{Tr}_{S:R}(\alpha); \)

2. for all \( \alpha, \beta \in S \): \( \text{Tr}_{S:R}(\alpha + \beta) = \text{Tr}_{S:R}(\alpha) + \text{Tr}_{S:R}(\beta); \)
(3) for all \( c \in \text{rad } S \), \( \text{Tr}_{S:R}(c) \in \text{rad } R \);

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

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

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

Define

\[
f(x) = \text{Tr}_{S:R}(x)
\]
**Theorem.** Let \( R = \text{GR}(q^2, p^2) \) 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 \( f(x) = \text{Tr}_{S:R}(x) \) determines

\[
\frac{q^m - 1}{q - 1} q^m
\]

directions in \( \text{AHG}(S^2_S) \). There exists a Rédei type blocking set in \( \text{PHG}(S^3_S) \) of size

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