Blocking Sets of Rédei type in Projective Hjelmslev Planes

Ivan Landjev[1] Stoyan Boev[2]

[1]Department of Informatics, New Bulgarian University
and
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences

[2]Department of Informatics, New Bulgarian University

June 16–22, 2008 / XI International Workshop on ACCT, Pamporovo

Outline

1. Chain rings
2. Projective Hjelmslev Planes over finite chain rings
   - The structure of PHG(R_R^3)
   - The affine planes AHG(R_R^2)
3. Blocking sets in PHG(R_R^3)
   - Definition
   - Bounds of blocking sets in PHG(R_R^3)
4. Blocking Sets of Rédei type in PHG(R_R^3)
   - Definition
   - Construction and examples

Finite chain rings

Definition

An associative ring with identity ($1 \neq 0$) is called a left (right) chain ring if the lattice of its left (right) ideals forms a chain.

$$R > R\theta > \ldots > R\theta^m = (0)$$

Fact

If R is a finite chain ring, then every proper left(right) ideal of R has the form $R\theta^i = \theta^i R$, for some positive integer i. If $\theta \in \operatorname{rad} R \setminus (\operatorname{rad} R)^2$, then $\operatorname{rad} R = R\theta$.

Example

$\mathbb{Z}_4 = \{0, 1, 2, 3\} > \operatorname{rad} \mathbb{Z}_4 = \{0, 2\} > (0)$

Chain rings of nilpotency index 2

$$R\colon\ R > \operatorname{rad} R > (0),\ \ R/\operatorname{rad} R \cong \mathbb{F}_q,\ \ |R| = q^2$$

Fact

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 – $(x_0 + x_1 t) + (y_0 + y_1 t) = (x_0 + y_0) + (x_1 + y_1)t$,
  multiplication – $(x_0 + x_1 t)(y_0 + y_1 t) = x_0 y_0 + (x_0 y_1 + x_1 y_0^\sigma)t$;
- *the Galois ring $\operatorname{GR}(q^2, p^2) = \mathbb{Z}_{p^2}[X]/(f(X))$, where $f(X)$ is monic polynomial of degree r, irreducible mod p.*

Projective Hjelmslev Plane PHG(R_R^3)

- $M = R_R^3$; $M^* := M \setminus M\theta$;
- $\mathcal{P} = \{xR \mid x \in M^*\}$;
- $\mathcal{L} = \{xR + yR \mid x, y \in M^*, x, y \text{ linearly independent}\}$;
- $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{L}$ – incidence relation;
- $\bigcirc$ - neighbour relation:

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

  (N2) $s \bigcirc t$ if $\exists X, Y \in \mathcal{P}, X \neq Y$: $X\mathcal{I}s, Y\mathcal{I}s, X\mathcal{I}t, Y\mathcal{I}t$.

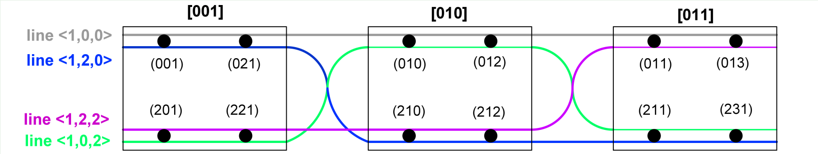
Definition

The incidence structure $\Pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ with neighbour relation $\bigcirc$ is called the (right) projective Hjelmslev plane over the chain ring R and we denote it by PHG(R_R^3).

Combinatorics in PHG(R_R^3)

- $|\mathcal{P}| = |\mathcal{L}| = q^2(q^2 + q + 1)$
- Every point (line) is incident with $q(q + 1)$ lines (points).
- Every point (line) has q^2 neighbours;
- Given a point P and a line ℓ containing P there exist q points on ℓ that are neighbours to P and, dually, exactly q lines through P that are neighbours to ℓ.

Example ($R = \mathbb{Z}_4$)



The structure of PHG(R_R^3)

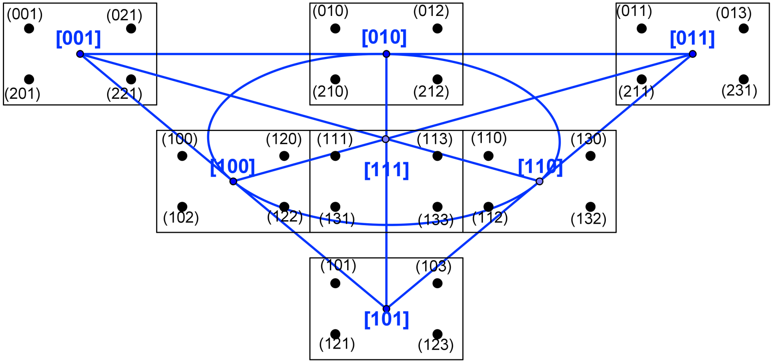
- $[P]$ – class of all neighbours to P;
  $[\ell]$ – class of all neighbours to ℓ;
- $\mathcal{P}'$ – the set of all neighbour classes of points;
- $\mathcal{L}'$ – the set of all neighbour classes of lines.
- $\mathcal{I}' \subseteq \mathcal{P}' \times \mathcal{L}'$ - incidence relation, defined by
  $\mathcal{I}' : [P]\mathcal{I}'[\ell] \Leftrightarrow \exists P_0 \in [P], \exists \ell_0 \in [\ell], P_0 \mathcal{I} \ell_0.$

Theorem

The incidence structure $(\mathcal{P}', \mathcal{L}', \mathcal{I}')$ *is isomorphic to the projective plane* PG$(2, q)$.

The structure of PHG(R_R^3)

Example ($R = \mathbb{Z}_4$)



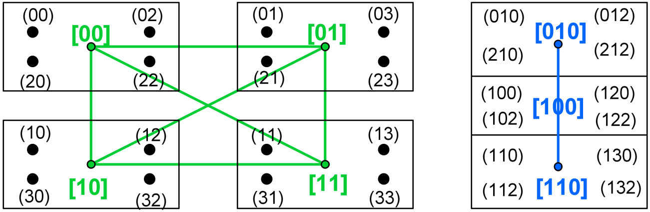
The structure of AHG(R_R^2)

AHG(R_R^2)

Points $\{(x, y) \mid x, y \in R\}$

Lines $\{Y = aX + b \mid a, b \in R\}$
$\{cY = X + b \mid c \in \operatorname{rad} R, b \in R\}$

Example ($R = \mathbb{Z}_4$)



Slopes of lines in AHG(R_R^2)

Fact

Let $\Gamma = \{\gamma_0 = 0, \gamma_1 = 1, \gamma_2, \ldots, \gamma_{q-1}\}, \gamma_i \not\equiv \gamma_j \mod \operatorname{rad} R$. *Then each element* r *of the chain ring* R *can be represented uniquely in the form* $r = a + \theta b$, *where* $\theta \in \operatorname{rad} R \setminus \{0\}$ *and* $a, b \in \Gamma$.

Definition

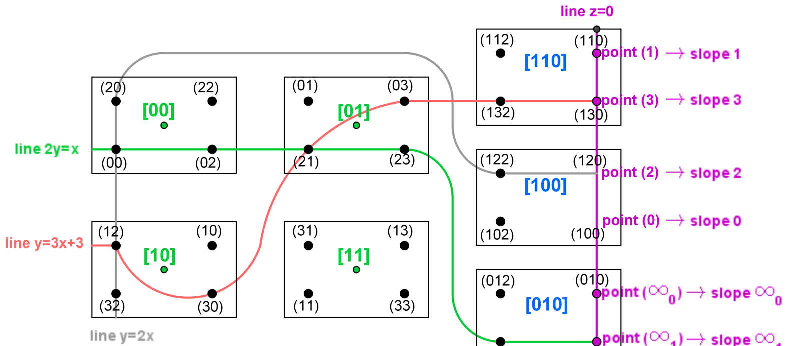
A line of type

$Y = aX + b$ has slope a

$cY = X + b$ has slope ∞_j, where $c = \gamma_i + \theta\gamma_j$

Slopes in AHG(R_R^2)

Example ($R = \mathbb{Z}_4$)



Definition

Definition

The pointset $\mathfrak{B} \subseteq \mathcal{P}$ is called a *k-blocking set* if

- $|\mathfrak{B} \cap \mathcal{P}| = k$,
- $|\mathfrak{B} \cap \ell| \geq 1$ for any line $\ell \in \mathcal{L}$,
- there exists a line ℓ_0 with $|\mathfrak{B} \cap \ell_0| = 1$.

Definition

The blocking set $\mathfrak{B}$ is called irreducible if $\mathfrak{B} \setminus P$ is not a blocking set for every point $P \in \mathfrak{B}$.

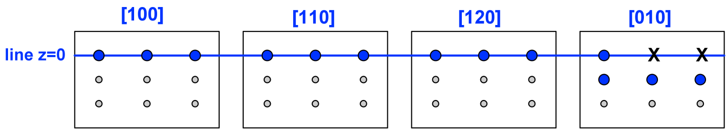
Theorem

Let R be a finite chain ring with $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. The minimal size of a blocking set $\mathfrak{B}$ in $\mathrm{PHG}(R_R^3)$ is $q(q+1)$ and then $\mathfrak{B}$ is a line.

Theorem

There exists an irreducible blocking set in $\mathrm{PHG}(R_R^3)$ of size $q^2 + q + 1$.

Example ($R = \mathbb{Z}_9$)

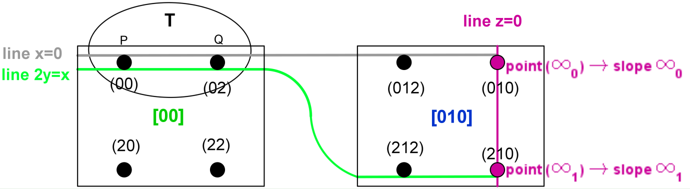


Blocking Sets of Rédei type in PHG(R_R^3)

Definition

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

Example ($R = \mathbb{Z}_4$, $T = \{(00), (02)\}$)



Blocking Sets of Rédei type in PHG(R_R^3)

Theorem

Assume T is a set of q^2 points in AHG(R_R^2)*, no two of which are neighbours. Denote by D the set of infinite points determined by T. If $|D| < q^2 + q$ then $B = T \cup D$ is an irreducible blocking set in* PHG(R_R^3).

Definition

A blocking set of size $q^2 + m$ in PHG(R_R^3) is said to be of Rédei type if it has an m-secant. Such a line is called a Rédei line.

Construction of T

If $f : R \to R$ then $T = \{(x, f(x)) \mid x \in R\}$.

The directions determined by T

If $P(x, f(x))$ and $Q(y, f(y))$ are two different points in T, then $\{P, Q\}$ determine the following directions:

1) if $x - y \notin \operatorname{rad} R \to$ point (a),
   where $a = (f(x) - f(y))(x - y)^{-1}$
2) if $x - y \in \operatorname{rad} R \setminus \{0\}$ and $f(x) - f(y) \notin \operatorname{rad} R \to$ point (∞_i),
   where $(x - y)(f(x) - f(y))^{-1} = \theta\gamma_i, \gamma_i \in \Gamma$.
3) if $x - y = \theta\alpha \in \operatorname{rad} R \setminus \{0\}$ and $f(x) - f(y) = \theta\beta \in \operatorname{rad} R$,
   a) $\beta \neq 0 \to$ class of all points (c) with $c \in \alpha\beta^{-1} + \operatorname{rad} R$;
   b) $\beta = 0 \to$ class of all infinite points (∞_i) with $i = 0, \ldots, q - 1$.

Example

Let $f : \begin{cases} R & \to & R \\ a+\theta b & \to & b+\theta a \end{cases}$ and consider the set of points $T = \{(x, f(x)) \mid x \in R\}$

- If $R = R_\sigma = \mathbb{F}_q \oplus \mathbb{F}_q t$, for some $\sigma \in \operatorname{Aut} \mathbb{F}_q$, then T determines $q+1$ infinite points.
- If $R = \mathrm{GR}(q^2, p^2)$, then T determines $q^2 - q + 2$ infinite points.