Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 166-170*

Blocking sets of Rédei type in projective Hjelmslev planes

IVAN LANDJEV ivan@math.bas.bg
Institute of Mathematics and Informatics Bulgarian Academy of Sciences,
8 G. Bonchev str., 1113 Sofia, BULGARIA
New Bulgarian University, 21 Montevideo str., 1618 Sofia, BULGARIA
STOYAN BOEV stoyan@nbu.bg
New Bulgarian University, 21 Montevideo str., 1618 Sofia, BULGARIA

1 Preliminary results

The aim of this paper is to generalize the notion of a Rédei type blocking set to projective Hjelmslev planes.

In what follows, we focus on Hjelmslev planes over chain rings of nilpotencey index 2, i.e. chain rings with rad $R \neq (0)$ and $(\text{rad } R)^2 = (0)$. Thus we have always $|R| = q^2$, where $R/\text{rad } R \cong \mathbb{F}_q$. Chain rings with this property have been classified in [1, 6]. If $q = p^r$ there are exactly $r+1$ isomorphism classes of such rings. These are:

- for every $\sigma \in \text{Aut } \mathbb{F}_q$ the ring $R_\sigma \cong \mathbb{F}_q[X;\sigma]/(X^2)$ of the so-called σ-dual numbers over $\mathbb{F}_q$ with underlying set $\mathbb{F}_q \times \mathbb{F}_q$, component-wise addition and multiplication given by $(x_0, x_1)(y_0, y_1) = \big(x_0y_0, x_0y_1 + x_1y_0^\sigma\big)$;
- the Galois ring $\text{GR}(q^2, p^2) \cong \mathbb{Z}_{p^2}[X]/(f(X))$, where $f(X) \in \mathbb{Z}_{p^2}[X]$ is a monic polynomial of degree r, which is irreducible modulo p.

The rings R_σ with $\sigma \neq \text{id}$ are noncommutative, while R_{id} is commutative. We have also that char $R_\sigma = p$ for every σ. The Galois ring $\text{GR}(q^2, p^2)$ is commutative and has characteristic p^2. From now on we denote by R a finite chain ring of nilpotency index 2.

In order to save space, we refer to [2, 3, 4] for the basic definitions and results about projective Hjelmslev planes over finite chain rings. We denote by $\text{PHG}(R_R^3)$ the (right) projective Hjelmslev plane over the chain ring R. Similarly, $\text{AHG}(R_R^2)$ denotes the (right) affine Hjelmslev plane over R.

Let $\Pi = (\mathcal{P}, \mathcal{L}, I)$ be a projective Hjelmslev plane. Any mapping from the pointset $\mathcal{P}$ to the nonnegative integers $\mathfrak{K} : \mathcal{P} \to \mathbb{N}_0$ is called a *multiset* in Π. The integer $\mathfrak{K}(P)$, $P \in \mathcal{P}$, is called the multiplicity of P. The mapping $\mathfrak{K}$ induces a mapping on the subsets of $\mathcal{P}$ by

$$\mathfrak{K}(\mathcal{Q}) = \sum_{P \in \mathcal{Q}} \mathfrak{K}(P), \quad \mathcal{Q} \subseteq \mathcal{P}.$$

The induced mapping is denoted again by $\mathfrak{K}$. The integer $|\mathfrak{K}| = \mathfrak{K}(\mathcal{P})$ is called the *cardinality* or the *size* of $\mathfrak{K}$. The support supp $\mathfrak{K}$ of a multiset $\mathfrak{K}$ is the set of points of positive multiplicity: supp $\mathfrak{K} = \{P \in \mathcal{P} \mid \mathfrak{K}(P) > 0\}$.

Two multisets $\mathfrak{K}'$ and $\mathfrak{K}''$ in the projective Hjelmslev plane Π are said to be equivalent if there exists a collineation σ in Π such that $\mathfrak{K}'(P) = \mathfrak{K}''(\sigma(P))$ for every point $P \in \mathcal{P}$.

Definition 1.1. *A multiset $\mathfrak{K}$ in $(\mathcal{P}, \mathcal{L}, I)$ is called a (k, n)-*blocking multiset *if*

(i) $\mathfrak{K}(P) = k$;

(ii) $\mathfrak{K}(\ell) \geq n$ for every line $\ell \in \mathcal{L}$;

(iii) there exists at least one line ℓ_0 with $\mathfrak{K}(\ell_0) = n$.

A (k, n)-blocking multiset $\mathfrak{K}$ is called *reducible* if there exists (k', n)-blocking multiset $\mathfrak{K}'$ with $k' < k$ and $\mathfrak{K}'(P) \leq \mathfrak{K}(P)$ for every point $P \in \mathcal{P}$. A blocking multiset that is not reducible is called *irreducible*.

A major problem is to determine the possible sizes of the irreducible blocking sets in the planes $\mathrm{PHG}(R^3_R)$, where R is a chain ring of nilpotency index 2. It is known that the minimal size of a blocking set in $\mathrm{PHG}(R^3_R)$, $|R| = q^2$, is $q^2 + q$.

2 Blocking sets of Rédei type in projective Hjelmslev planes

Until the end of the paper R will be a chain ring of nilpotency index 2, i.e. $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$, where q is a prime power. We denote by $\Gamma = \{\gamma_0 = 0, \gamma_1 = 1, \gamma_2, \ldots, \gamma_{q-1}\}$ a set of q elements of R no two of which are congruent modulo rad R. By θ we denote an arbitrary element of rad $R \setminus (0)$. The points of the affine plane $\mathrm{AHG}(R^2_R)$ are identified with the pairs (x, y), where $x, y \in R$. The lines of $AHG(R^2_R)$ have equations $Y = aX + b$ or $X = c$, $a, b, c \in R$. We say that the lines of the first type have slope a. A line with equation $X = c$ is said to have slope ∞_j, if $c = \gamma_i + \gamma_j\theta$, $j = 0, 1, \ldots, q-1$.

The infinite points on a fixed line ℓ from the neighbor class of infinite lines can be identified with the slopes. So, (a) (resp (∞_j)) will denote the infinite point from ℓ of the lines with slope (a) (resp (∞_j)).

Definition 2.1. *Let T be a set of q^2 points in $\mathrm{AHG}(R^2_R)$. 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 $\mathrm{PHG}(R^3_R)$.*

Theorem 2.2. *Assume T is a set of q^2 points in $\mathrm{AHG}(R^2_R)$. 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 $\mathrm{PHG}(R^3_R)$.*

The proof of this theorem is obvious.

The construction given by this theorem yields blocking sets of size at most $2q^2 + q - 1$. It is straightforward that every irreducible blocking set of size at most $2q^2 + q - 1$ with a line ℓ with $|B \setminus \ell| = q^2$ can be obtained by this construction.

Definition 2.3. *A blocking set of size q^2+m in $\mathrm{PHG}(R_R^3)$ is said to be of Rédei type if it has an m-secant. Such a line is called a Rédei line.*

We are interested in sets T that are the graph of a function $f\colon R \to R$. Such sets can be written in the form

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

Let x and y be two different elements from R We now have the following possibilities:

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

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

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

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

3) if $x-y \in \mathrm{rad}\ R\setminus\{0\}$, and $f(x)-f(y) \in \mathrm{rad}\ R$, say $x-y = \theta a$, $f(x)-f(y) = \theta b$, $a, b \in \Gamma$.

   a) if $b \neq 0$, $(x, f(x))$ and $(y, f(y))$ determine all points (c) with $c \in a/b + \mathrm{rad}\ R$;

   b) if $b = 0$, $(x, f(x))$ and $(y, f(y))$ determine the infinite points $(\infty_0), \ldots, (\infty_q)$.

Furthermore, for every set T of point of $\mathrm{AHG}(R_R^2)$ of size q^2 determining at most $q^2 + q - 1$ directions, we can always choose the coordinate system so that T is the graph of a function from R to R.

3 Examples

Let R be a chain ring with $|R| = q^2$, $R/\,\mathrm{rad}\ R \cong \mathbb{F}_q$ that contains a proper subring isomorphic to its residue field $\mathbb{F}_q$ Then $R = \mathbb{F}_q[\theta; \sigma]$ for some $\sigma \in \mathrm{Aut}\ \mathbb{F}_q$.

It has been noted in [5] that $\mathrm{PHG}(R_R^3)$ contains a subgeometry isomorphic to $\mathrm{PG}(2, q)$ which is an irreducible blocking set with two intersection numbers. As noted at the end of the previous section, this blocking set is of Rédei type.

Below we give an explicit construction of this blocking set as a graph of a function from R to R.

Define

$$f : \begin{cases} R & \to & R \\ a+\theta b & \to & b+\theta a \end{cases} . \tag{1}$$

We shall check that the set of points $T = \{(x, f(x)) \mid x \in R\}$ determines $q+1$ infinite points. Consider the points $P = (a+\theta b, b+\theta a)$ and $Q = (c+\theta d, d+\theta c)$, $a, b, c, d \in \Gamma = \mathbb{F}_q$.

1) Let $a = c$. Then $b \neq d$ since otherwise P and Q would coincide. We have

$$x - y = \theta(b-d), \quad f(x) - f(y) = b - d.$$

Hence P and Q determine the infinite point (∞_1).

2) Let $a \neq c$. We have

$$\begin{aligned}(f(x) \quad &- \quad f(y))(x-y)^{-1} = \\ &= ((b-d)+\theta(a-c))((a-c)+\theta(b-d))^{-1} \\ &= ((b-d)+\theta(a-c))((a-c)^{-1} - \theta(((a-c)^{\sigma})^{-1}(b-d)(a-c)^{-1} \\ &= (b-d)(a-c)^{-1} - \theta(b-d)^{\sigma}((a-c)^{\sigma})^{-1}(b-d)(a-c)^{-1}.\end{aligned}$$

Assume that $P' = (a'+\theta b', b'+\theta a')$ and $Q' = (c'+\theta d', d'+\theta c')$ are two point that determine an infinite point which is a neighbour to the infinite point determined by P and Q. Then $(b-d)(a-c)^{-1} = (b'-d')(a'-c')^{-1}$ which implies that

$$\begin{aligned}&(b-d)(a-c)^{-1} - \theta(b-d)^{\sigma}((a-c)^{\sigma})^{-1}(b-d)(a-c)^{-1} = \\ &\qquad (b'-d')(a'-c')^{-1} - \theta(b'-d')^{\sigma}((a'-c')^{\sigma})^{-1}(b'-d')(a'-c')^{-1}.\end{aligned} \tag{2}$$

Hence if P, Q on one side and P', Q' on the other determine infinite points that are neighbours, then they determine the same infinite point. Therefore, the points of T determine at most one point in each neighbour class of infinite points. On the other hand, $(b-a)(c-d)^{-1}$ runs all elements of $\mathbb{F}_q$ (take, for instance $a = 1, c = d = 0$, b free). Therefore exactly one infinite point is determined in each neighbour class. Hence the points of T determine exactly $q+1$ directions.

It is known that the projective Hjelmslev plane $\mathrm{PHG}(R^3_R)$, where $R = \mathrm{GR}(q^2, p^2)$, does not contain a subplane isomorphic to $\mathrm{PG}(2, q)$. It is interesting to know what are the parameters of the Rédei-type blocking sets given by (1). Let us note that (1) depends on the choice of Γ. Let $R = \mathbb{Z}_{p^2}/(f(X))$, where F is a monic polynomial of degree $n \geq 1$, that is irreducible over $\mathbb{Z}_p$. Then $|R| = p^{2n}$ and rad $R = (p)$. If

$$\Gamma = \{\gamma_0 \in \text{rad } R, \gamma_1 \in 1 + \text{rad } R, \gamma_2, \ldots, \gamma_{q-1}\},$$

where $\gamma_i - \gamma_j \notin \text{rad } R$, for $0 \leq i < j \leq q-1$, it can be shown that the set T determines exactly $q^2 - q + 2$ directions and the size of the corresponding Rédei-type blocking set is $2q^2 - q + 2$.

Let $P = (a + bp, b + ap)$ and $Q = (c + dp, d + cp)$, where $a, b, c, d \in \Gamma$. If $a = c$ and $b \neq d$, the points P and Q determine the infinite point (∞_1). If $a \neq c$, they determine the infinite point (α) with

$$\alpha = \frac{b-d}{a-c} + \left(1 - \frac{(b-d)^2}{(a-c)^2}\right) p. \tag{3}$$

The number of different directions determined by the points of T is equal to the different values taken by $\frac{b-d}{a-c}$, $a \neq c$. In the special case $b = d$, we have $(\alpha) = (p)$.

Now we are going to prove that if for every $\alpha \in R \setminus \text{rad } R$ there exist $a, b, c, d \in \Gamma$ such that $\alpha(a - b) = c - d$. Consider the elements $\alpha x + y$ where $x, y \in \Gamma$. If $\{\alpha x + y | x, y \in \Gamma\} = R$, there is nothing to prove. Otherwise, there exist $x_1, x_2, y_1, y_2 \in \Gamma$, $(x_1, y_1) \neq (x_2, y_2)$ such that

$$\alpha x_1 + y_1 = \alpha x_2 + y_2.$$

Hence $\alpha(x_1 - x_2) = y_2 - y_1$. Since $x_1 - x_2 \in \text{rad } R$ implies $x_1 = x_2$ and, similarly, $y_1 - y_2 \in \text{rad } R$ implies $y_1 = y_2$. If one of the differences $x_1 - x_2$, $y_2 - y_1$ is 0 then the other is also 0, which is a contradiction. Hence it is enough to set $a = x_1, b = x_2, c = y_1, d = y_2$.

References

[1] A. Cronheim, Dual numbers, Witt vectors, and Hjelmslev planes, *Geom. Dedic.* 7, 1978, 287-302.

[2] T. Honold, I. Landjev, Projective Hjelmslev geometries, *Proc. Second Intern. Workshop OCRT*, Sozopol, Bulgaria, 1998, 116-126.

[3] T. Honold, I. Landjev. On arcs in projective Hjelmslev planes, *Discr. Math.* 231, 2001, 265-278.

[4] T. Honold, I. Landjev, Arcs in projective Hjelmslev planes, *Discr. Math. Appl.* 11, 2001, 53-70.

[5] I. Landjev, On blocking sets in projective Hjelmslev planes, *Adv. Math. Commun.* 1, 2007, 65-82.

[6] R. Raghavendran, Finite associative rings, *Compos. Math.* 21, 1969, 195-229.