THE GENERALIZATION OF SOME CONSTRUCTIONS BY MÉGYESI TO HJELMSLEV PLANES

Stoyan Boev

New Bulgarian University

Ivan Landjev

Institute of Mathematics and Informatics, BAS

– XII International Workshop on ACCT, Novosibirsk, Russia, 05.-11.09.2010 –

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.

Theorem. For a finite ring R with radical $N \neq 0$ the following conditions are equivalent.

(i) R is a left chain ring;

(ii) the principal ideals form a chain;

(iii) R is a local ring and $N = R\theta$ for any $\theta \in N \setminus N^2$;

(iv) R is a right chain ring.

Moreover, if R satisfies the above conditions, every proper left (right) ideal of R has the form $N^i = R\theta^i = \theta^i R$, for some $i \in \mathbb{N}$.

W.E. Clark, D.A. Drake, Abh. aus dem Math. Sem. der Univ. Hamburg **39**(1974), 147–153.

B. McDonald, *Finite rings with identity*, 1974.

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 –

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

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

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

Projective and affine Hjelmslev planes

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

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

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

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

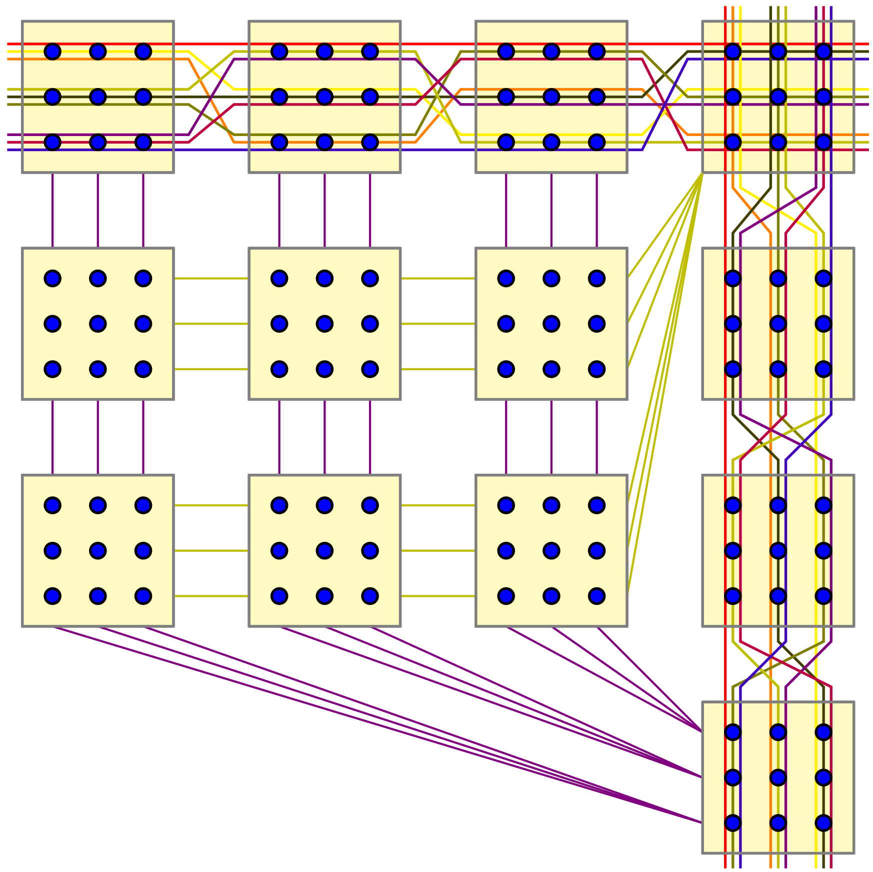
Notation: $\mathrm{PHG}(R^3_R)$

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.

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



$\mathrm{AHG}(R^2_R)$

Points: (x, y), $x, y \in R$

Lines: $Y = aX + b$, $X = cY + d$, $a, b, d \in R$, $c \in \mathrm{rad}\, R$

The line $Y = aX + b$ has slope a;

the line $X = cY + d$ has slope ∞_j if $c = \theta\gamma_j$, $\gamma_j \in \Gamma$

$\Gamma(R)$ – a set of q elements of R no two of which are congruent modulo $\mathrm{rad}\, R$

Multisets of points

Definition. A **multiset** in $\Pi = (\mathcal{P}, \mathcal{L}, I) = \mathrm{PHG}(R_R^3)$ is defined as a mapping

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

- $\mathcal{Q} \subset \mathcal{P}$: $\mathfrak{K}(\mathcal{Q}) = \sum_{x \in \mathcal{Q}} \mathfrak{K}(x)$.

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

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

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

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

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

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

Corollary. The minimal size of a $(n,1)$-blocking set is $q^{m-1}(q+1)$. In case of equality, it consists of the points of a line.

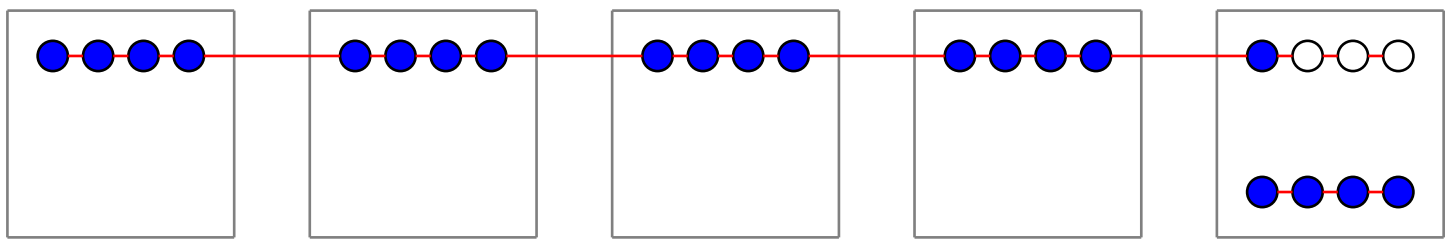
Blocking Sets with $n = q^2 + q + 1$

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

(2) Lines: ℓ_0, ℓ_1 with $\ell_0 \frown \ell_1$; $x \in \ell_0 \setminus \ell_1$.

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

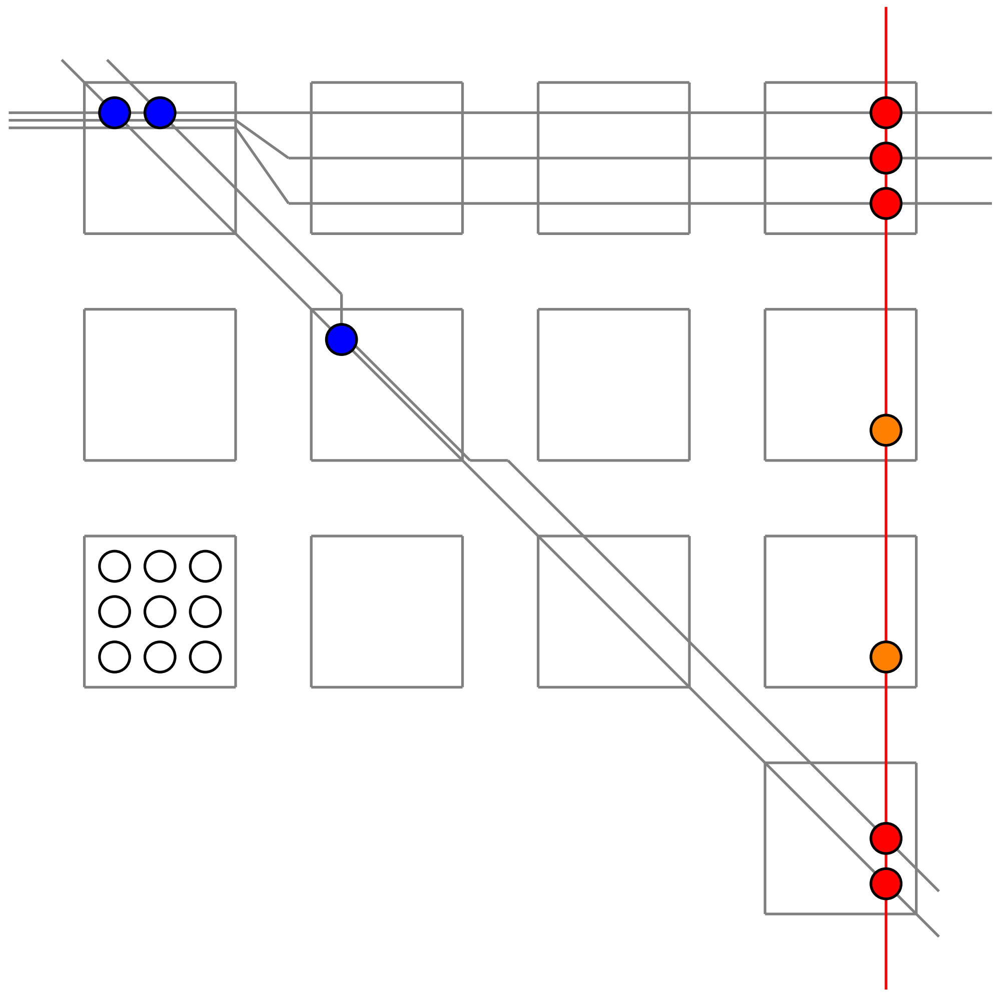
Theorem. Let $\mathfrak{K}$ be an irreducible $(q^2 + q + 1, 1)$-blocking set in $\mathrm{PHG}(R_R^3)$, $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Then either $\operatorname{Supp} \mathfrak{K}$ is a projective plane of order q or else $\mathfrak{K}$ is a blocking set of the type (2). If $R = \mathrm{GR}(q^2, p^2)$, then $\mathfrak{K}$ is of the type (2).



Rédei-type Blocking Sets in $\mathrm{PHG}(R_R^3)$

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:

Let $x, y \in R$, $x \neq y$. We have the following possibilities:

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

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

2) If $x - y \in \operatorname{rad} R \setminus \{0\}$, and $f(x) - f(y) \notin \operatorname{rad} R$ 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 $x - y = \theta a \in \operatorname{rad} R \setminus \{0\}$, and $f(x) - f(y) = \theta b \in \operatorname{rad} R$, $a, b \in \Gamma$

a) if $b \neq 0$, $(x, f(x))$ and $(y, f(y))$ determine all points (c) with $c \in ab^{-1} + \operatorname{rad} R$;

b) if $b = 0$, $(x, f(x))$ and $(y, f(y))$ determine the points $(\infty_0), \ldots, (\infty_{q-1})$.

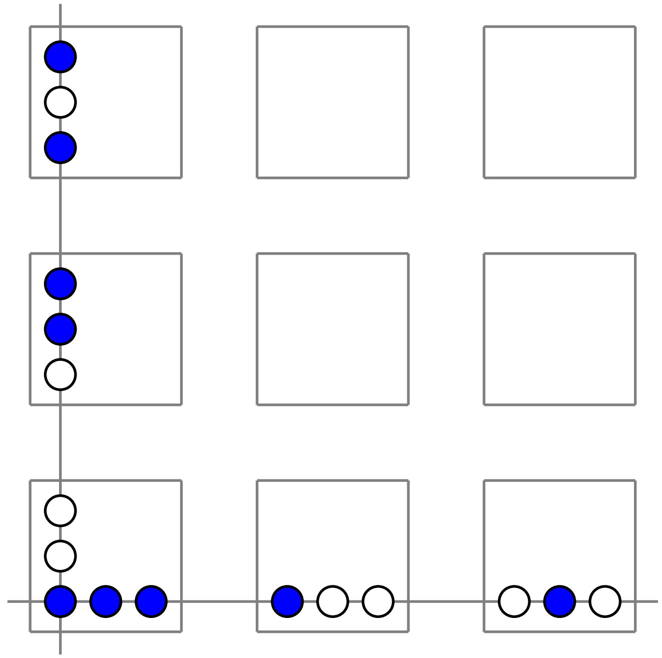
Theorem A. Let R be a chain ring with $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Let G be a subgroup of R^* with $q-1 < |G| < q^2 - q$. Define the pointset U by

$$U = \{(a\theta, 0) \mid a \in \Gamma\} \cup \{(a, 0) \mid a \in G\} \cup \{(0, b) \mid b \in R^* \setminus G\}. \qquad (1)$$

The number of directions determined by U is $q^2 + q - |G|$. There exists a blocking set of Rédei type of size at most

$$2q^2 + q - |G| + |H|,$$

where $H = \nu(G)$ is the homomorphic image of G under the natural homomorphism $\nu : R \to R/\operatorname{rad} R$.



In the case of Galois rings $R = \mathrm{GR}(q^2, p^2)$, $q = p^r$,

$$R^* = G_1 \times C_p \times \ldots \times C_p,$$

where G_1 is a cyclic group of order $q - 1$ and r cyclic groups of order p.

If we take G to be a subgroup of R^* containing G_1 then $|D^{(1)}| = q + 1$.

For example, if $|G| = (q^2 - q)/p$ then we get a blocking set B of size

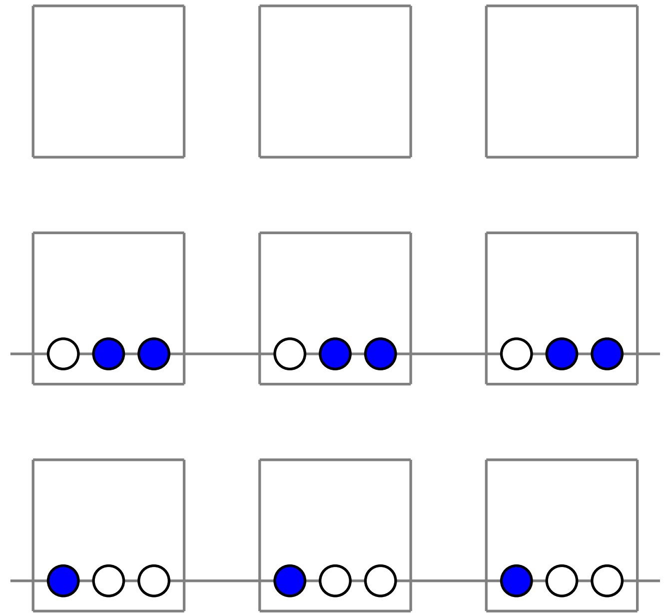
$$|B| = (2 - \frac{1}{p})q^2 + (1 + \frac{1}{p})q.$$

In the case of $p = 2$, we get $|B| = 3/2(q^2 + q)$.

Theorem B. Let G be a proper subgroup of $(R,+)$ with $q < |G| < q^2$. Define

$$U = \{(a,0) \mid a \in G\} \cup \{(b,1) \mid b \notin G\}. \tag{2}$$

The number of directions determined by U is $q^2 + 2q - |G|$. Consequently, there exist blocking sets of Rédei type of size at most $2q^2 + 2q - |G|$.



If G is a group of order q^2/p with $R = \langle G \cup \operatorname{rad} R \rangle$ then $\mathbb{G}/G \cap \operatorname{rad} R \cong R/\operatorname{rad} R$ and the blocking set in question has size

$$(2 - \frac{1}{p})q^2 + 2q,$$

which in case of $p = 2$ gives size

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