Caps in projective Hjelmslev spaces over finite chain rings of nilpotency index 2

Thomas Honold Ivan Landjev*

Abstract

We investigate caps in the projective Hjelmslev geometries $\mathrm{PHG}(R_R^k)$ over chain rings R with $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. We present a geometric construction for caps using ovoids in the factor geometry $\mathrm{PG}(3,q)$ as well as an algebraic construction that makes use of the Teichmüller group of units in the Galois extension of certain chain rings. We prove upper bounds on the size of a maximal cap in $\mathrm{PHG}(R_R^4)$. It has an order of magnitude q^4. This bound extends to higher dimensions, but gives the rather rough estimate q^{2k-4}.

Keywords: projective Hjelmslev plane, cap, arc, oval, hyperoval, linear code, finite chain ring
MSC 2000: 51E26, 51E21, 51E22, 94B05

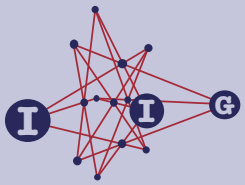
1. Introduction

In this paper, we will investigate caps in the projective Hjelmslev geometries $\mathrm{PHG}(R_R^k)$. There exists an extensive literature about caps in the projective geometries $\mathrm{PG}(k,q)$. The same objects in Hjelmslev geometries have attracted little or no attention despite the obvious connections to interesting areas as linear codes over finite chain rings.

We restrict ourselves to geometries over chain rings with q^2 elements and residue field of order q. The reason for this is threefold. Geometries over rings are structures that have less regularities than the usual projective geometries. Taking the simplest possible chain rings, and hence the Hjelmslev geometries

*This research has been supported by the Bulgarian NSRF under Contract M-1405/04.

ACADEMIA PRESS
UNIVERSITEIT GENT



with the simplest possible structure, we settle for a problem that is to some extent tractable. Secondly, the nested structure of the projective Hjelmslev geometries implies that results about caps in geometries over rings of large nilpotency index will necessarily depend on results in geometries over ring with a smaller index. Finally, there exists a classification for the chain rings R with $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$.

There is some interest in this problem that comes from coding theory. The existence of a cap in a projective Hjelmslev geometry over $\mathbb{Z}_4$ implies the existence of a corresponding linear code over $\mathbb{Z}_4$ ("cap code") with dual Lee distance at least four. Cap codes over other chain rings satisfy a similar lower bound for the dual homogeneous distance. Large caps are associated to codes that are usually good.

In Section 2 we give some basic facts about finite chain rings and projective Hjelmslev geometries over such rings. In Section 3 we present several constructions for caps. In Section 4, we derive bounds on the size of a cap in the projective Hjelmslev geometries $\mathrm{PHG}(R_R^k)$.

2. Basic facts on projective Hjelmslev geometries

A finite ring R (associative, with identity $1 \neq 0$, ring homomorphisms preserving the identity) is called a left (resp. right) chain ring if its lattice of left (resp. right) ideals forms a chain. It turns out that every left ideal is also a right ideal. Moreover, if $N = \operatorname{rad} R$ every proper ideal of R has the form $N^i = R\theta^i = \theta^i R$, for any $\theta \in N \setminus N^2$ and some positive integer i. The factors N^i/N^{i+1} are one-dimensional linear spaces over R/N. Hence, if $R/N \cong \mathbb{F}_q$ and m denotes the nilpotency index of N, the number of elements of R is equal to q^m. For further facts about chain rings we refer to [3, 14, 15].

As mentioned above, we consider chain rings of nilpotency index 2, i.e. chain rings with $N \neq (0)$ and $N^2 = (0)$. Thus we have always $|R| = q^2$, where $R/N \cong \mathbb{F}_q$. Chain rings with this property have been classified in [4, 17]. If $q = p^r$ there are exactly $r + 1$ isomorphism classes of such rings. These are:

- for every $\sigma \in \operatorname{Aut} \mathbb{F}_q$ the ring $R_\sigma \cong \mathbb{F}_q[X;\sigma]/(X^2)$ of 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 $(x_0, x_1)(y_0, y_1) = \big(x_0y_0, x_0y_1 + x_1\sigma(y_0)\big)$;
- the Galois ring $\mathrm{GR}(q^2, p^2) \cong \mathbb{Z}_{p^2}[X]/(f(X))$, 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 $\sigma \neq \mathrm{id}$ are noncommutative. Further R_{id} is commutative and $\operatorname{char} R_\sigma = p$ for every σ. The Galois ring $\mathrm{GR}(q^2, p^2)$ is commutative and

ACADEMIA PRESS
UNIVERSITEIT GENT

has characteristic p^2. From now on we denote by R any finite chain ring of nilpotency index 2.

Let R be a finite chain ring and consider the module $M = R_R^k$. Denote by M^* the set of all non-torsion vectors of M, i.e. $M^* = M \setminus M\theta$. Define sets $\mathcal{P}$ and $\mathcal{L}$ by

$$\mathcal{P} = \{xR; x \in M^*\},$$
$$\mathcal{L} = \{xR + yR; x, y \text{ linearly independent}\},$$

respectively, and take as incidence relation $I \subseteq \mathcal{P} \times \mathcal{L}$ set-theoretical inclusion. Further, define a neighbour relation $\backsim$ on the sets of points and lines of the incidence structure $(\mathcal{P}, \mathcal{L}, I)$ as follows:

(N1) the points $X, Y \in \mathcal{P}$ are neighbours (notation $X \backsim Y$) if there exist two different lines incident with both of them;

(N2) the lines $s, t \in \mathcal{L}$ are neighbours (notation $s \backsim t$) if there exist two different points incident with both of them.

Definition 2.1. The incidence structure $\Pi = (\mathcal{P}, \mathcal{L}, I)$ with the neighbour relation $\backsim$ is called the $(k-1)$-dimensional (right) projective Hjelmslev geometry over R and is denoted by $\mathrm{PHG}(R_R^k)$.

The point set $\mathcal{S} \subseteq \mathcal{P}$ is called a Hjelmslev subspace (or simply subspace) of $\mathrm{PHG}(R_R^k)$ if for every two points $X, Y \in \mathcal{S}$, there exists a line l incident with X and Y that is incident only with points of $\mathcal{S}$. The Hjelmslev subspaces of $\mathrm{PHG}(R_R^k)$ are of the form $\{xR; x \in (M')^*\}$, where M' is a free submodule of M. The (projective) dimension of a subspace is equal to the rank of the underlying module minus 1.

It is easily checked that $\backsim$ is an equivalence relation on each one of the sets $\mathcal{P}$ and $\mathcal{L}$. If $[X]$ denotes the set of all points that are neighbours to $X = xR$, then $[X]$ consists of all free rank 1 submodules of $xR + M\theta$. Similarly, the class $[l]$ of all lines which are neighbours to $l = xR + yR$ consists of all free rank 2 submodules of $xR + yR + M\theta$.

More generally, two subspaces $\mathcal{S}$ and $\mathcal{T}$, $\dim \mathcal{S} = s$, $\dim \mathcal{T} = t$, $s \leq t$, are neighbours if

$$\{[X]; X \in \mathcal{S}\} \subseteq \{[X]; X \in \mathcal{T}\}.$$

In particular, we say that the point X is a neighbour of the subspace $\mathcal{S}$ if there exists a point $Y \in \mathcal{S}$ with $X \backsim Y$. The neighbour class $[\mathcal{S}]$ contains all subspaces of dimension s that are neighbours to $\mathcal{S}$.

The next theorems give some insight into the structure of the projective Hjelmslev geometries $\mathrm{PHG}(R_R^k)$ and are part of more general results [1, 5, 7, 11, 12, 13, 19].

ACADEMIA PRESS
UNIVERSITEIT GENT

Theorem 2.2. *Let* $\Pi = \mathrm{PHG}(R_R^k)$ *where* R *is a chain ring with* $|R| = q^2$, $R/N \cong \mathbb{F}_q$. *Then*

(i) There are $q^{k-1} \cdot \frac{q^k-1}{q-1}$ *points (hyperplanes) and* $q^{2(k-2)} \cdot \frac{(q^k-1)(q^{k-1}-1)}{(q^2-1)(q-1)}$ *lines in* Π;

(ii) every point (hyperplane) has q^{k-1} *neighbours;*

(iii) 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* $t-1$, *where* $s \leq t \leq k$ *and* $\begin{bmatrix} n \\ k \end{bmatrix}_q$ *denotes the* q*-ary Gaussian binomial coefficient;*

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

Note that the Hjelmslev spaces $\mathrm{PHG}(R_R^k)$ are 2-uniform in the sense of [5]. Denote by η the natural homomorphism from R^k to $R^k/R^k\theta$ and by $\overline{\eta}$ the mapping induced by η on the submodules of R^k. It is clear that for every point X and every line l we have

$$[X] = \{Y \in \mathcal{P}; \overline{\eta}(Y) = \overline{\eta}(X)\},$$
$$[l] = \{m \in \mathcal{L}; \overline{\eta}(m) = \overline{\eta}(l)\}.$$

Let us denote by $\mathcal{P}'$ (resp. $\mathcal{L}'$) the set of all neighbour classes of points (resp. lines). The following result is straightforward.

Theorem 2.3. *The incidence structure* $(\mathcal{P}', \mathcal{L}', I')$ *with incidence relation* I' *defined by*

$$[X]\, I'\, [l] \iff \exists\, Y \in [X], \exists\, m \in [l] : Y\, I\, m$$

is isomorphic to the projective geometry $\mathrm{PG}(k-1, q)$.

Let $\mathcal{S}_0$ be a fixed subspace in $\mathrm{PHG}(R_R^k)$ with $\dim \mathcal{S}_0 = s$. Define the set $\mathfrak{P}$ of subsets of $\mathcal{P}$ by

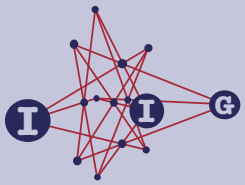
$$\mathfrak{P} = \{\mathcal{S} \cap [X]; X \backsim \mathcal{S}_0, \mathcal{S} \in [\mathcal{S}_0]\}.$$

The sets $\mathcal{S} \cap [X]$ are either disjoint or coincide. Define an incidence relation $\mathfrak{I} \subset \mathfrak{P} \times \mathcal{L}$ by

$$(\mathcal{S} \cap [X])\mathfrak{I}\, l \iff l \cap (\mathcal{S} \cap [X]) \neq \emptyset.$$

Let $\mathcal{L}(\mathcal{S}_0)$ be the set of all lines in $\mathcal{L}$ incident with at least one point in $\mathfrak{P}$. For the lines $l_1, l_2 \in \mathcal{L}(\mathcal{S}_0)$ we write $l_1 \sim l_2$ if they are incident (under $\mathfrak{I}$) with the same elements of $\mathfrak{P}$. The relation $\sim$ is an equivalence relation under which $\mathcal{L}(\mathcal{S}_0)$ splits into classes of equivalent lines. Denote by $\mathfrak{L}$ a set of representatives of the equivalence classes of lines in $\mathcal{L}(\mathcal{S}_0)$. The set of representatives $\mathfrak{L}$ contains only two types of lines: lines l with $l \backsim \mathcal{S}_0$ and lines l with $l \not\backsim \mathcal{S}_0$.

ACADEMIA PRESS
UNIVERSITEIT GENT



Theorem 2.4. *The incidence structure* $(\mathfrak{P}, \mathfrak{L}, \mathfrak{I}\,|_{\mathfrak{P}\times\mathfrak{L}})$ *can be embedded into* $\mathrm{PG}(k-1, q)$.

A special case of this result is obtained if we take $\mathcal{S}_0$ to be a point. Given $\Pi = (\mathcal{P}, \mathcal{L}, I) = \mathrm{PHG}(R_R^k)$ and a point $P \in \mathcal{P}$, let $\mathcal{L}(P)$ be the set of all lines in $\mathcal{L}$ incident with points in $[P]$. For two lines $s, t \in \mathcal{L}(P)$ we write $s \sim t$ if s and t coincide on $[P]$. Denote by $\mathcal{L}_1$ a complete list of representatives of the lines from $\mathcal{L}(P)$ with respect to the equivalence relation $\sim$. Then we have the following result:

Theorem 2.5.

$$([P], \mathcal{L}_1, I|_{[P]\times\mathcal{L}_1}) \cong \mathrm{AG}(k-1, q).$$

Finally, let two points X_1 and X_2 in $\Pi = \mathrm{PHG}(R_R^k)$ be neighbours. Then any two lines incident with both X_1 and X_2 are neighbours and belong to the same class, $[l]$ say. In such case we say that the neighbour class $[l]$ has the direction of the pair (X_1, X_2).

3. Constructions of caps in projective Hjelmslev geometries

Let $\Pi = (\mathcal{P}, \mathcal{L}, I)$ be a projective Hjelmslev space.

Definition 3.1. A set $\mathfrak{C}$ of points in Π is called a *cap* if no three points from $\mathfrak{C}$ are collinear. A cap of cardinality n is also referred to as an n-*cap*.

First we give a construction of caps in the 3-dimensional projective Hjelmslev space $\mathrm{PHG}(R_R^4)$. Let $[P_1], [P_2], \ldots, [P_{q^2+1}]$ be point classes that form an elliptic quadric $\mathfrak{K}$ in the factor geometry $(\mathcal{P}', \mathcal{L}', I') \cong \mathrm{PG}(3, q)$ (cf. Theorem 2.3).[1] It is well known that for each point $[P_i]$ there exists a unique plane of $(\mathcal{P}', \mathcal{L}', I')$, say $[\pi_i]$ that is tangent to $\mathfrak{K}$. The intersection $\pi_i \cap [P_i]$ has the structure of an affine plane isomorphic to $\mathrm{AG}(2, q)$ (cf. Theorem 2.5). Let $\mathfrak{O}_i \subset \pi_i \cap [P_i]$, $i = 1, \ldots, q^2+1$, be a set of points no three of which are collinear. It is a straightforward check that the point set

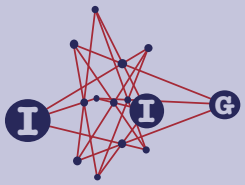
$$\mathfrak{C} = \bigcup_{i=1}^{q^2+1} \mathfrak{O}_i$$

is a cap in $\mathrm{PG}(R_R^4)$ for every chain ring R. If we choose the sets $\mathfrak{O}_i$ to contain the maximal possible number of points, i.e. $q+2$ for q even and $q+1$ for q odd,

[1] Actually, if $q > 2$ then $\mathfrak{K}$ can be an arbitrary (q^2+1)-cap.

ACADEMIA PRESS

UNIVERSITEIT GENT



we obtain a cap of cardinality

$$|\mathfrak{C}| = \begin{cases} (q^2+1)(q+2) & \text{for } q \text{ even;} \\ (q^2+1)(q+1) & \text{for } q \text{ odd.} \end{cases}$$

Remark 3.2. For $q = 2$ this construction gives the largest cap. Suppose that there exists a 21-cap $\mathfrak{C}$ in $\mathrm{PHG}(R_R^4)$, $R = \mathbb{Z}_4$ or $\mathbb{F}_2[X]/(X^2)$. Assume first that there exists a neighbour class of points, $[X]$ say, with $|[X] \cap \mathfrak{C}| = 3$. The three pairs of points in $[X]$ determine three directions (classes of neighbour lines), which do not contain points from $\mathfrak{C}$ apart from the points in $[X]$. The remaining four neighbour classes of lines through $[X]$ contain at most four additional points each. Hence $|\mathfrak{C}| \leq 3 + 4 \cdot 4 = 19$, a contradiction. Classes $[X]$ with $|[X] \cap \mathfrak{C}| > 3$ are ruled out in a similar way. Denote by λ_i the number of neighbour classes of points $[X]$ with $|[X] \cap \mathfrak{C}| = i$, $i = 0, 1, 2$. Clearly,

$$\begin{aligned} \lambda_0 + \lambda_1 + \lambda_2 &= 15\,, \\ \lambda_1 + 2\lambda_2 &= 21\,. \end{aligned}$$

Moreover, $\binom{\lambda_0}{2} \geq \lambda_2$ since every two-point class determines a couple of empty classes. The above system does not have a solution which satisfies this inequality. Consequently there is no 21-cap in $\mathrm{PHG}(R_R^4)$, where R is a chain ring with four elements.

As shown in [10, Th. 12], a nice class of caps related to the generalized Kerdock codes can be obtained in the projective Hjelmslev geometries of even dimension over the chain rings of characteristic 4, i.e. $\mathrm{GR}(q^2, 4)$. We shall now derive a corresponding result for projective Hjelmslev geometries over Galois rings of characteristic $p^2 > 4$. The special case $p = 3$ has already been considered in [6].

Let $q = p^r$ be a prime power and denote the Galois ring $\mathrm{GR}(q^2, p^2)$ of cardinality q^2 and characteristic p^2 by $\mathbb{G}$. For every $f \in \mathbb{N}$, the ring $\mathbb{G}$ has a unique Galois extension $\mathbb{G}_f \cong \mathrm{GR}(q^{2f}, p^2)$ of degree f. It is known that $\mathbb{G}_f$ is a free module of rank f over $\mathbb{G}$. Hence $\mathbb{G}_f$ can be viewed as the underlying module of the $(f-1)$-dimensional projective Hjelmslev geometry over $\mathbb{G}$. We denote this geometry by $\mathrm{PHG}(\mathbb{G}_f/\mathbb{G})$, i. e. $\mathrm{PHG}(\mathbb{G}_f/\mathbb{G}) = \mathrm{PHG}({}_{\mathbb{G}}\mathbb{G}_f) \cong \mathrm{PHG}(\mathbb{G}^f)$.

The group $\mathbb{G}_f^*$ of units of $\mathbb{G}_f$ contains a unique cyclic subgroup T_f^* of order $q^f - 1$, called the group of Teichmüller units. We set $T_f = \{x \in \mathbb{G}_f; x^{q^f} = x\} = T_f^* \cup \{0\}$ and abbreviate T_1, T_1^* as T resp. T^*. Note that $T_f^* = \langle \eta \rangle$ for any $\eta \in T_f$ such that $\beta = \eta + p\mathbb{G}_f$ is a primitive element of $\mathbb{G}_f/p\mathbb{G}_f \cong \mathbb{F}_{q^f}$.

Definition 3.3 (cf. [6, 10]). The set $\{\mathbb{G}\eta^j \mid 0 \leq j < (q^f - 1)/(q-1)\}$ in $\mathrm{PHG}(\mathbb{G}_f/\mathbb{G})$ is called the *Teichmüller set of* $\mathbb{G}_f/\mathbb{G}$ and is denoted by $\mathfrak{T}_f$.

ACADEMIA PRESS

UNIVERSITEIT GENT

Since $\{\eta^j \mid 0 \le j < (q^f-1)/(q-1)\}$ is a set of coset representatives for T^* in T_f^*, $\mathfrak{T}_f$ contains exactly one point from each neighbour class. In case of $\mathbb{G} = \mathbb{Z}_4$, f odd, the linear code over $\mathbb{Z}_4$ associated with $\mathfrak{T}_f$ (via the columns of a generator matrix) is isomorphic to the shortened quaternary Kerdock code; cf. [2, 16].

For the computations which follow we shall use the fact that $\mathrm{GR}(q^2, p^2)$ is isomorphic to the ring $W_2(\mathbb{F}_q)$ of Witt vectors of length 2 over $\mathbb{F}_q$ which is defined as the ring with underlying set $\mathbb{F}_q \times \mathbb{F}_q$ and operations

$$(a_0, a_1) + (b_0, b_1) = \left(a_0 + b_0, a_1 + b_1 - \sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j} a_0^j b_0^{p-j}\right), \tag{1}$$

$$(a_0, a_1) \times (b_0, b_1) = (a_0 b_0, a_0^p b_1 + b_0^p a_1). \tag{2}$$

Hence we can identify $\mathbb{G}$ with $W_2(\mathbb{F}_q)$ and $\mathbb{G}_f$ with $W_2(\mathbb{F}_{q^f})$. Viewed as a subset of $W_2(\mathbb{F}_{q^f})$, the set T_f consists of all elements $\{a\} := (a, 0)$, where $a \in \mathbb{F}_{q^f}$, and for $\boldsymbol{a} = (a_0, a_1) \in W_2(\mathbb{F}_{q^f})$ we have the p-adic representation $\boldsymbol{a} = \{a_0\} + \{a_1^{p^{-1}}\}p$. The Teichmüller set of $\mathbb{G}_f/\mathbb{G}$ becomes $\left\{\mathbb{G}\{\beta^j\} \mid 0 \le j < \frac{q^f-1}{q-1}\right\}$, where β is a fixed primitive element of $\mathbb{F}_{q^f}$.

The isomorphism $\mathrm{GR}(q^2, p^2) \cong W_2(\mathbb{F}_q)$ and other basic facts about rings of Witt vectors are described in [20, 17, 18, 10].

Lemma 3.4. *Suppose $\boldsymbol{a} = (a_0, a_1)$, $\boldsymbol{b} = (b_0, b_1)$, $\boldsymbol{c} = (c_0, c_1)$ are elements of $W_2(\mathbb{F}_{q^f})$ with $a_0 + b_0 + c_0 = 0$. If $p > 2$ then*

$$\boldsymbol{a} + \boldsymbol{b} + \boldsymbol{c} = \left(0, a_1 + b_1 + c_1 - \sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j} a_0^j b_0^{p-j}\right). \tag{3}$$

If $p = 2$ then $\boldsymbol{a} + \boldsymbol{b} + \boldsymbol{c} = (0, a_1 + b_1 + c_1 + a_0 b_0 + a_0^2 + b_0^2)$.

Proof. From (1) we get

$$\begin{aligned}
\boldsymbol{a} + \boldsymbol{b} + \boldsymbol{c} &= \left(a_0 + b_0, a_1 + b_1 - \sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j} a_0^j b_0^{p-j}\right) + (c_0, c_1) \\
&= \left(0, a_1 + b_1 + c_1 - \sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j} a_0^j b_0^{p-j} - \sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j} (-c_0)^j c_0^{p-j}\right) \qquad (4) \\
&= \left(0, a_1 + b_1 + c_1 - \sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j} a_0^j b_0^{p-j} - c_0^p \cdot \sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j} (-1)^j\right)
\end{aligned}$$

For $p > 2$ the result follows, since $\sum_{j=1}^{p-1} \binom{p}{j}(-1)^j = 0$ in this case (as an identity in $\mathbb{Z}$). For $p = 2$ it is easily checked directly. □

ACADEMIA PRESS
UNIVERSITEIT GENT

Lemma 3.5. *Let $\mathbb{G} = \mathrm{GR}(q^2, p^2)$ be a Galois ring of characteristic p^2 and $f \geq 3$ be an integer. The following assertions are equivalent:*

1. *The Teichmüller set $\mathfrak{T}_f$ in $\mathrm{PHG}(\mathbb{G}_f/\mathbb{G})$ is a cap.*
2. *None of the polynomials*

$$AX^p + \sum_{s=1}^{p-1} \frac{1}{p}\binom{p}{s} X^s + B \in \mathbb{F}_q[X] \qquad (A, B \in \mathbb{F}_q) \tag{5}$$

has a root in $\mathbb{F}_{q^f} \setminus \mathbb{F}_q$.

Proof. Throughout the proof we assume $p > 2$. The case $p = 2$ is similar and can be done without effort by inspecting the proof of [10, Th. 12].

Suppose $P_1 = \mathbb{G}\eta^i$, $P_2 = \mathbb{G}\eta^j$, $P_3 = \mathbb{G}\eta^k$ are distinct (and hence pairwise linearly independent) points in $\mathfrak{T}_f$. The points P_1, P_2, P_3 are collinear iff there exist units $u, v, w \in \mathbb{G}^*$ with $u\eta^i + v\eta^j + w\eta^k = 0$. W. l. o. g., let $k = 0$, $w = 1$. Viewing this as an equation in $W_2(\mathbb{F}_{q^f})$, we have $(1,0)+(u_0,u_1)\{\beta^i\}+(v_0,v_1)\times\{\beta^j\} = (0,0)$, where now $u_0, u_1, v_0, v_1 \in \mathbb{F}_q$, $u_0 v_0 \neq 0$. By Lemma 3.4 this is equivalent to

$$\begin{aligned} 1 + u_0\beta^i + v_0\beta^j &= 0\,, \\ u_1\beta^{ip} + v_1\beta^{jp} - \sum_{s=1}^{p-1} \frac{1}{p}\binom{p}{s} u_0^s \beta^{is} &= 0\,. \end{aligned} \tag{6}$$

Writing $\alpha = u_0\beta^i$, $\alpha' = v_0\beta^j$, $u_1' = u_1/u_0^p$, $v_1' = v_1/v_0^p$ and substituting $\alpha'^p = -1 - \alpha^p$ into the second equation, we get

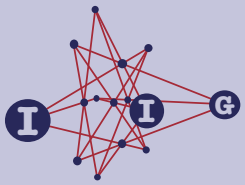
$$(u_1' - v_1')\alpha^p - \sum_{s=1}^{p-1} \frac{1}{p}\binom{p}{s}\alpha^s - v_1' = 0.$$

We must have $\alpha \in \mathbb{F}_{q^f} \setminus \mathbb{F}_q$, since $P_1 = \mathbb{G}\alpha \neq P_3 = \mathbb{G}1$. With $A := v_1' - u_1'$, $B := v_1'$ this proves (2)$\Longrightarrow$(1). For the reverse conclusion we need only to check that the points $P_1 = \mathbb{G}\alpha$, $P_2 = \mathbb{G}\alpha'$, $P_3 = \mathbb{G}1$ obtained from a root $\alpha \in \mathbb{F}_{q^f}\setminus\mathbb{F}_q$ of (5) are distinct. (Going backwards through the above computation easily gives that P_1, P_2, P_3 are collinear.) Since $\alpha' = -1-\alpha \notin \mathbb{F}_q$ and $\alpha'/\alpha = -\alpha^{-1}-1 \notin \mathbb{F}_q$, this is indeed the case, and the lemma is proved. □

Theorem 3.6. *Let $\mathbb{G} = \mathrm{GR}(q^2, p^2)$ be a Galois ring of characteristic p^2 and $f \geq 3$ be an integer.*

1. *If every prime divisor of f is greater than p, then the Teichmüller set $\mathfrak{T}_f$ is a cap in $\mathrm{PHG}(\mathbb{G}_f/\mathbb{G})$.*

ACADEMIA PRESS
UNIVERSITEIT GENT



2. *If f is even, $\mathfrak{T}_f$ is never a cap.*

Proof. If one of the polynomials in (5) has a root $\alpha \in \mathbb{F}_{q^f} \setminus \mathbb{F}_q$, then the degree $|\mathbb{F}_q[\alpha] : \mathbb{F}_q| \in \{2, 3, \ldots, p\}$ is a divisor of $f = |\mathbb{F}_{q^f} : \mathbb{F}_q|$. Hence f has a prime divisor that is not greater than p. In view of Lemma 3.5 this proves (1). Now suppose that f is even, and choose an element $\alpha \in \mathbb{F}_{q^f}$ which generates a quadratic extension of $\mathbb{F}_q$. Then $\mathbb{F}_q[\alpha] = \{A\alpha^p + B; A, B \in \mathbb{F}_q\}$, and so there exist $A, B \in \mathbb{F}_q$ such that

$$A\alpha^p + B = -\sum_{s=1}^{p-1} \frac{1}{p}\binom{p}{s}\alpha^s.$$

Again by Lemma 3.5, the set $\mathfrak{T}_f$ is not a cap in $\mathrm{PHG}(\mathbb{G}_f/\mathbb{G})$. □

Remark 3.7. Theorem 3.6 shows in particular that for a Galois ring $\mathbb{G}$ of characteristic 4 and an integer $f \geq 3$ the Teichmüller set $\mathfrak{T}_f$ is a cap in $\mathrm{PHG}(\mathbb{G}_f/\mathbb{G})$ if and only if f is odd. For a Galois ring $\mathbb{G}$ of characteristic 9 and integers $f \equiv 3 \pmod 6$ it can be ruled out with the help of Lemma 3.5 that $\mathfrak{T}_f$ is a cap in $\mathrm{PHG}(\mathbb{G}_f/\mathbb{G})$. (The proof uses the fact that $AX^3 + X^2 + X - A$ is irreducible over $\mathbb{F}_{3^r}$ if $A + A^3 + \cdots + A^{3^{r-1}} \neq 0$.) Hence for $\mathbb{G} = \mathrm{GR}(q^2, 9)$ the set $\mathfrak{T}_f$ is a cap in $\mathrm{PHG}(\mathbb{G}_f/\mathbb{G})$ if and only if $\gcd(f, 6) = 1$. For odd q the Teichmüller set $\mathfrak{T}_4$ in $\mathrm{PHG}(\mathbb{G}_4/\mathbb{G})$, $\mathbb{G} = \mathrm{GR}(q^2, p^2)$, has the same size as the caps constructed at the beginning of this section, but $\mathfrak{T}_4$ is never a cap according to Theorem 3.6.

The following result allows to double the size of a known cap in $\mathrm{PHG}(R_R^k)$ in the geometry $\mathrm{PHG}(R_R^{k+1})$.

Theorem 3.8. *Let $\mathfrak{C}$ be a cap in $\mathrm{PHG}(R_R^k)$. The set*

$$\mathfrak{C}' = \{(c_1, \ldots, c_k, 0) \mid (c_1, \ldots, c_k) \in \mathfrak{C}\} \cup \{(c_1, \ldots, c_k, 1) \mid (c_1, \ldots, c_k) \in \mathfrak{C}\}$$

is a cap in $\mathrm{PHG}(R_R^{k+1})$.

4. Upper bounds for caps in projective Hjelmslev geometries

In this section we derive upper bounds for the cardinality of caps in 3-dimensional projective Hjelmslev spaces.

Theorem 4.1. *Let $\mathfrak{C}$ be a cap in $\mathrm{PHG}(R_R^4)$, where R is a chain ring with $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Then $|\mathfrak{C}| \leq q^4 + 2q^2 + q$.*

ACADEMIA PRESS

UNIVERSITEIT GENT

Proof. We start by noting that

$$|\mathfrak{C}| \leq u(q^3+q^2+q+1), \tag{7}$$

where $u = \max\{|\mathfrak{C}\cap[X]|; [X] \in \mathcal{P}'\}$. Let $[X]$ be a neighbour class of points with $|\mathfrak{C}\cap[X]| = u$. The pairs of points from $[X]$ determine at least $u-1$ directions. All these neighbour classes of lines contain no points from $\mathfrak{C}$ (apart from the points in $[X]$). Each one of the remaining neighbour classes of lines contains at most q^2 points from $\mathfrak{C}$. This implies that

$$|\mathfrak{C}| \leq u + (q^2+q+1-(u-1))q^2 = q^4+q^3-(u-2)q^2+u. \tag{8}$$

By (7) and (8), we obtain

$$|\mathfrak{C}| \leq \max_{1\leq u\leq q^2+1} \min\{u(q^3+q^2+q+1), q^4+q^3-(u-2)q^2+u\}.$$

The maximum value is obtained for $u = q$ and gives the upper bound $|\mathfrak{C}| \leq q^4+2q^2+q$. (Our reasoning remains valid in the case $q=2$, even so $[X]$ is itself a cap of size 8 in this case.) □

In the case when q is odd we can improve on this bound using the fact that a cap (arc) in the projective Hjelmslev plane $\mathrm{PHG}(R_R^3)$ has at most q^2 points [8, 9].

Theorem 4.2. *Let $\mathfrak{C}$ be a cap in $\mathrm{PHG}(R_R^4)$, where R is a chain ring with $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$, q odd. Then $|\mathfrak{C}| \leq q^4 - q^2 + 1$.*

Proof. Let P be a point of $\mathfrak{C}$ for which $u = |\mathfrak{C}\cap[P]|$ is maximal, and let π be a plane such that $P \not\leftarrow \pi$. Define the projection φ from P onto π by

$$\varphi\colon \begin{cases} \mathcal{P}\setminus[P] & \to \ \pi\,, \\ Q & \mapsto \ \pi\cap\langle P,Q\rangle\,, \end{cases}$$

where $\mathcal{P}$ is the point set of $\mathrm{PHG}(R_R^4)$ and $\langle P,Q\rangle$ is the (unique) line through P and Q. Clearly, $\varphi(Q)$ is a point if $Q \not\leftarrow P$. If $Q \leftarrow P$, $\varphi(Q)$ is a set of q collinear points that are neighbours. The lines in π are images of the planes through P. Moreover two lines in π are neighbours iff their preimages are neighbours in $\mathrm{PHG}(R_R^4)$.

Define the induced arc $\mathfrak{C}^\varphi$ by

$$\mathfrak{C}^\varphi = \{\varphi(Q); Q \in \mathcal{P}\setminus[P]\}.$$

ACADEMIA PRESS
UNIVERSITEIT GENT

Every plane in $\mathrm{PHG}(R_R^4)$ contains at most q^2 points [8, 9]. Hence $\mathfrak{C}^\varphi$ is a $(n-1+q(u-1), r)$-arc in $\pi \cong \mathrm{PHG}(R_R^3)$, where $r \le q^2-1$. Now by Corollary 1 from [9]

$$|\mathfrak{C}^\varphi| \le \max_{1\le i\le q^2} \min\{i(q^2+q+1), q^2(q^2-2)+q(n-i)+i, q(q+1)(q^2-1+i-\lceil i/q\rceil\}.$$

The value of the right-hand side turns out to be q^4-2q, whence $n-1+q(u-1) \le q^4-2q$.

Now, as in the proof of Theorem 4.1,

$$|\mathfrak{C}| \le \max_{1\le u\le q^2+1} \min\{u(q^3+q^2+q+1), q^4-(u+1)q+1\}.$$

The maximum value is obtained for $u = q-1$ and gives $|\mathfrak{C}| \le q^4-q^2+1$. □

Remark 4.3. The order of magnitude of the upper bounds for the cardinality of a cap in $\mathrm{PHG}(R_R^4)$, where $|R| = q^2$, is approximately q^4. At the same time, we have constructions that give caps with approximately q^3 points. The argument used in the proof of Theorem 4.1 can be used to get a bound in Hjelmslev geometries of an arbitrary dimension. As expected, this bound stated in the theorem below turns out to be rather rough.

Theorem 4.4. *Let $\mathfrak{C}$ be a cap in $\mathrm{PHG}(R_R^k)$, where R is a chain ring with $|R| = q^2$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Then $|\mathfrak{C}| \le q^{2k-4} + O(q^{2k-6})$.*

Proof. Set $u = \max\{|\mathfrak{C} \cap [X]|; [X] \in \mathcal{P}'\}$. Clearly,

$$|\mathfrak{C}| \le u(q^{k-1}+q^{k-2}+\ldots+1). \tag{9}$$

On the other hand, we get as in (8)

$$|\mathfrak{C}| \le u+(q^{k-2}+\ldots+1-(u-1))q^{k-2} = q^{2k-4}+q^{2k-5}+q^{k-1}-(u-2)q^{k-2}+u. \tag{10}$$

Now

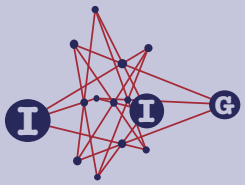
$$|\mathfrak{C}| \le \max_{1\le u\le q^{k-2}} \min\{u(q^{k-1}+q^{k-2}+\ldots+1), q^{2k-4}+q^{2k-5}+q^{k-1}-(u-2)q^{k-2}+u\}.$$

The maximum value is obtained for the lower or upper integer part of $u = (q^{2k-5}+\ldots+q^{k-2}+2q^{k-3})/(q^{k-2}+2q^{k-3}+q^{k-4}+\ldots+1)$. □

References

[1] **B. Artmann**, Hjelmslev-Ebenen mit verfeinerten Nachbarschaftsrelationen, *Math. Z.* **112** (1969), 163–180.

ACADEMIA PRESS
UNIVERSITEIT GENT



[2] **A. R. Hammons**, **P. Vijay Kumar**, **A. R. Calderbank**, **N. J. A. Sloane** and **P. Solé**, The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals and Related Codes, *IEEE Transactions on Information Theory* **40** (1994), 301–319.

[3] **W. E. Clark** and **D. A. Drake**, Finite chain rings, *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg* **39** (1974), 147–153.

[4] **A. Cronheim**, Dual numbers, Witt vectors, and Hjelmslev planes, *Geom. Dedicata* **7** (1978), 287–302.

[5] **D. Drake**, On n-Uniform Hjelmslev Planes, *J. Combinatorial Theory* **9** (1970), 267–288.

[6] **L. Hemme**, **T. Honold** and **I. Landjev**, Arcs in projective Hjelmslev spaces obtained from Teichmüller sets, **in** *Proceedings of the Seventh International Workshop on Algebraic and Combinatorial Coding Theory (ACCT-2000)*, 177–182, Bansko, Bulgaria, 2000.

[7] **Th. Honold** and **I. Landjev**, Projective Hjelmslev geometries, *Proc. of the International Workshop on Optimal Codes*, Sozopol, 1998, 97–115.

[8] ———, On arcs in projective Hjelmslev planes, *Discrete Math.* **231** (2001), 265–278.

[9] ———, Arcs in projective Hjelmslev planes, *Discrete Math. Appl.* **11**(1) (2001), 53–70, originally published in Russian in *Diskretnaya Matematika* **13** (2001), No. 1, 90–109.

[10] ———, On maximal arcs in projective Hjelmslev planes over chain rings of even characteristic. *Finite Fields Appl.* **11** (2005), no. 2, 292–304.

[11] **A. Kreuzer**, Hjelmslev-Räume, *Results Math.* **12** (1987), 148–156.

[12] ———, Projektive Hjelmslev-Räume, Dissertation, Technische Universität München, 1988.

[13] ———, Hjelmslevsche Inzidenzgeometrie - ein Bericht, Bericht TUM-M9001, Technische Universität München, January 1990, Beiträge zur Geometrie und Algebra Nr. 17.

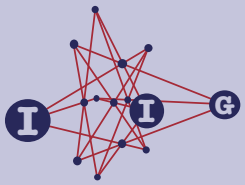
[14] **B. R. McDonald**, *Finite rings with identity*, Marcel Dekker, New York, 1974.

[15] **A. A. Nechaev**, Finite principal ideal rings, *Mat. Sbornik of the Russian Academy of Sciences* **20** (1973), 364–382.

[16] ———, Kerdock Code in Cyclic Form, *Discrete Math. Appl.* **1** (1991), 365–384. (English translation)

ACADEMIA PRESS

UNIVERSITEIT GENT



[17] **R. Raghavendran**, Finite associative rings, *Compos. Math.* **21** (1969), 195–229.

[18] **A. G. Shanbhag**, **P. V. Kumar** and **T. Helleseth**, An upper bound for the extended Kloosterman sums over Galois rings, *Finite Fields Appl.* **4** (1998), 218–238.

[19] **F. D. Veldkamp**, Geometry over rings, Handbook of Incidence Geometry—Buildings and Foundations (Francis Buekenhout, ed.), Elsevier Science Publishers, 1995, pp. 1033–1084.

[20] **E. Witt**, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n, *J. Reine Angew. Math.* **176** (1937), 126–140.

Thomas Honold

ZENTRUM MATHEMATIK (M11), TECHNISCHE UNIVERSITÄT MÜNCHEN, BOLTZMANNSTR. 3, D-85748, GARCHING, DEUTSCHLAND

e-mail: honold@ma.tum.de

Ivan Landjev

NEW BULGARIAN UNIVERSITY, 21 MONTEVIDEO STR., 1618 SOFIA, BULGARIA, AND, INSTITUTE OF MATHEMATICS AND INFORMATICS, BAS,, 8 ACAD. G. BONCHEV STR., 1113, SOFIA, BULGARIA

e-mail: ivan@moi.math.bas.bg

ACADEMIA PRESS

UNIVERSITEIT GENT