On maximal arcs in projective Hjelmslev planes over chain rings of even characteristic

Thomas Honold\textsuperscript{a,}, Ivan Landjev\textsuperscript{b}

\textsuperscript{a}Zentrum Mathematik (M11), Technische Universität München, Boltzmannstr. 3, D-85748 Garching, Germany
\textsuperscript{b}Institute of Mathematics and Informatics, BAS, 8 Acad. G. Bonchev str., 1113, Sofia, Bulgaria

Received 30 July 2003; revised 10 December 2004
Communicated by Simeon Ball
Available online 1 February 2005

Abstract

In this paper, we prove that maximal \((k, 2)\)-arcs in projective Hjelmslev planes over chain rings \(R\) of nilpotency index 2 exist if and only if \text{char} \(R = 4\).

© 2005 Elsevier Inc. All rights reserved.

Keywords: Projective Hjelmslev plane; Arc; Oval; Hyperovals; Linear codes over finite chain rings

1. Introduction

In this paper, we consider the problem of finding the maximal size \(m_2(R^3_R) = k\) of a \((k, 2)\)-arc, or simply \(k\)-arc in certain projective Hjelmslev planes \(\text{PHG}(R^3_R)\). The interest in this problem comes from coding theory since the existence of large arcs usually implies the existence of good codes. But the maximal arc problem is also interesting in its own right as a purely geometrical problem. In what follows, we restrict ourselves to planes over chain rings \(R\) with \(|R| = q^2\), \(R/\text{rad} R \sim \mathbb{F}_q\), where \(q\) is a prime power. On one hand, these are the simplest nontrivial chain rings. On the other hand, the nested structure of the projective Hjelmslev planes implies that results
on arcs in planes over chain rings with large nilpotency index necessarily rely on results on arcs in Hjelmslev planes over rings with a smaller index.

It is known that the maximal size of a $k$-arc in the projective plane $\text{PG}(2, q)$ is $q + 1$ for $q$ odd and $q + 2$ for $q$ even. It is shown in [13,14] that for projective Hjelmslev planes a similar result holds true:

$$m_2(R^3_R) \leq \begin{cases} q^2 + q + 1 & \text{for } q \text{ even}, \\
q^2 & \text{for } q \text{ odd}. \end{cases}$$

(1)

In this paper, we deal with Hjelmslev planes over rings of even characteristic and nilpotency index 2. We prove that for $q$ even the upper bound in (1) is achieved if and only if $\text{char } R = 4$.

In Section 2, we give some basic facts about finite chain rings and projective Hjelmslev planes over such rings. Section 3 deals with bounds on arcs in projective Hjelmslev planes. In Section 4 we prove the existence of $k$-arcs meeting the upper bound in (1) for planes over rings $R$ of nilpotency index 2 and $\text{char } R = 4$.

In Section 5, we prove that for rings of characteristic 2 and nilpotency index 2 the upper bound in (1) is not achieved.

2. Basic facts

A ring (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. The following theorem which is a compilation of results from [2,18,19] summarizes some important properties of chain rings.

**Theorem 1.** 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 left ideals of $R$ 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, then every proper left (right) ideal of $R$ has the form $N^i = R\theta^i = \theta^i R$ for some positive integer $i$.

From now on we will be using the symbols $R$, $N$, $\theta$ only in the meaning fixed by this theorem. We restrict ourselves to 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 the above property have been classified in [3,23]. If $q = p^r$ then there are exactly $r + 1$ isomorphism classes of such rings. These are:

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

The rings $R_q$ all have characteristic $p$ while $\text{GR}(q^2, p^2)$ has characteristic $p^2$.

Consider a finite chain ring $R$ and consider the module $H = R^3_R$. Denote by $H^*$ the set of all nontorsion vectors of $H$, i.e. $H^* = H \setminus H\theta$. Further define the set of points $\mathcal{P}$ and the set of lines $\mathcal{L}$ by

$$\mathcal{P} = \{xR | x \in H^*\},$$

$$\mathcal{L} = \{xR + yR | x, y \text{ linearly independent}\}$$

and take as incidence relation $I \subseteq \mathcal{P} \times \mathcal{L}$ set-theoretical inclusion. The incidence structure $(\mathcal{P}, \mathcal{L}, I)$ is further provided with a neighbour relation $\sim$ on the sets of points and lines as follows:

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

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

Definition 2. The incidence relation $\Pi = (\mathcal{P}, \mathcal{L}, I)$ with the neighbour relation $\sim$ is called the (right) projective Hjelmslev plane over $R$ and is denoted by $\text{PHG}(R^3_R)$.

It is easily checked that $\sim$ 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 contained in $xR + H\theta$. Similarly, the class $[s]$ of all lines which are neighbours to $s = xR + yR$ consists of all free rank 2 submodules contained in $xR + yR + H\theta$. The relation $\sim$ can be extended in the following way: we say that the point $X$ is a neighbour of the line $s$ if there exists a point $Ys$ with $X \sim Y$ or, equivalently, if there exists a line $tX$ with $s \sim t$.

The next theorems provide basic knowledge about the structure of projective Hjelmslev planes over finite chain rings and are part of more general results [1,4,8,15–17,25].

Theorem 3. Let $\Pi = \text{PHG}(R^3_R)$ where $R$ is a chain ring with $|R| = q^2$, $R/N \cong \mathbb{F}_q$. Then

(i) $|\mathcal{P}| = |\mathcal{L}| = q^2(q^2 + q + 1);
(ii) every point (line) has $q^2$ neighbours;
(iii) every point (line) is incident with $q(q + 1)$ lines (points);
(iv) given a point $P$ and a line $l$ with $PIl$, there exist exactly $q$ points on $l$ which are neighbours to $P$ and exactly $q$ lines through $P$ which are neighbours to $l$.

Denote by $\eta$ the natural homomorphism $\eta : R^3 \rightarrow R^3/R^3\theta$ and by $\bar{\eta}$ the mapping induced by $\eta$ on the submodules of $R^3$. It is clear that for every point $X$ and every
line $s$ we have

$$[X] = \{ Y \in \mathcal{P} | \overline{\eta}(Y) = \overline{\eta}(X) \},$$

$$[s] = \{ t \in \mathcal{L} | \overline{\eta}(t) = \overline{\eta}(s) \}.$$ 

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

**Theorem 4** (Honold and Landjev [12]). The incidence structure $(\mathcal{P}', \mathcal{L}', I')$ with incidence relation $I'$ defined by

$$[X] I' [s] \iff \exists X' \in [X], \exists s' \in [s]: X' I s'$$

is isomorphic to the projective plane $\text{PG}(2, q)$.

3. Arcs in projective Hjelmslev planes

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

**Definition 5.** A multiset in $II$ is a mapping $\mathcal{R}: \mathcal{P} \to \mathbb{N}_0$.

The integer $\mathcal{R}(P)$ is called the *multiplicity* of the point $P$. The mapping $\mathcal{R}$ can be extended to the subsets of $\mathcal{P}$ by

$$\mathcal{R}(Q) = \sum_{P \in Q} \mathcal{R}(P), \quad \text{for } Q \subseteq \mathcal{P}.$$ 

The integer $\mathcal{R}(P) = \sum_{P \in \mathcal{P}} \mathcal{R}(P)$ is called the *cardinality* of the multiset $\mathcal{R}$. The support of $\mathcal{R}$ is defined by $\text{Supp} \mathcal{R} = \{ P \in \mathcal{P} | \mathcal{R}(P) > 0 \}$.

**Definition 6.** Two multisets $\mathcal{R}'$ and $\mathcal{R}''$ in the projective Hjelmslev planes $II'$ and $II''$, respectively, are said to be equivalent if there exists an isomorphism $\sigma: II' \to II''$ such that $\mathcal{R}'(P) = \mathcal{R}''(\sigma(P))$, for every $P$ from the point set of $II'$.

**Definition 7.** The multiset $\mathcal{R}: \mathcal{P} \to \mathbb{N}_0$ is called a $(k, n)$-arc if $\mathcal{R}(P) = k$ and $\mathcal{R}(l) \leq n$ for any line $l \in \mathcal{L}$. A $(k, n)$-arc $\mathcal{R}$ is said to be complete if there is no $(k', n)$-arc $\mathcal{R}'$ with $k' > k$ and $\mathcal{R}'(P) \geq \mathcal{R}(P)$ for every $P \in \mathcal{P}$.

A $(k, 2)$-arc is simply referred to as a $k$-arc. Multisets with $\mathcal{R}(P) \in \{0, 1\}$ are called projective multisets. They can be viewed as sets of points by identifying them with their support. We denote by $m_n(R^3_R)$ the cardinality of the largest $(k, n)$-arc in $\text{PHG}(R^3_R)$. Similarly, we denote by $m_n(q)$ ($\mu_n(q)$, respectively) the largest size of a $(k, n)$-arc in $\text{PG}(2, q)$ ($\text{AG}(2, q)$, respectively).
The following general bound on \( m_n(R^3_R) \) has been proved in [13]:

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

For arcs with \( n = 2 \) this bound can be improved to:

\[ m_2(R^3_R) \leq \begin{cases} q^2 + q + 1 & \text{for } q \text{ even,} \\ q^2 & \text{for } q \text{ odd.} \end{cases} \tag{2} \]

If \( q \) is even and \( k = q^2 + q + 1 \) then \( \mathcal{R}([X]) = 1 \) for all neighbour classes \([X] \in \mathcal{P}'\).
If \( q \) is odd and \( k = q^2 \) then \( \mathcal{R}([X]) \leq 1 \) for all neighbour classes \([X] \in \mathcal{P}'\) and the classes \([Y]\) with \( \mathcal{R}([Y]) = 0 \) form a line in \((\mathcal{P}',\mathcal{L}',\mathcal{I}')\).

Multisets which meet the upper bound in (2) for \( q \) even are called hyperovals; multisets which meet this bound for \( q \) odd are called ovals. Note that the hyperovals are maximal arcs in the sense of Hirschfeld [7].

4. Hyperovals in projective Hjelmslev planes over chain rings of characteristic 4

Let \( q = p' \) be a prime power and denote the Galois ring \( \text{GR}(q^2, p^2) \) 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 \( \mathbb{G}_f = \text{GR}(q^{2f}, p^2) \) of degree \( f \). It is known that \( \mathbb{G}_f \) is a free module of rank \( f \) over \( \mathbb{G} \). Hence we can view \( \mathbb{G}_f \) as the underlying module of the \((f - 1)\)-dimensional projective Hjelmslev space over \( \mathbb{G} \). We denote this space by \( \text{PHG}(\mathbb{G}_f/\mathbb{G}) \), i.e. \( \text{PHG}(\mathbb{G}_f/\mathbb{G}) \cong \text{PHG}(\mathbb{G}^f) \).

The group \( \mathbb{G}_f^\ast \) of units of \( \mathbb{G}_f \) contains a unique cyclic subgroup \( T_f^\ast \) of order \( q^f - 1 \), called the group of Teichmüller units. We set \( T_f := \{x \in \mathbb{G}_f; xq^f = x\} = T_f^\ast \cup \{0\} \) and write \( T, T^\ast \) instead of \( T_1 \) resp. \( T_1^\ast \). For \( \eta \in T_f \) we have \( T_f^\ast = \langle \eta \rangle \) iff \( \beta := \eta + p \mathbb{G}_f \) is a primitive element of \( \mathbb{G}_f/p \mathbb{G}_f \cong \mathbb{F}_{q^f} \).

**Definition 10.** The multiset \( \{\mathbb{G}\eta^j \mid 0 \leq j < (q^f - 1)/(q-1)\} \) in \( \text{PHG}(\mathbb{G}_f/\mathbb{G}) \) is called the Teichmüller set of \( \mathbb{G}_f/\mathbb{G} \) and is denoted by \( \mathbb{T}_f \).

Since \( \{\eta^j \mid 0 \leq j < (q^f - 1)/(q-1)\} \) is a set of coset representatives for \( T_f^\ast/T^\ast \), \( \mathbb{T}_f \) is actually a set with exactly one point from each neighbour class.
Let now \( C(\mathfrak{T}_f) \) be the linear code over \( \mathcal{G} \) associated with \( \mathfrak{T}_f \) in the sense of [12, Theorem 5.1], i.e. \( C(\mathfrak{T}_f) \) is generated by an \( f \times \frac{q^f-1}{q-1} \) matrix over \( \mathcal{G} \) whose columns represent the points of \( \mathfrak{T}_f \).

In case of \( \mathcal{G} = \mathbb{Z}_4 \), the code \( C(\mathfrak{T}_f) \) is isomorphic to the shortened quaternary Kerdock code; cf. [5,20]. Generalized Kerdock codes, corresponding to the case \( \mathcal{G} = \text{GR}(4^r,4) \), have been investigated in [22].

The code \( C(\mathfrak{T}_f) \) can be obtained by Hensel lifting a \( q \)-ary Simplex code of dimension \( f \) over \( \mathcal{G}/\text{rad} \mathcal{G} \) to a constacyclic code over \( \mathcal{G} \). To see this, observe first that

\[
C(\mathfrak{T}_f) = \{ (\lambda(1), \lambda(\eta), \ldots, \lambda(\eta^{n-1})) \mid \lambda \in S \}, \tag{3}
\]

where \( n = (q^f - 1)/(q - 1) \) and \( S \) is the set of \( \mathcal{G} \)-linear mappings \( \lambda : \mathcal{G}_f \to \mathcal{G} \). If \( c(\lambda) = (x_0, \ldots, x_{n-1}) \) denotes the codeword corresponding to \( \lambda \) in (3) and \( \xi = \eta^n \), then \( (\xi x_{n-1}, x_0, \ldots, x_{n-2}) = c(\mu) \) where \( \mu \in S \) is defined by \( \mu(x) = \lambda(\eta^{-1}x) \). Hence \( C(\mathfrak{T}_f) \) is an ideal in \( \mathcal{G}[X]/(X^n - \xi) \). Since \( \text{ord}(\xi) = q - 1 \), \( \xi \) generates \( T^* \). Now \( C(\mathfrak{T}_f) \) has a check polynomial \( h \) such that \( h \in \mathbb{F}_q[X] \) is primitive, i.e. \( h \) checks a Simplex code as claimed.

Raghavendran [23, Theorem 7] established that Galois rings of characteristic \( p^m \) are essentially the same thing as the rings of so-called Witt vectors of length \( m \) introduced by Ernst Witt in [26] as a device for studying cyclic field extensions and cyclic algebras of prime power degree. Here, we confine ourselves to the special case \( m = 2 \).

The ring \( W_2(\mathbb{F}_q) \) of Witt vectors of length 2 over \( \mathbb{F}_q \) is defined as the algebraic structure with underlying set \( \mathbb{F}_q \times \mathbb{F}_q \) and operations

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

\[
(a_0, a_1) \times (b_0, b_1) = (a_0 b_0, a_0^p b_1 + b_0^p a_1).
\]

For \( p = 2, 3 \) the rules for addition/multiplication of pairs \( a = (a_0, a_1), b = (b_0, b_1) \) are recorded in the following table:

<table>
<thead>
<tr>
<th></th>
<th>( a + b )</th>
<th>( ab )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( W_2(\mathbb{F}_2) )</td>
<td>( (a_0 + b_0, a_1 + b_1 + a_0 b_0) )</td>
<td>( (a_0 b_0, a_0^2 b_1 + b_0^2 a_1) )</td>
</tr>
<tr>
<td>( W_2(\mathbb{F}_3) )</td>
<td>( (a_0 + b_0, a_1 + b_1 - a_0^2 b_0 - b_0^2 a_0) )</td>
<td>( (a_0 b_0, a_0^3 b_1 + b_0^3 a_1) )</td>
</tr>
</tbody>
</table>

The unit of \( W_2(\mathbb{F}_q) \) is 1 = (1, 0), and \( p a = (0, a_0^p) \) holds for \( a \in W_2(\mathbb{F}_q) \). Writing \( k = k_1 \) for \( k \in \mathbb{N} \) and \( \{a\} := (a, 0) \) for \( a \in \mathbb{F}_q \) one finds \( \{a_0\} + \{a_1\} p = (a_0, a_1^p) \). On the other hand, every \( x \in \mathcal{G} \) admits a unique representation \( x = t_0 + t_1 p \) with \( t_0, t_1 \in T \).
Theorem 11. $G \cong W_2(\mathbb{F}_q)$; more precisely, the map $\phi : G \to W_2(\mathbb{F}_q)$, $t_0 + t_1 p \mapsto (t_0, t_1 p)$, where $t_i = t_i + \text{rad } G$, is a ring isomorphism.

For a proof see [26, Satz 9], [23, Theorem 7] and [24, Theorem 4].

By Theorem 11 we can identify $G$ with $W_2(\mathbb{F}_q)$ and $G_f$ with $W_2(\mathbb{F}_q, r)$. The map $F : (a_0, a_1) \mapsto (a_0^q, a_1^q)$ then generates the Galois group of $G_f/G$, and $G$ is the ring of fixed points of $F$. The Teichmüller set of $G_f/G$ is simply $\{ G\{ \beta^j \} | 0 \leq j < n \}$.

Theorem 12. Let $G = GR(q^2, 4)$ be a Galois ring of characteristic 4 and $f \geq 3$ be an odd integer. Then no three points of the Teichmüller set $T_f$ in PHG($G_f/G$) are collinear. In particular, $m_2(G^3) = q^2 + q + 1$.

Proof. Assume $G\eta^j_1, G\eta^j_2, G\eta^k_j$ are collinear points in PHG($G_f/G$). The module $G\eta^j_1 + G\eta^j_2 + G\eta^k_j$ has rank 2, and there exist units $u, v, w \in \mathbb{G}^*$ with $uw^i + v\eta^j + w\eta^k = 0$. W.l.o.g., let $k = 0$, $w = 1$. Viewing this as an equation in $W_2(\mathbb{F}_2^r)$, we have $(1, 0) + (u_0, u_1)\{ \beta^j \} + (v_0, v_1)\{ \beta^j \} = (0, 0)$, i.e.

$$1 + u_0\beta^i + v_0\beta^j = 0,$$

$$u_1\beta^{2i} + v_1\beta^{2j} + u_0\beta^i + v_0\beta^j + u_0v_0\beta^{i+j} = 0,$$  

(4)

where now $u_0, u_1, v_0, v_1 \in \mathbb{F}_2^r$, $u_0v_0 \neq 0$. This leads to a quadratic equation with coefficients in $\mathbb{F}_2^r$ for $\beta^i : g(\beta^i) = A\beta^{2i} + B\beta^i + C = 0$, where $A = u_1 + u_0^2 + v_1u_0/v_0^2$, $B = u_0$, $C = 1 + v_1/v_0^2$. This equation is nontrivial since $B = u_0 \neq 0$. Furthermore, $\beta^i \notin \mathbb{F}_2^r$, since $G\{ \beta^j \} \neq G1$. Hence $g(x)$ is irreducible, and thus $f$ is even. Conversely, if $f$ is even we can choose $\beta^i \in \mathbb{F}_2^r \setminus \mathbb{F}_2^r$ satisfying some quadratic equation $\beta^{2i} + \beta^i + C = 0$. Then $(1, 0) + (1, 1 + C)\{ \beta^j \} + (1, 1 + C)\{ \beta^{2j} \} = 0$, showing that $G1, G\eta^j_1, G\eta^{2r}_j$ are collinear points of PHG($G_f/G$).}

5. The nonexistence of hyperovals in Hjelmslev planes over chain rings of characteristic 2

Throughout this section $R$ will denote a chain ring with $|R| = q^2$, $R/\text{rad } R \cong \mathbb{F}_q$, char $R = 2$, where $q = 2^r$. By the classification result mentioned in Section 2 we may assume that $R = R_\sigma$ for some $\sigma \in \text{Aut } \mathbb{F}_q$. Note that $R_\sigma$ contains the subfield $S = \mathbb{F}_q \times \{ 0 \} \cong \mathbb{F}_q$. In this section, we prove the following theorem.

Theorem 13. Let $R$ be a chain ring with $|R| = 2^{2r}$, $R/\text{rad } R \cong \mathbb{F}_2^r$ and char $R = 2$. There exists no $(2^{2r} + 2^{r} + 1)$-arc in the projective Hjelmslev plane PHG($R_3^3$).

The idea behind the proof is the following. We assume the existence of a $(q^2 + q + 1)$-arc $R$ in PHG($R_3^3$) and we associate a linear code $C$ over $R$ with $R$. This can always be done, according to Theorem 5.1 in [12]. The code $C$ is mapped to a binary code $D = \psi(C)$ using the so-called Reed–Solomon map $\psi$ (cf. (5) below). Note that since
char \( R = 2 \) the image of \( C \) can be made linear over \( \mathbb{F}_q \) according to Theorem 3.4 from [11] (see also [8,10]). Finally, a multiset \( \tilde{\mathcal{X}} \) in PG(5, q) can be associated with \( D \). We are going to show that a multiset \( \tilde{\mathcal{X}} \) with the special structure imposed on it by the Reed–Solomon map does not exist.

Identifying \( S \) with \( \mathbb{F}_q \) and writing \( \theta = (0, 1) \), every element \( r \in R \) can be (uniquely) represented in the form

\[
r = a + b\theta, \quad a, b \in \mathbb{F}_q.
\]

Products in \( R \) are computed using \( \theta^2 = 0 \) and \( \theta a = \sigma(a)\theta \) for \( a \in \mathbb{F}_q \). In the sequel we write \( a^\sigma \) instead of \( \sigma(a) \).

We define the Reed–Solomon map (or RS map, for short) \( \psi \) by

\[
\psi: \begin{cases} 
R & \to \mathbb{F}_q^n, \\
r & \to (a, b) \left( \begin{array}{c}
\alpha_0 \\
\alpha_1 \\
\alpha_2 \\
\vdots \\
\alpha_{q-1}
\end{array} \right),
\end{cases}
\]

where \( \alpha_0 = 0, \alpha_1 = 1, \alpha_2, \ldots, \alpha_{q-1} \) are the elements of \( \mathbb{F}_q \) taken in some order. The RS map can be extended to act on vectors from \( R^n \) by

\[
\psi(r_1, r_2, \ldots, r_n) = (\psi(r_1), \psi(r_2), \ldots, \psi(r_n)).
\]

The extension \( \psi: R^n \to \mathbb{F}_q^n \) is a monomorphism (injective linear map) from the left \( \mathbb{F}_q \)-space \( R^n \) into the \( \mathbb{F}_q \)-space \( \mathbb{F}_q^n \). Therefore it maps (left) linear codes over \( R \), i.e submodules of \( R^n \), onto linear codes over \( \mathbb{F}_q \). Moreover, \( \psi \) is a (scaled) isometry from \( (R, \rho_{\text{hom}}) \) to \( (\mathbb{F}_q^n, \rho_{\text{Ham}}) \), where \( \rho_{\text{hom}} \) is the homogeneous metric on \( R \) and \( \rho_{\text{Ham}} \) is the usual Hamming metric (cf. [11]).

Recall from [12] that every linear code \( C \subseteq_R R^n \) has a module basis of the form \( c_1, c_2, \ldots, c_h, \theta c_{h+1}, \ldots, \theta c_k \) where \( 0 \leq h \leq k \leq n \) and \( c_i \in (R^n)^* \). A matrix whose rows are a module basis of \( C \) is said to be generator matrix of \( C \).

**Lemma 14.** Let \( R \) be one of the rings \( R_\sigma \) and let \( C \subseteq_R R^n \) be a linear code with generator matrix

\[
[c_1, c_2, \ldots, c_h, \theta c_{h+1}, \ldots, \theta c_k]^t,
\]

where \( c_i \in (R^n)^* \). Then

\[
[\psi(c_1), \psi(c_2), \ldots, \psi(c_h), \psi(\theta c_1), \ldots, \psi(\theta c_h), \psi(\theta c_{h+1}), \ldots, \psi(\theta c_k)]^t,
\]

is a generator matrix for \( \psi(C) \).
Proof. The vectors \( c_i \) are linearly independent over \( R \) and \( 1, \theta \) is a basis of the left \( \mathbb{F}_q \)-space \( R \). Hence

\[
c_1, \theta c_1, c_2, \theta c_2, \ldots, c_h, \theta c_h, c_{h+1}, \ldots, c_k
\]

is a basis of \( C \) over \( \mathbb{F}_q \). Since \( \psi \) is a monomorphism, \( \psi(c_1), \psi(\theta c_1), \psi(c_2), \psi(\theta c_2), \ldots, \psi(c_h), \psi(\theta c_h), \psi(\theta c_{h+1}), \ldots, \psi(\theta c_k) \) is a basis of \( \psi(C) \) over \( \mathbb{F}_q \). \( \square \)

For the next lemma, let \( \mathcal{R} \) be a multiset in \( \text{PHG}(R^3_K) \) and let \( C \) be an associated linear code over \( R \) in the sense of [12, Theorem 5.1], i.e., \( C \) is generated by a \( 3 \times \mathcal{R}(\mathcal{P}) \) matrix over \( R \) whose columns represent the points of \( \mathcal{R} \). Let \( \hat{D} = \psi(C) \) be the linear code over \( \mathbb{F}_q \) which is the image of \( C \) under the RS map \( \psi \). Finally, denote by \( \tilde{\mathcal{R}} \) a multiset in \( \text{PG}(5, q) \) associated with \( \hat{D} \).

Lemma 15. If \( \mathcal{R} \) is projective then \( \tilde{\mathcal{R}} \) is also projective. The points of \( \tilde{\mathcal{R}} \) are contained in \( \mathcal{R}(\mathcal{P}) \) lines of multiplicity \( q \).

Proof. The first part is straightforward. For the second part consider a column

\[
(a_1 + b_1 \theta, a_2 + b_2 \theta, a_3 + b_3 \theta)^t
\]

of a generator matrix for \( C \) corresponding to a point from \( \text{Supp} \mathcal{R} \). By Lemma 14, the RS map \( \psi \) maps this column onto the \( q \) columns of the matrix

\[
\begin{pmatrix}
  a_1 & b_1 \\
  a_2 & b_2 \\
  a_3 & b_3 \\
  0 & a_1^\sigma \\
  0 & a_2^\sigma \\
  0 & a_3^\sigma \\
\end{pmatrix}
\begin{pmatrix}
  0 & 1 & x_2 & \ldots & x_{q-1} \\
\end{pmatrix}
= \begin{pmatrix}
  b_1 & a_1 & a_1 x_2 & a_2 & \ldots & a_1 x_{q-1} & b_1 \\
  b_2 & a_2 & a_2 x_2 & a_3 & \ldots & a_2 x_{q-1} & b_2 \\
  b_3 & a_3 & a_3 x_2 & a_4 & \ldots & a_3 x_{q-1} & b_3 \\
  a_1^\sigma & a_1^\sigma & a_1^\sigma & a_1^\sigma & \ldots & a_1^\sigma \\
  a_2^\sigma & a_2^\sigma & a_2^\sigma & a_2^\sigma & \ldots & a_2^\sigma \\
  a_3^\sigma & a_3^\sigma & a_3^\sigma & a_3^\sigma & \ldots & a_3^\sigma \\
\end{pmatrix}
\]

Since the rank of this matrix is 2, the points of \( \tilde{\mathcal{R}} \) represented by these columns are collinear.

Now let \( \mathcal{R} \) be a \( (q^2 + q + 1) \)-arc in \( \text{PHG}(R^3_K) \). We denote the \( q^2 + q + 1 \) lines containing the points of \( \hat{\mathcal{R}} \) by \( l_1, \ldots, l_{q^2+q+1} \). Any two different lines \( l_i, l_j \) are skew, for if we assume that \( l_i \cap l_j = P \) say, then \( P \) can be represented as

\[
(a_1 x + b_1, a_2 x + b_2, a_3 x + b_3, a_1^\sigma, a_2^\sigma, a_3^\sigma)
\]

and in the same time as

\[
(c_1 \beta + d_1, c_2 \beta + d_2, c_3 \beta + d_3, c_1^\sigma, c_2^\sigma, c_3^\sigma)
\]
for some \( \alpha, \beta, a_i, b_j, c_i, d_j \in \mathbb{F}_q \). This implies that \( a_1^2 = \lambda e_1^2 \), \( a_2^2 = \lambda e_2^2 \), \( a_3 = \lambda e_3^2 \), for some \( \lambda \in \mathbb{F}_q \). This means that the two lines sharing a point in \( \text{PG}(5, q) \) come from points in \( \text{PHG}(R_R^3) \) which are neighbours. This is impossible since \( \mathcal{R} \) contains exactly one point from each neighbour class (cf. Theorem 9).

Each one of the lines \( l_i \) contains a unique point which is not in \( \text{Supp} \tilde{\mathcal{R}} \). For the line \( l_i \) denote this point by \( P_i, i = 1, \ldots, q^2 + q + 1 \). As can be seen from the proof of Lemma 15, the points \( P_i \) are exactly the points of the plane in \( \text{PG}(5, q) \) defined by \( x_4 = x_5 = x_6 = 0 \). In what follows, we denote this plane by \( \pi \). □

**Lemma 16.** The spectrum of the multiset \( \tilde{\mathcal{R}} \) is

\[
\begin{align*}
a_{q^2+2q}^{\tilde{\mathcal{R}}} & = \frac{1}{2}q^2(q + 1)(q^2 + q + 1); \\
a_{q^2+q}^{\tilde{\mathcal{R}}} & = q^2 + q + 1; \\
a_{q^2}^{\tilde{\mathcal{R}}} & = \frac{1}{2}q^2(q - 1)(q^2 + q + 1); \\
a_i^{\tilde{\mathcal{R}}} & = 0, \quad \text{for all } i \neq q^2, q^2 + q, q^2 + 2q.
\end{align*}
\]  

**Proof.** The spectrum of a \((q^2 + q + 1, 2)\)-arc \( \mathcal{R} \) in \( \text{PHG}(R_R^3) \) is

\[
\begin{align*}
a_2^{\mathcal{R}} & = \frac{1}{2}q(q + 1)(q^2 + q + 1); \\
a_0^{\mathcal{R}} & = \frac{1}{2}q(q - 1)(q^2 + q + 1); \\
a_i^{\mathcal{R}} & = 0, \quad \text{for all } i \neq 0, 2.
\end{align*}
\]

By Theorem 9 in [11], the associated code \( C \) has spectrum

\[
\begin{align*}
A_{q^2, q+1, 0}^{\mathcal{R}}(C) & = \frac{1}{2}q^2(q - 1)(q^3 - 1), \\
A_{q^2, -1, 2}^{\mathcal{R}}(C) & = \frac{1}{2}q^2(q + 1)(q^3 - 1), \\
A_{0, q^2, q+1}^{\mathcal{R}}(C) & = q^3 - 1, \\
A_{0, 0, q^2+q+1}^{\mathcal{R}}(C) & = 1.
\end{align*}
\]

Here \( A_{i, j, \ell}(C) \) denotes the number of codewords in \( C \) which have exactly \( i \) components in \( R \setminus N \), exactly \( j \) components in \( N \setminus N^2 \) and exactly \( \ell \) components in \( N^2 = \{0\} \). By the definition of the RS map each word of \( C \) of type \((i, j, \ell)\) gives rise to a word of Hamming weight \((q - 1)i + jq \). Hence \( D \) has the spectrum

\[
\begin{align*}
A_{q^2+q}^{D} & = \frac{1}{2}q^2(q - 1)(q^3 - 1), \\
A_{q^2}^{D} & = q^3 - 1, \\
A_{q^2-q}^{D} & = \frac{1}{2}q^2(q + 1)(q^3 - 1), \\
A_0^{D} & = 1.
\end{align*}
\]

Each hyperplane \( H \) in \( \text{PG}(5, q) \) with \( \tilde{\mathcal{R}}(H) = w \) points corresponds to a set of \( q - 1 \) nonzero words which are scalar multiples of a word of weight \( q^3 + q^2 + q - w \). This implies that the multiset \( \tilde{\mathcal{R}} \) has the spectrum given in (8). □
Lemma 17. The multiset $\sim{\cal H}$ is an $(q(q^2 + q + 1), q^2 + 2q)$-arc in $\text{PG}(5, q)$ with the following properties:

(a) A hyperplane of multiplicity $q^2 + 2q$ contains two of the lines $l_i$.
(b) Any hyperplane of multiplicity $q^2 + q$ contains $\pi$ and $q + 1$ of the lines $l_i$. Moreover, if $l_1, l_2, \ldots, l_{q+1}$ are the lines in such hyperplane then the points $P_1, P_2, \ldots, P_{q+1}$ are collinear.
(c) A hyperplane of multiplicity $q^2$ does not contain any of the lines $l_i$.

Proof. Consider a solid $S$ defined by two of the skew lines $l_i$, say $l_{i1} = \langle P_{i1}, Q_1 \rangle$ and $l_{i2} = \langle P_{i2}, Q_2 \rangle$. Then without loss of generality, we can set:

$$P_{i1} = (a_1, a_2, a_3, 0, 0, 0), \quad Q_1 = (b_1, b_2, b_3, a_1^q, a_2^q, a_3^q),$$

$$P_{i2} = (c_1, c_2, c_3, 0, 0, 0), \quad Q_2 = (d_1, d_2, d_3, c_1^q, c_2^q, c_3^q),$$

where $a_i, b_i, c_i, d_i \in \mathbb{F}_q$, $\sigma \in \text{Aut} \mathbb{F}_q$. Moreover the vectors $(a_1, a_2, a_3)$ and $(c_1, c_2, c_3)$ are linearly independent since the lines $l_{i1}, l_{i2}$ are images of points that are not neighbours. Now any point in $S$ can be written as

$$\lambda_1 P_{i1} + \mu_1 Q_1 + \lambda_2 P_{i2} + \mu_2 Q_2,$$

where $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{F}_q$. The points in the intersection $\pi \cap S$ are the points with $x_4 = x_5 = x_6 = 0$. They have the form

$$\lambda_1 P_{i1} + \lambda_2 P_{i2},$$

whence it follows that the intersection of $S$ and $\pi$ is a line. Therefore, no solid through $\pi$ contains two of the lines $l_i$ and consequently every solid through $\pi$ is a $q$-solid and contains exactly one of the lines $l_i$.

This in turn implies that every hyperplane $H \supset \pi$ contains exactly $q + 1$ of the lines $l_i$. Hence $H$ is a $(q^2 + q)$-hyperplane. By Lemma 16 there are no further $(q^2 + q)$-hyperplanes, proving the first part of (b). Assume now $H$ is a $(q^2 + q)$-hyperplane containing the lines $l_{i1}, l_{i2}, \ldots, l_{i_{q+1}}$. Assume that the points $P_{i1}, P_{i2}, P_{i3}$ are not collinear. The solid $S = \langle l_{i1}, l_{i2} \rangle$ does not contain $\pi$ and therefore meets $l_{i3}$ in a point which is different from $P_{i3}$ (i.e. in a 1-point). Thus $\tilde{\cal H}(S) \geq 2q + 1$, a contradiction since a $(q^2 + q)$-hyperplane cannot contain solids with more than $2q$ points.\(^1\) This proves the second part of (b).

\(^1\)This is obtained by counting the number of points of $\tilde{\cal H}$ via the partition $\{S, H_1 \setminus S, H_2 \setminus S, \ldots, H_{q+1} \setminus S\}$ of $\cal P$, where $H_1, \ldots, H_{q+1}$ are the hyperplanes containing $S$. By assumption, at least one hyperplane $H_i$ is not a $(q^2 + 2q)$-plane. Hence $q(q^2 + q + 1) = \tilde{\cal H}(\cal P) = \tilde{\cal H}(S) + \sum_{i=1}^{q+1} \tilde{\cal H}(H_i \setminus S) < \tilde{\cal H}(S) + (q+1)(q^2 + 2q - \tilde{\cal H}(S))$ or, equivalently, $\tilde{\cal H}(S) < (q + 1)(q + 2) - (q^2 + q + 1) = 2q + 1$.\(^{1}\)
Finally, consider a hyperplane $H$ which meets $\pi$ in a line $l$. The hyperplane $H$ contains $z$ of the lines $l_i$ and meets $q^2$ of them in a point from $\text{Supp} \mathcal{R}$. Thus $\mathcal{R}(H) = zq + q^2$. By Lemma 16, $z \in \{0, 2\}$ and we get the rest of the lemma.  

Finally, in the proof of Theorem 13 we make use of the following simple observation: let $\mathcal{F}$ be an $(n, w)$-arc in $\text{PG}(k-1, q)$ and let $\delta$ be an $i$-dimensional flat in $\text{PG}(k-1, q)$. Fix a $(k-2-i)$-dimensional flat $\varepsilon$ such that $\delta \cap \varepsilon = \emptyset$. The projection $\varphi_{\delta, \varepsilon}$ from $\mathcal{P} \setminus \delta$ onto $\varepsilon$ is defined by

$$
\varphi_{\delta, \varepsilon} : \begin{cases} 
\mathcal{P} \setminus \delta & \rightarrow \varepsilon, \\
Q & \rightarrow \varepsilon \cap \langle \delta, Q \rangle.
\end{cases}
$$

The map from $\text{PG}(k-1, q) \setminus \text{PG}(\delta)$ to $\text{PG}(\varepsilon)$ induced by $\varphi_{\delta, \varepsilon}$ maps $(i+s)$-dimensional flats containing $\delta$ to $(s-1)$-dimensional flats in $\varepsilon$. The projection $\varphi := \varphi_{\delta, \varepsilon}$ induces a multiset $\mathcal{K}^\varphi$ in $\varepsilon$ by

$$
\mathcal{K}^\varphi : \begin{cases} 
\varepsilon & \rightarrow \mathbb{N}_0, \\
P & \rightarrow \sum_{Q : \varphi(Q) = P} \mathcal{K}(Q).
\end{cases}
$$

The multiset $\mathcal{K}^\varphi$ is an arc with parameters $(n - \mathcal{K}(\delta), w - \mathcal{K}(\delta))$, where $\mathcal{K}(\delta) = \sum_{P \not\in \delta} \mathcal{K}(P)$.

Now we can prove Theorem 13.

Proof (Proof of Theorem 13). Let $\delta$ be a plane that does not meet $\pi$ and consider the projection $\varphi := \varphi_{\delta, \pi}$. The induced arc $\mathcal{K}^\varphi$ does not have any lines of multiplicity $q^2 + q - \mathcal{K}(\delta)$ since every $(q^2 + q)$-hyperplane in $\text{PG}(5, q)$ contains $\pi$, but $\dim(\delta, \pi) = 5$. Hence $\mathcal{K}^\varphi$ is a two-weight arc with weights $q^2 + 2q - \mathcal{K}(\delta)$ and $q^2 - \mathcal{K}(\delta)$. Denote by $x$ (respectively, by $y$) the number of lines $l$ in $\pi$ with $\mathcal{K}^\varphi(l) = q^2 + 2q - \mathcal{K}(\delta)$ (respectively, $\mathcal{K}^\varphi(l) = q^2 - \mathcal{K}(\delta)$). Then, clearly,

$$
x + y = q^2 + q + 1,
(q^2 + 2q - \mathcal{K}(\delta))x + (q^2 - \mathcal{K}(\delta))y = (q + 1)(q^3 + q^2 + q - \mathcal{K}(\delta)),
$$

whence $2x = q^2 + q + 1 + q \cdot \mathcal{K}(\delta)$. This is a contradiction since the right-hand side is odd (note that $q = 2^m$).

Acknowledgments

The authors are indebted to the referee for pointing out a gap in the original proof of Theorem 13 and for valuable comments which helped to improve the presentation.

References


