Two-intersection sets in projective Hjelmslev spaces

Thomas Honold

***Abstract*— A set S of points in a finite incidence structure is said to be a two-intersection set if there are integers $a < b$ such that S meets every block in either a or b points (and both a, b actually occur as intersection numbers). For point-hyperplane designs of the classical geometries $\mathrm{PG}(k,q)$ such sets have been studied extensively and related to other combinatorial objects (maximal arcs, two-weight codes, strongly-regular graphs, partial difference sets). In this paper two-intersection sets in the coordinate projective Hjelmslev geometries $\mathrm{PHG}(k,R)$ over finite chain rings R of length 2 are investigated along similar lines.**

I. INTRODUCTION

Throughout the paper R denotes a chain ring of length 2 with residue field $R/\operatorname{Rad} R \cong \mathbb{F}_q$. If $q = p^r$, p prime, there are exactly $r+1$ isomorphism types of such rings, the Galois ring $\mathbb{G}_q = \mathrm{GR}(q^2, p^2)$ and r truncated skew polynomial rings $\mathbb{S}_q^\sigma = \mathbb{F}_q[X;\sigma]/(X^2)$, $\sigma \in \operatorname{Aut}\mathbb{F}_q$. All these rings have $|R| = q^2$, $|\operatorname{Rad} R| = q$. We will write $N = \operatorname{Rad} R = R\theta = \theta R$, where we can take $\theta = p$ if $R = \mathbb{G}_q$, respectively, $\theta = X$ if $R = \mathbb{S}_q^\sigma$.

For an integer $k \geq 1$ the k-dimensional (right) projective Hjelmslev geometry over R, denoted by $\mathrm{PHG}(k,R)$, is defined as the point-line incidence structure $(\mathcal{P}, \mathcal{L}, \subseteq)$ whose points (lines) are the free rank-1 submodules (resp. free rank-2 submodules) of R_R^{k+1} (or any other free right R-module of rank $k+1$) and whose incidence relation is set inclusion.[1]

Projective Hjelmslev geometries form an important tool for the investigation of linear codes over finite chain rings—just like the classical geometries $\mathrm{PG}(k,q)$ are used to describe linear codes over $\mathbb{F}_q$ in a geometric manner. The underlying theory has been developed in detail in [12], followed by a study of arcs and blocking sets in projective Hjelmslev planes [24], [13]. This and later work has unveiled the interesting fact—well-known in the classical case—that arcs of maximum size (i.e. point sets yielding good linear codes) often have only few distinct intersection numbers with hyperplanes.

This paper deals with the most important case—point sets in $\mathrm{PHG}(k,R)$ with only two distinct intersection numbers with respect to hyperplanes. In the planar case and for selected small chain rings a study of such sets was made in [20]. Rather than updating the tables of [20] and providing an exhaustive list of constructions, we will develop the general theory of such sets in this paper and mention only selected examples.

In what follows $\mathcal{H}$ denotes the set of hyperplanes of $\mathrm{PHG}(k,R)$ (free rank k submodules of R_R^{k+1}). It goes without saying that such hyperplanes (and similarly lines and other subspaces) are identified with subsets of the point set $\mathcal{P}$ in the obvious way.

Definition I.1 *Suppose a, b are integers satisfying $0 \leq a < b$. A* two-intersection set of type (a,b) *in $\mathrm{PHG}(k,R) = (\mathcal{P}, \mathcal{L}, \subseteq)$ is a point set $S \subseteq \mathcal{P}$ satisfying $\bigl\{|S \cap H|; H \in \mathcal{H}\bigr\} = \{a, b\}$.*

Remark I.2 *One-intersection sets in $\mathrm{PHG}(k,R)$ (defined in the same way) are trivial: Using the (easily established) fact that the incidence matrix of the point-hyperplane design of $\mathrm{PHG}(k,R)$ is invertible over $\mathbb{Q}$, it is immediate that the only such point sets are $\mathcal{P}$ and $\emptyset$.*

As is well-known, two-intersection sets in classical Galois geometries $\mathrm{PG}(k,q)$ give rise to two-weight linear codes over $\mathbb{F}_q$, and also to strongly regular Cayley graphs (equivalently, regular partial difference sets) for the additive groups of $\mathbb{F}_q$; see [6], [3], [26] for example. It was shown in [2] that the correspondence between two-weight codes and strongly regular graphs carries over to the case of so-called Frobenius rings (of which chain rings are a special case), provided one replaces the Hamming weight by the so-called homogeneous weight. In [2] nontrivial examples of the correspondence were given for the special case of chain rings of length 2. These examples were derived from two-intersection sets in the planes $\mathrm{PHG}(2,R)$. A generalization of one of the constructions in [2] to the higher-dimensional case can be found in [23] and will be the subject of Example II.2.

The two-intersection sets of [2], [23] are of a very special nature. Several further examples of two-intersection sets in $\mathrm{PHG}(k,R)$ are known, of which the point sets corresponding to the shortened Kerdock codes ("Teichmüller sets") are probably the most prominent representatives.

In the sequel we establish a similar correspondence—using three-weight codes and abelian association schemes—for a larger class of two-intersection sets.

Following common practice among coding theorists we will make a slight notational change, $\mathrm{PHG}(k-1,R)$ in place of $\mathrm{PHG}(k,R)$, so that from now on k matches the rank of the "ambient module" R_R^k rather than the geometric dimension of $\mathrm{PHG}(k-1,R)$. We will also switch to multiset notation for point sets in $\mathrm{PHG}(k-1,R)$ (by identifying $S \subseteq \mathcal{P}$ with

Supported by the National Natural Science Foundation of China under Grant No. 60872063

Thomas Honold is with the Department of Information and Electronic Engineering, Zhejiang University, 38 Zheda Road, 310027 Hangzhou, China
honold@zju.edu.cn

[1] The k-dimensional left projective Hjelmslev geometry over R, defined in an analogous way using left R-modules, is isomorphic to $\mathrm{PHG}(k, R^\circ)$, the corresponding right projective Hjelmslev geometry over the opposite chain ring R°; see Remark IV.2 below.

its characteristic function $\mathfrak{K}\colon \mathcal{P} \to \mathbb{N}_0$), so that by means of $\mathfrak{K}(X) = \sum_{x \in X} \mathfrak{K}(x)$ we can assign a multiplicity to arbitrary subsets $X \subseteq \mathcal{P}$.

The geometry $\mathrm{PHG}(k-1, R)$ has $q^{k-1} \cdot \frac{q^k-1}{q-1}$ points and hyperplanes, falling into $\frac{q^k-1}{q-1}$ neighbour classes $[x]$ resp. $[H]$ of size q^{k-1}. Here two points $x, x' \in \mathcal{P}$ are neighbours (notation: $x \subset x'$) if they are incident with two distinct lines $L, L' \in \mathcal{L}$, and two hyperplanes $H, H' \in \mathcal{H}$ are neighbours (notation: $H \subset H'$) if $\bigl\{[x]; x \in H\bigr\} = \bigl\{[x]; x \in H'\bigr\}$. The incidence structure induced on the point and hyperplane classes of $\mathrm{PHG}(k-1, R)$ is isomorphic to the point-hyperplane design of $\mathrm{PG}(k-1, q)$.

For further properties of $\mathrm{PHG}(k-1, R)$ (in particular various counting formulas, which will be needed in the sequel) we refer to [12], [16], [25].

II. EXAMPLES

Singleton point sets and their complements form trivial 2-intersection sets of type $(0,1)$ resp. $(h-1, h)$ in $\Pi = \mathrm{PHG}(k-1, R)$, $k \geq 2$, where $h = q^{k-2} \cdot \frac{q^{k-1}-1}{q-1}$ denotes the cardinality of a hyperplane. Slightly less trival examples are the neighbour classes $[T]$ of Hjelmslev subspaces T with $0 \leq \dim T \leq k-2$. We note that other subspaces do not form 2-intersection sets. For example, lines in $\mathrm{PHG}(k-1, R)$, $k \geq 3$, intersect hyperplanes in sets of three different sizes $1, q, q^2+q$.

Example II.1 *Suppose $\mathfrak{k}$ is a two-intersection set of type (a', b') in the quotient plane $\overline{\Pi} \cong \mathrm{PG}(k-1, q)$ of Π. Define a set $\mathfrak{K}$ of points in Π by $\mathfrak{K}(x) = \mathfrak{k}\bigl([x]\bigr)$ for $x \in \mathcal{P}$ (i.e., $\mathfrak{K}$ is the union of all point classes in $\mathfrak{k}$). Then $\mathfrak{K}$ is a two-intersection set of type $(a, b) = \bigl(a'q^{k-2}, b'q^{k-2}\bigr)$. The map $\mathfrak{k} \mapsto \mathfrak{K}$ will be called “lifting construction”.*

We note that neighbour classes of Hjelmslev subspaces are obtained by applying the lifting construction to subspaces of $\mathrm{PG}(k-1, q)$, so that the earlier example is a special case of Example II.1.

The next example (taken from [23]) uses so-called *hyperplane segments*, which are defined as non-empty intersections $H \cap [x]$ ($H \in \mathcal{H}$, $x \in \mathcal{P}$). It is known that a hyperplane segment $S = H \cap [x]$ forms a hyperplane of the affine space $[x] \cong \mathrm{AG}(k-1, q)$, and that $H' \cap [x] \parallel S$ for $H' \in \mathcal{H}$ iff $H' \in [H]$. The class $[H]$ is called the *direction* of the hyperplane segment S.

Example II.2 *In each point neighbour class $[x]$ choose a hyperplane segment S of direction $[H]$ in such a way that the resulting pairs $\bigl([x], [H]\bigr)$ (flags of the point-hyperplane design of the quotient geometry $\overline{\Pi} \cong \mathrm{PG}(k-1, q)$) form a perfect matching of the corresponding incidence graph. The union of all these hyperplane segments (a set of cardinality $q^{k-2} \cdot \frac{q^k-1}{q-1}$) is a 2-intersection set of type (a, b) with $a = q^{k-3}(q^{k-2} + q^{k-3} + \cdots + q^2 + q)$, $b = q^{k-3}(q^{k-2} + q^{k-3} + \cdots + q^2 + 2q)$.*

Another example is related to the $\mathbb{Z}_4$-linear representation of the binary Kerdock codes. For this example we need the fact that the ring extension $\mathbb{G}_{q^k}/\mathbb{G}_q$ is free of rank k and hence can be taken as the ambient module for $\mathrm{PHG}(k-1, \mathbb{G}_q)$. The Teichmüller set $\mathfrak{T}$ is defined as the set of points in $\mathrm{PHG}(k-1, \mathbb{G}_q)$ generated by the elements of the subgroup $T \leq \mathbb{G}_{q^k}^{\times}$ of order $q^k - 1$. (This subgroup is uniquely determined and cyclic.) The set $\mathfrak{T}$ has cardinality $\frac{q^k-1}{q-1}$ and forms a transversal for the point neighbour classes of $\mathrm{PHG}(k-1, \mathbb{G}_q)$.

Example II.3 *If q is even and $k \geq 3$ is odd then $\mathfrak{T}$ is a 2-intersection set of type $\Bigl(\frac{q^{k-2}-1}{q-1} - q^{(k-3)/2}, \frac{q^{k-2}-1}{q-1} + q^{(k-3)/2}\Bigr)$.*

This can be derived from the results in [27], [21], but we will give an independent proof in Theorem V.7. In the planar case Example II.3 reduces to the hyperovals of [14].

Several further examples of planar (i.e. $k = 3$) two-intersection sets are known (cf. [18], [22], [20], [10]), of which we mention only the following.

Example II.4 *In $\mathrm{PHG}(2, \mathbb{Z}_9)$ and $\mathrm{PHG}(2, \mathbb{G}_4)$ there exist two-intersection sets $\mathfrak{K}$ of type $(2,5)$ respectively $(2,6)$, which can be obtained as unions of orbits of a collineation of order q^2+q+1 (a “lifted Singer cycle”); see [18]. The points of $\mathfrak{K}$ in each point class form a triangle, respectively, a quadrangle with parallel sides. The first set is a maximal $(39,5)$ arc in $\mathrm{PHG}(2, \mathbb{Z}_9)$, and the second set is a maximal $(84,6)$-arc in $\mathrm{PHG}(2, \mathbb{G}_4)$; see [11], [10].*

Example II.5 *Suppose $q = 4$ (so $|R| = 16$), and let $[z]$, $[M]$ be a non-incident point-line pair of the quotient plane $\mathrm{PG}(2,4)$. The class $[z]$ and the point classes on $[M]$ remain empty. In each of the remaining point classes $[x]$ choose 2 parallel line segments with direction $[xz]$ in such a way that the 6 line segments with a fixed direction $[L]$ form a hyperoval in the projective plane induced on $[L]$. The so-defined set of $15 \cdot 8 = 120$ points in $\mathrm{PHG}(2, R)$ is a two-intersection set of type $(0, 8)$. For the two chain rings of characteristic 2 this construction provides $(k, 8)$-arcs of the largest known size k; see [10].*

Note that in the last example $\mathfrak{K}$ does not meet every point neighbour class in the same number of points.

III. RESTRICTIONS ON THE PARAMETERS

Suppose $\mathfrak{K}$ is a two-intersection set of type (a, b) in $\mathrm{PHG}(k-1, R)$, $\mathcal{H}_a = \bigl\{H \in \mathcal{H}; \mathfrak{K}(H) = a\bigr\}$, $\mathcal{H}_b = \bigl\{H \in \mathcal{H}; \mathfrak{K}(H) = b\bigr\}$, $n_a = |\mathcal{H}_a|$, $n_b = |\mathcal{H}_b|$ and $\mu_i = \sum_{H \in \mathcal{H}} \mathfrak{K}(H)^i$ for $i = 0, 1, 2, \ldots$ The frequencies n_a, n_b are computed from

$$n_a + n_b = \mu_0 = |\mathcal{H}| = q^{k-1} \cdot \frac{q^k - 1}{q-1},$$

$$an_a + bn_b = \mu_1 = |\mathfrak{K}| \cdot q^{k-2} \cdot \frac{q^{k-1} - 1}{q-1}.$$

Solving the system we obtain

$$n_a = \frac{b\mu_0 - \mu_1}{b-a}, \quad n_b = \frac{a\mu_0 - \mu_1}{a-b}. \tag{1}$$

The same reasoning can be applied to any subset $\mathcal{H}' \subset \mathcal{H}$ for which we can compute the corresponding moments μ_0', μ_1'.

For a 2-intersection set in the classical geometry $\mathrm{PG}(k-1,q)$ the number $b-a$ has to be a divisor of q^{k-2}; cf. [3, Cor. 5.5]. Here we have a similar restriction.

Theorem III.1 *Let $\mathfrak{K}$ be a 2-intersection set of type (a,b) in $\mathrm{PHG}(k-1,R)$, which is not a union of point classes (i.e. not obtained through the lifting construction), and let d be the g.c.d. of all numbers $\mathfrak{K}(S)-\mathfrak{K}(S')$, where S,S' are parallel hyperplane segments contained in the same point class. Then $d \mid q^{k-2}$ and $b-a \mid dq^{k-2}$.*

The theorem implies in particular $b-a \mid q^{2(k-2)}$, which is also true for 2-intersection sets obtained by the lifting construction.[2]

Proof: For a hyperplane class $[H]$ and a point $x \supset H$ we consider the subset $\mathcal{H}'(x) = \{H' \in [H]; x \in H'\}$. Using obvious notation we have

$$\begin{aligned} n_a'(x) + n_b'(x) &= \mu_0'(x) = |\mathcal{H}'(x)| = q^{k-2}, \\ an_a'(x) + bn_b'(x) &= \mu_1'(x) = \sum_{H' \in \mathcal{H}'(x)} \mathfrak{K}(H') \\ &= q^{k-2}\mathfrak{K}(S_x) + q^{k-3}\mathfrak{K}\big([H] \setminus [x]\big), \end{aligned}$$

where S_x denotes the hyperplane segment with direction $[H]$ through x. Solving for $n_a'(x)$ we obtain $n_a'(x) = \big(b\mu_0'(x) - \mu_1'(x)\big)(b-a)^{-1}$ (see (1)), and for $x,y \supset H$ with $[x]=[y]$ further

$$\begin{aligned} n_a'(x) - n_a'(y) &= \frac{\mu_1'(y) - \mu_1'(x)}{b-a} \\ &= \frac{q^{k-2}\big(\mathfrak{K}(S_y) - \mathfrak{K}(S_x)\big)}{b-a}. \end{aligned} \tag{2}$$

Since $n_a'(x) - n_a'(y)$ is an integer, we have $b-a \mid dq^{k-2}$.

Now let $[x]$ be an arbitrary point class and $\mathcal{S}$ the set of hyperplane segments contained in $[x]$ (i.e., $\mathcal{S}$ is the set of hyperplanes of the affine space $[x] \cong \mathrm{AG}(k-1,q)$). Further let $\mathcal{S}(x) = \{S \in \mathcal{S}; x \in S\}$. A straightforward counting argument yields

$$\begin{aligned} \sum_{S \in \mathcal{S}(x)} \mathfrak{K}(S) &= \frac{q^{k-1}-1}{q-1} \cdot \mathfrak{K}(x) + \frac{q^{k-2}-1}{q-1} \cdot \mathfrak{K}\big([x] \setminus \{x\}\big) \\ &= q^{k-2} \cdot \mathfrak{K}(x) + \frac{q^{k-2}-1}{q-1} \cdot \mathfrak{K}\big([x]\big). \end{aligned}$$

The set $\mathcal{S}(x)$ contains exactly one representative from each parallel class of hyperplane segments in $[x]$. Hence by definition of d we have $\sum_{S \in \mathcal{S}(x)} \mathfrak{K}(S) \equiv \sum_{S \in \mathcal{S}(y)} \mathfrak{K}(S) \pmod{d}$, provided only that $[x]=[y]$. Thus d divides $q^{k-2}\big(\mathfrak{K}(x) - \mathfrak{K}(y)\big)$ in this case. Choosing $x \in \mathfrak{K}$, $y \notin \mathfrak{K}$ (which is possible, since $\mathfrak{K}$ by assumption is not a union of point classes) we conclude that $d \mid q^{k-2}$. ■

IV. DUALITY

We now specialize the general duality theory for multisets in $\mathrm{PHG}(k-1,R)$ developed in [15] to the case of a 2-intersection set $\mathfrak{K}$.

We apply the method of the previous section to the sets $\mathcal{H}(x) = \{H \in \mathcal{H}; x \in H\}$, where $x \in \mathcal{P}$. The numbers $n_a(x) = \{H \in \mathcal{H}_a; x \in H\}$, $n_b(x) = \{H \in \mathcal{H}_b; x \in H\}$ satisfy the two equations

$$\begin{aligned} n_a(x) + n_b(x) &= \mu_0(x) = |\mathcal{H}(x)| = q^{k-2} \cdot \frac{q^{k-1}-1}{q-1}, \\ an_a(x) + bn_b(x) &= \mu_1(x) = \sum_{H \in \mathcal{H}(x)} \mathfrak{K}(H) \\ &= \mathfrak{K}(x)q^{2(k-2)} + \frac{q^{k-3}(q^{k-2}-1)}{q-1}\Big((q-1)\mathfrak{K}\big([x]\big) + |\mathfrak{K}|\Big), \end{aligned}$$

from which we can compute $n_a(x)$, $n_b(x)$. In general these numbers depend on $\mathfrak{K}(x)$ and $\mathfrak{K}\big([x]\big)$.

Theorem IV.1 *Suppose $\mathfrak{K}$ is a 2-intersection set in $\mathrm{PHG}(k-1,R)$, which meets every point neighbour class in the same number of points, and $x,y \in \mathcal{P}$ are such that $\mathfrak{K}(x)=1$, $\mathfrak{K}(y)=0$ (i.e. $x \in \mathfrak{K}$, $y \notin \mathfrak{K}$). Then $\mathcal{H}_a$ (and similarly $\mathcal{H}_b$) is a 2-intersection set of cardinality n_a and type $(a^*,b^*) = \big(n_a(x), n_a(y)\big)$ in the dual Hjelmslev geometry $\mathrm{PHG}(k-1,R^\circ)$. Moreover, the types of $\mathfrak{K}$ and $\mathcal{H}_a$ are related by*

$$(b-a)\cdot(b^*-a^*) = q^{2(k-2)}.$$

The two-intersection set $\mathcal{H}_a$ in $\mathrm{PHG}(k-1,R^\circ)$ is called the *dual* of the two-intersection set $\mathfrak{K}$ in $\mathrm{PHG}(k-1,R)$, and denoted by $\mathfrak{K}^*$. Since $\mathcal{H}_a^*$ is in turn equivalent to $\mathfrak{K}$, two-intersection sets come in dual pairs.[3]

Proof: By assumption $\mathfrak{K}\big([x]\big) = u$ is a constant, so that $n_a(x)$ depends only on $\mathfrak{K}(x)$, which takes the values 0 and 1. This shows already that $\mathcal{H}_a$ is a two-intersection set in the dual Hjelmslev geometry. If $x,y \in \mathcal{P}$ are such that $\mathfrak{K}(x)=1$, $\mathfrak{K}(y)=0$ then

$$n_a(y) - n_a(x) = \frac{\mu_1(x) - \mu_1(y)}{b-a} = \frac{q^{2(k-2)}}{b-a} > 0,$$

showing that the type of $\mathcal{H}_a$ is $\big(n_a(x), n_a(y)\big)$ and also the asserted relation to the type of $\mathfrak{K}$. ■

Remark IV.2 *The isomorphism between $\mathrm{PHG}(k-1,R^\circ)$, or rather the corresponding left projective Hjelmslev geometry $\Pi^\circ = (\mathcal{P}^\circ, \mathcal{L}^\circ, \subseteq)$ over R, and the dual Π^* of $\Pi = \mathrm{PHG}(k-1,R)$ can be made more explicit. Writing $\mathbf{x} \cdot \mathbf{y} = x_1y_1 + \cdots + x_ky_k$ for $\mathbf{x},\mathbf{y} \in R^k$ and $U^\perp = \{\mathbf{y} \in R^k; \mathbf{x} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{x} \in U\}$ for $U \leq {}_RR^k$, we have that $U \mapsto U^\perp$ induces an isomorphism $\Pi^\circ \cong \Pi^*$; cf. [12, Th. 3.1]. Under this isomorphism every hyperplane $H \in \mathcal{H}$*

[2] This follows from $b'-a' \mid q^{k-2}$.

[3] This does not exclude the possibility of self-dual two-intersection sets. In fact many of the known two-intersection sets, for example those of Examples II.2 and II.4, are self-dual.

corresponds to a unique point $R\mathbf{a} \in \mathcal{P}^\circ$ in Π°, which is determined by $H = (R\mathbf{a})^\perp$ or, viewing H as a set of points of Π, by $H = \{\mathbf{x}R \in \mathcal{P}; a_1x_1 + \cdots + a_kx_k = 0\}$. The condition $R\mathbf{a} \in \mathcal{P}^\circ$ is equivalent to $\mathbf{a}R \in \mathcal{P}$ (i.e. at least one a_i must be a unit in R).

Example IV.3 *For even q and odd $k \geq 3$ the dual $\mathfrak{T}^*$ of the Teichmüller set $\mathfrak{T}$ is again a 2-intersection set in $\mathrm{PHG}(k-1, \mathbb{G}_q)$. Its size is*

$$n_a = \frac{1}{2}\left(q^{k-1} - q^{(k-1)/2}\right) \cdot \frac{q^k - 1}{q-1},$$

and its type is

$$a^* = \frac{1}{2(q-1)}(q^{2k-3} - q^{(3k-3)/2} - q^{k-2} + q^{(k-1)/2}),$$
$$b^* = \frac{1}{2(q-1)}(q^{2k-3} - q^{(3k-5)/2} - q^{k-2} + q^{(k-1)/2}).$$

In the planar case $k = 3$ the set $\mathfrak{T}^*$ has type $(0, q^2/2)$ and forms a maximal $\left(\frac{1}{2}(q^4 - q), q^2/2\right)$-arc in $\mathrm{PHG}(2, \mathbb{G}_q)$.

The series of excellent $\mathbb{Z}_4$-linear codes constructed in [19] is related to the sets $\mathfrak{T}^*$ in $\mathrm{PHG}(2, \mathbb{Z}_4)$.

V. Relations to Other Combinatorial Objects

A. Linear Codes

According to [12], for any set S of points in $\mathrm{PHG}(k-1, R)$ there is an associated linear code $C \leq {}_RR^n$ of length $n = |S|$ over R. The code C is generated by a $k \times n$-matrix $\mathbf{G}$ over R, whose columns are coordinate vectors for the points of S; it is the "left row space" of $\mathbf{G}$. Defining $\Sigma = \{\mathbf{g} \in R^k; \mathbf{g}R \in S\}$, we have $\Sigma R^\times = \Sigma$ ("Σ is invariant") and $|C| = |\langle\Sigma\rangle|$, where $\langle\Sigma\rangle = \sum_{\mathbf{g}\in\Sigma} \mathbf{g}R = \sum_{\mathbf{g}R\in S} \mathbf{g}R$.

The (normalized) homogeneous weight on R is the function $\mathrm{w}_{\mathrm{hom}} \colon R \to \mathbb{Q}$ defined by

$$\mathrm{w}_{\mathrm{hom}}(x) = \begin{cases} 0 & \text{if } x = 0, \\ \frac{q}{q-1} & \text{if } x \in N \setminus \{0\}, \\ 1 & \text{if } x \in R \setminus N. \end{cases} \tag{3}$$

The function $\mathrm{w}_{\mathrm{hom}}$ is extended to R^n by means of $\mathrm{w}_{\mathrm{hom}}(\mathbf{x}) = \sum_{i=1}^n \mathrm{w}_{\mathrm{hom}}(x_i)$. In the case $R = \mathbb{Z}_4 = \mathbb{G}_2$ it coincides with the Lee weight.[4]

Proposition V.1 *Suppose S meets every point neighbour class in the same number $u \geq 1$ of points. Then the corresponding code C has nonzero homogeneous weights*

$$\frac{uq^k}{q-1} \quad \text{and} \quad \frac{u(q^k + q^{k-2} + q^{k-3} + \cdots + q) - q|S \cap H|}{q-1},$$

where H runs through all hyperplanes of $\mathrm{PHG}(k-1, R)$.

Proof: Apply [12, Th. 5.2]. ■

Thus the number of nonzero homogeneous weights of C is $t := \{|S \cap H|; H \in \mathcal{H}\}$ or $t + 1$. The first case occurs iff there exists a hyperplane H with $|S \cap H| = u(q^{k-3} + q^{k-2} + \cdots + 1)$.

B. Linear Association Schemes over R

Let $(M, +)$ be a finite abelian group and $\mathcal{D} = \{D_0, D_1, \ldots, D_t\}$ be a partition of M into $t+1$ sets satisfying $D_0 = \{0\}$ and $D_i = -D_i$ for all i. Define relations (i.e., Cayley graphs) G_i on M by $(x, y) \in G_i \iff x - y \in D_i$. Recall that $\mathcal{G} = \{G_0, G_1, \ldots, G_t\}$ is said to be an abelian t-class asssocation scheme (with relations G_i and abelian classes D_i) on M if for $x, y \in M$ and $0 \leq i, j \leq t$ the number of elements $z \in M$ such that $(x, z) \in G_i$ and $(z, y) \in G_j$ depends only on the relation G_k to which (x, y) belongs, but not on the particular choice of x, y.

Here we are interested in abelian association schemes on the additive group of a finite (right) R-module M_R. We further require $D_iR^\times = D_i$, i.e. the abelian classes (and hence also the relations G_i) should be invariant under the action of $R^\times$. Abelian association schemes with this property are said to be *linear over R*.

Abelian association schemes are best described in terms of the characteristic functions $\delta_{D_i} \colon M \to \mathbb{C}$ of their abelian classes D_i. The set $\mathbb{C}M = \mathbb{C}^M$ of all functions $f \colon M \to \mathbb{C}$ forms a $\mathbb{C}$-algebra in two different ways, first with respect to the point-wise multiplication ("Hadamard product") $(f \cdot g)(x) = f(x)g(x)$ and second with respect to the group algebra multiplication ("convolution") $(f * g)(x) = \sum_{y\in M} f(y)g(x-y)$; the latter is simply the $\mathbb{C}$-linear extension of the rule $\delta_x * \delta_y = \delta_{x+y}$ for $x, y \in M$.[5]

Now $\mathcal{D} = \{D_0, D_1, \ldots, D_t\}$ defines an abelian association scheme iff the $\mathbb{C}$-subspace generated by δ_{D_0}, δ_{D_1}, …, δ_{D_t}, which is obviously a subalgebra of $(\mathbb{C}M, \cdot)$, also is a subalgebra of $(\mathbb{C}M, *)$. This property in turn can be succintly expressed using complex characters of $(M, +)$. For characters χ, ψ we write $\chi \sim \psi$ if $\chi(D_i) = \psi(D_i)$ for $0 \leq i \leq t$.[6] Since $\sim$ is an equivalence relation on the character group $\widehat{M}$ of $(M, +)$, it induces a partition $\widehat{\mathcal{D}}$ of $\widehat{M}$.

Fact V.2 *We have $|\widehat{\mathcal{D}}| \geq |\mathcal{D}|$ with equality iff $\mathcal{D}$ defines an abelian association scheme on M.*

Proof: We sketch a proof of this important fact. Other proofs can be found in [7], [4].

The characters in $\widehat{M}$, scaled by $\frac{1}{|M|}$, form a complete set of primitive idempotens of $(\mathbb{C}M, *)$, so that $(\mathbb{C}M, *) \cong (\mathbb{C}M, \cdot)$ and any bijection $\widehat{M} \to \{\delta_x; x \in M\}$ extends linearly to an isomorphism from $(\mathbb{C}M, *)$ to $(\mathbb{C}M, \cdot)$.

The subalgebras of $(\mathbb{C}M, \cdot)$ are easily described. They are in one-to-one correspondence with the partitions $\mathcal{P} = \{P_1, \ldots, P_s\}$ of M, where for such a partition $\mathcal{P}$ the functions δ_{P_1}, …, δ_{P_s} are the primitive idempotents of the corresponding subalgebra $A_\mathcal{P}$. Elements $x, y \in M$ belong to the same member of $\mathcal{P}$ iff $f(x) = f(y)$ for all $f \in A_\mathcal{P}$.

Using this and the representation $\delta_{D_i} = |M|^{-1} \sum_{\psi\in\widehat{M}} \overline{\psi}(D_i)\psi$ we find that the dimension of

[4] For further information on homogeneous weight see [5], [17], [8].

[5] We write δ_X for the characteristic function of $X \subseteq M$ and use the shorthand δ_x in place of $\delta_{\{x\}}$.

[6] Here it is understood that a character χ is extended to $\mathbb{C}M$ by means of $\chi(f) = \chi\left(\sum_{x\in M} f(x)\delta_x\right) = \sum_{x\in M} f(x)\chi(x)$.

the subalgebra generated by δ_{D_0}, δ_{D_1}, …, δ_{D_t} is equal to $|\widehat{\mathcal{D}}|$. Fact V.2 now easily follows. ■

C. The Budapest Connection

In this subsection we assume that S is a set of points in $\mathrm{PHG}(k-1,R)$ which meets every point neighbour class in the same number u of points; in particular $|S| = u(q^{k-1} + q^{k-2} + \cdots + 1)$. In order to avoid trivialities we assume further $1 \leq u \leq q^{k-1} - 1$. Then the associated set Σ of vectors in R^k (cf. Section V-A) generates R^k_R. The linear code $C \leq {}_R R^n$ associated with S (cf. again Section V-A is free of rank k, and the rows of $\mathbf{G}$ form a basis of C. (This follows from $|C| = |\langle\Sigma\rangle| = |R|^k$.)

We fix a generating character χ of R (i.e. an additive character of R whose restriction to N is nontrivial) and denote the standard inner product of two vectors $\mathbf{x}, \mathbf{y} \in R^k$ by $\mathbf{x}\cdot\mathbf{y}$ (as in Remark IV.2). Then every character of $(R^k, +)$ has the form $\chi_{\mathbf{a}} \colon R^k \to \mathbb{C}^\times$, $\mathbf{x} \mapsto \chi(\mathbf{a}\cdot\mathbf{x})$ for a unique vector $\mathbf{a} \in R^k$. The following lemma, which relates the homogeneous weight of a typical codeword $\mathbf{aG} \in C$ to the value of the character $\chi_{\mathbf{a}}$ at Σ, is fundamental.

Lemma V.3 *For $\mathbf{a} \in R^k$ we have*

$$\mathrm{w}_{\mathrm{hom}}(\mathbf{aG}) = |S| - \frac{\chi_{\mathbf{a}}(\Sigma)}{|R^\times|}.$$

Proof: Using the formula $\mathrm{w}_{\mathrm{hom}}(x) = 1 - \frac{1}{|R^\times|}\sum_{u\in R^\times}\chi(xu)$ for $x \in R$ established in [9], we have

$$\begin{aligned}
\mathrm{w}_{\mathrm{hom}}(\mathbf{aG}) &= \sum_{\mathbf{g}R\in S} \mathrm{w}_{\mathrm{hom}}(\mathbf{a}\cdot\mathbf{g}) \\
&= \sum_{\mathbf{g}R\in S}\left(1 - \frac{1}{|R^\times|}\sum_{u\in R^\times}\chi(\mathbf{a}\cdot\mathbf{g}u)\right) \\
&= |S| - \frac{1}{|R^\times|}\sum_{\mathbf{g}R\in S}\sum_{u\in R^\times}\chi_{\mathbf{a}}(\mathbf{g}u) \\
&= |S| - \frac{1}{|R^\times|}\sum_{\mathbf{x}\in\Sigma}\chi_{\mathbf{a}}(\mathbf{x}),
\end{aligned}$$

proving the lemma. ■

The equation $\mathbf{a}\cdot\mathbf{x} = a_1x_1 + \cdots + a_kx_k = 0$ determines a hyperplane H of $\mathrm{PHG}(k-1,R)$, provided that $\mathbf{a} \in R^k \setminus N^k$. If $\mathbf{a} \in N^k \setminus \{\mathbf{0}\}$, then $\mathbf{a} = \theta\mathbf{a}'$ for some $\mathbf{a}' \in R^k \setminus N^k$ and $\mathbf{a}\cdot\mathbf{x} = 0$ determines exactly those points which are neighbours to the hyperplane H' with equation $\mathbf{a}'\cdot\mathbf{x} = 0$.

Lemma V.4

$$\chi_{\mathbf{a}}(\Sigma) = \begin{cases} u(q^{k+1} - q) & \textit{if } \mathbf{a} = \mathbf{0}, \\ -uq & \textit{if } \mathbf{a} \in N^k \setminus \{\mathbf{0}\}, \\ q^2|S \cap H| - \frac{u(q^k - q)}{q-1} & \textit{if } \mathbf{a} \in R^k \setminus N^k, \end{cases}$$

where in the last case H denotes the hyperplane in $\mathrm{PHG}(k-1,R)$ *with equation $\mathbf{a}\cdot\mathbf{x} = 0$.*

Proof: The lemma can be derived from [12, Th. 5.2] (see Prop. V.1) and Lemma V.3, but we give a direct proof.

We have $\chi(0) = 1$, $\chi\big(N \setminus \{0\}\big) = \chi(N) - \chi(0) = -1$, $\chi(R \setminus N) = \chi(R) - \chi(N) = 0$.

If $\mathbf{a} = \mathbf{0}$, then $\chi_{\mathbf{a}}(\Sigma) = |\Sigma| = |\Sigma||R^\times| = u \cdot \frac{q^k-1}{q-1} \cdot (q^2 - q) = u(q^{k+1} - q)$. For the other cases we use the formula

$$\chi_{\mathbf{a}}(\Sigma) = \sum_{\mathbf{g}R\in S}\sum_{u\in R^\times}\chi\big((\mathbf{a}\cdot\mathbf{g})u\big).$$

If $\mathbf{a} \in N^k \setminus \{\mathbf{0}\}$, then defining H' as above we obtain

$$\begin{aligned}
\chi_{\mathbf{a}}(\Sigma) &= |R^\times| \cdot \#\{gR; gR \subset H'\} - q \cdot \#\{gR; gR \not\subset H'\} \\
&= (q^2 - q) \cdot \frac{u(q^{k-1} - 1)}{q-1} - q \cdot q^{k-1}u \\
&= -uq.
\end{aligned}$$

If $\mathbf{a} \in R^k \setminus N^k$, then

$$\begin{aligned}
\chi_{\mathbf{a}}(\Sigma) &= |R^\times| \cdot |S \cap H| - q \cdot \#\{gR; gR \subset H \wedge gR \notin H\} \\
&= (q^2 - q)|S \cap H| - q\left(\frac{u(q^{k-1} - 1)}{q-1} - |S \cap H|\right),
\end{aligned}$$

which simplifies to the formula stated in Lemma V.4. ■

We are now ready to state the main result of this paper. For $S \subseteq \mathcal{P}$ we write $\overline{S} = \mathcal{P} \setminus S$ and define $\overline{\Sigma}$ accordingly, i.e. $\overline{\Sigma} = \{\mathbf{h} \in R^k \setminus N^k; \mathbf{h}R \notin S\}$.

Theorem V.5 *Let S be a set of points in* $\mathrm{PHG}(k-1,R)$ *meeting every point neighbour class in the same number of points. Then the following are equivalent.*

(i) S (or $\overline{S}$) is a two-intersection set;

(ii) Σ, $\overline{\Sigma}$, $N^k \setminus \{\mathbf{0}\}$, $\{\mathbf{0}\}$ determine an abelian 3-class association scheme on $(R^k, +)$.

(iii) The code $C \setminus \theta C$ has exactly two (nonzero) homogeneous weights $w_1 < w_2$.

Moreover, if S satisfies these conditions then the two sets $C_i = \{\mathbf{x} \in C \setminus \theta C; \mathrm{w}_{\mathrm{hom}}(\mathbf{x}) = w_i\}$, $i = 1, 2$, together with $\theta C \setminus \{\mathbf{0}\}$ and $\{\mathbf{0}\}$ determine an abelian 3-class association scheme on $(C, +)$, which is dual to the scheme in (ii).

Proof: Suppose first that (i) holds. Then $S \neq \emptyset$ and $\overline{S} \neq \emptyset$, so that the four sets in (ii) form a partition $\mathcal{S}$ of R^k.[7] Let $\widehat{\mathcal{S}}$ be the corresponding partition of the character group of $(R^k, +)$. Using the group isomorphism $\mathbf{a} \mapsto \chi_{\mathbf{a}}$ we may view $\widehat{\mathcal{S}}$ as a partition of R^k. Clearly $\chi_{\mathbf{a}}\big(\{\mathbf{0}\}\big) = 1$ for every $\mathbf{a} \in R^k$ and

$$\chi_{\mathbf{a}}\big(N^k \setminus \{\mathbf{0}\}\big) = \begin{cases} q^k - 1 & \text{if } \mathbf{a} \in N^k, \\ -1 & \text{if } \mathbf{a} \in R^k \setminus N^k. \end{cases} \tag{4}$$

Applying Lemma V.4 to Σ and $\overline{\Sigma}$ and using the fact that $|S \cap H|$ determines $|\overline{S} \cap H|$, we see that the members of $\widehat{\mathcal{S}}$ are unions of the four sets $\{\mathbf{0}\}$, $N^k \setminus \{\mathbf{0}\}$, $\Delta_a = \{\mathbf{a} \in R^k \setminus N^k; |S \cap H| = a\}$, and $\Delta_b = \{\mathbf{a} \in R^k \setminus N^k; |S \cap H| = b\}$.[8] Now Fact V.2 implies that $\widehat{\mathcal{S}} = \big\{\{\mathbf{0}\}, N^k\setminus\{\mathbf{0}\}, \Delta_a, \Delta_b\big\}$ and $\mathcal{S}$ determines an abelian 3-class association scheme. Thus (i) implies (ii).

[7] They are obviously distinct, and $S, \overline{S} \neq \emptyset$ implies $\Sigma, \overline{\Sigma} \neq \emptyset$.

[8] Here (a, b) denotes the type of S as a two-intersection set, and H denotes the hyperplane with equation $\mathbf{a}\cdot\mathbf{x} = 0$.

For a proof of the reverse implication we note that (4) and a straightforward argument imply that $\widehat{\mathcal{S}}$ contains $\{\mathbf{0}\}$ and $N^k \setminus \{\mathbf{0}\}$. Hence, if $|S \cap H|$ takes at least 3 distinct values then $|\widehat{\mathcal{S}}| \geq 5$ and $\mathcal{S}$ cannot yield an association scheme. Thus (ii) implies (i).

The equivalence of (i) and (iii) follows from Lemma V.3, Lemma V.4, and $\mathbf{aG} \in C \setminus \theta C \iff \mathbf{a} \in R^k \setminus N^k$.

Finally suppose S satisfies (i), (ii), (iii). Then $\mathcal{S} = \big\{\{\mathbf{0}\}, N^k \setminus \{\mathbf{0}\}, \Sigma, \overline{\Sigma}\big\}$ and $\widehat{\mathcal{S}} = \big\{\{\mathbf{0}\}, N^k \setminus \{\mathbf{0}\}, \Delta_a, \Delta_b\big\}$ determine dual abelian schemes. The module isomorphism ${}_R R^k \to C$, $\mathbf{a} \mapsto \mathbf{aG}$ takes $\widehat{\mathcal{S}}$ to $\mathcal{C} = \big\{\{\mathbf{0}\}, \theta C \setminus \{\mathbf{0}\}, C_1, C_2\big\}$. Hence the latter also determines an abelian scheme dual to that determined by $\mathcal{S}$. ■

Remark V.6 *Theorem V.5 does not exclude the case in which C is itself a homogeneous two-weight code. This happens precisely when the nonzero codewords in θC, a "simplex code", have weight w_2. Using Lemma V.4 (or Prop. V.1) it can be easily checked that this is equivalent to S being of type (a, b) with $a = u(q^{k-3} + q^{k-4} + \cdots + 1)$. In this special case we can "fuse" the corresponding two members of $\mathcal{S}$, $\widehat{\mathcal{S}}$, or $\mathcal{C}$ to obtain a pair of dual abelian 3-class association schemes (equivalently, strongly regular Cayley graphs or regular partial difference sets) on a group isomorphic to $(R^k, +)$; see [2]. The examples in [2] have $k = 2$, $a = 0$ and $k = 3$, $a = u \in \{1, q\}$.*

As an example application of Theorem V.5 we now provide a proof that the Teichmüller set $\mathfrak{T}$ (see Example II.3) in a projective Hjelmslev geometry of even dimension over a Galois ring $\mathbb{G}_{2^r}$ of characteristic 4 is a two-intersection set and compute its parameters.

Theorem V.7 *Suppose $q = 2^r$, $k \geq 3$ is odd, T is the Teichmüller subgroup of $\mathbb{G}_{q^k}^\times$, $M = \operatorname{Rad}(\mathbb{G}_{q^k}) = 2\mathbb{G}_{q^k}$, and $\mathfrak{T}$ is the set of points determined by T in $\operatorname{PHG}(k-1, \mathbb{G}_q)$.*

(i) The four sets $\Sigma = \mathbb{G}_q^\times T$, $\overline{\Sigma} = \mathbb{G}_{q^k}^\times \setminus \Sigma$, $M \setminus \{0\}$, and $\{0\}$ determine an abelian 3-class association scheme on the additive group of $\mathbb{G}_{q^k}$.

(ii) The Teichmüller set $\mathfrak{T}$ is a two-intersection set of type $\Big(\frac{q^{k-2}-1}{q-1} - q^{(k-3)/2}, \frac{q^{k-2}-1}{q-1} + q^{(k-3)/2}\Big)$.

Proof: (i) We have to show that $A = \mathbb{C}\delta_\Sigma + \mathbb{C}\delta_{\overline{\Sigma}} + \mathbb{C}\delta_{M\setminus\{0\}} + \mathbb{C}\delta_0$ is a subalgebra of the group algebra $(\mathbb{C}\mathbb{G}_{q^k}, *)$ of $(\mathbb{G}_{q^k}, +)$. Since A is generated as a $\mathbb{C}$-subspace by δ_0, δ_M, δ_Σ, and δ_R (where $R = \mathbb{G}_{q^k}$), it suffices to verify that products of these elements are again in A. This is clear[9] for all products except $\delta_M * \delta_\Sigma$ and $\delta_\Sigma * \delta_\Sigma$. For the former it is easy to verify (using $\Sigma = T(1+N)$) that $\delta_M * \delta_\Sigma = q\delta_{R\setminus M} \in A$. For the latter we invoke Lemma VI.1 in the appendix, which implies

$$\delta_\Sigma * \delta_\Sigma = (q^2 - 2q)\delta_\Sigma + q^2\delta_{\overline{\Sigma}} + (q^2 - q)\delta_{M\setminus\{0\}} + q(q^k - 1)\delta_0. \tag{5}$$

Hence $\delta_\Sigma * \delta_\Sigma \in A$ and the proof of (i) is complete.

(ii) By (i) and Theorem V.5, the set $\mathfrak{T}$ is a two-intersection set.

In order to determine the type (a, b) of $\mathfrak{T}$, we apply Lemma V.4. The characters of $(\mathbb{G}_{q^k}, +)$ which correspond to $\chi_{\mathbf{a}}$, $\mathbf{a} \in R^k \setminus N^k$ are those which are nontrivial on M. If ψ is such a character, then $\psi(\Sigma) + \psi(\overline{\Sigma}) = \psi(R \setminus M) = 0$, $\psi\big(M \setminus \{0\}\big) = -1$. Applying ψ to (5) we find

$$\begin{aligned}\psi(\Sigma)^2 &= (q^2 - q)\psi(\Sigma) - \psi(\Sigma) - (q^2 - q) + q(q^k - 1)\\ &= -2q \cdot \psi(\Sigma) + q^{k+1} - q^2,\end{aligned}$$

and hence $\psi(\Sigma) = -q \pm q^{(k+1)/2}$. So Lemma V.4 gives

$$\begin{aligned}|\mathfrak{T} \cap H| &= q^{-2}\left(-q + \frac{q^k - q}{q - 1} \pm q^{(k+1)/2}\right)\\ &= \frac{q^{k-2} - 1}{q - 1} \pm q^{(k-3)/2}\end{aligned}$$

as asserted. ■

Theorem V.7 does not hold for the projective Hjelmslev geometries of odd dimension ≥ 3 over $\mathbb{G}_{2^r}$; cf. Remark VI.2 in the appendix.[10]

VI. Appendix

In this section we provide a combinatorial lemma about odd-degree extensions $\mathbb{G}_{q^k}/\mathbb{G}_q$ of Galois rings of characteristic 4, i.e. with $q = 2^r$ and k odd. This lemma generalizes [1, Th. 1] and is needed for Example II.3 (see Theorem V.7).

Lemma VI.1 *Let $\mathbb{G}_{q^k}/\mathbb{G}_q$, $q = 2^r$, be an extension of Galois rings of characteristic 4 of odd degree $k \geq 3$, let T be the Teichmüller subgroup of $\mathbb{G}_{q^k}$, $\Sigma = T\mathbb{G}_q^\times$, and $\overline{\Sigma} = \mathbb{G}_{q^k}^\times \setminus \Sigma$. For $\gamma \in \mathbb{G}_{q^k}$ set $\mathrm{n}_\gamma = \#\big\{(x, y) \in \Sigma \times \Sigma; x + y = \gamma\big\}$. Then*

$$\mathrm{n}_\gamma = \begin{cases} (q^k - 1)q & \textit{if } \gamma = 0,\\ q^2 - q & \textit{if } \gamma \in 2\mathbb{G}_{q^k} \setminus \{0\},\\ q^2 - 2q & \textit{if } \gamma \in \Sigma,\\ q^2 & \textit{if } \gamma \in \overline{\Sigma}.\end{cases}$$

Proof: We represent $\mathbb{G}_q$, $q = 2^r$, as the ring $\mathrm{W}_2(\mathbb{F}_q)$ of Witt vectors of length 2 over $\mathbb{F}_q$, which has underlying set $\mathbb{F}_q^2$ and operations

$$\begin{aligned}(a_0, a_1) + (b_0, b_1) &= (a_0 + b_0, a_1 + b_1 + a_0 b_0),\\ (a_0, a_1) \cdot (b_0, b_1) &= (a_0 b_0, a_0^2 b_1 + b_0^2 a_1);\end{aligned}$$

cf. for example [14]. The extension ring $\mathbb{G}_{q^k}$ is represented in the same way as $\mathrm{W}_2(\mathbb{F}_{q^k})$. The Teichmüller subgroup of $\mathrm{W}_2(\mathbb{F}_{q^k})^\times$ is $T = \big\{(\alpha, 0); \alpha \in \mathbb{F}_{q^k}^\times\big\}$. The group $\Sigma \leq \mathrm{W}_2(\mathbb{F}_{q^k})^\times$ is generated by T and $\mathrm{W}_2(\mathbb{F}_q)^\times$ or, alternatively, by T and $1 + 2\mathrm{W}_2(\mathbb{F}_q)$; thus

$$\begin{aligned}\Sigma &= \big\{(\alpha, 0)(1, a); \alpha \in \mathbb{F}_{q^k}^\times, a \in \mathbb{F}_q\big\}\\ &= \big\{(\alpha, \alpha^2 a); \alpha \in \mathbb{F}_{q^k}^\times, a \in \mathbb{F}_q\big\}\\ &= \big\{(\gamma_0, \gamma_1) \in \mathrm{W}_2(\mathbb{F}_{q^k})^\times; \gamma_1/\gamma_0^2 \in \mathbb{F}_q\big\}.\end{aligned}$$

[9] Note that δ_0 is the identity of $(\mathbb{C}\mathbb{G}_{q^k}, *)$, δ_M is an idempotent up to scaling, and δ_R generates a 1-dimensional ideal of $(\mathbb{C}\mathbb{G}_{q^k}, *)$.

[10] For the projective Hjelmslev line $\operatorname{PHG}(1, \mathbb{G}_q)$ it holds trivially.

The integer n_γ, $\gamma = (\gamma_0, \gamma_1) \in \mathrm{W}_2(\mathbb{F}_{q^k})$, is the number of solutions of

$$\begin{aligned} \alpha + \beta &= \gamma_0 \\ \alpha^2 a + \beta^2 b + \alpha\beta &= \gamma_1 \end{aligned} \tag{6}$$

in $\alpha, \beta \in \mathbb{F}_{q^k}^\times$, $a, b \in \mathbb{F}_q$. For $\gamma_0 = 0$ the system (6) reduces to $\alpha = \beta \wedge \alpha^2(a+b+1) = \gamma_1$ which has $(q^k - 1) \cdot q$ solutions if $\gamma_1 = 0$, respectively, $1 \cdot (q^2 - q)$ solutions if $\gamma_1 \neq 0$.

Now assume $\gamma_0 \neq 0$. Substituting $\beta = \gamma_0 + \alpha$ into the second equation of (6) gives $\alpha^2 a + (\gamma_0 + \alpha)^2 b + \alpha(\gamma_0 + \alpha) = \alpha^2(a + b + 1) + \alpha\gamma_0 + \gamma_0^2 b = \gamma_1$ and, writing $\alpha' = \alpha/\gamma_0$, $u = a + b + 1$, further

$$u\alpha'^2 + \alpha' = \gamma_1/\gamma_0^2 + b. \tag{7}$$

From $\alpha, \beta \in \mathbb{F}_{q^k}^\times$ we have the condition $\alpha' \notin \{0, 1\} = \mathbb{F}_2$, but otherwise α' can be arbitrary in $\mathbb{F}_{q^k}$. Thus n_γ is equal to the number of solutions $(\alpha', u, b) \in (\mathbb{F}_{q^k} \setminus \mathbb{F}_2) \times \mathbb{F}_q \times \mathbb{F}_q$ of (7). Now we consider two subcases.

Case 1: $u = 0$. Here (7) has $q - 2$ solutions if $\gamma \in \Sigma$ (for then $\gamma_1/\gamma_0^2 \in \mathbb{F}_q$ and the right hand side of (7) can be equal to 0, 1) and q solutions if $\gamma \in \overline{\Sigma}$.

Case 2: $u \neq 0$. Here we multiply (7) by u to obtain $(u\alpha')^2 + u\alpha' = u(\gamma_1/\gamma_0^2 + b)$ and use the fact that the additive homomorphism $\mathbb{F}_{q^k} \to \mathbb{F}_{q^k}$, $x \mapsto x^2 + x$ is two-to-one with image $V_0 = \{y \in \mathbb{F}_{q^k}; \mathrm{Tr}(y) = 0\}$ and kernel $\mathbb{F}_2$, where Tr denotes the trace from $\mathbb{F}_{q^k}$ to $\mathbb{F}_2$. Moreover, since k is odd, we have $|V_0 \cap (c + \mathbb{F}_q)| = q/2$ for every $c \in \mathbb{F}_{q^k}$.

If $\gamma \in \Sigma$ then $u(\gamma_1/\gamma_0^2 + b)$, $(u, b) \in \mathbb{F}_q^\times \times \mathbb{F}_q$ represents each element of $\mathbb{F}_q$ (and hence of $V_0 \cap \mathbb{F}_q$) exactly $q-1$ times, so that there are $2 \cdot \frac{q}{2} \cdot (q-1) - 2(q-1) = (q-1)(q-2)$ solutions. (The term $-2(q-1)$ accounts for the fact that solutions with $\alpha' \in \mathbb{F}_2$ are not counted.)

If $\gamma \in \overline{\Sigma}$, then $u(\gamma_1/\gamma_0^2 + b)$, $(u, b) \in \mathbb{F}_q^\times \times \mathbb{F}_q$ represents the elements in $q - 1$ (disjoint) additive cosets of $\mathbb{F}_q$ in $\mathbb{F}_{q^k}$ exactly once. Since $|V_0 \cap (c + \mathbb{F}_q)| = q/2$ for each such coset and $\mathbb{F}_q$ is not among these cosets (so all solutions are counted), there are $2 \cdot \frac{q}{2} \cdot (q-1) = (q-1)q$ solutions in this case.

So alltogether (7) has $q - 2 + (q-1)(q-2) = q^2 - 2q$ solutions if $\gamma \in \Sigma$, and $q + (q-1)q = q^2$ solutions if $\gamma \in \overline{\Sigma}$. This completes the proof of the lemma. ■

Remark VI.2 *For extensions of even degree $k \geq 4$ of Galois rings of characteristic 4 the map $\gamma \mapsto \mathrm{n}_\gamma$ is not constant on $\overline{\Sigma}$. In this case $\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\gamma_1/\gamma_0^2)$, $\gamma \in \overline{\Sigma}$ (i.e. $\gamma_1/\gamma_0^2 \in \mathbb{F}_{q^k} \setminus \mathbb{F}_q$) takes both zero and nonzero values, and the number of solutions $(u, b) \in \mathbb{F}_q^\times \times \mathbb{F}_q$ of $\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_2}\big(u(\gamma_1/\gamma_0^2 + b)\big) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\big(u \cdot \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\gamma_1/\gamma_0^2)\big) = 0$ depends on whether $\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\gamma_1/\gamma_0^2) = 0$ or $\neq 0$.*

References

[1] A. Bonnecaze and I. M. Duursma. Translates of linear codes over $\mathbb{Z}_4$. *IEEE Transactions on Information Theory*, 43(4):1218–1230, 1997.

[2] E. Byrne, M. Greferath, and T. Honold. Ring geometries, two-weight codes, and strongly regular graphs. *Designs, Codes and Cryptography*, 48:1–16, July 2008.

[3] R. Calderbank and W. M. Kantor. The geometry of two-weight codes. *Bulletin of the London Mathematical Society*, 18:97–122, 1986.

[4] P. Camion. Codes and association schemes: Basic properties of association schemes relevant to coding. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, volume II, chapter 18, pages 1441–1566. Elsevier Science Publishers, 1998.

[5] I. Constantinescu and W. Heise. A metric for codes over residue class rings. *Problems of Information Transmission*, 33(3):208–213, 1997.

[6] P. Delsarte. Weights of linear codes and strongly regular normed spaces. *Discrete Mathematics*, 3:47–64, 1972.

[7] C. D. Godsil. *Algebraic Combinatorics*. Chapman and Hall, 1993.

[8] M. Greferath and S. E. Schmidt. Finite-ring combinatorics and MacWilliams' equivalence theorem. *Journal of Combinatorial Theory, Series A*, 92:17–28, 2000.

[9] T. Honold. Characterization of finite Frobenius rings. *Archiv der Mathematik*, 76(6):406–415, 2001.

[10] T. Honold, M. Kiermaier, A. Kohnert, I. Landjev, and J. Zwanzger. New results on arcs in projective Hjelmslev planes over small chain rings. In preparation.

[11] T. Honold, M. Kiermaier, and I. Landjev. New arcs of maximal size in projective Hjelmslev planes of order nine. *Comptes Rendus de l'Académie Bulgare des Sciences*, 63(2):171–180, Feb. 2010.

[12] T. Honold and I. Landjev. Linear codes over finite chain rings. *Electronic Journal of Combinatorics*, 7:Research Paper 11, 22 pp. (electronic), 2000.

[13] T. Honold and I. Landjev. On arcs in projective Hjelmslev planes. *Discrete Mathematics*, 231(1-3):265–278, 2001. 17th British Combinatorial Conference, University of Kent, Canterbury, 1999.

[14] T. Honold and I. Landjev. On maximal arcs in projective Hjelmslev planes over chain rings of even characteristic. *Finite Fields and their Applications*, 11(2):292–304, 2005.

[15] T. Honold and I. Landjev. The dual construction for arcs in projective Hjelmslev planes. Submitted for publication, Sept. 2009.

[16] T. Honold and I. Landjev. Linear codes over finite chain rings and projective Hjelmslev geometries. In Sol [28], pages 60–123.

[17] T. Honold and A. A. Nechaev. Weighted modules and representations of codes. *Problems of Information Transmission*, 35(3):205–223, 1999.

[18] M. Kiermaier and A. Kohnert. New arcs in projective Hjelmslev planes over Galois rings. In *Optimal Codes and Related Topics*, pages 112–119, White Lagoon, Bulgaria, 2007.

[19] M. Kiermaier and J. Zwanzger. A new series of $\mathbb{Z}_4$-linear codes of high minimum Lee distance derived from the Kerdock codes. Preprint, May 2010.

[20] A. Kohnert. Sets of type (d_1, d_2) in projective Hjelmslev planes over Galois rings. In M. Klin, G. A. Jones, A. Jurišić, M. Muzychuk, and I. Ponomarenko, editors, *Algorithmic Algebraic Combinatorics and Gröbner Bases*, pages 269–278. Springer-Verlag, 2009.

[21] A. S. Kuzmin and A. A. Nechaev. Complete weight enumerators of generalized Kerdock code and related linear codes over galois ring. *Discrete Applied Mathematics*, 111:117–137, 2001.

[22] I. Landjev. On blocking sets in projective Hjelmslev planes. *Advances in Mathematics of Communications*, 1(1):65–81, 2007.

[23] I. Landjev and S. Boev. A family of two-weight ring codes and strongly regular graphs. *Comptes Rendus de l'Académie Bulgare des Sciences*, 62(3):297–302, mar 2009.

[24] I. Landjev and T. Honold. Arcs in projective Hjelmslev planes. *Discrete Mathematics and Applications*, 11(1):53–70, 2001. Originally published in Diskretnaya Matematika (2001) 13, No. 1, 90–109 (in Russian).

[25] I. Landjev and T. Honold. Codes over rings and ring geometries. To appear in *Current research topics in Galois geometry*, Leo Storme et al. eds., Nova Science Publishers, Nov. 2009.

[26] S. L. Ma. A survey of partial difference sets. *Designs, Codes and Cryptography*, 4:221–261, 1994.

[27] A. A. Nechaev and A. S. Kuzmin. Trace function on a Galois ring in coding theory. In T. Mora and H. F. Mattson, Jr., editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC) 12*, number 1255 in Lecture Notes in Computer Science, pages 277–290. Springer-Verlag, 1997.

[28] P. Sol, editor. *Codes Over Rings. Proceedings of the CIMPA Summer School, Ankara, Turkey, 18–29 August, 2008*, volume 6 of *Series on Coding Theory and Cryptology*. World Scientific, July 2009.