Sixth International Workshop on Optimal Codes and Related Topics
June 16-22, 2009, Varna, Bulgaria *pp. 106-113*

New complete 2-arcs in the uniform projective Hjelmslev planes over chain rings of order 25

Michael Kiermaier michael.kiermaier@uni-bayreuth.de
Matthias Koch matthias.koch@uni-bayreuth.de
Mathematical Department, University of Bayreuth, D-95440 Bayreuth, GERMANY

Abstract. In this paper a 2-arc of size 21 in the projective Hjelmslev plane $\mathrm{PHG}(2, \mathbb{Z}_{25})$ and a 2-arc of size 22 in $\mathrm{PHG}(2, \mathbb{F}_5[X]/(X^2))$ are given. Both arcs are bigger than the 2-arcs previously known in the respective plane. Furthermore, we will give some information on the geometrical structure of the arcs.

1 Introduction

It is well known that a Desarguian projective plane of order q admits a 2-arc of size $q+2$ if and only if q is even. These 2-arcs are called *hyperovals*. The biggest 2-arcs in the Desarguian projective planes of odd order q have size $q+1$ and are called *ovals*.

For an uniform projective Hjelmslev plane over a chain ring R of size q^2, the situation is somewhat similar: In $\mathrm{PHG}(R, 2)$ there exists an hyperoval – that is a 2-arc of size q^2+q+1 – if and only if G is a Galois ring of size q^2 with q even, see [6, 5]

In the remaining uniform projective Hjelmslev planes, the situation is less clear. It is known [5] that for even q and R not a Galois ring, a 2-arc has at most size q^2+q, and for odd q a 2-arc has at most size q^2. For $\#R \leq 16$ the exact values were determined either by theory or computationally [5, 7, 4], leaving $\#R = 25$ as the smallest case where the exact sizes $n_2(R)$ of a maximum 2-arc in $\mathrm{PHG}(2, R)$ are not known. Up to isomorphism there are two finite chain rings of size 25 of composition length 2, these are $\mathbb{Z}_{25}$ and $\mathbb{F}_5[X]/(X^2)$. When we started our search, the biggest known 2-arcs had size 20 [5] or 18 [1], respectively.

In the following two sections, we give a brief introduction to finite chain rings and Hjelmslev geometries. For details, see for example [5] and the references cited there.

2 Finite chain rings

A ring[1] R is called *chain ring* if the lattice of the left-ideals is a chain. A chain ring is necessarily local, so there is a unique maximum ideal $N = \mathrm{rad}(R)$ and

[1] Rings are assumed to contain an unity element and to be associative, but not necessarily commutative.

the quotient ring R/N is a division ring. In the following we will only consider finite chain rings, where we get $R/N \cong \mathbb{F}_q$ with a prime power $q = p^r$, p prime. We will need the projection $\phi : R \to \mathbb{F}_q$, $a \mapsto a \mod N$, which is a surjective ring homomorphism.

The number of ideals of R reduced by 1 is the composition length of R, considered as a left module ${}_R R$. This number will be denoted by m.

An important subclass of the finite chain rings are the *Galois rings*. Their definition is a slight generalization of the construction of finite fields via irreducible polynomials:

Let p be prime, r and m positive integers, $q = p^r$ and $f \in \mathbb{Z}_{p^m}[X]$ be a monic polynomial of degree r such that the image of f modulo p is irreducible in $\mathbb{F}_p[X]$. Then the *Galois ring* of order q^m and characteristic p^m is defined as

$$\mathrm{GR}(q^m, p^m) = \mathbb{Z}_{p^m}[X]/(f)$$

Up to isomorphism, the definition is independent of the exact choice of f. The symbols p, q, r and m are consistent with the earlier definitions: It holds $\mathrm{GR}(q^m, p^m)/\operatorname{rad}(\mathrm{GR}(q^m, p^m)) \cong \mathbb{F}_q$ and the composition length of $\mathrm{GR}(q^m, p^m)$ is m. Furthermore, the Galois rings contain the finite fields and the integer residues modulo a prime power: $\mathrm{GR}(p^m, p^m) \cong \mathbb{Z}_{p^m}$ and $\mathrm{GR}(p^r, p) \cong \mathbb{F}_{p^r}$.

While the fields are exactly the chain rings of composition length 1, in this article we are interested in finite chain rings of composition length 2. The isomorphism types of these rings are known:

Theorem 2.1 (see [2])**.** *Let R be a finite chain ring of composition length 2, $N = \operatorname{rad}(R)$ and $R/N \cong \mathbb{F}_q$. Then $\#R = q^2$, and exactly one of the following statements is true:*

(a) R is isomorphic to the Galois ring $\mathrm{GR}(q^2, p^2)$ of order q^2 and characteristic p^2.

(b) There is an unique automorphism σ of $\mathbb{F}_q$ such that R is isomorphic to the σ-dual numbers $\mathbb{F}_q[X, \sigma]/(X^2)$.[2]

We see that there are $r+1$ isomorphism classes of chain rings of composition length 2 and order q^2. Among these rings 2 are commutative, namely $\mathrm{GR}(q^2, p^2)$ and $\mathbb{S}_q := \mathbb{F}_q[X]/(X^2)$. The Galois ring is the unique one with characteristic p^2, all the others have characteristic p. The smallest such chain rings are:

q	R		
2	$\mathbb{Z}_4$	$\mathbb{S}_2 = \mathbb{F}_2[X]/(X^2)$	
3	$\mathbb{Z}_9$	$\mathbb{S}_3 = \mathbb{F}_3[X]/(X^2)$	
4	$\mathbb{G}_4 := \mathrm{GR}(16, 4)$	$\mathbb{S}_4 = \mathbb{F}_4[X]/(X^2)$	$\mathbb{T}_4 := \mathbb{F}_4[X, a \mapsto a^2]/(X^2)$
5	$\mathbb{Z}_{25}$	$\mathbb{S}_5 = \mathbb{F}_5[X]/(X^2)$	

[2] $\mathbb{F}_q[X, \sigma]$ is a *skew polynomial ring* over $\mathbb{F}_q$. Its addition is defined as in the usual polynomial ring, and the multiplication is the distributive extension of the rule $X\lambda = \sigma(\lambda)X$ for each scalar $\lambda \in \mathbb{F}_q$.

The only non-commutative ring in this list is $\mathbb{T}_4$.

3 Arcs in projective Hjelmslev planes

The *projective Hjelmslev geometry* $\mathrm{PHG}(k,R)$ of dimension k over a finite chain ring R is defined as follows: The point set $\mathcal{P}(\mathrm{PHG}(k,R))$ [line set $\mathcal{L}(\mathrm{PHG}(k,R))$] is the set of the free rank 1 [rank k] right submodules of the module R^{k+1}, and the incidence is given by set inclusion.

We have $|\mathcal{P}(\mathrm{PHG}(k,R))| = |\mathcal{L}(\mathrm{PHG}(k,R))| = \frac{q^{k+1}-1}{q-1}q^{k(m-1)}$. For $m=1$, R is a finite field and $\mathrm{PHG}(k,R)$ is the classical projective geometry $\mathrm{PG}(R,k)$ of dimension k over R. For $m>1$ however, two different lines in $\mathrm{PHG}(k,R)$ may meet in more than one point.

The map ϕ, extended to R^{k+1}, is a collineation $\mathrm{PHG}(k,R) \to \mathrm{PG}(k,\mathbb{F}_q)$. Let $P,Q \in \mathcal{P}(\mathrm{PHG}(k,R))$. There is more than one line passing through P and Q if and only if $\phi(P) = \phi(Q)$. The preimages $\phi^{-1}(P)$ [$\phi^{-1}(L)$] with $P \in \mathcal{P}(\mathrm{PG}(k,\mathbb{F}_q))$ [$L \in \mathcal{L}(\mathrm{PG}(k,\mathbb{F}_q))$] are called *point* [*line*] *neighbor classes* of $\mathrm{PHG}(k,R)$. The restriction of a projective Hjelmslev geometry to a single point neighbor class is isomorphic to the affine geometry $\mathrm{PG}(k,\mathbb{F}_q)$. The group of collineations of $\mathrm{PGL}(k,R)$ is exactly the semilinear projective group $\mathrm{P\Gamma L}(k+1,R)$ [9].

In the following, we restrict us to the projective Hjelmslev *planes* $\mathrm{PHG}(2,R)$. If R has composition length 2, such a plane is called *uniform*. For $n \in \mathbb{N}$, a set of points $\mathfrak{k} \subseteq \mathfrak{P}(\mathrm{PHG}(2,R))$ of size n is called *projective* (n,u)*-arc*, if some u elements of $\mathfrak{k}$ are collinear, but no $u+1$ elements of $\mathfrak{k}$ are collinear. If we allow $\mathfrak{k}$ to be a *multi*set of points in this definition[3], $\mathfrak{k}$ is called (n,u)*-multiarc*. We denote by $n_u(R)$ the maximum size of an u-multiarc in the projective Hjelsmelv plane $\mathrm{PHG}(2,R)$.

In the case $u=2$ the discrimination of projective arcs and multiarcs is not important, since the only proper 2-multiarc is a single point of multiplicity 2. So we will simply use the expression 2-arc.

For a 2-arc $\mathfrak{k}$ in an uniform Hjelmslev plane over a chain ring with odd parameter q, it is known that the complement of the image $\phi(\mathfrak{k})$ is a blocking set in $\mathrm{PG}(2,\mathbb{F}_q)$.

The following table shows the known values of $n_2(R)$ for the finite chain rings R with $m=2$ and $\#R \le 25$. The values for the rings R with $\#R \le 9$, as well as the lower bound for $\mathbb{S}_4$ and the upper bounds for $\mathbb{G}_4$, $\mathbb{Z}_{25}$ and $\mathbb{S}_5$ were given in [5]. The lower bound for $\mathbb{G}_4$ was given in [3], and the upper bound for $\mathbb{S}_4$ as well as lower and upper bound for $\mathbb{T}_4$ can be found in [4]. For the chain rings R with $q=5$ the table shows a range, since the exact value of $n_2(R)$ is

[3] Of course we have to respect multiplicities for counting the number of collinear points.

not known. The lower bounds of these ranges are improved by our search.

q	2		3		4			5	
R	$\mathbb{Z}_4$	$\mathbb{S}_2$	$\mathbb{Z}_9$	$\mathbb{S}_3$	$\mathbb{G}_4$	$\mathbb{S}_4$	$\mathbb{T}_4$	$\mathbb{Z}_{25}$	$\mathbb{S}_5$
$n_2(R)$	7	6	9	9	21	18	18	$\mathbf{21}-25$	$\mathbf{22}-25$

4 The new arcs

In this section we give the new arcs and some analysis of their geometrical structure. The Hjelmslev planes $\mathrm{PHG}(2,\mathbb{Z}_{25})$ and $\mathrm{PHG}(2,\mathbb{S}_5)$ both consist of 775 points and lines, and of 31 point and line neighbor classes. A single neighbor class contains 25 points respectively lines.

4.1 A $(21,2)$-arc in $\mathrm{PHG}(2,\mathbb{Z}_{25})$

A $(21,2)$-arc $\mathfrak{k}_{\mathbb{Z}_{25}}$ in $\mathrm{PHG}(2,\mathbb{Z}_{25})$ is given by the points

$$\begin{array}{ccc}
(1:1:4) & (1:19:19) & (1:4:1)\\
(1:1:22) & (1:8:8) & (1:22:1)\\
(1:3:12) & (1:23:19) & (1:4:17)\\
(1:7:8) & (1:22:4) & (1:19:18)\\
(1:7:22) & (1:8:6) & (1:21:18)\\
(5:1:2) & (1:15:13) & (1:2:5)\\
(5:1:23) & (1:10:12) & (1:23:5).
\end{array}$$

Its automorphism group has order 3 and is generated by a rotation of the coordinate axes: $\mathrm{Aut}(\mathfrak{k}_{\mathbb{Z}_{25}}) = \langle\rho\rangle$ where

$$\rho = \langle v\rangle \mapsto \left\langle \begin{pmatrix} 0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 0 \end{pmatrix} v \right\rangle$$

The automorphism group partitions $\mathfrak{k}_{\mathbb{Z}_{25}}$ into 7 orbits, each of size 3. In the list of points above each row consists of a single orbit.

The 21 points are contained in 21 different point neighbor classes. The complement of $\phi(\mathfrak{k}_{\mathbb{Z}_{25}})$ in $\mathrm{PG}(2,\mathbb{F}_5)$ has size 10 and consists of the projective triangle

$$\bigcup_{a\in\mathbb{F}_5} \{(0:1:-a^2),(1:-a^2:0),(-a^2:0:1)\}$$

together with its center point $(1:1:1)$.

4.2 A $(22, 2)$-arc in $\mathbb{S}_5$

A $(22, 2)$-arc $\mathfrak{k}_{\mathbb{S}_5}$ in $\mathrm{PHG}(2, \mathbb{S}_5)$ is given by the points

$$\begin{array}{ccc}
(1 : X+1 : 4X) & (4X : 1 : X+1) & (1 : 4X : 4X+1) \\
(1 : 4X+1 : 4X) & (4X : 1 : 4X+1) & (1 : 4X : X+1) \\
(1 : X+1 : 3X+4) & (1 : 2X+4 : X+4) & (1 : 4X+4 : 4X+1) \\
(1 : 4X+1 : 4X+4) & (1 : X+4 : 2X+4) & (1 : 3X+4 : X+1) \\
\hline
(1 : 3X+2 : 3X+2) & (1 : 3X+3 : 1) & (1 : 1 : 3X+3) \\
(1 : 2X+3 : 4X+2) & (1 : 4X+3 : 3X+4) & (1 : 2X+4 : 2X+2) \\
(1 : 4X+2 : 2X+3) & (1 : 2X+2 : 2X+4) & (1 : 3X+4 : 4X+3) \\
 & (1 : 1 : 1). &
\end{array}$$

Again, the rotation ρ of the coordinate axes is an automorphism of $\mathfrak{k}_{\mathbb{S}_5}$, and each row in the point list consists of one orbit under the group action of $\langle\rho\rangle$, so there are 7 orbits of size 3 and the fixed point $(1 : 1 : 1)$. But in this case the full automorphism group $\mathrm{Aut}(\mathfrak{k}_{\mathbb{S}_5})$ is bigger than $\langle\rho\rangle$, another automorphism of $\mathfrak{k}_{\mathbb{S}_5}$ is given by

$$\tau = \langle v\rangle \mapsto \left\langle \begin{pmatrix} 1 & X & -X \\ X & 1 & -X \\ 2X+2 & 2X+2 & -X-1 \end{pmatrix} v \right\rangle$$

τ has order 2, $\rho\tau$ has order 5 and together, ρ and τ generate $\mathrm{Aut}(\mathfrak{k}_{\mathbb{S}_5})$: $\mathrm{Aut}(\mathfrak{k}_{\mathbb{S}_5}) = \langle\rho, \tau\rangle \cong \mathrm{PSL}(2, \mathbb{F}_5) \cong A_5$, where A_5 denotes the alternating group on a set of size 5.

While the ring $\mathbb{Z}_{25}$ has a trivial automorphism group, $\mathrm{Aut}(\mathbb{S}_5)$ is cyclic of order 4 and generated by the linear extension of $X \mapsto 2X$. So $\mathrm{PGL}(3, \mathbb{S}_5) \lneq \mathrm{P\Gamma L}(3, \mathbb{S}_5)$. But $\mathrm{Aut}(\mathfrak{k}_{\mathbb{S}_5}) < \mathrm{PGL}(3, \mathbb{S}_5)$, so all the automorphisms of $\mathfrak{k}_{\mathbb{S}_5}$ are purely linear. Under the action of $\mathrm{Aut}(\mathfrak{k}_{\mathbb{S}_5})$, $\mathfrak{k}_{\mathbb{S}_5}$ splits into 2 orbits O_1 and O_2. O_1 has size 12 and contains the points above the horizontal line in the list, O_2 has size 10 and contains the points below the horizontal line.

The 12 points in O_1 are contained in 6 point neighbor classes, each class containing 2 points of O_1. The image of these 6 point neighbor classes under ϕ is the oval

$$O = \{(0 : 1 : 1), (1 : 0 : 1), (1 : 1 : 0), (-1 : 1 : 1), (1 : -1 : 1) : (1 : 1 : -1)\}$$

in $\mathrm{PG}(2, \mathbb{F}_5)$. Each pair of points within the same point neighbor class is aligned in the tangent direction of the oval O.

The 10 points in O_2 are all in separate point neighbor classes, and their ϕ-images are exactly the internal points of the oval O. The 15 point neighbor classes corresponding to the external points of O are empty.

5 Computation

The arcs were found by a fast backtracking search.

One problem are the huge automorphism groups of the projective Hjelmslev planes[4], which cause "the same" point constellation to appear in billions of isomorphic copies during a naive depth-first search. On the other hand, a complete elimination of isomorphic copies would be too expensive, so the compromise was to filter out isomorphic copies in the first 7 levels of the search, and to do an additional isomorphism test for the leaf nodes of the search. These isomorphism tests and the determination of the automorphism groups were done implementing the *Leiterspiel* [13], see also [11].

Another bottleneck is the test in the innermost loop of the algorithm if a certain point can be added to the current point set without violating the 2-arc property. Here we exploit the fact that $\mathfrak{k} \subseteq \mathcal{P}(\mathrm{PHG}(2,R))$ is a 2-arc if and only if all the 3-element subsets of $\mathfrak{k}$ are a 2-arc: For any set $S \subset \mathcal{P}(\mathrm{PHG}(2,R))$ and any four points $P_1, P_2, P_3, P_4 \in \mathcal{P}(\mathrm{PHG}(2,R)) \setminus S$ it holds that $\mathfrak{a} := S \cup \{P_1, P_2, P_3, P_4\}$ is a 2-arc if and only if $\mathfrak{a}_1 := S \cup \{P_1, P_2, P_3\}$, $\mathfrak{a}_2 := S \cup \{P_1, P_2, P_4\}$, $\mathfrak{a}_3 := S \cup \{P_1, P_3, P_4\}$ and $\mathfrak{a}_4 := S \cup \{P_2, P_3, P_4\}$ are 2-arcs. So in each node of the depth-first search we do a local breadth-first search for 3 levels. The overhead of this additional search is compensated by the fact that the search depth of the outer depth-first search is reduced by 3. Now when the backtrack algorithm goes forward from the search node S to the search node $S \cup \{P_1\}$, the breadth-first search for the node $S \cup \{P_1\}$ can be performed easily only by doing look-ups in the breadth-first data of the node S. This process can be seen as *merging* the 4 arcs $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{a}_3$ and $\mathfrak{a}_4$ into the bigger arc $\mathfrak{a}$. The merging technique is a general idea to avoid repeated tests within a backtracking search. In [10] it was used on pairs of integral point sets, and then in [8] on triples of polyominoes.

6 Conclusion and future research

Up to isomorphism, the given 2-arcs were the only ones of size 21 respectively 22 that showed up in our search. Since we did not investigate the complete search space, there might still exist other isomorphism types or even bigger 2-arcs. But the current situation is quite remarkable: When we started our search, in the tables of the best known u-arcs in uniform projective Hjelmslev planes over finite chain rings all the u-arcs in planes over Galois rings were at least as large as the u-arcs in the Hjelmslev planes over the other rings R with the same parameter q, suggesting this being true in general. The Hjelmslev plane $\mathrm{PHG}(2,\mathbb{S}_5)$ admitting a 2-arc of size 22 on the one hand and the Hjelmslev plane $\mathrm{PHG}(2,\mathbb{Z}_{25})$ with its best known arc of size 21 on the other hand could be a counterexample to this conjecture.

Of course, the definitive knowledge of the biggest 2-arcs in $\mathrm{PHG}(2,\mathbb{Z}_{25})$ and $\mathrm{PHG}(2,\mathbb{S}_5)$ would be great. We think that it might be computationally feasible to exhaustively search the complete search space by further exploiting

[4] $\#\operatorname{Aut}(\mathrm{PHG}(2,\mathbb{Z}_{25})) = 145312500000$ and $\#\operatorname{Aut}(\mathrm{PHG}(2,\mathbb{S}_5)) = 581250000000$

the homomorphism ϕ of group actions

$$(\mathrm{P\Gamma L}(3,R),\mathrm{PHG}(2,R)) \to (\mathrm{PGL}(3,\mathbb{F}_5),\mathrm{PG}(2,\mathbb{F}_5))$$

via the homomorphism principle [12]: In a first step, all the $\mathrm{PGL}(3,\mathbb{F}_5)$-representatives for the images in $\mathrm{PG}(2,\mathbb{F}_5)$ are generated. At this point we can make use of some restrictions, for example that the empty point neighbor classes form a blocking set in $\mathrm{PG}(2,\mathbb{F}_5)$. Then for each such image $\bar{\mathfrak{k}}$, we need to exhaustively search all the 2-arcs among the preimages in $\phi^{-1}(\bar{\mathfrak{k}})$ up to $\mathrm{P\Gamma L}(3,R)$-isomorphism. In fact it is enough to consider the preimage of the $\mathrm{PGL}(3,\mathbb{F}_5)$-stablilizer of $\bar{\mathfrak{k}}$ as the operating group. Usually this group is much smaller than the full group of all collineations, a fact that benefits canonization and isomorphism tests.

Furthermore, the question arises if a generalization of the arc $\mathfrak{k}_{\mathbb{Z}_{25}}$ or $\mathfrak{k}_{\mathbb{S}_5}$ to uniform Hjelmslev planes over chain rings of higher order is possible. We hope that our analysis of the structure could be a first step into this direction.

References

[1] S. Boumova, I. Landjev, Some new arcs in projective Hjelmslev planes over small chain rings, *Proc. Ninth Intern. Workshop ACCT*, 2004, 56-61.

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

[3] L. Hemme, Th. Honold, I. Landjev, Arcs in projective Hjelmslev spaces obtained from Teichmüller sets, *Proc. Seventh Intern. Workshop ACCT*, 2000, 177-182.

[4] Th. Honold, M. Kiermaier, Classification of maximal arcs in small projective Hjelmslev geometries, *Proc. Tenth Intern. Workshop ACCT*, 2006, 112-117.

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

[6] Th. Honold, I. Landjev, On maximal arcs in projective Hjelmslev planes over chain rings of even characteristic, *Fin. Fields Appl.* 11 2005, 292-304.

[7] M. Kiermaier, Arcs und Codes über endlichen Kettenringen, Master's thesis, Techn. Univ. München, 2006.

[8] M. Koch, Anwendung von Konstruktionsalgorithmen in der diskreten Geometrie, Master's thesis, Univ. Bayreuth, 2006.

[9] A. Kreuzer, *Projektive Hjelmslev-Räume*, PhD thesis, Techn. Univ. München, 1988.

[10] S. Kurz, Konstruktion und Eigenschaften ganzzahliger Punktmengen, *Bayreuther Math. Schr.* 76, 2006.

[11] R. Laue, Construction of combinatorial objects – a tutorial. *Bayreuther Math. Schr.* 43, 1993, 53-96.

[12] R. Laue, Constructing objects up to isomorphism, simple 9-designs with small parameters, *Algebr. Combin. Appl.*, Berlin, Heidelberg, New York, 2001, Springer, 232-260.

[13] B. Schmalz, Verwendung von Untergruppenleitern zur Bestimmung von Doppelnebenklassen, *Bayreuther Math. Schr.* 31, 1993, 109-143.