New arcs in projective Hjelmslev planes over Galois rings

Michael Kiermaier and Axel Kohnert

ABSTRACT. It is known that some good linear codes over a finite ring (R-linear codes) arise from interesting point constellations in certain projective geometries. For example, the expurgated Nordstrom-Robinson code, a nonlinear binary $[14, 6, 6]$-code which has higher minimum distance than any linear binary $[14, 6]$-code, can be constructed from a maximal 2-arc in the projective Hjelmslev plane over $\mathbb{Z}_4$.

We report on a computer search for maximal arcs in projective Hjelmslev planes over proper Galois rings of order ≤ 27. The used method is to prescribe a group of automorphisms which shrinks the problem to a computationally feasible size. The resulting system of Diophantine linear equations is solved by lattice point enumeration.

We improve many of the known lower bounds on the size of maximal arcs. Furthermore, the Gray image of one of the constructed arcs yields a quaternary $[504, 6, 376]$-code. This code has higher minimal distance than any known $\mathbb{F}_4$-linear $[504, 6]$-code.

1. Galois Rings

For a prime power $q = p^r$ and a natural number $m \in \mathbb{N} \setminus \{0\}$, the *Galois ring* $\mathrm{GR}(q^m, p^m)$ of order q^m and characteristic p^m is defined as $\mathbb{Z}_{p^m}[X]/(f)$, where $f \in \mathbb{Z}_{p^m}[X]$ is a monic polynomial of degree r which is irreducible modulo p. For different choices of the polynomial f, the resulting Galois rings are isomorphic.

The class of the Galois rings contains the finite fields and the integers modulo a prime power:

(i) $\mathrm{GR}(q, p) \cong \mathbb{F}_q$.
(ii) $\mathrm{GR}(p^m, p^m) \cong \mathbb{Z}_{p^m}$

A Galois ring that is not a finite field will be called *proper* Galois ring.

The Galois rings are well suited for base rings of linear codes: Case (i) gives the classical linear codes, and case (ii) contains the $\mathbb{Z}_4$-codes. The smallest Galois ring which is neither a finite field nor a residue class ring is $\mathbb{G}_{16} := \mathrm{GR}(16, 4)$. This ring admits very good codes, too: One example can be found in [**11**], a new one will be given below. As a subset of the finite chain rings, we can apply the theory in [**14**] to linear codes over Galois rings, including a generalized Gray isometry [**10**].

2. Arcs in projective Hjelmslev planes

The *projective Hjelmslev plane* $\mathrm{PHG}(2, R)$ over a Galois ring $R = \mathrm{GR}(q^m, p^m)$ is defined as follows: The point set $\mathfrak{P}$ (line set $\mathfrak{L}$) is the set of the free rank 1 (rank 2) submodules of the module R^3, and the incidence is given by set inclusion.

Key words and phrases. Galois ring, arc, projective Hjelmslev plane, coding theory, Gray map, linear code over rings, incidence matrix, group of automorphisms, Diophantine system of equations.

We have $|\mathfrak{P}| = |\mathfrak{L}| = (q^2+q+1)q^{2(m-1)}$. For $m \neq 1$, a projective Hjelmslev plane is not a classical projective plane, because two different lines may meet in more than one point. More about projective Hjelmslev geometries can be found in [**15**] and the references cited there.

For $n \in \mathbb{N}$, a set of points $\mathfrak{k} \subseteq \mathfrak{P}$ 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[1], $\mathfrak{k}$ is called (n,u)*-multiarc*.

If R is a finite field, $\mathrm{PHG}(2,R)$ is a classical projective plane. In this case, the arc problem and related problems are heavily investigated, see f. e. [**1, 8, 12**]. To exclude the classical case from the search, we restrict ourself to proper Galois rings R.

[**15**] contains a table for arcs over chain rings of composition length $m = 2$ and order ≤ 25. A few new arcs can be found in [**11**], and further improvements for chain rings of composition length $m = 2$ and order 9 and 25 are published in [**3**]. In [**18**] a complete classification of (n,u)-multiarcs was done for small u in small Hjelmslev geometries over chain rings $\neq \mathbb{Z}_{16}$ of order ≤ 16, which again yielded some improvements of the bounds. The most important results of this search can also be found in [**13**].

3. Solving Linear Diophantine Equations

The construction of discrete objects using incidence preserving group actions is a general approach that works in many cases [**17**]. It was first applied in the 70's for the construction of designs [**19**]. Later this method was used for the construction of q-analogs of designs [**7, 5**], parallelisms in projective geometries [**6**], distance optimal codes [**4**] and arcs over projective planes [**8**].

For our problem, we study the *incidence matrix* M of $\mathrm{PHG}(2,R)$: The columns are labeled by the points and the rows are labeled by the lines. The entry of M indexed by the line $L \in \mathfrak{L}$ and the point $P \in \mathfrak{P}$ is defined as

$$M_{L,P} := \begin{cases} 1 & \text{if } P \subset L \\ 0 & \text{otherwise} \end{cases}$$

Using this incidence matrix we can restate the problem of finding an (n,u)-arc as follows:

THEOREM 3.1. *There is a projective* (n,u)*-arc in* $\mathrm{PHG}(2,R)$ *if and only if there is a* $0/1$*-solution* $x = (x_1, \ldots, x_{|\mathfrak{P}|})$ *of the following system of (in)equalities*

$$\begin{array}{lrcl} (1) & \sum_{i=1}^{|\mathfrak{P}|} x_i & = & n \\ (2) & Mx^T & \leq & \begin{pmatrix} u \\ \vdots \\ u \end{pmatrix} \end{array}$$

and at least one of the lines of the system (2) *is an equality.*

This comes from the fact that the entries equal to one in a solution vector x define the selection of points which go into the arc. The restriction to a zero-one solution ensures that we get a projective arc. If one admits non-negative integers for the entries of x, the resulting solutions will be multiarcs.

To solve this system for interesting cases we use lattice point enumeration based on the *LLL*-algorithm [**20**]. But to get new results we have to solve systems of sizes which are too large for the solving algorithm. (e.g. $|\mathfrak{P}| = 775$ for $R = \mathbb{Z}_{25}$). To reduce the size of the system we

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

prescribe automorphisms $\phi \in \mathrm{GL}(3,R)$, so we are looking for solutions (i.e. arcs $\mathfrak{k}$) with the additional property that

$$P \in \mathfrak{k} \Rightarrow \phi(P) \in \mathfrak{k}$$

This means for the matrix M of the system that we can sum up columns which correspond to points lying in the same orbit. As the defining incidence property of the matrix M is invariant under the prescribed automorphism, i.e.

$$P \subset L \Rightarrow \phi(P) \subset \phi(L)$$

we get (after the fusion of points which are in the same orbit) identical rows in the matrix. These are the rows corresponding to the lines in the orbits, which we get by applying the automorphisms to the lines. Therefore we can also reduce the number of rows of the matrix M. As the number of orbits is identical on lines and points, the reduced matrix is again a square matrix of size m which is the number of orbits. We call this new matrix M^G where G is the group generated by the prescribed automorphisms. The rows are indexed by the orbits $\Omega_1, \ldots, \Omega_m$ of the lines, and the columns are labeled by the orbits $\omega_1, \ldots, \omega_m$ of the points. An entry of M^G is given by

$$M^G_{\Omega_i,\omega_j} := |\{P \in w_j : P \subset L\}|$$

where L is a representative of Ω_i. Now we can restate the above theorem:

THEOREM 3.2. *There is an (n,u)-arc in $\mathrm{PHG}(2,R)$ whose automorphism-group H contains the group $G < \mathrm{GL}(3,R)$ as a subgroup, if and only if, there is a $0/1-$solution $x = (x_1, \ldots, x_m)$ to the following system of (in)equalities*

$$\begin{array}{lrcl} (1) & \sum |\omega_i| x_i & = & n \\ (2) & M^G x^T & \leq & \begin{pmatrix} u \\ \vdots \\ u \end{pmatrix} \end{array}$$

and at least one of the lines of the system (2) is an equality.

For computational purposes we transform the system of inequalities into a system of equations. We solve the following system (we denote by $-I$ the negative unit matrix, and $(M^G, -I)$ denotes the $m \times 2m$ block matrix) :

$$\begin{array}{lrcl} (1) & \sum |\omega_i| x_i & = & n \\ (2) & (M^G, -I)(x,y)^T & = & \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \end{array}$$

The additional variables $y = (y_1, \ldots, y_m)$ in a solution may have values in $\{0, \ldots, u\}$. From these values we obtain the intersection numbers between an arc and the lines in $\mathrm{PHG}(2,R)$, so we easily get the secant distribution of an arc from these values. This is the system of Diophantine equations we finally solve to get new arcs.

4. An Example

We constructed a projective $(126,8)$-arc in $\mathrm{PHG}(2,\mathbb{G}_{16}) = (\mathfrak{P},\mathfrak{L})$. This plane has 336 points and lines, so the incidence matrix M has 336^2 entries which would it make difficult to solve the corresponding system of equations given in theorem 3.1.

To reduce the size, we take a matrix $A \in \mathbb{G}_{16}^{3\times 3}$ such that its image $\bar{A} \in \mathbb{F}_4^{3\times 3}$ modulo 2 generates a Singer cycle on $\mathrm{PG}(2,\mathbb{F}_4)$. So $\mathrm{ord}(A) = 21k$ where $k \in \mathbb{N}$. By replacing A by A^k we can assume $\mathrm{ord}(A) = 21$. Let G the cyclic group generated by A.

G operates on the point set $\mathfrak{P}$ by left-multiplication and partitions $\mathfrak{P}$ into 16 orbits of length 21. Each orbit contains exactly one point of each neighborhood class of $\mathrm{PHG}(2,\mathbb{G}_{16})$, so each neighborhood class contains exactly 6 points of $\mathfrak{k}$.

The smaller system corresponding to the 16×16 matrix M^G could be solved in a few seconds and we got a solution (x, y), which necessarily has exactly 6 entries from the first part x equal to 1. The second part y of the solution contains the secant distribution. The entries of y are either 0 or 8, so this $(126, 8)$-arc has only two different intersection numbers. There is exactly one entry of y equal to zero, so the arc intersects with $15 \cdot 21 = 315$ lines in 8 points and with 21 lines it has no intersection.

There is a further remarkable property of this arc $\mathfrak{k}$: Each orbit of G on $\mathfrak{P}$ is a maximal $(21, 2)$-arc, a socalled hyperoval. So $\mathfrak{k}$ can be split into 6 hyperovals. The hyperovals in $\mathrm{PHG}(2, \mathbb{G}_16)$ are unique up to geometric isomorphism [**18**]. More on their structure can be found in [**16**].

5. A nonlinear quaternary $[504, 6, 376]$-code

We take the homogeneous coordinates of the above $(126, 8)$-arc $\mathfrak{k}$ and put them as columns into a generator matrix of a $\mathbb{G}_{16}$-linear code C. We equip $\mathbb{G}_{16}$ with the homogeneous weight $w_{\mathrm{hom}} : \mathbb{G}_{16} \to \mathbb{N}$, that is

$$w_{\mathrm{hom}}(a) = \begin{cases} 0 & \text{if } a = 0 \\ 3 & \text{if } a \text{ is a unit} \\ 4 & \text{otherwise} \end{cases}$$

To calculate the homogeneous weight distribution of the code C, we use the theory and notation in [**14**]. Using the information on the intersection numbers and the neighborhood distribution, we see that there are only these two $\mathfrak{k}$-types of lines:

- 21 lines of $\mathfrak{k}$-type $(a_0, a_1, a_2) = (96, 30, 0)$
- 315 lines of $\mathfrak{k}$-type $(a_0, a_1, a_2) = (96, 22, 8)$

That gives the homogeneous weight enumerator

$$315 \cdot 12 \cdot X^{96\cdot 3+22\cdot 4} + 21 \cdot 12 \cdot X^{96\cdot 3+30\cdot 4} + 21 \cdot 3 \cdot X^{96\cdot 4} + 1 = 252X^{408} + 63X^{384} + 3780X^{376} + 1$$

So C is a $\mathbb{G}_{16}$-linear $[126, 3, 376]$-code. Using the generalized Gray map ψ as defined in [**10**], the code C yields a nonlinear[2] distance-invariant quaternary $[504, 6, 376]$-code $\psi(C)$.

By applying the one-step Griesmer bound (see f. e. [**2**], page 88), the existence of a linear quaternary $[504, 6, 376]$-code would imply the existence of a linear quaternary $[128, 5, 94]$-code. According to [**9**], no such code is known.

So $\psi(C)$ clearly is a very good nonlinear code and it might be better than any linear quaternary code of equal length and size.

6. New projective Arcs

Table 1 contains the sizes of the arcs we constructed with our method. All these sizes are at least as big as the previously best known sizes, with one exception: We only found a projective $(184, 12)$-arc in $\mathrm{PHG}(2, \mathbb{G}_{16})$, while the construction in Example 4.7 in [**15**] gives a projective $(186, 12)$-arc. This value is indicated by italic font in the table. If we know that an entry meets some known upper bound and therefore a corresponding arc is of maximal possible size, we use bold font. A lower index $*$ denotes an improvement against the previously known value.

[2] We used a computer check to make sure that C is nonlinear.

$u \backslash R$	$\mathbb{Z}_8$	$\mathbb{Z}_9$	$\mathbb{G}_{16}$	$\mathbb{Z}_{16}$	$\mathbb{Z}_{25}$	$\mathbb{Z}_{27}$
$\lvert\mathfrak{P}\rvert$	112	117	336	448	775	1053
2	**10**	**9**	**21**	**16**	20	21
3	**21**	**19**	27	28	34_*	39
4	28	$\mathbf{30}_*^E$	$\mathbf{52}_*$	49	60_*	65
5	37	39_*	68_*^E	61	79_*^E	91
6	48	48_*	$\mathbf{84}_*$	84	105_*^E	117
7	56	60_*^E	93_*	100	124_*	130
8	68	69_*	$\mathbf{126}_*$	120	150_*	172^E
9	79	**81**	140_*	136	175_*	193
10	88	**93**	152_*	156	199_*	234
11	100	**105**	164_*^E	172	223_*	240^E
12	**112**	**117**	*184*	208	256_*^E	288
13			200_*	212^E	310_*	302^E
14			216_*	232	311_*^E	351
15			236_*	252	328_*	369
16			**256**	276	355_*^E	390
17			**276**	292	385_*	417^E
18			**296**	312	417_*	468
19			**316**	331^E	465_*	505
20			**336**	360	480_*	520^E
21				376	510	567
22				400	534_*^E	595^E
23				424	565_*	617^E
24				**448**	592_*	657
25					**625**	676^E
26					**655**	702
27					**685**	747
28					**715**	783
29					**745**	819^E
30					**775**	840
31						873
32						909
33						945
34						981
35						**1017**
36						**1053**

TABLE 1. Sizes of the constructed projective (n, u)-arcs

We do not use the $*$-symbol for $\mathbb{Z}_8$, $\mathbb{Z}_{16}$ and $\mathbb{Z}_{27}$, since for these rings only very few values were published before. An upper index E denotes an arc we found by extension, this means that we used a program, which cheks whether it is possible to add a further point, which is not yet in the arc, without violating the defining condition of maximal u projective collinear points.

All the values in the table are for projective arcs. However, we know a non-projective multiarc which is bigger than the best known projective arc. This is a $(155, 8)$-multiarc in $\mathrm{PHG}(2, \mathbb{Z}_{25})$, it can be constructed in a similar way as the arc in the above example: The action of a lifted Singer cycle splits the point set of $\mathrm{PHG}(2, \mathbb{Z}_{25})$ into 25 orbits of length 31. It is possible to select 4 of these orbits, one of them twice, such that they together give the $(155, 8)$-multiarc.

More information on the arc (secant distribution, used group of automorphisms) can be found on the home pages of the authors.

References

[1] Simeon Ball. Multiple blocking sets and arcs in finite planes. *J. Lond. Math. Soc., II. Ser.*, 54(3):581–593, 1996.

[2] Anton Betten, Michael Braun, Harald Fripertinger, Adalbert Kerber, Axel Kohnert, and Alfred Wassermann. *Error-Correcting Linear Codes*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[3] Silvia Boumova and Ivan Landjev. Some new arcs in projective Hjelmslev planes over small chain rings. In *Proceedings of the Ninth International Workshop on Algebraic and Combinatorial Coding Theory 2004*, pages 56–61, 2004.

[4] M. Braun, A. Kohnert, and A. Wassermann. Optimal linear codes from matrix groups. *IEEE Transactions on Information Theory*, 12:4247–4251, 2005.

[5] Michael Braun. Some new designs over finite fields. *Bayreuther Math. Schr.*, 74:58–68, 2005.

[6] Michael Braun. Construction of a point-cyclic resolution in PG(9,2). *Innov. Incidence Geom.*, 3:33–50, 2006.

[7] Michael Braun, Adalbert Kerber, and Reinhard Laue. Systematic construction of q-analogs of t-(v, k, λ)-designs. *Des. Codes Cryptography*, 34(1):55–70, 2005.

[8] Michael Braun, Axel Kohnert, and Alfred Wassermann. Construction of (n, r)-arcs in $PG(2, q)$. *Innov. Incidence Geom.*, 1:133–141, 2005.

[9] Markus Grassl. Code Tables: Bounds on the parameters of various types of codes. `www.codetables.de`.

[10] Marcus Greferath and Stefan E. Schmidt. Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code. *IEEE Trans. Inf. Theory*, 45(7):2522–2524, 1999.

[11] Ludger Hemme, Thomas Honold, and Ivan Landjev. Arcs in projective Hjelmslev spaces obtained from Teichmüller sets. In *Proceedings of the Seventh International Workshop on Algebraic and Combinatorial Coding Theory 2000*, pages 4–12, 2000.

[12] J.W.P. Hirschfeld and L. Storme. The packing problem in statistics, coding theory and finite projective spaces: Update 2001. Blokhuis, A. (ed.) et al., Finite geometries. Proceedings of the fourth Isle of Thorns conference, Brighton, UK, April 2000. Dordrecht: Kluwer Academic Publishers. Dev. Math. 3, 201-246 (2001)., 2001.

[13] Thomas Honold and Michael Kiermaier. Classification of Maximal Arcs in Small Projective Helmslev Geometries. In *Proceedings of the Tenth International Workshop on Algebraic and Combinatorial Coding Theory 2006*, pages 112–117, 2006.

[14] Thomas Honold and Ivan Landjev. Linear codes over finite chain rings. *Electr. J. Comb.*, 7, 2000.

[15] Thomas Honold and Ivan Landjev. On arcs in projective Hjelmslev planes. *Discrete Math.*, 231(1–3):265–278, 2001.

[16] Thomas Honold and Ivan Landjev. On maximal arcs in projective Hjelmslev planes over chain rings of even characteristic. *Finite Fields Appl.*, 11(2):292–304, 2005.

[17] Adalbert Kerber. *Applied finite group actions. 2nd, rev. and exp. ed.* Algorithms and Combinatorics. 19. Berlin: Springer, 1999.

[18] Michael Kiermaier. Arcs und Codes über endlichen Kettenringen. Master's thesis, Technische Universität München, 2006.

[19] Earl S. Kramer and Dale M. Mesner. t-designs on hypergraphs. *Discrete Math.*, 15:263–296, 1976.

[20] Alfred Wassermann. Finding simple t-designs with enumeration techniques. *J. Comb. Des.*, 6(2):79–90, 1998.

MICHAEL KIERMAIER, MATHEMATICAL DEPARTMENT, UNIVERSITY OF BAYREUTH, D-95440 BAYREUTH, GERMANY

E-mail address: `michael.kiermaier@uni-bayreuth.de`

URL: `http://www.mathe2.uni-bayreuth.de/michaelk/`

AXEL KOHNERT, MATHEMATICAL DEPARTMENT, UNIVERSITY OF BAYREUTH, D-95440 BAYREUTH, GERMANY

E-mail address: `axel.kohnert@uni-bayreuth.de`

URL: `http://www.mathe2.uni-bayreuth.de/people/axel.html`