Sets of Type (d_1, d_2) in projective Hjelmslev planes over Galois Rings

Axel Kohnert *

Mathematisches Institut
University of Bayreuth
95440 Bayreuth
Germany
axel.kohnert@uni-bayreuth.de

Summary. In this paper we construct sets of type (d_1, d_2) in the projective Hjelmslev plane. For computational purposes we restrict ourself to planes over $\mathbb{Z}_{p^s}$ with p a prime and $s > 1$, but the method is described over general Galois rings. The existence of sets of type (d_1, d_2) is equivalent to the existence of a solution of a Diophantine system of linear equations. To construct these sets we prescribe automorphisms, which allows to reduce the Diophantine system to a feasible size. At least two of the newly constructed sets are 'good' $u-$arcs. The size of one of them is close to the known upper bound.

Key words: projective Hjelmslev plane, two-weight codes, arcs

1 Introduction and Motivation

The projective Hjelmslev plane over a Galois ring is a generalization of the projective plane over a finite field $GF(q)$ with field size q a power of a prime p. Similar to the finite field case the Galois ring $GR(p^s, p^{sm})$ is defined for positive integers s, m as the ring $\mathbb{Z}_{p^s}[x]/(h)$ where h is a monic polynomial of degree m over $\mathbb{Z}_{p^s}$ which is irreducible over $\mathbb{Z}_p$. For different choices of the polynomial h, the resulting Galois rings are isomorphic.

Two limiting special cases of Galois rings are the finite fields $GF(q)$ which are isomorphic to $GR(p, q)$ and the modular integers $\mathbb{Z}_{p^s}$ which are isomorphic to

* The author is pleased to acknowledge Prof. Bruno Buchberger and the coordinators of the Special Semester on Gröbner Bases (February 1 - July 31, 2006), organized by RICAM, Austrian Academy of Sciences, and RISC, Johannes Kepler University, Linz Austria for their interest to this project.

$GR(p^s, p^s)$. Basic facts about Galois rings can be found in [21]. For computational purposes we will restrict us to $\mathbb{Z}_{p^s}$ in this paper.

To construct the projective Hjelmslev plane we define the points as the free rank 1 submodules of $GR(p^s, p^{sm})^3$. The lines are the free submodules of rank 2. The incidence is given by set inclusion. In general this construction works for the larger class of chain rings R, the corresponding projective Hjelmslev plane is denoted by $PHG(2, R)$. In this paper the ring R is always a Galois ring. Much more on projective Hjelmslev planes can be found in the work of Honold, Landjev and their coworkers [12, 13, 17, 16]. A useful tool is the homomorphism $\phi : \mathbb{Z}_{p^{s+1}} \to \mathbb{Z}_{p^s}$ which maps an representing element from $\mathbb{Z}_{p^{s+1}}$ to its remainder modulo p^s. ϕ can be extended to a mapping $\hat{\phi} : PHG(2, GR(p^{s+1}, p^{(s+1)m})) \to PHG(2, GR(p^s, p^{sm}))$. This function maps points to points and lines to lines. It allows to define a neighborhood of a point (or a line) in $PHG(2, GR(p^{s+1}, p^{(s+1)m}))$ as the set of points (or lines) having the same image under $\hat{\phi}$.

For two nonnegative integers d_1 and d_2 a set C of type (d_1, d_2) (also called two-intersection set) in a projective Hjelmslev plane is a set of points such that every line of the plane contains either d_1 or d_2 points of C. We always assume $d_1 < d_2$. In the case of a finite field the problem of sets of type (d_1, d_2) has been studied in a large number of papers (e.g. [10, 9, 11, 18, 19, 20]). They also study the more general case of point sets in $PG(k, q)$ with two intersection numbers with respect to the hyperplanes.

The interest in such point sets in the projective plane comes from the fact that they include hyperovals, some maximal arcs, unitals and Baer subplanes [11]. In the general case of the projective space $PG(k, q)$ with $k > 2$ the sets of type (d_1, d_2) have been also studied in the equivalent language of linear codes. Then these point sets are two-weight codes. For a survey see [8]. In coding theory one is interested in a high minimum distance for a fixed length n of the code, this corresponds to a point set with n points and intersection numbers as low as possible. There are cases where the best (for coding theory) point sets are such of type (d_1, d_2). More on the connection between linear codes and projective geometry can be found in [1, 3].

Also in the case of a projective Hjelmslev plane over a Galois ring there are links to coding theory. There are famous codes like the Nordstrom-Robinson-Code which are 'better' than the linear codes which are connected to $PG(k, q)$. These better codes are $\mathbb{Z}_4-$linear codes. To describe these $\mathbb{Z}_4-$linear codes using projective geometry we need the projective Hjelmslev geometry. Now the hope is to find more good codes studying $PHG(k, GR(p^s, p^{sm}))$ in general.

2 Parameters

There are several relations connecting the two parameters of the set C of type (d_1, d_2) to the number of lines and points in $PHG(2, GR(p^s, p^{sm}))$. These will

allow to restrict the search to the cases of feasible pairs of parameters. We denote by t_1 and t_2 the number of lines intersecting with d_1 points respectively d_2 points from the set C. For a projective Hjelmslev plane over $GR(p^s, p^{sm})$ with point set P and line set L we know with $q := p^m$:

Lemma 1. *([16] Fact 1)*

1. $|L| = |P| = (q^2 + q + 1)q^{2(s-1)}$
2. *Each line (point) is incident with* $(q + 1)q^{s-1}$ *points (lines).*

The first equations show that the numbers of lines and points in a Hjelmslev plane over a Galois ring is a multiple of the number of points and lines in $PG(2, q)$. It is possible to get the Hjelmslev plane by substituting one point of $PG(2, q)$ by $q^{2(s-1)}$ points building a neighborhood in $PHG(2, GR(p^s, p^{sm}))$. Using the lemma above we can derive the following relations with $c = |C|$:

1. $t_1 + t_2 = (q^2 + q + 1)q^{2(s-1)}$
2. $d_1t_1 + d_2t_2 = c(q + 1)q^{s-1}$

   These two equations give restrictions on possible values of d_1 and d_2 as t_1 and t_2 have to be integral numbers. In the case $s = 1$ (i.e. finite field) there is a third relation, which we get by counting the number of pairs of different points in C in two ways:

3. $d_1(d_1 - 1)t_1 + d_2(d_2 - 1)t_2 = c(c - 1)$

The right hand is the number of different pairs in C. The left hand side we get when we look at the unique line corresponding to the pair of points. In t_1 cases this is a line having intersection number d_1. Counting the possible pairs in C corresponding to this line we get the first summand. This last equation can not easily be generalized to an s greater than 1 as the number of lines through a pair of different points from C depends then on the neighbor relation between the two points. There may be more than one line through two points, which changes relation 3 into an inequality.

In general it is possible to construct new sets of type (d_1, d_2) over $PHG(2, GR(p^{s+1}, p^{(s+1)m}))$ using two-intersection sets in $PHG(2, GR(p^s, p^{sm}))$. A useful starting point for these recursive constructions are the single points and complete lines in $PG(2, p)$ which is isomorphic to $PHG(2, GR(p, p))$ or a single point in an arbitrary projective Hjelmslev plane.

Lemma 2. *(Recursive construction)*

Let S be a set of type (d_1, d_2) over $GR(p^s, p^{sm})$, then there is a set of type (pd_1, pd_2) over $GR(p^{s+1}, p^{(s+1)m})$.

Proof. The key is the function $\hat{\phi}$: $PHG(2, GR(p^{s+1}, p^{(s+1)m})) \to PHG(2, GR(p^s, p^{sm}))$. It maps two-intersection sets to two-intersection sets. Each element in S is replaced by the p^2 elements of the complete neighborhood (the preimages under $\hat{\phi}$) in $PHG(2, GR(p^{s+1}, p^{(s+1)m}))$. The t_1 lines intersecting in d_1 points are mapped to $p^2 t_1$ lines intersecting in pd_1 points, and the t_2 lines intersecting in d_2 points are mapped to $p^2 t_2$ lines intersecting in pd_2 points.

Example 1. Take a line in the Fano plane $PG(2,2) = PHG(2, GR(2,2))$. This is a set of type $(1,3)$ with $t_1 = 6$ and $t_2 = 1$ and order 3. From this we construct a set of type $(2,6)$ in $PHG(2, GR(4,4))$ with $t_1 = 24$ and $t_2 = 4$ and order 12.

3 Constrution of Sets of Type (d_1, d_2)

The set P of points and the set L of lines of a projective Hjelmslev plane $PHG(2, GR(p^s, p^{sm}))$ define an incidence system. Denote by M the corresponding incidence matrix. The rows are labeled by the lines, the columns are labeled by the points, then we have for a point p and a line l:

$$M_{l,p} := \begin{cases} 1 \text{ if } p \text{ is incident with } l, \\ 0 \qquad \text{otherwise.} \end{cases}$$

It is then possible to state the existence of a (d_1, d_2) using a Diophantine system of equations:

Theorem 1.

There is a set of type (d_1, d_2) in $PHG(2, GR(p^s, p^{sm}))$ if and only if there is a $0/1-$solution $x = (x_1, \ldots, x_{|P|})^T$ of the following system of equations

$$Mx = \begin{pmatrix} d_1 \text{ or } d_2 \\ \vdots \\ d_1 \text{ or } d_2 \end{pmatrix}.$$

This set of equation has to be read as follows: A solution x has the property that the product of a single with x is d_1 or d_2. As we want to solve this Diophantine system using some standard method we restate it as a linear equation as follows. Denote by D the matrix of the same size as M with $(d_1 - d_2)$ on the diagonal and 0 elsewhere. We denote by $(M|D)$ the block matrix built from the incidence matrix M and the matrix D :

$$(M|D) := \begin{pmatrix} m_{1,1} & m_{1,2} & & m_{1,|P|} & d_1 - d_2 & 0 & \ldots & 0 & 0 \\ m_{2,1} & m_{2,2} & & m_{2,|P|} & 0 & d_1 - d_2 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ & & \ddots & & 0 & 0 & \ldots & d_1 - d_2 & 0 \\ m_{|L|,1} & m_{|L|,2} & & m_{|L|,|P|} & 0 & 0 & \ldots & 0 & d_1 - d_2 \end{pmatrix}.$$

Corollary 1.

There is a set of type (d_1, d_2) *in* $PHG(2, GR(p^s, p^{sm}))$ *if and only if there is a* $0/1-$*solution* $x|y = (x_1, \ldots, x_{|P|}, y_1, \ldots, y_{|L|})^T$ *of the following system of equalities*

$$(M|D)(x|y) = \begin{pmatrix} d_1 \\ \vdots \\ d_1 \end{pmatrix}.$$

Given the solution it is possible to read off if a line l intersects with d_1 points. This is the case if $y_l = 0$, or with d_2 points, in this case $y_l = 1$.

The size of this problem is given by the number of points. In general this number is growing too fast. To handle also larger cases we apply the following method. We no longer look for an arbitrary set of type (d_1, d_2). We are now only interested in a set which has a prescribed group $G < PGL(2, GR(p^s, p^{sm}))$ of automorphisms. An automorphism φ of a point set $C = \{c_1, \ldots, c_n\}$ is an element from $PGL(2, GR(p^s, p^{sm})$ such that $C = \{\varphi(c_1), \ldots, \varphi(c_n)\}$.

The main advantage of this method is that the size of the system of equations is much smaller, it will only have the size equal to the number of orbits of G on the points of $PHG(2, GR(p^s, p^{sm}))$. We can summarize this construction as a two-step process:

- In a first step the solution of a construction problem is described as a solution of a Diophantine system of linear equations.
- In a second step the size of the linear system is reduced by prescribing automorphisms.

This construction method is a general approach that works for many discrete structures as designs [15, 2], q-analogs of designs [6], arcs in projective geometries [7] or linear codes [1, 4, 5]. The general method is as follows: The matrix M is reduced by adding up columns (labeled by the points of $PHG(2, GR(p^s, p^{sm}))$ corresponding to the orbits of G. Now because of the relation

$$p \in l \iff \varphi(p) \in \varphi(l) \tag{1}$$

for any point p and line l and any automorphism $\varphi \in G$ the rows corresponding to lines from a orbit of G are equal, therefore these are removed from the system of equations and we get a square matrix denoted by M^G. The number of orbits on the points and the number of orbits on the lines is equal, as we can label the lines by the orthogonal point and then act with the transposed matrix. We denote by $\omega_1, \ldots, \omega_s$ the orbits on the points and by $\Omega_1, \ldots, \Omega_s$ the orbits on the lines. For an entry of M^G we have:

$$M^G_{\Omega_i, \omega_j} = |\{p \in \omega_j : p \in l\}|$$

where l is a representative of the line orbit Ω_i. Because of property (1) this definition is independent of the representative. Now we can restate the above theorem in a version with the condensed matrix M^G :

Theorem 2.

Let G be a subgroup of $PGL(2, GR(p^s, p^{sm}))$. There is a set of type (d_1, d_2) in $PHG(2, GR(p^s, p^{sm}))$ whose group of automorphisms contains G as a subgroup if, and only if, there is a $0/1-$solution $x = (x_1, \ldots, x_{|s|})^T$ of the following system of equations:

$$M^G x = \begin{pmatrix} d_1 \text{ or } d_2 \\ \vdots \\ d_1 \text{ or } d_2 \end{pmatrix}.$$

To solve this using a computer we transform it like in the above corollary into a Diophantine system of linear equations and using the slack variables we get the information which lines intersect in d_1 points and which one in d_2 points.

4 Example

We describe the construction of the set of type $(2, 5)$ over $\mathbb{Z}_9$ with 39 points, which is a very good $5-$arc as explained in the following section with results. $PHG(2, \mathbb{Z}_9)$ has 117 points, therefore the Diophantine system of equations which is to be solved would have 234 variables and 117 equations. We prescribe a group G of automorphisms generated by a single element:

$$G := \left\langle \begin{pmatrix} 7\,1\,0 \\ 4\,8\,4 \\ 5\,3\,8 \end{pmatrix} \right\rangle.$$

This group has 9 orbits, each of size 13. In fact this group is a lifted version (i.e. a preimage under ϕ) of the Singer cycle in $PGL(2, 3)$. $PHG(2, \mathbb{Z}_9)$ can be constructed from $PG(2, 3)$ by substituting each point in $PG(2, 3)$ by 9 'lifted' points of $PHG(2, \mathbb{Z}_9)$. Each orbit now contains for each point of $PG(2, 3)$ one lifted point. The condensed matrix M^G is a 9×9 matrix:

$$M^G = \begin{pmatrix} 0\,3\,2\,2\,1\,1\,0\,1\,2 \\ 0\,0\,2\,2\,1\,1\,3\,1\,2 \\ 1\,1\,0\,3\,2\,2\,1\,2\,0 \\ 2\,2\,1\,1\,0\,0\,2\,3\,1 \\ 1\,1\,0\,0\,2\,2\,1\,2\,3 \\ 3\,0\,2\,2\,1\,1\,0\,1\,2 \\ 1\,1\,3\,0\,2\,2\,1\,2\,0 \\ 2\,2\,1\,1\,3\,0\,2\,0\,1 \\ 2\,2\,1\,1\,0\,3\,2\,0\,1 \end{pmatrix}.$$

The solution $x = (1, 0, 0, 0, 1, 1, 0, 0, 0)$ of the equation from Theorem 2 corresponds to the set of type $(2, 5)$ with 39 points built from three orbits. From

$$M^G x^T = \begin{pmatrix} 2 \\ 2 \\ 5 \\ 2 \\ 5 \\ 5 \\ 5 \\ 5 \\ 5 \end{pmatrix}$$

we read off which line orbits have intersection size 2 and which one size 5.

5 Results

In this section we give results for projective Hjelmslev planes over the Galois rings isomorphic to $\mathbb{Z}_4, \mathbb{Z}_8, \mathbb{Z}_9, \mathbb{Z}_{16}, \mathbb{Z}_{25}, \mathbb{Z}_{27}$. As the complement of a set of type (d_1, d_2) is again a set with only two intersection numbers, we list only those sets C where $|C|$ is at most half of the points. In the following table we list the parameters (d_1, d_2) of two-intersection sets we constructed with the method described. By t_1 and t_2 we denote the number of lines having intersection numbers d_1 and d_2. We denote by * in the second column if this set can not be constructed using the recursive method from 2. We do not list the trivial set consisting of one point. This list is not complete, as we only construct a two-intersection set C if we first choose a group G such that there is a C with this group of automorphism, and secondly the resulting Diophantine system is small enough to be solved. So it may happen that further parameters (d_1, d_2) are possible and for pairs (d_1, d_2) already in the list there may be other sets, with different groups of automorphisms.

R	$\|C\|$	d_1	d_2	t_1	t_2
$\mathbb{Z}_4$	4	0	2	16	12
	6^*	0	2	10	18
	7^*	0	2	7	21
	12	2	6	24	4
	14^*	2	4	14	14

R	$\|C\|$	d_1	d_2	t_1	t_2
$\mathbb{Z}_8$	4	0	2	88	24
	6^*	0	2	76	36
	8^*	0	2	64	48
	16	0	4	64	48
	24	0	4	40	72
	28^*	2	6	84	28
	28	0	4	28	84
	32^*	2	6	72	40
	36^*	3	7	88	24
	36^*	2	6	60	52
	44^*	2	6	36	76
	48^*	2	6	24	88
	48^*	4	8	80	32
	48	4	12	96	16
	52^*	3	7	40	72
	52^*	4	8	68	44
	56	4	8	56	56

R	$\|C\|$	d_1	d_2	t_1	t_2
$\mathbb{Z}_9$	9	0	3	81	36
	30^*	2	5	75	42
	36	3	12	108	9
	39^*	3	6	78	39
	39^*	2	5	39	78
	42^*	3	6	66	51

R	$\|C\|$	d_1	d_2	t_1	t_2
$\mathbb{Z}_{16}$	4	0	2	400	48
	6^*	0	2	376	72
	8^*	0	2	352	96
	12^*	0	2	304	144
	16	0	4	352	96
	24	0	4	304	144
	28^*	0	4	280	168
	32	0	4	256	192
	40^*	0	4	208	240
	64	0	8	256	192
	96	0	8	160	288
	112	4	12	336	112
	112	0	8	112	336
	128	4	12	288	160
	144	4	12	240	208
	144	6	14	352	96
	176	4	12	144	304
	192	8	24	384	64
	192	8	16	320	128
	192	4	12	96	352
	208	6	14	160	288
	208	8	16	272	176
	224	10	14	224	224

R	$\|C\|$	d_1	d_2	t_1	t_2
$\mathbb{Z}_{25}$	25	0	5	625	150
	155^*	5	10	620	155
	310^*	9	14	310	465
	310^*	10	15	465	310

These results are also interesting if you look for arcs. There are at least two cases where we found improvements against previously known values for the maximal size of $u-$arcs. More on arcs in projective Hjelmslev planes can be found in [12]. The construction of $u-$arcs over Galois rings will also be covered in a forthcoming paper with M. Kiermaier. Some first results can be found in the proceedings of the 2007 conference on optimal codes [14].

The most interesting set is the $39-$set of type $(2, 5)$ in $\mathbb{Z}_9$. This is a $5-$arc just one point below the upper-bound of 40 points. It improves the previously known $5-$arc with 31 points. The other improvement is the $310-$set of type $(9, 14)$ in $\mathbb{Z}_{25}$. The paper by Landjev and Honold only cover the cases with $s = 2$. We didn't find tables for $\mathbb{Z}_8$ and $\mathbb{Z}_{16}$.

References

1. Anton Betten, Michael Braun, Harald Fripertinger, Adalbert Kerber, Axel Kohnert, and Alfred Wassermann. *Error-correcting linear codes. Classification by isometry and applications. With CD-ROM.* Algorithms and Computation in Mathematics 18. Berlin: Springer. xxix, 798 p. , 2006.
2. Anton Betten, Adalbert Kerber, Axel Kohnert, Reinhard Laue, and Alfred Wassermann. The discovery of simple 7-designs with automorphism group PΓL$(2, 32)$. Cohen, Gérard (ed.) et al., Applied algebra, algebraic algorithms and error-correcting codes. 11th international symposium, AAECC-11, Paris, France, July 17-22, 1995. Proceedings. Berlin: Springer-Verlag. Lect. Notes Comput. Sci. 948, 131-145 (1995)., 1995.
3. Juergen Bierbrauer. *Introduction to coding theory.* Discrete Mathematics and its Applications. Boca Raton, FL: Chapman & Hall/CRC. xxiii, 390 p., 2005.
4. M. Braun. Construction of linear codes with large minimum distance. *IEEE Transactions on Information Theory*, 50(8):1687–1691, 2004.
5. M. Braun, A. Kohnert, and A. Wassermann. Optimal linear codes from matrix groups. *IEEE Transactions on Information Theory*, 12:4247–4251, 2005.
6. Michael Braun. Some new designs over finite fields. *Bayreuther Math. Schr.*, 74:58–68, 2005.
7. Michael Braun, Axel Kohnert, and Alfred Wassermann. Construction of (n, r)-arcs in $PG(2, q)$. *Innov. Incidence Geom.*, 1:133–141, 2005.
8. R. Calderbank and W.M. Kantor. The geometry of two-weight codes. *Bull. Lond. Math. Soc.*, 18:97–122, 1986.
9. Massimo de Finis. On k-sets of type (m,n) in projective planes of square order. Finite geometries and designs, Proc. 2nd Isle of Thorns Conf. 1980, Lond. Math. Soc. Lect. Note Ser. 49, 98-103 (1981)., 1981.
10. Massimo de Finis. On k-sets in PG(3,q) of type (m,n) with respect to planes. *Ars Comb.*, 21:119–136, 1986.
11. J.W.P. Hirschfeld. *Projective geometries over finite fields. 2nd ed.* Oxford Mathematical Monographs. Oxford: Clarendon Press. xiv, 555 p. , 1998.
12. Thomas Honold and Ivan Landjev. On arcs in projective Hjelmslev planes. *Discrete Math.*, 231(1-3):265–278, 2001.
13. 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.
14. Michael Kiermaier and Axel Kohnert. New arcs in projective Hjelmslev planes over Galois rings. Fifth International Workshop on Optimal Codes and Related Topics, Balchik 2007, 112-119 (2007)., 2007.
15. Earl S. Kramer and Dale M. Mesner. t-designs on hypergraphs. *Discrete Math.*, 15:263–296, 1976.
16. Ivan Landjev. On blocking sets in projective Hjelmslev planes. *Adv. Math. Commun.*, 1(1):65–81, 2007.
17. Ivan Landjev and Thomas Honold. Arcs in projective Hjelmslev planes. *Discrete Math. Appl.*, 11(1):53–70, 2001.
18. Tim Penttila and Gordon F. Royle. Sets of type (m, n) in the affine and projective planes of order nine. *Des. Codes Cryptography*, 6(3):229–245, 1995.
19. Giuseppe Tallini. Some new results on sets of type (m,n) in projective planes. *J. Geom.*, 29:191–199, 1987.
20. Maria Tallini Scafati. The k-sets of type (m, n) in a Galois space $S_{r,q}$ $(r \geq 2)$. Colloq. int. Teorie comb., Roma 1973, Tomo II, 459-463 (1976)., 1976.

21. Zhe-Xian Wan. *Lectures on finite fields and Galois rings.* River Edge, NJ: World Scientific. x, 342 p., 2003.