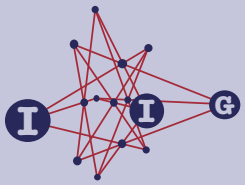


Construction of (n, r)-arcs in $PG(2, q)$

Michael Braun Axel Kohnert Alfred Wassermann

Abstract

We construct new (n, r)-arcs in $PG(2, q)$ by prescribing a group of automorphisms and solving the resulting Diophantine linear system with lattice point enumeration. We can improve the known lower bounds for $q = 11, 13, 16, 17, 19$ and give the first example of a double blocking set of size n in $PG(2, p)$ with $n < 3p$ and p prime.

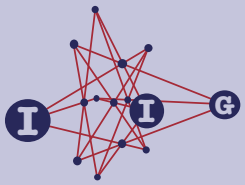
Keywords: arcs, blocking set, projective plane, incidence matrix, group of automorphisms, lattice point enumeration

MSC 2000: 05B25, 51E20, 51E20

1. Introduction

An (n, r)-arc is a set of n points of $PG(2, q)$ such that at most r of these points are collinear, but some r of these n points are collinear. We define $m_r(2, q)$ as the maximum n such that an (n, r)-arc does exist. There are many results [1, 12] concerning these numbers, and for $q < 11$ the exact values are known. In this paper we explicitly construct new arcs for $11 \leq q \leq 19$ which contain more points than the previously known ones. So we improved the previous known lower bounds on $m_r(2, q)$ in several cases. This method works also well for higher values of r, so we can also construct multiple blocking sets as these are complements of arcs.

We first restate the problem of finding arcs as the solution of a system of Diophantine equations which is formulated using the incidence matrix of the projective plane $PG(2, q)$. As this system is too large for interesting cases we prescribe automorphisms on the arcs, so that the dimension of the problem is no longer the number of points (or lines) but the number of orbits of points (resp. lines) under the prescribed automorphisms.



2. Solving Linear Equations

We start with the projective plane $PG(2,q)$ over a finite field $GF(q)$ and with the set P of q^2+q+1 points which are the 1-dimensional subspaces of $GF(q)^3$ and the set L of q^2+q+1 lines which are the 2-dimensional subspaces of $GF(q)^3$.

Now, we study the incidence matrix M of $PG(2,q)$: the columns are labeled by the points and the rows are labeled by the lines. The entry of M indexed by the two subspaces $l \in L$ and $p \in P$ is defined as

$$M_{l,p} := \begin{cases} 1 & \text{if } p \text{ is a subspace of } l, \\ 0 & \text{otherwise.} \end{cases}$$

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

Theorem 2.1. *There is an (n,r)-arc in $PG(2,q)$*

$$\Longleftrightarrow$$

There is a $0/1$-solution $x = (x_1, \ldots, x_{|P|})$ of the following system of (in)equalities

$$\begin{array}{lccc} (1) & \sum x_i & = & n \\ (2) & Mx & \leq & \begin{pmatrix} r \\ \vdots \\ r \end{pmatrix} \end{array}$$

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 a selection of points which goes into the arc.

To solve this system for interesting cases we use lattice point enumeration based on the $LLL-$algorithm [15]. But to get new results we have to solve systems of sizes which are too large for the solving algorithm. (e.g. $q^2+q+1 = 273$ for $q = 16$). To reduce the size of the system we prescribe automorphisms $\phi \in GL(3,q)$, so we are looking for arcs S with the additional property that

$$p \in S \Rightarrow \phi(p) \in S.$$

This means for the matrix M of the system that we add 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.

$$p \leq l \Rightarrow \phi(p) \leq \phi(l)$$

we get after the fusion of the points in the orbits identical rows in the matrix for the lines in the orbits if we apply the automorphism to the lines. So 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. 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

$$M^G_{\Omega_i,\omega_j} := \big|\{p \in w_j : p \text{ is a subspace of } l\}\big|$$

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

Theorem 2.2. *There is an (n, r)-arc in $PG(2, q)$ with automorphism-group H where $GL(3, q) \geq H \geq G$*

$$\Longleftrightarrow$$

There is a $0/1$-solution $x = (x_1, \ldots, x_m)$ to the following system of (in)equalities

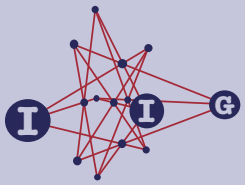
$$\begin{array}{lrcl} (1) & \sum |\omega_i| x_i & = & n \\ (2) & M^G x & \leq & \begin{pmatrix} r \\ \vdots \\ r \end{pmatrix} \end{array}$$

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:

$$\left[\begin{array}{c|c} & \begin{matrix} -1 & 0 & \cdots & 0 \\ 0 & -1 & & \vdots \\ \vdots & & \ddots & \\ & & & -1 \;\; 0 \\ 0 & \cdots & & 0 \;\; -1 \end{matrix} \\ M^G & \\ & \\ \hline |\omega_1| \ldots\ldots |\omega_m| & \begin{matrix} 0 & \cdots & \cdots & 0 \end{matrix} \end{array}\right] \times \left[\begin{array}{c} x_1 \\ \vdots \\ x_m \\ y_1 \\ \vdots \\ y_m \end{array}\right] = \left[\begin{array}{c} 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \\ \hline n \end{array}\right]$$

The additional variables $y = (y_1, \ldots, y_m)$ in a solution may have values in $\{0, 1, \ldots, r\}$. From these values we obtain the intersection numbers between an arc and the lines in the projective plane, 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.



3. Related Work

It is well known [11] that there is an equivalence between the existence of a projective linear $[n, 3]$-code over $GF(q)$ with minimum distance d and the existence of an $(n, n-d)$-arc over $PG(2, q)$. This equivalence comes from the fact that both problems can be formulated using the incidence matrix between subspaces of $GF(q)^3$. Previously, we applied the same method successfully in the construction of linear codes [3, 4] .

The construction of discrete objects using incidence preserving group actions [13] is a general approach that works in many other cases like designs [2, 14], q-analogs of designs [6], parallelisms in projective geometries [5] .

4. Two Examples

4.1. Construction of a $(32, 4)$-arc in $PG(2, 11)$

We will show in the case of a $(32, 4)$-arc in $GF(11)$ how our method works. Without prescribing automorphisms the size of the incidence matrix is 133×133. We reduce the size by prescribing a randomly chosen cyclic subgroup $G \leq GL(3, 11)$. We started with the generator

$$g := \begin{pmatrix} 5\,0\;5 \\ 9\,6\;2 \\ 3\,4\,10 \end{pmatrix}$$

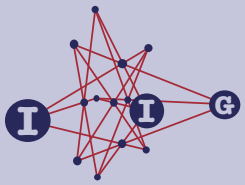
over $GF(11) = \mathbb{Z}_{11}$. The next step is the computation of the orbits. For example the lexicographically first orbit of the column labeling 1-dimensional subspaces is

$$\omega_1 = G(\langle 0, 0, 1\rangle) = \left\{ \begin{array}{c} \langle 0, 0, 1\rangle, \langle 1, 7, 2\rangle, \\ \langle 1, 0, 10\rangle, \langle 0, 1, 10\rangle, \\ \langle 1, 8, 10\rangle \end{array} \right\}.$$

Altogether there are 29 orbits which is a reduction of a factor of about 5 in rows and columns. The orbits in the rows which are orbits of lines are labeled by the 1-dimensional orthogonal spaces. The first orbit is

$$\Omega_1 = G(\langle 0, 0, 1\rangle^\perp) = \left\{ \begin{array}{c} \langle 0, 0, 1\rangle^\perp, \langle 1, 5, 7\rangle^\perp, \\ \langle 1, 5, 6\rangle^\perp, \langle 1, 5, 10\rangle^\perp, \\ \langle 1, 5, 9\rangle^\perp \end{array} \right\}.$$

To compute the reduced incidence matrix we take one representative of the lines, e.g. $\langle 1, 5, 10\rangle^\perp$ and compute the number of entries in the orbits of the



lines which are orthogonal, i.e. which are collinear. In the example there are no orthogonal pairs, which says $M^G_{\Omega_1,\omega_1} = 0$. The complete matrix is given below:

$$M^G = \begin{pmatrix}
0100010000001111100001101010 1 \\
1221110000110010100000000000 0 \\
0001101001101100200000012000 0 \\
0200001001101100021000000011 0 \\
1000011111111111000000000000 0 \\
0101000000022001001111000100 0 \\
0011020002001000001010101001 0 \\
1001101000101010000021000020 0 \\
1010100020002000110010100010 0 \\
0010110000001111010100010101 0 \\
1010001000101010001200002010 0 \\
0000010010110001201100000012 0 \\
0000100002010020110111000010 0 \\
0110000100000000110111101101 0 \\
0011002000000012111010100000 0 \\
2001010000000200111111000000 0 \\
1100001011010000101001111000 0 \\
2100100001000002000010001111 0 \\
0005000100000000000000010050 0 \\
1000010000110010011000200210 0 \\
0100122010000000000111000110 0 \\
0020000011100101001002000110 0 \\
0010101000020200000010101011 0 \\
0101100011100101000200200000 0 \\
0101000020000120001010001101 0 \\
1011001011010000010100000101 1 \\
0000000000500000000050010000 1 \\
0000500100000000005000000000 1 \\
0001110010110001020001002000 0
\end{pmatrix}$$

Together with the sizes of the point orbits

$$w = (|\omega_1|, \ldots, |\omega_{29}|) =$$

$$(5555555155555555555555155551)$$

we can state the system of equations

$$(1) \quad wx = 32$$
$$(2) \quad M^G x \leq \begin{pmatrix} 4 \\ \vdots \\ 4 \end{pmatrix}$$

which we solved within seconds using the LLL-Algorithm and got the solution

$$x = (11000101000010000001000000011)$$

which also has the requested property of reaching the bound 4 for some 4-set of points. From this solution we can read off the orbits whose union gives the arc. As $x_1 = 1$ we know for example that ω_1 is part of the arc, altogether we get the arc

$$\omega_1 \cup \omega_2 \cup \omega_6 \cup \omega_8 \cup \omega_{13} \cup \omega_{20} \cup \omega_{28} \cup \omega_{29} =$$

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 7 & 8 & 1 & 0 & 6 & 9 & 9 & 5 & 7 & 8 & 9 & 10 & 10 & 1 & 1 & 3 & 4 & 10 & 2 & 4 & 4 & 7 & 8 & 1 & 0 & 2 & 3 & 3 & 2 \\ 1 & 10 & 10 & 2 & 10 & 5 & 3 & 10 & 0 & 7 & 2 & 5 & 8 & 6 & 0 & 2 & 0 & 7 & 8 & 2 & 7 & 8 & 3 & 7 & 6 & 3 & 9 & 8 & 6 & 6 & 10 & 0 \end{bmatrix}$$

where each column is the generator of one point of the arc. The first 5 columns are the 5 points in the first orbit. To get the secant distribution we have to study the second part of the solution:

$$y = (4\ 4\ 1\ 4\ 4\ 4\ 4\ 4\ 3\ 4\ 4\ 4\ 1\ 4\ 0\ 4\ 2\ 4\ 1\ 2\ 4\ 0\ 1\ 3\ 2\ 4\ 1\ 2\ 1)$$

together with the size of the line orbits

$$(5\ 5\ 5\ 5\ 5\ 5\ 5\ 5\ 5\ 5\ 5\ 5\ 5\ 5\ 5\ 5\ 5\ 5\ 1\ 5\ 5\ 5\ 5\ 5\ 5\ 5\ 1\ 1\ 5).$$

Now we can see from $y_1 = 4$ that the 5 lines in the first orbit are incident with 4 points. On the other hand we get from $y_{15} = 0$ that the 5 lines in orbit number 15 do not intersect with the points from the arc. Altogether we get for the $i-$secant numbers τ_i, where τ_i is the number of lines meeting the arc in exactly i points:

$$\tau = (\tau_0, \ldots, \tau_4) = (10, 22, 16, 10, 75).$$

4.2. Construction of the first double blocking set with 38 points in $PG(2, 13)$

Using the above method with the prescribed group

$$G = \left\langle \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \right\rangle$$

we found a $(145, 12)$-arc. The complement of this arc is a double blocking set with 38 points, which is given below (one generator of a point per column):

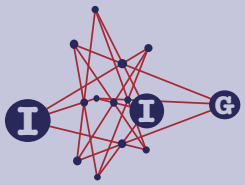
$$\left[\begin{array}{cccccccccccccccccccccccccccccccccccc}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&12&12&2&2&4&4&5&5&8&8&9&9&11&11&3&3&10&10&3&3&5&5&6&6&7&7&8&8&10&10&1&1&0&0\\
1&12&1&12&3&10&5&8&6&7&6&7&5&8&3&10&4&9&4&9&5&8&2&11&4&9&4&9&2&11&5&8&3&10&4&9&0&0
\end{array}\right]$$

This is the first example of a double blocking set in $PG(2, p)$ of size n with $n < 3p$ and p prime.

5. Results

Using the above method we improved lower bounds on the values $m_r(2, q)$. Tables with upper bounds on q up to 13 can be found in [1, 8, 12]. Tables for $q = 17$ can be found in [7, 9, 10]. The following table contains the sizes of the arcs we constructed with our method. With an upper index $^+$ we denote if the entry is the exact value for $m_r(2, q)$. The lower index $_*$ denotes an improvement against the published tables. In the cases $q = 16, 19$ we found no published tables.

$r \backslash q$	11	13	16	17	19
2	12^+	14^+	18^+	18^+	20^+
3	21	23	28	28_*	31
4	32_*	38_*	52^+	48_*	52
5	43	49_*	65	61_*	68
6	56^+	64_*	78	78_*	86
7	67^+	79^+	93	94_*	105
8	77	92^+	120^+	114_*	124
9	89	105^+	128	137^+	147
10	100	118_*	142	154^+	172^+
11		132_*	159	166_*	191^+
12		145_*	180		204
13			195	204_*	225
14			210	219	242
15			231	239	262
16				256	285
17					304
18					324



Acknowledgement. The authors thank S. Ball for valuable comments and fruitful discussions. We also thank R. N. Daskalov and M. E. J. Contreras, who made available copies of their papers.

References

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

[2] **A. Betten**, **A. Kerber**, **A. Kohnert**, **R. Laue** and **A. Wassermann**, The discovery of simple 7-designs with automorphism group $P\Gamma L(2, 32)$, *Lect. Notes Comput. Sci.* **948** (1995), 131–145.

[3] **M. Braun**, Construction of linear codes with large minimum distance, *IEEE Transactions on Information Theory* **50** (2004).

[4] **M. Braun**, **A. Kohnert** and **A. Wassermann**, Optimal linear codes from matrix groups, Submitted.

[5] **M. Braun** and **J. Sarmiento**, Parallelisms in projective geometries with a prescribed group of automorphisms, Submitted.

[6] **M. Braun**, **A. Kerber** and **R. Laue**, Systematic construction of q-analogs of designs, *Des. Codes Cryptogr.* **34** (2005), 51–66.

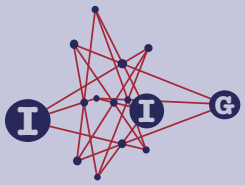
[7] **R. Daskalov**, On the existence and the nonexistence of some (k, r)-arcs in $PG(2, 17)$, in: *Proceedings of Ninth International Workshop on Algebraic and Combinatorial Coding Theory*, Kranevo, Bulgaria, June 19–25 2004 (2004), 95–100.

[8] **R. Daskalov** and **M. E. J. Contreras**, New (k, r)-arcs in the projective plane of order thirteen, *J. Geom.* **80** (2004), 10–22.

[9] **R. Daskalov** and **E. Metodieva**, New (k, r)-arcs in $PG(2, 17)$ and the related optimal linear codes, *Mathematica Balkanica, New Series* **18** (2004), 121–127.

[10] _____, New (k, r)-arcs in $PG(2, 17)$, in: *Proceedings of Ninth International Workshop on Algebraic and Combinatorial Coding Theory*, Kranevo, Bulgaria, June 19–25 2004 (2004), 107–112.

[11] **J. W. P. Hirschfeld**, *Projective Geometries over Finite Fields*, Oxford University Press, 1998.



[12] **J. W. P. Hirschfeld** and **L. Storme**, The packing problem in statistics, coding theory and finite projective spaces, Update 2001, in: *Finite Geometries*, Proceedings of the Fourth Isle of Thorns Conference, Chelwood Gate, July 16–21, 2000 (2001), 201–246.

[13] **A. Kerber**, *Applied Finite Group Actions*, Springer, 1999.

[14] **E. Kramer** and **D. Mesner**, *t-designs on hypergraphs*, *Discrete Math.* **15** (1976), 263–296.

[15] **A. Wassermann**, Finding simple t-designs with enumeration techniques, *J. Combin. Des.* **6** (1998), 79–90.

Michael Braun
MATHEMATICAL DEPARTMENT, UNIVERSITY OF BAYREUTH, D-95440 BAYREUTH, GERMANY
e-mail: michael.braun@uni-bayreuth.de
website: http://www.mathe2.uni-bayreuth.de/michael/

Axel Kohnert
MATHEMATICAL DEPARTMENT, UNIVERSITY OF BAYREUTH, D-95440 BAYREUTH, GERMANY
e-mail: axel.kohnert@uni-bayreuth.de
website: http://www.mathe2.uni-bayreuth.de/people/axel.html

Alfred Wassermann
MATHEMATICAL DEPARTMENT, UNIVERSITY OF BAYREUTH, D-95440 BAYREUTH, GERMANY
e-mail: alfred.wassermann@uni-bayreuth.de
website: http://did.mat.uni-bayreuth.de/~alfred/home/