Large Arcs in Small Planes

Awss Al-ogaidi
School of Physical and Mathematical Sciences
University of Sussex
Brighton BN1 9QH
The United Kingdom
a.al-ogaidi@sussex.ac.uk

Anton Betten
Department of Mathematics
Colorado State University
Fort Collins, CO 80523-1874, U.S.A.
betten@math.colostate.edu

February, 2019

Abstract

In a finite projective plane $\mathrm{PG}(2,q)$, a set of k points is called (k,n)-arc if the following two properties hold: Every line intersects in at most n points. There exists a line which intersects in exactly n point. We are interested in determining for each q and each n, the largest value of k for which a (k,n)-arc exists in $\mathrm{PG}(2,q)$. If possible, we would like to classify those arcs up to isomorphism. We look at the problem for $q = 11$.

CONGRESSUS NUMERANTIUM 232 (2019), pp.119-136

1 Introduction

In a finite projective plane $\mathrm{PG}(2,q)$, a set of k points is called (k,n)-arc if the following two properties hold:

(a) Every line intersects in at most n points.

(b) There exists a line which intersects in exactly n point.

Examples arise from algebraic curves of degree n. For this reason, the parameter n is called the degree of the arc. We are interested in large arcs. The largest value of k for which a (k,n)-arc in $\mathrm{PG}(s,q)$ exists is denoted

$$m_n(s,q).$$

Let S be a (k,n)-arc. Then S is **complete** if there is no larger arc containing S. Thus, $m_n(2,q)$ is the size of the largest complete arc in $\mathrm{PG}(2,q)$. The known values of $m_n(2,q)$ for small q and n are summarized in Table 1. If a value of $m_n(2,q)$ is not known, an interval is shown which contains it. Yet another related concept is that of a maximal arc. A (k,n)-arc $\mathcal{K}$ is maximal of degree n in $\mathrm{PG}(2,q)$ if $k=(q+1)(n-1)+1$. If $\mathcal{K}$ is a maximal $(k,n)-$arc in $\mathrm{PG}(2,q)$ then each line meets $\mathcal{K}$ in either 0 or n points. It is known that maximal arcs exist only when q is even. This paper is not about maximal arcs.

A collineation of $\mathrm{PG}(s,q)$ $(s \geq 2)$ is a bijective mapping from the points to the points with the property that the image of three points is collinear if and only if the points are collinear. The collineation group of $\mathrm{PG}(s,q)$ is the projective semilinear group $\mathrm{P\Gamma L}(s,q)$. An important subgroup of $\mathrm{P\Gamma L}(s,q)$ is the group of projectivities $\mathrm{PGL}(s,q)$. These are the collineations which are induced by linear maps of the underlying vector space (for $s=2$, we assume that the projective plane is Desarguesian).

Two sets S_1 and S_2 in $\mathrm{PG}(2,q)$ are equivalent if there exists a collineation α such that $S_1^\alpha = S_2$. The classification problem is the problem of determining the distinct objects of a kind in a space. For us, the classification problem is determining the distinct arcs up to equivalence.

Large arcs have been constructed by various authors. For $q = 11$, there is one example of a $(43, 5)$-arc in $\mathrm{PG}(2, 11)$ due to Ball [1]. In that same paper, the bounds $43 \leq m_5(2, 11) \leq 45$ are shown. Cook [5] studies $m_n(2, 11)$ for $n \leq 4$, and finds four isomorphism types of $(32, 4)$-arcs in $\mathrm{PG}(2, 11)$. Cook also classifies the $(21, 3)$-arcs in $\mathrm{PG}(2, 11)$: Up to isomorphism there are exactly two such arcs.

A line ℓ with $|\ell \cap \mathcal{K}| = i$ is called an i-secant. It is easy to see that a (k, n)-arc $\mathcal{K}$ in $\mathrm{PG}(2, q)$ is complete if and only if its n-secants cover the whole plane $\mathrm{PG}(2, q)$.

For a (k, n)-arc $\mathcal{K}$ in $\mathrm{PG}(2, q)$, let τ_i denotes the number of i-secants of $\mathcal{K}$. The **secant distribution** or **line type** of $\mathcal{K}$ is

$$[\tau_n, \tau_{n-1}, \cdots, \tau_2, \tau_1].$$

Let ρ_i denote the number of i-secants of $\mathcal{K}$ through a point P in $\mathcal{K}$. The **point type** of P w.r.t. $\mathcal{K}$ is the vector

$$[\rho_n, \rho_{n-1}, \cdots, \rho_2, \rho_1].$$

Lemma 1.1. *For a $(k, n)-$arc $\mathcal{K}$ in* $\mathrm{PG}(2, q)$ *the following equations hold:*

$$\sum_{i=0}^{n} \tau_i = q^2 + q + 1, \qquad (1)$$

$$\sum_{i=1}^{n} i\tau_i = k(q + 1), \qquad (2)$$

Table 1: $m_n(2,q),\ q \leq 13$

n \ q	2	3	4	5	7	8	9	11	13
2	4	4	6	6	8	10	10	12	14
3	7	9	9	11	15	15	17	21	23
4		13	16	16	22	28	28	32	38 – 40
5			21	25	29	33	37	43 – 45	49 – 53
6				31	36	42	48	56	64 – 66
7					49	49	55	67	79
8					57	64	65	78	92
9						73	81	89 – 90	105
10							91	100 – 102	118 – 119
11								121	132 – 133
12								133	145 – 147
13									169
14									183

$$\sum_{i=0}^{n}(q+1-i)\tau_i = (q^2+q+1-k)(q+1), \qquad (3)$$

$$\sum_{i=2}^{n}\binom{i}{2}\tau_i = \binom{k}{2}, \qquad (4)$$

$$\sum_{i=0}^{n}\binom{q+1-i}{2}\tau_i = \binom{q^2+q+1-k}{2}, \qquad (5)$$

$$\sum_{i=0}^{n} i(q+1-i)\tau_i = k(q^2+q+1-k). \qquad (6)$$

Table 1 shows the values of $m_n(2,q)$ for $q \leq 13$, or upper and lower bounds for it if the exact value is unknown. Regarding the problem of classification, much less is known. Table 2 shows the cases for which the largest arcs are classified. For $n = 2$, the

Table 2: Classification of largest arcs in PG$(2, q)$

n \ q	2	3	4	5	7	8
2	4 [18]	4 [18]	6 [8]	6 [18]	8 [18]	10 [8]
3	7	9	9	11 [20]	15 [12]	15 [11]
4		13	16	16	22 [10]	28
5			21	25	29	33
6				31	36	42 [4]

n \ q	9	11	13
2	10 [18]	12 [18]	14 [18]
3	17 [11]	21 [5]	23 [13]
4	28	32	$38 - 40$
5	37	$43 - 45$	$49 - 53$
6	48 [14]	56	$64 - 66$

result of Segre [18] shows that every $q+1$ arc in PG$(2, q)$, is a conic, for q. For q even, the situation is more complicated. In this case, the largest arcs are hyperovals, which consist of $q+2$ points. For $q = 2, 4, 8$, all hyperovals have the form conic plus nucleus and are unique (this fact is left as an exercise to the reader in [8]).

2 Isomorph Classification

A graph Γ is a pair (V, E) where V is a set of elements that called verticies, and E is a set of pairs of V. If $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$ are two graphs, an isomorphism from Γ_1 to Γ_2 is a bijection $\varphi : V_1 \to V_2$ such that $E_1^\varphi = E_2$. Here, $E^\varphi = \{\{x^\varphi, y^\varphi\} \mid (x, y) \in E\}$. If Γ_1 and Γ_2 are isomorphic, we write $\Gamma_1 \simeq \Gamma_2$. The set of isomorphisms of a graph Γ to itself forms a group with respect to composition. This group is known as the automorphism group of Γ. Let $\pi = (C_1, \ldots, C_k)$ be a set-partition of V. A π-isomorphism of $\Gamma_1 = (V, E_1)$ and $\Gamma_2 = (V, E_2)$ is an isomorphism $\varphi \in \mathrm{Sym}(V)$ which preserves the partition π. This means that $C^\varphi = C$ for all parts C of the partition π. We write $\Gamma_1 \simeq_\pi \Gamma_2$ if Γ_1 and Γ_2 are isomorphic under a π-preserving isomorphism.

A bipartite graph is a graph whose vertex set can be partitioned into two disjoint cocliques (sets whose elements are pairwise non-adjacent). Let $\iota = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ be an incidence structure. We can associate to ι a graph Γ_ι, called the **Levi graph** associated to ι. Γ_ι is the bipartite graph (V, E) where $V = \mathcal{P} \cup \mathcal{L}$ and E is the set of all $(\mathcal{P}, \ell)$ where $\mathcal{P} \in \ell$ holds in ι. Given a set of points S with $S \subseteq P$, the **extended Levi graph** $\Gamma_{\iota,S}$ is defined as

$$\Gamma_{\iota,S} = (V^*, E^*),$$

where

$$V^* = \mathcal{P} \cup \mathcal{L} \cup \{p_*, \ell_*\},$$

with incidences of the form

1. (p, ℓ) where $p \in \mathcal{P}, \ell \in \mathcal{L}, p \in \ell$,
2. (p, ℓ_*) where $p \in S$,
3. (p_*, ℓ_*).

Let $\mathcal{G}(V)$ be the set of graphs whose vertex set is V. A map $\mathcal{C} : \mathcal{G}(V) \to \mathrm{Sym}(V)$ is called a **canonical labeling map** if the following property holds:

$$\Gamma_1 \simeq \Gamma_2 \iff \Gamma_1^{\mathcal{C}(\Gamma_1)} = \Gamma_2^{\mathcal{C}(\Gamma_2)} \quad \forall \Gamma_1, \Gamma_2 \in \mathcal{G}(V). \tag{7}$$

Let $\pi = (C_1, \ldots, C_k)$ be a set-partition of V. A π-preserving canonical labeling map on $\mathcal{G}(V)$ is a map $\mathcal{C} : \mathcal{G}(V) \to \mathrm{Sym}(V; \pi)$ such that

$$\Gamma_1 \simeq_\pi \Gamma_2 \iff \Gamma_1^{\mathcal{C}(\Gamma_1)} = \Gamma_2^{\mathcal{C}(\Gamma_2)} \quad \forall \Gamma_1, \Gamma_2 \in \mathcal{G}(V). \tag{8}$$

Here, $\mathrm{Sym}(V;\pi)$ is the stabilizer of the partition π in $\mathrm{Sym}(V)$. That is, $f \in \mathrm{Sym}(V;\pi)$ if $f \in \mathrm{Sym}(V)$ and $C^f = C$ for each class $C \in \pi$. For Levi graphs, the partition $\pi = (V, \mathcal{L})$ is important. For extended Levi graphs, the partition

$$\pi = (\mathcal{P}, \mathcal{L}, \{p_*\}, \{\ell_*\}) \tag{9}$$

is important. We have the following results:

Theorem 2.1. *1. Let $\iota_1 = (\mathcal{P}, \mathcal{L}, \mathcal{I}_1)$ and $\iota_2 = (\mathcal{P}, \mathcal{L}, \mathcal{I}_2)$ be two incidence structures. Then*

$$\iota_1 \simeq \iota_2 \iff \Gamma_{\iota_1}^{\mathcal{C}(\Gamma_{\iota_1})} = \Gamma_{\iota_2}^{\mathcal{C}(\Gamma_{\iota_2})}.$$

2. Let S and T be to subsets of $\mathcal{P}$. Let π be the partition of the Levi graph from (9). Let $\mathcal{C}_\pi$ be a π-preserving canonical labeling map. Then

$$S \simeq T \iff \Gamma_{\iota,S}^{\mathcal{C}_\pi(\Gamma_{\iota,S})} = \Gamma_{\iota,T}^{\mathcal{C}_\pi(\Gamma_{\iota,T})}$$

A few remarks on canonical labeling mappings are in order. It is very simple to define a canonical labeling mapping. For instance, the labeling which takes the graph to the lex-least form of the adjacency matrix is one such mapping. However, the real difficulty is to make an algorithmic procedure which computes the canonical labeling of a graph in reasonable time. In order to be able to do this, the lex-least form is often not the best choice. For instance, the program Nauty [16] computes a canonical labeling of graphs which is different from the lex-least mapping. Using Theorem 2.1, it is possible to use Nauty to classify objects in finite projective spaces: Simply consider the incidence structure ι given by the points and lines of the projective space. This also works well for other incidence structures, such as non-desarguesian projective planes. However, the order of the geometry is restricted, as computing the canonical labeling is slow, even for efficient implementations such as Nauty.

3 Poset Classification

A large number of combinatorial problems involving classification can be reduced to classifying orbits of groups acting on partially ordered sets. The partially ordered set that we consider is the set of points in the plane which satisfy the condition that each line intersects in at most n points.

There are many different ways in which such a classification can be performed. First, there is the technique of **canonical augmentation,** developed by McKay [15]. It relies on the notion of canonical labelings. At present, the only implementation available is McKay's own Nauty [16].

The scarcity of canonical form algorithms and implementations leads us to look for different approaches. One alternative is an algorithm for poset-classification originally due to Schmalz [17]. For a modernized version, see [3]. The algorithm is available for many different posets, and an implementation in the software package Orbiter [2] can be used.

4 Arcs of degree 3 in PG(2, 11)

Cook [5] classifies the arcs of degree 3 in PG(2, 11). Because we are interested in n-arcs in PG(2, 11) with $n > 3$, this result will be important for our work. We start by verifying this result using different techniques. Using Orbiter [2], we confirm the numbers in the third column of Table 3. This table was first established in [5]. In the table, Aut stands for the order of the automorphism group, Line type is the vector

$$[3^{\tau_3}, 2^{\tau_2}, 1^{\tau_1}, 0^{\tau_0}],$$

and point types are of the form

$$[3^{\rho_3}, 2^{\rho_2}, 1^{\rho_1}].$$

Table 3: Number of $(k,3)$-arcs in PG$(2,11)$ up to isomorphism

k	complete	incomplete	total
12	0	15,291,641	15291641
13	5	44,020,755	44,020,760
14	146	76,935,881	76,936,027
15	715,84,677	73086254	73,157,838
16	1,573,677	31,342,655	32,916,332
17	2,082,781	3801624	5,884,405
18	259,585	742,73	333,858
19	4,176	291	4,467
20	15	2	17
21	2	0	2

Table 4: Classification of $(21,3)$-arcs in PG$(2,11)$

# of Arcs	Aut	Line types	Point types
2	$C_7 \rtimes C_3$	$[3^{63}, 2^{21}, 1^{21}, 0^{28}]$	21 $[3^9, 2^2, 1^1]$

Cook finds exactly two isomorphism types of $(21,3)$-arcs in PG$(2,11)$. These are the largest arcs of degree 3 in this plane. For more information on these arcs, see Table 4. Interestingly, the largest 3-arcs that we get from curves are elliptic curves whose number of points reaches the Hasse-Weil upper bound:

$$\#\text{pts. over } \mathbf{F}_q \leq q + 1 + 2\sqrt{q}$$

Up to isomorphism, there are exactly two curves for which the number of points is 18, which is the value of the Hasse-Weil bound for $q = 11$ (cf. Table 5). The equation of the first curve is

$$\begin{gathered} 5X_0^2X_1 + 10X_0^2X_2 + 6X_0X_1^2 + \\ 10X_1^2X_2 + X_0X_2^2 + 2X_1X_2^2 + 10X_0X_1X_2 = 0. \end{gathered} \tag{10}$$

Table 5: Elliptic curves in PG(2, 11)

Equation	# of pts	Ago	Line type
(10)	18	3	3^{18}, 2^{12}, 1^{66}, 0^{37}
(11)	18	6	3^{46}, 2^{15}, 1^{48}, 0^{24}

The equation of the second curve is

$$\begin{gathered} 7X_0^2X_1 + 8X_0^2X_2 + 4X_0X_1^2 + \\ 8X_1^2X_2 + 3X_0X_2^2 + 4X_1X_2^2 + 10X_0X_1X_2 = 0. \end{gathered} \tag{11}$$

The curves were found using a classification algorithm for cubic curves in small projective planes developed by the authors. The software package Orbiter [2] was used. The internet table *Manypoints* [7] can be used to query the largest algebraic curves over small finite fields, and to find out references for the curves. For instance, elliptic curves with 18 points in PG(2, 11) have been found by [19], and earlier work was done by Hasse [9] and Deuring [6]. Soomro lists the curve with equation $y^2 = x^3 + x + 3$, which is equivalent to the curve with automorphism group of order 6 in Table 5.

5 Arcs of degree 4 in PG(2, 11)

The largest arcs of degree 4 in PG(2, 11) have 32 points. Here is the classification of these arcs:

Theorem 5.1. *Up to isomorphism, there are exactly* 210,692 *largest complete* (32, 4)*-arcs in* PG(2, 11)*. Information is given in Table 6 and 7.*

Cook [5] proves that to extend an $(s, 3)$–arc to a $(33, 4)$-arc in PG(2, 11), then $s \geq 12$. Cook [5] finds one arc in each

Table 6: (32, 4)-arcs in PG(2, 11)

# Arcs	Aut	Line types	t_1	t_2	t_3	t_4	t_5
26945	D_{20}	$[4^{65}, 3^{30}, 2^{16}, 1^{2}, 0^{20}]$	2	0	10	10	10
34517	D_{20}	$[4^{75}, 3^{10}, 2^{16}, 1^{22}, 0^{10}]$	12	10	10	0	0
70078	C_{10}	$[4^{75}, 3^{10}, 2^{16}, 1^{22}, 0^{10}]$	12	10	10	0	0
79152	D_8	$[4^{71}, 3^{20}, 2^{10}, 1^{20}, 0^{12}]$	8	12	0	12	0

Table 7: Point types

Notation	Point types
t_1	$[4^{10}, 3^{0}, 2^{1}, 1^{1}]$
t_2	$[4^{9}, 3^{2}, 2^{0}, 1^{1}]$
t_3	$[4^{9}, 3^{1}, 2^{2}, 1^{0}]$
t_4	$[4^{8}, 3^{3}, 2^{1}, 1^{0}]$
t_5	$[4^{7}, 3^{5}, 2^{0}, 1^{0}]$

line of Table 6. Our result is based on lifting all isomorphism types of $(s, 3)$-arcs (complete and incomplete) from Table 3 for $12 \leq s \leq 21$. Parallel computing was used to perform this computation. The lifting of each arc is done by solving systems of Diophantine equations. The isomorph classification is done using Orbiter, which in turn relies on Nauty. The method of Levi graphs described in Section 2 is used.

6 Arcs of degree 5 in PG(2, 11)

It is possible to increase the degree of an arc by adding points. The conditions for adding points can be expressed using Diophantine equations and inequalities. Suppose we want to extend the degree d of an arc by one. A d-secant can accept at most on new point. In general, a $d-i$ secant can accept $i+1$ new points. For each line in the plane, one inequality is formed. Suppose we start from a (k, d)-arc and we wish to construct an $(s, d+1)$-arc for some $s > k$. The variables in the system are the points off the (k, d)-arc. One additional equation captures the fact that we want to add $s - k$ points. Consider an example. To construct a $(43, 5)$-arc we try extending one of the $(32, 4)$-arcs from Table 6. The first of these arcs (due to Cook) can indeed be extended. The Diophantine system is shown in Table 8. The new $(43, 5)$-arc has a stabiliser group of order 10. Table 9 summarizes the known $(43, 5)$-arcs in $\mathrm{PG}(2, 11)$. So far, no $(44, 5)$-arc or $(45, 4)$-arc in known, but they have not been ruled out either. The following theorem gives information about a putative $(45, 5)$-arc:

Theorem 6.1. *In* $\mathrm{PG}(2, 11)$, *the number of* 5*-secants of a* $(45, 5)$*-arc satisfies the following bound:*

$$\tau_5 \geq 72.$$

Proof: We consider the column-tactical decomposition scheme of the incidence matrix of $\mathrm{PG}(2, 11)$:

$\downarrow$	τ_5	τ_4	τ_3	τ_2	τ_1	τ_0
45	5	4	3	2	1	0
88	7	8	9	10	11	12

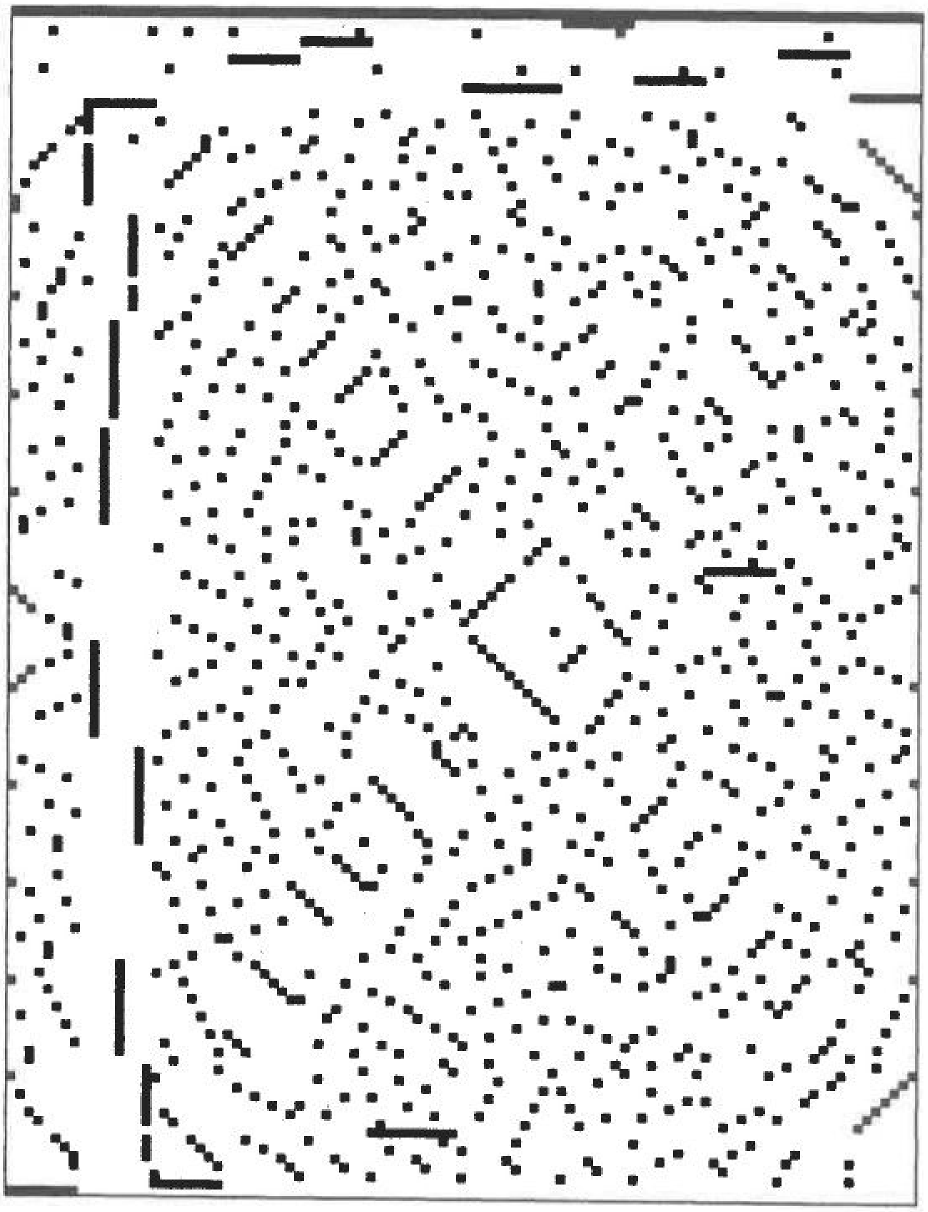

Table 8: The system for extending to (43, 5)-arcs

Table 9: Known (43, 5)-arcs in PG(2, 11)

	Ago	Lines type
Ball arc	12	$[5^{63}, 4^{42}, 3^{3}, 2^{12}, 0^{13}]$
New arc	10	$[5^{60}, 4^{45}, 3^{10}, 2^{3}, 0^{15}]$

The equations from Lemma 1.1 are:

$$\sum_{j=0}^{5} \binom{j}{2} \tau_j = \binom{45}{2} \quad J_1$$

$$\sum_{j=0}^{5} \binom{12-j}{2} \tau_j = \binom{88}{2} \quad J_2$$

$$\sum_{j=0}^{5} j(12-j)\tau_j = 45 \cdot 88 \quad J_{1,2}$$

$$\sum_{j=0}^{5} j\tau_j = 45 \cdot 12 \quad F_1$$

$$\sum_{j=0}^{5} (12-j)\tau_j = 88 \cdot 12 \quad F_2$$

$$\sum_{j=0}^{5} \tau_j = 133 \quad C$$

So,

τ_5	τ_4	τ_3	τ_2	τ_1	τ_0	= RHS
10	6	3	1	0	0	990
21	28	36	45	55	66	3828
35	32	27	20	11	0	3928
5	4	3	2	1	0	540
7	8	9	10	11	12	1056
1	1	1	1	1	1	133

To show that $\tau_5 \geq 72$, we assume $\tau_5 \leq 71$ and show that the system has no solution. Considering the second row, we deduce that $\tau_3 \leq 106$, $\tau_2 \leq 85$, $\tau_1 \leq 69$, and $\tau_0 \leq 58$. Elementary row operations lead to

τ_5	τ_4	τ_3	τ_2	τ_1	τ_0	= RHS
10	6	3	1	0	0	990
0	1	6	15	28	45	765
0	10	15	15	10	0	450
5	4	3	2	1	0	540
0	2	4	6	8	10	250
1	1	1	1	1	1	133

Considering the second row, we deduce that $\tau_0 \leq 17$. This leaves 18 cases to consider for τ_0. We perform a case-by-case analysis. Each case is similar, so we only look at one of the cases: $\tau_0 = 0$ (the hardest case). The general idea is to make lower and upper bounds for τ_j say

$$l_j \leq \tau_j \leq u_j.$$

Let $a_{i,j}$ be the (i, j) entry in the reduced coefficient matrix. If at some point

$$\sum_{j=0}^{5} a_{i,j} u_j < \mathrm{RHS}_i$$

for some equation i, then we know the system has no solution (the stopping rule). It remains to tighten the bounds l_j and u_j. The following to observations are helpful:

1. For all (i, j) we have

$$u_j \leq \left\lfloor \frac{\mathrm{RHS}_i - \sum_{\substack{h=0 \\ h \neq j}}^{5} a_{i,h} l_h}{a_{i,j}} \right\rfloor$$

2. For all (i, j) we have

$$l_j \geq \left\lceil \frac{\mathrm{RHS}_i - \sum_{\substack{h=0 \\ h \neq j}}^{5} a_{i,h} u_h}{a_{i,j}} \right\rceil$$

Table 10: Sharpening of bounds in the proof of Theorem 6.1

Eqn	τ_5	τ_4	τ_3	τ_2	τ_1	τ_0
	$0-71$	$0-123$	$0-106$	$0-85$	$0-69$	0
1	$0-71$	$0-123$	$0-106$	$0-51$	$0-27$	0
2	$0-71$	$0-45$	$0-30$	$0-30$	$0-27$	0
3	$37-71$	$2-45$	$0-30$	$0-30$	$0-27$	0
0	$60-71$	$27-45$	$0-30$	$0-30$	$0-27$	0
1	$60-71$	$27-45$	$0-30$	$0-30$	$4-26$	0
2	$60-71$	$27-41$	$0-9$	$0-9$	$4-18$	0
3	$63-71$	$31-41$	$0-9$	$0-9$	$4-18$	0
4	$63-71$	$31-41$	$0-9$	$0-9$	$10-18$	0
0	$71-71$	$41-41$	$9-9$	$7-9$	$10-18$	0

We consider all pairs (i, j) and tighten the bounds using the two observations. If an improvement is made, all pairs (i, j) are tested again. This is repeated until either there are no more improvements, or for one equation i the stopping rule is reached. For $\tau_0 = 0$, this leads to the bounds shown in Table 10. Recall:

	τ_5	τ_4	τ_3	τ_2	τ_1	τ_0	= RHS
$a_{1,j}$	0	1	6	15	28	45	765

and

τ_5	τ_4	τ_3	τ_2	τ_1	τ_0
$71-71$	$41-41$	$9-9$	$7-9$	$10-18$	0

At this point, the stopping rule is reached in equation $i = 1$:

$$\sum_{j=0}^{5} a_{i,j} u_j = 0 \cdot 71 + 1 \cdot 41 + 6 \cdot 9 + 15 \cdot 9 + 28 \cdot 18 + 45 \cdot 0 = 734 < 765$$

This means that the case $\tau_5 \leq 71$ and $\tau_0 = 0$ is ruled out. The other cases of τ_0 are dealt with in a similar fashion. This shows that $\tau_5 \geq 72$.

References

[1] Simeon Ball. Multiple blocking sets and arcs in finite planes. *J. London Math. Soc. (2)*, 54(3):581–593, 1996.

[2] Anton Betten. Orbiter – A program to classify discrete objects, 2018,
https://github.com/abetten/orbiter.

[3] Anton Betten. Poset classification and optimal linear codes. Submitted.

[4] Anton Betten, Eun Ju Cheon, Seon Jeong Kim, and Tatsuya Maruta. The classification of $(42,6)_8$ arcs. *Adv. Math. Commun.*, 5(2):209–223, 2011.

[5] G. R. Cook. Arcs in a Finite Projective Plane, Ph.D. thesis, University of Sussex, 2011.

[6] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[7] Gerard van der Geer, Everett W. Howe, Kristin E. Lauter, and Christophe Ritzenthaler. Tables of curves with many points, 2009. Retrieved 11/14/2019.

[8] Marshall Hall, Jr. Ovals in the Desarguesian plane of order 16. *Ann. Mat. Pura Appl. (4)*, 102:159–176, 1975.

[9] Helmut Hasse. Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung. *J. Reine Angew. Math.*, 175:193–208, 1936.

[10] Ray Hill and Chris P. Love. On the $(22,4)$-arcs in $\mathrm{PG}(2,7)$ and related codes. *Discrete Math.*, 266(1-3):253–261, 2003. The 18th British Combinatorial Conference (Brighton, 2001).

[11] Stefano Marcugini, Alfredo Milani, and Fernanda Pambianco. Classification of the $[n, 3, n-3]_q$ NMDS codes over GF(7), GF(8) and GF(9). *Ars Combin.*, 61:263–269, 2001.

[12] Stefano Marcugini, Alfredo Milani, and Fernanda Pambianco. Classification of the $(n, 3)$-arcs in PG$(2, 7)$. *J. Geom.*, 80(1-2):179–184, 2004.

[13] Stefano Marcugini, Alfredo Milani, and Fernanda Pambianco. Maximal $(n, 3)$-arcs in PG$(2, 13)$. *Discrete Math.*, 294(1-2):139–145, 2005.

[14] Tatsuya Maruta, Ayako Kikui, and Yuri Yoshida. On the uniqueness of $(48, 6)$-arcs in PG$(2, 9)$. *Adv. Math. Commun.*, 3(1):29–34, 2009.

[15] Brendan D. McKay. Isomorph-free exhaustive generation. *J. Algorithms*, 26(2):306–324, 1998.

[16] Nauty User's Guide (Version 2.6), Brendan McKay, Australian National University, 2016.

[17] Bernd Schmalz. Verwendung von Untergruppenleitern zur Bestimmung von Doppelnebenklassen. *Bayreuth. Math. Schr.*, (31):109–143, 1990.

[18] Beniamino Segre. Ovals in a finite projective plane. *Canad. J. Math.*, 7:414–416, 1955.

[19] Muhammed Afsal Soomro. Algebraic curves over finite fields, Thesis, University of Groningen, 2013.

[20] M. O. Yazdi. The Classification of $(k; 3)$-arcs over the Galois Field of Order Five, Ph.D. thesis, University of Sussex, 1983.