The Classification of $(42, 6)_8$-Arcs

Anton Betten[1], Eun-Ju Cheon[2],
Seon Jeong Kim[2], Tatsuya Maruta[3]

[1]Colorado State University, U.S.A.
[2]Geongsang National University, South Korea
[3]Osaka Prefecture University, Japan

April 2010

(Some) Finite Geometry:

Let q be a prime power, $q = p^h$, with p prime.

A nondegenerate conic in $\mathrm{PG}(2, q)$

EXAMPLE:

$$Y^2 = XZ$$

The $q + 1$ points are parametrized as

- $(t^2, t, 1)$ $(t \in \mathbb{F}_q)$ together with
- $(1, 0, 0)$.

Properties of Conics

- A large automorphism group:

$$\mathrm{P\Gamma L}(2,q) \;\text{ embedded in }\; \mathrm{P\Gamma O}(3,q)$$

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix}_i \to \begin{bmatrix} a^2 & ac & c^2 \\ 2ab & ad+bc & 2cd \\ b^2 & bd & d^2 \end{bmatrix}_i$$

Order: $h(q+1)q(q-1)$

- Any line intersects in at most 2 points.

Arcs

Definition: $A \subseteq \mathrm{PG}(2, q)$ is $(n, s)_q$-arc if

- $|A| = n$,
- no $s + 1$ points of A are collinear,
- some s points of A are collinear.

Equivalent Objects:

- $(n, s)_q$ arcs
- $[n, 3, n - s]_q$ linear codes (projective)
- $\{q^2 + q + 1 - n, q + 1 - s; 2, q\}$ minihyper (without multiplicities)

Arcs

EXAMPLES:

Conics are $(q+1,2)_q$-arcs (a.k.a. ovals)

If q is even, conics together with their nucleus are $(q+2,2)_q$-arcs (a.k.a. hyperovals)

Arcs

An $(n, s)_q$ arc is largest
if there is no $(n+1, s)_q$-arc.

Q: Given s and q, what is the largest n for which an $(n, s)_q$ arc exists?

A: It depends, but for

- $s = 2$ and q odd, the answer is $q + 1$ (i.e., ovals).
- $s = 2$ and q even, the answer is $q + 2$ (i.e., hyperovals).
- $s = 6$ and $q = 8$, the answer is 42.

Arcs

Q: Can we classify all arcs?

A: Sometimes, but we first need to discuss projective equivalence.

Symmetry in $\mathrm{PG}(k-1, q)$

THEOREM:

$$\mathrm{Aut}(\mathrm{PG}(k-1, q)) = \mathrm{P\Gamma L}(k, q)$$

Q: What is $\mathrm{P\Gamma L}(k, q)$?

Symmetry in $\mathrm{PG}(k-1, q)$

$\mathrm{PGL}(k, q)$ is the group of linear automorphisms of $\mathrm{PG}(k-1, q)$.

$$|\mathrm{PGL}(k, q)| = q^{k(k-1)/2} \prod_{i=2}^{k} (q^i - 1)$$

EXAMPLE:

$$|\mathrm{PGL}(2, q)| = q(q^2 - 1) = (q+1)q(q-1)$$

Symmetry in $\mathrm{PG}(k-1, q)$

Semilinear maps:

Write $q = p^h$ with p prime

Let $\phi : x \mapsto x^p$ be the Frobenius automorphism of $\mathbb{F}_q$

$$(x_0, \ldots, x_k)^\phi := (x_0^\phi, \ldots, x_k^\phi)$$

induces an automorphism of $\mathrm{PG}(k-1, q)$.

Symmetry in $\mathrm{PG}(k-1, q)$

A semilinear map of $\mathrm{PG}(k-1, q)$
is the map induced by

$$\mathbf{x} \mapsto (\mathbf{x}A)^{\phi^i}$$

where

$$A \in \mathrm{GL}(k, q), \quad i \in \mathbb{Z}_h.$$

Symmetry in $\mathrm{PG}(k-1, q)$

$\mathrm{P\Gamma L}(k, q)$ is the group of all semilinear automorphisms of $\mathrm{PG}(k-1, q)$.

Write A_i for the semilinear map induded by (A, i).

Composition rule for semilinear maps:

$$A_i \cdot B_j = C_k \quad \text{where} \quad C = A \cdot B^{\phi^{-i}}, \text{ and } k = i + j \bmod h.$$

EXAMPLE: $|\mathrm{P\Gamma L}(2, q)| = h(q+1)q(q-1)$

Classification of Arcs: $s = 2$

Segre

For q odd, all ovals are conics.

For q even, not every hyperoval is of the form "conic $+$ nucleus" (a.k.a. regular).

EXAMPLE: Lunelli/Sce when $q = 16$.

Can be written as the symmetric difference of two cubics (Glynn).

Classification of Arcs: $s > 2$

Q: Can we classify all $(42, 6)_8$-arcs?

A: For $(n, s)_q = (42, 6)_8$, one arc is due to Mason 1984.

For the complete classification, see below...

Observe that $\mathrm{P\Gamma L}(3, 8)$ is a group of order 49448448.

Notation

$$(\mathcal{V}, \mathcal{B}) = \mathrm{PG}(2, 8)$$

Let A be an $(42, 6)_8$-arc.

$$B = \mathcal{V} \setminus A$$

$$(P) = \{l \in \mathcal{B} \mid P \in l\}$$

the pencil of lines through the point P.

Notation

A line l is called i-line if $|A \cap l| = i$. So, $i \leq 6$.

$\mathcal{L}_i$ the set of i-lines

$$a_i = |\mathcal{L}_i|$$

$(a_0, a_1, \ldots, a_6)$ the *line type*

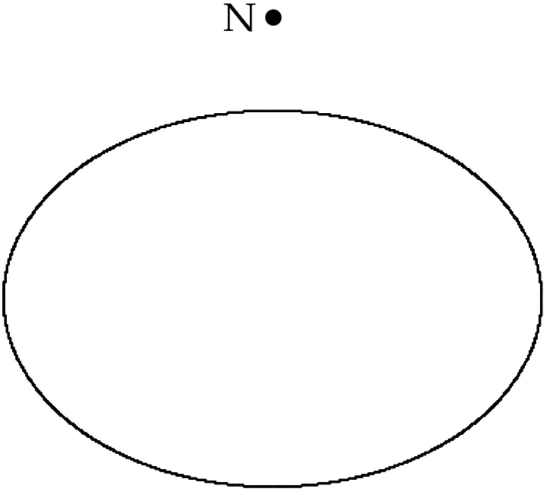
Exponential notation: i^{a_i}

THEOREM

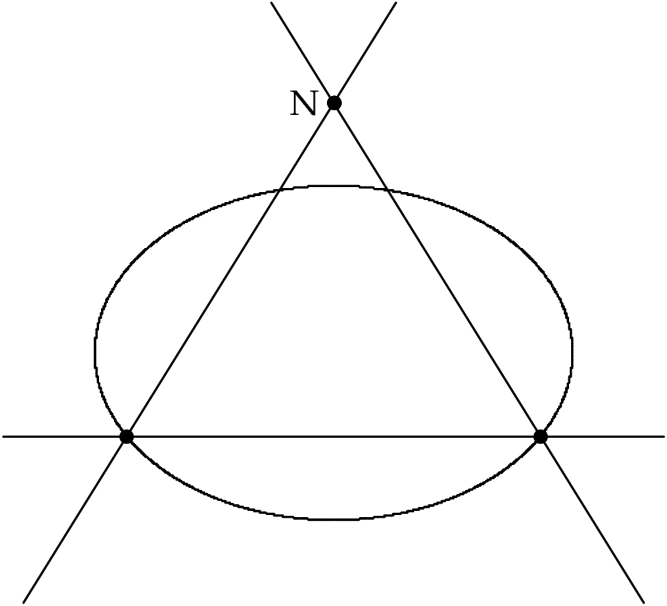
There are five $(42, 6)_8$-arcs, with groups of order $42, 18, 72, 63, 2$. They are...

The constructions will show the complement of the arc.

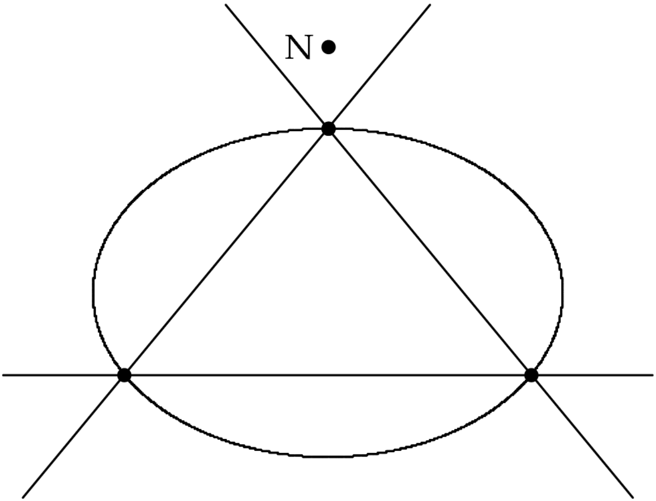
Take a hyperoval in $\mathrm{PG}(2,8)$:
group order $9 \cdot 8 \cdot 7 \cdot 3$



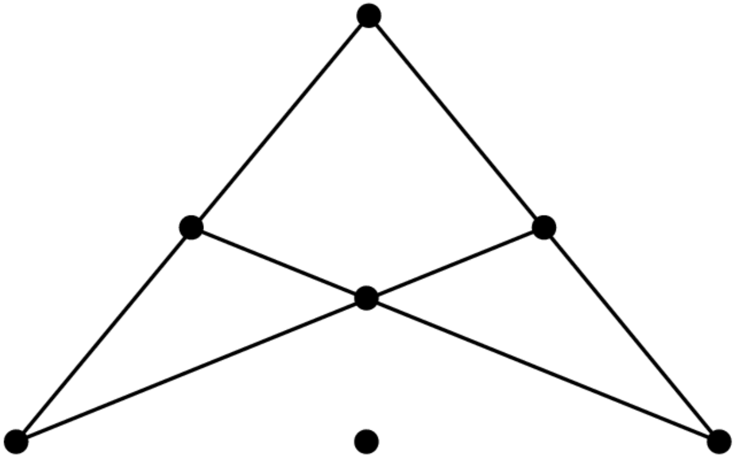
Arc I (Mason arc): group order $7 \cdot 2 \cdot 3 = 42$



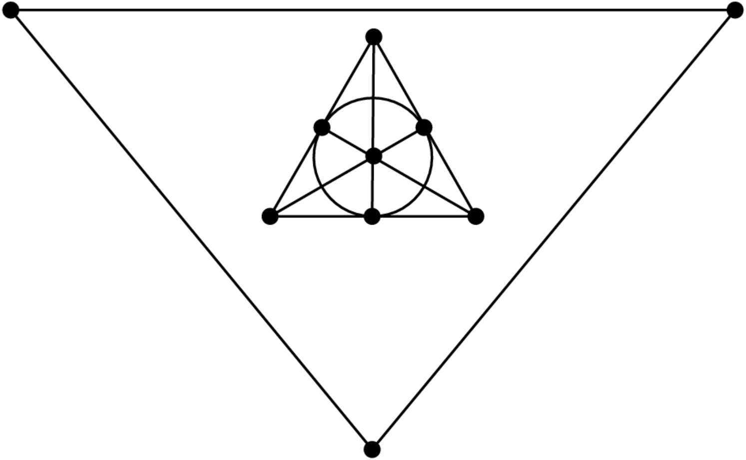
Arc II: group order $3 \cdot 6 = 18$



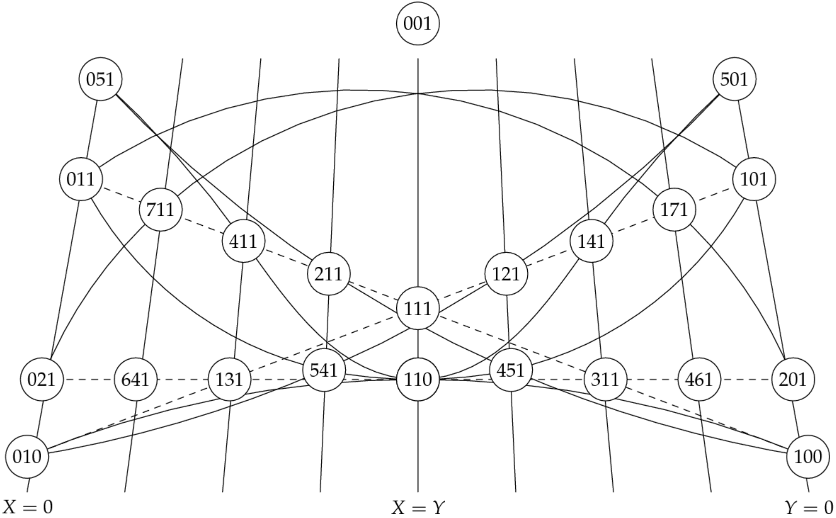
Arc III: group order $\frac{168 \cdot 3}{7} = 72$

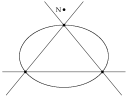
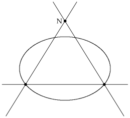
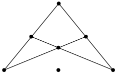
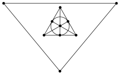
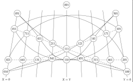


Arc IV: group order 63



Arc V: group order 2



$\lvert \mathrm{Aut} \rvert$	Arc	
18	I	
42	II	
72	III	
63	IV	
2	V	

Lemma 1

An $(n, s)_q$-arc satisfies

$$\sum_{i=0}^{s} a_i = q^2 + q + 1, \sum_{i=1}^{s} i a_i = (q+1)n, \sum_{i=2}^{s} \binom{i}{2} a_i = \binom{n}{2},$$

This leads to 330 cases of line types.

Lemma 2

$$a_1 = 0$$

This reduces the number of cases to 111.

Point Types

For a point P, let

$$c_i = |(P) \cap \mathcal{L}_i|$$

The point type is $(c_0, \ldots, c_6)$, often written as $6^{c_6} \cdots 0^{c_0}$

Let $\mathbf{p}_i$ be the point types for points in A.

Let $\mathbf{q}_i$ be the point types for points in B.

Point Types

Lemma 3

The $\mathbf{p}_i$ are determined by

$$\sum_{i=2}^{6}(i-1)c_i = 41, \quad \sum_{i=0}^{6} c_i = 9$$

Lemma 4

The $\mathbf{q}_i$ are determined by

$$\sum_{i=0}^{6}(9-i-1)c_i = 30, \quad \sum_{i=0}^{6} c_i = 9$$

Point Types

There are 5 $\mathbf{p}_i$ and 40 $\mathbf{q}_i$

Observe: the only point type $\mathbf{q}_i$ with at least two 0-lines is $\mathbf{q}_1 = 6^7, 0^2$

Thus:

- No three 0-lines are concurrent (the 0-lines form an arc with $s = 2$ in the dual plane).
- For $2 \leq w < 6$, a w-line intersects a 0-line in a point not on another 0-line

Q: How many points of type $\mathbf{p}_i$, $\mathbf{q}_i$ are there?

Define

$$x_i = \text{the number of points of type } \mathbf{p}_i$$

$$y_i = \text{the number of points of type } \mathbf{q}_i$$

Write $s_{i,j}$ for the c_j in points of type $\mathbf{p}_i$

Write $t_{i,j}$ for the c_j in points of type $\mathbf{q}_i$

The x_i and y_i satisfy the following equations:

Lemma 7

$$\sum_{i=1}^{5} x_i = 42 \qquad (F_1), \qquad \sum_{i=1}^{40} y_i = 31 \qquad (F_2)$$

$$\sum_{i=1}^{5} x_i s_{i,j} = j a_j \qquad (F_{1,j}), \qquad \sum_{i=1}^{40} y_i t_{i,j} = (9-j) a_j \qquad (F_{2,j})$$

$$\sum_{i=1}^{5} x_i \binom{s_{i,j}}{2} + \sum_{i=1}^{40} y_i \binom{t_{i,j}}{2} = \binom{a_j}{2} \qquad (J_j)$$

$$\sum_{i=1}^{5} x_i s_{i,j_1} s_{i,j_2} + \sum_{i=1}^{40} y_i t_{i,j_1} t_{i,j_2} = a_{j_1} a_{j_2} \qquad (J_{j_1,j_2})$$

for $j, j_1, j_2 \in \{0, \ldots, 6\}$ with $j_1 \neq j_2$.

If Lemma 7 has no solution, that case can be ruled out.

This reduces the number of cases to 27.

EXAMPLE: Case 72

Example: Case 72 is the following column tactical decomposition:

		$\mathcal{L}_6$	$\mathcal{L}_4$	$\mathcal{L}_2$	$\mathcal{L}_0$
	$\downarrow$	50	18	3	2
A	42	6	4	2	0
B	31	3	5	7	9

Lemma 3 and 4: We find 2 point types $\mathbf{p}_i$ and 7 point types $\mathbf{q}_i$.

Lemma 7 amounts to solving the following system:

x_1	x_2	y_1	y_2	y_3	y_4	y_5	y_6	y_7		
8	7	0	0	0	0	0	0	0	$= 300$	$F_{1,1}$
0	2	0	0	0	0	0	0	0	$= 72$	$F_{2,1}$
1	0	0	0	0	0	0	0	0	$= 6$	$F_{3,1}$
1	1	0	0	0	0	0	0	0	$= 42$	F_1
0	0	7	6	6	5	5	4	3	$= 150$	$F_{1,2}$
0	0	0	1	0	3	2	4	6	$= 90$	$F_{2,2}$
0	0	0	1	3	0	2	1	0	$= 21$	$F_{3,2}$
0	0	2	1	0	1	0	0	0	$= 18$	$F_{4,2}$
0	0	1	1	1	1	1	1	1	$= 31$	F_2
28	21	21	15	15	10	10	6	3	$= 1225$	J_1
0	1	0	0	0	3	1	6	15	$= 153$	J_2
0	0	0	0	3	0	1	0	0	$= 3$	J_3
0	0	1	0	0	0	0	0	0	$= 1$	J_4
0	14	0	6	0	15	10	16	18	$= 900$	$J_{1,2}$
8	0	0	6	18	0	10	4	0	$= 150$	$J_{1,3}$
0	0	14	6	0	5	0	0	0	$= 100$	$J_{1,4}$
0	0	0	1	0	0	4	4	0	$= 54$	$J_{2,3}$
0	0	0	1	0	3	0	0	0	$= 36$	$J_{2,4}$
0	0	0	1	0	0	0	0	0	$= 6$	$J_{3,4}$

The Parameters

We find two solutions. They correspond to the following two row-tactical refinements:

Case.72.1

	$\mathcal{L}_6$	$\mathcal{L}_4$	$\mathcal{L}_2$	$\mathcal{L}_0$
$\rightarrow$	50	18	3	2
6	8	0	1	0
36	7	2	0	0
1	7	0	0	2
6	6	1	1	1
1	6	0	3	0
10	5	3	0	1
12	4	4	1	0
1	3	6	0	0

2-lines concurrent

Case.72.2

	$\mathcal{L}_6$	$\mathcal{L}_4$	$\mathcal{L}_2$	$\mathcal{L}_0$
$\rightarrow$	50	18	3	2
6	8	0	1	0
36	7	2	0	0
1	7	0	0	2
6	6	1	1	1
10	5	3	0	1
3	5	2	2	0
9	4	4	1	0
2	3	6	0	0

2-lines form a triangle

The Johnson bound for Tactical Decompositions

$(\mathfrak{V}, \mathfrak{B})$ a row-tactical decomposition

$$
\begin{array}{cc|cccc}
 & & B_1 & B_2 & \cdots & B_n \\
 & \rightarrow & b_1 & b_2 & \cdots & b_n \\
\hline
V_1 & v_1 & r_{11} & r_{12} & \cdots & r_{1n} \\
V_2 & v_2 & r_{21} & r_{22} & \cdots & r_{2n} \\
\vdots & \vdots & \vdots & & & \vdots \\
V_m & v_m & r_{m1} & r_{m2} & \cdots & r_{mn}
\end{array}
$$

Here, $\mathfrak{V} = (V_1, \ldots, V_m)$ and $\mathfrak{B} = (B_1, \ldots, B_n)$.

The Johnson bound for Tactical Decompositions

Lemma 8 (BB 2010)

Let $1 \leq i_1 < i_2 < \cdots < i_s \leq m$. Assume that

$$\sum_{j=1}^{n} \left\{ e_j \binom{f_j + 1}{2} + (b_j - e_j) \binom{f_j}{2} \right\} > \binom{\sum_{u=1}^{s} v_{i_u}}{2}$$

where f_j and e_j are determined by

$$\sum_{u=1}^{s} r_{i_u, j} v_{i_u} = f_j b_j + e_j \quad 0 \leq e_j < b_j.$$

Then the decomposition scheme is not realizable.

This reduces the number of cases to 25.

Case	a_6	a_5	a_4	a_3	a_2	a_1	a_0	Lem 7	Lem 8	Comment
15	52	0	12	0	9	0	0	2	2	
37	49	8	3	8	4	0	1	23	15	
41	49	7	6	5	5	0	1	11	11	
44	51	0	15	0	6	0	1	2	2	
59	48	9	3	11	0	0	2	2	0	ruled out
63	48	8	6	8	1	0	2	21	0	ruled out
64	47	11	3	9	1	0	2	16	12	
68	48	7	9	5	2	0	2	32	18	
69	47	10	6	6	2	0	2	1351	1060	
70	46	13	3	7	2	0	2	13	9	
72	50	0	18	0	3	0	2	2	2	Arc V
75	47	9	9	3	3	0	2	197	196	
76	46	12	6	4	3	0	2	2139	1338	
77	45	15	3	5	3	0	2	2	2	
80	46	11	9	1	4	0	2	62	53	
81	45	14	6	2	4	0	2	112	80	

Case	a_6	a_5	a_4	a_3	a_2	a_1	a_0	Lem 7	Lem 8	Comment
88	49	0	21	0	0	0	3	1	1	Arcs I & II
91	46	9	12	3	0	0	3	8	1	
92	45	12	9	4	0	0	3	214	32	
93	44	15	6	5	0	0	3	188	11	
94	43	18	3	6	0	0	3	4	2	
95	42	21	0	7	0	0	3	1	1	Arc IV
97	45	11	12	1	1	0	3	33	3	
98	44	14	9	2	1	0	3	447	12	
99	43	17	6	3	1	0	3	77	8	
102	43	16	9	0	2	0	3	66	11	
108	39	24	6	0	0	0	4	1	1	Arc III

Case by Case

The remainder is a case-by-case analysis of these 25 line-types.

For this talk, we wish to look at a few cases only.

Recall that the 0-lines form an arc in the dual plane (i.e., no 3 concurrent)

Case 108 with $a_0 = 4$

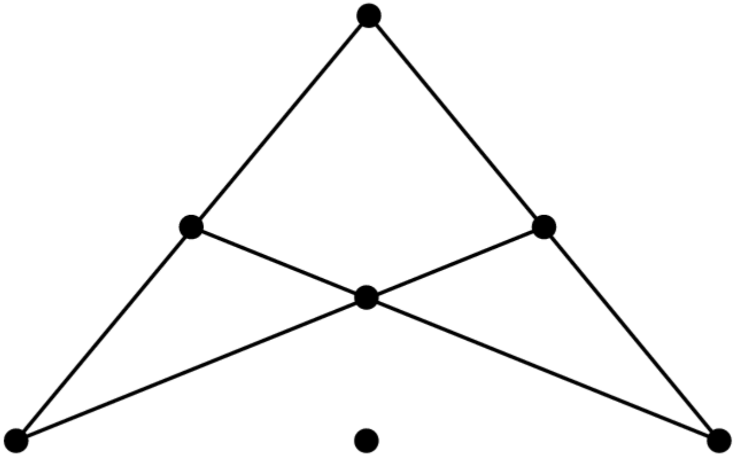
The four 0-lines form a quadrilateral with 6 intersection points.

Thus, it determines a 7th point Q, say, and this point completes a Fano plane $\mathrm{PG}(2, 2)$.

One can show: the points on the quadrilateral together with Q form the complement of an arc.

This is Arc III with a stabilizer of order 72.

Arc III: group order $\frac{168 \cdot 3}{7} = 72$



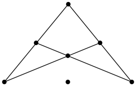
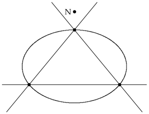
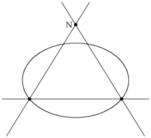
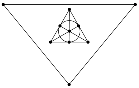
Cases 88 - 102 with $a_0 = 3$

The three 0-lines form a triangle.

The stabilizer of the triangle has order 882.

For the remaining 7 points X, we do a computer search.

We find that there are 133 possibilities for such sets X.

Orbit	Length	properties of X	$\lvert\mathrm{Aut}\rvert$	Arc	
1	49	all collinear	18	III	
2	49	$(7,2)$-arc	18	I	
3	21	$(7,2)$-arc	42	II	
4	14	$\mathrm{PG}(2,2)$	63	IV	

(18 $=$ subgroup of index 4)

Case by Case

Search Algorithm – Two Parts:

Algebra:

Use symmetry to reduce the search

Combinatorics:

Use parameters to gain more information

Combinatorics:

1.) How do w-lines intersect 0-lines?

2.) How do w-lines intersect themselves?

We restrict to $2 \leq w < 6$.

1.) How do w-lines intersect 0-lines? ($w = 2$)

Case.72.1

	$\mathcal{L}_6$	$\mathcal{L}_4$	$\mathcal{L}_2$	$\mathcal{L}_0$
$\rightarrow$	50	18	3	2
6	8	0	1	0
36	7	2	0	0
1	7	0	0	2
6	6	1	1	1
1	6	0	3	0
10	5	3	0	1
12	4	4	1	0
1	3	6	0	0

1^6

Case.72.2

	$\mathcal{L}_6$	$\mathcal{L}_4$	$\mathcal{L}_2$	$\mathcal{L}_0$
$\rightarrow$	50	18	3	2
6	8	0	1	0
36	7	2	0	0
1	7	0	0	2
6	6	1	1	1
10	5	3	0	1
3	5	2	2	0
9	4	4	1	0
2	3	6	0	0

1^6

2.) How do w-lines intersect themselves? ($w = 2$)

	$\mathcal{L}_6$	$\mathcal{L}_4$	$\mathcal{L}_2$	$\mathcal{L}_0$
$\rightarrow$	50	18	3	2
6	8	0	1	0
36	7	2	0	0
1	7	0	0	2
6	6	1	1	1
1	6	0	3	0
10	5	3	0	1
12	4	4	1	0
1	3	6	0	0

1^6

$1^{12}\,3^1$

	$\mathcal{L}_6$	$\mathcal{L}_4$	$\mathcal{L}_2$	$\mathcal{L}_0$
$\rightarrow$	50	18	3	2
6	8	0	1	0
36	7	2	0	0
1	7	0	0	2
6	6	1	1	1
10	5	3	0	1
3	5	2	2	0
9	4	4	1	0
2	3	6	0	0

1^6

$1^9\,2^3$

Notation

$m_P(\mathcal{L})$ the multiplicity of the point P on the line set $\mathcal{L}$.

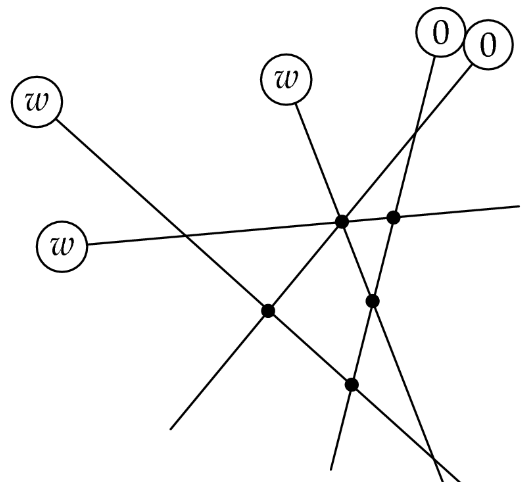
P is i-point w.r.t $\mathcal{L}$ if $m_P(\mathcal{L}) = i$.

$M_i(X;\mathcal{L})$ the set of i-points in the subset $X \subseteq \mathcal{V}$.

$$m_i := m_i(X;\mathcal{L}) = |M_i(X;\mathcal{L})|.$$

Special cases:

$$M_i(\mathcal{L}) = M_i(\mathcal{V};\mathcal{L}) \text{ and } m_i(\mathcal{L}) = m_i(\mathcal{V};\mathcal{L})$$



$$a_0 = 2,\ a_w = 3,\ \mu = 1^4\,2^1,$$
$$\|\mu\| = |S| = 5,\ |\mu| = 6$$

Notation

A Partition μ of the integer n is an expression

$$n = n_1 + n_2 + \cdots + n_k$$

for some k (with $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$

Let m_i or $\mu(i)$ be the number of n_j with $n_j = i$.

Exponential Notation: write i^{m_i}

$$|\mu| = \sum_i i\mu(i) \quad \text{and} \quad \|\mu\| = \sum_i \mu(i).$$

Also, for partitions μ, ν, define a new partition $\mu + \nu$ by putting

$$(\mu + \nu)(i) = \mu(i) + \nu(i) \quad \text{for all } i.$$

Since any two lines intersect, we have:

Lemma

For $i \neq j$, $|\mu_{[\mathcal{L}_i];\mathcal{L}_j}| = a_i a_j$.

Here,

$$[\mathcal{L}] = \bigcup_{l \in \mathcal{L}} l$$

the set of points covered by the set of lines $\mathcal{L}$.

The Search Algorithm

Use the parameters

1. $\mu_{[\mathcal{L}_0];\mathcal{L}_w}$ (i.e., 1^6)
2. $\mu_{A;\mathcal{L}_w} + \mu_{B^*;\mathcal{L}_w}$ (i.e., $1^6 + 1^{12}3^1 = 1^{18}3^1$)

Here, $B^* = B \setminus ([\mathcal{L}_0] \cap [\mathcal{L}_w])$.

Find and classify all realizations.

The Search Algorithm

Step 1:

Up to $\mathrm{P\Gamma L}(3, q)$-equivalence,

choose a_0 lines $\mathcal{L}_0$,

compute the stabilizer H.

The Search Algorithm

Step 2:

Up to H-equivalence,
search for sets S with

- $S \subseteq [\mathcal{L}_0] \setminus M_2(\mathcal{L}_0)$
- $|S| = \|\mu_{[\mathcal{L}_0];\mathcal{L}_w}\|$
- $|S \cap l| \leq a_w$ for all $l \in \mathcal{L}_0$

Compute K, the stabilizer
of the set S in the group H.

The Search Algorithm

Step 3:

Up to K-equivalence,
compute possibilities for a set of lines $\mathcal{L}$
such that:

- $[\mathcal{L}] \cap [\mathcal{L}_0] = S$
- $\sum_{P \in l \cap S} m_P(\mathcal{L}) = a_w$ for all $l \in \mathcal{L}_0$.
- $\mu_{\mathcal{V} \setminus S; \mathcal{L}} = \mu_{A; \mathcal{L}_w} + \mu_{B^*; \mathcal{L}_w}$.

Put $\mathcal{L}_w := \mathcal{L}$

Step 4:

Identify more points of either A or B by their intersection number.

For instance,

if $\mu_{A;\mathcal{L}_w}(i) > 0$ and $\mu_{B^*;\mathcal{L}_w}(i) = 0$

then all i-points in $\mathcal{V} \setminus S$ go into A.

The Search Algorithm

Step 5:

Perform a backtrack search
on the remaining points (details omitted).

Thus, A and B are determined

Check the line type

Conclusion

- Finite geometry:
  - Conics,
  - Arcs, ovals, hyperovals
- Combinatorial tools:
  - Tactical decompositions, diophantine equations
  - Parameters (line type, point type, multiplicities, intersection numbers)
- Algebraic tools:
  - Symmetry groups
- Algorithmic tools:
  - Computing orbits of finite groups
- Theoretical tools:
  - Geometric reasoning.

References

- S. Johnson 1962: A new upper bound for error-correcting codes. *IRE Trans.*, IT-8:203–207, 1962.

- J.R.M. Mason 1984: A class of $((p^n - p^m)(p^n - 1), p^n - p^m)$-arcs in PG$(2, p^n)$. *Geom. Dedicata*, 15(4):355–361, 1984.

- A. Betten and D. Betten 2010: There is no Drake/Larson linear space on 30 points. Journal of Combinatorial Designs 18:48–70, 2010.