The maximal size of a 3-arc in $PG(2,8)$

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

March 25, 1997

Abstract

We prove that 15 is the maximal size of a 3-arc in the projective plane of order 8.

1 Introduction

Let $PG(2,q) = (\mathcal{P}, \mathcal{L})$ be the desarguesian projective plane of order q. A point set $\mathcal{K} \subseteq \mathcal{P}$ is a (k,n)-**arc** if $\mathcal{K}$ has cardinality k and no more than n points of $\mathcal{K}$ are collinear. Denote by $m_2(n,q)$ the maximum cardinality k of a (k,n)-arc in $PG(2,q)$. The objective of this paper is a proof of the following:

Theorem 1 $m_2(3,8) = 15$.

This closes the last gap in our knowledge of the numbers $m_2(n,q)$ for $q \leq 9$. For more details and references we refer to [1].
Two nonequivalent $(15,3)$-arcs will be constructed (see Lemma 5, Corollary 2).
An (n,k)-arc in $PG(2,q)$ is equivalent to a linear q-ary code $[n,3,n-k]_q$. In terms of coding theory Theorem 1 states that an 8-ary code $[16,3,13]_8$ does not exist while codes $[15,3,12]_8$ do exist.
The most important tool in the proof is the determination of the weight

distribution (see [5] and Theorem 2) of the code generated by the plane. In section 2 we will use these numbers to describe the codewords of weights up to 25 explicitly. Especially important is a set of 18 points which arises naturally in connection with the codewords of weight 25.
Occasionally we will have to calculate in coordinates. We use homogeneous coordinates. The point $(\alpha : \beta : \gamma)$ is incident with line $[a : b : c]$ if and only if $\alpha a + \beta b + \gamma c = 0$. We fix a primitive element ϵ of $\mathbb{F}_8$ such that

$$\epsilon + \epsilon^5 = \epsilon^2 + \epsilon^3 = \epsilon^4 + \epsilon^6 = 1.$$

In order to study the embedding of a point set $\mathcal{B}$ in $PG(2,8)$ we use the following terminology:
$\mathcal{L}_i(\mathcal{B})$ is the set of lines meeting $\mathcal{B}$ in precisely i points (the i-**secants** of $\mathcal{B}$), and $a_i(\mathcal{B}) = |\mathcal{L}_i(\mathcal{B})|$.
$\mathcal{L}_i(\mathcal{B})$ denotes the set of i-secants passing through point P, and $a_i(P,\mathcal{B}) = |\mathcal{L}_i(P,\mathcal{B})|$. In the dual situation when a set $\mathcal{G}$ of lines is given we use analogous terminology. In particular $\mathcal{P}_i(\mathcal{G})$ is the set of points, which are on precisely i lines of $\mathcal{G}$, $a_i(\mathcal{G}) = |\mathcal{P}_i(\mathcal{G})|$.
J.W.P. Hirschfeld informed me that A.L.Yasin, a student of his, has proven $m_2(3,8) = 15$ by an exhaustive computer search (see [6]). An unpublished manuscript of mine [3] containing proofs of $m_2(3,8) = 15$ and $m_2(7,8) = 49$ existed since March 1988. While there is now a short proof for the fact that $m_2(7,8) = 49$ (see [2]) this does not seem to be the case for the result proved in this paper.

2 The structure of $PG(2,8)$ and its code

Put $\Pi = PG(2,8) = (\mathcal{P}, \mathcal{L})$.

Lemma 1 *1. The group $PGL_3(8)$ has order $2^9 \cdot 3^2 \cdot 7^2 \cdot 73$ and operates transitively on quadrangles, 5-arcs, hyperovals and Fano planes of* Π.

2. *Π has $2^6 \cdot 3 \cdot 7^2 \cdot 73 = 686,784$ quadrangles, $2^7 \cdot 3^2 \cdot 7^2 \cdot 73$ 5-arcs, $2^6 \cdot 7 \cdot 73$ hyperovals and $2^6 \cdot 3 \cdot 7 \cdot 73 = 98,112$ Fano planes.*

3. *A complete arc in Π is either a 6-arc or a hyperoval.*

4. *Every 5-arc in Π is contained in exactly two hyperovals and in exactly three complete 6-arcs.*

Proof: The order of $PGL_3(8)$ and the transitivity of its action on quadrangles and on Fano planes are classical results. As $PGL_3(8)$ is regular on ordered quadrangles, the number of non-ordered quadrangles is $|PGL_3(8)|/4!$ The number of Fano planes is $|PGL_3(8)|/|GL_3(2)|$. The remaining statements are to be found in [4],pp. 209f,401f,406.■

Let V be the binary vector space with the point set $\mathcal{P}$ as basis. We define the binary point code $\mathcal{C}$ and the binary line code $\mathcal{C}^*$ and state without proof some of the basic properties of these codes.

Definition 1 *The* **binary point code** $\mathcal{C}$ *of* Π *is the subspace of* V *generated by the lines. Interpret elements* $v \in \mathcal{C}$ *as point sets by identifying* v *with its support. The* **weight** $|v|$ *is its cardinality. Let* $\mathcal{C}_i$ *the set of codewords* $v \in \mathcal{C}$ *of weight* i *and* $A_i = |\mathcal{C}_i|$.
The **binary line code** $\mathcal{C}^*$ *of* Π *is the point code of the dual plane. The weights, the sets* $\mathcal{C}_i^*$ *and numbers* A_i^* *are defined in analogy with the case of the point code.*
If $\mathcal{A} \subseteq \mathcal{P}$ *is a set of points, then* $\sum_{A \in \mathcal{A}} A \in \mathcal{C}^*$. *Here* $\sum_{A \in \mathcal{A}} A$ *denotes the set of those lines, which intersect* $\mathcal{A}$ *in odd cardinality.*
If $\mathcal{B} \subseteq \mathcal{L}$ *is a set of lines, then* $\sum_{g \in \mathcal{B}} g \in \mathcal{C}$, *where* $\sum_{g \in \mathcal{B}} g$ *denotes the set of those points, which are on an odd number of lines from* $\mathcal{B}$.

Lemma 2

1. *If* g *is a line and* $v \in \mathcal{C}$, *then* $|g \cap v| \equiv |v|$ *(mod* 2*).*
   If P *is a point and* $v^* \in \mathcal{C}^*$, *then* $|\{g \mid g \in v^*, P \in g\}| \equiv |v^*|$ *(mod* 2*).*
2. $\mathcal{P} \in \mathcal{C}, \mathcal{L} \in \mathcal{C}^*$.
3. *If* $v \in \mathcal{C}$, *then* $\mathcal{P} \setminus v \in \mathcal{C}$.
   If $v^* \in \mathcal{C}^*$, *then* $\mathcal{L} \setminus v^* \in \mathcal{C}^*$.

Proof: 1. is a classical result, 2. follows from $\sum_{g \in \mathcal{L}} g = \mathcal{P}$ and the corresponding dual statement, 3. follows from 2.■

Lemma 3

1. $A_i = A_i^*$ *for all* i.
2. $A_{73-i} = A_i$ *for all* i.

Proof: 1. is clear as Π is self-dual, 2. follows from Lemma 2,2.$\blacksquare$

Recall that we consider code words $v \in \mathcal{C}$ as sets of points, words $v^* \in \mathcal{C}^*$ as sets of lines.

Theorem 2 (Mezzaroba) *The weight distribution of $\mathcal{C}$ is as given in the following table. The larger weights are determined by using $A_{73-i} = A_i$.*

i	A_i	i	A_i	i	A_i
0	1	24	784896	32	29369214
9	73	25	1379700	33	36301440
16	2628	28	6671616	36	49056000
21	56064	29	10596096		

We are going to describe explicitly all the code words of $\mathcal{C}^*$ of weight up to 25.

Lemma 4 $\mathcal{C}_0^* = \{0\}, \mathcal{C}_9^* = \{P \mid P \in \mathcal{P}\}$
$\mathcal{C}_{16}^* = \{P + Q \mid P, Q \in \mathcal{P}, P \neq Q\}$,
$\mathcal{C}_{21}^* = \{P + Q + R \mid P, Q, R \in \mathcal{P}$ *form a triangle* $\}$.

Proof: Comparison with Theorem 2 shows we found precisely A_i elements in each case. Thus there are no others. Recall that we interpret a point P here as the set of lines through P. Addition is formal binary addition. Thus $P + Q$ is a set of 16 lines.$\blacksquare$

Proposition 1 *Let $E \subset \mathcal{P}$ be (the point set of) a Fano plane. Put $\mathcal{L}_i = \mathcal{L}_i(E), a_i = a_i(E), i = 0, 1, 3$. Further $\mathcal{P}_i = \mathcal{P}_i(\mathcal{L}_3(E)), p_i = |\mathcal{P}_i|, i = 0, 1, 3$. Elements of $\mathcal{L}_1, \mathcal{L}_0$ are tangents and exterior lines, respectively, elements of $\mathcal{P}_0$ are exterior points of E. Then the following hold:*

1. $a_3 = p_3 = 7, a_1 = p_1 = 42, a_0 = p_0 = 24$.
   Every exterior line contains exactly 2 exterior points, every exterior point is on exactly 2 exterior lines.

2. *$\mathcal{L}_0$ is an element of $\mathcal{C}^*$.*

3. *Put $G_0 = PGL_3(8), G = P\Gamma L_3(8)$. The stabilizer G_E of E in G is the direct product of $GL_3(2)$ and a cyclic group Z of order 3. Exactly then are exterior points P, Q in the same Z-orbit if PQ is an exterior line. The eight orbits of Z on the exterior points are regions of imprimitivity for the action of G_0.*

Proof: 1. follows from trivial counting arguments, 2. from $\mathcal{L}_0 = \sum_{P\in\mathcal{P}_1} P$. 3. We know that G_0 operates regularly on ordered quadrangles and induces the full automorphism group $GL_3(2)$ on E. It follows that G_E is a direct product as claimed. Z is the Galois group of $\mathbb{F}_8 \mid \mathbb{F}_2$. It follows that Z has no fixed points outside E and no fixed lines outside $\mathcal{L}_3(E)$. The eight orbits of Z in $\mathcal{P}_0$ are regions of imprimitivity of G_0. In the light of 1. it suffices to prove that $g = PQ$ is an exterior line if P, Q are exterior points in the same Z-orbit. Assume $g \notin \mathcal{L}_0$. Then $g \in \mathcal{L}_1$. Put $g \cap E = \{R\}$. As R is fixed under Z we obtain the contradiction that g is fixed by Z.$\blacksquare$

We remark at this point that the action of G_0 on the eight Z-orbits of exterior points may be identified with the operation of $PSL_2(7)$ on the projective line, thus yielding another proof of the exceptional isomorphism between the simple groups $GL_3(2)$ and $PSL_2(7)$.

Corollary 1 *$\mathcal{C}_{24}^*$ consists of 686,784 sums of quadrangles and of 98,112 sets of exterior lines of Fano planes.*

Proof: This follows from comparison with Theorem 2.$\blacksquare$

The case of weight 25 is somewhat more difficult.

Definition 2 *A* **pentatrio** *(short* **pio***) is a set of three pairwise disjoint 5-arcs, such that the union of any two of these 5-arcs is always a hyperoval.*

Lemma 5 *Every 5-arc $\mathcal{K}$ is in a unique pio $T(\mathcal{K})$. The point set of a pio is a $(15,3)$-arc. All pios are projectively equivalent. There are $2^7 \cdot 3 \cdot 7^2 \cdot 73$ pios.*

Proof: Put $\mathcal{K}_1 = \{N_1, (1:0:0), (0:0:1), (1:1:1), (\epsilon^2 : \epsilon : 1)\}$, where $N_1 = (0:1:0)$. Then $\mathcal{K}_1$ is a 5-arc. The hyperovals containing $\mathcal{K}_1$ (see Lemma 1,4.) are $\mathcal{O}_2 = \mathcal{K}_1 \cup \mathcal{K}_3$ and $\mathcal{O}_3 = \mathcal{K}_1 \cup \mathcal{K}_2$, where
$\mathcal{K}_2 = \{N_2, (\epsilon^4 : \epsilon^2 : 1), (\epsilon^6 : \epsilon^3 : 1), (\epsilon^3 : \epsilon^5 : 1), (\epsilon^5 : \epsilon^6 : 1)\}, N_2 = (\epsilon : \epsilon^4 : 1)$

and
$\mathcal{K}_3 = \{N_3, (\epsilon^5 : \epsilon^3 : 1), (\epsilon^6 : \epsilon^2 : 1), (\epsilon^4 : \epsilon^6 : 1), (\epsilon^3 : \epsilon^4 : 1)\}, N_3 = (\epsilon : \epsilon^5 : 1)$.
It is easily checked that $\mathcal{O}_1 = \mathcal{K}_2 \cup \mathcal{K}_3$ is a hyperoval. As different hyperovals cannot intersect in more than half their points (see [4],p.165), different pios must have different point sets. The Lemma follows.■

Lemma 6 *Let $\mathcal{K}$ be a 5-arc, $\mathcal{G} = \mathcal{G}(\mathcal{K}) = \sum_{P\in\mathcal{K}} P \in \mathcal{C}^*$. Then $\mathcal{G}$, the set of tangents of $\mathcal{K}$, is in $\mathcal{C}^*_{25}$. Exactly then is $\mathcal{G}(\mathcal{K}) = \mathcal{G}(\mathcal{K}')$ for a 5-arc $\mathcal{K}' \neq \mathcal{K}$ if $\mathcal{K} \cup \mathcal{K}'$ is a hyperoval.*

Proof: $\mathcal{G}(\mathcal{K})$ is the set of 25 tangents to $\mathcal{K}$. Clearly $\mathcal{G}(\mathcal{K}) = \mathcal{G}(\mathcal{K}')$ if $\mathcal{K}$ and $\mathcal{K}'$ are in a common pio. Let now $\mathcal{G}(\mathcal{K}) = \mathcal{G}(\mathcal{K}')$ for some $\mathcal{K}' \neq \mathcal{K}$. Then $\mathcal{K} \cup \{Q\}$ is a 6-arc for every $Q \in \mathcal{K}' \setminus \mathcal{K}$.
If $P \in \mathcal{K} \cap \mathcal{K}'$, then necessarily $\mathcal{L}_1(P;\mathcal{K}) = \mathcal{L}_1(P;\mathcal{K}')$, whence $\mathcal{L}_2(P;\mathcal{K}) = \mathcal{L}_2(P;\mathcal{K}')$. It follows $|PQ \cap \mathcal{K}| = 2$ for every $Q \in \mathcal{K}' \setminus \mathcal{K}$, contradicting the fact that $\mathcal{K} \cup \{Q\}$ is a 6-arc. We have proved $\mathcal{K} \cap \mathcal{K}' = \emptyset$. The Lemma follows.■

Proposition 2 *$\mathcal{C}^*_{25}$ consists of 6132 sums of three collinear points and of $2^7 \cdot 3 \cdot 7^2 \cdot 73 = 1,373,568$ sums of 5-arcs.*

Proof: There are $73\binom{9}{3} = 6132$ sets of three collinear points and these yield as many codewords of weight 25. By Lemmas 5 and 6 there are exactly $2^7 \cdot 3 \cdot 7^2 \cdot 73$ different elements in $\mathcal{C}^*_{25}$, which are sums of 5-arcs. As $2^7 \cdot 3 \cdot 7^2 \cdot 73 + 6132 = A_{25}$ there are no other codewords of weight 25.■

Definition 3 *Let $\mathcal{K}$ be a 5-arc. Denote by $\mathcal{R}(\mathcal{K})$ the set of points R which complement $\mathcal{K}$ to a complete 6-arc.*

It follows from Lemma 1,4. that $|\mathcal{R}(\mathcal{K})| = 3$.

Lemma 7 *Let $\mathcal{T} = \{\mathcal{K}_1, \mathcal{K}_2, \mathcal{K}_2\}$ be a pio. Then $\mathcal{R}(\mathcal{K}_1) = \mathcal{R}(\mathcal{K}_2) = \mathcal{R}(\mathcal{K}_3)$. Denote this set by $\mathcal{R}(\mathcal{T})$.*

Proof: Let $R \in \mathcal{R}(\mathcal{K}_1)$. By definition of a pio we have $R \notin \mathcal{K}_1 \cup \mathcal{K}_2 \cup \mathcal{K}_3$. As $\mathcal{K}_1 \cup \{R\}$ is a 6-arc we have $PR \in \mathcal{G}(\mathcal{K}_1)$ (see Lemma 6). By Lemma 6 we have $\mathcal{G}(\mathcal{K}_1) = \mathcal{G}(\mathcal{K}_2) = \mathcal{G}(\mathcal{K}_3)$. It follows that $\mathcal{K}_2 \cup \{R\}$ and $\mathcal{K}_3 \cup \{R\}$ are 6-arcs. By Lemma 1,3. and the definition of a pio these are complete 6-arcs.■

Definition 4 *A* **complete pentatrio** *(short* **clio***) is a set*

$$\mathcal{M} = \{\mathcal{T}, \mathcal{R}\},$$

where $\mathcal{T}$ is a pio and $\mathcal{R} = \mathcal{R}(\mathcal{T})$.

Lemma 8 *Clios are projectively equivalent. Every 5-arc is in a unique clio. There are $2^7 \cdot 3 \cdot 7^2 \cdot 73$ clios.*

This is trivial.

Lemma 9 *There is a canonical bijection σ between clios and words in $\mathcal{C}_{25}^*$, which are sums of 5-arcs. This bijection is defined as follows:*
If $\mathcal{M} = \{\mathcal{K}_1, \mathcal{K}_2, \mathcal{K}_3, \mathcal{R}\}$ is a clio, then $\sigma(\mathcal{M}) = \mathcal{G}(\mathcal{K}_1) = \mathcal{G}(\mathcal{K}_2) = \mathcal{G}(\mathcal{K}_3)$.
If $\mathcal{G} = \sum_{P \in \mathcal{K}_1} P \in \mathcal{C}_{25}^*$, where $\mathcal{K}_1$ is a 5-arc, then
$\sigma^{-1}(\mathcal{G}) = \mathcal{T}(\mathcal{K}_1) \cup \mathcal{R}(\mathcal{K}_1) = \mathcal{P}_5(\mathcal{G})$.

Proof: It follows from Lemma 1,4. and Lemmas 5, 6 that σ is a bijection. The inverse image of $\mathcal{G}$ is by definition $\mathcal{T}(\mathcal{K}_1) \cup \mathcal{R}(\mathcal{K}_1)$. We wish to identify this set with $\mathcal{P}_5(\mathcal{G})$, the set of all points, which are on 5 lines from $\mathcal{G}$. Put $a_i = a_i(\mathcal{G})$. As one inclusion is obvious it suffices to show $a_5 = 18$. We have $a_i = 0$ for $i > 5$, by definition. It follows from Lemma 2 that $a_i = 0$ when i is even. We have only three unknowns, a_1, a_3, a_5. By counting

- the lines,
- incidences (Q, g), where $Q \in \mathcal{P}, g \in \mathcal{G}, Q \in g$, and
- pairs of lines

we obtain the equations

$$\boxed{\begin{array}{rcl} a_1 + a_3 + a_5 & = & 73 \\ a_1 + 3a_3 + 5a_5 & = & 225 \\ 3a_3 + 10a_5 & = & 300 \end{array}}$$

The unique solution is $a_5 = 18, a_3 = 40, a_1 = 15$.■

Lemma 10 *Let $\mathcal{M} = \{\mathcal{K}_1, \mathcal{K}_2, \mathcal{K}_3, \mathcal{R}\}$ be a clio, $\mathcal{O}_i = \mathcal{K}_j \cup \mathcal{K}_k$ for $\{i, j, k\} = \{1, 2, 3\}$. Let $N_i \in \mathcal{K}_i$ such that N_1, N_2, N_3 are the nuclei of $\mathcal{O}_3, \mathcal{O}_1, \mathcal{O}_2$, respectively.*
Then there is a line $s_0 = s_0(\mathcal{M}) \in \sigma(\mathcal{M})$ such that

$$s_0 \cap \mathcal{M} = \mathcal{R} \cup \{N_1, N_2, N_3\}.$$

We call $s_0(\mathcal{M})$ the **strong line** *of $\mathcal{M}$.*

Proof: Because of projective equivalence we can start from the pio given in the proof of Lemma 5. Put

$$R_1 = (\epsilon : \epsilon^2 : 1), R_2 = (\epsilon : \epsilon^3 : 1), R_3 = (\epsilon : \epsilon^6 : 1).$$

An easy calculation with coordinates shows that for each i the lines $R_i P, P \in \mathcal{K}_1$ are pairwise different. It follows $\mathcal{R} = \{R_1, R_2, R_3\}$. The strong line of $\mathcal{M}$ is $s_0 = [\epsilon^6 : 0 : 1]$.$\blacksquare$

Lemma 11 *The stabilizer of a clio in $P\Gamma L_3(8)$ is isomorphic to $A_4 \times Z_3$.*

Proof: It follows from Lemmas 8 and 1 that the stabilizer in question has order 36. Consider the group $H =< M_1, M_2, \rho_1 > \times < \rho_2 >$, where

$$M_1 = \begin{pmatrix} 0 & 0 & \epsilon^6 \\ 0 & 1 & 0 \\ \epsilon & 0 & 0 \end{pmatrix}, M_2 = \begin{pmatrix} \epsilon^2 & \epsilon^2 & \epsilon^2 \\ 0 & 1 & 0 \\ \epsilon^4 & \epsilon^3 & \epsilon^2 \end{pmatrix}$$

and $\rho_1 = M\phi, \rho_2 = M'\phi$, where ϕ is the Frobenius automorphism and

$$M = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, M' = \begin{pmatrix} \epsilon^6 & \epsilon^3 & \epsilon \\ 1 & \epsilon^2 & \epsilon^3 \\ \epsilon^6 & \epsilon^4 & \epsilon^3 \end{pmatrix}.$$

Operation is from the right. Then H stabilizes the clio as introduced in the proofs of Lemma 5 and 10.$\blacksquare$

Lemma 12 *Let $\mathcal{M} = \{\mathcal{K}_1, \mathcal{K}_2, \mathcal{K}_3, \mathcal{R}\}$ be a clio. Identify $\mathcal{M}$ with its point set. Then the following hold:*

$$a_6(\mathcal{M}) = 1, a_5(\mathcal{M}) = 0, a_4(\mathcal{M}) = a_3(\mathcal{M}) = a_1(\mathcal{M}) = 12,$$
$$a_2(\mathcal{M}) = 30, a_0(\mathcal{M}) = 6.$$

We have

$$\mathcal{L}_6(\mathcal{M}) = \{s_0(\mathcal{M})\}, \mathcal{L}_4(\mathcal{M}) = \cup_{i=1}^3 \mathcal{L}_4(R_i;\mathcal{M}), \mathcal{L}_3(\mathcal{M}) = \cup_{i=1}^3 \mathcal{L}_3(N_i;\mathcal{M}),$$
$$\mathcal{G} = \mathcal{L}_6(\mathcal{M}) \cup \mathcal{L}_4(\mathcal{M}) \cup \mathcal{L}_3(\mathcal{M}), \mathcal{L}_1(\mathcal{M}) = \cup_{i=1}^3 \mathcal{L}_1(R_i;\mathcal{M}).$$

The proof is trivial.

Proposition 3 *Let $\mathcal{M} = \{\mathcal{K}_1, \mathcal{K}_2, \mathcal{K}_3, \mathcal{R}\}$ be a clio. Then $\{s_0(\mathcal{M})\} \cup \mathcal{L}_0(\mathcal{M})$ is the set of lines of a Fano plane E.*
The word $\sum_{M \in \mathcal{M}} M = \mathcal{L}_1(\mathcal{M}) \cup \mathcal{L}_3(\mathcal{M})$ of the line code is the set of 0-secants of E.
We have $E \cap s_0(\mathcal{M}) = s_0(\mathcal{M}) \setminus \mathcal{M}$. If $A \in E \setminus s_0(\mathcal{M})$, then $AR \in \mathcal{L}_4(\mathcal{M})$ for all $R \in \mathcal{R}$ and $AN_i \in \mathcal{L}_2(\mathcal{M}), i = 1, 2, 3$.

Proof: We use the same clio as before. Then

$$\mathcal{L}_0(\mathcal{M}) = \{[\epsilon^6 : \epsilon : 1], [\epsilon^6 : \epsilon^2 : 1], [\epsilon^4 : \epsilon : 1], [\epsilon : \epsilon^3 : 1], [\epsilon^2 : \epsilon : 1], [\epsilon^3 : \epsilon^5 : 1]\}$$

and $E = \{A_1, \ldots, A_7\}$, where

$$A_1 = (\epsilon : 0 : 1), A_2 = (\epsilon : 1 : 1), A_3 = (\epsilon : \epsilon : 1), A_4 = (0 : \epsilon^6 : 1),$$

$A_5 = (\epsilon^2 : 1 : 0), A_6 = (\epsilon^2 : \epsilon^3 : 1), A_7 = (1 : \epsilon^2 : 1), s_0(\mathcal{M}) \cap E = \{A_1, A_2, A_3\}$. Let $A \in E \setminus s_0(\mathcal{M})$. As $\mathcal{K}_i \cup \{R_j\}$ is a complete 6-arc $(i, j = 1, 2, 3)$ the point A must be collinear with two points of $\mathcal{K}_i$. Thus $a_2(A;\mathcal{M}) \geq 3$. As $a_0(A;\mathcal{M}) = 3$ and $|\mathcal{M}| = 18$, a counting argument yields $a_4(A;\mathcal{M}) = 3 = a_2(A;\mathcal{M})$ (see Lemma 12). It follows $AR_i \in \mathcal{L}_4(\mathcal{M}), AN_i \in \mathcal{L}_2(\mathcal{M}), AA_i \in \mathcal{L}_0(\mathcal{M}), i = 1, 2, 3$. The word $U = \sum_{M \in \mathcal{M}} M = \mathcal{L}_1(\mathcal{M}) \cup \mathcal{L}_3(\mathcal{M})$ has weight 24 by Lemma 12. No point of E is on a line of U. Thus U cannot be the sum of a quadrangle. It follows from Proposition 1 and Corollary 1 that U is the set of 0-secants of E.■

Let $\mathcal{G} \in \mathcal{C}_{25}^*$ be the sum of a 5-arc and $\mathcal{M} = \mathcal{P}_5(\mathcal{G})$ the corresponding clio (see Lemma 9). In the following table we list, for every line $g \in \mathcal{L}_i(\mathcal{M})$, the number of points from $\mathcal{P}_j(\mathcal{G})$ it contains, $j = 1, 3, 5$.

Table 1:

i	$\mathcal{P}_5(\mathcal{G})$	$\mathcal{P}_3(\mathcal{G})$	$\mathcal{P}_1(\mathcal{G})$
6	6	0	3
4	4	4	1
3	3	6	0
2	2	4	3
1	1	6	2
0	0	8	1

Corollary 2 *Let $\mathcal{G} \in \mathcal{C}_{25}^*$ be the sum of a 5-arc. Then $\mathcal{P}_1(\mathcal{G})$ is a $(15,3)$-arc but not a pio.*

Proof: We have seen in the proof of Lemma 9 that $a_1(\mathcal{G}) = 15$. The last column of the Table shows that $\mathcal{P}_1(\mathcal{G})$ is a $(15,3)$-arc. As $a_3(\mathcal{P}_1(\mathcal{G})) = 31$, this point set cannot be a pio (see Definition 2 and Lemma 5).■

Lemma 13 *Let $\mathcal{O}$ be a hyperoval,H, H_0 the stabilizers of $\mathcal{O}$ in $P\Gamma L_3(8)$ and in $PGL_3(8)$, respectively.*
$\mathcal{O}$ is the union of a conic and its nucleus N and the following hold:

1. *$H_0 \cong PGL_2(8), H \cong P\Gamma L_2(8), |H_0| = 7 \cdot 8 \cdot 9, |H| = 3 \cdot |H_0|$.*

2. *H_0 is sharply 3-transitive on $\mathcal{O} \setminus \{N\}$.*

3. *H_0 is transitive on the flags $(X, g), X \in g, X \notin \mathcal{O}, g \cap \mathcal{O} = \emptyset$.*

4. *The stabilizer of a flag (X, g) in H has order 6.*

Proof: It follows from Lemma 1 that $\mathcal{O}$ is the union of a conic and its nucleus. 1. and 2. are classical results, see [4],pp.143f.
3. As every $X \notin \mathcal{O}$ can be written as an intersection $X = g_1 \cap g_2$, where $g_1 = XN, |g_2 \cap \mathcal{O}| = 2$, it is obvious that the triple transitivity of H_0 on $\mathcal{O} \setminus \{N\}$ implies the transitivity on the 63 points $X \notin \mathcal{O}$. Denote by K the stabilizer of X in H_0. Then K is elementary abelian of order 8. We have to show that K is transitive on the four 0-secants passing through X. Let

$U \leq K$ be the stabilizer of the 0-secant g through X in K. We have to prove $|U| \leq 2$.
Let $1 \neq u \in U$. As u fixes N and $P = (XN \cap \mathcal{O}) \setminus \{N\}$ and because of the sharp triple transitivity of H_0 on $\mathcal{O} \setminus \{N\}$, the involution u must be fixed-point-free on $\mathcal{O} \setminus \{N, P\}$. Let $A \in \mathcal{O} \setminus \{N, P\}, B = A^u$. We claim that A, B, X are collinear.
Assume this is not the case, let $Y = AB \cap g$. Then $Y \neq X$ and Y is fixed by u. Further u fixes $(XN \cap \mathcal{O}) \setminus \{N\}$, but this contradicts the fixed-point-free action on $\mathcal{O} \setminus \{N, P\}$.
We have proved that $B = A^u$ is the unique point of $\mathcal{O}$ on AX different from A. It follows that the action of u is uniquely determined. We have $|U| \leq 2$. This shows $|U| = 2$ and claim 3.
4. follows from 1. and 3.■

Lemma 14 *If $\mathcal{O}$ is a set of 10 points in the dual of the point code $\mathcal{C}$, then $\mathcal{O}$ is a hyperoval.*

Proof: The assumption says that every line intersects $\mathcal{O}$ in an even number of points. Let $P \in \mathcal{O}$. As each of the 9 lines through P picks up at least one further point of $\mathcal{O}$, the Lemma follows. ■

3 The proof

3.1 $m_2(3,8) \leq 16$

Assume $\mathcal{B}$ is a $(17,3)$-arc in Π. Put $\mathcal{L}_i = \mathcal{L}_i(\mathcal{B}), a_i = a_i(\mathcal{B}), i = 0,1,2,3$. Let $\mathcal{G} = \mathcal{L}_0 \cup \mathcal{L}_2$. We know from Lemma 2 that $\mathcal{G} \in \mathcal{C}^*$. Denote by $w^* = a_0 + a_2$ the weight of $\mathcal{G}$.

Lemma 15 *1. We have $\mathcal{B} = \mathcal{A}_2 \cup \mathcal{A}_1$, where $\mathcal{A}_2 = \{P \mid P \in \mathcal{B}, a_3(P) = 7, a_2(P) = 2\}, \mathcal{A}_1 = \{P \mid P \in \mathcal{B}, a_3(P) = 8, a_1(P) = 1\}$. Further $|\mathcal{A}_2| = a_2, |\mathcal{A}_1| = a_1$. In particular $a_1 + a_2 = 17$.*

*2. $w^* \in \{16, 24, 28, 32\}, a_0 = 8 + w^*/4, a_1 = 25 - 3w^*/4,$
$a_2 = 3w^*/4 - 8, a_3 = 48 - w^*/4$.*

Proof: 1. follows from a trivial counting argument.
2. By definition $a_0 + a_1 + a_2 + a_3 = 73$. Counting pairs of points in $\mathcal{B}$ yields $a_2 + 3a_3 = 136$. An easy calculation yields the formulae expressing the a_i in terms of w^*.
Count incidences $(P, g), P \in \mathcal{B}, g \in \mathcal{L}_3 \cup \mathcal{L}_1, P \in g$. We obtain $a_3 + a_1 \geq 17 \cdot 7/3$, hence $a_3 + a_1 \geq 40$ and $w^* \leq 32$ by Lemma 2 and Theorem 2. As $a_0 > 0$, Theorem 2 yields the first statement of 2. ∎

We shall consider seperately the four cases in Lemma 15,2.

Lemma 16 $w^* \neq 16$.

Proof: Assume $w^* = 16$. Then $\mathcal{L}_0 \cup \mathcal{L}_2 = P_1 + P_2$ by Lemma 4 and $a_2 = 4, a_0 = 12$. Without restriction $a_2(P_1) \leq 2$. It follows $a_0(P_1) \geq 6$. In particular $P_1 \notin \mathcal{B}$ and $|\mathcal{B}| = \sum_{P_1 \in g} |g \cap \mathcal{B}| \leq 9$, contradiction.∎

Lemma 17 $w^* \neq 24$.

Proof: Assume $w^* = 24$. We have $a_0 = 14, a_1 = 7, a_2 = 10, a_3 = 42$. If $\mathcal{G}$ is sum of a quadrangle, then the same contradiction as in Lemma 16 is obtained. It follows from Corollary 1 that $\mathcal{G}$ is the set of 0-secants of a Fano plane E. Let $P \in E$. Then P is on no line of $\mathcal{G}$, whence $P \notin \mathcal{A}_2$. If $P \notin \mathcal{B}$, then $a_1(P) = 5$ by the standard counting argument. As $a_1 = 7$, at most one point of E is not in $\mathcal{A}_1$. Let $g \in \mathcal{L}_3(E)$. By Definition of $\mathcal{G}$ we have $g \in \mathcal{L}_1 \cup \mathcal{L}_3$. If $X \in g \setminus E$, then $a_0(X) + a_2(X) = 4$. It follows $X \notin \mathcal{B}$. The preceding remark shows $g \in \mathcal{L}_3$ and consequently:

$$E = \mathcal{A}_1, \mathcal{L}_3(E) \subset \mathcal{L}_3.$$

We have seen that $\mathcal{A}_2$ consists of exterior points of the Fano plane $\mathcal{A}_1$. Assume more than two points of $\mathcal{A}_2$ are collinear on a line h. As $\mathcal{B}$ is a $(17, 3)$-arc, h is an exterior line of $\mathcal{A}_1$, contradicting the fact that an exterior line of a Fano plane contains only two exterior points.
Thus $\mathcal{A}_2$ is a hyperoval. By definition of the $\mathcal{A}_i$ we have $\mathcal{L}_2 \subset \mathcal{L}_0(\mathcal{A}_1)$ and $g \cap \mathcal{B} \subset \mathcal{A}_2$ for every $g \in \mathcal{L}_2$. As every point in $\mathcal{A}_2$ is on two 2-secants, it follows from Lemma 1,3. that the points of $\mathcal{A}_2$ occur in triples whence the contradiction that a_2 is a multiple of 3.∎

Lemma 18 $w^* \neq 28$.

Proof: If $w^* = 28$, then $a_0 = 15, a_1 = 4, a_2 = 13, a_3 = 41$. No three words P_1, P_2, P_3 of $\mathcal{A}_1$ are collinear as otherwise the sum of the $P \in \mathcal{B}$ different from P_1, P_2, P_3 would yield a codeword of weight 20, contradicting Theorem 2. Denote by $\mathcal{D}_i$ the set of 3-secants of $\mathcal{B}$, which meet $\mathcal{A}_1$ in i points, put $d_i = |\mathcal{D}_i|$. We have seen $d_i = 0$ for $i > 2$. Clearly $d_2 = 6$. The standard counting argument yields $d_1 = 20, d_0 = 15$.
Let V be the sum of the $P \in \mathcal{A}_2$. Then $V = \mathcal{D}_2 \cup \mathcal{D}_0$ and V has weight 21. By Lemma 4 we have $\mathcal{D}_2 \cup \mathcal{D}_0 = P_1 + P_2 + P_3$, where the P_i form a triangle. As $a_3(P_i) \geq 7$ we have $\{P_1, P_2, P_3\} \subset \mathcal{B}$. It follows that none of the P_i is on a tangent to $\mathcal{B}$, hence $\{P_1, P_2, P_3\} \subset \mathcal{A}_2$ and $\{P_1P_2, P_1P_3, P_2P_3\} \subset \mathcal{L}_2$. Each P_i is the intersection of two lines from $\mathcal{D}_2$. It follows that $\mathcal{A}_1 \cup \{P_1, P_2, P_3\}$ is a Fano plane. This is a contradiction as the P_i are not collinear.$\blacksquare$

Lemma 19 $w^* \neq 32$.

Proof: If $w^* = 32$, then $a_0 = 16, a_1 = 1, a_2 = 16, a_3 = 40$. Let P_0 be the point in $\mathcal{A}_1$. Consider $\mathcal{D}_i, d_i$ as in the proof of Lemma 18. Clearly $d_1 = 8, d_0 = 32$. We have $\mathcal{D}_0 = \sum_{P \in \mathcal{A}_2} P \in \mathcal{C}^*$.
For $g \in \mathcal{D}_1, g \cap \mathcal{B} = \{P_0, P_1, P_2\}$, let $V(g) = \mathcal{D}_0 + P_1 + P_2 \in \mathcal{C}^*$. Then $V(g)$ has weight 24. Set $\{Q_1, Q_2\} = \{Q \mid Q \in \mathcal{A}_2, P_1Q \in \mathcal{L}_2\}, \{R_1, R_2\} = \{R \mid R \in \mathcal{A}_2, P_2R \in \mathcal{L}_2\}, \mathcal{N} = \{Q_1, Q_2, R_1, R_2\}$. It is impossible that $Q_1 = R_1$ as this would yield a codeword $\mathcal{D}_0 + P_1 + P_2 + Q_1$ of weight 17, contradicting Theorem 2. It follows that $|\mathcal{N}| = 4$. As every $N \in \mathcal{N}$ is on six lines of $V(g)$, we must have $V(g) = Q_1 + Q_2 + R_1 + R_2$, and $\mathcal{N}$ is a quadrangle (see Corollary 1). As $P_0N \notin V(g)$ for $N \in \mathcal{N}$ we can choose notation such that $\{P_0, Q_1, R_1\}$ and $\{P_0, Q_2, R_2\}$ are collinear on lines g_2, g_3, respectively. The six lines through Q_1, which are disjoint from the set $\{Q_2, R_1, R_2\}$, consist of five lines of $\mathcal{D}_0$ and the 2-secant P_1Q_1. Thus the points $\{P_2, Q_2, R_2\}$ are on one 3-secant and one 2-secant through Q_1. We get $Q_1P_2Q_2 \in \mathcal{L}_3, Q_1R_2 \in \mathcal{L}_2$. In the same way we get $Q_2R_1 \in \mathcal{L}_2$. We have seen that every line $g \in \mathcal{D}_1$ determines canonically a set $\{g, g_2, g_2\}$ of three lines of $\mathcal{D}_1$ with the property that for every $P \in \mathcal{A}_2, P \in g \cup g_2 \cup g_3, Q \in \mathcal{A}_2, PQ \in \mathcal{L}_2$ the point Q is in $g \cup g_2 \cup g_3$. We get the contradiction that d_1 is a multiple of 3.$\blacksquare$
We have shown the following:

Lemma 20 $m_2(3, 8) \leq 16$.

3.2 The final step

We work under the assumption that a $(16,3)$-arc $\mathcal{B}$ exists in Π. Put $\mathcal{L}_i = \mathcal{L}_i(\mathcal{B}), a_i = a_i(\mathcal{B}), i = 0,1,2,3$. Let $\mathcal{G} = \mathcal{L}_0 \cup \mathcal{L}_2, \mathcal{U} = \mathcal{L}_1 \cup \mathcal{L}_3$ (both in $\mathcal{C}^*$). Denote by $w_G^* = a_0 + a_2, w_U^* = a_1 + a_3$ the weights of these code words.

Lemma 21 *1. We have $\mathcal{B} = \mathcal{B}_0 \cup \mathcal{A}_1$, where $\mathcal{B}_0 = \{P \mid P \in \mathcal{B}, a_3(P) = 6, a_2(P) = 3, a_1(P) = 0\}, \mathcal{A}_1 = \{P \mid P \in \mathcal{B}, a_3(P) = 7, a_2(P) = a_1(P) = 1\}$. Further $|\mathcal{A}_1| = a_1$.*

2. $a_0 = 17 - a_1/3, a_2 = 24 - a_1, a_3 = 32 + a_1/3$, $w_G^* = 41 - 4a_1/3$, $w_U^* = 32 + 4a_1/3, a_1 \in \{0,3,6,9,12,15\}$.

Proof: 1. is immediate. The standard counting argument yields three equations for the a_i. We can express everything in terms of a_1. The equation for a_0 shows that a_1 is a multiple of 3. As $a_1 \le |\mathcal{B}| = 16$, it follows $0 \le a_1 \le 15$.∎

We will consider the cases corresponding to different values of a_1 seperately, starting from the easier cases.

Lemma 22 $a_1 \neq 15$.

Proof: If $a_1 = 15$, then $a_0 = 12, w_G^* = 21$ by Lemma 21, hence $\mathcal{L}_0 \cup \mathcal{L}_2 = P_1 + P_2 + P_3$ (see Lemma 4). We can choose notation such that $a_0(P_1) \ge 4$. Counting elements of $\mathcal{B}$ on lines through P_1 yields the contradiction $|\mathcal{B}| \le 15$.∎

Lemma 23 $a_1 \neq 0$.

Proof: If $a_1 = 0$, then $w_U^* = a_3 = 32, a_2 = 24$ by Lemma 21. Let $z \in \mathcal{L}_2, z \cap \mathcal{B} = \{P_1, P_2\}$, put $V(z) = \mathcal{U} + P_1 + P_2$. Then $V(z)$ has weight 24. Let $\{Q_1, Q_2\} = \{Q \mid Q \in \mathcal{B}, Q \neq P_2, QP_1 \in \mathcal{L}_2\}, \{Q_3, Q_4\} = \{Q \mid Q \in \mathcal{B}, Q \neq P_1, QP_2 \in \mathcal{L}_2\}$ and $\mathcal{N} = \{Q_1, Q_2, Q_3, Q_4\}$. If $Q \in \mathcal{N}$, then Q is on at least six lines of $V(z)$. Corollary 1 yields the following:
$|\mathcal{N}| = 4, \{P_2Q_1, P_2Q_2, P_1Q_3, P_1Q_4\} \subset \mathcal{L}_3, \mathcal{N}$ is a quadrangle, $V(z) = \sum_{Q \in \mathcal{N}} Q$. We obtain $\mathcal{L}_3 = \mathcal{U} = \sum_{N \in \mathcal{N}'} N$, where $\mathcal{N}' = \mathcal{N} \cup \{P_1, P_2\}$.

As every 3-secant intersects $\mathcal{N}'$ nontrivially, $\mathcal{B} \setminus \mathcal{N}'$ must be a hyperoval. As hyperovals do not have tangents there must be 3-secants $g_1 = P_1Q_3Q_4$ and $g_2 = P_2Q_1Q_2$, and these are the only 3-secants having all their $\mathcal{B}$-points in $\mathcal{N}'$. We conclude $\mathcal{N}' = \mathcal{N}'(z) = \mathcal{N}'(g)$ for every $g \in \mathcal{L}_2, g \cap \mathcal{B} \subset \mathcal{N}'$. As exactly nine 2-secants have their $\mathcal{B}$-points in $\mathcal{N}'$, we get the contradiction that a_2 is a multiple of 9.$\blacksquare$

Lemma 24 $a_1 \neq 3$.

Proof: If $a_1 = 3$, then $a_3 = 33, a_2 = 21, a_0 = 16$. Let $\mathcal{A}_1 = \{P_1, P_2, P_3\}$. Then $\mathcal{A}_1$ is not collinear as otherwise $\sum_{P \in \mathcal{B}_0} P$ would have weight 17, contradicting Theorem 2. If $P_iP_j \in \mathcal{L}_2$, then $\mathcal{U} + P_i + P_j$ has weight 20, contradiction. It follows that there is some $Q_k \in \mathcal{B}_0$ such that $Q_k \in g_k = P_iP_j, \{i,j,k\} = \{1,2,3\}$. Put $\mathcal{N} = \{P_1, P_2, P_3, Q_1, Q_2, Q_3\}$ and $\mathcal{O} = \mathcal{B} \setminus \mathcal{N}$. The word $\sum_{P \in \mathcal{B}_0} P = \mathcal{U} + P_1 + P_2 + P_3$ has weight 21. It follows from Lemma 4 and the fact that Q_k is on more than three lines of this word that $\mathcal{U} + P_1 + P_2 + P_3 = Q_1 + Q_2 + Q_3$, hence $\mathcal{U} = \mathcal{L}_3 \cup \mathcal{L}_1 = \sum_{N \in \mathcal{N}} N$. It follows that $\mathcal{O}$ is a hyperoval. Further $f \cap \mathcal{O} = \emptyset$ whenever $|f \cap \mathcal{N}| > 1$.
We introduce coordinates. Let $\mathcal{O} = \mathcal{K}_1 \cup \mathcal{K}_2$ be the hyperoval introduced in the proof of Lemma 5. Then $\mathcal{N}$ is a set of six points with the property that any two points of $\mathcal{N}$ are joined by a 0-secant of $\mathcal{O}$. By Lemma 13 we can choose without restriction $P_1 = (1:1:0), P_1Q_1 = [1:1:1]$. The stabilizer W of the flag (P_1, P_1Q_1) in H has order 6 (see Lemma 13). It is easily checked that W is cyclic, generated by $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ and the Frobenius automorphism ϕ. The operation of W shows that we can choose $Q_1 = (1:0:1)$ or $Q_1 = (\epsilon : \epsilon^5 : 1)$. Let $\{h_1, h_2, h_3\} = \{h \mid P_1 \in h \in \mathcal{L}_0(\mathcal{O}), h \neq [1:1:1]\}, \{g_1, g_2, g_3\} = \{g \mid Q_1 \in g \in \mathcal{L}_0(\mathcal{O}), g \neq [1:1:1]\}, P_{i,j} = h_i \cap g_j$. We have $h_1 = [\epsilon^3 : \epsilon^3 : 1], h_2 = [\epsilon^5 : \epsilon^5 : 1], h_3 = [\epsilon^6 : \epsilon^6 : 1]$.
Assume $Q_1 = (1:0:1)$. Then $g_1 = [1 : \epsilon^3 : 1], g_2 = [1 : \epsilon^5 : 1], g_3 = [1 : \epsilon^6 : 1]$. We still have ϕ at our disposition. We have $P_{1,1}P_{i,j} \in \mathcal{L}_2(\mathcal{O})$ whenever $i \neq 1, j \neq 1$. This shows $P_{1,1} \notin \mathcal{N}$, thus $P_{2,2} \notin \mathcal{N}, P_{3,3} \notin \mathcal{N}$. The operation of ϕ allows us to choose $h_3 \in \mathcal{L}_1(P_1)$. Thus $\mathcal{N} = \{P_1, Q_1, P_{1,2}, P_{1,3}, P_{2,1}, P_{2,3}\}$. This is impossible as $P_{1,2}P_{2,1} \in \mathcal{L}_2(\mathcal{O})$.
We have $Q_1 = (\epsilon : \epsilon^5 : 1), g_1 = [\epsilon^3 : \epsilon : 1], g_2 = [\epsilon^3 : \epsilon^4 : 1], g_3 = [\epsilon^5 : \epsilon^6 : 1]$. In

the same way as before we see $P_{1,1} = (\epsilon^4 : 0 : 1) \notin \mathcal{N}, P_{1,3} = (\epsilon^6 : 1 : 1) \notin \mathcal{N}$. Thus $\{h_1\} = \mathcal{L}_1(P_1)$. As $P_{3,3} = (0 : \epsilon : 1) \notin \mathcal{N}$, necessarily $\{P_{3,1}, P_{3,2}\} \subset \mathcal{N}$. However $P_{2,3}P_{3,2} \in \mathcal{L}_2(\mathcal{O}), P_{2,2}P_{3,2} \in \mathcal{L}_2(\mathcal{O})$, hence $\{P_{2,3}, P_{2,2}\} \cap \mathcal{N} = \emptyset$, contradiction. ■

Lemma 25 $a_1 \neq 6$.

Proof: If $a_1 = 6$, then $a_3 = 34, a_2 = 18, a_0 = 15$. Assume $z \in \mathcal{L}_2, z \cap \mathcal{B} = \{P_1, P_2\} \subset \mathcal{A}_1$. Then $\mathcal{U}+P_1+P_2$ has weight 24, and as every $P \in \mathcal{A}_1 \setminus \{P_1, P_2\}$ is on at least six lines of $\mathcal{U}+P_1+P_2$, we have $\mathcal{U} = \sum_{P \in \mathcal{A}_1} P$ by Proposition 1 and Corollary 1. Further $\mathcal{B}_0$ is a hyperoval and P_1, P_2 are on the diagonal of the Fano plane generated by the quadrangle $\mathcal{A}_1 \setminus \{P_1, P_2\}$. Let $X \in z$ be the third point of this Fano plane on z. Then $a_3(X) = 0$. It follows that $\mathcal{B} \cup \{X\}$ is a $(17, 3)$-arc, contradiction.
Assume $d \in \mathcal{L}_3, d \cap \mathcal{B} = \{P_1, P_2, P_3\} \subset \mathcal{A}_1$. Then $\mathcal{U}+P_1+P_2+P_3$ has weight 21, hence $\mathcal{U} = \sum_{P \in \mathcal{A}_1} P$ by Lemma 4. Let $P \in \mathcal{A}_1 \setminus \{P_1, P_2, P_3\}$. Then P is on seven lines of $\mathcal{U}+P_1+P_2+P_3$, hence without restriction $PP_1 \in \mathcal{L}_2$, but this has been excluded above.
We have $g = P_1P_2 \in \mathcal{L}_3, g \cap \mathcal{B} = \{P_1, P_2, Q\}$, where $Q \in \mathcal{B}_0$, for every $P_1, P_2 \in \mathcal{A}_1$. The word $\mathcal{V} = \mathcal{U}+P_1+P_2+Q$ has weight 25. If $\mathcal{V}$ is the sum of three collinear points X_1, X_2, X_3, then clearly $X_i \notin g$ and $\mathcal{U} = X_1+X_2+X_3+P_1+P_2+Q$ cannot have weight 40, contradiction.
Consequently $\mathcal{V}$ is the sum of a 5-arc (see Proposition 2). Let $P \in \mathcal{A}_1 \setminus \{P_1, P_2\}$. As P cannot be on more than five lines of $\mathcal{V}$, necessarily $PQ \in \mathcal{L}_2$. Thus $a_2(Q) \geq 4$, contradicting Lemma 21.■

Lemma 26 $a_1 \neq 12$.

Proof: If $a_1 = 12$, then $a_3 = 36, a_2 = 12, a_0 = 13$. As no $(17, 3)$-arc exists there is no point P such that $a_0(P) + a_2(P) = 9$. By Proposition 2 $\mathcal{G}$ is sum of a 5-arc. Consider the clio $\mathcal{M} = \mathcal{P}_5(\mathcal{G})$ (see Lemma 9, Definition 4) and the strong line $s_0 = s_0(\mathcal{M})$ (see Lemma 10). Clearly $s_0 \in \mathcal{L}_0 \cup \mathcal{L}_2$. By Lemma 21 we have $\mathcal{B} \cap \mathcal{M} = \emptyset, \mathcal{A}_1 \subset \mathcal{P}_1(\mathcal{G}), \mathcal{B}_0 \subset \mathcal{P}_3(\mathcal{G})$.
Assume $s_0 \in \mathcal{L}_0$. Then $\mathcal{A}_1 = \mathcal{P}_1(\mathcal{G}) \setminus s_0$. Let $\mathcal{D}_i = \{g \mid g \in \mathcal{L}_3, |g \cap \mathcal{A}_1| = i\}, i = 0, 1, 2, 3$. By Lemma 12 we have $\mathcal{L}_2(\mathcal{M}) \cup \mathcal{L}_1(\mathcal{M}) \cup \mathcal{L}_0(\mathcal{M}) = \mathcal{L}_3 \cup \mathcal{L}_1$.

Let $P \in \mathcal{A}_1, P \in g \in \mathcal{L}_1$. Table 1 shows $g \in \mathcal{L}_1(\mathcal{M})$, whence $\mathcal{L}_1 = \mathcal{L}_1(\mathcal{M})$. Let $h \in \mathcal{L}_0(\mathcal{M})$. We know $h \in \mathcal{L}_3$. The Table shows $h \cap \mathcal{A}_1 = \emptyset$. Let $P \in s_0 \cap \mathcal{P}_1(\mathcal{G})$. As P is a point of the Fano plane E generated by s_0 and $\mathcal{L}_0(\mathcal{M})$ (see Proposition 3) the point P is on three lines of $\mathcal{D}_0$. This yields the contradiction $|\mathcal{B}_0| \geq 9$.
We have $s_0 \in \mathcal{L}_2, s_0 \cap \mathcal{B} = \{A_1, A_2\} \subset \mathcal{A}_1$. Each $P \in \mathcal{P}_1(\mathcal{G}) \setminus s_0$ is on exactly one 4-secant v of $\mathcal{M}$. If in addition $P \in \mathcal{A}_1$, then v is a 2-secant of $\mathcal{B}$. As v contains only one point of $\mathcal{P}_1(\mathcal{G})$ (see Table 1), we get exactly ten 2-secants v of $\mathcal{B}$ satisfying $|v \cap \mathcal{B}_0| = 1$. The presence of s_0 shows that there is exactly one $z_0 \in \mathcal{L}_2$ such that $|z_0 \cap \mathcal{B}_0| = 2$. Thus there are two points $P \in \mathcal{B}_0 \setminus z_0$. We have $a_2(P) = 3, \mathcal{L}_2(P) \subset \mathcal{L}_4(\mathcal{M})$. As $P \in \mathcal{P}_3(\mathcal{G})$, our point is on three 4-secants but on no 3-secant of $\mathcal{M}$. By Lemma 12 P is on no tangent to $\mathcal{M}$. Thus, by Proposition 3, P belongs to the Fano plane E generated by s_0 and $\mathcal{L}_0(\mathcal{M})$. With $\{X\} = s_0 \setminus (\mathcal{M} \cup \mathcal{B})$ we get $\{PA_1, PA_2, PX\} \subset \mathcal{L}_3 \cup \mathcal{L}_0(\mathcal{M})$. As $\mathcal{A}_1 \subset \mathcal{P}_1(\mathcal{G})$, Table 1 shows that none of these lines contains points of $\mathcal{A}_1$ outside s_0. Thus $|PA_1 \cap \mathcal{B}_0| = |PA_2 \cap \mathcal{B}_0| = 2, |PX \cap \mathcal{B}_0| = 3$. This yields the contradiction $|\mathcal{B}_0| \geq 5$.■

Remains to consider the hardest case:

$$a_1 = 9, a_3 = 35, a_2 = 15, a_0 = 14.$$

Let us call a 3-secant **special** if it contains three points of $\mathcal{A}_1$. Let s be the number of special lines, $s(P)$ the number of special lines through point P, and x the number of points in $\mathcal{A}_1$, which are not contained in special lines. A line g has **type** (a, b) if $|g \cap \mathcal{A}_1| = a, |g \cap \mathcal{B}_0| = b$.

Lemma 27 *If $P, P' \in \mathcal{A}_1$ and either $s(P) \neq 0$ or $s(P') \neq 0$, then $PP' \in \mathcal{L}_3$.*

Proof: Let g be a special line, $g \cap \mathcal{A}_1 = \{P_1, P_2, P_2\}$. Then $\mathcal{V} = \mathcal{U} + P_1 + P_2 + P_3$ has weight 25. As every $P \in \mathcal{A}_1 \setminus g$ is on at least five lines of $\mathcal{V}$, the word $\mathcal{V}$ is sum of a 5-arc (see Proposition 2). This also shows that P is on exactly fice lines of $\mathcal{V}$, hence $PP_i \in \mathcal{L}_3, i = 1, 2, 3$.■

Lemma 28 *1. If $P \in \mathcal{A}_1$ is not contained in a special line, then P is on seven lines of type (2,1) and on one line of types (2,0) and (1,0) each.*

2. *If $P \in \mathcal{A}_1$ is on some special line, then P is on $8 - 2s(P)$ lines of type (2,1), on $s(P) - 1$ lines of type $(1,2)$, one line of type (1,1) and one line of type (1,0).*

Proof: 1. is clear. 2. The 2-secant through P has type (1,1) by Lemma 27. The usual counting argument then yields our claim (compare Lemma 21).■

Lemma 29 *$x = 0$ or $x = 2$.*

Proof: Clearly x is even as 2-secants of type (2,0) do not intersect in $\mathcal{B}$. Assume there are two such secants, z_1 and z_2, where $z_1 \cap \mathcal{A}_1 = \{A, B\}$, $z_2 \cap \mathcal{A}_1 = \{C, D\}$. Then $\mathcal{G} + A + B + C + D$ has weight 20, contradicting Theorem 2.■

Lemma 30 *There is no triangle of special lines intersecting pairwise in $\mathcal{A}_1$.*

Proof: Assume $\{g_1, g_2, g_3\}$ is such a triangle, $g = ABD, g_2 = ACE, g_3 = BCF, \mathcal{N} = \{A, B, \ldots, F\} \subset \mathcal{A}_1$. Let $\mathcal{Z} = \mathcal{U} + \sum_{N \in \mathcal{N}} N$. If D, E, F are not collinear, then $\mathcal{Z}$ has weight 20, contradicting Theorem 2. It follows that D, E, F are collinear on a special line g_4, and $|\mathcal{Z}| = 16$. Thus $\mathcal{Z} = X + Y$ (see Lemma 4). Let M be the seventh point of the Fano plane generated by g_1, g_2, g_3, g_4. Then $M = AF \cap BE \cap CD$ is on at least three lines of $\mathcal{Z}$, without restriction $M = X$. As Y is on six 2-secants through points of $\mathcal{N}$, we have $Y \notin \mathcal{B}$ (see Lemma 21). Upon counting the points of $\mathcal{B}$ on lines through Y we see that Y is on no 3-secant at all. This yields the contradiction that $\mathcal{B} \cup \{Y\}$ is a (17,3)-arc.■

Lemma 31 *Special lines never intersect in $\mathcal{B}$.*

Proof: Let $g_1 = ABC, g_2 = ADE$ be special lines, $\mathcal{N} = \mathcal{N}(g_1, g_2) = \{A, B, C, D, E\}$. Then $\mathcal{Z} + \sum_{N \in \mathcal{N}} N$ is a word of weight 21, hence $\mathcal{Z} = X_1 + X_2 + X_3$, where $\Delta = \{X_1, X_2, X_3\}$ is a triangle. Now, $\mathcal{Z}$ consists of

- four 3-secants $PP', P \in \{B, C\}, P' \in \{D, E\}$,
- four tangents through the points in $\mathcal{A}_1 \setminus \mathcal{N}$,

- five 2-secants through the points of $\mathcal{N}$, and
- eight 3-secants disjoint from $\mathcal{N}$.

A counting argument shows $\Delta \cap \mathcal{B} \neq \emptyset$. Assume $P \in \Delta \cap \mathcal{A}_1$. By Lemmas 27 and 30 our point is on five different 3-secants $PN, N \in \mathcal{N}$, which are not in $\mathcal{Z}$, contradiction.
Thus $\Delta \cap \mathcal{B} \subset \mathcal{B}_0$. The presence of tangents shows $\Delta \not\subset \mathcal{B}_0$.
Assume $|\Delta \cap \mathcal{B}| = 1$, let $\Delta = \{Q, X, Y\}$, where $Q \in \mathcal{B}_0$. Counting $\mathcal{B}$ on lines through X or Y and keeping in mind that $\{XQ, YQ\} \subset \mathcal{L}_2 \cup \mathcal{L}_3$ (see Lemma 21) we see that X and Y are on at most three 3-secants of $\mathcal{Z}$. This forces $Q \in \mathcal{B}_0$ to be on exactly six 3-secants and one 2-secant of $\mathcal{Z}$. We can choose notation such that X is on three 3-secants and on at least two 2-secants of $\mathcal{Z}$. The argument above when applied to X yields a contradiction.
We have $\Delta = \{Q_1, Q_2, X\}$, where $\{Q_1, Q_2\} \subset \mathcal{B}_0, X \notin \mathcal{B}$. As $Q_i \in \mathcal{B}_0$, the point X is in the intersection of the tangents through the points in $\mathcal{A}_1 \setminus \mathcal{N}$.
Put

$$\mathcal{O}(g_1, g_2) = \cup_{P \in \mathcal{A}_1 \setminus \mathcal{N}} P \cup \cup_{Q \in \mathcal{B}_0 \setminus \{Q_1, Q_2\}} Q \cup \{X\}.$$

By definition of $\mathcal{Z}$ we get that the sum of the $P \in \mathcal{O}(g_1, g_2)$ is the 0-word. Lemma 14 shows that $\mathcal{O}(g_1, g_2)$ is a hyperoval. Thus every special line intersects $\mathcal{N}$ nontrivially. Assume A is on a third special line g_3. Then $\mathcal{O}(g_1, g_3) \neq \mathcal{O}(g_1, g_2)$, but $\mathcal{O}(g_1, g_3)$ has at least two points of $\mathcal{A}_1$ and three points of $\mathcal{B}_0$ in common with $\mathcal{O}(g_1, g_2)$. Let Y be the point in $\mathcal{O}(g_1, g_3) \setminus \mathcal{B}$. As Y is the intersection of the tangents through the points in $\mathcal{A}_1 \setminus \mathcal{N}(g_1, g_3)$, we get $X = Y \in \mathcal{O}(g_1, g_3) \cap \mathcal{O}(g_1, g_2)$. We have found two different hyperovals having more than half of their points in common. This is impossible (see [4],p.165).
As $x \leq 2$ there must be a third special line g_3. As $g_3 \cap \mathcal{N} \neq \emptyset$ and because of Lemma 30 we have without restriction $g_3 \cap g_1 \in \mathcal{A}_1, g_3 \cap g_2 \notin \mathcal{A}_1$. The same method as above yields the contradiction $6 \leq |\mathcal{O}(g_1, g_3) \cap \mathcal{O}(g_1, g_2)| < 10$. ∎

Lemmas 29 and 31 show the following:
$s = 3$, every point of $\mathcal{A}_1$ is in exactly one special line. Let $g_1 = ABC, g_2 = DEF, g_3 = GHI$ be the special lines, where $\mathcal{A}_1 = \{A, B, \ldots, I\}$, set $\mathcal{W} = \sum_{P \in \mathcal{A}_1} P$. Then $\mathcal{W}$ has weight 21. It consists of

- the special lines g_1, g_2, g_3,

- $\mathcal{L}_1$, and
- the nine secants of type (1,1).

We have $\mathcal{W} = X_1 + X_2 + X_3$, where $\Delta = \{X_1, X_2, X_3\}$ is a triangle. Clearly $\Delta \cap \mathcal{A}_1 = \emptyset$ as $P \in \mathcal{A}_1$ is on only three points of $\mathcal{W}$. If $Q \in \Delta \cap \mathcal{B}_0$, then Q would have to be on seven 2-secants of $\mathcal{W}$, contradiction to Lemma 21. Thus $\Delta \cap \mathcal{B} = \emptyset$. Clearly each $X \in \Delta$ is on exactly one special line. Consider the numbers $a_1(X_i)$. We have $a_1(X_1) + a_1(X_2) + a_1(X_3) = 9$. The word $\mathcal{G} = \mathcal{U} + A + B + C$ has weight 25. As every $P \in \mathcal{A}_1 \setminus \{A, B, C\}$ is on exactly five lines of $\mathcal{G}$, the word $\mathcal{G}$ is sum of a 5-arc (see Proposition 2). If $a_1(X_1) \geq 5$, then X_1 would be on more than five lines of $\mathcal{G}$, contradiction. Assume $a_1(X_1) = 0$. Then exactly one point $Q \in \mathcal{B}$ satisfies $X_1Q \notin \mathcal{G}$. Thus X_1Q is a tangent, contradiction as $Q \in \mathcal{B}_0$. Assume $a_1(X_1) = 3$. Then exactly four points $Q \in \mathcal{B}$ satisfy $X_1Q \notin \mathcal{G}$. As all these points are in $\mathcal{B}_0$, they must be distributed on two 2-secants. Thus g_1 is the only 3-secant through X_1. It follows that $\mathcal{B}' = \mathcal{B} \setminus \{A\} \cup \{X_1\}$ is a (16,3)-arc. However, we have $a_3(\mathcal{B}') = a_3 - 6 + a_2(X_1) = a_3 - 1 = 34$. This case has been excluded already. Assume $a_1(X_1) = 1$. Then $X_1 \in \mathcal{P}_1(\mathcal{G})$ by the same reasoning as above. However, A, B, C, X_1 are now four collinear points in $\mathcal{P}_1(\mathcal{G})$. This contradicts Corollary 2.
We have $a_1(X_i) \in \{2, 4\}, i = 1, 2, 3$. It follows that the equation $a_1(X_1) + a_1(X_2) + a_1(X_3) = 9$ cannot be satisfied. This is our final contradiction.

References

[1] S.Ball: *Multiple blocking sets and arcs in finite planes, Journal of the London Mathematical Society* **54** (1996),581-593.

[2] S.Ball,A.Blokhuis: *On the size of a double blocking set in $PG(2,q)$, Finite Fields and Their Applications* **2**(1996),125-137.

[3] J.Bierbrauer: *(k,n)-arcs of maximal size in the plane of order 8,* March 1988, unpublished manuscript.

[4] J.W.P.Hirschfeld: *Projective geometries over finite fields,* Clarendon, Oxford 1979.

[5] J.A.Mezzaroba: Ph.D. thesis, Lehigh University, Bethlehem 1975.

[6] A.L.Yasin: *Cubic arcs in the projective plane of order eight,* Ph.D. thesis, University of Sussex 1986.