HYPERFOCUSED ARCS IN $PG(2, 32)$

C. PARRETTINI, F. PASTICCI

Abstract. All hyperfocused arcs of size 12 and 14 in $PG(2, 32)$ are classified.

1. Introduction

Hyperfocused arcs were introduced in connection with a secret sharing scheme based on geometry due to Simmons [13]. Let a point $X \in PG(3, q)$ be a secret. We fix a line $s$ containing $X$ and we distribute participants on two sets: the top level and the lower level. We call shadow each piece of information that is given to each participant. The shadows of the participants on the top level is a subset of points $\{P_1, \ldots, P_m\}$ of a line $l$ such that $l \cap s = \{X\}$ and the set of shadows for the participants of the lower level is a subset $S \subset \pi$ with $\pi \cap s = \{X\}$ and $l \subset \pi$. Two participants of the top level $I = \{X, P_1, \ldots, P_m\}$ can reconstruct the secret and also three participants in $S \cap I$, but two participants in $S$ are not enough. Simmons showed that $S$ must be an arc and the secants of the arc $S$ cannot contain any point of $I$.

These schemes require a plane arc with the property that its secant lines meet an external line in a minimal number of points. Simmons studied the problem in planes of odd order, where the minimal number above is equal to the number of the points of the arc. Let $S$ be a $k$-arc and $l$ be an exterior line. $S$ is called sharply focused on $l$ if the chords of $S$ cover exactly $k$ points of $l$. $S$ is called hyperfocused on $l$ if the chords of $S$ cover exactly $k - 1$ points of $l$. In plane of odd order, Wettl [14] proved the following characterization of sharply focused set. Let $q = p^a$ be odd and let $S$ be sharply focused on $l$. Then $S$ is contained in a conic, $|S| = k$ divides $q + 1$, $q - 1$ or $q$ and $S$ is affinely regular $k$-gon if $p^2$ does not divide $k$.

Bichara and Korchmáros proved [4] that hyperfocused arcs exist if and only if $q$ is even. Wettl [14] proved that there are hyperfocused arcs not contained in a conic. Cherowitzo and Holder [5] constructed hyperfocused arcs contained in a hyperoval or subplane. moreover they classified small hyperfocused arcs and solved an open problem, posed by Drake and Keating [7] on possible size of hyperfocused arcs, giving a negative answer. Giulietti and Montanucci [8] constructed hyperfocused translation arcs not contained in a hyperoval or subplane. These arcs, hyperfocused on a line $l$ are complete in the sense that every point not belonging to $l$, belongs to some chord of the arc. In [8] is given the

---

2000 Math. Subj. Class.: 51E21.

This research was performed within the activity of GNSAGA of the Italian INDAM, with the financial support of the Italian Ministry MIUR, project “Strutture geometriche, combinatorica e loro applicazioni”, PRIN 2006-2007.
notion of generalized hyperfocused \( k \)-arc where a set of \( k - 1 \) points that block the chords of the arc is not collinear. It is also proven the existence of a generalized hyperfocused 8-arc which is not hyperfocused. In [1] the authors show that, in Desarguesian planes, any generalized hyperfocused arc contained in a conic is hyperfocused. For sizes up to 10, Giulietti and Montanucci give a complete list of examples.

The aim of this paper is to deal with the classification of hyperfocused arcs in \( \mathbb{P}G(2, 32) \). By known results, the problem is open precisely for \( k = 12, 14 \) and \( 16 \). An answer to the cases \( k = 12 \) and \( k = 14 \) is given.

2. Definitions and Preliminaries

Let \( \mathbb{F}_q \) be the finite fields with \( q \) elements and let \( \mathbb{P}G(2, q) \) be the projective plane over \( \mathbb{F}_q \). A \( k \)-arc \( K \) in \( \mathbb{P}G(2, q) \) is a set of \( k \) points no three of which are collinear. A secant (or chord) of \( K \) is any line \( l \) containing two points of \( K \). A blocking set of the secants of \( K \) is a point set \( B \subset \mathbb{P}G(2, q) \setminus K \) such that \( B \cap l \neq \emptyset \) for each \( l \) secant of \( K \). It is easy to prove that the size of \( B \) is at least \( k - 1 \) and, if this lower bound is reached, \( B \) is said of minimum size.

**Definition 2.1.** In a projective plane a \( k \)-arc \( K \) is said to be hyperfocused on a line \( l \) (exterior to \( K \)) if all the secants of \( K \) meet \( l \) in a set of exactly \( k - 1 \) points.

**Example 2.2.** In \( \mathbb{P}G(2, q) \), \( q \) even every 4-arc is hyperfocused on the diagonal line of the 4-arc.

The following theorem, consequence of a result of Bichara and Korchmáros [4], gives conditions on \( q \) and \( k \).

**Theorem 2.3.** If \( K \) is a non-trivial hyperfocused \( k \)-arc in \( \mathbb{P}G(2,q) \) then \( q \) is even. Furthermore, if \( K \) is not a hyperoval then \( k \leq \frac{q}{2} \).

This leads us to focus our attention on \( q \) even, i.e. \( q = 2^s, \ s \in \mathbb{N} \). Some constructions of hyperfocused arcs are given in [5].

**Theorem 2.4** (Holder 1997). For every divisor \( d \) of \( e \), there are hyperfocused arcs of size \( 2^d \) and \( 2^d + 2 \) in \( \mathbb{P}G(2, 2^e) \).

**Theorem 2.5.** A set of points \( K \), with \( |K| > 3 \), on a conic in \( \mathbb{P}G(2, q) \) is hyperfocused on a tangent line to that conic if and only if \( q \) is even and \( K \) is projectively equivalent to a set of points determined by a subgroup of \((\mathbb{F}_q, +)\). In particular \( |K| \mid q \) (i.e. \( |K| = 2^e, \ e > 1 \)).

Another class of hyperfocused arcs are translation arcs which are studied in [8]. Let \((X_1, X_2, X_3)\) be homogeneous coordinates for points in \( \mathbb{P}G(2, q) \) and let \( \ell_\infty \) be the line of equations \( X_3 = 0 \). Given a pair \( A = (a, b) \in \mathbb{F}_q \times \mathbb{F}_q \) denote \( \overline{A} \) the point in \( \mathbb{P}G(2, q) \) with coordinates \((a, b, 1)\) and let \( \phi_A \) be the projectivity

\[
\phi_A : (X_1, X_2, X_3) \rightarrow (X_1 + a_1X_3, X_2 + a_2X_3, X_3)
\]
Let $G$ be an additive subgroup of $\mathbb{F}_q \times \mathbb{F}_q$ and let $K_G(P)$ be the orbit of the point $P \in PG(2,q)$ under the action of the group

$$T_G := \{ \phi_A | A \in G \}.$$ 

**Definition 2.6.** A translation arc is a $k$-arc coinciding with $K_G(P)$ for some $P \in PG(2,q)$ and some additive subgroup of $\mathbb{F}_q \times \mathbb{F}_q$.

The following proposition shows that any translation arc is an hyperfocused arc on $l_\infty$.

**Proposition 2.7.** Let $K$ be a translation arc. Then there exists a blocking set of the secants of $K$ of minimum size which is contained in $l_\infty$.

**Example 2.8.** We consider $G := \{ (\alpha, \alpha^2) | \alpha \in H \}$ where $H$ is any subgroup of $\mathbb{F}_q$. Then $K_G$, as previously defined, is a translation arc.

**Example 2.9.** We consider $G := \{ (\alpha, \alpha^{2i}) | \alpha \in H \}$ where $H$ is any subgroup of $\mathbb{F}_q$ and $(i, s) = 1$ with $s = \log_2 q$. Then the arc $K_G$, as previously defined, is contained in a translation hyperoval.

**Definition 2.11.** Let $K$ be an arc and let $l$ be the focus line, the set of all the intersection points between $l$ and the secant lines of $K$ is called focus set and is denoted by $F_K$.

**Proposition 2.12.** Let $K$ and $K \subseteq K$ be two hyperfocused arcs in $PG(2,q)$ on the same line $l$. Then $|K| \geq 2|K|$.

**Proof.** Each line joining a point of $F_K \setminus F_{K'}$ and a point of $K$ is a tangent line of $K$ and a secant line of $K$. Then $|K \setminus K| \geq k$. □

### 3. 12-arcs in $PG(2,32)$

**Lemma 3.1.** Let $K \subseteq PG(2,32)$ be an hyperfocused 12-arc on the focus line $l$ and $P_1, P_2, P_3 \in K$. Let $l_1 = P_2P_3$, $l_2 = P_1P_3$ and $l_3 = P_1P_2$. Then exists a projectivity $\phi$ of $PG(2,32)$ acting on $l, l_1, l_2, l_3$ as follows:

- $l$ maps to $Z = 0$
- $l_1$ maps to $X = 0$
- $l_2$ maps to $Y = 0$
- $l_3$ maps to $X + Y + Z = 0$

**Proof.** $\{l, l_1, l_2, l_3\}$ is a set of lines, no three of which are concurrent. Then by definition of arc and by the fundamental theorem of projective geometry we have the proof. □

Then a hyperfocused 12-arc is projectively equivalent to an arc satisfying the following conditions:
The focus line has equation \( Z = 0; \)

- \( l_1 \cap l_2 = (0, 0, 1) \in K; \)
- \( l_1 \cap l_3 = (0, 1, 1) \in K; \)
- \( l_2 \cap l_3 = (1, 0, 1) \in K; \)
- \( (0, 1, 0), (1, 1, 0) \) and \( (1, 0, 0) \) are in the focus set.

From Proposition 2.12 any 8-arc \( K_0 \) contained in a hyperfocused 12-arc, has a focus set of size bigger than 7.

As \( q \) is even, every sharply focused \( k \)-arc is contained in a hyperfocused \((k + 1)\)-arc. Therefore, the cardinality of the focus set of \( K_0 \) must be bigger than 8.

An exhaustive algorithm should check every 12-set of pairs of elements in \( \mathbb{F}_{32} \), i.e. \((a_1, b_1), \ldots, (a_{12}, b_{12})\) with \( a_i, b_i \in \mathbb{F}_{32}\), that is, \(32^{24}\) cases. We prove that it is enough to test \(32^5\) possible sets. The first step is to find all possible 8-arcs \( K_0 \) contained in \( K \) with \( K \) satisfying (\(*\)). From (\(*\)) we already know three of the eight points, hence we have to choose only 5 more points. We deal with this problem using affine coordinates of the points: \( X_\infty, Y_\infty, P_\infty \) are focuses and \((0, 1), (0, 0) \) and \((1, 0) \) belong to \( K \). As \( Y_\infty \) is a focus and \((1, 0) \) belongs to \( K \), one of the 5 points must be \((1, a)\). Then

\[
K_0 = \{(0, 0), (0, 1), (1, 0), (1, a), (c, d), (c, e), (f, g), (f, h)\}
\]

for some \( a, c, d, e, f, g, h \in \mathbb{F}_{32} \).

**Lemma 3.2.** The function \( f : (x, y, t) \mapsto (x^2, y^2, t^2) \) and its powers

\[
f^i : (x, y, t) \mapsto (x^{2i}, y^{2i}, t^{2i})
\]

for all \( i \in \mathbb{N} \), are collineations of \( \text{PG}(2, 32) \).

The function \( f^i \) fixes the points \((0, 0), (1, 0), (0, 1), X_\infty, Y_\infty \) and \( P_\infty \). It is possible that \((1, a, 1) \neq f^i(1, a, 1)\). More precisely, once \( a \) is checked, we do not need to check \( a^2, a^4, a^8 \) and \( a^{16} \). Then, instead of 32 cases for \( a \), we have to check \((32 - 2) : 5\) cases.

Without loss of generality, assume \( a \in \{1, \omega, \omega^3, \omega^5, \omega^7, \omega^{11}, \omega^{15}\} \). This means that we must study \( 7 \cdot 32^6 \) cases for \( K_0 \). By adding 4 points to \( \{(0, 0), (0, 1), (1, 0), (1, a)\} \) we have 38 secant lines (for each new point we have a number of secants equal to the number of old points). These should give us new focuses. These focuses, added to those of the 8-arc must be exactly 11 in total. We know that the 8-arcs have already 9 focuses and so it is enough to find the 4 points in such a way that they add at most 2 focuses.

Actually, a first search shows that any 8-arc \( K_0 \) with at least 9 focuses has at least 11 focuses. Among these 11 focuses, we look for two points \( Q_1 \) and \( Q_2 \) such that through each of them there pass exactly 4 tangents to \( K_0 \). There are 16 possible choices, namely the points of the grid defined by the two set of tangents. Among them, we choose all possible 4-uples such that no two of them belong to a unique tangent. For each 4-uple \( \{P_1, P_2, P_3, P_4\} \) we check if \( K_0 \cup \{P_1, P_2, P_3, P_4\} \) is a hyperfocused 12-arc.

As a result, we have 60 hyperfocused 12-arcs and we check if each of them is contained in a hyperconic. For this purpose we construct a list of the 12 points of a single arc and...
we consider the first 5 points. We compute an equation of the conic passing through these 5 points and check if the remaining 7 points, but one, satisfy this equation. If 6 points satisfy the equation then they are all contained in a hyperconic. Otherwise it is possible that the nucleus of the hyperconic is one the first 5 points. Therefore we repeat the procedure starting from other 5 points. It turns out that all these hyperfocused arcs are contained in a hyperconic.

4. 14 arcs

We start by considering an 8-arc $K_0$. It defines a focus set $\mathcal{F}_K$ such that $9 \leq |\mathcal{F}_K| \leq 13$. We add six points and we have 63 new secant lines. These lines add new points to the focus set that must have 13 elements. Now for each 8-arc we find all focuses $Q_1, \ldots, Q_s$ such that for each of them pass 6 tangent lines. We select 2 focuses in $\{Q_1, \ldots, Q_s\}$. Their tangent lines meet in 36 points. Among them we consider the focuses that meet a tangent line for each focus. We consider all 6-uple and we verify if the union of $K$ with these 6 points is a hyperfocused 14-arc. By computer search we see that do not exists any hyperfocused 14-arc. In conclusion it is worthy to note that the classification of 16-arcs is an open problem yet.

REFERENCES

[1] A. Aguglia, G. Korchmáros and A. Siciliano, Minimal coverings of all chords of a conic in $PG(2,q)$, $q$ even, Bull. Belg. Math. Soc. Simon Stevin Vol. 12 No. 5 (2005), pp. 651-655.
[2] L.D. Andersen, Factorizations of graphs. In The CRC handbook of combinatorial designs, CRC Press Series on Discrete Mathematics and its Applications, Boca Raton, CA, (1996) pp. 653–667.
[3] A. Beutelspacher and F. Wettl, On 2-level secret sharing, Des. Codes Cryptogr., Vol. 3 No. 2 (1993), pp. 127–134.
[4] A. Bichara and G. Korchmáros, Note on $(q+2)$-sets in a Galois plane of order $q$. In Combinatorial and Geometric Structures and their Applications, Vol. 14 of Ann. Discrete Math., pp. 117–122, North-Holland, Amsterdam, 1982.
[5] W.E. Cherowitzo and L.D. Holder, Hyperfocused Arcs, Simon Stevin, Vol. 12 No. 5 (2005), pp. 685–696.
[6] D. Drake, Hyperovals in nets of small degree, J. Combin. Des., Vol. 10 (2002), pp. 322–334.
[7] D. Drake and K. Keating, Ovals and hyperovals in Desarguesian nets, Des. Codes Cryptogr., Vol. 31 No. 3 (2004), pp. 195–212.
[8] M. Giulietti and E. Montanucci, On hyperfocused arcs in $PG(2,q)$, Discrete Mathematics, Vol. 306 No. 24 (2006), pp. 3307–3314.
[9] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, Clarendon Press, Oxford (1998).
[10] L.D. Holder, The construction of Geometric Threshold Schemes with Projective Geometry, Master’s Thesis, University of Colorado at Denver, 1997.
[11] B. Segre, Ovals in a finite projective plane, Canad. J. Math, Vol. 7 (1955), pp. 414–416.
[12] G. Simmons, How to (really) share a secret, Adv.in Cryptology - CRYPTO ’88, LNCS, Vol. 403 (1989), pp. 390–448.
[13] G. Simmons, Sharply Focused Sets of Lines on a Conic in $PG(2,q)$, Congr. Numer., Vol. 73 (1990), pp. 181–204.
[14] F. Wettl, On the nuclei of a pointset of a finite projective plane, J. Geom., Vol. 30 (1987), pp. 157–163.
[15] www.dipmat.unipg.it/giuliet/triangles.tex
Dipartimento di Matematica e Informatica Università degli Studi di Perugia, I-06123 Perugia, Italy

E-mail address: pasticci@dipmat.unipg.it