ON HYPERFOCUSED ARCS IN $PG(2,q)$

M. GIULIETTI AND E. MONTANUCCI

Abstract. A k-arc in a Dearguesian projective plane whose secants meet some external line in $k-1$ points is said to be hyperfocused. Hyperfocused arcs are investigated in connection with a secret sharing scheme based on geometry due to Simmons. In this paper it is shown that point orbits under suitable groups of elations are hyperfocused arcs with the significant property of being contained neither in a hyperoval, nor in a proper subplane. Also, the concept of generalized hyperfocused arc, i.e. an arc whose secants admit a blocking set of minimum size, is introduced: a construction method is provided, together with the classification for size up to 10.

1. Introduction

Hyperfocused arcs were introduced in connection with a secret sharing scheme based on geometry due to Simmons [11]. The implementation of this scheme needs an arc in a Desarguesian projective plane with the property that its secant lines intersect some external line in a minimal number of points. Simmons only considered planes of odd order, where this minimal number equals the number of points of the arc [4]. He introduced the term sharply focused set for arcs satisfying the aforementioned property. Sharply focused sets in Desarguesian projective planes of odd order were classified by Beutelspacher and Wettl [3], whose result was based on a previous paper by Wettl [12].

In 1997 Holder [9] extended Simmons's investigation to Desarguesian planes of even order. In such planes the secants of an arc of size k may meet an external line in only $k-1$ points, yet the classification of arcs having this property seems to be an involved problem. Holder used the term super sharply focused sets for such arcs and gave some constructions for them.

In a recent paper [5], Cherowitzo and Holder proposed the term hyperfocused arc instead of super sharply focused set. They provided the classification of small hyperfocused arcs, and constructed new examples, one of which gave a negative answer to a question raised by Drake and Keating [7] on the possible sizes of a hyperfocused arc.

Some open problems were pointed out by Cherowitzo and Holder, including the existence of hyperfocused arcs which are neither contained in a proper subplane nor in a hyperoval. In this paper a positive answer to this question is given. The main tool is the investigation

2000 *Math. Subj. Class.*: Primary 51E21, Secondary 51A30, 05B25, 05C70.
Keywords: Desarguesian plane, arc, blocking set, 1-factorization, secret sharing scheme.
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 2004-2005.

of the so-called translation arcs, i.e. arcs which are point orbits under a group of elations. In Section 3 it is shown that such arcs are hyperfocused, and it is proved that sometimes they are contained neither in a hyperoval nor in a proper subplane, see Theorem 3.8.

The concept of hyperfocused arc can be naturally extended to that of generalized hyperfocused arc, that is an arc of size k for which there exists an external point set of size $k-1$ meeting each of its secants. Recently, Aguglia, Korchmáros and Siciliano [1] proved that in Desarguesian planes of even order any generalized hyperfocused arc is hyperfocused, provided that it is contained in a conic. In Section 4 we provide a construction of generalized hyperfocused arcs which are not hyperfocused. Also, a classification of small generalized hyperfocused arcs is proved using the graph-theoretic concept of 1-factorizations of a complete graph, see Section 5.

2. Definitions and Notation

Let $PG(2,q)$ be the Desarguesian plane over $\mathbb{F}_q$, the finite field with q elements. A k-arc $\mathcal{K}$ in $PG(2,q)$ is a set of k points no three of which are collinear. Any line containing two points of $\mathcal{K}$ is said to be a *secant* of $\mathcal{K}$. A *blocking set of the secants of* $\mathcal{K}$ is a point set $\mathcal{B} \subset PG(2,q) \setminus \mathcal{K}$ having non-empty intersection with each secant of $\mathcal{K}$. As the number of secants of $\mathcal{K}$ is $k(k-1)/2$, the size of $\mathcal{B}$ is at least $k-1$. If this lower bound is attained, $\mathcal{B}$ is said to be *of minimum size*. Also, $\mathcal{B}$ is *linear* if it is contained in a line.

Arcs in $PG(2,q)$ admitting a linear blocking set of minimum size of their secants are called *hyperfocused arcs*. As mentioned in the Introduction, hyperfocused arcs exist only in $PG(2,q)$ for q even. Therefore in the whole paper we assume $q = 2^r$.

Throughout, we fix the following notation. Let (X_1, X_2, X_3) be homogeneous coordinates for points in $PG(2,q)$, and let ℓ_∞ be the line of equation $X_3 = 0$. Given a pair $A = (a,b)$ in $\mathbb{F}_q \times \mathbb{F}_q$, denote $\overline{A}$ the point in $PG(2,q)$ with coordinates $(a,b,1)$, and $\overline{A}_\infty$ the point $(a,b,0)$. Also, let φ_A be the projectivity

$$\varphi_A : (X_1, X_2, X_3) \mapsto (X_1 + a_1X_3, X_2 + a_2X_3, X_3)\,.$$

Clearly, φ_A is an elation with axis ℓ_∞, and conversely for any non-trivial elation φ with axis ℓ_∞ there exists $A \in \mathbb{F}_q \times \mathbb{F}_q$, $A \neq (0,0)$, such that $\varphi = \varphi_A$.

Given an additive subgroup G of $\mathbb{F}_q \times \mathbb{F}_q$, let $\mathcal{K}_G(P)$ be the orbit of the point $P \in PG(2,q) \setminus \ell_\infty$ under the action of the group

$$T_G := \{\varphi_A \mid A \in G\}\,.$$

Clearly, any two orbits $\mathcal{K}_G(P)$ and $\mathcal{K}_G(Q)$ with P, $Q \in PG(2,q) \setminus \ell_\infty$ are projectively equivalent. For brevity, write $\mathcal{K}_G$ for $\mathcal{K}_G(O)$, where $O = (0,0,1)$. Note that

$$\mathcal{K}_G := \{\overline{A} \mid A \in G\}\,.$$

A k-arc in $PG(2,q)$ coinciding with $\mathcal{K}_G(P)$ for some additive subgroup $G \subset \mathbb{F}_q \times \mathbb{F}_q$ and some $P \in PG(2,q) \setminus \ell_\infty$ will be called a *translation arc*.

3. Translation arcs

The following proposition shows that any translation arc is a hyperfocused arc.

Proposition 3.1. *Let $\mathcal{K}$ be a translation arc. Then there exists a blocking set of the secants of $\mathcal{K}$ of minimum size which is contained in ℓ_∞.*

Proof. Let G be an additive subgroup of $\mathbb{F}_q \times \mathbb{F}_q$ such that $\mathcal{K}$ is projectively equivalent to $\mathcal{K}_G$. To prove the assertion, it is enough to show that every secant of $\mathcal{K}$ meets ℓ_∞ in a point $\overline{C}_\infty$ for some $C \in G \setminus \{(0,0)\}$. For $A, B \in G$, $A \neq B$, let l_{AB} be the secant of $\mathcal{K}$ passing through $\overline{A}$ and $\overline{B}$. The intersection point of l_{AB} and ℓ_∞ is $\overline{(A+B)}_\infty$. Then the claim is proved, as $A+B$ is a non-zero element of G. $\square$

According to Proposition 3.1 groups G in both Examples 3.2 and 3.3 provide examples of translation arcs $\mathcal{K}_G$.

Example 3.2. (see [7]) For any additive subgroup H of $\mathbb{F}_q$, let $G = \{(\alpha, \alpha^2) \mid \alpha \in H\}$.

Example 3.3. For H any additive subgroup of $\mathbb{F}_q$ and i any positive integer with $(i, r) = 1$, let $G = \{(\alpha, \alpha^{2^i}) \mid \alpha \in H\}$. Note that the arc $\mathcal{K}_G$ is contained in a translation hyperoval (see [8, Ch. 8]).

The following result shows that any translation k-arc is either complete in $PG(2,q) \setminus \ell_\infty$ (i.e. it is not contained in any $(k+1)$-arc $\mathcal{K}' \subset PG(2,q) \setminus \ell_\infty$), or it is contained in a translation $2k$-arc.

Proposition 3.4. *Let $\mathcal{K}_G$ be a translation k-arc in $PG(2,q)$. Assume that there exists a point $\overline{A} \in PG(2,q)$ belonging to no secant of $\mathcal{K}_G$. Then the set $\mathcal{K}' := \mathcal{K}_G \cup \varphi_A(\mathcal{K}_G)$ is a translation $2k$-arc.*

Proof. Assume that $\overline{A_1}$, $\overline{A_2}$ and $\overline{A_3}$ are three collinear points in $\mathcal{K}'$. Clearly neither $\mathcal{K}_G$ nor $\varphi_A(\mathcal{K}_G)$ can contain all of such points. Also, as φ_A is an involution we may assume $\overline{A_1}, \overline{A_2} \in \mathcal{K}_G$, $\overline{A_3} \in \varphi_A(\mathcal{K}_G)$. Note that the elation $\varphi := \varphi_{A+A_3}$ acts on both $\mathcal{K}_G$ and $\varphi_A(\mathcal{K}_G)$. Then, as $\varphi(\overline{A_3}) = \overline{A}$, the secant of $\mathcal{K}_G$ through $\varphi(\overline{A_1})$ and $\varphi(\overline{A_2})$ contains $\overline{A}$, which is a contradiction. Hence $\mathcal{K}'$ is a $2k$-arc. It is actually a translation arc because $\mathcal{K}' = \mathcal{K}_{G'}$, where $G' = G \cup (G + A)$.

$\square$

Example 3.5. For q a square, let $\eta \in \mathbb{F}_q \setminus \mathbb{F}_{\sqrt{q}}$ such that $\eta^2 \in \mathbb{F}_{\sqrt{q}}$. Choose $b \in \mathbb{F}_{\sqrt{q}}$, $b \neq 1$, and let $G = \{(\alpha, \alpha^2) \mid \alpha \in \mathbb{F}_{\sqrt{q}}\}$, $A = (\eta, b\eta^2)$. Then by Proposition 3.4 the point set $\mathcal{K}' := \mathcal{K}_G \cup \varphi_A(\mathcal{K}_G)$ is a translation $(2\sqrt{q})$-arc. Note that half of the points of $\mathcal{K}'$ are contained in the conic of equation $X_2X_3 = X_1^2$, the other half in the conic $X_2X_3 = X_1^2 + (b+1)\eta^2X_3^2$.

Example 3.5 provides hyperfocused arcs which are not contained in any regular hyperoval. Actually, the existence of hyperfocused arcs which are neither contained in any hyperoval nor in any proper subplane of $PG(2,q)$ can be proved. The proof of such a result needs the following two lemmas.

Lemma 3.6. *Let $\mathcal{K}$ be a translation q-arc containing both points $(0,0,1)$ and $(1,1,1)$. Then there exist $\alpha,\beta\in\mathbb{F}_q$ and a positive integer i with $(i,r)=1$, such that*

$$\mathcal{K}=\{(x,y,1)\mid \alpha x+(\alpha+1)y+\beta x^{2^i}+(\beta+1)y^{2^i}=0\}.$$

Proof. Let $\psi_{\alpha\gamma}$ be the linear collineation

$$\psi_{\alpha,\gamma}:(X_1,X_2,X_3)\mapsto(\alpha X_1+(\alpha+1)X_2,\gamma X_1+(\gamma+1)X_2,X_3),$$

with $\alpha,\gamma\in\mathbb{F}_q$, and let $\mathcal{K}'=\psi_{\alpha,\gamma}(\mathcal{K})$. Choose α and γ in such a way that the two points on ℓ_∞ which belong to no secant of $\mathcal{K}'$ are $(1,0,0)$ and $(0,1,0)$. Note that $\mathcal{K}'$ contains $(0,0,1)$ and $(1,1,1)$. Also, for each $t\in\mathbb{F}_q$ there exists exactly one point P_t of $\mathcal{K}'$ on the line $X_2=tX_3$. Let F be the function on $\mathbb{F}_q$ such that $P_t=(F(t),t,1)$. As $\mathcal{K}'$ is a translation arc containing $(0,0,1)$, the set $\{(F(t),t)\mid t\in\mathbb{F}_q\}$ is an additive subgroup of $\mathbb{F}_q\times\mathbb{F}_q$. This implies $F(s+t)=F(s)+F(t)$ for any $s,t\in\mathbb{F}_q$. Theorem 8.41 in [8] yields $F(t)=t^{2^i}$ for some i with $(i,r)=1$, that is

$$\mathcal{K}'=\{(x,y,1)\mid x=y^{2^i}\},$$

whence

$$\mathcal{K}=\{(x,y,1)\mid(\alpha x+(\alpha+1)y)=(\gamma x+(\gamma+1)y)^{2^i}\}.$$

Then the assertion follows by letting $\beta=\gamma^{2^i}$. □

Lemma 3.7. *Assume that r has a proper divisor $s>2$, and let $q'=2^s$. Let $\mathcal{K}=\mathcal{K}_G$ with $G=\{(a,a^2)\mid a\in\mathbb{F}_{q'}\}$. Then there exist at most $\frac{r}{s}$ translation q-arcs containing $\mathcal{K}$.*

Proof. Let $\mathcal{I}$ be any translation arc of size q containing $\mathcal{K}$. Then by Lemma 3.6 there exist $\alpha,\beta\in\mathbb{F}_q$ with $\alpha\neq\beta$, and a positive integer i with $(i,r)=1$, such that

$$\alpha a+(\alpha+1)a^2+\beta a^{2^i}+(\beta+1)a^{2^{i+1}}=0,$$

for any $a\in\mathbb{F}_{q'}$. This means that the polynomial $g(T):=\alpha T+(\alpha+1)T^2+\beta T^{2^i}+(\beta+1)T^{2^{i+1}}$ must be divisible by $T^{q'}+T$. If $2^{i+1}<q'$ this can only happen for $g(T)\equiv 0$, that is $i=1$, $\beta=1$, $\alpha=0$. If $2^{i+1}=q'$, that is $i=s-1$, then $\alpha=1$, $\beta=0$. Finally, if $2^{i+1}>q'$, then also $2^i>q'$ as $(i,r)=1$. Write $i=us+v$ with u,v integers with $0\le v<s$. Then $2^i=(q'-1)^{2^u}2^v+2^v$, and $g(T)$ mod $T^{q'}+T$ is the polynomial $\alpha T+(\alpha+1)T^2+\beta T^{2^v}+(\beta+1)T^{2^{v+1}}$, which has to be the zero polynomial. This implies $\beta=1$, $\alpha=0$, $i\in\{s+1,2s+1,\ldots,(\frac{r}{s}-1)s+1\}$. Note that the arc defined by $i=s-1$, $\alpha=1$, $\beta=0$ coincides with that defined by $i=(\frac{r}{s}-1)s+1$, $\alpha=0$, $\beta=1$. Then the assertion follows. □

Now we are in a position to prove the following theorem.

Theorem 3.8. *Let $q=2^r$ be such that there r admits a proper divisor $s>2$. Then there exists a translation arc $\mathcal{K}$ in $PG(2,q)$ such that*

(a) *every point in $PG(2,q)\setminus\ell_\infty$ belongs to some secant of $\mathcal{K}$;*
(b) *$\mathcal{K}$ is not contained in any hyperoval;*
(c) *$\mathcal{K}$ is not contained in any proper subplane.*

Proof. Let $\mathcal{K}_G$ be as in Lemma 3.7, and let $\mathcal{I}_1, \ldots, \mathcal{I}_h$ be the translation q-arcs containing $\mathcal{K}_G$. Note that $h \leq \frac{r}{s}$ by Lemma 3.7. As there are exactly $q'(q'-1)/2$ secants of $\mathcal{K}_G$, the number of points in $PG(2,q) \setminus \ell_\infty$ contained in no secant of $\mathcal{K}_G$ is at least $q^2 - q({q'}^2 - q')/2 = q(2^r - 2^{2s-1} + 2^{s-1})$. On the other hand, the number of points in $\cup_{i=1,\ldots,h}\mathcal{I}_i$ is at most $\frac{qr}{s}$. It is straightforward to check that $2^r - 2^{2s-1} + 2^{s-1} > \frac{r}{s}$. Hence, there exists a point $\overline{A_1} \in PG(2,q) \setminus \ell_\infty$ which is contained neither in a $\mathcal{I}_i$ nor in a secant of $\mathcal{K}_G$. Define $G_1 = G + A_1$ and $\mathcal{K}_1 = \mathcal{K}_{G_1}$. If every point in $PG(2,q) \setminus \ell_\infty$ belongs to some secant of $\mathcal{K}_1$, let $\mathcal{K} := \mathcal{K}_1$. Otherwise choose a point $\overline{A_2}$ not belonging to any secant of $\mathcal{K}_1$ and let $G_2 = G_1 + A_2$, $\mathcal{K}_2 = \mathcal{K}_{G_2}$. Repeat the process until the arc $\mathcal{K}_i$ has the property that every point in $PG(2,q) \setminus \ell_\infty$ belongs to some secant of $\mathcal{K}_i$, and define $\mathcal{K} = \mathcal{K}_i$. Clearly, (a) is fulfilled by construction. Assume now that $\mathcal{K}$ is contained in a hyperoval $\mathcal{I}'$. By (a), $\mathcal{K}$ coincides with the points of $\mathcal{I}'$ not on ℓ_∞, that is $\mathcal{K}$ is one of the translation q-arcs containing $\mathcal{K}_G$. But this is impossible as $\mathcal{K}_1$ is not contained in any $\mathcal{I}_i$ by construction. Finally, (c) holds when s is chosen to be the maximum proper divisor of r. In fact, in this case the maximum order of a subplane of $PG(2,q)$ is 2^s, whereas $\#\mathcal{K} \geq 2^{s+1} > 2^s + 2$.

$\square$

Theorem 3.8 suggests that it might be hard to deal with the problem of characterizing hyperfocused arcs.

4. Generalized hyperfocused arcs

In this section we consider generalized hyperfocused arcs, that is arcs admitting a non-necessarily linear blocking set of minimum size. In [1] it is shown that an arc in $PG(2,q)$, q even, does not admit a non-linear blocking set of its secants of minimum size, provided that it is contained in a conic. The following theorem proves that k-arcs admitting non-linear blocking sets of size $k-1$ actually exist.

Theorem 4.1. *Let $\mathcal{K}$ be a translation k-arc, $k \geq 4$, and let φ be a homology with axis ℓ_∞ and centre not in $\mathcal{K}$. If the set $\mathcal{K}' = \mathcal{K} \cup \varphi(\mathcal{K})$ is an arc, then there exists a non-linear blocking set $\mathcal{B}$ of the secants of $\mathcal{K}'$ of minimum size.*

Proof. Assume that $(0,0,1) \in \mathcal{K}$, and let $\mathcal{K} = \mathcal{K}_G$, with G an additive subgroup of $\mathbb{F}_q \times \mathbb{F}_q$. Let $\overline{C}$ be the centre of φ. Define $\mathcal{B}$ as the subset of $2k-1$ points $PG(2,q)$ which comprises points $\overline{A}_\infty$, together with the centres of the homologies $\varphi\varphi_A$, with A ranging over $G \setminus \{(0,0)\}$. Let l_{PQ} be any secant of $\mathcal{K}'$. If both P and Q are either in $\mathcal{K}$ or in $\varphi(\mathcal{K})$, then l_{PQ} meets $\mathcal{B}$ in a point $\overline{A}_\infty$, for some $A \in G \setminus \{(0,0)\}$. Now assume that $P = \overline{A}$ and $Q = \varphi(\overline{B})$ for some $A, B \in G$. Then l_{PQ} passes through the centre of $\varphi\varphi_{A+B}$. This proves that $\mathcal{B}$ is a blocking set of the secants of $\mathcal{K}'$. As $\mathcal{B}$ has size $2k-1$ and is not contained in any line, the assertion is proved. $\square$

Example 4.2. Let $\mathcal{K} = \mathcal{K}_G$ with $G = \{(0,0),(0,1),(1,0),(1,1)\}$. Consider the homology

$$\varphi : (X_1, X_2, X_3) \mapsto (\lambda X_1 + a_1 X_3, \lambda X_2 + a_2 X_3, X_3)\,, \tag{4.1}$$

with

- $\lambda \in \mathbb{F}_q$, $\lambda \neq 0, 1$, $a_1, a_2 \in \mathbb{F}_q$;
- $\{a_1, a_2, a_1 + a_2\} \cap \{0, 1, \lambda, \lambda + 1\} = \emptyset$.

Then it is straightforward to check that $\mathcal{K}' = \mathcal{K} \cup \varphi(\mathcal{K})$ is an arc. A non-linear blocking set $\mathcal{B}$ of the secants of $\mathcal{K}'$ of minimum size is

$$\begin{aligned}\mathcal{B} = \ & \{(1,0,0),(0,1,0),(1,1,0),(a_1,a_2,1+\lambda),(a_1+\lambda,a_2,1+\lambda),\\ & (a_1,a_2+\lambda,1+\lambda),(a_1+\lambda,a_2+\lambda,1+\lambda)\}\,,\end{aligned}$$

which consists of the points of a subplane of $PG(2,q)$ of order 2.

The following result shows that a non-linear blocking set of minimum size of the secants of a k-arc cannot be an arc itself. Also, it will be useful for the classification of small generalized hyperfocused arcs which will be given in next section.

Proposition 4.3. *Let $\mathcal{B}$ be a blocking set of minimum size of the secants of a k-arc $\mathcal{K}$ in $PG(2,q)$, q even. Then any three points in $\mathcal{B}$ blocking the secants of a 3-arc contained in $\mathcal{K}$ are collinear.*

Proof. This proof relies on the idea of Segre's celebrated Lemma of Tangents [10]. Let P_1, P_2 and P_3 be any three distinct points in $\mathcal{K}$. For each $i \in \{1,2,3\}$, let $Q_i \in \mathcal{B}$ be collinear with P_j and P_k, where $j,k \in \{1,2,3\}$, $j = i+1 \pmod 3$, $k = i-1 \pmod 3$. It has to be proved that Q_1, Q_2 and Q_3 are collinear. Assume without loss of generality that $P_1 = (1,0,0)$, $P_2 = (0,1,0)$ and $P_3 = (0,0,1)$. For a point P distinct from P_i, $i = 1,2,3$, let α_P^1, α_P^2, α_P^3 be the elements of $\mathbb{F}_q$ such that

- $X_3 = \alpha_P^1 X_2$ is the line through P_1 and P,
- $X_1 = \alpha_P^2 X_3$ is the line through P_2 and P,
- $X_2 = \alpha_P^3 X_1$ is the line through P_3 and P.

It is straightforward to check that if P does not belong to the triangle with vertices P_1, P_2, P_3, then

$$\alpha_P^1 \alpha_P^2 \alpha_P^3 = 1\,. \tag{4.2}$$

Now, consider the set of secants of $\mathcal{K}$ passing through exactly one point among P_1, P_2 and P_3. Clearly, it coincides with the set which comprises the lines joining P_1, P_2 and P_3 to any point of $\mathcal{B} \setminus \{Q_1, Q_2, Q_3\}$, together with the lines through P_i and Q_i, $i = 1,2,3$. Hence,

$$\prod_{P \in \mathcal{K},\ P \neq P_1,P_2,P_3} \alpha_P^1 \alpha_P^2 \alpha_P^3 = \alpha_{Q_1}^1 \alpha_{Q_2}^2 \alpha_{Q_3}^3 \left(\prod_{Q \in \mathcal{B},\ Q \neq Q_1,Q_2,Q_3} \alpha_Q^1 \alpha_Q^2 \alpha_Q^3 \right).$$

Then by (4.2), $\alpha_{Q_1}^1 \alpha_{Q_2}^2 \alpha_{Q_3}^3 = 1$ holds. As q is even, this is equivalent to the collinearity of Q_1, Q_2 and Q_3 and the assertion is proved. □

5. Classification of small generalized hyperfocused arcs

The aim of this section if to classify the small arcs admitting blocking sets of minimum size for their secants. The linear case has already been settled in [7] and [5]. The main result of the section is the following.

Theorem 5.1. *Let $\mathcal{K}$ be a k-arc in $PG(2,q)$, q even, with $k \leq 10$. If there exists a minimal non-linear blocking set of the secants of $\mathcal{K}$, then $k = 8$ and $\mathcal{K}$ is projectively equivalent to the arc $\mathcal{K}'$ in Example 4.2.*

The proof of this result relies on a connection between blocking sets of the secants of an arc and 1-factorizations of complete graphs. For the sake of completeness, some basic definitions from graph theory are reported.

Let K_{2n} be the complete graph with $2n$ vertices. A 1-*factor* of K_{2n} is a set of vertex disjoint edges which cover the vertices of K_{2n}. An edge disjoint set of 1-factors covering the edges of K_{2n} is said to be a 1-*factorization* of K_{2n}. The set of vertices of K_{2n} will be denoted by $V(K_{2n})$.

Definition 5.2. *Let $\mathcal{F}$ be a 1-factorization of K_{2n}. An* embedding *of $\mathcal{F}$ in $PG(2,q)$ is an injective map $\psi : V(K_{2n}) \cup \mathcal{F} \to PG(2,q)$ such that*

i) *for any $i,j,k \in V(K_{2n})$, the points $\psi(i)$, $\psi(j)$, $\psi(k)$ are not collinear;*
ii) *for any $F \in \mathcal{F}$, the point $\psi(F)$ is collinear with $\psi(i)$ and $\psi(j)$, for every edge $(i,j) \in F$.*

Given an embedding ψ of a 1-factorization $\mathcal{F}$ of K_{2n} in $PG(2,q)$, the set $\psi(V(K_{2n}))$ is an arc, whereas $\psi(\mathcal{F})$ is a blocking set of minimum size of the secant of such arcs. The following equivalent formulation of Theorem 5.1 will be proved.

Theorem 5.3. *Let ψ be an embedding of a 1-factorization $\mathcal{F}$ of K_{2n} in $PG(2,q)$, q even, with $3 \leq n \leq 5$. If the points $\{\psi(F) \mid F \in \mathcal{F}\}$ are not collinear, then $n = 4$ and $\psi(V(K_{2n}))$ is projectively equivalent to the arc $\mathcal{K}'$ in Example 4.2.*

Assume that $V(K_{2n}) = \{1,2,\ldots,2n\}$, $n \geq 3$, and let $\mathcal{F} = \{F_1, F_2, \ldots, F_{2n-1}\}$ be a 1-factorization of K_{2n}. Let ψ be an embedding of $\mathcal{F}$ in $PG(2,q)$.

5.1. **Proof of Theorem 5.3 for $n = 3$.** As all the 1-factorizations of the complete graph with 6 vertices are isomorphic, we may assume that:

- $\psi(F_1)$ is the common point of the lines $\psi(1)\psi(2)$, $\psi(3)\psi(4)$, $\psi(5)\psi(6)$;
- $\psi(F_2)$ is the common point of the lines $\psi(1)\psi(3)$, $\psi(2)\psi(5)$, $\psi(4)\psi(6)$;
- $\psi(F_3)$ is the common point of the lines $\psi(1)\psi(4)$, $\psi(2)\psi(6)$, $\psi(3)\psi(5)$;
- $\psi(F_4)$ is the common point of the lines $\psi(1)\psi(5)$, $\psi(2)\psi(4)$, $\psi(3)\psi(6)$;
- $\psi(F_5)$ is the common point of the lines $\psi(1)\psi(6)$, $\psi(2)\psi(3)$, $\psi(4)\psi(5)$.

By Proposition 4.3 the following triples of points are collinear:

$$\psi(F_1), \psi(F_2), \psi(F_3), \qquad \psi(F_1), \psi(F_2), \psi(F_4), \qquad \psi(F_1), \psi(F_2), \psi(F_5)\,.$$

Then all points in $\{\psi(F) \mid F \in \mathcal{F}\}$ are collinear, which proves the assertion.

5.2. **Proof of Theorem 5.3 for $n = 4$.** There are 6 non-isomorphic 1-factorizations of K_8 (see e.g. [2]). From the proof of Theorem 5.3 in [5], it follows that 4 of them cannot be embedded in $PG(2, q)$. We are left with the following two cases.

Case 1: $\mathcal{F} = \{F_1, \ldots, F_7\}$ with

$$\begin{array}{ll} F_1 = \{(8,1),(2,3),(4,5),(6,7)\}, & F_2 = \{(8,2),(1,3),(4,6),(5,7)\}, \\ F_3 = \{(8,3),(1,2),(4,7),(5,6)\}, & F_4 = \{(8,4),(1,5),(2,6),(3,7)\}, \\ F_5 = \{(8,5),(1,4),(2,7),(3,6)\}, & F_6 = \{(8,6),(1,7),(2,4),(3,5)\}, \\ F_7 = \{(8,7),(1,6),(2,5),(3,4)\}. & \end{array}$$

Assume without loss of generality that $\psi(4) = (0, 0, 1)$, $\psi(5) = (0, 1, 1)$, $\psi(6) = (1, 0, 1)$, $\psi(7) = (1, 1, 1)$, that is $\{\psi(4), \psi(5), \psi(6), \psi(7)\}$ coincides with $\mathcal{K}_G$, with G as in Example 4.2. Then $\psi(F_1) = (0, 1, 0)$, $\psi(F_2) = (1, 0, 0)$ and $\psi(F_3) = (1, 1, 0)$. Now, note that by Proposition 4.3 the following triples of points are collinear:

$$\psi(F_4), \psi(F_5), \psi(F_1), \qquad \psi(F_4), \psi(F_6), \psi(F_2), \qquad \psi(F_4), \psi(F_7), \psi(F_3)\,.$$

Hence, if $\psi(F_4)$ lies on ℓ_∞, then the whole $\{\psi(F) \mid F \in \mathcal{F}\}$ is contained in a line. Now assume that $\psi(F_4) \notin \ell_\infty$.

Let φ be the linear collineation of $PG(2, q)$ such that $\varphi(\psi(4)) = \psi(8)$, $\varphi(\psi(5)) = \psi(1)$, $\varphi(\psi(6)) = \psi(2)$ and $\varphi(\psi(7)) = \psi(3)$. Clearly, φ fixes $\psi(F_1)$, $\psi(F_2)$, $\psi(F_3)$, and hence φ is a central collineation with axis ℓ_∞. The centre of φ is $\psi(F_4)$, which is assumed not to belong to ℓ_∞. Therefore, φ is as in Equation (4.1) for some $a_1, a_2, \lambda \in \mathbb{F}_q$. As $\psi(V(K_8)) = \mathcal{K}_G \cup \varphi(\mathcal{K}_G)$ is an arc, it is straightforward to check that

- $\lambda \in \mathbb{F}_q$, $\lambda \neq 0, 1$, $a_1, a_2 \in \mathbb{F}_q$;
- $\{a_1, a_2, a_1 + a_2\} \cap \{0, 1, \lambda, \lambda + 1\} = \emptyset$.

Then the assertion is proved.

Case 2: $\mathcal{F} = \{F_1, \ldots, F_7\}$ with

$$\begin{array}{ll} F_1 = \{(8,1),(2,3),(4,5),(6,7)\}, & F_2 = \{(8,2),(1,4),(3,6),(5,7)\}, \\ F_3 = \{(8,3),(1,6),(2,5),(4,7)\}, & F_4 = \{(8,4),(1,7),(2,6),(3,5)\}, \\ F_5 = \{(8,5),(1,2),(3,7),(4,6)\}, & F_6 = \{(8,6),(1,5),(2,7),(3,4)\}, \\ F_7 = \{(8,7),(1,3),(2,4),(5,6)\}. & \end{array}$$

By Proposition 4.3, any point $\psi(F_i)$ with $3 \leq i \leq 7$ is collinear with $\psi(F_1)$ and $\psi(F_2)$. Then all points in $\{\psi(F) \mid F \in \mathcal{F}\}$ are collinear, which proves the assertion.

5.3. **Proof of Theorem 5.3 for $n = 5$.** Define $\mathcal{T}^0_{\mathcal{F}}$ as the set of all triples $\{F_i, F_j, F_k\}$ such that $(i, j) \in F_k$, $(i, k) \in F_j$, $(j, k) \in F_i$, with i, j, k ranging over $V(K_{10})$. By Proposition 4.3, for any $\{F_i, F_j, F_k\} \in \mathcal{T}^0_{\mathcal{F}}$ the points $\psi(F_i)$, $\psi(F_j)$ and $\psi(F_k)$ are collinear.

Now define recursively a set $\mathcal{T}^i_{\mathcal{F}}$, $i \geq 1$, as follows: $\mathcal{T}^i_{\mathcal{F}}$ contains all the joins of two sets in $\mathcal{T}^{i-1}_{\mathcal{F}}$ sharing at least two elements of $\mathcal{F}$. Clearly, for any $\mathcal{A} \in \mathcal{T}^i_{\mathcal{F}}$, the points $\{\psi(F) \mid F \in \mathcal{A}\}$ are collinear. By the following lemma, all points in $\{\psi(F) \mid F \in \mathcal{F}\}$ are collinear, which completes the proof of Theorem 5.3.

Lemma 5.4. *For any 1-factorization $\mathcal{F}$ of K_{10}, there exists an integer i for which $\mathcal{T}^i_{\mathcal{F}}$ contains $\mathcal{F}$.*

The proof of Lemma 5.4 consists of a computer based investigation of all 396 non-isomorphic 1-factorizations of K_{10} ([2]). For the details of the proof the reader is referred to [13].

References

[1] A. Aguglia, G. Korchmáros and A. Siciliano, Minimal coverings of all chords of a conic in $PG(2, q)$, q even, *Simon Stevin*, to appear.

[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 (2004), pp. 195–212.

[8] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford (1998).

[9] L.D. Holder, The construction of Geometric Threshold Schemes with Projective Geometry, Master's Thesis, University of Colorado at Denver, 1997.

[10] B. Segre, Ovals in a finite projective plane, *Canad. J. Math*, Vol. 7 (1955), pp. 414–416.

[11] G. Simmons, Sharply Focused Sets of Lines on a Conic in $PG(2, q)$, *Congr. Numer.*, Vol. 73 (1990) pp. 181–204.

[12] F. Wettl, On the nuclei of a pointset of a finite projective plane, *J. Geom.*, Vol. 30 (1985), pp. 157–163.

[13] www.dipmat.unipg.it/~giuliet/triangles.tex

Dipartimento di Matematica Università di Perugia, 06123 Perugia, Italy

E-mail address: giuliet@dipmat.unipg.it, montanuc@dipmat.unipg.it