Contributions to Discrete Mathematics

Volume 3, Number 1, Pages 96–108
ISSN 1715-0868

ARCS IN DESARGUESIAN NETS

ANNALISA BEATO, GIORGIO FAINA, AND MASSIMO GIULIETTI

Dedicated to the centenary of the birth of Ferenc Kárteszi (1907–1989).

Abstract. A trivial upper bound on the size k of an arc in an r-net is $k \leq r+1$. It has been known for about 20 years that if the r-net is Desarguesian and has odd order, then the case $k = r+1$ cannot occur, and $k \geq r-1$ implies that the arc is contained in a conic. In this paper, we show that actually the same must hold provided that the difference $r - k$ does not exceed $\sqrt{k/18}$. Moreover, it is proved that the same assumption ensures that the arc can be extended to an oval of the net.

1. Introduction

An r-net of *order* n is an incidence structure Σ with n^2 points whose blocks, called *lines*, are partitioned into $r \geq 3$ parallel classes so that each class partitions the points of Σ and each two lines from different classes have precisely one common point. A net Σ is said to be Desarguesian if it is embedded in an affine plane $AG(2,q)$ coordinatized over the finite field with q elements $\mathbb{F}_q$.

A subset K of k points in Σ is said to be a k-arc if each pair of points of K is joined by a line, but no three points of K belong to the same line. The arc K will be said to be *proper* if each parallel class of Σ contains some secant of K. A trivial upper bound on the size of a k-arc is $k \leq r+1$. An $(r+1)$-arc in Σ is said to be a *hyperoval*, whereas an r-arc is said to be an *oval*. The *defect* Δ of a k-arc in an r-net is the difference $\Delta = r+1-k$. Ovals in Desarguesian r-nets of order q were first used by Simmons [25] in connection with a geometry based secret sharing scheme. For fixed r and q, the implementation of such a scheme needs an arc with the smallest defect as possible. This provides a motivation for investigating the minimum defect of a k-arc in a Desarguesian r-net of order q, and for classifying k-arcs with small defect (in particular, ovals and hyperovals). Any non-proper k-arc in an r-net is a proper k-arc with smaller defect in an r'-net with $r' < r$; therefore, throughout the paper we only deal with proper k-arcs.

2000 *Mathematics Subject Classification.* 51E20.

Key words and phrases. Desargusian net, complete arc, projective plane.

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.

Examples of ovals in Desarguesian r-nets of order q are provided by affinely regular polygons in $AG(2,q)$. Let $A_1A_2\dots A_d$ be a regular d-gon in the Euclidean plane. Kárteszi [15] called a d-gon $B_1B_2\dots B_d$ in an affine plane *(affinely) regular* if the bijection $A_i \mapsto B_i$ preserves all parallelisms between chords (i.e. sides, and diagonals), that is,

$$A_iA_j \parallel A_kA_m \Longleftrightarrow B_iB_j \parallel B_kB_m\,,$$

for all $1 \le i < j \le d$, and $1 \le k < m \le d$. Kárteszi's idea was developed by his Ph.D. students Nguyen Mong Hy [14] and G. Korchmáros [16, 18, 17, 19]. A useful geometric property pointed out by Korchmáros [16] and independently by Van de Craats and Simonis [27] is that every affinely regular d-gon is inscribed in a conic, see also the survey papers [8, 20].

Simmons only considered Desarguesian nets of odd order, where hyperovals do not exist [2]. Desarguesian nets of odd order holding an oval were classified by Beutelspacher and Wettl [1], whose result was based on a previous paper by Wettl [28]: any oval in a Desarguesian r-net is contained in a conic $\mathcal{C}$ of $AG(2,q)$, and it consists of the points of a coset of the abelian group $(\mathcal{C},\oplus)$ arising from the conic (the precise definition of the group law $\oplus$ is recalled in Section 4). Therefore, a Desarguesian r-net with ovals exists if and only if r divides q, $q-1$ or $q+1$; in addition, if p^2 does not divide r, then the oval must coincide with an affinely regular polygon in $AG(2,q)$. Szőnyi's [21] proved that proper k-arcs with defect $\Delta = 2$ and $k \ge 28$ can be uniquely extended to an oval, provided that q is odd. Furthermore, if the order of magnitude of Δ does not exceed $\sqrt{q}/8$, then either $k \le (q+1)/2$ or $r = q+1$. It should be noted that the results in [2, 21, 28] come from more general results about internal nuclei. Let A be a pointset in the projective plane $PG(2,q)$. A point $P \in A$ is said to be an internal nucleus of A if each line through P meets A in at most two points including P. This notion was introduced for sets of size $q+2$ by Bichara and Korchmáros [2] and generalized by Wettl [28]. If K is a proper k-arc with defect Δ in a Desarguesian net, and N denotes the set of points of the infinite line of $AG(2,q)$ which do not belong to any secant of K, then $A = K \cup N$, viewed as a subset of the projetive plane $PG(2,q)$, is clearly a set of size $q+2-\Delta$ and the k points of K are internal nuclei of A.

In 1997, Holder [13] extended Simmons's investigation to Desarguesian nets of even order, where hyperovals can exist. However, classification of Desarguesian nets holding a hyperoval seems to be an involved problem. In a recent paper [3], Cherowitzo and Holder provided the classification of small hyperfocused arcs, and constructed new examples. Further examples are provided in [9]. The problem of the existence of r-nets of fixed order n with either ovals or hyperovals has been recently investigated in [4, 5, 6, 7] as well.

In this paper, some generalizations of the classifications in [1] and [21] are obtained. In particular, it is shown that if q is odd and the defect of the arc is small with respect to its size, then the arc is contained in an oval.

For most values of k and Δ, this can be read as a non-existence result of a proper k-arc of defect Δ in a Desarguesian r-net; in other cases, this gives a Segre-type embedding result.

Theorem 1.1. *Let K be a proper k-arc with defect $\Delta = 3$ in a Desarguesian r-net Σ of odd order q. Assume that either $k > 145$, or $k > 108$ and $p > 5$ hold. Then K is contained in a coset of size $r = k + 2$ of the abelian group arising from a conic of $AG(2, q)$. In particular, r divides $q, q - 1$ or $q + 1$.*

Theorem 1.2. *Let $q = p^s$, with p an odd prime. Let k and Δ be positive integers. Assume that one of the following holds:*

(i) $\Delta < \sqrt{k/18}$,
(ii) $\Delta < \sqrt{k}/4$ *and* $p > 2\Delta$.

Then any proper k-arc K with defect Δ in a Desarguesian r-net Σ of odd order q is contained in a coset of size $r = k + \Delta - 1$ of the abelian group arising from a conic of $AG(2, q)$. In particular, r divides $q, q - 1$ or $q + 1$.

For r-nets of small order, the following result can provide an improvement on Theorem 1.2.

Theorem 1.3. *Let q be odd, and let k and Δ be positive integers. Let e be the maximum integer such that all the three following conditions hold: $k > e(\Delta + 4e)$, $k > e(2\Delta - e)$, and $k > (9/2)e^2$. Assume that $e \geq 3$. If*

$$k > \frac{2}{d}(q + 1) + \frac{2(d - 1)(d - 2)}{d}\sqrt{q}$$

holds for any integer d with $e < d \leq 2\Delta$, then any proper k-arc K with defect Δ in a Desarguesian r-net Σ of odd order q is contained in a coset of size $r = k + \Delta - 1$ of the abelian group arising from a conic of $AG(2, q)$. In particular, r divides $q, q - 1$ or $q + 1$.

For q even, Theorem 6 in [21] yields that every arc with defect $\Delta \leq q/2 - 1$ has size at most $q/2$. Here the following result is proved for the case $\Delta = 3$.

Theorem 1.4. *Let K be a proper k-arc with defect $\Delta = 3$ in a Desarguesian net Σ of even order q. Then either K is contained in a hyperoval of Σ, or in a $(k + 1)$-arc with defect 2, or*

$$k \leq \frac{q + 1}{3} + \frac{2}{3}\sqrt{q}.$$

The key tool for proving our results is the algebraic envelope of a k-arc in a Desarguesian net, which is defined in Section 2. For q odd, some results of independent interest on the number of multitangents of an irreducible plane algebraic curve are needed, see Theorems 3.2 and 3.5 in Section 3. Finally, Theorems 1.1-1.4 are proved in Section 4.

2. The algebraic envelope of a k-arc in a Desarguesian net

The idea of associating an algebraic curve to a k-arc in a Desarguesian projective plane $PG(2,q)$ goes back to Segre. Wettl [28] showed that when the arc is an arc in an r-net, then this algebraic curve has a component of small degree, see Proposition 2.1 below. This is the key tool for investigating arcs with small defect in Desarguesian nets.

Throughout this section we assume that K is a proper k-arc of defect Δ in a Desarguesian r-net of order q. It is also assumed that $k \geq 3$. Without loss of generality, we identify K with a set of k points in the affine plane $AG(2,q)$ no three of which collinear, and such that the number of directions of the secants of K is precisely $k+\Delta-1$. Embed $AG(2,q)$ in the projective plane $PG(2,q)$, and denote ℓ_∞ the line of $PG(2,q)$ corresponding to the infinite line of $AG(2,q)$. With a little abuse of notation, the image of K by this embedding will be still denoted by K.

Let $M(K)$ denote the set of points on ℓ_∞ which are collinear with two points of K. Then $\Delta = |M(K)| - k + 1$. As a matter of terminology, any tangent to K meeting ℓ_∞ in a point of $M(K)$ is said to be *special*. Clearly the number of special tangents through a point of K is equal to Δ.

Consider the set $A = K \cup (\ell_\infty \setminus M(K))$. It was already noted in the Introduction that the internal nuclei of A are precisely the points of K. Also, the tangents to A are the special tangents to K. Then Theorem 4 in [28] reads as follows.

Proposition 2.1. *Let K be a proper k-arc in a Desarguesian r-net of order q, embedded in $PG(2,q)$. Assume that $k \geq 3$. Then the $k\Delta$ special tangents to K belong to an algebraic envelope Γ with the following properties:*

(1) *for q even, the class of Γ is Δ;*
(2) *for q odd,*
  (i) *the class of Γ is 2Δ;*
  (ii) *if $\mathcal{L}_P$ is the pencil of lines with vertex $P \in K$, and m is a special tangent at P, then the intersection multiplicity $I(m, \mathcal{L}_P \cap \Gamma)$ of $\mathcal{L}_P$ and Γ at m is two;*
  (iii) *Γ may contain components of multiplicity at most two, but does not consist entirely of double components.*

Throughout the paper, the algebraic curve corresponding to Γ in Proposition 2.1, that is, the algebraic curve consisting of points whose coordinates are the Plücker coordinates of the lines of Γ, will be denoted as $\mathcal{X}(K)$, and will be said to be the *algebraic envelope* of K.

A k-arc is said to be *complete* in its r-net if it is maximal with respect to set theoretical inclusion. Note that the k-arc K is complete in its Desarguesian r-net if and only if there is no point Q in $PG(2,q) \setminus \ell_\infty$ such that $K \cup Q$ is an arc and $M(K \cup \{Q\}) = M(K)$.

Proposition 2.2. *Let K be a proper k-arc in a Desarguesian r-net, and let $\mathcal{X}(K)$ be the algebraic envelope of K.*

(1) *If K is complete (in its r-net), then $\mathcal{X}(K)$ has no $\mathbb{F}_q$-rational linear component.*
(2) *If K is complete (in its r-net) and $k > 2$, then $\mathcal{X}(K)$ has no linear component.*
(3) *If either q is even or $k > \Delta$, then $\mathcal{X}(K)$ has no non-$\mathbb{F}_q$-rational component.*

Proof.

(1) Let ℓ be an $\mathbb{F}_q$-rational linear component of $\mathcal{X}(K)$. Let Q be the point whose coordinates are the Plücker coordinates of ℓ. Then clearly $K \cup \{Q\}$ is a $(k+1)$-arc with $M(K \cup \{Q\}) = M(K)$.
(2) Any linear component ℓ of $\mathcal{X}(K)$ contains at least k $\mathbb{F}_q$-rational points. As $k > 2$, ℓ is $\mathbb{F}_q$-rational. Then the assertion follows from (1).
(3) Assume that $\mathcal{X}_1$ is a non-$\mathbb{F}_q$-rational component of $\mathcal{X}(K)$ of degree d. Then the image $\mathcal{X}_2$ of $\mathcal{X}_1$ via the Frobenius map $(X_0, X_1, X_2) \mapsto (X_0^q, X_1^q, X_2^q)$ is another non-$\mathbb{F}_q$-rational component of $\mathcal{X}(K)$ of degree d. Then every $\mathbb{F}_q$-rational point of $\mathcal{X}_1$ is a singular point of $\mathcal{X}(K)$. This is impossible when q is even, as every point corresponding to a tangent to K is a non-singular point of $\mathcal{X}(K)$. Assume then that q is odd and that $k > \Delta$. Clearly, $2d \leq 2\Delta$, whence $k > d$. Note that $\mathcal{X}_1$ has at least d $\mathbb{F}_q$-rational points on every line corresponding to a point of K. This gives $kd > d^2$ common points of $\mathcal{X}_1$ and $\mathcal{X}_2$, which is a contradiction.

□

3. On the number of multitangents of a plane algebraic curve

The aim of this section is to provide an upper bound on the number of multitangents of an irreducible plane algebraic curve of even degree, see Theorems 3.2 and 3.5 below. This will be useful for investigating the algebraic envelope of a k-arc in a Desarguesian r-net of odd order.

Let $\mathcal{X} : F(X_0, X_1, X_2)$ be an irreducible plane curve defined over an algebraically closed field of characteristic p. The Gauss map of $\mathcal{X}$ is the rational map

$$\pi_{\mathcal{X}} = (F_{X_0} : F_{X_1} : F_{X_2}).$$

To every non-singular point P of $\mathcal{X}$, the Gauss map associates the Plücker coordinates of the tangent line of $\mathcal{X}$ at P. If the degree d of $\mathcal{X}$ is greater than 1, then $\pi_{\mathcal{X}}$ is not constant, and the image $\pi_{\mathcal{X}}(\mathcal{X})$ is an irreducible plane curve, called the dual curve $\mathcal{X}^*$ of $\mathcal{X}$. If the characteristic p is equal to 0, then $\mathcal{X}^*$ is never a line. On the other hand, when $p > 0$ the degree d^* of $\mathcal{X}^*$ can be equal to 1, and in this case $\mathcal{X}$ is said to be a *strange* curve. A conic in characteristic 2 is an example of a strange curve.

Some results on the Gauss map in positive characteristic are summarized in Proposition 3.1 below, see e.g. [12, Section 5.11].

Proposition 3.1. *Let $\mathcal{X}$ be a plane algebraic curve, and let $\mathcal{X}^*$ be its dual curve.*

(1) *If $p > d$, then $\mathcal{X}$ is not strange.*
(2) *Let $\mathcal{X}$ be a non-strange curve. If $\mathcal{X}$ is not the locus of its singular points and its inflections, then*
 (i) *$\mathcal{X}^*$ is birationally equivalent to $\mathcal{X}$,*
 (ii) *$(\mathcal{X}^*)^* = \mathcal{X}$ holds,*
 (iii) *the degree d^* of $\mathcal{X}^*$ satisfies $d^* \leq d(d-1)$.*
(3) *If $p > d$, then $\mathcal{X}$ is not the locus of its singular points and its inflections.*

Throughout the rest of this section, we assume that d is even and greater than 2, and that $\mathcal{X}$ is not strange. Let N_1 be the number of singular points of $\mathcal{X}$, and N_2 the number of lines that are tangents to $\mathcal{X}$ in $d/2$ distinct points. We recall that for an irreducible plane algebraic curve $\mathcal{X}$,

$$g + \sum_{P \in \mathcal{X}} \frac{m_P(m_P - 1)}{2} \leq \frac{(d-1)(d-2)}{2} \tag{3.1}$$

holds, where g denotes the genus of $\mathcal{X}$ and m_P is the multiplicty of P as a point of $\mathcal{X}$. As the genus of any algebraic curve is a non-negative integer, clearly

$$N_1 \leq \frac{(d-1)(d-2)}{2}$$

holds. Any tangent to $\mathcal{X}$ in $d/2$ distinct points corresponds to a $\frac{d}{2}$-fold point in $\mathcal{X}^*$. Then, (3.1) implies

$$\frac{d}{4}\left(\frac{d}{2} - 1\right) N_2 \leq \frac{(d^*-1)(d^*-2)}{2}.$$

Taking into account Proposition 3.1, the following inequality can be easily achieved.

Theorem 3.2. *Let $\mathcal{X}$ be a non-strange curve of even degree $d > 2$. If $\mathcal{X}$ is not the locus of its singular points and its inflections, then*

$$N_1 + N_2 \leq \frac{9}{2}d^2 - \frac{3}{2}d - 7 - \frac{4}{d}.$$

If the characteristic p is greater than d, Theorem 3.2 can be significantly improved. Let $\mathcal{B}$ be the set of branches of $\mathcal{X}$. For a branch $\gamma \in \mathcal{B}$, let r_γ denote the order, and s_γ denote the class of γ. The center P_γ of a branch γ or order r_γ is a t-fold point for $\mathcal{X}$ with $t \geq r_\gamma$. If γ is the only branch centered at P_γ, then equality holds; moreover, $r_\gamma + s_\gamma$ is the intersection multiplicity at P_γ of $\mathcal{X}$ and the unique tangent line of $\mathcal{X}$ at P_γ. The integer sequence $(0, r_\gamma, r_\gamma + s_\gamma)$ is called the *order sequence at γ with respect to the linear series cut out by lines.*

Let γ' be the image of γ by the Gauss map $\pi_{\mathcal{X}}$. The following is a classical result, see e.g. [24, II.35], which also holds when $p > d$, see [12, Section 5.12, Exercise 7].

Proposition 3.3. *Let γ be any branch of $\mathcal{X}$. If $p > d$, then*

$$r_\gamma = s_{\gamma'}, \qquad s_\gamma = r_{\gamma'}.$$

Now we are in a position to provide a precise formula for the degree of the dual curve.

Proposition 3.4. *Let g be the genus of $\mathcal{X}$. If $p > d$, then the degree of the dual curve is*

$$d^* = 2g - 2 + 2d - \epsilon,$$

where

$$\epsilon = \sum_{\gamma\in\mathcal{B}} (r_\gamma - 1).$$

Proof. By Proposition 3.1, the Gauss map is a birational isomorphism. This yields that the genus of $\mathcal{X}^*$ is equal to g. Since $p > d$, $\mathcal{X}$ is not the locus of its singular points and its inflections. Proposition 3.3 implies that the same holds for $\mathcal{X}^*$. Let R (resp. R^*) be the ramification divisors of $\mathcal{X}$ (resp. $\mathcal{X}^*$) with respect to the linear series cut out by lines, see [26]. We compute the orders of R and R^*. By [26, Corollary 1.7], the hypothesis on the characteristic p ensures that the weight of a branch γ in R is $2r_\gamma + s_\gamma - 3$, while the weight of γ' in R^* is $2s_\gamma + r_\gamma - 3$.

The following equalities are then obtained:

$$\sum_{\gamma\in\mathcal{B}} (2r_\gamma + s_\gamma - 3) = 3(2g-2) + 3d,$$
$$\sum_{\gamma\in\mathcal{B}} (2s_\gamma + r_\gamma - 3) = 3(2g-2) + 3d^*.$$

Then the claim follows from straightforward computation. □

Theorem 3.5. *If $p > d > 2$, d even, then*

$$N_1 + N_2 \leq 4(d^2 - 9).$$

Proof. Any tangent to $\mathcal{X}$ at $d/2$ distinct points corresponds to a $d/2$-fold point of $\mathcal{X}^*$. Also, any branch of positive class s corresponds to a branch of order s in $\mathcal{X}^*$. Then, (3.1) implies

$$\frac{d}{4}\left(\frac{d}{2} - 1\right) N_2 + \delta \leq \frac{(d^*-1)(d^*-2)}{2} - g,$$

where $\delta = \sum_{\gamma\in\mathcal{B}}(s_\gamma - 1)$. Note that

$$\delta = 3d^* - 3d + \epsilon.$$

Therefore

$$\frac{d}{4}\left(\frac{d}{2} - 1\right) N_2 \leq \frac{(d^*-1)(d^*-2)}{2} - g - 3d^* + 3d - \epsilon.$$

Since $\epsilon \leq 3(g-1)+(3/2)d$ and $d>3$, the maximum possible right hand side correspond to $\epsilon = 0$ and $d^* = 2g-2+2d$. Then

$$\frac{d}{4}\left(\frac{d}{2}-1\right)N_2 \leq \frac{(2g+2d-3)(2g+2d-4)}{2} - g - 3(2g-2+2d)+3d,$$

whence

$$\frac{d}{2}\,(d-2)\,N_2 \leq 4g^2+4g(2d-7)+12-6d,$$

that is,

$$\frac{d}{16}(d-2)N_2 \leq g^2+g(2d-7)+(d-2)(d-3).$$

Taking into account that $g \leq (d-1)(d-2)/2 - N_1$, we obtain

$$\frac{d}{16}(d-2)N_2 \leq \frac{d(d-2)(d^2-9)}{4} - N_1\left(d^2-d-5-N_1\right).$$

Since

$$N_1 \leq \frac{(d-1)(d-2)}{2},$$

we have

$$\frac{d}{16}(d-2)N_2 \leq \frac{d(d-2)(d^2-9)}{4} - N_1\left(d^2-d-5-\frac{(d-1)(d-2)}{2}\right),$$

whence

$$\frac{d}{16}(d-2)N_2 \leq \frac{d(d-2)(d^2-9)}{4} - N_1\left(\frac{d^2+d-12}{2}\right).$$

Finally,

$$N_2 + 8N_1\left(\frac{d^2+d-12}{d(d-2)}\right) \leq 4(d^2-9)$$

holds, and the claim follows from straightforward computation. □

4. Proof of the main results

We keep the notation of the previous sections. In particular, K is a proper k-arc of defect Δ in a Desarguesian r-net of order q.

Lemma 4.1. *Let q be odd, and let $\mathcal{C}$ be any non-linear non-double component of $\mathcal{X}(K)$. If $k > 2\Delta+1$, then $\mathcal{C}$ is not strange, and $(\mathcal{C}^*)^* = \mathcal{C}$ holds.*

Proof. Let s be the number of lines corresponding to points of K intersecting $\mathcal{C}$ in $d = deg(\mathcal{C})$ distinct points. Then $\mathcal{C}$ has at least sd points in common with a curve of degree $2\Delta - d$, namely the curve obtained from $\mathcal{X}(K)$ by dismissing $\mathcal{C}$. Therefore, by Bézout's Theorem, $s \leq 2\Delta - d$ holds. As $d \geq 2$, the hypothesis $k > 2\Delta+1$ ensures the existence of at least three tangent lines to $\mathcal{C}$ corresponding to points of K. As no three points of K are collinear, these tangent lines are not concurrent. This proves that $\mathcal{C}$ is not strange. Also, $\mathcal{C}$ is not the locus of its singular points and of its inflections by (ii) in Proposition 2.1. Then the assertion follows from Proposition 3.1. □

Lemma 4.2. *Let q be odd. If $k > 2\Delta - 1$, then $\mathcal{X}(K)$ does not contain any non-double line.*

Proof. Let ℓ be a non-double linear component of $\mathcal{X}(K)$. Then the intersection points of ℓ and the k lines corresponding to the points of K must belong to a curve of degree $2\Delta - 1$, namely the curve obtained from $\mathcal{X}(K)$ by dismissing ℓ. As such intersection points are collinear, $k \leq 2\Delta - 1$ must hold. □

Lemma 4.3. *Let q be odd, and assume that $\mathcal{X}(K)$ consists of double components and of $s > 1$ conics. Then $k \leq 4\Delta$.*

Proof. Let $\ell_1, \ldots, \ell_k$ be the lines corresponding to the points of K. Let n_i be the number of points on ℓ_i that are not tangency point with any of the s conics. Then we have

$$n_1 + n_2 + \ldots + n_k$$

singular points on the union of the s conics. As the number of singular points of a (non-necessarily irreducible) plane curve of degree d is at most $\binom{d}{2}$ (see e.g. [10]), $n_1 + \ldots + n_k \leq \binom{2s}{2}$ holds. On the other hand, for each i we have $s - n_i$ tangent conics to ℓ_i. That is, ℓ_i correspond to an intersection point of $\binom{s-n_i}{2}$ pairs of dual conics. Therefore

$$\binom{s-n_1}{2} + \ldots + \binom{s-n_k}{2} \leq 4\binom{s}{2}.$$

As $\binom{s-n_i}{2} \geq s - n_i - 1$ we obtain

$$n_1 + (s - n_1 - 1) + \ldots + n_k + (s - n_k - 1) \leq \binom{2s}{2} + 4\binom{s}{2},$$

that is,

$$k(s-1) \leq 4s(s-1),$$

whence

$$k \leq 4s \leq 4\Delta.$$

□

Lemma 4.4. *Let q be odd. Assume that $\mathcal{X}(K)$ has a non-double component of odd degree d. Then*

$$k \leq d(2\Delta - d) \leq \Delta^2.$$

Proof. Let $\mathcal{C}$ be a non-double component of $\mathcal{X}(K)$ of odd degree d. Then any line corresponding to a point of K contains at least one intersection point of $\mathcal{C}$ and a curve of degree $2\Delta - d$, namely the curve obtained from $\mathcal{X}(K)$ by dismissing $\mathcal{C}$. Therefore by Bézout's Theorem, $k \leq d(2\Delta - d)$ holds. Then the claim follows. □

Lemma 4.5. *Let q be odd. Assume that $\mathcal{X}(K)$ has precisely one non-double component $\mathcal{C}$ of degree $d > 2$. Then*

$$k \leq 18\Delta^2 - 3\Delta - 7 - \frac{2}{\Delta}.$$

If in addition $p > d$, then

$$k \leq 4(4\Delta^2 - 9).$$

Proof. If d is odd, then the assertion follows from Lemma 4.4. Assume then that d is even. As $\mathcal{C}$ is the unique non-double component of $\mathcal{X}(K)$, any line corresponding to a point of K is either a tangent to $\mathcal{C}$ at $d/2$ points, or contains a double point of $\mathcal{C}$. Then the assertions follow from Theorems 3.2 and 3.5, taking into account that $d \leq 2\Delta$. □

Lemma 4.6. *Let q be odd. Assume that $\mathcal{X}(K)$ has more than one non-double components $\mathcal{C}$, all of which are of even degree. Then*

$$k \leq 18\Delta^2.$$

If in addition $p > d$, then

$$k \leq 16\Delta^2.$$

Proof. By Lemma 4.3, we can assume that there exists a non-double component $\mathcal{C}$ of $\mathcal{X}(K)$ of (even) degree d with $2 < d \leq 2\Delta - 2$. Let $\mathcal{R}$ be the set of lines ℓ corresponding to points of K and containing at least one point P with $I(P, \ell \cap \mathcal{C}) = 1$. As d is even, on each line in $\mathcal{R}$ there are at least two points P with $I(P, \ell \cap \mathcal{C}) = 1$. Then, arguing as in the proof of Lemma 4.4, we obtain $\mid \mathcal{R} \mid \leq d(2\Delta - d)/2$. Any line corresponding to a point in K but not in $\mathcal{R}$, is either a tangent to $\mathcal{C}$ at $d/2$ points, or contains a double point of $\mathcal{C}$. Then Theorem 3.2 yields

$$k \leq \frac{d}{2}(2\Delta - d) + \frac{9}{2}d^2 \leq d(\Delta + 4d) \leq 18\Delta^2.$$

If $p > d$, then by Theorem 3.5 we obtain

$$k \leq \frac{d}{2}(2\Delta - d) + 4d^2 \leq d(\Delta + \frac{7}{2}d) \leq 16\Delta^2.$$

□

The next step is to prove that, for q odd, an arc in a Desarguesian net with small defect whose algebraic envelope consists of double components and of a conic can actually be extended to an oval. For this purpose, a known result on the abelian group arising from a conic in an affine plane is needed, see e.g. [28]. Let $\mathcal{C}$ be a conic in $AG(2, q)$. Fix a point $Q_0 \in \mathcal{C}$, and consider the following binary operation on the set of points of $\mathcal{C}$:

$$Q_1 \oplus Q_2 = Q_3 \iff Q_0Q_3 \parallel Q_1Q_2$$

(when $Q_i = Q_j$ by the line Q_iQ_j we mean the tangent line of $\mathcal{C}$ at Q_i). Then $(\mathcal{C}, \oplus)$ is an abelian group, whose neutral element is Q_0. It may be noted that $(\mathcal{C}, \oplus)$ is isomorphic to the additive (or the multiplicative) group of the groundfield, when $\mathcal{C}$ is a parabola (or a hyperbole). Also, if $\mathcal{C}$ is an ellipse, then $(\mathcal{C}, \oplus)$ is isomorphic to a subgroup of the multiplicative group of a quadratic extension of the groundfield. So for a hyperbole (or an ellipse) the group $(\mathcal{C}, \oplus)$ is cyclic, but this holds true for a parabola as far as the groundfield is a finite field of prime order.

The next lemma is a trivial consequence of Kneser's theorem (see also [22, 23]).

Lemma 4.7 ([22, Theorem 2]). *Let D be a non-empty subset of a finite abelian group $(G,+)$. If $\mid D+D \mid < 3/2 \mid D \mid$, then $D+D$ is a coset of a subgroup H of $(G,+)$ (and D is also contained in a coset of H).*

Proposition 4.8. *Let q be odd, and assume that $\mathcal{X}(K)$ consists of double components and of a conic. If $k > 2\Delta - 2 > 0$, then K can be extended to a $(k+\Delta-1)$-arc with defect 1, consisting of the points of a coset of the abelian group $(\mathcal{C},\oplus)$, with $\mathcal{C}$ a conic of $AG(2,q)$.*

Proof. Let $\mathcal{X}(K)$ consist of double components and of a conic $\mathcal{Y}$. Then each line corresponding to a point of K is a tangent to $\mathcal{Y}$. That is, K is contained in the dual curve $\mathcal{Y}^*$ of $\mathcal{Y}$. As $p > 2$, the curve $\mathcal{Y}^*$ is a conic. Let $\mathcal{C} = \mathcal{Y}^* \cap AG(2,q)$. Then K can be viewed as a non-empty subset of the finite abelian group $(\mathcal{C},\oplus)$. Note that the set $\{P_i \oplus P_j \mid P_i, P_j \in K, P_i \neq P_j\}$ corresponds to the set of $k+\Delta-1$ directions determined by the secants of K. Note that $k > 2\Delta-2$ is equivalent to $\mid K \oplus K \mid < 3/2 \mid K \mid$. Then Lemma 4.7 yields that $K \oplus K = H \oplus Q$ for some subgroup H of size $k+\Delta-1$, and some point $Q \in \mathcal{C}$. Then, for any $P \in K$, we have

$$K \oplus P \subseteq K \oplus K = H \oplus Q,$$

that is, K is contained in a coset $K' = H \oplus (Q \ominus P)$ of size $k+\Delta-1$. As clearly $\mid K' \oplus K' \mid = \mid K' \mid$, we have that K' is an arc of defect 1, whence the assertion. □

Now we are in a position to prove the main results of the paper.

Proof of Theorem 1.1. Note that if $\mathcal{X}(K)$ has a line as a component, then K is contained in an arc of defect 2, and hence in an oval as $k > 28$. Note also that by Proposition 4.8, it is enough to show that $\mathcal{X}(K)$ consists of double components and of a conic. If $\mathcal{X}(K)$ consists of conics, this is guaranteed by Lemma 4.3. By Lemma 4.5, the envelope $\mathcal{X}(K)$ cannot be an irreducible sextic curve. Also, $\mathcal{X}(K)$ cannot consist of two cubic curves by Lemma 4.4. We are left with the case where $\mathcal{X}(K)$ splits into a conic $\mathcal{C}$ and a quartic curve $\mathcal{Q}$. The number of lines corresponding to points of K and containing points from both $\mathcal{C}$ and $\mathcal{Q}$ is at most 4. Then there are at least 104 lines that are either bitangent to $\mathcal{Q}$ or contain some singular points of $\mathcal{Q}$. But this is impossible by Theorem 3.5. □

Proof of Theorem 1.2. The assertion follows from Lemmas 4.4, 4.5, and 4.6, together with Proposition 4.8. □

Proof of Theorem 1.3. Assume on the contrary that K is not contained in an oval. By Proposition 4.8, the envelope $\mathcal{X}(K)$ does not consist of double components and of a conic. Taking into account Lemmas 4.2, 4.3 and 4.4, we have that $\mathcal{X}(K)$ has at least one non-double component $\mathcal{C}$ of degree d with $4 \leq d \leq 2\Delta$. By the proofs of Lemmas 4.4, 4.5 and 4.6, the conditions on k rule out the possibility that all non-double components have degree less than or equal to e. Whence $d > e$ can be assumed. Note that $\mathcal{C}$ has at least $kd/2$ $\mathbb{F}_q$-rational points. Also, $\mathcal{C}$ is $\mathbb{F}_q$-rational by (3) of Proposition 2.2. By [11, Corollary 2.30], then we have

$$\frac{kd}{2} \leq q + 1 + (d-1)(d-1)\sqrt{q},$$

a contradiction. □

Proof of Theorem 1.4. If K is not complete, then the claim is straightforward. Then it can be assumed that $\mathcal{X}(K)$ has no linear components, that is, $\mathcal{X}(K)$ is an irreducible cubic curve. It is well known that any irreducible cubic curve defined over $\mathbb{F}_q$ can have at most $q + 1 + 2\sqrt{q}$ points, see e.g. [11]. As $\mathcal{X}(K)$ has at least $3k$ $\mathbb{F}_q$-rational points, the claim follows. □

Acknowledgements

The authors would like to thank G. Korchmáros and T. Szőnyi for their helpful comments.

References

1. A. Beutelspacher and F. Wettl, *On 2-level secret sharing*, Des. Codes Cryptogr. **3** (1993), no. 2, 127–134.
2. A. Bichara and G. Korchmáros, *Note on $(q+2)$-sets in a Galois plane of order q*, Combinatorial and Geometric Structures and their Applications, Ann. Discrete Math., vol. 14, North-Holland, Amsterdam, 1982, pp. 117–122.
3. W. E. Cherowitzo and L. D. Holder, *Hyperfocused arcs*, Simon Stevin **12** (2005), no. 5, 685–696.
4. C. J. Colbourn, D. A. Drake, and W. Myrvold, *Ovals and hyperovals in nets*, Discrete Math. **294** (2005), 53–74.
5. D. A. Drake, *Hyperovals in nets of small degree*, J. Combin. Des. **10** (2002), 322–334.
6. D. A. Drake and K. Keating, *Ovals and hyperovals in Desarguesian nets*, Des. Codes Cryptogr. **31** (2004), 195–212.
7. D. A. Drake and W. Myrvold, *Nets of small degree without ovals*, Des. Codes Cryptogr. **32** (2004), 167–183.
8. J. C. Fisher and R. E. Jamison, *Properties of affinely regular polygons*, Geom. Dedicata **69** (1998), 241–259.
9. M. Giulietti and E. Montanucci, *On hyperfocused arcs in $PG(2,q)$*, Discrete Math. **306** (2006), 3307–3314.
10. M. Giulietti, F. Pambianco, F. Torres, and E. Ughi, *On large complete arcs: odd case*, Discrete Math. **255** (2002), 145–159.
11. J. W. P. Hirschfeld, *Projective geometries over finite fields*, Clarendon Press, Oxford, 1998.
12. J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over finite fields*, Princeton University Press, London, 2008.
13. L. D. Holder, *The construction of geometric threshold schemes with projective geometry*, Master's thesis, University of Colorado at Denver, 1997.
14. N. M. Hy, *Regular polygons on an affine Galois plane of order nine*, Mat. Lapok **22** (1971), 323–329, Hungarian, Italian summary.
15. F. Kárteszi, *Affinely regular polygons*, Seminars given at the E 1971/72.

16. G. Korchmáros, *Poligoni affin regolari dei piani di Galois d'ordine dispari*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **56** (1974), 690–697.
17. ______, *Darstellung der Einheitsmatrix über einen kommutativen Körperals zyklische Matrixsumme. Eine Anwendung in der Theorie dei n-Ecke*, Periodica Polytechnica, Transportation Engineering (Budapest) **4** (1976), 201–210.
18. ______, *Estensioni del concetto di poligono affin regolare ad un qualunque piano affine*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **60** (1976), 119–125.
19. ______, *Eine geometrische Begründung der Theorie der affin-regulären n-Ecke von F. Bachmann und E. Schmidt*, Periodica Polytechnica, Transportation Engineering (Budapest) **5** (1977), 29–42.
20. G. Korchmáros and T. Szőnyi, *Affinely regular polygons in an affine plane*, Contributions to Discrete Mathematics **3** (2008), no. 1, 20–38.
21. T. Szőnyi, *k-sets in* pg$(2, q)$ *having a large set of internal nuclei*, Combinatorics '88, Vol. 2 (Ravello, 1988), Res. Lecture Notes Math., Mediterranean, Rende, 1991, pp. 449–458.
22. T. Szőnyi and F. Wettl, *On complexes in a finite abelian group. i*, Proc. Japan Acad. Ser. A Math. Sci **64** (1988), 245–248.
23. ______, *On complexes in a finite abelian group. ii*, Proc. Japan Acad. Ser. A Math. Sci **64** (1988), 286–287.
24. F. Severi, *Trattato di geometria algebrica*, Zanichelli, Bologna, 1926.
25. G. Simmons, *Sharply focused sets of lines on a conic in $PG(2, q)$*, Congr. Numer. **73** (1990), 181–204.
26. K.O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. **52** (1986), 1–19.
27. J. van de Craats and J. Simonis, *Affinely regular polygons*, Nieuw Archief voor Viskunde **IV** (1986), 225–240.
28. F. Wettl, *On the nuclei of a pointset of a finite projective plane*, J. Geom. **30** (1985), 157–163.

Dipartimento di Matematica, Università di Perugia,
06123 Perugia, Italy
E-mail address: beatame82@libero.it
E-mail address: faina@dipmat.unipg.it
E-mail address: giuliet@dipmat.unipg.it