ON COMPLETE ARCS ARISING FROM PLANE CURVES

M. GIULIETTI, F. PAMBIANCO, F. TORRES, AND E. UGHI

Abstract. We show that the set of $\mathbf{F}_q$-rational points of either certain Fermat curves or certain $\mathbf{F}_q$-Frobenius non-classical plane curves is a complete (k,d)-arc in $\mathbf{P}^2(\mathbf{F}_q)$, where k and d are respectively the number of $\mathbf{F}_q$-rational points and the degree of the underlying curve.

1. Introduction and statement of results

A (k,d)-*arc* $\mathcal{K}$ in the projective plane $\mathbf{P}^2(\mathbf{F}_q)$, $\mathbf{F}_q$ being the finite field with q elements, is a set of k elements such that no line in $\mathbf{P}^2(\mathbf{F}_q)$ meets $\mathcal{K}$ in more than d points. The (k,d)-arc is called *complete* if it is not contained in a $(k+1,d)$-arc. For basic facts on arcs the reader is refered to [7, Ch. 12] (see also the references therein), [10, Sec. 5], [1], and [18].

A natural example of a (k,d)-arc is the set $\mathcal{X}(\mathbf{F}_q)$ of $\mathbf{F}_q$-rational points of a plane curve $\mathcal{X}$ without linear components and defined over $\mathbf{F}_q$, where $k=\#\mathcal{X}(\mathbf{F}_q)$ and d is the degree of $\mathcal{X}$. As a matter of terminology, we shall say that $\mathcal{X}$ has the *arc property* whenever $\mathcal{X}(\mathbf{F}_q)$ is a complete (k,d)-arc with k and d as above. As a matter of fact, the interplay between the theory of algebraic curves and finite geometries was initiated by Segre around 1955. In [14] (see also [7, Sec. 10.4]) he established an upper bound for the second largest size that a complete $(k,2)$-arc in $\mathbf{P}^2(\mathbf{F}_q)$ can have. He proved this result by applying the Hasse-Weil upper bound to the non-singular model of the envelope associated to $(k,2)$-arcs. For further results on these arcs see Hirschfeld and Korchmáros' papers [8] and [9]. For other applications of curves to finite geometries see the surveys [17] and [16].

In this paper we are concerning with the problem of determining plane curves having the arc property. This was asked around 1988 by Hirschfeld and Voloch [11, Problem III]. Only few examples of such curves are known. Among them we have the irreducibles conics in odd characteristic [7, Ch. 8], certain cubics [11, Sect. 5], [5, Sect. 6], and Hermitian curves [7, Lemma 7.20].

For q a square, the Hermitian curve $\mathcal{X}_{\sqrt{q}+1}$ can be defined by

$$X^{\sqrt{q}+1}+Y^{\sqrt{q}+1}+Z^{\sqrt{q}+1}=0\,. \tag{1.1}$$

Then $\mathcal{X}_{\sqrt{q}+1}(\mathbf{F}_q)$ is a complete $(q\sqrt{q}+1,\sqrt{q}+1)$-arc (loc. cit.). The completeness property means that for each $P\in\mathbf{P}^2(\mathbf{F}_q)\setminus\mathcal{X}_{\sqrt{q}+1}(\mathbf{F}_q)$ there exists a $\mathbf{F}_q$-rational line ℓ such that

1991 Math. Subj. Class.: Primary 05B, Secondary 14H.

$\#\ell\cap\mathcal{X}_{\sqrt{q}+1}(\mathbf{F}_q)=\sqrt{q}+1$. This property can be easily shown by using the special feature of Eq. (1.1) (see the proof of Theorem 1.1(1)). Moreover, this property is also a consequence of the fact that the image of $P\in\mathcal{X}_{\sqrt{q}+1}$ by the $\mathbf{F}_q$-Frobenius morphism lies on the tangent line of $\mathcal{X}_{\sqrt{q}+1}$ at P (see the proof of Theorem 1.2). A plane curve satisfying the above property for general points is called $\mathbf{F}_q$-*Frobenius non-classical* [15], [6].

The Hermitian curve is a member of the family of Fermat curves $\mathcal{X}_d(a,b)$ defined by

$$aX^d+bY^d+Z^d=0\,, \tag{1.2}$$

where $d=(q-1)/(q'-1)$, $q=p^n$, $q'=p^e$, $p:=\mathrm{char}(\mathbf{F}_q)$ such that $e<n$ and $e|n$, and where $a,b\in\mathbf{F}^*_{q'}:=\mathbf{F}_{q'}\setminus\{0\}$.

The first aim of this paper is to extend the arc property of the Hermitian curve to the curves $\mathcal{X}_n(a,b)$ above as well as to the Fermat curve $\mathcal{X}_{q-1}$ defined by

$$X^{q-1}+Y^{q-1}=2Z^{q-1}\,, \tag{1.3}$$

provided that $p\geq 3$.

Theorem 1.1. *For $p\geq 3$, the following statements hold:*

1. *the set of $\mathbf{F}_q$-rational points of the Fermat curve defined by Eq. (1.2) is a complete (k,d)-arc, where $k=d(q-d+2)$;*
2. *the set of $\mathbf{F}_q$-rational points of the Fermat curve defined by Eq. (1.3) is a complete $((q-1)^2,q-1)$-arc.*

The arc in part (2) of this theorem is maximal among $(k,q-1)$-arcs for which there exists an external line, see Remark 3.3. On the other hand, it seems that the arcs in part (1) are new.

We notice that the curves in Theorem 1.1 are among the Fermat curves having a large number of $\mathbf{F}_q$-rational points [4]. We also notice that the hypothesis $p\geq 3$ is necessary, see Remark 3.2.

The second aim of this paper is to show that certain $\mathbf{F}_q$-Frobenius non-classical plane curves do satisfy the arc property.

Theorem 1.2. *Let $\mathcal{X}$ be a non-singular $\mathbf{F}_q$-Frobenius non-classical plane curve of degree d. Let ϵ be the order of contact of $\mathcal{X}$ with the tangent at a general point. If*

$$d(d-1)<(q+1)\epsilon\,, \tag{1.4}$$

then the set of $\mathbf{F}_q$-rational points of $\mathcal{X}$ is a complete (k,d)-arc, where $k=\#\mathcal{X}(\mathbf{F}_q)=d(q-d+2)$.

The Fermat curve in Theorem 1.1(2) is $\mathbf{F}_q$-classical by [4, Thm. 2]. Hence the hypothesis of being $\mathbf{F}_q$-Frobenius non-classical in Theorem 1.2 is not necessary. We observe that $d(d-1)/\epsilon$ is the degree of the dual curve of $\mathcal{X}$; see Remark 2.3.

For the Hermitian curve $\mathcal{X}_{\sqrt{q}+1}$, $\epsilon = \sqrt{q}$ (see e.g. [2]) and therefore it satisfies (1.4) in Theorem 1.2. The Fermat curves in Theorem 1.1(1) are $\mathbf{F}_q$-Frobenius non-classical, see [4, Thm. 2]. For these curves, $\epsilon = q'$ [6, Thm. 2], and so they satisfy (1.4) if and only if they are Hermitian curves. So far, we could not find examples of non-singular $\mathbf{F}_q$-Frobenius non-classical curves fulfilling (1.4) which are not $\mathbf{F}_q$-isomorphic to Hermitian curves; see Remark 4.3.

2. Frobenius non-classical planes curves

The study of Frobenius non-classical curves was initiated by Hefez and Voloch [6] based on a fundamental paper by Stöhr and Voloch [15], where an approach to the Hasse-Weil bound was given.

In this paper we only consider irreducible non-linear plane curves defined over $\mathbf{F}_q$. Let $\mathcal{X} \subseteq \mathbf{P}^2(\bar{\mathbf{F}}_q)$ be such a curve. For $i = 0, 1, 2$, let x_i be the coordinates functions of $\mathbf{P}^2(\bar{\mathbf{F}}_q)$ on $\mathcal{X}$. Let t be a separating variable of $\mathbf{F}_q(\mathcal{X})|\mathbf{F}_q$ and denote by $D^i = D^i_t$ the i-th Hasse derivative on $\mathcal{X}$. The order sequence of $\mathcal{X}$ (see [15, p. 5]) are the numbers $0, 1$ and $\epsilon = \epsilon(\mathcal{X})$, where $\epsilon > 1$ is the least integer such that

$$\det \begin{pmatrix} x_0 & x_1 & x_2 \\ D^1 x_0 & D^1 x_1 & D^1 x_2 \\ D^\epsilon x_0 & D^\epsilon x_1 & D^\epsilon x_2 \end{pmatrix} \neq 0 \,.$$

Geometrically, the numbers 0, 1 and ϵ represent all the possible intersection multiplicities of the curve $\mathcal{X}$ with lines in $\mathbf{P}^2(\bar{\mathbf{F}}_q)$ at general points.

The $\mathbf{F}_q$-Frobenius order sequence of $\mathcal{X}$ (see [15, p. 9]) are the numbers 0 and $\nu = \nu(\mathcal{X}, q)$, where $\nu > 0$ is the least integer such that

$$\det \begin{pmatrix} x_0^q & x_1^q & x_2^q \\ x_0 & x_1 & x_2 \\ D^\nu x_0 & D^\nu x_1 & D^\nu x_2 \end{pmatrix} \neq 0 \,. \tag{2.1}$$

We have that $\nu \in \{1, \epsilon\}$ [15, Prop. 2.1]. The plane curve $\mathcal{X}$ is called $\mathbf{F}_q$-Frobenius non-classical if $\nu = \epsilon$ (or equivalently if $\nu > 1$).

Remark 2.1. From Eq. (2.1) follows that $\mathcal{X}$ is $\mathbf{F}_q$-Frobenius non-classical if and only if $\mathbf{F}r_{\mathcal{X}}(P) \in T_P\mathcal{X}$ for all non-singular points $P \in \mathcal{X}$, where $\mathbf{F}r_{\mathcal{X}}$ is the $\mathbf{F}_q$-Frobenius morphism on $\mathcal{X}$ and $T_P\mathcal{X}$ is the tangent line to $\mathcal{X}$ at P.

Remark 2.2. Let $\mathcal{X}$ be a curve as above.

(i) If $\epsilon(\mathcal{X}) > 2$ then it is a power of p [3, Prop. 2].

(ii) If $\mathcal{X}$ is $\mathbf{F}_q$-Frobenius non-classical and $p > 2$, then $\epsilon(\mathcal{X}) > 2$ [6, Prop. 1].

(iii) If $\mathcal{X}$ is $\mathbf{F}_q$-Frobenius non-classical, then $\epsilon(\mathcal{X}) \leq q$ [6, p. 266]. If in addition $\mathcal{X}$ is non-singular, then $\epsilon(\mathcal{X}) \leq \sqrt{q}$ [6, Prop. 6].

(iv) Let $\mathcal{X}$ be non-singular $\mathbf{F}_q$-Frobenius non-classical plane curve. Let d the degree of d and suppose that $\epsilon = \epsilon(\mathcal{X}) > 2$. Then [6, Props. 5, 6]

$$\sqrt{q} + 1 \le d \le (q-1)/(\epsilon - 1)\,.$$

Remark 2.3. Let $\mathcal{X}$ be a non-singular plane curve of degree $d \geq 2$, $\mathcal{X}^*$ the dual curve of $\mathcal{X}$ and $T : \mathcal{X} \to \mathcal{X}^*$ the dual map; i.e, $T(P) = T_P\mathcal{X}$. Then $d(d-1) = \deg(T)d^*$, where d^* is the degree of $\mathcal{X}^*$; this follows e.g. from [12, Lemma 4.3]. Now by a result of Kaji [13, Cor. 4.5], T is purely inseparable. If in addition, $\mathcal{X}$ is $\mathbf{F}_q$-Frobenius non-classical, then $\deg(T) = \epsilon(\mathcal{X})$ [6, Props. 3 and 4]. Therefore, in Theorem 1.2 we look for $\mathbf{F}_q$-Frobenius non-classical plane curves such that the degree of its dual curve is upper bounded by $(q+1)$.

Let $F = F(X_0, X_1, X_2) = 0$ be the equation of $\mathcal{X}$ over $\mathbf{F}_q$. From [3, Thm. 1], $\epsilon = \epsilon(\mathcal{X}) > 2$ if and only if there exist homogeneous polynomials $H, P_0, P_1, P_2 \in \mathbf{F}_q[X_0, X_1, X_2] \setminus \{0\}$ such that

$$FH = X_0P_0^{\epsilon} + X_1P_1^{\epsilon} + X_2P_2^{\epsilon}\,. \tag{2.2}$$

We have that $H = 1$ if $\mathcal{X}$ is non-singular (loc. cit, p. 462). Now it is easy to see that $\mathcal{X}$ is $\mathbf{F}_q$-non-classical if and only if there exists $H_1 \in \mathbf{F}_q[X_0, X_1, X_2]$ such that

$$FH_1 = X_0^{q/\epsilon}P_0 + X_1^{q/\epsilon}P_1 + X_2^{q/\epsilon}P_2\,. \tag{2.3}$$

Finally, we mention a formula for the precise number of $\mathbf{F}_q$-rational points of non-singular $\mathbf{F}_q$-Frobenius non-classical curves.

Lemma 2.4. ([6, Thm. 1]) *Let $\mathcal{X}$ be a plane non-singular $\mathbf{F}_q$-Frobenius non-classical curve of degree d. Then*

$$\#\mathcal{X}(\mathbf{F}_q) = d(q - d + 2)\,.$$

3. Proof of Theorem 1.1

(1) That $\#\mathcal{X}_d(a, b) = d(q - d + 2)$ is well known, see e.g. [4, p. 354]. (This result also follows from [4, Thm. 2] and Lemma 2.4).

Next, for $P \in \mathbf{P}^2(\mathbf{F}_q) \setminus \mathcal{X}_d(\mathbf{F}_q)$, we will show that there exists a $\mathbf{F}_q$-rational line ℓ which passes through P and intersects the curve $\mathcal{X}_d(a, b)$ in d distinct $\mathbf{F}_q$-rational points. We recall the following easy fact.

Claim 3.1. *Let $A, B \in \mathbf{F}_{q'}^*$. Then the equation $AX^d + B = 0$ has d distinct solutions in $\mathbf{F}_q$.*

Proof. Since p does not divide d, the equation has d solutions in $\bar{\mathbf{F}}_q$. If x is a solution, then $x^{q-1} = 1$, as $d = (q-1)/(q'-1)$, and hence $x \in \mathbf{F}_q$. $\square$

We consider four cases:

Case 1: $P = (\alpha : \beta : 0)$. Let $\ell : Z = 0$. Then $P \in \ell$ and

$$\ell \cap \mathcal{X}_d(a,b) = \{(\lambda : 1 : 0) : a\lambda^d + b = 0\}\,.$$

Case 2: $P = (\alpha : \beta : 1)$ and $a\alpha^d + 1 \neq 0$. Let $\ell : X = \alpha Z$. Then $P \in \ell$ and

$$\ell \cap \mathcal{X}_d(a,b) = \{(\alpha : \lambda : 1) : b\lambda^d + a\alpha^d + 1 = 0\}\,.$$

Case 3: $P = (\alpha : \beta : 1)$ and $b\beta^d + 1 \neq 0$. Let $\ell : Y = \beta Z$. Then $P \in \ell$ and

$$\ell \cap \mathcal{X}_d(a,b) = \{(\lambda : \beta : 1) : a\lambda^d + b\beta^d + 1 = 0\}\,.$$

Case 4: $P = (\alpha : \beta : 1)$ and $a\alpha^d + 1 = b\beta^d + 1 = 0$. Let $\ell : \beta X = \alpha Y$. Then $P \in \ell$ and

$$\ell \cap \mathcal{X}_d(a,b) = \{(\alpha, \beta, \beta\lambda) : \lambda^d + 2b = 0\}\,.$$

Now by Claim 3.1 all the sets above have cardinality d and are contained in $\mathcal{X}_d(a,b)(\mathbf{F}_q)$. This completes the proof of Theorem 1.1(1).

(2) We have that

$$\mathcal{X}_{q-1}(\mathbf{F}_q) = \{(\alpha : \beta : \gamma) \in \mathbf{P}^2(\mathbf{F}_q) : \alpha\beta\gamma \neq 0\}\,,$$

so that $\#\mathcal{X}_{q-1}(\mathbf{F}_q) = q^2 + q + 1 - 3q = (q-1)^2$. Let $P = (\alpha : \beta : \gamma) \in \mathbf{P}^2(\mathbf{F}_q) \setminus \mathcal{X}_{q-1}(\mathbf{F}_q)$. The proof of the arc property for $\mathcal{X}_{q-1}$ follows from the following five computations.

Case 1: $\beta = \gamma = 0$. Let $\ell : Y = Z$. Then $P \in \ell$ and

$$\ell \cap \mathcal{X}_{q-1} = \{(\lambda : 1 : 1) : \lambda \in \mathbf{F}_q^*\}\,.$$

Case 2: $\beta \neq 0$ and $\gamma = 0$. Let $\ell : Y = bX$. Then $P \in \ell$ and

$$\ell \cap \mathcal{X}_{q-1} = \{(1 : b : \lambda) : \lambda \in \mathbf{F}_q^*\}\,.$$

Case 3: $\alpha = \beta = 0$. Let $\ell : X = Y$. Then $P \in \ell$ and

$$\ell \cap \mathcal{X}_{q-1} = \{(1 : 1 : \lambda) : \lambda \in \mathbf{F}_q^*\}\,.$$

Case 4: $\alpha \neq 0$ and $\gamma = 1$. Let $\ell : X = aZ$. Then $P \in \ell$ and

$$\ell \cap \mathcal{X}_{q-1} = \{(a : \lambda : 1) : \lambda \in \mathbf{F}_q^*\}\,.$$

Case 5: $\beta \neq 0$ and $\gamma = 1$. Let $\ell : Y = bZ$. Then $P \in \ell$ and

$$\ell \cap \mathcal{X}_{q-1} = \{(\lambda : b : 1) : \lambda \in \mathbf{F}_q^*\}\,.$$

Remark 3.2. The hypothesis $p \geq 3$ in Theorem 1.1(1) is necessary. Indeed, consider the Fermat curve $\mathcal{X}$ defined by

$$X^{q-1} + Y^{q-1} + Z^{q-1} = 0\,,$$

where q is a power of two. Take $P = (1 : 1 : 1)$. Then it is easy to see that $\#\ell \cap \mathcal{X} < q-1$ for any $\mathbf{F}_q$-rational line ℓ passing through P.

Remark 3.3. For a $(k, q-1)$-arc $\mathcal{K}$ having an external line (i.e. a $\mathbf{F}_q$-rational line ℓ such that $\ell \cap \mathcal{K} = \emptyset$), we have that $k \le (q-2)q + 1 = (q-1)^2$ $(*)$ [7, Thm. 12.40]. Since the line $\ell : Z = 0$ is external to the $((q-1)^2, q-1)$-arc in Theorem 1.1(2), we have that the upper bound in $(*)$ is attained by this arc.

Remark 3.4. Notice that the $((q-1)^2, q-1)$-arc in Theorem 1.1(2) is the complement of three non-concurrent lines in $\mathbf{P}^2(\mathbf{F}_q)$. Moreover, it can be shown that any such set is a complete $((q-1)^2, q-1)$-arc which is also the set of $\mathbf{F}_q$-rational points of a plane curve of degree $q-1$; it turns out that this curve is $\mathbf{F}_q$-isomorphic to the Fermat curve $\mathcal{X}_{q-1}$.

Example 3.5. Taking $q = p^3$ and $q' = p$ in Theorem 1.1(1), we have that there exists a complete (k, p^2+p+1)-arc in $\mathbf{P}^2(\mathbf{F}_q)$ with $k = (p^2+p+1)(p^3-p^2-p+1)$. In particular, there exists a complete $(208, 13)$-arc in $\mathbf{F}_{27}$.

4. Proof of Theorem 1.2

Theorem 1.2 will be a consequence of the following more general result.

Theorem 4.1. *Let $\mathcal{X}$ be a $\mathbf{F}_q$-Frobenius non-classical (possible singular) plane curve. Let d be the degree of $\mathcal{X}$ and $k = \#\mathcal{X}(\mathbf{F}_q)$. Then $\mathcal{X}(\mathbf{F}_q)$ is a complete (k, d)-arc provided that*

$$k > (d-\epsilon)(q+1-\#S) + (d-1)\#S\,,$$

where S is the set of singular points of $\mathcal{X}$ and ϵ is as in Theorem 1.2.

Proof. Suppose that $\mathcal{X}(\mathbf{F}_q)$ is not complete. Then there exists $P \in \mathbf{P}^2(\mathbf{F}_q) \setminus \mathcal{X}(\mathbf{F}_q)$ such that for any $\mathbf{F}_q$-rational line ℓ through P,

$$\#\ell \cap \mathcal{X}(\mathbf{F}_q) < d\,. \tag{4.1}$$

Claim 4.2. *If ℓ is a line such that (4.1) holds and that $\ell \cap S = \emptyset$, then*

$$\#\ell \cap \mathcal{X}(\mathbf{F}_q) \le (d-\epsilon)\,.$$

Proof. **Case 1: $\ell \cap \mathcal{X} \not\subseteq \mathcal{X}(\mathbf{F}_q)$.** Let $Q \in \ell \cap \mathcal{X} \setminus \mathcal{X}(\mathbf{F}_q)$. Then, as ℓ is $\mathbf{F}_q$-rational, $\mathbf{F}r_{\mathcal{X}}(Q) \in \ell$ and thus, as $\ell \cap S = \emptyset$, ℓ is the tangent line of $\mathcal{X}$ at Q (see Remark 2.1). Therefore

$$\#\ell \cap \mathcal{X}(\mathbf{F}_q) \le d - \epsilon\,,$$

since $I(\mathcal{X}, \ell; Q) \ge \epsilon$; see [15, p.5].

Case 2: $\ell \cap \mathcal{X} \subseteq \mathcal{X}(\mathbf{F}_q)$. From (4.1) and Bezout's theorem there exists $Q \in \ell \cap \mathcal{X}(\mathbf{F}_q)$ such that $j(Q) := I(\mathcal{X}, \ell; Q) > 1$. Then, as $\ell \cap S = \emptyset$, ℓ is the tangent line of $\mathcal{X}$ at Q. We have that

$$\#\ell \cap \mathcal{X}(\mathbf{F}_q) \le d - j(Q) + 1$$

and the claim follows from the fact that $j(Q) \ge \epsilon + 1$ [15, Cor. 2.10]. ☐

Now there are at most $N \le \#S$ lines ℓ' such that $\ell' \cap S \neq \emptyset$. For each of these lines, $\ell' \cap \mathcal{X}(\mathbf{F}_q) \le d-1$; hence from Claim 4.2 we have

$$k \le (d-\epsilon)(q+1-N) + (d-1)N\,.$$

Then $k \le (d-\epsilon)(q+1) + N(\epsilon-1) \le (d-\epsilon)(q+1) + (\epsilon-1)\#S$, a contradiction. This finishs the proof of Theorem 4.1. □

Proof of Theorem 1.2. We have $S = \emptyset$ and so the hypothesis in Theorem 4.1 is

$$k > (d-\epsilon)(q+1)\,. \tag{4.2}$$

Since $k = d(q-d+2)$ (see Lemma 2.4), it turns out that (4.2) is equivalent to $d(d-1) < (q+1)\epsilon)$ and the result follows.

Remark 4.3. Let $\mathcal{X}$ be a non-singular $\mathbf{F}_q$-Frobenius non-classical curve of degree d. Assume $\epsilon = \epsilon(\mathcal{X}) > 2$. Then from Eqs. (2.2) and (2.3), $d = \lambda\epsilon + 1$ for some $\lambda \in \mathbf{N}$. If (1.4) holds, then

$$\sqrt{q}/\epsilon \le \lambda < \sqrt{q/\epsilon}\,,$$

where the first inequality follows from Remark 2.2(iv).

For a concrete example take $q = p^3$. Then $\epsilon = p$ by Remark 2.2(i)(iii) and so $\sqrt{p} \le \lambda < p$. Therefore $\mathcal{X}$ will satisfy (1.4) if $\lambda = p-1$, i.e. if $\mathcal{X}$ has degree $d = p^2-p+1$. The existence of a such curve is equivalent to the existence of polynomials $P_0, P_1, P_2 \in \mathbf{F}_q[X_0, X_1, X_2]$ of degree $p-1$ and $H_1 \in \mathbf{F}_q[X_0, X_1, X_2]$ such that Eqs. (2.2) and (2.3) hold true. This seems an involved problem. On the other hand, the curve $\mathcal{X}$ will rise to the existence of a complete $((p^2-p+1)(p^3-p^2+p+1), p^2-p+1)$-arc. Unfortunately, the existence of such an arc is not known.

Acknowledgments. The authors wish to thank J.W.P. Hirschfeld and G. Korchmáros for useful comments. This research was carried out with the support of the Italian Ministry for Research and Technology (project 40% "Strutture geometriche, combinatorie e loro applicazioni"). Part of this paper was written while Torres was visiting Perugia in February and December 1999.

References

[1] S. Ball and A. Blokhuis, On the incompleteness of (k, n)-arcs in Desarguesian planes of order q where n divides q, *Geom. Dedicata* **74** (1999), 325–332.
[2] A. Garcia and P. Viana, Weierstrass points on certain non-classical curves, *Arch. Math.* **46** (1986), 315–322.
[3] A. Garcia and J.F. Voloch, Wronskians and linear independence in fields of prime characteristic, *Manuscripta Math.* **59** (1987), 457–469.
[4] A. Garcia and J.F. Voloch, Fermat curves over finite fields, *J. Number Theory* **30** (1988), 345–356.
[5] M. Giulietti, On plane arcs and cubic curves, preprint.
[6] A. Hefez and J.F. Voloch, Frobenius non classical curves, *Arch. Math.* **54** (1990), 263–273.

[7] J.W.P. Hirschfeld, *Projective Geometries Over Finite Fields*, second edition, Oxford University Press, Oxford, 1998.
[8] J.W.P. Hirschfeld and G. Korchmáros, On the number of rational points on an algebraic curve over a finite field, *Bull. Belg. Math. Soc. Simon Stevin* **5** (1998), 313–340.
[9] J.W.P. Hirshfeld and G. Korchmáros, Arcs and curves over a finite field, *Finite Fields Appl.* **5** (1999), 393–408.
[10] J.W.P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces, *J. Statist. Plann. Inference* **72** (1998), 355–380.
[11] J.W.P. Hirschfeld and J.F. Voloch, The characterization of elliptic curves over finite fields, *J. Austral. Math. Soc. Ser. A* **45** (1988), 275–286.
[12] M. Homma, Funny curves in characteristic $p > 0$, *Comm. Algebra* **15**(7) (1987), 1469–1501.
[13] H. Kaji, On the Gauss maps of space curves in characteristic p, *Compositio Math.* **70** (1989), 177–197.
[14] B. Segre, Ovals in a finite projective plane, *Canad. J. Math.* **7** (1955), 414–416.
[15] K.O. Stöhr and J.F. Voloch, Weierstrass points and curves over finite fields, *Proc. London Math. Soc.* **52** (1986), 1–19.
[16] P. Sziklai and T. Szönyai, Blocking sets and algebraic curves, *Rend. Circ. Mat. Palermo Suppl.* **51** (1998), 71–86.
[17] T. Szönyi, Some applications of algebraic curves in finite geometry and combinatorics, "Surveys in Combinatorics" (R.A. Bailey Ed.), 197–236, Cambridge Univ. Press, Cambridge, 1997.
[18] T. Szönyi, On the embedding of (k, p)-arcs in maximal arcs, *Design, Codes and Cryptography* **18** (1999), 235–246.

Dipartimento di Matematica - Università degli Studi di Perugia, Via Vanvitelli 1 - 06123 Perugia (Italy)

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

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

IMECC-UNICAMP, Cx. P. 6065, Campinas, 13083-970-SP, Brazil

E-mail address: ftorres@ime.unicamp.br

Dipartimento di Matematica - Università degli Studi di Perugia, Via Vanvitelli 1 - 06123 Perugia (Italy)

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