On arcs and plane curves

Beatriz Motta[1]***, Fernando Torres***[2,3]

May, 2019

Abstract

We investigate complete plane arcs which arise from the set of rational points of certain Frobenius non-classical plane curves over finite fields. We also point out direct consequences of the Griesmer bound for some linear codes.

MSC(2010): Primary 05B25, 11T23, 11T24; Secondary 14H25.

Keywords: Finite fields, plane arcs, Frobenius non-classical curves.

[1] *DM-ICE-UFJF, MG, Brasil.*
[2] *IMECC-UNICAMP, Campinas, SP, Brasil.*
[3] *Partially supported by the grant CNPq 310623/2017.*

1 Introduction

In all that follows $\mathbb{F} = \mathbb{F}_q$ will denote the finite field of order q. Let $n \geq 2$, $r \geq 2$ be integers. In this paper we are interested in certain subsets $\mathcal{A}$ of the projective plane $PG(\mathbb{F}) = PG(q)$; we follow closely Giulietti *et al.* [5]. In what follows # will denote cardinality of a set.

Let us consider the following conditions:

(A_0) the number of points in $\mathcal{A}$ is n;

(A_1) there is no line ℓ in $PG(q)$ such that $\#\mathcal{A} \cap \ell > r$;

(A_2) for any point $P_0 \in PG(q) \setminus \mathcal{A}$, there exists a line ℓ_0 in $PG(q)$ subject to $P_0 \in \ell_0$ and $\#\mathcal{A} \cap \ell_0 = r$.

If (A_0) and (A_1) hold, $\mathcal{A}$ is called an (n, r)**-arc**. If in addition (A_2) is true, $\mathcal{A}$ is said to be a **complete** (n, r)**-arc**.

These objects are mainly studied in the context of Finite Geometry, where many results can be reformulated in terms of Curve Theory over Finite Fields, Coding Theory or Cryptography; see e.g. Hirschfeld's work [8], [9], [1]. The general problem we are dealing with is the following.

Problem 1.1. Giving q and r as above, for which n there exist a complete (n, r)-arc in $PG(q)$?

Remark 1.2. Let $\mathcal{A}$ be an (n, r)-arc in $PG(q)$ and $P \in \mathcal{A}$. Then each line ℓ in $PG(q)$ that satisfies $P \in \ell$ contains at most $(r-1)$ points of $\mathcal{A}$. Thus (see [8, Corollary 2.15]) we have

$$n \leq (r-1)(q+1) + 1 = (r-1)q + r\,.$$

In particular, we have $n \leq q^2 + q + 1$ as $r \leq \#\ell_0 = q + 1$. We observe then that trivially the plane $PG(q)$ is a (complete) $(q^2+q+1, q+1)$-arc. Further upper bounds can be found in [9, Table 5.2] or [1].

Therefore it makes sense to explore arcs related to plane curves over finite fields; our main reference on curves is the book by Hirschfeld *et al.* [7]. In this sense, we present examples and results related to this problem, see for instance Proposition 3.3 and Example 3.6 in Section 3. But, first, we present some preliminary examples.

Example 1.3. Let $F(X,Y,Z) \in \mathbb{F}[X,Y,Z]$ be an absolutely irreducible, homogeneus polynomial of degree $r \geq 2$. We consider the projective plane curve $\mathcal{C} : F = 0$ over the algebraic closure $\bar{\mathbb{F}}$ of $\mathbb{F}$, where in addition (by simplicity) $\mathcal{C}$ will be assumed to be non-singular. Let $(X : Y : Z)$ be homogeneus coordinates on the projective plane $PG(\bar{\mathbb{F}})$. Then we have $\phi_q(\mathcal{C}) \subseteq \mathcal{C}$, where $\phi_q : (a : b : c) \mapsto (a^q : b^q : c^q)$ is the $\mathbb{F}$-Frobenius map on $PG(\bar{\mathbb{F}})$.

Then we are led to consider $\mathcal{C}(\mathbb{F})$ as being the set of **$\mathbb{F}$-rational points** of $\mathcal{C}$ (namely, the points $P \in \mathcal{C}$ such that $\phi_q(P) = P$). We assume $n = \#\mathcal{C}(\mathbb{F}) \geq 2$.

For a line ℓ in $PG(q)$ set $r_\ell = \#\mathcal{C}(\mathbb{F}) \cap \ell$. We have $r_\ell \leq r$ by Bezout's theorem (see e.g. [7]) and hence $\mathcal{C}(\mathbb{F})$ is in fact an (n,r)-arc.

Now concerning $n = \#\mathcal{C}(\mathbb{F})$ we have the following key obstruction (Hasse-Weil bound):

$$n \leq q + 1 + 2g\sqrt{q}\,,$$

where $g = (r-1)(r-2)/2$ is the genus of $\mathcal{C}$ (see e.g. [7, Theorem 9.18]).

Example 1.4. Let $\mathcal{A} \subseteq PG(q)$ be a $(n,2)$-arc. We get $n \leq q+2$ by Remark 1.2. Notice that if $\mathcal{A} = \mathcal{C}(\mathbb{F})$ were defined as in Example 1.3 (i.e. from a non-singular plane curve of degree $n = 2$), then $n \leq q+1$.

As a matter of fact, we work on plane curves with a special geometrical property from which an "easy" solution to Problem 1.1 is expected (cf. Question 2.5 below).

2 Number of $\mathbb{F}$-rational ponts

Here we use the notation and assumptions of Example 1.3. Let $\mathcal{C}$ be a projective, non-singular plane curve defined by $F = F(X,Y,Z) = 0$. For $P \in \mathcal{C}$ the relation

$$F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0$$

defines the tangent line $T_P\mathcal{C}$ of $\mathcal{C}$ at P, where F_X, F_Y, F_Z are, respectively, the partial derivative of F with respect to the indeterminates X, Y, Z.

It is a fundamental observation that a "large number" of $\mathbb{F}$-rational points of $\mathcal{C}$ are related to the property "$\phi_q(P) \in T_P\mathcal{C}$ for almost all $P \in \mathcal{C}$" (cf. Remark 3.5 below). In this case $\mathcal{C}$ is called **Frobenius non-classical**, otherwise it is called **Frobenius classical**; cf. [12], [6] (compare Propositions 2.1, 2.4 below).

Proposition 2.1. *For $\mathcal{C}$ a projective, non-singular, Frobenius classical plane curve over $\mathbb{F}$ of degree r, we have*

$$\#\mathcal{C}(\mathbb{F}) \leq r(r+q-1)/2\,.$$

Proof. Let $\mathcal{C}$ be defined by $F = F(X,Y,Z) = 0$. For $P = (a:b:c) \in \mathcal{C}$ we notice that $\phi_q(P) \in T_P\mathcal{C}$ holds if and only if we have

$$a^q F_X(P) + b^q F_Y(P) + c^q F_Z(P) = 0\,.$$

This led us to consider the (possible singular) curve $\mathcal{C}_1$ defined for

$$G(X,Y,Z) = X^q F_X(X,Y,Z) + Y^q F_Y(X,Y,Z) + Z^q F_Z(X,Y,Z)\,.$$

Now, by Bezout's theorem, we obtain

$$\sum_{P \in \mathcal{C}(\mathbb{F})} I(P; \mathcal{C} \cap \mathcal{C}_1) \leq r(q+r-1)\,,$$

since $\mathcal{C} \not\subseteq \mathcal{C}_1$ as $\mathcal{C}$ is Frobenius classical; here $I(P; \mathcal{C} \cap \mathcal{C}_1)$ is the intersection multiplicity of $\mathcal{C}$ and $\mathcal{C}_1$ at P. We have then

$$G(X,Y,Z) = F_X(X^q - X) + F_Y(Y^q - Y) + F_Z(Z^q - Z) + rF(X,Y,Z)\,,$$

and hence $P \in \mathcal{C}_1$ for $P \in \mathcal{C}(\mathbb{F})$. This way we get $I(P; \mathcal{C} \cap \mathcal{C}_1) \geq 2$ for $P \in \mathcal{C}(\mathbb{F})$, and the result follows. □

Remark 2.2. ([2, Theorem 2]) Let $q = p$ be a prime with $p \equiv 1 \pmod 4$, and c a non-square in $\mathbb{F}$. The following plane curve $\mathcal{C}$ over $\mathbb{F}$ defined by

$$(Y + cZ)^{(p-1)/2} + Y^{(p-1)/2} - Z^{(p-1)/2} - X^{(p-1)/2} = 0$$

is non-singular, Frobenius classical and satisfies the upper bound in Proposition 2.1, that is $\#\mathcal{C}(\mathbb{F}) = 3(p-1)^2/8$.

Question 2.3. Is the set of $\mathbb{F}$-rational points of the curve $\mathcal{C}$ in Remark 2.2 above a complete $(n,(p-1)/2)$-arc with $n=3(p-1)^2/8$, that is, does Condition (A_2) hold?

We have the following complementary result.

Proposition 2.4. ([6, Theorem 1]) *Let $\mathcal{C}$ a projective, non-singular, Frobenius non-classical plane curve over $\mathbb{F}$ of degree r. Then we have*

$$\#\mathcal{C}(\mathbb{F}) = r(q-r+2)\,.$$

□

Question 2.5. Is the set of $\mathbb{F}$-rational points of the curve $\mathcal{C}$ in Proposition 2.4 a complete (n,r)-arc with $n=r(q-r+2)$?

Remark 2.6. According to [1, Section 5], an (n,r)-arc in $PG(q)$ is said to be **large** whenever $n/q > r-2$. Thus, arcs related to Question 2.5 would be large if and only if $q > r(r-2)/2$. On the other hand, those related to Question 2.3 would not be so.

3 Complete arcs: Property A_2

Throughout this section $\mathcal{C}: F(X,Y,Z)=0$ will be a projective, non-singular, Frobenius non-classical plane curve of degree $r\geq 2$ defined over $\mathbb{F}$.

If $P\in\mathcal{C}$ and ℓ is a line in $PG(\bar{\mathbb{F}})$, then there are three possibilities: $P\notin\ell$, ℓ is transversal to $\mathcal{C}$ at P or ℓ is the tangent line $T_P\mathcal{C}$ of $\mathcal{C}$ at P. In each of these cases, we will write the intersection multiplicity $I(P;\mathcal{C}\cap\ell)$ at $P\in\mathcal{C}$ as $j_0(P)$, $j_1(P)$ and $j_2(P)$ to stress the fact that they are, respectivelly, 0, 1 or greater than 1; see e.g. [12]. Moreover, $j_2(P)$ is the same for almost all P; this common value will be denoted by $\epsilon=\epsilon(\mathcal{C})$. The finitely many points P where $j_2(P)\neq\epsilon$ are the so-called **inflexion points of** $\mathcal{C}$ (or the **Weierstrass points** of $\mathcal{C}$ with respect to the embedding $\mathcal{C}\subseteq PG(\bar{\mathbb{F}})$). These points include the $\mathbb{F}$-rational points since for such points P we have $j_2(P)\geq\epsilon+1$ (see [12]).

Observe that for $P\notin\mathcal{C}(\mathbb{F})$, $T_P\mathcal{C}$ is determinated by P and $\phi_q(P)$.

Lemma 3.1. ([6, Section 3]) *Suppose $\epsilon>2$. Then*

(1) ϵ *is a power of the characteristic of* $\mathbb{F}$ *and satisfies* $\epsilon \leq \sqrt{q}$;

(2) $r \equiv 1 \pmod{\epsilon}$;

(3) $\sqrt{q}+1 \leq r \leq (q-1)/(\epsilon-1)$. □

Now we study property (A_2) for $\mathcal{C}(\mathbb{F})$.

Lemma 3.2. *Let* $\mathcal{C}$ *be a projective, non-singular, Frobenius non-classical plane curve. Let* ℓ_0 *be a line in* $PG(q)$ *such that* $\ell_0 \neq T_P$ *for any* $P \in \mathcal{C}$. *Then we have* $\ell_0 \cap \mathcal{C} \subseteq \mathcal{C}(\mathbb{F})$.

Proof. Suppose there exists $P \in \ell_0 \cap \mathcal{C}$ with $\phi_q(P) \neq P$. Since $\phi_q(\ell_0) = \ell_0$, then $\phi_q(P) \in \ell_0$. Thus we get $\ell_0 = T_P\mathcal{C}$ as $T_P\mathcal{C}$ is determined by P and $\phi_q(P)$. □

Proposition 3.3. *Let* $\mathcal{C}$ *be a projective, non-singular, Frobenius non-classical plane curve of degree* r. *Suppose that for any* $P_0 \in PG(q) \setminus \mathcal{C}(\mathbb{F})$ *there is a line* ℓ_0 *in* $PG(q)$ *such that* $P_0 \in \ell_0$ *and* $\ell_0 \neq T_P$ *for any* $P \in \mathcal{C}$. *Then* $\mathcal{C}(\mathbb{F})$ *is a complete* $(r(q-r+2), r)$*-arc.*

Proof. We have $\#\mathcal{C}(\mathbb{F}) = r(q-r+2)$ by Proposition 2.4 above. Let $P_0 \in PG(q) \setminus \mathcal{C}(\mathbb{F})$ and ℓ_0 be as in the hypothesis. By Lemma 3.1 we have $\ell_0 \cap \mathcal{C}(\mathbb{F}) \subseteq \mathcal{C}(\mathbb{F})$. If $\#\ell_0 \cap \mathcal{C} < n$, we obtain $I(P, \ell_0 \cap \mathcal{C}) > 1$ for some $P \in \ell_0 \cap \mathcal{C}$ and we reach $\ell_0 = T_P\mathcal{C}$, a contradiction. □

We have the following numerical sufficient condition.

Corollary 3.4. *Consider* $\mathcal{C}$ *a projective, non-singular, Frobenius non-classical plane curve of degree* r *and let* ϵ *be the generic order of contact of* $\mathcal{C}$ *with tangent lines. If* $r(r-1) < \epsilon(q+1)$, *then* $\mathcal{C}(\mathbb{F})$ *is a complete* $(r(q-r+2), r)$*-arc.*

Proof. By a result of Kaji [10], the dual curve of $\mathcal{C}$ has degree $r^* = r(r-1)/\epsilon$. Thus the hypothesis $r^* < q+1$ allows us to apply Proposition 3.3. □

Remark 3.5. For $\mathcal{C}$, r and ϵ as in Corollary 3.4, we have $\#\mathcal{C}(\mathbb{F}) = r(q-r+2)$ (Proposition 2.4). Therefore, after some elementary computations we obtain

$$r^* = \frac{r(r-1)}{\epsilon} < q+1 \text{ if and only if } \#\mathcal{C}(\mathbb{F}) > (q+1)(r-\epsilon)\,.$$

Example 3.6. Let $q = m^2$ be a perfect square. We consider the Hermitian curve $\mathcal{C} \subseteq PG(\overline{\mathbb{F}})$ over $\mathbb{F}$ defined by the equation

$$X^{m+1} + Y^{m+1} + Z^{m+1} = 0\,.$$

After some computations we see that $\mathcal{C}$ is non-singular. Next we show that $\mathcal{C}$ is Frobenius non-classical.

For $P = (a : b : c) \in \mathcal{C}$, the tangent line $T_P\mathcal{C}$ is given by

$$a^m X + b^m Y + c^m Z = 0\,. \tag{3.1}$$

Then we have $\phi_q(P) = (a^{m^2} : b^{m^2} : c^{m^2})$ and hence

$$a^m a^{m^2} + b^m b^{m^2} + c^m c^{m^2} = (a^{m+1} + b^{m+1} + c^{m+1})^m = 0\,,$$

which implies $\phi_q(P) \in T_P\mathcal{C}$.

Next let us compute the set $\mathcal{C}(\mathbb{F})$.

• If $Z = 0$ then $(1 : \alpha : 0) \in \mathcal{C}$ with

$$\alpha^{m+1} = -1\,,$$

hence $\alpha \in \mathbb{F}$. Thus there are $m + 1$ $\mathbb{F}$-rational points over $Z = 0$.
• Let $Z \neq 0$ and consider the affine equation $y^{m+1} = -x^{m+1} - 1$. There are $m + 1$ elements of $\mathcal{C}(F)$ of type $(\alpha : 0 : 1)$ with α subject to $\alpha^{m+1} = -1$.
• Let $\alpha \in \mathbb{F}$ so that $\alpha^{m+1} \neq -1$. There are $(m^2 - (m+1))(m+1)$ points of $\mathcal{C}$ of type $(\alpha : \beta : 1)$ with $\beta^{m+1} = -\alpha^{m+1} - 1$.

Summing up, we have $\#\mathcal{C}(\mathbb{F}) = (m+1)+(m+1)+(m^3+m^2-m^2-2m-1) = m^3+1$ (this result also follows from Proposition 2.4 above). We do observe that the set of $\mathbb{F}$-rational points of $\mathcal{C}$ attains the Hasse-Weil bound, namely $\#\mathcal{C}(\mathbb{F}) = m^2 + 1 + 2g_0 m$, where $g_0 = m(m-1)/2$. In this case, we say that $\mathcal{C}$ is $\mathbb{F}$**-maximal**. As a matter of fact, $\mathcal{C}$ is, up to isomorphism, the unique $\mathbb{F}$-maximal curve of genus g_0, compare [11].

Finally we show that $\mathcal{C}(\mathbb{F})$ is a complete $(m^3 + 1, m + 1)$-arc.

We shall apply Corollary 3.4. From (3.1) we can identify $T_P\mathcal{C}$ with the point $(a^m : b^m : c^m)$, where $P = (a : b : c) \in \mathcal{C}$. Thus we get

$$(a^m)^{m+1} + (b^m)^{m+1} + (c^m)^{m+1} = 0$$

and hence the degree of the dual curve of $\mathcal{C}$ is $r^* = m+1$ and so $r^* < m^2+1$; the result now follows immediately.

Remark 3.7. Let $\mathcal{C}$ be the Hermitian curve of degree $r = m+1$ in Example 3.6. Let ϵ be the generic order of contact of $\mathcal{C}$ with lines. Since the degree of the dual curve of $\mathcal{C}$ is $r^* = m+1$, by Kaji [10] we have $\epsilon = m$ as $r^* = n(n-1)/\epsilon$. Thus the intersection divisor of $\mathcal{C}$ and $T_P\mathcal{C}$ at a point P with $j_2(P) = \epsilon$ is of type

$$\mathcal{C} \cdot T_P\mathcal{C} = mP + \phi_q(P)\,. \tag{3.2}$$

We observe that in fact $j_2(P) = \epsilon$ holds for any $P \notin \mathcal{C}(\mathbb{F})$. If $P \in \mathcal{C}(\mathbb{F})$ we have $j_2(P) \geq \epsilon + 1$ and hence we get

$$\mathcal{C} \cdot T_P\mathcal{C} = (m+1)P\,. \tag{3.3}$$

Finally, the arc $\mathcal{C}(\mathbb{F})$ has the following incident property:

- For $P \in \mathcal{C}(\mathbb{F}) \cap \ell$, we get either $\#\ell \cap \mathcal{C}(\mathbb{F}) = 1$, or $\#\ell \cap \mathcal{C}(\mathbb{F}) = m+1$.

Indeed, if $\ell = T_P\mathcal{C}$, from (3.3) we have $\#\ell \cap \mathcal{C}(\mathbb{F}) = 1$. On the contrary if $\ell \neq T_P\mathcal{C}$, then $I(P; \ell \cap \mathcal{C}) = 1$. If there is $Q \in \ell \cap \mathcal{C}$, with $\phi_q(Q) \neq Q$, then we have $\phi_q(Q) \in \ell \cap \mathcal{C}$, and so we conclude $\ell = T_Q\mathcal{C}$, which is not possible by (3.2). Now for $Q \in \ell \cap \mathcal{C} \subseteq \mathcal{C}(\mathbb{F})$, we have $I(Q; \ell \cap \mathcal{C}(\mathbb{F})) = 1$ by (3.1), and the result follows from Bezout's theorem.

Remark 3.8. For the Hermitian curve $\mathcal{C}$ in Example 3.6 we just observed the equality $\epsilon = \epsilon(\mathcal{C}) = m$. As a matter of fact this curve is the unique non-singular Frobenius non-classical curve $\mathcal{C}$ of degree at most $m+1$ that verifies $\epsilon = \epsilon(\mathcal{C})m > 2$ (see [6, Proposition 6]).

Example 3.9. (Related to a Serre's question; compare [15, Proposition 1.1]) We look for a projective non-singular quartic plane curve $\mathcal{C}$ over $\mathbb{F}$ subject to $\#\mathcal{C}(\mathbb{F}) > 4(4+q-1)/2 = 2(3+q)$. Such a curve must be Frobenius non-classical by Proposition 2.1; therefore, we should get $\#\mathcal{C}(\mathbb{F}) = 4q-8$ by Proposition 2.4. Let ϵ be the generic order of contact of $\mathcal{C}$ with lines. Then $\epsilon \in \{2,3\}$ by Lemma 3.1(2).

Suppose $\epsilon = 3$. Then $q = 9$ by Lemma 3.1(3) and so $\#\mathcal{C}(\mathbb{F}) = 28 = 9+1+2g\cdot 3$, with $g = 3$. This means that $\mathcal{C}$ must be a $\mathbb{F}$-maximal curve

of genus $g_0 = 3$; i.e., $\mathcal{C}$ is the Hermitian curve $X^4 + Y^4 + Z^4 = 0$ by [11] (see also [6, Proposition 6]).

Otherwise $\epsilon = 2$. Since ϵ has to be a power of the characteristic, we have that q is a power of two, see [6, Section 3] (or [4, Corollary 3]). Moreover, there exists a $\mathbb{F}$-divisor $S = \sum_{P \in S} v_P(S)P$ on $\mathcal{C}$ (see [12, p. 9]) such that

$$\deg(S) = \epsilon \cdot 4 + (q+2) \cdot 4 \geq 2(4q-8),$$

and hence $q \in \{2, 4, 8\}$. As a matter of fact, Top [15] concluded that q must be 8 and $\mathcal{C}$ must be $\mathbb{F}$-isomorphic to the plane curve $\mathcal{C}$ defined by

$$X^4 + Y^4 + Z^4 + X^2Y^2 + Y^2Z^2 + Z^2X^2 + X^2YZ + XY^2Z + XYZ^2 = 0\,.$$

In the explicit case $\mathcal{A} = \mathcal{C}(\mathbb{F}_8)$, we have $n(n-1) = 12 < 2(8+1)$ and so, by Corollary 3.4, $\mathcal{A}$ is a complete $(24, 4)$-arc in $PG(\mathbb{F}_8)$. We do remark that the largest complete $(n, 4)$-arc in $PG(\mathbb{F}_8)$ is found for $n = 28$; see [8, Table 12.3].

Next we present examples of complete arcs obtained from non-singular, Frobenius non-classical plane curves which do not satisfy the numerical hypothesis in Corollary 3.4.

Example 3.10. ([3], [7, Theorem 8.81]) Let $p > 2$ be a prime, $\alpha \geq 2$ be an integer, $q = p^\alpha$ and set $r = (p^\alpha - 1)/(p-1)$. Let $\mathcal{C}$ be the plane curve in $PG(\overline{\mathbb{F}})$ defined by the afin equation

$$y^r = f(x) = xg^p(x) + h^p(x),$$

where

$$g(x) = x^{\sum_{i=0}^{\alpha-2} p^i} + 1 \quad \text{and} \quad h(x) = \sum_{i=0}^{\alpha-2} x^{p^i}\,.$$

Observe that for $x \in \mathbb{F}$, we have $f(x) = \mathrm{N}(x) + \mathrm{T}(x)$ being T and N respectively the trace and norm functions from $\mathbb{F}$ to $\mathbb{F}_p$.

This curve is non-singular, Frobenius non-classical with $\epsilon(\mathcal{C}) = p$ and degree r. In particular, the condition $r(r-1) < \epsilon(q+1)$ holds only for $\alpha = 2$. In this case we have $r = p+1$ and we obtain a complete $(n, p+1)$-arc with $n = p^3 + 1$.

Let $\alpha \geq 3$. We claim that $\mathcal{C}(\mathbb{F})$ is a complete (n,r)-arc with $n = r(q-r+2)$ (this follows from Proposition 2.4). We have to show property (A_2). Let $P_0 = (a:b:c) \in PG(q) \setminus \mathcal{C}(\mathbb{F})$.

If $c = 0$, the line $\ell_0 : Z = 0$ intersects $\mathcal{C}$ in r points in $PG(\mathbb{F})$, namely those $(\alpha:\beta:0)$ subject to $\alpha^r = \beta^r$ (notice that any r-th root of unity belongs to $\mathbb{F}$).

Let $P_0 = (a:b:1)$. Suppose $f(a) \neq 0$ and consider the line $\ell_0 : X = aZ$. Since $f(a) \in \mathbb{F}_p$, then the points $(a:\beta:1)$ with $\beta^n = f(a)$ belong to $PG(\mathbb{F})$ and we get $\#\mathcal{C}(\mathbb{F}) \cap \ell_0 = r$. For $f(a) = 0$, we have $a \neq 1, -1$ since $p > 2$ and $b \neq 0$ as $P_0 \notin \mathcal{A}$. Let $\ell_1 : Y = m_1(X - aZ) + bZ$ (respectively $\ell_2 : Y = m_2(X - aZ) + bZ$) be the line with $m_1 = b/(a+1)$ (respectively $m_2 = b/(a-1)$). Let

$$(m_1(X-a)+b)^n - f(X) = 0\,, \quad (m_2(X-a)+b)^n - f(X) = 0\,.$$

Whenever $m_1^n = 1$ and $m_2^n = 1$ we would have $(a+1)^n = (a-1)^n$, which together with $f(a) = 0$ forces a contradiction. Hence one of the lines ℓ_i makes (A_2) work and thus $\mathcal{C}(\mathbb{F})$ should be a (n,r)-arc.

Remark 3.11. (On the uniqueness of arcs) In $PG(p^3)$, with $p > 2$ a prime, there are at least two non-isomorphic complete (n,r)-arcs with $r = (p^3-1)/(p-1) = p^2+p+1$ and $n = r(q-r+2)$. Indeed Example 3.10 above defines one such arc, say $\mathcal{A}_1$. Consider also the curve $\mathcal{D}$ given by

$$y^{p^2+p+1} = x^{p^2+p+1} + 1\,.$$

After some computation one concludes that $\mathcal{D}$ is also non-singular and Frobenius non-classical with $\mathcal{D}(\mathbb{F})$ a complete (n,r)-arc. Suppose that there exists a projective bijective map $T : PG(p^3) \to PG(p^3)$ such that $T(\mathcal{A}_1) = \mathcal{A}_2$. By [3] we have $T(\mathcal{C}) \neq \mathcal{D}$ (recall the characterization $\mathcal{A}_1 = \mathcal{C}(\mathbb{F})$) so that by Bezout's theorem we have

$$k = (p^2+p+1)(p^3-p^2-p+1) \leq (p^2+p+1)^2,$$

which is impossible.

Example 3.12. As for a numerical example we let $p = 3$ in Remark 3.11 and so $r = 3^2+3+1 = 13$, $n = 13(27-13+2) = 208$. This yields at least two complete non-isomorphic $(208, 13)$-arcs in $PG(27)$.

Let us recall that the **deficiency** of an (n, r) arc in $PG(q)$ is $D = (r-1)q+r-n$ (cf. Remark 1.2); in our case, $D = 129$. Arcs with "large D" (say $D > n$) can be constructed in general via several combinatorial methods [8, Section 12.4], [9]. Our examples, on the other hand, depict arcs of small deficiency which can be constructed via non-Frobenius plane curves.

Finally, for m the biggest integer for which there is a complete $(m, 13)$-arc in $PG(27)$, we have $208 \leq m \leq 337$. We ask if these bounds can be improved.

We end this paper with a remark on linear codes (cf. [8, Section 2.14], [1]). First of all we notice that an (n, r)-arc in $PG(q)$ can be raised to a linear code over $\mathbb{F}$ with length n, dimension 3 and minimum distance $d = n - r$. We are concerned with the so-called Griesmer bound on n [16, Theorem 5.2.6], namely with the inequality

$$n \geq g_q(3, d) = \sum_{i=0}^{2} \lceil d/q^i \rceil \, .$$

Proposition 3.13. *For a code $[n, 3, d]$ associated to an (n, r)-arc on a projective, non-singular, Frobenius non-classical curve over $\mathbb{F}$ of degree r we have $n = g_q(3, d)$ provided that $r(q - r + 1) \leq q^2$ holds.*

Proof. Here we have $d = n - r = r(q - r + 1)$ by Proposition 2.4 and so we get

$$n \geq n - r + \lceil (n - r)/q \rceil + 1 \, .$$

The result follows from Remark 1.2. □

Example 3.14. The arcs obtained from the Hermitian curve (Example 3.6) and those from the quartics in Example 3.9 satisfy Proposition 3.13. For further considerations see Storme [14].

References

[1] S. Ball and J.W.P. Hirschfeld, *Bounds on (n, r)-arcs and their application to linear codes*, Finite Fields Appl. **11**(3) (2005), 326–336.

[2] M.L. Carlin and J.F. Volcoh, *Plane curves with many points over finite fields*, Rocky Mountain J. Math. **34**(4) (2004), 1255–1259.

[3] A. Garcia, *The curves $y^n = f(x)$ over finite fields*, Arch. Math. **54**(1) (1990), 36–44.

[4] A. Garcia and M. Homma, *Frobenius order-sequences of curves*, "Algebra and Number Theory", G. Frey, J. Ritter (Eds.) de Gruyter, Berlin, 27–41, 1994.

[5] M. Giulietti, F. Pambianco, F. Torres and E. Ughi, *On complete arcs arising from plane curves*, Designs Codes Crypt. **25** (2002), 237–246.

[6] A. Hefez and J.F. Voloch, *Frobenius non clasical curves*, Arch. Math. **54** (1990), 263–273.

[7] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves over a Finite Field*, Princeton University Press, Princeton, 2008.

[8] J.W.P. Hirschfeld, *Projective Geometries Over Finite Fields*, Second edition, Oxford University Press, Oxford, 1998.

[9] J.W.P. Hirschfeld and L. Storme, *The packing problem in statistics, coding theory and finite projective spaces: update 2001*, *Finite Geometries*, Developments in Mathematics **3**, Kluwer, 2001, 201–246.

[10] H. Kaji, *On the Gauss maps of space curves in characteristic p*, Compositio Math. **70** (1989), 177–197.

[11] H.G. Rück and H. Stichtenoth, *A characterization of Hermitian functions fields over finite fields*, J. Reine Angew. Math. **457** (1994), 185–188.

[12] K.O. Stöhr and J.F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. **52** (1986), 1-19.

[13] T. Szönyi, *On the embedding of* (k, p)*-arcs*, Des. Codes Cryptogr. **18** (1999), 235–246.

[14] L. Storme, *Linear codes meeting the Griesmer bound, minihypers, and geometric applications*, preprint.

[15] J. Top, *Curves of genus 3 over small finite fields*, Indag. Mathem. **14**(2) (2003), 275–283.

[16] J.H. van Lint, *An Introduction to Coding Theory*, Third edition, Springer–Verlag, 1998.

Resumen

Investigamos arcos planos completos que emergen del conjunto de puntos racionales de ciertas curvas Frobenius no clásicas planas sobre cuerpos finitos. También apuntamos consecuencias directas de la cota de Griesmer para algunos códigos lineales.

Keywords: Cuerpos finitos, arcos planos, curvas Frobenius no clásicas.

Beatriz Motta
DM-ICE-UFJF, R. Jose Lourenco Kelmer
Campus Universitário 36036-900
Juiz de Fora, MG, Brasil
e-mail: beatriz@ice.ufjf.br

Fernando Torres
IMECC-UNICAMP, R. Sérgio Buarque de Holanda 651
Cidade Universitária "Seferino Vaz" 13083-859
Campinas, SP, Brasil
e-mail: ftorres@ime.unicamp.br