The Dissertation Committee for Herivelto Martins Borges Filho
certifies that this is the approved version of the following dissertation:

Characterization of multi-Frobenius non-classical plane curves and construction of complete plane (N, d)-arcs.

Committee:

José Felipe Voloch, Supervisor

Arnaldo Garcia

Fernando Rodriguez Villegas

Jeffrey Vaaler

John Tate

Sean Keel

Characterization of multi-Frobenius non-classical plane curves and construction of complete plane (N, d)-arcs.

by

Herivelto Martins Borges Filho, M.S.

Dissertation

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Doctor of Philosophy

The University of Texas at Austin

August 2009

To my wife

Acknowledgments

I would like to thank my advisor Professor Felipe Voloch for his time, patience, guidance, support and encouragement during the course of my graduate program. I thank all the Professors of my dissertation committee for their time, availability and careful reading of my work. I want to thank the math department of The University of Texas at Austin for such a supportive environment, with a special thank to Nancy Lamm for the invaluable help and attention she has provided me for all these years. My appreciation and thanks is also owed to my family and many friends in Brazil. Their moral support has always been a key ingredient to most of my achievements. I specially thank Professor Orlando Stanley Juriaans, from the University of São Paulo, for all the motivation he gave me to the pursuit of my PhD. I thank CAPES, a Brazilian governmental agency, for four years of financial support. Above all, I thank my lovely wife and kids for their existence in my world which naturally gives me the greatest motivation to succeed in many aspects of my life.

Herivelto Martins Borges Filho

The University of Texas at Austin

August 2009

Characterization of multi-Frobenius non-classical plane curves and construction of complete plane (N, d)-arcs.

Publication No. _____

Herivelto Martins Borges Filho, Ph.D.
The University of Texas at Austin, 2009

Supervisor: José Felipe Voloch

This work is composed of two independent parts, both addressing problems related to algebraic curves over finite fields.

In the first part, we characterize all irreducible plane curves defined over $\mathbb{F}_q$ which are Frobenius non-classical for different powers of q. Such characterization gives rise to many previously unknown curves which turn out to have some interesting properties. For instance, for $n \geq 3$ a curve which is both q- and q^n-Frobenius non-classical will have its number of $\mathbb{F}_{q^n}$-rational points attaining the Stöhr-Voloch bound.

In the second part, we study the arc property of several plane curves and present new complete (N, d)-arcs in $PG(2, q)$. Some of these arcs (viewed as linear

$(N, 3, N - d)$-codes) are just a small constant away from the Griesmer bound and for some small values of q the bound is achieved. In addition, this part also answers a question of Voloch about the arc property of a certain family of curves with many rational points, and another question of Giulietti et al about the arc property of q-Frobenius non-classical plane curves.

Contents

Chapter 1

Introduction

The theory of algebraic curves over finite fields is of fundamental importance to mathematics and has essential applications in many areas such as finite geometry, number theory, error-correcting codes, and cryptography. In many of such applications it is desirable to count/estimate the number of $\mathbb{F}_q$-rational points of a curve. A remarkable example is the construction of linear codes using curves over finite fields discovered by Goppa in the 1970s. It turns out that such codes can have good parameters if the underlying curve has many points (relative to the genus).

The main purpose of this chapter is to recall some few (but deep) results related to the number of points on curves over finite fields. We will also give the definition of (N, d)-arc and briefly present its connection with linear codes. As a general rule, our discussion here will be limited to the concepts and results that are relevant to the next chapters. Throughout this text the projective plane $\mathbb{P}^2(\mathbb{F}_q)$ will be often denoted by $PG(2, q)$.

1.1 The Hasse-Weil bound

The following theorem, also known as the Riemann hypothesis for curves over finite fields, is one of the deepest results in the theory of algebraic curves. It was originally proved by Hasse [9] in the case of elliptic curves and later by Weil [23] in its generality.

Theorem 1.1. *(Hasse-Weil) Let $\mathcal{F}$ be a (projective, irreducible, non-singular) curve of genus g defined over $\mathbb{F}_q$. If $N = \#\mathcal{F}(\mathbb{F}_q)$ is the number of $\mathbb{F}_q$-rational points of $\mathcal{F}$, then*

$$| N - (q+1) | \leq 2gq^{1/2}. \tag{1.1}$$

There are many examples of curves attaining the Hasse-Weil upper bound, and because this can only happen if $g = 0$ or q is a square, such curves are usually called $\mathbb{F}_{q^2}$-maximal. A very well-known example of an $\mathbb{F}_{q^2}$-maximal curve is the Hermitian curve

$$\mathcal{H} : x^{q+1} + y^{q+1} + z^{q+1} = 0,$$

which is a non-singular plane curve of genus $\frac{1}{2}(q^2 - q)$ with exactly $1 + q^3$ points in $PG(2, q^2)$. Actually, Rück and Stichtenoth [17] proved that (up to isomorphism) the Hermitian curve is the unique $\mathbb{F}_{q^2}$-maximal curve of genus $\frac{1}{2}(q^2 - q)$.

It follows from a result of Serre (see Proposition 6 of [13]) that the Hermitian curve, together with its large automorphism group, gives rise to many other $\mathbb{F}_{q^2}$-maximal curves (see [6] for more details). A very simple example of this is given by the following result.

Theorem 1.2. *If q is a prime power and d is a divisor of $q + 1$, then the curve*

$$x^d + y^d + z^d = 0$$

is $\mathbb{F}_{q^2}$-maximal.

If $q \geq 11$, the curve corresponding to $d = (q+1)/2$ in the above theorem is the unique (up to $\mathbb{F}_{q^2}$-isomorphism) smooth $\mathbb{F}_{q^2}$-maximal curve of such degree (see [3]). This particular curve will be considered in Chapther 3.

The next result (see for example Chapter 7 of [11]), which will be used in the proof of Theorem 3.7, states another interesting property of the Hermitian curve.

Theorem 1.3. *Let $\mathcal{H}$ be the Hermitian curve, P a point in $PG(2,q^2)\backslash\mathcal{H}(\mathbb{F}_{q^2})$ and L_P the set of q^2+1 lines in $PG(2,q^2)$ incident with P. If $l \in L_P$ such that $\#(l \cap \mathcal{H}(\mathbb{F}_{q^2})) < q+1$ then $\#(l \cap \mathcal{H}) = 1$. Moreover, there are exactly $q+1$ such lines in L_P.*

1.2 Frobenius classicality and the Stöhr-Voloch bound

In 1986, Stöhr and Voloch [18], using a more geometric approach, obtained new upper bounds for the the number of rational points on curves over finite fields. In many cases, their method provides improvements on the Hasse-Weil upper bound. A prototype of their results is the following:

Theorem 1.4. *Let q be an odd prime power. If $\mathcal{F} = Z(f(x,y))$ is an absolutely irreducible plane curve of degree d defined over $\mathbb{F}_q$ then*

$$\#\mathcal{F}(\mathbb{F}_q) \leq d(d+q-1)/2,$$

provided that f does not divide $(f_y)^2 f_{xx} - 2f_{xy}f_x f_y + (f_x)^2 f_{yy}$.

Note that the last condition in the theorem above only means that $\mathcal{F}$ has finitely many inflection points.

For a more general version of their results, we need to develop the notion of Frobenius classicality for curves. The case of plane curves will be sufficient for our needs, and for a complete exposition of the theory we refer to [18].

Let X be an irreducible plane curve defined over the finite field $\mathbb{F}_q$. The curve $\mathcal{F}$ is called q-Frobenius non-classical if the image $Fr(P)$ of each simple point P of $\mathcal{F}$ under the Frobenius map lies on the tangent line at P. A more technical approach can be used to rephrase this concept:

Let $X \subset \mathbb{P}^2$ be an irreducible non-linear algebraic curve. The numbers $0 = \epsilon_0 < \epsilon_1 = 1 < \epsilon_2$ represent all possible intersection multiplicities of X with lines of $\mathbb{P}^2$ at a generic point of X. Such a sequence is called the order sequence of X and is also characterized as the smallest sequence (in lexicographic order) such that $\det(D_t^{\epsilon_i} x_j) \neq 0$, where D_t^k denotes the k-th Hasse derivative [1] with respect to a separating variable t and x_0, x_1, x_2 are the coordinate functions on $X \subset \mathbb{P}^2$. The curve X is called classical if $\epsilon_2 = 2$.

If X is defined over a finite field $\mathbb{F}_q$, then there is a smallest integer $\nu_1 \in \{1, \epsilon_2\}$ such that

$$\det \begin{pmatrix} x_0^q & x_1^q & x_2^q \\ x_0 & x_1 & x_2 \\ D_t^{\nu_1} x_0 & D_t^{\nu_1} x_1 & D_t^{\nu_1} x_2 \end{pmatrix} \neq 0.$$

The numbers $\nu_0 = 0, \nu_1$ are called the Frobenius orders of X, and such a curve is called q-Frobenius classical if $\nu_1 = 1$ (this is equivalent to the previous definition).

[1] For a field F, we define the k-th Hasse derivative $D^k : F[[t]] \longrightarrow F[[t]]$ for $k \geq 1$ as follows:

$$D^k(\sum_{n=0}^{\infty} a_n t^n) = \sum_{n=1}^{\infty} a_n \binom{n}{k} t^{n-k}.$$

Theorem 1.5. *(Stöhr-Voloch) Let X be an irreducible plane curve of degree d and genus g defined over $\mathbb{F}_q$. If X has Frobenius orders (ν_0, ν_1), then*

$$\#X(\mathbb{F}_q) \leq \frac{\nu_1(2g-2)+(q+2)d}{2}$$

Not many q-Frobenius non-classical curves ($\nu_1 > 1$) are known. Such curves are rare but very important; for example, they can have many rational points. Some additional properties of these curves can be found in [10]. For instance, for $p > 2$ a q-Frobenius non-classical curve is the locus of its singular and inflection points. Also, with the additional hypothesis that $\mathcal{X}$ is smooth, Hefez and Voloch (Theorem 1 of [10]) managed to prove that

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

where d is the degree of $\mathcal{F}$.

Examples of q-Frobenius non-classical curves are the Fermat curves

$$x^d + y^d + z^d = 0 \tag{1.2}$$

where $d = \frac{q-1}{q'-1}$ and q' is a power of $p > 2$. Note that the Hermitian curve, which is known for many of its special properties, lies in this family of curves.

1.3 (N, d)-arcs and the Griesmer bound

A linear $[n, k, r]$-code over $\mathbb{F}_q$ is a subspace C of dimension k of the vector space $\mathbb{F}_q^n$ in which every non-zero vector has at least r non-zero coordinates, and there is a vector with exactly r non-zero coordinates. The value r is called minimum distance

of C. The Griesmer bound (Theorem 5.2.6 of [21]) states that

$$n \geq \sum_{i=0}^{k-1} \lceil \frac{r}{q^i} \rceil \tag{1.3}$$

Let G be a $k \times n$ matrix whose rows form a basis for C, i.e. G is a generator matrix for C, and let $x = (x_1, \cdots, x_k) \in \mathbb{F}_q^k$ be the j-th column of G. The codeword which is a linear combination of the rows of G, given by a vector $a = (a_1, \cdots, a_k) \in \mathbb{F}_q^k$, has a zero in the j-th coordinate if and only if

$$\sum_{i=0}^{k} a_i x_i = 0. \tag{1.4}$$

Since each codeword has at least r non-zero coordinates, there are at most $n - r$ columns of G, which are incident with the hyperplane defined by the equation (1.4). Now, since the columns of G can be viewed as points of $PG(k-1, q)$, we see that a linear $[n, r, k]$-code C over $\mathbb{F}_q$ is equivalent to a set $\mathcal{A}$ of n points in $PG(k-1, q)$ with the property that some hyperplane is incident with $d = n - r$ points of $\mathcal{A}$ and no hyperplane is incident with more. Such a set $\mathcal{A}$ is called (n, d)-arc in $PG(k-1, q)$. In particular, an (n, d)-arc $\mathcal{A}$ in $PG(2, q)$ is a set of n points with at most d points on any line and with d points on some line. If the (n, d)-arc $\mathcal{A}$ is not contained in an $(n+1, d)$-arc, then we say that $\mathcal{A}$ is complete.

Natural examples of (n, d)-arcs in $PG(2, q)$ are frequently obtained from a set $\mathcal{F}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points of a plane curve $\mathcal{F}$ without linear components and defined over $\mathbb{F}_q$, where $n = \#\mathcal{F}(\mathbb{F}_q)$ and d is the degree of $\mathcal{F}$. If the underlying curve gives a complete (n, d)-arc, then the corresponding code cannot be extended to a code with larger minimum distance. In chapter 3 we will present many curves with such a property and discuss the Griesmer bound for the corresponding codes. Our reason for considering this particular bound (out of many options) is because of the values/range of our parameters; we found that the Griesmer bound would be

the most suitable choice.

Chapter 2

Multi-Frobenius non-classical curves

Based on [18], Hefez and Voloch extended the study of the q-Frobenius non-classical curves in [10], where some interesting arithmetic and geometric properties of such curves were first pointed out. They also remarked that characterizing all such curves seemed to be a very involved problem.

In 1990, Garcia [5] characterized (under certain conditions) q-Frobenius non-classical curves of type $y^n = f(x)$. Among such curves, we have the Fermat curves given in (1.2).

Here, given a prime power q and distinct positive integers $k_1, \cdots, k_s$, we address the problem of finding plane curves being q^{k_i}-Frobenius non-classical for all $i = 1, \cdots, s$. It turns out that there is no such curve for $s \geq 3$, and the case $s = 2$ gives us a unique plane curve. Our work here will provide a characterization of such a curve. More precisely, we will prove the following:

Theorem 2.1. *For any given triple (q, n, m) where q is a prime power and $n > 2$ and $m \geq 1$ are integers such that $n > m$ and $\gcd(n, m) = 1$, the curve given by*

$$\mathcal{F}: \frac{(x^{q^n}-x)(y^{q^m}-y)-(y^{q^n}-y)(x^{q^m}-x)}{(x^{q^2}-x)(y^q-y)-(y^{q^2}-y)(x^q-x)}=0$$

is the unique q^n- and q^m-Frobenius non-classical irreducible plane curve over $\mathbb{F}_q$. Moreover, $\mathcal{F}$ has Frobenius orders $(\nu_0,\nu_1)=(0,q^m)$, and if g and $\mathcal{F}(\mathbb{F}_{q^k})$ are the genus and the set of $\mathbb{F}_{q^k}$-rational points of $\mathcal{F}$, respectively, then

$$g=(q^{n-m}+q^m)(\frac{q^n}{2}-(1+q+q^2))+(q+1)(1+q+q^2)$$

and

$$\#\mathcal{F}(\mathbb{F}_{q^k})=\begin{cases}(q^m-q^2)(q^m-q)+(q^2+q+1)(q^m-q), & \text{if } k=m,\\ (q^n-q^2)(q^n-q), & \text{if } k=n,\\ 0, & \text{if } k=1.\end{cases}$$

Corollary 2.1. *Let q be a prime power and $k_1>k_2>\cdots>k_r$ $(r>1)$ be positive integers. If $\mathcal{F}$ is a q^{k_i}-Frobenius non-classical plane curve for all $i=1,\cdots,r$, then $r=2$, $k_1\neq 2k_2$, and $\mathcal{F}$ can be given as in Theorem 2.1.*

In addition to the above assertions, we point out some of the special properties of these curves obtained for particular cases of q,n and m.

For $m=1$, $\mathcal{F}$ has Frobenius orders $(\nu_0,\nu_1)=(0,q)$, degree $d=q^n-q^2$, and it can be checked that its number of $\mathbb{F}_{q^n}$-rational points is given by

$$N=(\nu_1(2g-2)+(q^n+2)d)/2.$$

In other words, the curve attains the upper bound of Theorem 1.5. In particular, for $q=2$, the curve is classical Frobenius non-classical of genus $g=4^{n-1}-5\cdot 2^{n-1}+7$ and $N=4^n-6\cdot 2^n+8$ $\mathbb{F}_{2^n}$-rational points. Furthermore, $n=3$ gives a curve having

affine equation

$$x^4 + x^2y^2 + y^4 + x^2y + xy^2 + x^2 + xy + y^2 + 1 = 0,$$

genus $g = 3$, and with N=24 $\mathbb{F}_8$-rational points. This curve, which is the unique (up to isomorphism) curve of genus 3 with more than 22 $\mathbb{F}_8$-rational points (proved by Top in [19]), carries the additional property of being the unique non-singular multi-Frobenius non-classical plane curve (Remark 2.11). One more special curve is obtained for the case $n = 4$: the curve has genus $g = 31$ and $N = 168$ $\mathbb{F}_{16}$-rational points, and this beats the current record ($N = 165$) on the number of $\mathbb{F}_{16}$-rational points for curves of genus 31 (see [20]).

Another interesting aspect (from the Finite Geometry viewpoint) of the case $m = 1$ lies with the fact $\mathcal{F}(\mathbb{F}_{q^n})$ gives rise to a complete $((q^n - q)(q^n - q^2), q^n - q^2)$-arc in $PG(2, q^n)$. This is not obvious but can be easily verified, for instance, while proving Lemma 2.10. More details about plane curves giving rise to complete arcs will be given in the next chapter (see also [7]).

For $n - m = 1$, the set of singular points of $\mathcal{F}$ is the whole $PG(2, q)$ (Proposition 2.8), and from Remark 2.9, we have that all such sigularities are ordinary. In this case, $\mathcal{F}$ gives one more example of curves attaining the lower bound in the theorem below (see Theorem 1.4 of [12]).

Theorem 2.2. *(Hirschfeld-Korchmáros) Let $\mathcal{F}$ be a non-classical irreducible plane curve of degree d and genus g. If $\mathcal{F}$ is q-Frobenius non-classical, and has only tame branches, then*

$$B_q \geq (q - 1)d - (2g - 2),$$

where B_q is the number of branches of $\mathcal{F}$ with centre in $PG(2, q)$. Also, equality holds if and only if every non-linear branch of $\mathcal{F}$ is centred at a point of $PG(2, q)$.

With some further calculation, it can also be shown that $\#\mathcal{F}(\mathbb{F}_{q^{n-m}}) =$

$q^{2(n-m)}+q^{n-m}-q^2-q$ and that (observed by Voloch) the dual curve of $\mathcal{F}$, denoted by $\mathcal{F}^*$, is the unique (q^n, q^{n-m})-Frobenius non-classical plane curve over $\mathbb{F}_q$.

The proof of Theorem 2.1 will be deduced through a series of steps given in the next sections. In Section 2.1, we construct the curve $\mathcal{F}$ and establish some immediate properties. In Section 2.2, we characterize the singular points of $\mathcal{F}$ and prove its irreducibility. In Sections 2.3 and 2.4, we obtain explicit formulas for the number of $\mathbb{F}_{q^k}$-rational points ($k \in \{n, m, 1\}$) and genus of $\mathcal{F}$, respectively. We end Section 2.4 by proving Corollary 2.1.

2.1 The curve $\mathcal{F}$

From now on, $n > 2$ and $m \geq 1$ will be integers such that $n > m$ and $\gcd(n, m) = 1$. Also, any plane curve which is q^k-Frobenius non-classical for all $k \in \{n, m\}$ will be referred to as a (q^n, q^m)-Frobenius non-classical curve.

Lemma 2.2. *If $\mathcal{F}$ is a (q^n, q^m)-Frobenius non-classical curve with affine equation given by $f(x, y) = 0$, then the polynomial $f(x, y)$ is a factor of*

$$g(x, y) = (x^{q^n} - x)(y^{q^m} - y) - (y^{q^n} - y)(x^{q^m} - x).$$

Proof. It may be assumed that x is a separating variable, and for $k \in \{n, m\}$, the q^k-Frobenius non-classicality of $\mathcal{F}$ gives

$$0 = \det \begin{pmatrix} 1 & x^{q^k} & y^{q^k} \\ 1 & x & y \\ 0 & 1 & D_x^1 y \end{pmatrix} = (x^{q^k} - x) D_x^1 y - (y^{q^k} - y).$$

Now we have $(x^{q^n} - x) D_x^1 y = (y^{q^n} - y)$ and $(x^{q^m} - x) D_x^1 y = (y^{q^m} - y)$, which gives $(x^{q^n} - x)(y^{q^m} - y) = (y^{q^n} - y)(x^{q^m} - x)$ and finishes the proof.

□

If we let $G(x,y,z)$ be the homogenization of $g(x,y)$ in Lemma 2.2, it is easy to check that every projective line defined over $\mathbb{F}_q$ is a component of $zG(x,y,z)=0$. In other words, $F(x,y,z)=$

$$\frac{(x^{q^n}-xz^{q^n-1})(y^{q^m}-yz^{q^m-1})-(y^{q^n}-yz^{q^n-1})(x^{q^m}-xz^{q^m-1})}{(x^{q^2}-xz^{q^2-1})(y^q-yz^{q-1})-(y^{q^2}-yz^{q^2-1})(x^q-xz^{q-1})} \tag{2.1}$$

is a polynomial in $\mathbb{F}_q[x,y,z]$.

The curve $\mathcal{F}$, given by $F(x,y,z)=0$, will be the main object of study in this chapter.

The statements of the next proposition will be used throughout our proofs.

Proposition 2.3. *(i) $F(x,y,z)$ is symmetric; that is, it is invariant under permutations of x, y and z.*

(ii) $\gcd(n,m)=1$ *implies* $\mathbb{F}_{q^i}\cap\mathbb{F}_{q^j}=\mathbb{F}_q$ *for i and j distinct elements of* $\{n,m,n-m\}$.

(iii) $g(x,y)=(x^{q^n}-x^{q^m})(y^{q^k}-y)-(y^{q^n}-y^{q^m})(x^{q^k}-x)$ *for* $k\in\{n,m\}$, *including the case* $(n,m)=(2,1)$.

(iv) If $\gcd(r,s)=1$ *and* $a,b\in\mathbb{F}_{q^r}$, *then* $\mu=\dfrac{a^{q^s}-a}{b^{q^s}-b}\in\mathbb{F}_{q^s}$ *implies* $\mu=\dfrac{a^q-a}{b^q-b}\in\mathbb{F}_q$.

Proof. Statements (i),(ii) and (iii) are easy to prove, and our proof will be limited to statement (iv). Note that from (ii), we have that $\mu\in\mathbb{F}_q$, which gives $(\mu b-a)^{q^s}=\mu b-a$. Once again (ii) implies $\mu b-a\in\mathbb{F}_q$, i.e. $(\mu b-a)^q=\mu b-a$, and thus $\mu=\dfrac{a^q-a}{b^q-b}\in\mathbb{F}_q$. □

We should mention that our proofs will often take the symmetry of $F(x,y,z)$ into account. In particular, we will only work with affine points, and $F(x,y,1)$ and

$P = (x_0 : y_0 : 1)$ will be referred to as $F(x, y)$ and $P = (x_0, y_0)$ respectively. Also, from now on, the set of points in $PG(2, \overline{\mathbb{F}_q})$ lying on the union of all lines defined over $\mathbb{F}_q$ will be denoted by S; that is, S is the set of zeros of

$$H(x, y, z) = z((x^{q^2} - xz^{q^2-1})(y^q - yz^{q-1}) - (y^{q^2} - yz^{q^2-1})(x^q - xz^{q-1}))$$

in $PG(2, \overline{\mathbb{F}_q})$.

Lemma 2.4. *If S is the set defined above, then*

$$\mathcal{F} \cap S = \begin{cases} (PG(2, q^{n-m}) \backslash PG(2, q)) \cap S, & \text{if } m = 1, \\ PG(2, q^{n-m}) \cap S, & \text{otherwise.} \end{cases}$$

In particular, $\mathcal{F}$ has no linear components defined over $\mathbb{F}_q$.

Proof. From (2.1), it is clear that

$$F(x, y) = \frac{\dfrac{(x^{q^n} - x)(y^{q^m} - y)}{(x^q - x)(y^q - y)} - \dfrac{(y^{q^n} - y)(x^{q^m} - x)}{(x^q - x)(y^q - y)}}{\dfrac{x^{q^2} - x}{x^q - x} - \dfrac{y^{q^2} - y}{y^q - y}}, \tag{2.2}$$

and if we define $g_k(t) = t^{q^{k-2}+\cdots+q+1} + t^{q^{k-3}+\cdots+q+1} + \cdots + t^{q+1} + t + 1$ (with $g_1(t) \equiv 1$) and

$$R(x, y) = \frac{g_n(x)g_m(y) - g_n(y)g_m(x)}{x - y},$$

then it can be easily checked that

(i) $F(x, y) = R((x^q - x)^{q-1}, (y^q - y)^{q-1})$.

(ii) $R(x, x) = g_n'(x)g_m(x) - g_m'(x)g_n(x)$.

(iii) $g_k((x^q - x)^{q-1}) = \dfrac{x^{q^k} - x}{x^q - x}$ and $g_k'((x^q - x)^{q-1}) = (\dfrac{x^{q^{k-1}} - x}{x^q - x})^q$.

Now consider a line given by $y = ax + b$, with $a, b \in \mathbb{F}_q$. If $a \neq 0$, then from (i) we have $F(x, ax + b) = R((x^q - x)^{q-1}, (x^q - x)^{q-1})$, and using (ii) and (iii) we find

$$F(x, ax + b) = \frac{(x^{q^{n-m}} - x)^{q^m}}{(x^q - x)^q} \tag{2.3}$$

Also, using $\dfrac{x^{q^k} - x}{x^q - x}(\lambda) = 1$ for all $\lambda \in \mathbb{F}_q$, it can be verified directly from (2.2) that (2.3) also holds true for $a = 0$, and the result follows.

□

Lemma 2.5. *The set of points of $PG(2, q^{n-m})$ lying on $\mathcal{F}$ is either $PG(2, q^{n-m}) \backslash PG(2, q)$ or the whole $PG(2, q^{n-m})$. The latter case occurs if and only if $m > 1$.*

Proof. If $P \in PG(2, q^{n-m}) \backslash S$, then Remark 2.3.$(iii)$ implies that P is a point on $\mathcal{F}$. For $P \in PG(2, q^{n-m}) \cap S$, the result follows directly from Lemma 2.4. □

If $P = (x_0, y_0)$ is a point of $\mathcal{F}$, and $\ell : (x, y) = (x_0 + aT, y_0 + bT)$ is a line through P, then it follows from (2.1) that $F(x_0 + aT, y_0 + bT) =$

$$\frac{\alpha_1 T^{q^n+q^m} + \alpha_2 T^{q^n+1} + \alpha_3 T^{q^n} + \alpha_4 T^{q^m+1} + \alpha_5 T^{q^m} + \alpha_6 T}{\beta_1 T^{q^2+q} + \beta_2 T^{q^2+1} + \beta_3 T^{q^2} + \beta_4 T^{q+1} + \beta_5 T^q + \beta_6 T + \beta_7} \tag{2.4}$$

where α_i and β_i are given in Table 1 below. This arrangement will be very useful

i	α_i	β_i
1	$a^{q^n} b^{q^m} - a^{q^m} b^{q^n}$	$a^{q^2} b^q - a^q b^{q^2}$
2	$ab^{q^n} - a^{q^n} b$	$ab^{q^2} - a^{q^2} b$
3	$a^{q^n}(y_0^{q^m} - y_0) - b^{q^n}(x_0^{q^m} - x_0)$	$a^{q^2}(y_0^q - y_0) - b^{q^2}(x_0^q - x_0)$
4	$a^{q^m} b - ab^{q^m}$	$a^q b - ab^q$
5	$b^{q^m}(x_0^{q^n} - x_0) - a^{q^m}(y_0^{q^n} - y_0)$	$b^q(x_0^{q^2} - x_0) - a^q(y_0^{q^2} - y_0)$
6	$b(x_0^{q^m} - x_0^{q^n}) - a(y_0^{q^m} - y_0^{q^n})$	$b(x_0^q - x_0^{q^2}) - a(y_0^q - y_0^{q^2})$
7	0	$(x_0^{q^2} - x_0)(y_0^q - y_0) - (y_0^{q^2} - y_0)(x_0^q - x_0)$

Table 2.1: Coefficients

to prove the next assertions.

Lemma 2.6. *The polynomial $F(x, y, z)$ is square-free and has no linear factors.*

Proof. For the first part, it suffices to prove that $g(x, y)$ is square-free, and this can be easily done by considering suitable lines given by either $x = x_0$ or $y = y_0$. Next, we will prove that any linear component of $\mathcal{F}$ is defined over $\mathbb{F}_q$. For this, using Table 1, it suffices to show that $(\alpha_1, \cdots, \alpha_7) = (0, \cdots, 0)$ implies $(\beta_1, \cdots, \beta_7) = (0, \cdots, 0)$. If $ab = 0$, say $a = 0$, then we have $\beta_1 = \beta_2 = \beta_4 = 0$. Also, $\alpha_3 = \alpha_5 = 0$ and Proposition 2.3.(ii) imply $x_0^q = x_0$ which gives $(\beta_1, \cdots, \beta_7) = (0, \cdots, 0)$. For $ab \neq 0$, $\alpha_2 = \alpha_4 = 0$ implies $(a/b)^q = a/b$, and thus $\beta_1 = \beta_2 = \beta_4 = 0$. If $x_0 \in \mathbb{F}_q$, we can easily finish the proof, so we assume $x_0^q \neq x_0$. Now $\alpha_3 = 0$ implies $\dfrac{b}{a} = \dfrac{y_0^{q^m} - y_0}{x_0^{q^m} - x_0} \in \mathbb{F}_q$, and Proposition 2.3.$(iv)$ gives $\dfrac{b}{a} = \dfrac{y_0^q - y_0}{x_0^q - x_0} \in \mathbb{F}_q$, which implies $(\beta_1, \cdots, \beta_7) = (0, \cdots, 0)$. On the other hand, by Lemma 2.4, the curve $\mathcal{F}$ has no linear components defined over $\mathbb{F}_q$. Hence, the result follows.

□

Theorem 2.3. *Any irreducible component $\tilde{\mathcal{F}}$ of $\mathcal{F}$ has order sequence $(0, 1, q^m)$. Moreover, if $k \in \{n, m\}$ and $\tilde{\mathcal{F}}$ is defined over $\mathbb{F}_{q^k}$, then $\tilde{\mathcal{F}}$ is a q^k-Frobenius non-classical curve.*

Proof. Let $\tilde{\mathcal{F}}$ be an irreducible component of $\mathcal{F}$. Suppose $\ell : (x, y) = (x_0 + aT, y_0 + bT)$ is the line tangent to $\tilde{\mathcal{F}}$ at $P = (x_0, y_0)$, a simple point that satisfies

$$(x_0^{q^{2m}} - x_0^{q^m})(y_0^{q^m} - y_0) - (y_0^{q^{2m}} - y_0^{q^m})(x_0^{q^m} - x_0) \neq 0 \tag{2.5}$$

and

$$(x_0^{q^m} - x_0^{q^n})(y_0^{q^m} - y_0^{q^n})(y_0^{q^m} - y_0)(y_0^{q^n} - y_0) \neq 0 \tag{2.6}$$

Note that, because $\mathcal{F}$ has no linear components, only a finite number of points is

being excluded. Also, since ℓ is the tangent line, (2.4) implies $\alpha_6 = 0$, and we claim that $\alpha_5 \neq 0$. In fact, if $\alpha_5 = \alpha_6 = 0$, then Proposition 2.3.(iii) and (2.6) yield

$$(\frac{a}{b})^{q^m} = \frac{x_0^{q^n} - x_0}{y_0^{q^n} - y_0} = \frac{x_0^{q^m} - x_0}{y_0^{q^m} - y_0} = \frac{x_0^{q^n} - x_0^{q^m}}{y_0^{q^n} - y_0^{q^m}} = \frac{a}{b}$$

which implies $(\frac{x_0^{q^m} - x_0}{y_0^{q^m} - y_0})^{q^m} = \frac{x_0^{q^m} - x_0}{y_0^{q^m} - y_0}$, contradicting (2.5). Therefore, we have $\alpha_5 \neq 0$. Now, since (2.5) implies $\beta_7 \neq 0$, from (2.4) we obtain

$$F(x_0 + aT, y_0 + bT) = \frac{\alpha_5}{\beta_7} T^{q^m} + a_1 T^{q^m+1} + \cdots \tag{2.7}$$

On the other hand, by Lemma 2.6, we have $F(x, y) = F_1(x, y) \cdots F_s(x, y)$, where F_i are irreducible non-linear polynomials, and $\gcd(F_i, F_j) = 1$ for $i \neq j$. Thus it may be assumed that $\tilde{\mathcal{F}}$ is the component corresponding to $F_1(x, y)$, and $P = (x_0, y_0)$ does not lie on the remaining components of $\mathcal{F}$. Again, by Bezout's theorem, we are neglecting only a finite number of points, and thus (2.7) gives

$$F_1(x_0 + aT, y_0 + bT) = \gamma T^{q^m} + b_1 T^{q^m+1} + \cdots$$

for some $\gamma \neq 0$, which finishes the first part.

For the other part, using the same point P and $\alpha_6 = 0$, from (2.6) and Table 1 we obtain $ab \neq 0$ and $b = (\frac{y_0^{q^n} - y_0^{q^m}}{x_0^{q^n} - x_0^{q^m}})a$. Now setting $T_1 = \frac{x_0^{q^n} - x_0}{a}$, we obtain $x_0 + aT_1 = x_0^{q^n}$ and $y_0 + bT_1 = y_0 + (\frac{y_0^{q^n} - y_0^{q^m}}{x_0^{q^n} - x_0^{q^m}})(x_0^{q^n} - x_0) = y_0^{q^n} + (\frac{y_0^{q^n} - y_0^{q^m}}{x_0^{q^n} - x_0^{q^m}})(x_0^{q^m} - x_0) - (y_0^{q^m} - y_0) = y_0^{q^n}$, where the last equality follows from Proposition 2.3.(iii) . Therefore, P^{q^n} (the image of P under the Frobenius map) lies on the tangent line at P. A similar argument, with $T_2 = \frac{x_0^{q^m} - x_0}{a}$, shows that P^{q^m} also lies on the tangent line at P, which completes the proof. $\square$

2.2 The Singular Points

In this section, we investigate the singular points of $\mathcal{F}$. A characterization of such points is obtained and used to prove that $F(x, y)$ is absolutely irreducible.

Let $P = (x_0, y_0)$ be a point on $\mathcal{F}$ and consider $f(x, y) = F(x + x_0, y + y_0) = \frac{\sum_{i=0}^{7} g_i}{\sum_{i=0}^{7} h_i} = f_1 + \cdots + f_d$, where g_i, h_i, given in Table 2 below, are obtained from (2.1), and the f_i's are homogeneous components of f of degree i.

i	g_i	h_i
1	$x^{q^n}y^{q^m} - x^{q^m}y^{q^n}$	$x^{q^2}y^q - x^q y^{q^2}$
2	$xy^{q^n} - x^{q^n}y$	$xy^{q^2} - x^{q^2}y$
3	$x^{q^n}(y_0^{q^m} - y_0) - y^{q^n}(x_0^{q^m} - x_0)$	$x^{q^2}(y_0^q - y_0) - y^{q^2}(x_0^q - x_0)$
4	$x^{q^m}y - xy^{q^m}$	$x^q y - xy^q$
5	$y^{q^m}(x_0^{q^n} - x_0) - x^{q^m}(y_0^{q^n} - y_0)$	$y^q(x_0^{q^2} - x_0) - x^q(y_0^{q^2} - y_0)$
6	$y(x_0^{q^m} - x_0^{q^n}) - x(y_0^{q^m} - y_0^{q^n})$	$y(x_0^q - x_0^{q^2}) - x(y_0^q - y_0^{q^2})$
7	0	$(x_0^{q^2} - x_0)(y_0^q - y_0) - (y_0^{q^2} - y_0)(x_0^q - x_0)$

Table 2.2: Components g_i and h_i.

Lemma 2.7. *Let $P = (x_0, y_0) \in PG(2, q^{n-m}) \backslash PG(2, q)$ be a point on $\mathcal{F}$. If $\gcd(g_4, g_5) \neq 1$, then $h_7 = 0$ and $\gcd(g_4, g_5) = h_6$. Also, $h_7 = 0$ implies $h_6 \mid h_5$.*

Proof. This follows from a straightforward calculation using the data from Table 2 and Proposition 2.3. □

Henceforth, for any point P on $\mathcal{F}$, we will denote by $J_P = \{j_1, \cdots, j_k\}$, with $j_i < j_{i+1}$, the set of all intersection numbers given by the pencil of lines through P. Note that $j_1 = m_P$, the multiplicity of P on $\mathcal{F}$. Also, for the next theorem, recall from Section 2.1 that S is the set of points in $PG(2, \overline{\mathbb{F}_q})$ lying on the lines defined over $\mathbb{F}_q$.

Proposition 2.8. *If $(m,q) \neq (1,2)$, then the set of singular points of $\mathcal{F}$ is either $PG(2,q^{n-m})$ or $PG(2,q^{n-m})\backslash PG(2,q)$. The latter case occurs if and only if $m = 1$. If $(m,q) = (1,2)$, then the set of singular points is given by $PG(2,2^{n-1})\backslash S$. Moreover, if $P \in PG(2,q^{n-m})$ lies on $\mathcal{F}$, then*

$$J_P = \begin{cases} \{q^m, q^m+1\}, & \text{if } P \notin S, \\ \{q^m-1, q^m\}, & \text{if } P \in S\backslash PG(2,q), \\ \{q^m-q, q^n-q\}, & \text{if } P \in PG(2,q). \end{cases}$$

Proof. Let $P = (x_0, y_0)$ be a point of $\mathcal{F}$. Table 2 gives $P \in PG(2,q^{n-m})$ if and only if $g_6 = 0$. Now if P is a singular point, then $f_1 = 0$ and from $(\sum_{i=0}^{7} h_i)(f_1 + \cdots + f_d) = \sum_{i=0}^{7} g_i$ we have $g_6 = 0$, i.e. $P \in PG(2,q^{n-m})$. Conversely, for $P \in PG(2,q^{n-m})$, we have following two cases:

(i) $P \notin PG(2,q)$: Since $g_6 = 0$, Proposition 2.3.(ii) implies $g_5 \neq 0$ and $h_6 \neq 0$, and after a simple computation using

$$(\cdots + h_6 + h_7)f(x,y) = \cdots + g_4 + g_5,$$

we have

$$f(x,y) = \begin{cases} \frac{g_5}{h_7} + (\frac{g_4}{h_7} - h_6\frac{g_5}{h_7^2}) + \cdots, & \text{if } h_7 \neq 0, \\ \frac{g_5}{h_6} + (\frac{g_4}{h_6} - h_5\frac{g_5}{h_6^2}) + \cdots, & \text{if } h_7 = 0 \text{ and } q = 2, \\ \frac{g_5}{h_6} + \frac{g_4}{h_6} + \cdots, & \text{if } h_7 = 0 \text{ and } q \neq 2, \end{cases} \tag{2.8}$$

where $\cdots$ represents the terms of higher degree. Note that, from Lemma 2.7, the first two homogeneous components of $f(x,y)$ given in (2.8) have no common factors. Now, since $h_7 = 0$ if and only if $P \in S$, the decomposition

in (2.8) implies

$$J_P = \begin{cases} \{q^m, q^m + 1\}, & \text{if } P \notin S, \\ \{q^m - 1, q^m\}, & \text{if } P \in S. \end{cases} \tag{2.9}$$

On the other hand, from Lemma 2.5, all points of $PG(2, q^{n-m})\backslash PG(2, q)$ are points on $\mathcal{F}$. Now (2.9) shows that all such points are singular, except in the case $(q, m) = (2, 1)$, where the singular points are restricted to $PG(2, 2^{n-1})\backslash S$.

(ii) $P \in PG(2, q)$: Table 2 and $(\cdots + h_4)f(x, y) = \cdots + g_4$ give us

$$f(x, y) = \frac{x^{q^m} y - x y^{q^m}}{x^q y - x y^q} + \tilde{f}(x, y), \tag{2.10}$$

where $\tilde{f}(x, y)$ comprises the homogeneous terms of higher degree. Since $f(x, y) = \dfrac{g_1 + g_2 + g_4}{h_1 + h_2 + h_4}$, for $\lambda \in \mathbb{F}_{q^m}\backslash\mathbb{F}_q$, we have $f(x, \lambda y) = \tilde{f}(x, \lambda x) = c x^{q^n - q} + \cdots$ with $c \neq 0$, and hence

$$J_P = \{q^m - q, q^n - q\}. \tag{2.11}$$

Since $P \in PG(2, q)$ is a point on $\mathcal{F}$, from Lemma 2.5, we have $m > 1$, and thus all points of $PG(2, q)$ lie on $\mathcal{F}$. Now (2.11) implies that all such points are singular, which completes the proof. □

Remark 2.9. *Note that if $P = (x_0, y_0) \in PG(2, q^{n-m})$ is a singular point of $\mathcal{F}$, then Table 2 with (2.8) and (2.10) in the proof of Proposition 2.8 characterize the tangent lines at P, i.e. the lines giving maximum intersection number. For instance, since $g_5 = y^{q^m}(x_0^{q^n} - x_0) - x^{q^m}(y_0^{q^n} - y_0)$ is a power of a linear form, (2.8) implies that the singular points $P \in PG(2, q^{n-m})\backslash PG(2, q)$ have only one tangent line, which will be named ℓ in the proof of the next theorem. Also, if $m > 1$, then (2.10) implies that all points of $PG(2, q)$ are ordinary singularities of $\mathcal{F}$. Such points have multiplicity $m_P = q^m - q$ and their tangent lines are defined over $\mathbb{F}_{q^m}$ but not over $\mathbb{F}_q$.*

Theorem 2.4. *The curve $\mathcal{F}$ is irreducible and is the unique (q^n, q^m)-Frobenius non-classical plane curve over $\mathbb{F}_q$. Also, $\mathcal{F}$ has Frobenius orders given by $(\nu_0, \nu_1) = (0, q^m)$.*

Proof. Once we prove irreducibility, Lemma 2.2 gives the uniqueness, and Theorem 2.3 gives the remaining parts. Suppose $\mathcal{F}$ has multiple components. Clearly, such components will intersect at singular points of $\mathcal{F}$. Let $P \notin PG(2,q)$ be a common point of two irreducible components, say $\mathcal{F}_1$ and $\mathcal{F}_2$. Now Remark 2.9 implies that the branches of $\mathcal{F}_i$ centred at P have the same tangent line, say ℓ, and by (2.9) we have $\mathcal{I}(P, \mathcal{F} \cap \ell) \leq q^m + 1$. On the other hand, by Theorem 2.3, each component $\mathcal{F}_i$ has order sequence $(0, 1, q^m)$ which gives $\mathcal{I}(P, \mathcal{F}_i \cap \ell) \geq q^m$, and then

$$q^m + 1 \geq \mathcal{I}(P, \mathcal{F} \cap \ell) \geq \mathcal{I}(P, \mathcal{F}_1 \cap \ell) + \mathcal{I}(P, \mathcal{F}_2 \cap \ell) \geq 2q^m,$$

a contradiction. Therefore, $\mathcal{F}$ has no components meeting at a singular point $P \notin PG(2,q)$.

Now suppose $F = F_1F_2$, and $P \in PG(2,q)$ is a point lying on the intersection of the two corresponding components, $\mathcal{F}_1$ and $\mathcal{F}_2$. We may assume $P = (0,0)$, and using (2.10) in the proof of Proposition 2.8 we have $f(x,y) = f_1(x,y)f_2(x,y)$, where

- $f(x,y) = \prod_{\alpha_i \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q} (x - \alpha_i y) + \cdots$
- $f_1(x,y) = \prod_{i=1}^{s} (x - \alpha_i y) + \cdots$
- $f_2(x,y) = \prod_{i=s+1}^{q^m - q} (x - \alpha_i y) + \cdots$

and $\cdots$ represents homogeneous components of higher degree. For $i = 1, 2$, let ℓ_i be a tangent line of $\mathcal{F}_i$ at P. It is clear that $\ell_1 \neq \ell_2$, and from (2.11) in the proof of Proposition 2.8 we have $\mathcal{I}(P, \mathcal{F} \cap \ell_i) = q^n - q$. Therefore, if d_1 and d_2 are the degrees of f_1 and f_2, respectively, then

$$q^n - q = \mathcal{I}(P, \mathcal{F} \cap \ell_1) = \mathcal{I}(P, \mathcal{F}_1 \cap \ell_1) + \mathcal{I}(P, \mathcal{F}_2 \cap \ell_1) \leq d_1 + q^m - q - s$$

and

$$q^n - q = \mathcal{I}(P, \mathcal{F} \cap \ell_2) = \mathcal{I}(P, \mathcal{F}_1 \cap \ell_2) + \mathcal{I}(P, \mathcal{F}_2 \cap \ell_2) \leq s + d_2$$

Now, since $d_1 + d_2 = q^n + q^m - q^2 - q$, we have $q^n + 2q^m - q^2 - 2q \geq 2q^n - 2q$, which implies $n \leq m$, a contradiction. Hence, the result follows. □

2.3 The Rational Points

Here, for $k \in \{n, m, 1\}$, we will compute the number of $\mathbb{F}_{q^k}$-rational points of $\mathcal{F}$. For this, we will first look at $M_{q^k}(\mathcal{F})$ which will denote the set of solutions of $F(x, y, z) = 0$ in $PG(2, q^k)$.

With simple combinatorial arguments, one can easily prove the following:

Lemma 2.10. *Let q be a prime power and k a positive integer. If N is the number of points in $PG(2, q^k)$ lying on the complement of the union of all lines defined over $\mathbb{F}_q$, then*

$$N = (q^k - q^2)(q^k - q).$$

Remark 2.11. *Note that Lemma 2.10 is a statement about the set S (defined in Section 2.1) and gives us $\#(PG(2, q^k) \cap S) = q^k(q^2 + q + 1) + 1 - q^3$ which will be used in Theorem 2.6. Also, since $N = \#(PG(2, q^k) \backslash S) = 0$ if and only if $k \in \{1, 2\}$, it follows from Proposition 2.8 that $\mathcal{F}$ is smooth if and only if $(q, n, m) = (2, 3, 1)$.*

Lemma 2.12. *If $k \in \{n, m, 1\}$, then*

$$\#M_{q^k}(\mathcal{F}) = \begin{cases} (q^k - q^2)(q^k - q), & \text{if } m = 1, \\ (q^k - q^2)(q^k - q) + q^2 + q + 1, & \text{otherwise.} \end{cases}$$

Proof. Since $F(x, y) = \dfrac{(x^{q^n} - x)(y^{q^m} - y) - (y^{q^n} - y)(x^{q^m} - x)}{(x^{q^2} - x)(y^q - y) - (y^{q^2} - y)(x^q - x)}$, it is clear that for $k \in \{n, m, 1\}$ we have $PG(2, q^k) \backslash S \subset M_{q^k}(\mathcal{F})$. Also, Lemma 2.10 gives $\#(PG(2, q^k) \backslash S) = (q^k - q^2)(q^k - q)$, and since $\mathbb{F}_{q^k} \cap \mathbb{F}_{q^{n-m}} = \mathbb{F}_q$, Lemma 2.4 finishes the proof.

□

Theorem 2.5. *If $\mathcal{F}(\mathbb{F}_{q^k})$ is the set of $\mathbb{F}_{q^k}$-rational points of $\mathcal{F}$, then*

$$\#\mathcal{F}(\mathbb{F}_{q^k}) = \begin{cases} (q^m - q^2)(q^m - q) + (q^2 + q + 1)(q^m - q), & \text{if } k = m, \\ (q^n - q^2)(q^n - q), & \text{if } k = n, \\ 0, & \text{if } k = 1. \end{cases}$$

Proof. Since $\mathbb{F}_{q^k} \cap \mathbb{F}_{q^{n-m}} = \mathbb{F}_q$, by Proposition 2.8 the $(q^k - q^2)(q^k - q)$ points of $PG(2, q^k) \backslash S$ are non-singular points of $\mathcal{F}$. This gives us $(q^k - q^2)(q^k - q)$ $\mathbb{F}_{q^k}$-rational points. For $m > 1$, from Remark 2.9, we have that the extra $1 + q + q^2$ points of $M_{q^k}(\mathcal{F})$, given by Lemma 2.12, are ordinary singularities of $\mathcal{F}$. Since the $q^m - q$ tangent lines are defined over $\mathbb{F}_{q^m}$ but not over $\mathbb{F}_{q^k}$, with $k \in \{n, 1\}$, the result follows.

□

2.4 The Genus

To compute the genus of $\mathcal{F}$, we first recall a genus formula based on the notion of *infinitely near points*.

Suppose $\mathcal{F}$ is an irreducible plane curve and P is a singular point of $\mathcal{F}$. Let $\mathcal{F}_1$ be the blowing up of $\mathcal{F}$ at P and E be the exceptional curve of the blow up. If $P_1 \in \mathcal{F}_1 \cap E$ is a singular point of $\mathcal{F}_1$, then P_1 is called an infinitely near singular point of $\mathcal{F}$ over P. In a similar way, the infinitely near singular points of $\mathcal{F}_1$ over P_1 are also called infinitely near singular point of $\mathcal{F}$ over P, and so on. Regarding P itself as an infinitely near singular point of $\mathcal{F}$ over P, we consider the integer given by

$$\delta_P = \sum_Q \frac{m_Q(m_Q - 1)}{2}$$

where Q runs over all infinitely near singular points of $\mathcal{F}$ over P, and m_Q is the multiplicity of each point Q. If d is the degree of $\mathcal{F}$, it turns out that the genus of $\mathcal{F}$ is given by

$$g = \frac{(d-1)(d-2)}{2} - \sum_P \delta_P \tag{2.12}$$

where the sum is taken over all singular points P of $\mathcal{F}$. For a more detailed discussion on this topic we refer to chapter V of [8].

Here, we will make use of (2.12) to compute the genus of the curve $\mathcal{F}$, and for this we also recall the following.

Lemma 2.13. *Let $\mathcal{F} : f(x, y) = 0$ be an irreducible plane curve of degree d and P be a singular point of $\mathcal{F}$ of multiplicity m_P. If the tangent lines [2] $\ell_1, \cdots, \ell_{m_P}$ of $\mathcal{F}$ at P are all distinct, or if $\mathcal{I}(P, \mathcal{F} \cap \ell_i) = m_P + 1$, for $i = 1, \cdots, m_P$, then $\delta_P = m_P(m_P - 1)/2$.*

Proof. We will prove that the infinitely near points $P_1, \cdots, P_s$ in the first neighborhood of P are smooth points of $\tilde{\mathcal{F}}$, the blowing up of $\mathcal{F}$ at P. It may be assumed that $P = (0, 0)$ and that $x = 0$ is not a tangent line at P. We set with $r = m_P$, and

[2] Here, a line ℓ is called tangent to $\mathcal{F}$ at the point P if $\mathcal{I}(P, \mathcal{F} \cap \ell) > m_P$.

from $f(x,y) = f_r(x,y) + f_{r+1}(x,y) + \cdots + f_d(x,y)$, we have $f(x,xy) = x^r \tilde{f}(x,y)$, where $\tilde{f}(x,y) = f_r(1,y) + x f_{r+1}(1,y) + \cdots + x^{d-r} f_d(1,y)$.

Now we claim that the points $Q = (0,\alpha)$ such that $f_r(1,\alpha) = 0$ are smooth points of $\tilde{f}(x,y) = 0$. In fact, since $\tilde{f}_y(0,\alpha) = g'(\alpha)$ (where $g(y) = f_r(1,y)$) and $\tilde{f}_x(0,\alpha) = f_{r+1}(1,\alpha)$, we have:

- If the tangent lines are all distinct, then $f_r(1,y) = 0$ has no repeated roots, which gives $g'(\alpha) \neq 0$, and thus $\tilde{f}_y(0,\alpha) \neq 0$.
- If $\mathcal{I}(P, \mathcal{F} \cap \ell_i) = r+1$ for all the tangent lines ℓ_i, then $\gcd(f_r(x,y), f_{r+1}(x,y)) = 1$. Therefore, $f_r(1,\alpha) = 0$ implies $f_{r+1}(1,\alpha) \neq 0$, which gives $\tilde{f}_x(0,\alpha) \neq 0$.

Hence, in either case, $Q = (0,\alpha)$ is a smooth point of $\tilde{f}(x,y) = 0$ and we obtain $\delta(P) = m_P(m_P - 1)/2$.

□

Theorem 2.6. *The curve $\mathcal{F}$ has genus given by*

$$g = (q^{n-m} + q^m)(\frac{q^n}{2} - (1 + q + q^2)) + (q+1)(1+q+q^2).$$

Proof. If $P \notin PG(2,q)$ is a singular point of $\mathcal{F}$, then Proposition 2.8 implies $J_P = \{m_P, m_P+1\}$ and Lemma 2.13 gives $\delta_P = m_P(m_P-1)/2$. For $P \in PG(2,q)$, Remark 2.9 and Lemma 2.13 also give $\delta_P = m_P(m_P-1)/2$. Now, based on Proposition 2.8, the number of points of multiplicity $m_P = q^m$ can be obtained from Lemma 2.10 for $k = n - m$. The number of singularities with $m_P = q^m - 1$ and $m_P = q^m - q$ in the other two cases can also be easily deduced (see Remark 2.11). In summary, each singular point P of $\mathcal{F}$ satisfies $\delta_P = m_P(m_P-1)/2$, and lies in $PG(2, q^{n-m})$, which can the be partitioned into

1. $(q^{n-m} - q)(q^{n-m} - q^2)$ points of multiplicity q^m,
2. $(q^{n-m} - 1)(1 + q + q^2) + 1 - q^3$ points of multiplicity $q^m - 1$,

3. q^2+q+1 points of multiplicity q^m-q.

Now, using this data together with $d = q^n + q^m - q^2 - q$ and (2.12), we obtain the above value of g. □

Finally, putting together Theorems 2.3, 2.4, 2.5 and 2.6, we have a proof of Theorem 2.1. We finish this section with the following:

Proof of Corollary 2.1. Note that for any prime power q and $k_1 > k_2$ positive integers with $k_1 \neq 2k_2$, one can replace q by $q^{\gcd(k_1,k_2)}$ and apply Theorem 2.1 for $n = k_1/\gcd(k_1,k_2)$ and $m = k_1/\gcd(k_1,k_2)$. That is, if $k_1 \neq 2k_2$, then we have a unique (q^{k_1}, q^{k_2})-Frobenius non-classical plane curve, and such a curve has Frobenius orders given by $(0,\nu_1) = (0, q^{k_2})$.

Now suppose $k_1 > k_2 > k_3$ are positive integers, and $\mathcal{F}$ is a $(q^{k_1}, q^{k_2}, q^{k_3})$-Frobenius non-classical plane curve. Thus $\mathcal{F}$ is automatically both, a (q^{k_1}, q^{k_2})- and (q^{k_1}, q^{k_3})-Frobenius non-classical plane curve, which implies $\nu_1 = q^{k_2} = q^{k_3}$ and contradicts $k_2 > k_3$. Hence, the result follows. □

Chapter 3

Complete (N, d)-arcs derived from plane curves.

In this part, we will be mainly interested in (N, d)-arcs arising from plane curves. As a matter of terminology, we shall say that a curve $\mathcal{F}$ of degree d has the arc property whenever $\mathcal{F}$ gives rise to a complete $(\#\mathcal{F}(\mathbb{F}_q), d)$-arc in $PG(2, q)$. Deciding whether or not certain curves have the arc property is, in general, a difficult problem. With the exception of conics, cubics and Hermitian curves, very little is known about the arc property of curves in general. In Theorem 3.5 of [7], the authors give sufficient conditions for a Frobenius non-classical curve to have the arc property [3]. They also present new complete arcs arising from plane curves, most having irreducible components given by q-Frobenius non-classical curves. In contrast, our work here presents new complete arcs which are mostly derived from curves with q-Frobenius classical components.

In [16], the authors constructed plane curves over $\mathbb{F}_p$, with the number of $\mathbb{F}_p$-rational points attaining the upper bound on Theorem 1.4. In [22], Voloch remarked

[3] It should be noted that not all q-Frobenius non-classical curves have the arc property. For instance, one can check that the curve $x^{13} = y^9 + y^3 + y$ is 27-Frobenius non-classical and does not have the arc property. This gives a negative answer for a question raised in [7].

that such curves would be somewhat large as (N, d)-arcs, and asked whether or not those (N, d)-arcs are complete.

In Section 3.1, after extending the construction of such curves to non-prime fields $\mathbb{F}_q$, we answer Voloch's question.

In Section 3.2, we consider a particular case of Theorem 3.1 and construct complete (N, d)-arcs of parameters $((q^2+4q-5)/4, (q-1)/2)$ and $((q^2+4q+7)/4, (q+3)/2)$ in $PG(2, q)$.

In Section 3.3, we intersect the Hermitian curve with certain conics, and prove that the $\mathbb{F}_{q^2}$-maximal curve $x^{\frac{q+1}{2}} + y^{\frac{q+1}{2}} + z^{\frac{q+1}{2}} = 0$ gives rise to a complete $((q^3+3q+4)/4, (q+1)/2)$-arc in $PG(2, q^2)$. We also present complete $(q^3+q+2, q+3)$-arcs in $PG(2, q^2)$ by considering the union of the Hermitian curve with some conics.

In Section 3.4, we present a small complete (N, d)-arc of parameters $(2q - \sqrt{q} - 1, \sqrt{q} - 1)$ in $PG(2, q)$ obtained from another Fermat curve.

In Section 3.5, we have a table summarizing the (N, d)-arcs and compare some of our parameters with others previously obtained. The Griesmer bound is also discussed.

A special set of lines will play an important role in the development of the first section. Some of the basic properties of such a set are presented next .

Theorem 3.1. *Let q be a prime power and k be a divisor of $q-1$. If L is the set of $3(k+1)$ lines in $PG(2, q)$ given by the components of $xyz(x^k-y^k)(x^k-z^k)(y^k-z^k) = 0$, then the number of points in $PG(2, q)$ comprised by the union of such lines is given by*

$$3q(k+1) - 3k - 2k^2. \tag{3.1}$$

In addition, if we define the sets

$A = \{(\xi_i : \xi_j : 1) | 1 \leq i, j \leq k \text{ and } \xi_i^k = \xi_j^k = 1\}$

$B = \{(\xi_i : 1 : 0), (\xi_i : 0 : 1), (0 : 1 : \xi_i) | 1 \leq i \leq k \text{ and } \xi_i^k = 1\}$

$C = \{(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)\},$

then the following holds:

(1) $A \cup B \cup C$ *is the set of all points that occur as the intersection of lines in* L*.*

(2) Each point in C *lies on exactly* $k + 2$ *lines in* L*.*

(3) Each point P *in* A *lies on exactly three lines in* L*. These three lines are the ones connecting* P *wih each point in* C*.*

(4) Each point P *in* B *lies on exactly two lines in* L*. One such line connects the two points of* C *collinear with* P*, and the other line connects* P *with the third point of* C*.*

Proof. Let L_1, L_2 and L_3 be the sets of lines corresponding to the linear components of $y^k - z^k = 0$, $x^k - z^k = 0$ and $x^k - y^k = 0$ respectively. It is clear that the k lines in each of the three sets are incident with a point in $C = \{(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)\}$. Therefore, the union of lines in each set L_i comprises $kq + 1$ points of $PG(2, q)$. Also, intersecting the lines from any two different sets L_i and L_j, gives us the same set of k^2 points, namely $A = \{(\xi_i : \xi_j : 1) | 1 \leq i, j \leq k$ and $\xi_i^k = \xi_j^k = 1\}$. Thus, by the inclusion-exclusion principle we have collected $3(kq + 1) - 2k^2$ points in $PG(2, q)$ comprised by the union of the lines in the sets L_i, $i = 1, 2, 3$. One can also see that the line $x = 0$ intersects the lines from L_1 in a set of k points, namely $\{(0 : 1 : \xi_i) | 1 \leq i \leq k$ and $\xi_i^k = 1\}$ and intersects the lines from L_2 and L_3 at $(0 : 1 : 0)$ and $(0 : 0 : 1)$ respectively. Thus, including

the line $x = 0$ will only give us $(q+1)-(k+2) = q-k-1$ extra points. By symmetry, including the three components of $xyz = 0$ will give us $3(q-k-1)$ extra points. Therefore, the union of the $3(k+1)$ lines of L will provide a set of $3(kq+1)-2k^2+3(q-k-1) = 3q(k+1)-3k-2k^2$ points in $PG(2,q)$. Finally, one should note that the counting process above automatically reveals the properties claimed for the sets A, B and C. □

Corollary 3.1. *If $S \subset PG(2,q)$ is the set of points comprised by the union of the $3(k+1)$ lines in L, and l is a line in $PG(2,q)$ which is not in L, then the following holds:*

(1) $S = PG(2,q)$ if and only if $k = (q-1)/2$ or $k = q-1$.

(2) If $\#(l \cap C) > 0$, then $\#(l \cap A) = \#(l \cap B) = 0$ and $\#(l \cap S) = 2k+2$.

(3) If $\#(l \cap C) = 0$, then $\#(l \cap S) = 3(k+1) - (2\#(l \cap A) + \#(l \cap B))$.

Proof. (1) This follows directly from $\#S = 3q(k+1) - 3k - 2k^2$.

(2) We may assume $l \cap C = \{(1:0:0)\}$, with l given by $y - \alpha z = 0$ and $\alpha \neq 0$. It is clear that if we have either $\#(l \cap A) > 0$ or $\#(l \cap B) > 0$, then we get $\alpha^k = 1$ which implies $l \in L$, a contradiction. Therefore, $\#(l \cap A) = \#(l \cap B) = 0$. Now, by Theorem 3.1(2), l intersects $k+2$ lines in L at $P = (1:0:0)$, and, by Theorem 3.1 (1), l intersects the remaining $2k+1$ lines at $2k+1$ distinct points. That gives $\#(l \cap S) = 2k+2$.

(3) Since $l \notin L$, items (3) and (4) of Theorem 3.1 imply that, for each $P \in l \cap A$, l intersects three lines in L meeting at P, and for each $Q \in l \cap B$, l intersects two lines of L meeting at Q. Therefore l intersects $3\#(l \cap A) + 2\#(l \cap B)$ lines in L in a set of $\#(l \cap A) + \#(l \cap B)$ points. Since $\#(l \cap C) = 0$, Theorem 3.1(1) implies that l intersects the remaining $3(k+1) - (3\#(l \cap A) + 2\#(l \cap B))$

lines in exactly $3(k+1) - (3\#(l \cap A) + 2\#(l \cap B))$ points. Hence, $\#(l \cap S) = 3(k+1) - (2\#(l \cap A) + \#(l \cap B))$.

□

3.1 Arcs obtained from curves with many points

A construction of curves (over $\mathbb{F}_p$) attaining the upper bound in Theorem 1.4 is presented in [16]. Here, we present the corresponding construction over non-prime fields $\mathbb{F}_q$, and referring to such curves as "$\mathcal{C}_k$", we investigate $\mathcal{C}_k(\mathbb{F}_q)$ viewed as (N, d)-arcs.

Theorem 3.2. *Let $q = p^u$ be an odd prime power and $k < (q-1)/2$ be a divisor of $q-1$ such that $p \nmid (k+1)$. If $m = \frac{q-1-2k}{k}$, then the plane curve*

$$\mathcal{C}_k : \sum_{r+s+t=m} (x^r y^s z^t)^k = 0$$

is smooth of degree $d = q-1-2k$, and $\#\mathcal{C}_k(\mathbb{F}_q) = d(d+q-1)/2$.

Proof. Defining $h(t) = (t^{q-1} - 1)/(t^k - 1)$, we can see that $f(x, y) = (h(x) - h(y))/(x^k - y^k)$ is a polynomial of degree $d = q - 1 - 2k$. Also, since $d = mk$, one can check that $z^d f(\frac{x}{z}, \frac{y}{z}) = \sum_{r+s+t=m} (x^r y^s z^t)^k$.
The smoothness part can be derived from the fact that $f(x, y) = G_m(x^k, y^k, 1)$, where $G_m(x, y, z) = 0$ is the curve in Theorem 1 of [**?**], which is smooth whenever $p \nmid (m+1)(m+2)$.

To count the $\mathbb{F}_q$-solutions of $f(x, y) = 0$, note that $h(\alpha) = h(\beta) = 0$ with $\alpha^k \neq \beta^k$ implies $f(\alpha, \beta) = 0$. Therefore, all the pairs $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q$ satisfying $1 \neq \alpha^k \neq \beta^k \neq 1$ and $\alpha\beta \neq 0$ will be solutions of $f(x, y) = 0$. Since $k(m+2) = q-1$, the $m+1$ choices of α^k followed by the m choices of β^k give $(m+1)mk^2 = d(d+q-1)/2$ such solutions.

To show that $\mathcal{C}_k$ is attaining the upper bound in Theorem 1.4, it suffices to prove that $\mathcal{C}_k$ has finitely many inflection points. This is indeed the case because $p \nmid (d-1)$, and we can apply Corollary 2.2 of [15]. Hence, $\#\mathcal{C}_k(\mathbb{F}_q) = d(d+q-1)/2$. $\square$

We point out that because the upper bound was achieved, $f(x,y) = 0$ has no solution $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q$ with either coordinate being zero or a k-th root of unity. An immediate consequence is that the $3(k+1)$ lines given by the components of $xyz(x^k - y^k)(x^k - z^k)(y^k - z^k) = 0$ do not intersect $\mathcal{C}_k(\mathbb{F}_q)$. This fact will be used later in Proposition 3.2.

The next theorem is the main result of this section.

Theorem 3.3. *Let $q = p^m$ be a prime power, $p > 5$, and let $k < (q-1)/2$ be a divisor of $q-1$. If N is the number of $\mathbb{F}_q$-rational points and d is the degree of the curve $\mathcal{C}_k$, then $\mathcal{C}_k(\mathbb{F}_q)$ is a complete (N,d)-arc if and only if k=$1, 2, 4, 6, (p^r-1)/2$ or $2(p^r-1)$, where $r|m$, $r < m$ and m/r is assumed to be even in the last case. Moreover, if $k = 3 \neq (p-1)/2$, then one can always adjoin exactly 9 points and have a complete $(q^2 - 11q + 37, q-7)$-arc.*

The proof of this theorem will be given through a sequence of several partial results. The first partial result provides a very useful way of seeing the $\mathbb{F}_q$-rational points of the curves $\mathcal{C}_k$.

Proposition 3.2. *The set of $\mathbb{F}_q$-rational points of a curve $\mathcal{C}_k$ is the complement, in $PG(2,q)$, of the union of the $3(k+1)$ lines given by the components of $xyz(x^k - y^k)(x^k - z^k)(y^k - z^k) = 0$.*

Proof. Note that we have the same set L of the $3(k+1)$ lines of Theorem 3.1 and $\#(l \cap \mathcal{C}_k(\mathbb{F}_q)) = 0$ for each line $l \in L$. Now, using (3.1) and

$$3q(k+1) - 3k - 2k^2 + \#\mathcal{C}_k(\mathbb{F}_q) = 1 + q + q^2,$$

we get the result.

□

We will stick to the notation used in Theorem 3.1 and Corollary 3.1 for the remaining of this section. The sets A, B, C, L and S will be used throughout, and the points in the sets A, B and C will be often referred to as A-points, B-points and C-points respectively. Also, for future purposes, the following remark (based on Proposition 3.2) should be kept in mind:

Remark 3.3. *For any line l of $PG(2,q)$, since $d = q-1-2k$, we have $\#(l \cap S) \geq 2k+2$. Equality holds if and only if $\#(l \cap \mathcal{C}_k(\mathbb{F}_q)) = d$.*

Now, if $N = \#\mathcal{C}_k(\mathbb{F}_q)$ and d is the degree of $\mathcal{C}_k$, the next result shows that $\mathcal{C}_k(\mathbb{F}_q)$ is indeed an (N,d)-arc. In addition, we will also see that the check for the arc property can later be restricted to the points of $A \cup B$. Recall thatt A, B and C are given in Theorem 3.1.

Proposition 3.4. *If $P \in PG(2,q)$ is a point in the complement of $\mathcal{C}_k(\mathbb{F}_q)$ such that $P \notin A \cup B$, then there exists a line l containing P such that $\#(l \cap \mathcal{C}_k(\mathbb{F}_q)) = d$.*

Proof. Since $P \notin A \cup B$ by Theorem 3.1 we can pick a line $l \notin L$ containing P and a point in C. Since $\#(l \cap C) > 0$, Corollary3.1(2) gives $\#(l \cap S) = 2k+2$. Now, Remark 3.3 completes the proof.

□

Later on, we will notice that there is a set of Fermat curves associated with each curve $\mathcal{C}_k$. It turns out that requiring our (N,d)-arcs to be complete is nearly equivalent to requiring such Fermat curves to have "many" $\mathbb{F}_q$-rational points. Considering this, we will first recall some results regarding upper bounds on the number of $\mathbb{F}_q$-rational points on Fermat curves.

The following lemma is a consequence of inequality $(4')$ and Theorem 3 of [4].

Lemma 3.5. *Let $\mathbb{F}_{p^m}$ be a finite field of characteristic $p > 5$, and $n > 2$ be a divisor of $p^m - 1$ not satisfying any of the following conditions:*

(i) $p \mid (n-1)$.

(ii) $n = 2(p^m - 1)/(p^r - 1)$ *for some divisor r of m, with $r < m$.*

(iii) $n = (p^m - 1)/2(p^r - 1)$ *for some divisor r of m, where m/r is an even number.*

If $q = p^m$ and $a, b \in \mathbb{F}_q^\star$, then the number $N_n(a, b, q)$ of $\mathbb{F}_q$-rational points of the Fermat curve $ax^n + by^n + z^n = 0$ satisfies:

$$N_n(a, b, q) \leq n^2 \lfloor \frac{2(q - 1 + 2n - \delta)}{5n} \rfloor + \delta$$

where δ is the number of such points with $xyz = 0$.

Lemma 3.6. *Let $q = p^m$ be a prime power, $p > 5$, and k a divisor of $q - 1$ such that $n = (q-1)/k$ satisfies the same hypotheses as in the previous lemma. If l is a line given by $ax + by + z = 0$ with $a, b \in \mathbb{F}_q^\star$, then the following holds*

(1) *l contains at most $\lfloor \frac{2(k + 2 - \epsilon(l))}{5} \rfloor$ A-points, where $\epsilon(l)$ is the number of B-points on l.*

(2) *for $p > 7$, if $k = 3$ and $\epsilon(l) \geq 2$ then l does not contain an A-point.*

(3) *for $k = 5$, if $\epsilon(l) \geq 2$ then l contains at most one A-point.*

Proof.

(1) This follows directly from Lemma 3.5.

Note that the last two statements do not follow from the first one. Also, $\epsilon(l) \in \{0, 1, 2, 3\}$ for every line l.

(2) Suppose we have two B-points of l given by $(0 : 1 : -b)$ and $(1 : 0 : -a)$. It follows that $-a$ and $-b$ are cubic roots of unity and therefore the line l can be given by $x + y = z$. If l contains an A-point, then the equation $x + y = 1$ has a solution for x and y in $\{1, \omega, \omega^2\}$, the cubic roots of unity. Since $1+\omega+\omega^2 = 0$, we clearly see there is no solution for $x \neq y$. On the other hand, a solution for $2x = 1$ implies $p = 7$, contradicting one hypothesis.

If the B-points are not the ones we considered, we may assume they are given by $(0 : 1 : -b)$ and $(1 : -a/b : 0)$. This implies that a and $-b$ are cubic roots of unity, and the line equation may be given by $x + z = y$. The result then follows from an equivalent argument given in the previous case.

(3) Again, suppose l contains the B-points given by $(0 : 1 : -b)$ and $(1 : 0 : -a)$. It follows that $-a$ and $-b$ are fifth roots of unity, and the equation of l can be given by $x + y = z$. If l contains two A-points, then the equation $x + y = 1$ has two solutions for x and y in $\{1, \omega_1, \cdots, \omega_4\}$, the fifth roots of unity. It is clear that we have $x \neq 1 \neq y$. If $x \neq y$ for both solutions, then we may assume the two solutions are given by $\omega_1 + \omega_2 = 1$ and $\omega_3 + \omega_4 = 1$. This implies $\omega_1 + \omega_2 + \omega_3 + \omega_4 = 2$ and then $p = 3 \leq 5$, a contradiction. If we have a solution with $x = y$, then we get $2x = 1$, which implies $p = 31$. However, the fifth roots of unity for this case are given by $\{1, 2, 4, 8, 16\}$, and there is no way we can have a second distinct solution. Similarly to the previous case, for a different choice of B-points, we get an equivalent situation, and again the result follows.

□

In the next two results, k satisfies the hypotheses of Lemma 3.6. We also recall that N and d will stand for the number of $\mathbb{F}_q$-rational points and the degree of the curve $\mathcal{C}_k$, respectively.

Lemma 3.7. *For $k > 6$, $\mathcal{C}_k(\mathbb{F}_q)$ is not a complete (N, d)-arc.*

Proof. We will argue by contradiction. Let P be an A-point and l a line containing P such that $\#(l \cap \mathcal{C}_k(\mathbb{F}_q)) = d$. If l contains m A-points and $\epsilon(l)$ B-points, then by Corollary 3.1(3) we have $\#(l \cap S) = 3k + 3 - 2m - \epsilon(l)$ points. By Remark 3.3, we have $3k+3-2m-\epsilon(l) = 2k+2$, which gives $m = (k+1-\epsilon(l))/2$. Now, from Lemma 3.6(1), we have $(k + 1 - \epsilon(l))/2 \leq 2(k + 2 - \epsilon(l))/5$ which gives $k \leq \epsilon(l) + 3 \leq 6$.

□

Lemma 3.8. *If $k = 3$ or $k = 5$, then $\mathcal{C}_k(\mathbb{F}_q)$ is not a complete (N, d)-arc. However, in the first case, we can always adjoin 9 points to $\mathcal{C}_k(\mathbb{F}_q)$ and obtain a complete $(q^2 - 11q + 37, q - 7)$-arc.*

Proof.

(i) Case $k = 3$. Note this implies $p > 7$. In fact, if $p = 7$, we have $k = (p - 1)/2$, violating our hypotheses on k. Assume the arc is complete. Let P be a B-point, and suppose l is a line through P such that $\#(l \cap \mathcal{C}_k(\mathbb{F}_q)) = d$. Since $\epsilon(l) \geq 1$, by Lemma 3.6(1), l contains at most one A-point. If the number of A-points is zero, then Corollary 3.1(3) gives $\#(l \cap S) \geq 3(k+1) - 3 = 9 > 2k+2$. If l contains one A-point, then by Lemma 3.6(2) the line contains only one B-point and then $\#(l \cap S) = 3(k+1) - 2 - 1 = 9 > 2k+2$. Both cases contradict Remark 3.3. Hence, the arc is not complete. On the other hand, one can easily check that any line $l \notin L$ connecting two A-points satisfies $\#(l \cap \mathcal{C}_k(\mathbb{F}_q)) = d$. Since by Lemma 3.6(1) such a line does not contain a B-point, we can use

Lemma 3.6(2) to include all 9 B-points into our set without having $d+1$ collinear points. That will finally give us a complete $(q^2-11q+37, q-7)$-arc.

(ii) Case $k=5$; Again we suppose the arc is complete and take a line l containing an A-point P and satisfying $\#(l \cap \mathcal{C}_k(\mathbb{F}_q)) = d$. If $\epsilon(l) \geq 2$, then by Lemma 3.6(3) l contains only one A-point, which implies $\#(l \cap S) \geq 3(k+1)-2-3 = 13 > 2k+2$. If $\epsilon(l) \leq 1$, then Lemma 3.6(1) states l contains at most two A-points, and we have $\#(l \cap S) \geq 3(k+1)-4-1 = 13 > 2k+2$. In either case, we contradict Remark 3.3. Therefore, the arc is not complete.

□

Next, we will prove that we have complete (N,d)-arcs in the remaining cases.

Lemma 3.9. *If there exists a line l in $PG(2,q)$ connecting an A-point to a B-point such that $\#(l \cap \mathcal{C}_k(\mathbb{F}_q)) = d$, then $\mathcal{C}_k(\mathbb{F}_q)$ is a complete (N,d)-arc.*

Proof. This follows directly from the fact that $H \cong (\mathbb{Z}/k\mathbb{Z})^2 \rtimes S_3$ is a subgroup of $\mathrm{Aut}(\mathcal{C}_k)$, and H acts transitively on the sets A and B.

□

Proposition 3.10. *Let $p > 5$ be a prime and m and r be positive integers such that $m > r$ and $r|m$.*

1. *If m/r is even and $k = 2(p^r-1)$, then the line $l : x+y+z = 0$ contains exactly p^r-2 A-points and three B-points defined over $\mathbb{F}_{p^m}$.*

2. *Let χ_{p^r}: $\mathbb{F}_{p^r}^{\times} \longrightarrow \{\pm 1\}$ be the quadratic character, and consider the line $l : x + \chi_{p^r}(-1)y = z$. For $k = (p^r-1)/2$, the line l contains exactly $(p^r-5)/4$ A-points and three B-points if $\chi_{p^r}(-1) = 1$, and l contains exactly $(p^r-3)/4$ A-points and two B-points if $\chi_{p^r}(-1) = -1$. Such points are also defined over $\mathbb{F}_{p^m}$.*

Proof. The statements follow directly from the computation of the number of $\mathbb{F}_{p^m}$-rational points on the curves $ax^{e/2} + by^{e/2} + z^{e/2} = 0$ (with $a^2, b^2 \in \mathbb{F}_{p^r}$) and $ax^{2e} + by^{2e} + z^{2e} = 0$ (with $a, b \in \mathbb{F}_{p^r}$), where $e = (p^m - 1)/(p^r - 1)$. For such computation, see Examples (vii) and (viii) of [4]. □

The proof of Theorem 3.3 is completed by the following lemma.

Lemma 3.11. *If $k = 1, 2, 4, 6, (p^r - 1)/2$ or $2(p^r - 1)$, then $\mathcal{C}_k(\mathbb{F}_q)$ are complete (N,d)-arcs. In particular, using the two last values of k and $q = p^m$, we prove the existence in $PG(2, q)$ of a complete*

$$(\frac{2q^2 - (3p^r + 1)q + p^{2r} + p^r}{2}, q - p^r)\text{-arc, where } r \mid m \text{ and } r < m, \tag{3.2}$$

and a complete

$$(q^2+(4-6p^r)q+8p^{2r}-10p^r+3, q-4p^r+3)\text{-arc, where } r \mid m \text{ and } \frac{m}{r} \text{ is even.} \tag{3.3}$$

Proof. For each given k, it suffices to find a line l fulfilling the conditions of Lemma 3.9.

- Case $k = 2(p^r - 1)$: We consider the line $l : x + y + z = 0$. By Proposition 3.10, l contains $p^r - 2$ A-points and $\epsilon(l) = 3$. Thus, using Corollary 3.1(3), one can check that $\#(l \cap S) = 2k + 2$. Therefore, by Remark 3.3, we have $\#(l \cap \mathcal{C}_k(\mathbb{F}_q)) = d$, and Lemma 3.9 completes the proof.

- Case $k = (p^r - 1)/2$: We take the line $l : x + \chi_{p^r}(-1)y = z$ from Proposition 3.10, and similar to the previous case, one can check that $\#(l \cap \mathcal{C}_k(\mathbb{F}_q)) = d$ and the result follows.

- Case $k = 6$: Let $\{\pm 1, \pm\omega, \pm\omega^2\}$ be the set of the sixth roots of unity. It is clear that the line $l : \omega x + \omega^2 y + z = 0$ contains the A-points $P = (1 : 1 : 1)$, $Q = (\omega : \omega^2 : 1)$ and the B-points $(-\omega : 1 : 0), (-\omega^2 : 0 : 1), (0 : -\omega : 1)$. The usual check shows that $\#(l \cap S) = 14 = 2k + 2$, and the result follows again. The cases $k = 1, 2$ and 4 can be handled in a similar (or even simpler) way.

□

3.2 Arcs of parameters $((q^2+4q-5)/4, (q-1)/2)$ and $((q^2+4q+7)/4, (q+3)/2)$ in $PG(2,q)$.

In the previous section, we considered the (N, d)-arcs in $PG(2, q)$ given by the complement of the union of the $3(k + 1)$ lines in L. Now, we will be interested in the case where such a complement is empty, i.e., the set S is the whole $PG(2, q)$. By Corollary 3.1(1), this happens if and only if $k = q - 1$ or $k = (q - 1)/2$. We will consider the case where $k = (q - 1)/2$ and use the sets A, B and C to construct complete (N, d)-arcs. The same can be done in the case $k = q - 1$, but we will get either the trivial complete $(1 + q + q^2, q + 1)$-arc or the complete $((q-1)^2, q-1)$-arc arising from the curve $x^{q-1} + y^{q-1} = 2z^{q-1}$, which was already considered in [**?**].

Theorem 3.4. *Let $q > 11$ be an odd prime power. If Γ is the curve given by $(x^k + y^k - 2z^k)(x^k + z^k - 2y^k)(y^k + z^k - 2x^k) = 0$ where $k = (q - 1)/2$, then $\Gamma(\mathbb{F}_q)$ is a complete $((q^2 + 4q - 5)/4, (q - 1)/2)$-arc.*

Proof. Let $\mathcal{F}$ be the curve given by $x^k + y^k - 2z^k = 0$. It is easy to check that $\mathcal{F}(\mathbb{F}_q) = A \cup \{(\xi_i : 1 : 0) : \xi_i^k = -1\}$, where A is given as in Theorem 3.1. Therefore, by symmetry, we have $\#\Gamma(\mathbb{F}_q) = k^2 + 3k = (q^2 + 4q - 5)/4$. It is clear that we have k collinear points in $\Gamma(\mathbb{F}_q)$, and we now suppose the existence of a line incident with

$k+1$ points of this set. Note that $\Gamma(\mathbb{F}_q)\backslash A$ is a subset of the lines given by the components of $xyz = 0$. So, any line containing $k+1$ points of $\Gamma(\mathbb{F}_q)$ would take at most three points from this subset and at least $k-2$ points from A. Suppose $l : ax + by + cz = 0$ is such a line. If $abc = 0$, then it is easy to check that l is a line in L intersecting $\Gamma(\mathbb{F}_q)$ in exactly k points. Therefore, we may assume l is given by $ax + by + z = 0$, and $ab \neq 0$. On the other hand, such a condition implies that each A-point in l gives rise to four affine points on the conic $ax^2 + by^2 + z^2 = 0$. This fact yields $4(k-2) \leq q+1$ and thus $q \leq 11$, a contradiction. Therefore $\Gamma(\mathbb{F}_q)$ is a $((q^2+4q-5)/4, (q-1)/2)$-arc. The arc property follows from the fact that $PG(2,q)$ is covered by the $3(k+1)$ lines of L and that $\Gamma(\mathbb{F}_q)$ has k points on each one of those lines.

□

With a similar reasoning using the sets A, B and C, the next result presents another complete (N,d)-arc. However, unlike Theorem 3.4, the underlying set is not apparently given by the $\mathbb{F}_q$-rational points of a curve.

Theorem 3.5. *Let q be an odd prime power and $k = (q-1)/2$. If $W = \{(x_0 : x_1 : x_2) \in PG(2,q) \mid x_i^k \in \{0,1\}\}$, then W is a complete $((q^2+4q+7)/4, (q+3)/2)$-arc.*

Proof. It is clear that $W = A \cup B \cup C$ and $\#W = k^2 + 3k + 3 = (q^2+4q+7)/4$. Note that each of the $3(k+1)$ lines of L is incident with $k+2 = (q+3)/2$ points of W. Suppose we have $(q+3)/2 + 1 = k+3$ points in W incident with a line $l : ax + by + cz = 0$, $l \notin L$. Observe that $B \cup C$ is a subset of the union of lines given by $xyz = 0$ and A is a subset of the $\mathbb{F}_q$-rational points of $x^k + y^k - 2z^k = 0$. Therefore, l must be incident with three points in $B \cup C$ and k points in A. Now, from an argument similar to the one used in the proof of the previous theorem, we conclude $4k \leq q+1$ and thus $q \leq 3$. On the other hand, one can easily check that such a line does not exist for $q = 3$. Therefore, W is an $((q^2+4q+7)/4, (q+3)/2)$-arc. Completeness also follows similarly to Theorem 3.4.

□

3.3 An $\mathbb{F}_{q^2}$-maximal curve

Recall from Theorem 1.2 that for any divisor d of $q+1$ the curve $x^d + y^d + z^d = 0$ is $\mathbb{F}_{q^2}$-maximal. Given that such curves are somewhat large as (N, d)-arcs, it is natural to ask about their arc property. Among these curves, we consider a special one given by

$$x^{(q+1)/2} + y^{(q+1)/2} + z^{(q+1)/2} = 0, \tag{3.4}$$

which was previously mentioned in chapter 1.
In this section, after investigating the intersection of the Hermitian curve with certain conics, we prove the following :

Theorem 3.6. *Let q be an odd prime power. If Γ is the curve given by $x^{(q+1)/2} + y^{(q+1)/2} + z^{(q+1)/2} = 0$, then $\Gamma(\mathbb{F}_{q^2})$ is a complete $((q^3+3q+4)/4, (q+1)/2)$-arc.*

Theorem 3.7. *If $q > 3$ is an odd prime power, and $\mathcal{H} : x^{q+1}+y^{q+1}+z^{q+1} = 0$ is the Hermitian curve, then there exists a conic $\mathcal{C}$, defined over $\mathbb{F}_{q^2}$, such that $\mathcal{H}(\mathbb{F}_{q^2}) \cap \mathcal{C}(\mathbb{F}_{q^2}) = \emptyset$. Moreover, $\mathcal{H}(\mathbb{F}_{q^2}) \cup \mathcal{C}(\mathbb{F}_{q^2})$ gives rise to a complete $(q^3+q^2+2, q+3)$-arc in $PG(2, q^2)$.*

We proceed by presenting a list of preliminary results that will lead to the proof of both theorems. The following notation will be carried out for the rest of this chapter.

For $i = 1, 2$, we set $N_i := \{\xi \in \mathbb{F}_{q^2} : \xi^{(q+1)/2} = (-1)^i\}$, and the quadratic character $\chi_{q^i} : \mathbb{F}_{q^i}^{\times} \mapsto \{\pm 1\}$. Note that $N = \{\xi \in \mathbb{F}_{q^2} : \xi^{q+1} = 1\} = N_1 \cup N_2$ and $N_2 = \{\xi^2 : \xi \in N\}$.

Lemma 3.12. *If $\chi_{q^2}(r) = -1$, then $\{(r-\xi)^{q+1} : \xi \in N_1\} = \{(r-\xi)^{q+1} : \xi \in N_2\}$.*

Proof. For $\xi \in N_1$, the condition $\chi_{q^2}(r) = -1$ implies $\dfrac{1}{\xi r^{q-1}} \in N_2$. Now we have $(r-\xi)^{q+1} = (r-\xi)^{q(q+1)} = (r^q - \dfrac{1}{\xi})^{q+1} = (r^{q-1}(r - \dfrac{1}{\xi r^{q-1}}))^{q+1} = (r - \dfrac{1}{\xi r^{q-1}})^{q+1}$, from which we conclude that the two sets are the same. □

The following remark will be a useful tool in the proofs of the next results.

Remark 3.13. *If* $N = \{\xi \in \mathbb{F}_{q^2} : \xi^{q+1} = 1\}$ *and* $\epsilon \in \mathbb{F}_{q^2}$ *is such that* $\epsilon^{q-1} = -1$, *then* $N = \{\dfrac{t+\epsilon}{t-\epsilon} : t \in \mathbb{F}_q \cup \{\infty\}\}$.

Proof. First we identify N with the $\mathbb{F}_q$-rational points of the conic $x^2 + \epsilon^{q+1}y^2 = z^2$. More precisely, if $(x_0 : y_0 : 1)$ is such a point, then we have $\xi = x_0 + \epsilon y_0 \in N$. Now, if we consider the parametrization $t \mapsto (x_t, y_t) = (\dfrac{t^2+\epsilon^2}{t^2-\epsilon^2}, \dfrac{2t}{t^2-\epsilon^2})$ of the affine conic, we can endow the elements of N with such a parametrization and write $\xi_t = x_t + \epsilon y_t = \dfrac{t+\epsilon}{t-\epsilon}$.

□

Proposition 3.14. *For every* $r \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$, *there exists* $\xi \in N$ *such that* $\chi_q(1 - (r - \xi)^{q+1}) = 1$.

Proof. We need to find $\xi \in N$ such that $\chi_q(r^q\xi + r\xi^{-1} - r^{q+1}) = 1$. By Remark 3.13, it suffices to find $t \in \mathbb{F}_q$ such that

$$\chi_q(\frac{t+\epsilon}{t-\epsilon}r^q + \frac{t-\epsilon}{t+\epsilon}r - r^{q+1})$$

$$= \chi_q(\frac{(r^q + r - r^{q+1})t^2 + 2\epsilon(r^q - r)t + \epsilon^2(r^q + r + r^{q+1})}{t^2 - \epsilon^2})$$

$$= \chi_q((t^2-\epsilon^2)((r^q + r - r^{q+1})t^2 + 2\epsilon(r^q - r)t + \epsilon^2(r^q + r + r^{q+1}))) = 1.$$

Now, it is just a matter of finding a lower bound on the number of $\mathbb{F}_q$-solutions for

$u^2 = f(t)$, where

$$f(t) = (t^2 - \epsilon^2)((r^q + r - r^{q+1})t^2 + 2\epsilon(r^q - r)t + \epsilon^2(r^q + r + r^{q+1})) \in \mathbb{F}_q[t] \quad (3.5)$$

Note that since $r^q - r \neq 0$, the above equation is not of the form $u^2 = \mu g(t)^2$, where $\chi_q(\mu) = -1$. Therefore, if q is not too small, we can find a solution we need. In fact, if $f(t)$ has repeated roots, we can replace the above equation by a conic's equation. If the roots are all distinct, we will have an elliptic curve, and using the Hasse-Weil bound ($\mid N - (q+1) \mid \leq 2q^{1/2}$), we find $q > 9$ provides a solution we need. Finally, a quick computer check reveals that such fact also holds true for $q \leq 9$. □

Corollary 3.15. *If $\chi_{q^2}(r) = -1$ and $s \in N_1$, then there exist b and c in $\mathbb{F}^\star_{q^2}$ satisfying the following:*

1. $r - b^2 s = c$.
2. $b^{q+1} = 1$.
3. $\chi_q(1 - c^{q+1}) = 1$.

Proof. Since we have $\chi_{q^2}(r/s) = -1$, by Proposition 3.14, there exists $\xi' \in N$ such that $\chi_q(1 - (r/s - \xi')^{q+1}) = 1$. On the other hand, because of Lemma 3.12, we may assume $\xi' \in N_2$, which implies $\xi' = \xi^2$ for some $\xi \in N$. Therefore, we have $\chi_q(1-(r/s-\xi^2)^{q+1}) = \chi_q(1-(r-\xi^2 s)^{q+1}) = 1$. Now, taking $b = \xi$ and $c = r - \xi^2 s$, we get the result .

□

PROOF OF THEOREM 3.6.

Let $P = (x_0 : y_0 : z_0) \in PG(2, q^2)$ be a point in the complement of Γ. If one of its coordinates is zero, for instance $z_0 = 0$, then we take the line $z = 0$ which

clearly intersects $\Gamma(\mathbb{F}_{q^2})$ in $d = (q+1)/2$ distinct points. Suppose the point is given by $P = (x_0 : y_0 : 1)$ with $x_0 y_0 \neq 0$, and consider the following possibilities:

- $\chi_{q^2}(x_0) = 1$ or $\chi_{q^2}(y_0) = 1$.

  Without loss of generality, we assume $\chi_{q^2}(y_0) = 1$, and since $y_0^{(q+1)/2} \in \mathbb{F}_q$, the line $y = y_0 z$ intersects Γ in d distinct points, unless $y_0^{(q+1)/2} = -1$. On the other hand, if we also have $\chi_{q^2}(x_0) = 1$, then this problem can be fixed by taking either the line $x = x_0 z$ or $x = \dfrac{x_0}{y_0} y$. Thus, we only need to consider the case $y_0^{(q+1)/2} = \chi_{q^2}(x_0) = -1$.

- $\chi_{q^2}(x_0) = \chi_{q^2}(y_0) = -1$.

  Since $P = (x_0 : y_0 : 1) = (1 : \frac{y_0}{x_0} : \frac{1}{x_0})$, using the symmetry of the curve, one can see that we fall on the previous case.

Based on this, we may assume that $P = (r : s : 1)$ with r, s satisfying $\chi_{q^2}(r) = s^{(q+1)/2} = -1$.

We take the values b and c provided by Corollary 3.15, and consider the line l containing P and given by $x - b^2 y = cz$. In order to prove that l is incident with $(q+1)/2$ distinct points of $\Gamma(\mathbb{F}_{q^2})$, it suffices to prove that the conic $\mathcal{C} : x^2 - b^2 y^2 = cz^2$ intersects the Hermitian curve $\mathcal{H} : x^{q+1} + y^{q+1} + z^{q+1} = 0$ in $2(q+1)$ distinct points $P = (x : y : 1) \in PG(2, q^2)$. One can check that $(t : u) \mapsto (bct^2 + bu^2 : ct^2 - u^2 : 2btu)$ parametrizes $\mathcal{C}$, and that the intersection restricted to the affine points of both curves yields:

$$b^{q+1}(ct^2 + 1)^{q+1} + (ct^2 - 1)^{q+1} + 4b^{q+1}t^{q+1} = 0$$

Since $b^{q+1} = 1$, we have

$$c^{q+1}t^{2(q+1)} + 2t^{q+1} + 1 = 0. \tag{3.6}$$

For $\Delta = 4(1 - c^{q+1})$, Corollary 3.15(3) gives us $\chi_q(\Delta) = 1$, which implies that (3.6) has $2(q+1)$ distinct nonzero roots in $\mathbb{F}_{q^2}$. Since this gives $2(q+1)$ affine points of $(\mathcal{H} \cap C)(\mathbb{F}_{q^2})$, the result follows.

□

In the previous computation, we noted a way to find conics not intersecting the Hermitian curve in $PG(2, q^2)$. Also, it is well-known that the intersection of these curves with lines in $PG(2, q^2)$ can be easily characterized. These two facts will be the tools to prove Theorem 3.7.

PROOF OF THEOREM 3.7.

Since $q > 3$, we can find $c \in \mathbb{F}_{q^2}^{\star}$ such that $\chi_q(1 - c^{2(q+1)}) = -1$, and we claim the conic $\mathcal{C} : x^2 - y^2 = (cz)^2$ does not intersect the Hermitian curve $\mathcal{H} : x^{q+1} + y^{q+1} + z^{q+1} = 0$ in $PG(2, q^2)$. In fact, considering the same parametrization used in the proof of Theorem 3.6, one can check that we end up with the following:

$$c^{2(q+1)}t^{2(q+1)} + 2t^{q+1} + 1 = 0. \tag{3.7}$$

For $\Delta = 4(1-c^{2(q+1)})$, we have $\chi_q(\Delta) = -1$, which implies $\mathcal{C}$ intersects $\mathcal{H}$ in $2(q+1)$ points defined over a non-trivial extension of $\mathbb{F}_{q^2}$. Now, Bezout's theorem implies our claim.

For the arc property, we consider a point $P \in PG(2, q^2)$ in the complement of the two curves. Among the $q^2 + 1$ lines incident with P, we know that there are $q + 1$ lines tangent to $\mathcal{H}$, and each of the remaining $q^2 - q$ lines intersects the

Hermitian curve in $q+1$ distinct points (see Theorem 1.3). On the other hand, we also know that there are at most $(q^2+3)/2$ lines through P which are not secant to $\mathcal{C}$. Therefore, if we have $q^2-q>(q^2+3)/2$, which means $q>3$, then the (N,d)-arc is complete.

□

3.4 A Fermat Curve

Here, we obtain a small complete (N,d)-arc in $PG(2,q^2)$ given by the $\mathbb{F}_{q^2}$-rational points of the Fermat curve $\mathcal{C}: x^{q-1}+y^{q-1}+z^{q-1}=0$. In [14], Moisio presented an explicit formula for the number of $\mathbb{F}_{q^2}$-rational points of a certain family of Fermat curves. It turns out that $\mathcal{C}$ lies in this family. However, to make our future discussion clearer, the computation of $\mathcal{F}(\mathbb{F}_{q^2})$ is also presented here.

Theorem 3.8. *Let $q\equiv 2 \mod 3$ be a power of a prime $p>2$. If $\mathcal{C}$ is the Fermat curve $x^{q-1}+y^{q-1}+z^{q-1}=0$, then $\#\mathcal{C}(\mathbb{F}_{q^2})=2q^2-q-1$.*

Proof. It is clear that $\mathcal{C}$ has $3(q-1)$ points in $PG(2,q^2)$ with $xyz=0$. To count the points with non-zero coordinates, it suffices to count the number of solutions of $x+y+1=0$ for x and y in $\mathcal{N}=\{\xi\in\mathbb{F}_{q^2}:\xi^{q+1}=1\}$.

Recall from Remark 3.13 that if we fix $\epsilon\in\mathbb{F}_{q^2}$, such that $\epsilon^{q-1}=-1$, then we have $\mathcal{N}=\{\frac{t+\epsilon}{t-\epsilon}: t\in\mathbb{F}_q\cup\{\infty\}\}$. Since $p\neq 3$, the pairs $(u,v)\in\mathcal{N}\times\mathcal{N}$ with $u+v+1=0$ correspond to the pairs $(t_1,t_2)\in\mathbb{F}_q\times\mathbb{F}_q$ with

$$\frac{t_1+\epsilon}{t_1-\epsilon}+\frac{t_2+\epsilon}{t_2-\epsilon}+1=0$$

and thus

$$3t_1t_2-\epsilon(t_1+t_2)-\epsilon^2=0. \tag{3.8}$$

Since $\epsilon\notin\mathbb{F}_q$, (3.8) gives $t_1=-t_2$ and $\epsilon^2=-3t_1^2$. Note that $\epsilon^2=-3t_1^2$

is consistent only if -3 is a non-square in $\mathbb{F}_q$, which turns out to be equivalent to $3 \mid (q+1)$. From $t_1 = -t_2$ we have $1 + u + u^2 = 0$, i.e. u is a primitive cubic root of unity. Therefore, (u, u^{-1}) and (u^{-1}, u) are the only solutions of $x + y + 1 = 0$ for x and y in $\mathcal{N}$ (such characterization will be important in the proof of Theorem 3.9).

Clearly, each solution above gives rise to $(q-1)^2$ points in $\mathcal{C}(\mathbb{F}_{q^2})$ with non-zero coordinates. Hence, we have $\#\mathcal{C}(\mathbb{F}_{q^2}) = 2(q-1)^2 + 3(q-1) = 2q^2 - q - 1$.

□

Theorem 3.9. *Let q be an odd prime power such that $3 \mid (q+1)$. If $\mathcal{C}$ is the Fermat curve $x^{q-1} + y^{q-1} + z^{q-1} = 0$, then $\#\mathcal{C}(\mathbb{F}_{q^2})$ is a complete $(2q^2 - q - 1, q - 1)$-arc.*

Proof. Let $P = (x_0 : y_0 : z_0) \in \mathrm{PG}(2, q^2)$ be a point in the complement of $\mathcal{C}$. If one of the coordinates of P is zero, say $z_0 = 0$, then the line $z = 0$ obviously contains P and intersects $\mathcal{C}$ in $q - 1$ distinct points of $\mathrm{PG}(2, q^2)$. Therefore, we can assume $P = (r : s : 1)$ with $rs \neq 0$; The following claim excludes several more possibilities for $P = (r : s : 1)$.

Claim I. Let μ be a fixed element of $\mathbb{F}_{q^2}$ satisfying $\mu^{2(q-1)} + \mu^{q-1} + 1 = 0$. If $r, s \in \mathbb{F}_{q^2}^\star$ such that $\{\mu r/s, \mu^2/s, \mu/r\} \cap \mathbb{F}_q \neq \emptyset$, then there exists a line l incident with $P = (r : s : 1)$ with $\#(l \cap \mathcal{C}(\mathbb{F}_{q^2})) = q - 1$.

Proof. Suppose we have $\mu r/s = \alpha \in \mathbb{F}_q$ and consider the line $l : x = (r/s)y$. Clearly $P \in l$, and since $1 + \mu^{q-1} + \mu^{2(q-1)} = 0$, the polynomial $((\alpha/\mu)y)^{q-1} + y^{q-1} + 1$ has $q - 1$ distinct roots in $\mathbb{F}_{q^2}$ which implies $\#(l \cap \mathcal{C}(\mathbb{F}_{q^2})) = q - 1$. The other two cases can be handled in an identical way if we consider the lines $y = sz$ and $x = rz$ respectively. □

From now on, we will use the same fixed μ defined in Claim I and assume $r, s \in \mathbb{F}_{q^2}^\star$ do not satisfy the hypotheses of that claim. To deal with the remaining cases, we will prove the existence of $\lambda \in \mathbb{F}_{q^2}$ such that the polynomial $f(x) = x^{q-1} + (\lambda(x -$

$r) + s)^{q-1} + 1$ has $q-1$ distinct zeros in $\mathbb{F}_{q^2}$. Suppose $f(x)$ has a zero $x_0 \in \mathbb{F}_{q^2}$ corresponding to an $\mathbb{F}_{q^2}$-rational point of $\mathcal{C}$ with nonzero coordinates. Based on such points of $\mathcal{C}$ (characterized in Theorem 3.8), we can find x_1 and y_1 in $\mathbb{F}_{q^2}^\star$ such that one of the following holds:

1. $x_0 = \mu x_1^{q+1}$ and $\lambda(x_0 - r) + s = \mu^2 y_1^{q+1}$, and thus $\lambda(\mu x_1^{q+1} - r) + s = \mu^2 y_1^{q+1}$.
2. $x_0 = \mu^2 x_1^{q+1}$ and $\lambda(x_0 - r) + s = \mu y_1^{q+1}$, and thus $\lambda(\mu^2 x_1^{q+1} - r) + s = \mu y_1^{q+1}$.

Note that in each case, such a zero of $f(x)$ gives rise to $(q+1)^2$ $\mathbb{F}_{q^2}$-rational solutions (with nonzero coordinates) of the equations given by

$$\lambda\mu X^{q+1} - \mu^2 Y^{q+1} + s - \lambda r = 0 \tag{3.9}$$

and

$$\lambda\mu^2 X^{q+1} - \mu Y^{q+1} + s - \lambda r = 0 \tag{3.10}$$

respectively. Conversely, we can also see that such $(q+1)^2$ solutions for (3.9) or (3.10) give rise to a unique zero of $f(x)$.

Now, the idea is to find $\lambda \in \mathbb{F}_{q^2}$ such that either (3.9) or (3.10) has the maximum possible number of $\mathbb{F}_{q^2}$-solutions. This will be achieved if the coefficients of either equation can be replaced by elements of $\mathbb{F}_q^\times$.

Claim II. There exist m, n in $\mathbb{F}_q^\times$ such that $s - \mu r m = \mu^2 n$.

Proof. Since $s, \mu r, \mu^2 \in \mathbb{F}_{q^2}^\star$, we can certainly find $\alpha_1, \alpha_2, \alpha_3$ in $\mathbb{F}_q$, not all zero, such that

$$\alpha_1 s + \alpha_2 \mu r + \alpha_3 \mu^2 = 0$$

On the other hand, it is easy to check that if $\alpha_i = 0$ for some $i \in \{1, 2, 3\}$, then r, s will satisfy the hypotheses of Claim I, violating our assumption. Finally, defining

$m = -\alpha_2/\alpha_1$ and $n = -\alpha_3/\alpha_1$ completes the proof. □

Using the previous claim, we take $\lambda = \mu m$, and after some scaling (if necessary), (3.9) and (3.10) can be replaced by

$$X^{q+1} + Y^{q+1} + 1 = 0 \tag{3.11}$$

and

$$\mu X^{q+1} + \mu^2 Y^{q+1} + 1 = 0 \tag{3.12}$$

Lastly, counting the number of $\mathbb{F}_{q^2}$-solutions with non-zero coordinates of the above equations, one can check that the $(q-2)(q+1)^2$ solutions of (3.11) together with the $(q+1)^2$ solutions of (3.12) provide $(q-2)+1 = q-1$ distinct roots for $f(x)$. Hence, we have a complete $(2q^2 - q - 1, q-1)$-arc.

□

3.5 The Parameters

Here, we present a table summarizing our (N, d)-arcs and briefly compare some of our parameters with others previously obtained. We also provide an upper bound on the distance of the corresponding codes to the Griesmer bound.

It can be easily checked that an (N, d)-arc in $PG(2, q)$, with $N > (d-2)q + d$, is equivalent to a code meeting the Griesmer bound. Table 1 of [1] lists many of the known families of such (N, d)-arcs, and, more recently, Ball and Montanucci (see [2]) presented new $[N, 3, N-d]$-codes over $\mathbb{F}_q$, with $d = q-3$ and $d = q-4$, meeting

the Griesmer bound. Despite the given examples, constructing codes meeting the Griesmer bound is a difficult problem. Actually, obtaining (N, d)-arcs with N/q large, say $N/q > d-2$, is not easy in general. As mentioned in Section 5 of [1], the best that can be done in general is to take (a) for $d < q/2$ the union of $\lfloor d/2 \rfloor$ conics, which gives $N/q > d/2$, and (b) for $d > q/2$ large the complement of the union of $2(q-d)+1$ lines of a dual $(2(q-d)+1, 2)$-arc, which gives $N/q > q-2d+(2d^2-d)/q$.

After comparing parameters, we see the (N, d)-arcs obtained from our work here are smaller than the ones from Table 1 of [1], and in general larger than the ones obtained from the above procedures. For instance, each (N, d)-arc derived from Theorem 3.3 satistifies $N/q > d - \alpha$ for some constant $\alpha \geq 2$. To give a better idea of the general scenario, we present a table that displays the parameters of the (N, d)-arcs constructed in the previous sections. The last column shows an upper bound for the difference of N and the Griesmer bound $G = \sum_{i=0}^{2} \lceil \frac{N-d}{q^i} \rceil$ of the corresponding $[N, 3, N-d]$-code.

	d	$q = p^m$ odd	N	$N - G \leq$
1	$q-3$	$p > 5$	$q^2 - 5q + 6$	1
2	$q-5$	$p > 5$	$q^2 - 8q + 15$	2
3	$q-7$	$3 \mid (q-1)$ and $p > 5$	$q^2 - 11q + 37$	3
4	$q-9$	$4 \mid (q-1)$ and $p > 5$	$q^2 - 14q + 45$	4
5	$q-13$	$6 \mid (q-1)$ and $p > 7$	$q^2 - 20q + 91$	6
6	$q-p^h$	$h \mid m$ and $p > 5$	$\frac{2q^2-(3p^h+1)q+p^{2h}+p^h}{2}$	$\frac{p^r-1}{2}$
7	$q-4p^h+3$	m/h is even and $p > 5$	$q^2+(4-6p^h)q+8p^{2h}-10p^h+3$	$2(p^h-1)$
8	$\sqrt{q}+3$	$q > 9$ square	$q\sqrt{q}+q+2$	1
9	$(q-1)/2$	$q > 11$	$(q^2+4q-5)/4$	$\lceil (q-11)/4 \rceil$
10	$(q+3)/2$	q	$(q^2+4q+7)/4$	$\lceil (q-3)/4 \rceil$
11	$(\sqrt{q}+1)/2$	q square	$(q\sqrt{q}+3\sqrt{q}+4)/4$	$\lceil (\sqrt{q}-5)/4 \rceil$
12	$\sqrt{q}-1$	q square and $3 \mid (\sqrt{q}+1)$	$2q-\sqrt{q}-1$	$\sqrt{q}-4$

Table 3.1: Complete (N, d)-arcs

Note that for $d = (q-1)/2$ the (N, d)-arc from procedure (a) above and the one from row 9 in Table 1 give similar values for N. On the other hand, after a careful analysis of the configuration of our points (Theorem 3.4), we see that such a set can never be given by a union of conics. This leads us to suspect that the (N, d)-arcs will not be the same in general.

It is also worth noting that, in contrast with the other cases in Table 1, row 12 presents a very small (N, d)-arc. We have $N/q < 2$, and as far as we know, there is no construction of arcs with similar parameters.

Table 1 above also shows that, in general, the codes corresponding to our (N, d)-arcs will not meet the Griesmer bound. However, in many cases, they are just a constant away from this bound. It can be checked that, with the exception of rows 6 and 7, the numbers on the last column are the actual value of $N - G$ if q is sufficiently large.

For another comparison, we point out that Ball and Montanucci (see [2]) also presented a (non-explicit) construction of (N, d)-arcs where, under certain conditions, the corresponding codes are one away from the Griesmer bound. It can be checked that the (N, d)-arcs from rows 1 and 8 in Table 1 are not particular cases of this construction. In the case of row 1, we have a smaller value for N. In the case of row 8, our (N, d)-arc does not have the parameters satisfying the required conditions of their construction.

We have noticed that, out of the explicit constructions of (N', d')-arcs in $PG(2, q)$ where the parameter d' matches with our d, our N has a different value and, in some cases, it is slightly smaller. This means we indeed have new parameters. Of course, we are not including the cases where q is too small.

We end this section by presenting three particular cases where some of our (N, d)-arcs ($d \geq 4$) have the corresponding codes meeting the Griesmer bound. The notation $[N, d]_q$ will stand for an (N, d)-arc in $PG(2, q)$. Such arcs are: $[20, 4]_7$,

$[63, 6]_{13}$ and $[32, 4]_{13}$, and they are obtained from rows $1, 3$ and 4 respectively. We have not seen such (N, d)-arcs listed in the most recently updated tables.

Bibliography

[1] S. Ball and J. W. P. Hirschfeld, *Bounds on (n, r)-arcs and their application to linear codes*, Finite Fields Appl. **11** (2005), no. 3, 326–336.

[2] Simeon Ball and Elisa Montanucci, *Affine blocking sets, three-dimensional codes and the Griesmer bound*, Discrete Math. **307** (2007), no. 13, 1600–1608.

[3] A. Cossidente, J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *On plane maximal curves*, Compositio Math. **121** (2000), no. 2, 163–181.

[4] A. Garcia and J. F. Voloch, *Fermat curves over finite fields*, J. Number Theory **30** (1988), no. 3, 345–356.

[5] Arnaldo García, *The curves $y^n = f(x)$ over finite fields*, Arch. Math. (Basel) **54** (1990), no. 1, 36–44.

[6] Arnaldo Garcia, Henning Stichtenoth, and Chao-Ping Xing, *On subfields of the Hermitian function field*, Compositio Math. **120** (2000), no. 2, 137–170.

[7] Massimo Giulietti, Fernanda Pambianco, Fernando Torres, and Emanuela Ughi, *On complete arcs arising from plane curves*, Des. Codes Cryptogr. **25** (2002), no. 3, 237–246.

[8] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[9] H. Hasse, *Zur theorie der abstrakten elliptischen funktionenkörper*, J. Reine Angew. Math. **175** (1936), 69–88 and 193–208.

[10] Abramo Hefez and José Felipe Voloch, *Frobenius nonclassical curves*, Arch. Math. (Basel) **54** (1990), no. 3, 263–273.

[11] J. W. P. Hirschfeld, *Projective geometries over finite fields*, second ed., Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1998.

[12] J. W. P. Hirschfeld and G. Korchmáros, *On the number of solutions of an equation over a finite field*, Bull. London Math. Soc. **33** (2001), no. 1, 16–24.

[13] Gilles Lachaud, *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C. R. Acad. Sci. Paris Sér. I Math. **305** (1987), no. 16, 729–732.

[14] Marko Moisio, *On the number of rational points on some families of Fermat curves over finite fields*, Finite Fields Appl. **13** (2007), no. 3, 546–562.

[15] Rita Pardini, *Some remarks on plane curves over fields of finite characteristic*, Compositio Math. **60** (1986), no. 1, 3–17.

[16] F. Rodríguez Villegas, J. F. Voloch, and D. Zagier, *Constructions of plane curves with many points*, Acta Arith. **99** (2001), no. 1, 85–96.

[17] Hans-Georg Rück and Henning Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. **457** (1994), 185–188.

[18] Karl-Otto Stöhr and José Felipe Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) **52** (1986), no. 1, 1–19.

[19] Jaap Top, *Curves of genus 3 over small finite fields*, Indag. Math. (N.S.) **14** (2003), no. 2, 275–283.

[20] Gerard van der Geer and Marcel van der Vlugt, *Tables of curves with many points*, Math. Comp. **69** (2000), no. 230, 797–810.

[21] J. H. van Lint, *Introduction to coding theory*, third ed., Graduate Texts in Mathematics, vol. 86, Springer-Verlag, Berlin, 1999.

[22] José Felipe Voloch, *A note on* (k, n)*-arcs*, Discrete Math. **294** (2005), no. 1-2, 223–224.

[23] André Weil, *Variétés abéliennes et courbes algébriques*, Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946), Hermann & Cie., Paris, 1948.

Vita

Herivelto Martins Borges Filho was born in Fortaleza, Brazil on the 26th of October 1974, son of Neila Pontes Borges and Herivelto Martins Borges. He received the Licenciatura degree in Mathematics from the Universidade of São Paulo in 2000. In 2003 he received the Master of Science degree in Mathematics from the Universidade of São Paulo, advised by Prof. Orlando Stanley. In 2004 he was accepted by the Department of Mathematics of the University of Texas at Austin to start on the Ph.D. program, advised by Prof. José Felipe Voloch.

Permanent Address: 3561 Lake Austin Blvd Ap. A
Austin, Texas 78703

This dissertation was typeset with LaTeX 2_ε[1] by the author.

[1] LaTeX 2_ε is an extension of LaTeX. LaTeX is a collection of macros for TeX. TeX is a trademark of the American Mathematical Society. The macros used in formatting this dissertation were written by Dinesh Das, Department of Computer Sciences, The University of Texas at Austin, and extended by Bert Kay, James A. Bednar, and Ayman El-Khashab.