Compositio Mathematica **128:** 95–113, 2001.

Embedding of a Maximal Curve in a Hermitian Variety

GÁBOR KORCHMÁROS[1] and FERNANDO TORRES[2]
[1] *Dipartimento di Matematica, Universitá della Basilicata, via N. Sauro 85, 85100 Potenza, Italy. e-mail: korchmaros@unibas.it*
[2] *IMECC-UNICAMP, Cx. P. 6065, Campinas-13083-970-SP, Brazil. e-mail: ftorres@ime.unicamp.br*

(Received: 7 March 2000)

Abstract. Let $\mathcal{X}$ be a projective, geometrically irreducible, non-singular, algebraic curve defined over a finite field $\mathbf{F}_{q^2}$ of order q^2. If the number of $\mathbf{F}_{q^2}$-rational points of $\mathcal{X}$ satisfies the Hasse–Weil upper bound, then $\mathcal{X}$ is said to be $\mathbf{F}_{q^2}$-maximal. For a point $P_0 \in \mathcal{X}(\mathbf{F}_{q^2})$, let π be the morphism arising from the linear series $\mathcal{D} := |(q+1)P_0|$, and let $N := \dim(\mathcal{D})$. It is known that $N \geqslant 2$ and that π is independent of P_0 whenever $\mathcal{X}$ is $\mathbf{F}_{q^2}$-maximal.

Mathematics Subject Classifications (2000). 11G20, 11G25, 14G05, 14H05.

Key words. finite field, maximal curve, Hermitian variety, linear series.

1. Introduction

Let $\mathcal{X}$ be a projective, geometrically irreducible, non-singular, algebraic curve defined over $\mathbf{F}_\ell$, the finite field of order ℓ. There is a natural way to define a $\mathbf{F}_\ell$-linear series $\mathcal{D}$ on the curve $\mathcal{X}$ provided that $\mathcal{X}(\mathbf{F}_\ell) \neq \emptyset$, and geometrical and arithmetical properties of $\mathcal{X}$ may be investigated by using $\mathcal{D}$. This linear series $\mathcal{D}$ arises from the characteristic polynomial $h(t)$ of the Jacobian $\mathcal{J}$ (over $\mathbf{F}_\ell$) of $\mathcal{X}$ in the following way; see [7, Section 1.3]. Let $\prod_{i=1}^{T} h_i^{r_i}(t)$ be the factorization of $h(t)$ over $\mathbf{Z}[t]$. Since the Frobenius morphism $\mathbf{Fr}_{\mathcal{J}}$ (over $\mathbf{F}_\ell$) on $\mathcal{J}$ is semisimple and the representation of endomorphisms of $\mathcal{J}$ on the Tate module is faithful [22, Theorem 2], [17, VI, Section 3], we have

$$\prod_{i=1}^{T} h_i(\mathbf{Fr}_{\mathcal{J}}) = 0, \quad \text{on } \mathcal{J}.$$

Now let $P_0 \in \mathcal{X}(\mathbf{F}_\ell)$ and set $m := |\prod_{i=1}^{T} h_i(1)|$. Then the foregoing equation is equivalent to the following linear equivalence of $\mathbf{F}_\ell$-divisors on $\mathcal{X}$:

$$\sum_{i=1}^{U} \alpha_i \mathbf{Fr}_{\mathcal{X}}^{U-i}(P) + \mathbf{Fr}_{\mathcal{X}}^{U}(P) \sim mP_0, \quad P \in \mathcal{X}, \tag{1.1}$$

where $\sum_{i=1}^{U} \alpha_i t^{U-i} + t^U := \prod_{i=1}^{T} h_i(t)$; see [7, Section 1.3].

Assume from now on that ℓ is a square, and let $q := \sqrt{\ell}$. Then $h(t) = (t+q)^{2g}$ if and only if $\mathcal{X}$ is $\mathbf{F}_{q^2}$-maximal, that is $\#\mathcal{X}(\mathbf{F}_{q^2})$ attains the Hasse–Weil upper bound $1 + q^2 + 2qg$, where g is the genus of $\mathcal{X}$. From (1.1), every $\mathbf{F}_{q^2}$-maximal curve $\mathcal{X}$ is equipped with a $\mathbf{F}_{q^2}$-linear series $\mathcal{D} = \mathcal{D}_{\mathcal{X}} = |(q+1)P_0|$ which is independent of $P_0 \in \mathcal{X}(\mathbf{F}_{q^2})$ and satisfies the so-called "Fundamental Equivalence" [6, Corollary 1.2]:

$$qP + \mathbf{Fr}_{\mathcal{X}}(P) \sim (q+1)P_0, \quad \text{for any } P \in \mathcal{X}. \tag{1.2}$$

In particular, $(q+1)P \sim (q+1)P_0$ for all points $P \in \mathcal{X}(\mathbf{F}_{q^2})$; see [19, Lemma 1].

Maximal curves have been intensively studied also in connection with coding theory and cryptography. The pioneer work by Stöhr and Voloch [21], giving among other things an alternative proof of the Hasse–Weil bound via Weierstrass Point Theory, has been widely used to investigate maximal curves, their $\mathcal{D}$-Weierstrass points and the support of the $\mathbf{F}_{q^2}$-Frobenius divisor associated to $\mathcal{D}$. However, the fundamental question in this context, namely whether the $\mathbf{F}_{q^2}$-morphism $\pi : \mathcal{X} \to \pi(\mathcal{X})$ associated to $\mathcal{D}$ is an isomorphism, has only had a partial answer so far [6, Proposition 1.9]. Our Theorem 2.5, which is the first statement in Theorem 0.1, states that π is indeed an isomorphism. This result was originally stated in [7, Section 2.3] but the proof giving there is not correct. Hence the maximal curve $\mathcal{X}$ may be identified with a curve of degree $q+1$ embedded in the projective space $\mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$ with $N = \dim(\mathcal{D})$.

This allows us to investigate in more detail the geometric behaviour of $\mathcal{X}$. In the smallest case, $N = 2$, the curve $\mathcal{X}$ is a non-degenerate Hermitian curve, according to a result due to Rück and Stichtenoth; see [19]. Our Theorem 3.4, which is actually the second statement in Theorem 0.1, is a generalization for $N > 2$, as it states that $\mathcal{X}$ lies on a Hermitian variety $\mathcal{H} \subseteq \mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$ defined over $\mathbf{F}_{q^2}$. It might be that $\mathcal{H}$ is degenerate in some cases, such a possibility occurring when $\mathcal{X}$ is $(N-1)$-strange, that is, the osculating hyperplanes to $\mathcal{X}$ at generic points have a non-empty intersection. This kind of pathology in positive characteristic has been considered by several authors; see for example [9, 12, 15, 16]. What we are able to prove in this direction is the existence of a projection $\phi : \mathbf{P}^N(\bar{\mathbf{F}}_{q^2}) \to \mathbf{P}^M(\bar{\mathbf{F}}_{q^2})$ such that $\phi(\pi(\mathcal{X}))$ lies on a *non-degenerate* Hermitian variety defined over $\mathbf{F}_{q^2}$ of $\mathbf{P}^M(\bar{\mathbf{F}}_{q^2})$; see Theorem 0.2 and Section 3. Here M is the dimension of the smallest linear series $\mathcal{R}$ containing all divisors $qP + \mathbf{Fr}_{\mathcal{X}}(P)$ with P ranging over $\mathcal{X}$. In other words, M is the dimension of the smallest $\mathbf{F}_{q^2}$-vector subspace V of the function field $\mathbf{F}_{q^2}(\mathcal{X})$ such that for any two points $P_1, P_2 \in \mathcal{X}$ there exists $f \in V$ satisfying $qP_1 + \mathbf{Fr}_{\mathcal{X}}(P_1) = qP_2 + \mathbf{Fr}_{\mathcal{X}}(P_2) + \mathrm{div}(f)$. The converse of the first statement of Theorem 0.2 also holds; see Theorem 0.3 and Section 4. Putting together these two theorems we see that the study of $\mathbf{F}_{q^2}$-maximal curves is equivalent to that of projective geometrically irreducible non-singular curves of degree $q+1$ lying on a non-degenerate Hermitian variety defined over $\mathbf{F}_{q^2}$ in a projective space over

$\bar{\mathbf{F}}_{q^2}$. Note that $q+1$ is the minimum degree that a non-singular curve of degree bigger than one lying on a non-degenerate Hermitian variety can have.

2. Maximal Curves and their Natural Embedding in a Projective Space

Our terminology in this and subsequent sections is the same as employed in Section 2 of [21], and in [6].

In this section we assume that $\mathcal{X}$ is a $\mathbf{F}_{q^2}$-maximal curve. Our aim is to show that $\mathcal{X}$ is $\mathbf{F}_{q^2}$-isomorphic to a curve in $\mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$, where N is the dimension of the linear series $\mathcal{D} = \mathcal{D}_{\mathcal{X}} = |(q+1)P_0|$ with $P_0 \in \mathcal{X}(\mathbf{F}_{q^2})$. Let $\pi\colon \mathcal{X} \to \mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$ be the morphism associated to $\mathcal{D}$.

LEMMA 2.1 ([6, Prop. 1.9]). *The following statements are equivalent:*

(1) *$\mathcal{X}$ is $\mathbf{F}_{q^2}$-isomorphic to $\pi(\mathcal{X})$;*
(2) *$\pi(P) \in \mathbf{P}^N(\mathbf{F}_{q^2})$ if and only if $P \in \mathcal{X}(\mathbf{F}_{q^2})$, for $P \in \mathcal{X}$;*
(3) *q is a Weierstrass non-gap at P, for $P \in \mathcal{X}$.*

Hence we can limit ourselves to prove the above statement (2). To do this we need some previous results concerning $\mathcal{D}$-orders and $\mathbf{F}_{q^2}$-Frobenius $\mathcal{D}$-orders.

Let $\varepsilon_0 = 0 < \varepsilon_1 = 1 < \cdots < \varepsilon_N$ and $v_0 = 0 < v_1 < \cdots < v_{N-1}$ denote respectively the $\mathcal{D}$-orders and the $\mathbf{F}_{q^2}$-Frobenius $\mathcal{D}$-orders of the curve $\mathcal{X}$.

LEMMA 2.2 ([6, Thm. 1.4]). *The following statements hold:*

(1) $\varepsilon_N = q$;
(2) $v_{N-1} = q$;
(3) $v_1 = 1$ *if and only if* $N \geqslant 3$;
(4) $0, 1$, *and* q *(resp.* $q+1$*) are* $(\mathcal{D}, P)$*-orders provided that* $P \notin \mathcal{X}(\mathbf{F}_{q^2})$ *(resp.* $P \in \mathcal{X}(\mathbf{F}_{q^2})$*).*

Let $\pi = (f_0 : \ldots : f_N)$ where each projective coordinate f_i belongs to $\mathbf{F}_{q^2}(\mathcal{X})$, the function field over $\mathbf{F}_{q^2}$ of $\mathcal{X}$. As in [21], we will consider $\pi\colon \mathcal{X} \to \mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$ as a parametrized curve in $\mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$, and the points $P \in \mathcal{X}$ will be viewed as its places (or branches). Then the intersection divisor $\pi^{-1}(H)$ of $\mathcal{X}$ arising from a hyperplane H of $\mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$ is defined in the usual manner, and $\mathcal{D}$ turns out be the linear series of hyperplane sections, see [21, p. 3]. In particular, the osculating hyperplane at P is the hyperplane in $\mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$ which intersects the branch P with multiplicity j_N, where $(j_0, j_1, \ldots, j_N)$ is the $(\mathcal{D}, P)$-order sequence, see [21, p. 4].

Put $\mathcal{L}((q+1)P_0) = \langle f_0, \ldots, f_N \rangle$. By Lemma 2.2(1) and [8, Thm.1], there exist $z_0, \ldots, z_N \in \mathbf{F}_{q^2}(\mathcal{X})$, not all zero, such that

$$z_0^q f_0 + \ldots + z_N^q f_N = 0\,. \tag{2.1}$$

Some features of the homogeneous N-tuple $(z_0, \ldots, z_N)$ are stated in the following lemma.

https://doi.org/10.1023/A:1017553432375 Published online by Cambridge University Press

LEMMA 2.3

(1) *The osculating hyperplane at* $P \in \mathcal{X}$ *has equation*

$$w_0^q(P)X_0 + w_1^q(P)X_1 + \ldots + w_N^q(P)X_N = 0$$

where $w_i := t^{e_P} z_i$, *with* t *a local parameter at* P, *and* $e_P := -\min\{v_P(z_0), \ldots, v_P(z_N)\}$;

(2) *The following relation also holds:*

$$z_0 f_0^q + \ldots + z_N f_N^q = 0. \tag{2.2}$$

(3) *The* $\mathbf{F}_{q^2}$*-rational functions* $z_0, z_1, \ldots z_N$ *are uniquely determined by Equation (2.1) up to a non-zero factor in* $\mathbf{F}_{q^2}(\mathcal{X})$;

Proof. (1) For $i = 0, \ldots, N$, let

$$w_i(t) = \sum_{j=0}^{\infty} a_j^{(i)} t^j \in \bar{\mathbf{F}}_{q^2}[[t]]$$

be the local expansion of w_i at P. As there exists $i \in \{0, \ldots, N\}$ such that $a_0^{(i)} \neq 0$ (e.g. i satisfying $e_P = -v_P(z_i)$), we can consider the following hyperplane in $\mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$:

$$H : \sum (a_0^{(i)})^q X_i = 0.$$

Then, thanks to Lemma 2.2(4), part (1) follows, once we have shown that $v_P(\pi^{-1}(H)) \geqslant q$. Taking Equation (2.1) into consideration,

$$v_P\left(\sum_{i=0}^{N} (a_0^{(i)})^q f_i\right) = v_P\left(t^q \sum_{i=0}^{N} \sum_{j=1}^{\infty} a_j^{(i)} t^{qj-q} f_i\right), \tag{2.3}$$

yielding the desired relation $v_P(\pi^{-1}(H)) \geqslant q$.

(2) By the Fundamental Equivalence (1.2), $\mathbf{Fr}_{\mathcal{X}}(P)$ belongs to the osculating hyperplane at P for every $P \in \mathcal{X}$. Then from Equation (2.1) we infer for all but a finitely many points $P \in \mathcal{X}$ that

$$\sum_{i=0}^{N} z_i(P)^q f_i(P)^{q^2} = 0$$

and part (2) follows.

(3) This is clear because once the projective coordinates are fixed, then the osculating hyperplane at any point is uniquely determined modulo a non-zero element of $\bar{\mathbf{F}}_{q^2}$. □

LEMMA 2.4. *Let* $P \in \mathcal{X}$ *be such that* $\pi(P) \in \mathbf{P}^N(\mathbf{F}_{q^2})$. *Then* $P \in \mathcal{X}(\mathbf{F}_{q^2})$.

Proof. Since $\pi(P)$ is $\mathbf{F}_{q^2}$-rational we can take it to be the point $(1 : 0 : \ldots : 0)$ by means of a $\mathbf{F}_{q^2}$-linear transformation. The new coordinates still satisfy Equations

https://doi.org/10.1023/A:1017553432375 Published online by Cambridge University Press

(2.1) and (2.2). In addition, we can assume that $\pi = (1 : f_1 : \ldots : f_N)$ so that $v_P(f_i) \geqslant 1$ for $i \geqslant 1$. Now, the set-up and the results of the computation involving local expansion in the proof of Lemma 2.3(2) together with Lemma 2.2(4) allow us to limit ourselves to check that $v_P(\pi^{-1}(H)) \geqslant q+1$ for every point P chosen such that $\pi(P) \in \mathbf{P}^N(\mathbf{F}_{q^2})$. As we have already noted, $v_P(f_i) \geqslant 1$ for $i \geqslant 1$. Then, taking also into consideration Equation (2.3), we only need to see that $a_1^{(0)} = 0$. As a matter of fact, this follows from Equation (2.2), and hence the proof of the lemma is complete. □

As a corollary to Lemmas 2.1 and 2.4, we obtain the following result.

THEOREM 2.5. *The morphism π is a closed embedding, i.e., $\mathcal{X}$ is $\mathbf{F}_{q^2}$-isomorphic to $\pi(\mathcal{X})$.*

Remark 2.6. (1) As was shown in [6, Section 2], [7, Section 2.3], a class of $\mathbf{F}_{q^2}$-maximal curves can be characterized by the type of the Weierstrass semigroup at some $\mathbf{F}_{q^2}$-rational point of the curve. The semigroups involved in such a characterization belong to a special family of numerical semigroups H defined by the following two properties:

(i) $q, q+1 \in H$;
(ii) there exist $r, s \in H$ so that each $h \in H$ with $h \leqslant q+1$ is generated by r and s.

Indeed, if a $\mathbf{F}_{q^2}$-maximal curve has a $\mathbf{F}_{q^2}$-rational point P_0 such that the Weierstrass semigroup $H(P_0)$ at P_0 satisfies each of the above two conditions, then $H(P_0) = \langle r, s \rangle$. In particular, the genus of such a curve is $(r-1)(s-1)/2$. Other interesting properties of maximal curves depending on the behaviour of their Weierstrass points were pointed out in [7, Section 2.4].

(2) Theorem 2.5 implies that

$$\mathrm{Aut}_{\mathbf{F}_{q^2}}(\mathcal{X}) \cong \{A \in PGL(N+1, q^2) : A\pi(\mathcal{X}) = \pi(\mathcal{X})\}. \tag{2.4}$$

For a stronger result on $\mathrm{Aut}(\mathcal{X})$, see Theorem 3.7.

Remark 2.7. For an application of Theorem 2.5 in Section 3 we stress that the condition of $\mathcal{D}$ being a complete linear series was not used. Hence Theorem 2.5 holds true if $\mathcal{D}$ is replaced by a (non-complete) linear subseries $\mathcal{R}$ of $\mathcal{D}$ as long as $\mathcal{R}$ contains all divisors $qP + \mathbf{Fr}_{\mathcal{X}}(P)$ with $P \in \mathcal{X}$, and π means the morphism associated to $\mathcal{R}$.

3. On the Dual of $\pi(\mathcal{X})$

The *dual* curve (also called *strict dual*) $\mathcal{Z}^\star$ of a non-degenerate, projective, geometrically irreducible, algebraic curve $\mathcal{Z}$ of a projective space $\mathbf{P}$ is the closure

https://doi.org/10.1023/A:1017553432375 Published online by Cambridge University Press

in the dual projective space $\mathbf{P}^\star$ of the subset of points which represent the osculating hyperplane L_P^{N-1} to $\mathcal{Z}$ at some general point $P \in \mathcal{Z}$, see for instance [12] and [9].

In this section, we assume that $\mathcal{X}$ is a maximal curve over $\mathbf{F}_{q^2}$, and identify $\mathcal{X}$ with $\pi(\mathcal{X})$ according to Theorem 2.5. Let $\pi^\star : \mathcal{X} \to \mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$ be the morphism with coordinate functions $z_0, z_1, \ldots, z_N$ introduced in the previous section. By Lemma 2.3(1), $\mathbf{Fr}_q \circ \pi^\star$ is the Gauss map $P \mapsto L_P^{(N-1)}$, where $\mathbf{Fr}_q : (X_0 : \ldots : X_N) \mapsto (X_0^q : \ldots : X_N^q)$. This leads us to consider the curve $\pi^\star(\mathcal{X})$ in $\mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$. Note that, $\pi^\star(\mathcal{X})$ might be a degenerate curve in the sense that it might happen that $\pi^\star(\mathcal{X})$ is contained and non-degenerated in a subspace $\mathbf{P}^M$ of $\mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$. By a result due to Kaji [16, Prop. 1], see also [9, Prop. 2], if this is the case then there is a $(N-M)$-dimensional subspace $\mathbf{P}^{N-M}$ of $\mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$ which is the intersection of the osculating hyperplane to $\mathcal{X}$ at general points $P \in \mathcal{X}$, that is apart from a finite number of points $P \in \mathcal{X}$.

In our situation, no point of $\mathcal{X}$ lies on $\mathbf{P}^{N-M}$. In fact, let $R \in \mathbf{P}^{N-M}$, and assume on the contrary that $R \in \mathcal{X}$. Choose a point $Q \in \mathcal{X}$ such that $Q \neq R$ but the osculating hyperplane L_Q to $\mathcal{X}$ at Q contains P^{M-N}. Since L_Q meets $\mathcal{X}$ in $\{Q, \mathbf{Fr}_{\mathcal{X}}(Q)\}$ we have that $\mathbf{Fr}_{\mathcal{X}}(Q) = R$, and hence Q is uniquely determined by R. But this is a contradiction, as we can choose Q in infinite different ways.

Furthermore, $\mathbf{P}^M$ is invariant under the Frobenius collineation $(X_0 : \ldots : X_N) \mapsto (X_0^{q^2} : \ldots : X_N^{q^2})$. This yields that $\mathbf{P}^M$ is defined over $\mathbf{F}_{q^2}$. Take a new $\mathbf{F}_{q^2}$-invariant frame in $\mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$ in such a way that $\mathbf{P}^M$ has equation $X_{M+1} = 0, \ldots, X_N = 0$. Then $z_{M+1} = 0, \ldots, z_N = 0$ and $\pi^\star : \mathcal{X} \to \mathbf{P}^M$ is given by $(z_0 : \ldots : z_M)$. Hence, according to Lemma 2.3(1), the equation of the osculating hyperplane to $\mathcal{X}$ at Q is $\gamma_0^q X_0 + \ldots + \gamma_M^q X_M = 0$, where $\pi^\star(Q) = (\gamma_0 : \ldots : \gamma_M)$.

LEMMA 3.1. *We have* $\deg(\pi^\star(\mathcal{X})) = q + 1$, *and the linear series cut out on* $\pi^\star(\mathcal{X})$ *by hyperplanes of* $\mathbf{P}^M$ *contains all divisors* $qP + \mathbf{Fr}_{\mathcal{X}}(P)$ *with* $P \in \mathcal{X}$.

Proof. Choose a point $P_0 = (\alpha_0 : \ldots : \alpha_N) \in \mathcal{X}(\mathbf{F}_{q^2})$. Here, $\alpha_i \neq 0$ for some i with $0 \leqslant i \leqslant M$. In fact, if $\alpha_i = 0$ for $i = 0, \ldots, M$, then P_0 would belong to the hyperplane osculating at general points of $\mathcal{X}$ and so P_0 would be in the above $\mathbf{P}^{N-M}$ which is impossible as we have shown before. Now consider the hyperplane H of equation $\alpha_0^q X_0 + \cdots + \alpha_M^q X_M = 0$ which can be regarded as a hyperplane of $\mathbf{P}^M$.

Let $P \in \mathcal{X}$ such that $\pi^\star(P) = (\gamma_0 : \ldots : \gamma_M) \in H \cap \pi^\star(\mathcal{X})$, $\gamma_i \in \bar{\mathbf{F}}_{q^2}$. We have that $\alpha_0^q \gamma_0 + \cdots + \alpha_M^q \gamma_M = 0$ so that $\gamma_0^q \alpha_0 + \ldots + \gamma_M^q \alpha_M = 0$. This shows that the osculating hyperplane to $\mathcal{X}$ at P passes through P_0 (Lemma 2.3(1)). Since $P_0 \in \mathcal{X}(\mathbf{F}_{q^2})$, this is only possible when $P = P_0$. Thus we have proved that $H \cap \pi^\star(\mathcal{X})$ contains no point different from $\pi^\star(P_0)$. We want to show next that the divisor $(\pi^\star)^{-1}(H)$ of $\mathcal{X}$ is $(q+1)P_0$. To do this we have to show that

$$v_{P_0}((\pi^\star)^{-1}(H)) = v_{P_0}(\alpha_0^q w_0 + \ldots + \alpha_N^q w_N) = q + 1,$$

where v_{P_0} denotes the valuation at P_0, $w_i := t^{e_{P_0}} z_i$, t is a local parameter at P_0 and $e_{P_0} := -\min\{v_{P_0}(z_0), \ldots, v_{P_0}(z_N)\}$. (Recall that $z_{M+1} = \ldots = z_N = 0$.)

https://doi.org/10.1023/A:1017553432375 Published online by Cambridge University Press

After a $\mathbf{F}_{q^2}$-linear transformation of $\mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$ we may assume that $P_0 = (1 : 0 : \ldots : 0)$ and that

$$f_0 = 1, \quad f_1 = a_1 t^{j_1} + \cdots, \quad f_N = a_N t^{j_N} + \cdots,$$

where $f_i = f_i/f_0$ and $(0, j_1, \ldots, j_N)$ is the $(\mathcal{D}, P_0)$-order sequence of $\mathcal{X}$. Then we have to show that $v_{P_0}(w_0) = q + 1$.

From Equation (2.2) we deduce that

$$w_0(t) + w_1(t)(a_1 t^{j_1} + \cdots)^q + \cdots + w_N(t)(a_N t^{j_N} + \cdots)^q = 0. \tag{3.1}$$

On the other hand, we claim that $v_{P_0}(w_1(t)) = 1$. By (2.1)

$$w_0(t)^q + w_1(t)^q(a_1 t^{j_1} + \cdots) + \cdots + w_N(t)^q(a_N t^{j_N} + \cdots) = 0.$$

From the definition of w_i it follows that $v_{P_0}(w_i(t)) = 0$ for almost one index i. Since $1 = j_1 < j_2 < \cdots < j_N = q + 1$ and $j_{N-1} \leqslant q$ the only possibility is $i = N$, and $w_1(t) = ut + \cdots$ with $u \neq 0$. The latter relation proves the claim. Now, this together with Equation (3.1) yield that $v_{P_0}((\pi^\star)^{-1}(H)) = q + 1$. Hence, $(\pi^\star)^{-1}(H)$ of $\mathcal{X}$ is $(q + 1)P_0$ from which the first part of the Lemma 3.1 follows. The second part follows from the Fundamental Equivalence (1.2). □

This lemma together with Remark 2.7 have the following corollary.

LEMMA 3.2. *The curves $\mathcal{X}$ and $\pi^\star(\mathcal{X})$ are $\mathbf{F}_{q^2}$-isomorphic.*

Also, since $\mathcal{D}$ is a complete linear series, Lemma 3.1 gives the following result:

LEMMA 3.3. *Every $z_i, 0 \leqslant i \leqslant N$, is an $\mathbf{F}_{q^2}$-linear combination of $f_0, \ldots, f_N$.*

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

THEOREM 3.4. *The curve $\mathcal{X}$ lies on a Hermitian variety defined over $\mathbf{F}_{q^2}$ of $\mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$.*

Proof. Without loss of generality we may suppose that $f_0 = z_0 = 1$. For $i = 0, \ldots, N$, let $z_i = \sum_{j=0}^N c_{ij} f_j$ with $c_{ij} \in \mathbf{F}_{q^2}$. Note that $c_{ij} = 0$ for $M + 1 \leqslant i \leqslant N$ and that the matrix $C = (c_{ij})$ has rank $M + 1$. We prove that C is actually a Hermitian matrix over $\mathbf{F}_{q^2}$. To do this, we re-write Equation (2.2) in the following manner:

$$1 + \sum_{i=0}^N (c_{i1}^q f_i)^q f_1 + \cdots + \sum_{i=0}^N (c_{iN}^q f_i)^q f_N = 0.$$

Taking into account the uniqueness of the N-tuple $(z_0 = 1, z_1, \ldots, z_N)$ proved in

https://doi.org/10.1023/A:1017553432375 Published online by Cambridge University Press

Lemma 2.3(3), comparison with Equation (2.1) gives

$$\sum_{i=0}^{N} c_{i1}^q f_i = \sum_{i=0}^{N} c_{1i} f_i, \ldots, \sum_{i=0}^{N} c_{iN}^q f_i = \sum_{i=0}^{N} c_{Ni} f_i.$$

Since $f_0 = 1, f_1, \ldots, f_N$ are linearly independent over $\mathbf{F}_{q^2}$, this yields $c_{ij} = c_{ji}^q$ for every $0 \leqslant i, k \leqslant N$. This proves that C is Hermitian. After a $\mathbf{F}_{q^2}$-linear transformation of $\mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$ we may assume that C is the $N \times N$ diagonal matrix with $M+1$ ones on its diagonal. Then (2.1) becomes $f_0^{q+1} + \ldots + f_M^{q+1} = 0$, and hence $\mathcal{X}$ lies on the Hermitian variety of equation $X_0^{q+1} + \ldots + X_M^{q+1} = 0$. □

Remark 3.5. From the proof above, $z_i = f_i$ for $0 \leqslant i \leqslant M$. Hence $\pi^\star(\mathcal{X})$ is the projection $(f_0 : \ldots : f_N) \to (f_0 : \ldots : f_M)$, and $\pi^\star(\mathcal{X})$ lies on a non-degenerate Hermitian variety defined over $\mathbf{F}_{q^2}$ of $\mathbf{P}^M(\bar{\mathbf{F}}_{q^2})$.

Taking into account Lemma 3.2 we obtain the following result.

THEOREM 3.6. *$\mathcal{X}$ admits a non-singular model given by a curve defined over $\mathbf{F}_{q^2}$ which has degree $q+1$ and lies on a non-degenerate Hermitian variety defined over $\mathbf{F}_{q^2}$ of $\mathbf{P}^M(\bar{\mathbf{F}}_{q^2})$ of dimension $M \leqslant N$.*

From the above arguments, it also turns out that the osculating hyperplane to $\mathcal{X}$ at any point $P \in \mathcal{X}$ coincides with the tangent hyperplane to the non-degenerate Hermitian variety at the same point P. This allows us to improve the previous result (2.4) on $\mathrm{Aut}_{\mathbf{F}_{q^2}}(\mathcal{X})$:

THEOREM 3.7. *$\mathrm{Aut}_{\mathbf{F}_{q^2}}(\mathcal{X})$ is isomorphic to a subgroup of the projective unitary group $PGU(M+1, \mathbf{F}_{q^2})$.*

Proof. By a way of contradiction, assume that $\mathcal{X}$ lies not only on $\mathcal{H}$ but also on the non-degenerate Hermitian variety $\mathcal{H}'$ which is assumed to be the image of $\mathcal{H}$ by a non-trivial $\mathbf{F}_{q^2}$-linear collineation fixing $\mathcal{X}$. Choose any point $P \in \mathcal{X}$. Then the $\mathcal{H}$ and $\mathcal{H}'$ have the same tangent hyperplane at P, as each of these tangent hyperplanes coincides with the osculating hyperplane to $\mathcal{X}$ at P. To express this geometric condition in algebraic terms, set $P := (x_0 : \ldots : x_M)$, and write the equations of $\mathcal{H}$ and $\mathcal{H}'$ explicitly: $\mathcal{H} := X_0^{q+1} + \cdots + X_N^{q+1} = 0$; $\mathcal{H}' := \mathbf{X}^t C(\mathbf{X})^q = 0$ where $\mathbf{X} := (X_0, \ldots, X_M)$, and C is a non-singular non-identity unitary matrix of rank $M+1$. Then the above geometric condition in algebraic terms is that the homogeneous $(M+1)$-tuples $(x_0^q, \ldots, x_M^q)$ and $(c_{0,0}x_0^q + \cdots + c_{M,0}x_M^q, \ldots, c_{0,M}x_0^q + \cdots + c_{M,M}x_M^q)$ are equal up to a non-zero factor. Another meaning of the latter relation is that the non-trivial $\mathbf{F}_{q^2}$-linear collineation associated to the matrix C fixes $\mathcal{X}$ pointwise. Since $\mathcal{X}$ is not contained in a hyperplane of $\mathbf{P}^M$, so C must be the identity up to a non-zero factor. But this occurs only if $\mathcal{H}$ and $\mathcal{H}'$ coincide; a contradiction. □

Remark 3.8. We point out that the possibility mentioned in the Introduction and Remark 2.7 can actually occur.

Let $\mathbf{F}_{q^2}(x)$ be the rational function field, and let $\mathcal{X}$ be the normal rational curve $\mathcal{X}$ of degree $q+1$ in $\mathbf{P}^{q+1}(\bar{\mathbf{F}}_{q^2})$ given by the coordinate functions $f_i = x^i$, $i = 0, \ldots, q+1$. Clearly $\mathcal{X}$ is an $\mathbf{F}_{q^2}$-maximal curve of genus $g = 0$. For a point $P(a) = (1 : a : \ldots : a^{q+1}) \in \mathcal{X}$, the hyperplane of $\mathbf{P}^{q+1}(\bar{\mathbf{F}}_{q^2})$ of equation $a^{q^2+q}X_0 - a^qX_1 - a^{q^2}X_q + X_{q+1} = 0$ cuts out on $\mathcal{X}$ the divisor $qP + \mathbf{Fr}_{\mathcal{X}}(P)$. To show it note that $\mathbf{Fr}_{\mathcal{X}}(P(a)) = P(a^{q^2})$, and choose a local parameter t of $\mathcal{X}$ at $P(a)$. Then $x_i = (a+t)^i$, $i = 0, \ldots, q+1$, is a local expansion of $\mathcal{X}$ at $P(a)$, and the claim follows from the following straightforward computations

$$a^{q^2+q} - a^q(a+t) - a^{q^2}(a+t)^q + (a+t)^{q+1} = t^q(a - a^{q^2} + t)$$

and

$$a^{q^2+q} - a^q a^{q^2} - a^{q^2}(a^q)^{q^2} + (a^{q+1})^{q^2} = 0.$$

This shows that the smallest linear series $\mathcal{R}$ containing all divisors $qP + \mathbf{Fr}_{\mathcal{X}}(P)$ with P ranging over all points P of $\mathcal{X}$ is cut out by the 3-dimensional linear systems of all hyperplanes of equation $u_0X_0 + u_1X_1 + u_qX_q + u_{q+1}X_{q+1} = 0$; that is $M = 3$ in our case. On the other hand, since $\mathcal{X}$ is rational, the complete linear series $|(q+1)P|$ with $P \in \mathcal{X}(\mathbf{F}_{q^2})$ has dimension $N = q+1$. Hence, for $q > 2$, the strict inequality $M < N$ occurs.

Our final remark is that $\mathcal{X}$ is in the intersection of the Hermitian variety $X_0^qX_3 + X_0X_3^q - X_1^{q+1} - X_2^{q+1} = 0$ and the quadric $X_0X_3 - X_1X_2 = 0$.

4. Curves Lying on a Hermitian Variety

The aim of this section is to show that the property given in Theorem 3.6 characterizes $\mathbf{F}_{q^2}$-maximal curves. For this purpose, we assume from now on that $\mathcal{X}$ is a projective geometrically irreducible non-singular algebraic curve defined over a finite field $\mathbf{F}_{q^2}$ which is equipped with a non-degenerated $\mathbf{F}_{q^2}$-birational morphism $\pi = (f_0 : \ldots : f_M) : \mathcal{X} \to \mathbf{P}^M(\bar{\mathbf{F}}_{q^2})$ such that the curve $\mathcal{Y} := \pi(\mathcal{X})$ has the following properties:

- It has degree $q+1$, and it lies on a non-degenerate Hermitian variety $\mathcal{H} \subseteq \mathbf{P}^M(\bar{\mathbf{F}}_{q^2})$ defined over $\mathbf{F}_{q^2}$.

The main result in this section is the following theorem.

THEOREM 4.1. *The curve $\mathcal{X}$ is $\mathbf{F}_{q^2}$-maximal.*

The Hermitian variety $\mathcal{H}$ of $\mathbf{P}^M(\bar{\mathbf{F}}_{q^2})$ is assumed to be in its canonical form $X_0^{q+1} + \ldots + X_M^{q+1} = 0$. By our hypothesis,

$$f_0^{q+1} + \cdots + f_M^{q+1} = 0\,. \tag{4.1}$$

https://doi.org/10.1023/A:1017553432375 Published online by Cambridge University Press

For any point $P \in \mathcal{X}$, let $\pi(P) = (\alpha_0 : \ldots : \alpha_M)$. Choose a local parameter t at P, and arrange the coordinate functions to have $v_P(f_i) \geqslant 0$ for $i = 0, \ldots, M$ and $v_P(f_k) = 0$ for at least one index $k \in \{0, \ldots, M\}$. Then

$$f_i(t) = \sum_{j=0}^{\infty} a_{i,j} t^j \in \bar{\mathbf{F}}_{q^2}[[t]]$$

is the local expansion of f_i at P. Here, $\alpha_i = a_{i,0}$ and $a_{k,0} \neq 0$. The tangent hyperplane H_P to the Hermitian variety at $\pi(P)$ has equation $\alpha_0^q X_0 + \cdots + \alpha_M^q X_M = 0$.

The first step toward Theorem 4.1 is the following lemma.

LEMMA 4.2. *The linear series $\mathcal{R}$ cut out on $\mathcal{Y}$ by hyperplanes contains the divisor $qP + \mathbf{Fr}_{\mathcal{X}}(P)$ for every $P \in \mathcal{X}$.*

Proof. We show that H_P cuts out on $\mathcal{Y}$ the divisor $qP + \mathbf{Fr}_{\mathcal{X}}(P)$. From Equation (4.1),

$$\left(\sum_{j=0}^{\infty} a_{0,j} t^j\right)^q f_0 + \cdots + \left(\sum_{j=0}^{\infty} a_{M,j} t^j\right)^q f_M = 0. \tag{4.2}$$

Writing the lower order terms in t, we have

$$\sum_{i=0}^{M} a_{i,0}^q f_i + t^q \sum_{i=0}^{M} a_{i,0} a_{i,1}^q + t^{q+1} \sum_{i=0}^{R} a_{i,1}^{q+1} + t^{q+2}[\ldots] = 0.$$

Hence $v_P(\pi^{-1}(H_P) \geqslant q$ and equality holds if and only if $\sum_{i=0}^{M} a_{i,1}^q a_{i,0} \neq 0$. We show that, if $P \in \mathcal{X}(\mathbf{F}_{q^2})$, then $\sum_{i=0}^{M} a_{i,1}^q a_{i,0} = 0$. From (4.2),

$$\sum_{i=0}^{M} a_{i,0}^{q+1} + t \sum_{j=0}^{M} a_{i,0}^q a_{i,1} + t^q[\ldots] = 0.$$

Thus, $\sum_{i=0}^{M} a_{i,0}^q a_{i,1} = 0$. Since $(\sum_{i=0}^{M} a_{i,0}^q a_{i,1})^q = \sum_{i=0}^{M} a_{i,0} a_{i,1}^q$ for $P \in \mathcal{X}(\mathbf{F}_{q^2})$, the claim follows. Since π is birational and $\deg(\mathcal{Y}) = q + 1$, we obtain $\pi^{-1}(H_P) = (q+1)P$ for every $P \in \mathcal{X}(\mathbf{F}_{q^2})$, which shows the lemma for every $P \in \mathcal{X}(\mathbf{F}_{q^2})$. For the case $P \notin \mathcal{X}(\mathbf{F}_{q^2})$, we also need to check that $\mathbf{Fr}_{\mathcal{X}}(P) \in H_P$. This inclusion occurs when $\sum_{i=0}^{M} \alpha_i^{q^2+q} = 0$. Since the latter relation is a consequence of (4.2), the claim follows. Hence, $\pi^{-1}(H_P) = qP + \mathbf{Fr}_{\mathcal{X}}(P)$ because π is birational and $\deg(\mathcal{Y}) = q + 1$, □

Then, from Remark 2.7 and Lemma 4.2, follows that $\mathcal{X}$ and $\mathcal{Y} = \pi(\mathcal{X})$ are $\mathbf{F}_{q^2}$-isomorphic. Hence, if $M = 2$, $\mathcal{Y}$ is the Hermitian curve and so $\mathcal{X}$ is $\mathbf{F}_{q^2}$-maximal. From now on we assume $M \geqslant 3$.

Our approach is based on a certain relationship between the Wronskians determinants of $\mathcal{Y}$ and its projection to a $(M-1)$-dimensional subspace of $\mathbf{P}^M(\bar{\mathbf{F}}_{q^2})$. More precisely, let $\bar{\pi} : \mathcal{X} \to \mathbf{P}^{M-1}(\bar{\mathbf{F}}_{q^2})$ be defined by $\mathcal{X} \to (f_0 : \ldots : f_{M-1})$; i.e., $\bar{\mathcal{Y}}$ is the projection of $\mathcal{Y}$ from the point $(0 : \ldots 0 : 1)$ to

https://doi.org/10.1023/A:1017553432375 Published online by Cambridge University Press

the hyperplane $X_M = 0$. It might happen that $\mathcal{Y}$ and $\bar{\mathcal{Y}}$ are not $\mathbf{F}_{q^2}$-birationally equivalent. However, it is always possible to avoid this situation by changing the coordinate system in $\mathbf{P}^M(\bar{\mathbf{F}}_{q^2})$. A technical lemma is needed.

LEMMA 4.3. (1) *The space* $\mathbf{P}^M(\mathbf{F}_{q^2})$ *contains a point* P *satisfying each of the following three conditions:*

- P *is not on* $\mathcal{H}$;
- *no tangent line to* $\mathcal{Y}$ *at a* $\mathbf{F}_{q^2}$*-rational point passes through* P;
- *no chord through two* $\mathbf{F}_{q^2}$*-rational points of* $\mathcal{Y}$ *passes through* P.

(2) *Let* r *be a* $\mathbf{F}_{q^2}$*-rational line through a* $\mathbf{F}_{q^2}$*-rational point* R *of* $\mathcal{Y}$. *Then* $r \cap \mathcal{Y}$ *only contains* $\mathbf{F}_{q^2}$*-rational points from* $\mathcal{Y}$.

Proof. (1) Take a $\mathbf{F}_{q^2}$-rational point $Q \in \mathcal{Y}$. Since the number of $\mathbf{F}_{q^2}$-rational points of $\mathcal{X}$ is $q^2 + 1 + 2gq \leqslant q^3 + 1$, there are at most q^3 chords through Q and another $\mathbf{F}_{q^2}$-rational point of $\mathcal{Y}$. But, since $M \geqslant 3$, the number of $\mathbf{F}_{q^2}$-rational lines through Q is at least $q^4 + q^2 + 1$ and hence one of these lines is neither a line contained in $\mathcal{H}$, nor a tangent line to $\mathcal{Y}$ at Q, nor a chord through Q and another $\mathbf{F}_{q^2}$-rational point of $\mathcal{Y}$. Now, any $\mathbf{F}_{q^2}$-rational point P outside $\mathcal{H}$ is a good choice for P.

(2) Assume on the contrary that r meets $\mathcal{Y}$ in a non $\mathbf{F}_{q^2}$-rational point S. Then r is the line joining S and $\mathbf{F}r(S)$. This implies that r is contained in the osculating hyperplane of $\mathcal{Y}$ at S. Hence the common points of r with $\mathcal{Y}$ are only two, namely S and $\mathbf{F}r(S)$. But this contradicts the hypothesis that $R \in r \cap \mathcal{Y}$. □

Take a point P as in Lemma 4.3(1). By a classical result (see [20], and also [14, 23.4]), the linear collineation group $PGU(M+1, q^2)$ preserving $\mathcal{H}$ acts transitively on the set of all points of $\mathbf{P}^M(\bar{\mathbf{F}}_{q^2})$ not on $\mathcal{H}$. Hence a linear collineation of $\mathbf{P}^M(\bar{\mathbf{F}}_{q^2})$ can be applied which preserves $\mathcal{H}$ and maps P to $(0 : \ldots : 0 : 1)$. Lemma 4.3 ensures now that $\mathcal{Y}$ and $\bar{\mathcal{Y}}$ are $\mathbf{F}_{q^2}$-birationally equivalent.

So we can assume that $\mathcal{Y}$ is $\mathbf{F}_{q^2}$-birationally equivalent to $\bar{\mathcal{Y}}$.

Choose a separating variable t of $\mathcal{X}$, and define D_t as the Hasse derivative with respect to t; see [11]. Then [21, Section 1]:

$$\mathcal{W}(f_0, \ldots, f_{M-1}) := \det \begin{bmatrix} D_t^{\varepsilon_0} f_0 & D_t^{\varepsilon_0} f_1 & \ldots & D_t^{\varepsilon_0} f_{M-1} \\ \vdots & \vdots & \ldots & \vdots \\ D_t^{\varepsilon_{M-1}} f_0 & D_t^{\varepsilon_{M-1}} f_1 & \ldots & D_t^{\varepsilon_{M-1}} f_{M-1} \end{bmatrix}$$

and

$$\mathcal{W}(f_0, \ldots, f_M) := \det \begin{bmatrix} D_t^{\varepsilon_0} f_0 & D_t^{\varepsilon_0} f_1 & \ldots & D_t^{\varepsilon_0} f_M \\ \vdots & \vdots & \ldots & \vdots \\ D_t^{\varepsilon_M} f_0 & D_t^{\varepsilon_M} f_1 & \ldots & D_t^{\varepsilon_M} f_M \end{bmatrix}.$$

Note that in our case $\varepsilon_0 = 0, \varepsilon_1 = 1, \ldots, \varepsilon_M = q$.

https://doi.org/10.1023/A:1017553432375 Published online by Cambridge University Press

LEMMA 4.4. *We have that*

$$\begin{aligned}\operatorname{div}(\mathcal{W}(f_0,\ldots,f_M)) = \operatorname{div}(\mathcal{W}(f_0,\ldots,f_{M-1})) - q\operatorname{div}(f_M)\\ + \operatorname{div}(f_0 D_t^q f_0^q + \cdots + f_M D_t^q f_M^q).\end{aligned}$$

Proof. Multiplying the last column by f_M^q and adding to it f_0^q times the first column plus f_1^q times the second column etc. plus f_{M-1}^q times the penultimate column gives

$$f_M^q \mathcal{W}(f_0,\ldots,f_M) = \begin{bmatrix} f_0 & f_1 & \ldots & f_0^{q+1}+\cdots+f_M^{q+1} \\ D_t f_0 & D_t f_1 & \ldots & f_0^q D_t f_0 + \cdots + f_M^q D_t f_M \\ \vdots & \vdots & \ldots & \vdots \\ D_t^q f_0 & D_t^q f_1 & \ldots & f_0^q D_t^q f_0 + \cdots + f_M^q D_t^q f_M \end{bmatrix}.$$

Each element but the last one in the last column is actually 0. In fact, this follows from the relation (4.1) by derivation. Furthermore, the qth Hasse derivative of the same relation gives

$$f_0^q D_t f_0 + \cdots + f_M^q D_t f_M + f_0 D_t^q f_0^q + \cdots + f_M D_t^q f_M^q = 0,$$

and this completes the proof. □

Let R_M be the ramification divisor of the linear series cut out on $\mathcal{Y}$ by hyperplanes of $\mathbf{P}^M(\bar{\mathbf{F}}_{q^2})$. The following result comes from [21, p. 6]:

LEMMA 4.5. *Let $P \in \mathcal{X}$. If t is a local parameter of $\mathcal{X}$ at P, then*

$$v_P(R_M) = v_P(\mathcal{W}(f_0,\ldots,f_M)).$$

Similarly, let R_{M-1} be the ramification divisor of the linear series cut out on $\bar{\mathcal{Y}}$ by hyperplanes of $\mathbf{P}^{M-1}(\bar{\mathbf{F}}_{q^2})$.

LEMMA 4.6. *Let $P \in \mathcal{X}$. If t is a local parameter of $\mathcal{X}$ at P, then*

$$v_P(R_{M-1}) = v_P(\mathcal{W}(f_0,\ldots,f_{M-1})).$$

Proof. By [21, p. 6],

$$v_P(R_{M-1}) = v_P(\mathcal{W}(f_0,\ldots,f_{M-1})) + (\varepsilon_0+\varepsilon_1+\cdots\varepsilon_{M-1})v_P(dt) + M\bar{e}_P\,,$$

where $\bar{e}_P := -\min\{v_P(f_0),\ldots,v_P(f_{M-1})\}$. Actually, $\bar{e}_P = 0$. In fact, $\bar{e}_P > 0$ together with $e_P = 0$ would imply that the point $U_M := (0:\ldots:0:1)$ lies on $\mathcal{Y}$ but this contradicts (4.1). Since t is a local parameter at P, we also have $v_P(dt) = 0$, and the claim follows. □

The following result will play a crucial role in the sequel.

https://doi.org/10.1023/A:1017553432375 Published online by Cambridge University Press

LEMMA 4.7.

$$v_P(f_0 D_t^q f_0^q + \ldots + f_M D_t^q f_M^q) = \begin{cases} 1 & \text{when } P \in \mathcal{X}(\mathbf{F}_{q^2}), \\ 0 & \text{when } P \notin \mathcal{X}(\mathbf{F}_{q^2}). \end{cases}$$

Proof. From the proof of Lemma 4.2 we obtain the following result. For any point $P \in \mathcal{X}$,

- $P \notin \mathcal{X}(\mathbf{F}_{q^2})$ if and only if $\sum_{i=0}^{M} a_{i,1}^q a_{M,1} \neq 0$,
- $P \in \mathcal{X}(\mathbf{F}_{q^2})$ if and only if $\sum_{i=0}^{M} a_{i,1}^q a_{M,1} = 0$ but $\sum_{i=0}^{M} a_{i,1}^{q+1} \neq 0$.

On the other hand,

$$f_0 D_t^q f_0^q + \ldots + f_M D_t^q f_M^q = \left(\sum_{j=0}^{\infty} a_{0,j} t^j\right)(a_{0,1}^q + t^q[\ldots]) + \cdots + \left(\sum_{j=0}^{\infty} a_{M,j} t^j\right) \times \\ \times (a_{M,1}^q + t^q[\ldots]).$$

Hence

- $v_P(f_0 D_t^q f_0^q + \ldots + f_M D_t^q f_M^q) = 0$ if and only if $\sum a_{i,0} a_{i,1}^q \neq 0$.
- $v_P(f_0 D_t^q f_0^q + \ldots + f_M D_t^q f_M^q) = 1$ if and only if $\sum a_{i,0} a_{i,1}^q = 0$ but $\sum a_{i,1}^{q+1} \neq 0$.

Now, comparison with the previous result proves Lemma 4.7. □

Now we are in a position to finish the proof of Theorem 4.1. By [21, p. 6],

$$\sum v_P(R_M) = (\varepsilon_0 + \varepsilon_1 + \cdots \varepsilon_M)(2g-2) + (M+1)(q+1)$$

and

$$\sum v_P(R_{M-1}) = (\varepsilon_0 + \varepsilon_1 + \cdots \varepsilon_{M-1})(2g-2) + M(q+1).$$

Hence $\sum(v_P(R_M) - v_P(R_{M-1})) = q(2g-2) + q + 1$. Lemmas 4.4, 4.5, 4.6, and 4.7 together with $\sum v_P(f_M) = q+1$ give Theorem 4.1.

5. Examples

We will show how each of the known examples of maximal curves with $\deg(\mathcal{D}) = 3$ can be embedded in a non-degenerate Hermitian variety of $\mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$. In this way we obtain an independent proof of the maximality of these curves.

EXAMPLE 5.1 ([4, Thm. 2.1.(IV)(2)]). Let $q \equiv 2 \pmod 3$, and fix a primitive third root of unity $\varepsilon \in \mathbf{F}_{q^2}$. For $i = 0, 1, 2$, let $\mathcal{C}_i$ be a projective, geometrically irreducible, non-singular, algebraic curve defined over $\mathbf{F}_{q^2}$ whose function field over $\mathbf{F}_{q^2}$ is generated by x and y satisfying the irreducible polynomial relation

$$\varepsilon^i x^{(q+1)/3} + \varepsilon^{2i} x^{2(q+1)/3} + y^{q+1} = 0\,.$$

https://doi.org/10.1023/A:1017553432375 Published online by Cambridge University Press

Let

$$f_0 := x, f_1 := x^2, f_2 := y^3, f_3 := xy$$

be the coordinate functions of a morphism $\pi : \mathcal{C}_i \to \mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$. Note that these three curves $\pi(\mathcal{C}_i)$ are pairwise $\mathbf{F}_{q^2}$-projectively equivalent in $\mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$. In fact, the linear transformation induced by the matrix

$$T_4^{(i)} = \begin{bmatrix} \varepsilon^i & 0 & 0 & 0 \\ 0 & \varepsilon^{2i} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \varepsilon^i \end{bmatrix}$$

maps $\pi(\mathcal{C}_0)$ to $\pi(\mathcal{C}_i)$. We show that $\pi(\mathcal{C}_i)$ is a non-singular algebraic curve defined over $\mathbf{F}_{q^2}$ of degree $q+1$ and contained in the non-degenerate Hermitian surface $\mathcal{H}_3$ of equation $X_0^{q+1} + X_1^{q+1} + X_2^{q+1} + X_3^{q+1} = 0$. To do this we start with the relation in $\mathbf{F}_{q^2}[X, Y]$:

$$(X^{(q+1)/3} + X^{2(q+1)/3} + Y^{q+1})(\varepsilon X^{(q+1)/3} + \varepsilon^2 X^{2(q+1)/3} + Y^{q+1})$$

$$(\varepsilon^2 X^{(q+1)/3} + \varepsilon X^{2(q+1)/3} + Y^{q+1}) = X^{q+1} + X^{2(q+1)} + Y^{3(q+1)} - 3X^{q+1}Y^{q+1}$$

which is just a special case of the classical identity

$$a^3 + b^3 + c^3 - 3abc = (a + b + c)(a + \varepsilon b + \varepsilon^2 c)(a + \varepsilon^2 b + \varepsilon c).$$

This yields $x^{q+1} + x^{2(q+1)} + y^{3(q+1)} - 3x^{q+1}y^{q+1} = 0$ and thus, $f_0^{q+1} + f_1^{q+1} + f_2^{q+1} - 3f_3^{q+1} = 0$. This shows that $\pi(\mathcal{C}_i)$ lies on the non-degenerate Hermitian variety $\mathcal{H}_3$, up to the projective transformation $(X_0 : X_1 : X_2 : X_3) \mapsto (X_0 : X_1 : X_2 : wX_3)$ with $w^{q+1} = -3$. Furthermore, $\pi(\mathcal{C}_i)$ is contained in the cubic surface Σ_3 of $P^3(\bar{\mathbf{F}}_{q^2})$ of equation $X_3^3 + w^3 X_0 X_1 X_2 = 0$. More precisely, the intersection curve of $\mathcal{H}_3$ and Σ_3 splits into the above three pairwise projectively equivalent curves, namely $\pi(\mathcal{C}_0)$, $\pi(\mathcal{C}_1)$, and $\pi(\mathcal{C}_2)$, each of degree $q+1$. By Theorem 0.3, $\pi(\mathcal{C}_i)$ is a non-singular maximal curve defined over $\mathbf{F}_{q^2}$. According to [4, Thm. 2.1.(IV)(2)], its genus is equal to $(q^2 - q + 4)/6$.

EXAMPLE 5.2 ([3, Section 6]). A similar but non-isomorphic example is given in [3]. Again, assume that $q \equiv 2 \pmod 3$, and fix a primitive third root of unity $\varepsilon \in \mathbf{F}_{q^2}$. For $i = 0, 1, 2$, let $\mathcal{C}_i$ be curves as in Example 5.1 whose function field over $\mathbf{F}_{q^2}$ is generated by x and y satisfying the irreducible polynomial relation

$$\varepsilon^i y x^{(q-2)/3} + y^q + \varepsilon^{2i} x^{(2q-1)/3} = 0\,.$$

Let

$$f_0 := x,\ f_1 := x^2,\ f_2 := y^3,\ f_3 := -3xy$$

https://doi.org/10.1023/A:1017553432375 Published online by Cambridge University Press

be the coordinate functions of a morphism $\pi : \mathcal{C}_i \to \mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$. Note that these three curves $\pi(\mathcal{C}_i)$ are pairwise $\mathbf{F}_{q^2}$-projectively equivalent in $\mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$. In fact, the linear transformation induced by the matrix $T_4^{(i)}$ in Example 5.1 maps $\pi(\mathcal{C}_0)$ to $\pi(\mathcal{C}_i)$.

We show that $\pi(\mathcal{C}_i)$ is a non-singular algebraic curve defined over $\mathbf{F}_{q^2}$ of degree $q+1$ and contained in the non-degenerate Hermitian surface $\mathcal{H}_3$ of equation $X_0^{q+1} + X_1^{q+1} + X_2^{q+1} + X_3^{q+1} = 0$. As in Example 5.1 we start with the relation in $\mathbf{F}_{q^2}[X, Y]$:

$$(YX^{\frac{q-2}{3}} + Y^q + X^{\frac{2q-1}{3}})(\varepsilon YX^{\frac{q-2}{3}} + Y^q + \varepsilon^2 X^{\frac{2q-1}{3}})(\varepsilon^2 YX^{\frac{q-2}{3}} + Y^q + \varepsilon X^{\frac{2q-1}{3}})$$
$$= Y^3X^{q-2} + Y^{3q} + X^{2q-1} - 3X^{q-1}Y^{q+1}.$$

This implies $y^3x^{q-2} + y^{3q} + x^{2q-1} - 3x^{q-1}y^{q+1} = 0$ so that $y^3x^q + y^{3q+2} + x^{2q+1} - 3x^{q+1}y^{q+1} = 0$. Hence $f_2f_0^q + f_2^q f_1 + f_1^q f_0 - 3f_3^{q+1} = 0$ and this shows that $\pi(\mathcal{C}_i)$ lies on the surface Σ_{q+1} of equation $X_0^qX_1 + X_1^qX_2 + X_2^qX_0 - 3X_3^{q+1} = 0$. Furthermore, $\pi(\mathcal{C}_i)$ is contained in the cubic surface Σ_3 of $P^3(\bar{\mathbf{F}}_{q^2})$ of equation $X_3^3 + 27X_0X_1X_2 = 0$. More precisely, the intersection curve of Σ_{q+1} and Σ_3 splits into the above three pairwise projectively equivalent curves, namely $\pi(\mathcal{C}_0)$, $\pi(\mathcal{C}_1)$, and $\pi(\mathcal{C}_2)$, each of degree $q+1$.

To prove that Σ_{q+1} is projectively equivalent to $\mathcal{H}_3$, we use the same argument employed in [3]. Choose a root a of the polynomial $p(X) := X^{q+1} + X + 1$. Then $a^{q^2+q+1} = 1$, and hence $a \in \mathbf{F}_{q^3}$. By [3, Lemma 4], $a^{q+1} + a^{q^2+q+1} + a = 0$ and $a^{q^2+q+2} + a^{q+1} + 1 = 0$, but $a^{q+2} + a^{q^2+1} + a^q \neq 0$ as $(a^{q+2} + a^{q^2+1} + a^q)^{q-1} = a^{-1}$. Furthermore, the matrix

$$M_3 = \begin{bmatrix} a & 1 & a^{q^2+1} \\ a^{q^2+1} & a & 1 \\ 1 & a^{q^2+1} & a \end{bmatrix}$$

is non-singular. Also, choose an element $\mu \in \mathbf{F}_q$ satisfying $-3\mu^{q+1} = a^{q^3+q+1} + a^{q^2+1} + a^q$, and define κ as the projective linear transformation $\kappa : P^3(\bar{\mathbf{F}}_q) \to P^3(\bar{\mathbf{F}}_q)$ induced by the non-singular matrix

$$M_4 = \begin{bmatrix} a & 1 & a^{q^2+1} & 0 \\ a^{q^2+1} & a & 1 & 0 \\ 1 & a^{q^2+1} & a & 0 \\ 0 & 0 & 0 & -\mu \end{bmatrix}.$$

A straightforward computation shows that κ^{-1} maps Σ_{q+1} to $\mathcal{H}_3$, and Σ_3 to the cubic surface $\bar{\Sigma}_3$ of equation

$$(X_0^3 + X_1^3 + X_2^3) + \mathrm{Tr}[a^{q+1}](X_0^2X_1 + X_1^2X_2 + X_2^2X_0) +$$
$$+ \mathrm{Tr}[a](X_0^2X_2 + X_1^2X_0 + X_2^2X_1) + (3 + \mathrm{Tr}[a^{q-1}])X_0X_1X_2 - a^{q-1}\mu^3X_3^3$$
$$= 0$$

where $\mathrm{Tr}[u] := u + u^q + u^{q^2}$ is the trace of $u \in \mathbf{F}_{q^3}$ over $\mathbf{F}_q$. Furthermore $a^{q-1}\mu^3 \in \mathbf{F}_{q^2}$, and this shows that $\bar{\Sigma}_3$ is actually defined over $\mathbf{F}_{q^2}$. Now, $\pi(\mathcal{C}_i)$ is mapped under κ^{-1} to

https://doi.org/10.1023/A:1017553432375 Published online by Cambridge University Press

a projectively irreducible algebraic curve of degree $q+1$ defined over $\mathbf{F}_{q^2}$ and contained in $\mathcal{H}_3$. By Theorem 0.3, $\kappa^{-1}(\mathcal{C}_i)$ is a non-singular maximal curve defined over $\mathbf{F}_{q^2}$. By [3, Lemma 6.1.(5)], its genus is equal to $(q^2-q-2)/6$.

EXAMPLE 5.3 ([6]). Let q be odd and for $i=1,2$, let $\mathcal{C}_i(\mathbf{F}_{q^2})$ be curves as in Example 5.1 whose function field over $\mathbf{F}_{q^2}$ is generated by x and y such that

$$y^q + y + (-1)^i x^{(q+1)/2} = 0\,.$$

The functions

$$f_0 := 1, f_1 := x, f_2 := y, f_3 := y^2$$

define a morphism $\pi : \mathcal{C}_i \to \mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$. The resulting curves $\pi(\mathcal{C}_i)$ are projectively equivalent, since the linear transformation induced by the matrix

$$T_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \varepsilon & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

with $\varepsilon^{(q+1)/2} = -1$, maps $\pi_0(\mathcal{C}_0)$ to $\pi(\mathcal{C}_1)$. The polynomial relation

$$(Y^q + Y - X^{(q+1)/2})(Y^q + Y + X^{(q+1)/2}) = Y^{2q} + 2Y^{q+1} + Y^2 - X^{q+1}$$

implies that $y^{2q} + 2y^{q+1} + y^2 - x^{q+1} = 0$ and so that $f_3^q + f_3 + 2f_2^{q+1} - f_1^{q+1} = 0$. This proves that $\pi(\mathcal{C}_i)$ lies on the surface Σ of equation $X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0$ which is actually a non-degenerate Hermitian variety of $\mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$. Also, $\mathcal{C}_i$ lies on the quadratic cone K of equation $X_2^2 - X_0 X_3 = 0$, and hence the intersection of Σ and K splits into the curves $\pi(\mathcal{C}_0)$ and $\pi(\mathcal{C}_1)$. By Theorem 0.3, $\pi(\mathcal{C}_i)$ is a non-singular maximal curve defined over $\mathbf{F}_{q^2}$. Its genus is equal to $(q-1)^2/4$, according to [6].

EXAMPLE 5.4 ([1]). Let $q = 2^t$, and put $\mathrm{Tr}[Y] := Y + Y^2 + \ldots + Y^{q/2}$. For $i = 0, 1 \in \mathbf{F}_2 \subseteq \mathbf{F}_{q^2}$, let $\mathcal{C}_i$ be curves as in Example 5.1 whose function field over $\mathbf{F}_{q^2}$ is generated by x and y such that

$$\mathrm{Tr}[y] + x^{q+1} + i = 0.$$

Let $\pi : \mathcal{C}_i \to \mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$ be given by the coordinate functions

$$f_0 := 1, f_1 := x, f_2 := y, f_3 := x^2.$$

Since

$$(\mathrm{Tr}[Y] + X^{q+1}) + (\mathrm{Tr}[Y] + X^{q+1} + 1) = Y^q + Y + X^{q+1} + X^{2q+2},$$

we have $y^q + y + x^{q+1} + x^{2q+2} = 0$. This implies that $\pi(\mathcal{C}_i)$ lies on the non-degenerate Hermitian variety H of equation $X_2^q X_0 + X_2 X_0^q + X_1^{q+1} + X_3^{q+1} = 0$. Furthermore,

https://doi.org/10.1023/A:1017553432375 Published online by Cambridge University Press

the quadratic cone K of equation $X_3X_0 = X_1^2$ also contains $\pi(\mathcal{C}_i)$. Hence $H \cap K$ splits into $\pi(\mathcal{C}_0)$ and $\pi(\mathcal{C}_1)$. Note that $\pi(\mathcal{C}_0)$ and $\pi(\mathcal{C}_1)$ are projectively equivalent curves in $\mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$, and hence both have degree $q+1$. Again, by Theorem 0.3, $\pi(\mathcal{C}_i)$ is a non-singular maximal curve defined over $\mathbf{F}_{q^2}$. Its genus is equal to $q(q-2)/4$.

Remark 5.5. Let $\mathcal{X}$ be a $\mathbf{F}_{q^2}$-maximal curve with $\dim(\mathcal{D}) = 3$. Suppose that $\mathcal{X}$ admits a plane model with equation $Y^d = f(X)$, where $f(X) \in \mathbf{F}_{q^2}[X]$ is assumed to have all its roots in $\mathbf{F}_{q^2}$, and $f(0) = 0$. Furthermore, we assume that d is coprime to $\ell := \deg(f)$, $d, \ell \leqslant q+1$, and that either $2d \leqslant q+1$ or $2\ell \leqslant q+1$. Then $\mathcal{X}$ turns out to be $\mathbf{F}_{q^2}$-isomorphic to either to (any) one of the curves in Example 5.3 or to (any) one of the curves in Example 5.4. This can be shown by using previous results from [6] and [1]. Here we give a independent proof via Theorem 3.4.

To do this, we note at first that $\gcd(d, \ell) = 1$ implies the existence of just one point $P_0 \in \mathcal{X}(\mathbf{F}_{q^2})$ lying over $x = \infty$. Moreover, $\mathrm{div}_\infty(x) = dP_0$ and $\mathrm{div}_\infty(y) = \ell P_0$. Now, by $\dim(\mathcal{D}) = 3$, the second and third non-negative elements of the Weierstrass semigroup at P_0 are q and $q+1$, respectively. Hence

$$(d, \ell) \in \{(q+1, q/2), (q, (q+1)/2), (q/2, q+1), ((q+1)/2, q)\}.$$

Then we have a $\mathbf{F}_{q^2}$-morphism $\pi = (f_0 : f_1 : f_2 : f_3) : \mathcal{X} \to \mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$. By Theorem 3.4, π satisfies a relation of type

$$\sum_{0 \leqslant i,j \leqslant 3} u_{i,j} f_i f_j^q = 0, \tag{5.1}$$

where $u_{i,j} = u_{j,i}^q$ and $u_{i,j} \in \mathbf{F}_{q^2}$, that is $U = \{u_{i,j}\}$ is a 4×4 non-trivial Hermitian matrix with entries in $\mathbf{F}_{q^2}$. For $(d, \ell) = (q+1, q/2)$ (resp. $((q+1)/2, q)$), we have $\pi = (1 : y : y^2 : x)$ (resp. $(1 : x : y : x^2)$) and, after some computations, from Equation (5.1) one finds that $f(X) = X^{q/2} + X^{q/4} + \ldots + X^2 + X$ (resp. $f(X) = X^q + X$).

For $(d, \ell) = (q, (q+1)/2)$ (resp. $(q/2, q+1)$), we have $\pi = (1 : y : x : y^2)$ (resp. $(1 : x : x^2 : y)$), but no Hermitian matrix U exists such that Equation (5.1) holds.

EXAMPLE 5.6 ([10]). Let $q = 3^t$, and put $\mathrm{Tr}[Y] := Y + Y^3 + \ldots + Y^{q/3}$. For $i = 0, 1, 2 \in \mathbf{F}_3 \subseteq \mathbf{F}_{q^2}$, let $\mathcal{C}_i$ be curves as in Example 5.1 whose function field over $\mathbf{F}_{q^2}$ is generated by x and y such that

$$\mathrm{Tr}[y]^2 - x^q - x + i(\mathrm{Tr}[y] + i) = 0.$$

Since
$(\mathrm{Tr}[Y]^2 + X^q - X)(\mathrm{Tr}[Y]^2 - X^q - X + \mathrm{Tr}[Y] + 1)(\mathrm{Tr}[Y]^2 - X^q - X - \mathrm{Tr}[Y] + 1) = (X^q + X)(X^q + X - 1)^2 - (Y^q - Y)^2$, we have

$$(x^3 + x^2 - y^2 + x)^q + (x^3 + x^2 - y^2 + x) - x^{q+1} - y^{q+1} = 0.$$

Let $\pi = \mathcal{C}_i \to \mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$ be given by the coordinate functions $f_0 := 1$, $f_1 := x$, $f_2 := y$, $f_3 := x^3 + x^2 - y^2 + x$. It can be checked that these three curves are pairwise

https://doi.org/10.1023/A:1017553432375 Published online by Cambridge University Press

projectively equivalent in $\mathbf{P}^3(\mathbf{F}_{q^2})$. From the equation above, $\pi(\mathcal{C}_i)$ lies on the non-degenerate Hermitian variety of equation $X_0X_3^q + X_0^qX_3 - X_1^{q+1} - X_2^{q+1} = 0$. Furthermore, the cubic surface of equation $X_3X_0^2 - X_1^3 + X_1^2X_0 + X_2^2X_0 - X_1X_0^2$ also contains $\pi(\mathcal{C}_i)$. It turns out that $\pi(\mathcal{C}_i)$ has degree $q+1$, and Theorem 0.3 ensures that $\pi(\mathcal{C}_i)$ is a non-singular maximal curve defined over $\mathbf{F}_{q^2}$. Its genus is equal to $q(q-1)/6$.

Remark 5.7. In all the above examples $\mathcal{X}$ lies not only on a non-degenerate Hermitian surface but also on a cubic surface. This is related to a classical result of Halphen on reduced and irreducible complex algebraic curves in $\mathbf{P}^3$ not lying on a quadratic surface which states that the degree d and the genus g of such a curve satisfy the following inequality:

$$g \leqslant \pi_1(d,3) = \begin{cases} d^2/6 - d/2 + 1 & \text{for } d \equiv 0 \bmod 3; \\ d^2/6 - d/2 + 1/3 & \text{for } d \not\equiv 0 \bmod 3. \end{cases}$$

A rigorous proof of the Halphen theorem and its extension to higher-dimensional spaces is found in the book [5]. Rathmann [18] (see also [2]) pointed out that the proof also works in positive characteristic apart from some possible exceptional cases related to the monodromy group of the curve.

Acknowledgement

This research was performed within the activity of GNSAGA of the Italian CNR, with the financial support of the Italian Ministry MURST, project "Srutture algebriche, geometriche, combinatoria e loro applicazioni", and of the NATO grant 970185. The present paper was partly written while the second author was visiting ICTP-Italy (July–August 1999), as a Regular Associate, and the University of Basilicata at Potenza-Italy (July 1999).

References

1. Abdón, M. and Torres, F.: On maximal curves in characteristic two, *Manuscripta Math.* **99** (1999), 39–53.
2. Ballico E. and Cossidente, A: On the generic hyperplane section of curves in positive characteristic, *J. Pure Appl. Algebra* **102** (1995), 243–250.
3. Cossidente, A., Korchmáros, G. and Torres, F.: On curves covered by the Hermitian curve, *J. Algebra* **216** (1999), 56–76.
4. Cossidente, A., Korchmáros, G. and Torres, F.: Curves of large genus covered by the Hermitian curve, *Comm. Algebra* **28** (10) (2000), 4707–4728.
5. Eisenbud, D. and Harris, J.: *Curves in Projective Space*, Les Presses de l'Université de Montréal, Montréal, 1982.
6. Fuhrmann, R., Garcia, A. and Torres, F.: On maximal curves, *J. Number Theory* **67** (1997), 29–51.
7. Fuhrmann, R. and Torres, F.: On Weierstrass points and optimal curves, *Rend. Circ. Mat. Palermo* **51** (1998), 25–46.

8. Garcia, A. and Voloch, J. F.: Wronskians and independence in fields of prime characteristic, *Manuscripta Math.* **59** (1987), 457–469.
9. Garcia, A. and Voloch, J. F.: Duality for projective curves, *Bol. Soc. Brazil. Mat (N.S.)* **21** (1991), 159–175.
10. van der Geer, G. and van der Vlugt, M.: Generalized Reed–Müller codes and curves with many points, preprint.
11. Hefez, A.: Non-reflexive curves, *Compositio Math.* **69** (1989), 3–35.
12. Hefez, A. and Kakuta, N.: Tangent envelopes of higher order duals of projective curves, *Rend. Circ. Mat. Palermo, Suppl.* **51** (1998), 47–56.
13. Hefez, A. and Voloch, J. F.: Frobenius non classical curves, *Arch. Math.* **54** (1990), 263–273.
14. Hirschfeld, J. W. P. and Thas, J. A.: *General Galois Geometries*, Oxford University Press, Oxford, 1991.
15. Homma, M.: Space curves with degenerate strict duals, *Comm. Algebra* **20** (1992), 867–874.
16. Kaji, H.: Strangeness of higher order space curves, *Comm. Algebra* **20** (1992), 1535–1548.
17. Lang, S.: *Abelian Varieties*, Interscience, New York, 1959.
18. Rathmann, J.: The uniform position principle for curves in characteristic *p*, *Math. Ann.* **276** (1987), 565–579.
19. Rück H. G. and Stichtenoth, H.: A characterization of Hermitian function fields over finite fields, *J. Reine Angew. Math.* **457** (1994), 185–188.
20. Segre, B.: Forme e geometrie Hermitiane, con particolare riguardo al caso finito, *Ann. Mat. Pura Appl.* **70** (1965), 1–201.
21. Stöhr, K. O. and Voloch, J. F.: Weierstrass points and curves over finite fields, *Proc. London Math. Soc.* **52** (1986), 1–19.
22. Tate, J.: Endomorphisms of abelian varieties over finite fields, *Invent. Math.* **2** (1966), 134–144.