ON MAXIMAL CURVES

RAINER FUHRMANN, ARNALDO GARCIA, AND FERNANDO TORRES

Abstract. We study arithmetical and geometrical properties of maximal curves, that is, curves defined over the finite field $\mathbb{F}_{q^2}$ whose number of $\mathbb{F}_{q^2}$-rational points reaches the Hasse-Weil upper bound. Under a hypothesis on non-gaps at a rational point, we prove that maximal curves are $\mathbb{F}_{q^2}$-isomorphic to $y^q + y = x^m$, for some $m \in \mathbb{Z}^+$. As a consequence we show that a maximal curve of genus $g = (q - 1)^2/4$ is $\mathbb{F}_{q^2}$-isomorphic to the curve $y^q + y = x^{(q+1)/2}$.

0. Introduction

The interest on curves over finite fields was renewed after Goppa [Go] showed their applications to Coding Theory. One of the main features of linear codes arising from curves is the fact that one can state a lower bound for their minimum distance. This lower bound is meaningful only if the curve has many rational points. The subject of this paper is the study of maximal curves.

Let $X$ be a projective, geometrically irreducible and non-singular algebraic curve defined over the finite field $\mathbb{F}_\ell$ with $\ell$ elements. A celebrated theorem of Weil states that:

$$\# X(\mathbb{F}_\ell) \leq \ell + 1 + 2g\sqrt{\ell},$$

where $X(\mathbb{F}_\ell)$ denotes the set of $\mathbb{F}_\ell$-rational points of $X$ and $g$ is the genus of the curve. This bound was proved for elliptic curves by Hasse.

The curve $X$ is called maximal over $\mathbb{F}_\ell$ (in this case, $\ell$ must be a square; say $\ell = q^2$) if it attains the Hasse-Weil upper bound; that is,

$$\# X(\mathbb{F}_{q^2}) = q^2 + 1 + 2gq.$$ 

Ihara [Ih] shows that the genus of a maximal curve over $\mathbb{F}_{q^2}$ satisfies:

$$g \leq (q - 1)q/2.$$ 

Rück and Stichtenoth [R-St] show that the Hermitian curve (that is, the curve given by $y^q + y = x^{q+1}$) is the unique (up to $\mathbb{F}_{q^2}$-isomorphisms) maximal curve over $\mathbb{F}_{q^2}$ having genus $g = (q - 1)q/2$.

It is also known that the genus of maximal curves over $\mathbb{F}_{q^2}$ satisfies (see [F-T] and the remark after Theorem 1.4 here):

$$g \leq (q - 1)^2/4 \quad \text{or} \quad g = (q - 1)q/2.$$ 

The Hermitian curve is a particular case of the following maximal curves over $\mathbb{F}_{q^2}$:

$$y^q + y = x^m, \text{ with } m \text{ being a divisor of } (q + 1).$$ 

Note that the genus of the above curve is given by $g = (q - 1)(m - 1)/2.$
In Section 1 we derive properties of maximal curves. The main tools being the application to the linear system $D = [(q + 1)P_0]$, $P_0$ a rational point, of Stöhr-Voloch’s approach [S-V] to the Hasse-Weil bound via Weierstrass Point Theory; and Castelnuovo’s genus bound for curves in projective spaces: [C], [ACGH, p. 116], [Ra, Corollary 2.8]. A key result here is the fact that for any point $P$ of the curve, the divisor $qP + F_X(P)$ is linearly equivalent to $D$ (Corollary 1.2). This is a consequence of the particular fashion of the characteristic polynomial $h(t)$ of the Frobenius endomorphism of the Jacobian of the curve, that is, $h(t)$ is a power of a linear polynomial. This property also affects the geometry of the curve. More precisely, we show that maximal curves over $\mathbb{F}_{q^2}$ of genus $g \geq q - 1$ are non-classical curves for the canonical morphism (Proposition 1.7). In some other cases one can deduce the non-classicality (for the canonical morphism) of the curve from the knowledge of $h(t)$. We will see this for the Deligne-Lusztig curve associated to the Suzuki group and to the Ree group (Proposition 1.8). The non-classicality of the curve corresponding to the Suzuki group was already proved in [G-St]. Our proof is different. It seems that the curve corresponding to the Ree group provides a new example of a non-classical curve.

In Section 2, we characterize the curves

$$y^q + y = x^m, \ m \text{ being a divisor of } (q + 1),$$

among the maximal curves over $\mathbb{F}_{q^2}$. This characterization being in terms of non-gaps at a rational point (Theorem 2.3). Finally in Section 3, applying the results of Section 2, we show that

$$y^q + y = x^{(q+1)/2}, \text{ with } q \text{ odd},$$

is the unique (up to $\mathbb{F}_{q^2}$-isomorphisms) maximal curve over $\mathbb{F}_{q^2}$ with $g = (q - 1)^2/4$.

1. Maximal curves

Throughout this paper we use the following notation:

- By a curve we mean a projective, geometrically irreducible, non-singular algebraic curve defined over a finite field.
- Let $k$ denote the finite field with $q^2$ elements, where $q$ is a power of a prime $p$. Let $k$ denote its algebraic closure.
- The symbol $X(k)$ (resp. $k(X)$) stands for the set of $k$-rational points (resp. for the field of $k$-rational functions) of a curve $X$ defined over $k$.
- If $x \in k(X)$, then $\text{div}(x)$ (resp. $\text{div}_\infty(x)$) denotes the divisor (resp. the pole divisor) of the function $x$.
- Let $P$ be a point of a curve. Then $\nu_P$ (resp. $H(P)$) stands for the valuation (resp. for the Weierstrass non-gap semigroup) associated to $P$. We denote by $m_i(P)$ the $i$th non-gap at $P$.
- Let $D$ be a divisor on $X$ and $P \in X$. We denote by $\deg(D)$ the degree of $D$, by $\text{Supp}(D)$ the support of $D$, and by $\nu_P(D)$ the coefficient of $P$ in $D$. If $D$ is a $k$-divisor, we set

$$L(D) := \{ f \in k(X) \mid \text{div}(f) + D \geq 0 \}, \quad \ell(D) := \dim_k L(D).$$

- The symbol “$\sim$” denotes linear equivalence of divisors.
- The symbol $g_d^r$ stands for a linear system of projective dimension $r$ and degree $d$. 

We first review some facts from Weierstrass Point Theory (see [Sch] and [S-V]).

**Weierstrass points.** Let \(X\) be a curve of genus \(g\), and \(D = g^d\) be a base-point-free \(k\)-linear system on \(X\). Then associated to a point \(P \in X\) we have the Hermitian \(P\)-invariants \(j_0(P) = 0 < j_1(P) < \ldots < j_r(P) \leq d\) of \(D\) (also called the \((D, P)\)-orders). This sequence is the same for all but finitely many points. These finitely many points \(P\), where exceptional \((D, P)\)-orders occur, are called the \(D\)-Weierstrass points of \(X\). The Weierstrass points of the curve are those exceptional points obtained from the canonical linear system.

A curve is called *non-classical* if the generic order sequence (for the canonical linear system) is different from \(\{0, 1, \ldots, g - 1\}\).

Associated to the linear system \(D\) there exists a divisor \(R\) supporting exactly the \(D\)-Weierstrass points. Let \(\epsilon_0 < \epsilon_1 < \ldots < \epsilon_r\) denote the \((D, Q)\)-orders for a generic point \(Q \in X\). Then we have

\[
\epsilon_i \leq j_i(P), \quad \text{for each } i = 0, 1, 2, \ldots, r \text{ and for any point } P,
\]

and also that

\[
\deg(R) = (\epsilon_1 + \ldots + \epsilon_r)(2g - 2) + (r + 1)d.
\]

Associated to \(D\) we also have a divisor \(S\) whose support contains the set \(X(k)\) of \(k\)-rational points on \(X\). Its degree is given by

\[
\deg(S) = (\nu_1 + \ldots + \nu_{r-1})(2g - 2) + (q^2 + r)d,
\]

where the \(\nu_i\)'s form a subsequence of the \(\epsilon_i\)'s. More precisely, there exists an integer \(I\) with \(0 < I \leq r\) such that \(\nu_i = \epsilon_i\) for \(i < I\), and \(\nu_i = \epsilon_{i+1}\) otherwise. Moreover, for \(P \in X(k)\),

\[
\nu_i(S) \geq \sum_{i=1}^{r}(j_i(P) - \nu_i - 1), \quad \text{and} \quad \nu_i \leq j_i + 1(P) - j_1(P), \quad \text{for each } i = 1, 2, \ldots, r.
\]

**Maximal curves.** We study some arithmetical and geometrical properties of maximal curves. To begin with we recall the following basic result concerning Jacobians. Let \(X\) be a curve, \(\text{Fr}_J\) the Frobenius endomorphism (relative to the base field) of the Jacobian \(J\) of \(X\), and \(h(t)\) the characteristic polynomial of \(\text{Fr}_J\). Let \(h(t) = \prod_{i=1}^{T} h_i^c(t)\) be the factorization over \(\mathbb{Z}[t]\) of \(h(t)\). Then

\[
\prod_{i=1}^{T} h_i(\text{Fr}_J) = 0 \quad \text{on } J.
\]

This follows from the semisimplicity of \(\text{Fr}_J\) and the fact that the representation of endomorphisms of \(\text{Fr}_J\) on the Tate module is faithful (cf. [13], Thm. 2, [1], VI, §3]).

In the case of a maximal curve over \(k = \mathbb{F}_{q^2}\), \(h(t) = (t + q)^2g\). Therefore from (1.4) we obtain the following result, which is contained in the proof of [R-StI, Lemma 1].

**Lemma 1.1.** The Frobenius map \(\text{Fr}_J\) (relative to \(k\)) of the Jacobian \(J\) of a maximal curve over \(k\) acts as multiplication by \((-q)\) on \(J\).

Let \(X\) be a maximal curve over \(k\). Fix \(P_0 \in X(k)\), and consider the map \(f = f^{P_0} : X \rightarrow J\) given by \(P \mapsto [P - P_0]\). We have

\[
f \circ \text{Fr} = \text{Fr}_J \circ f,
\]

where \(\text{Fr}\) denotes the Frobenius morphism on \(X\) relative to \(k\). Hence, from (1.3) and Lemma 1.1, we get:
Corollary 1.2. For a maximal curve $X$ over $k$, it holds
\[ \text{Fr}(P) + qP \sim (q + 1)P_0, \text{ for all points } P \text{ on } X. \]

It follows then immediately that

Corollary 1.3. ([K-S, Lemma 1]) Let $X$ be a maximal curve over $k$, $P_0, P_1 \in X(k)$. Then $(q + 1)P_1 \sim (q + 1)P_0$.

Consider now the linear system $D = g_{q+1}^n := [(q + 1)P_0]$. Corollary 1.2 says that $D$ is a $k$-invariant of the curve. In particular, its dimension $n + 1$ is independent of the choice of $P_0 \in X(k)$. Moreover from Corollary 1.2 we have that $q + 1 \in H(P_0)$; i.e., $(q + 1)$ is a non-gap at a rational point, and hence $D$ is base-point-free. From now on the letter $D$ will always denote the linear system $|(q + 1)P_0|$. $P_0$ a rational point, $(n + 1)$ being its projective dimension, $R$ will always mean the divisor supporting exactly the $D$-Weierstrass points, and $\text{Fr}$ will always stand for the Frobenius morphism on $X$ relative to $k$.

Theorem 1.4. For a maximal curve $X$ over $k$, the $D$-orders satisfy (notations being as above):

(i) $\epsilon_{n+1} = \nu_n = q$.
(ii) $j_{n+1}(P) = q + 1$ if $P \in X(k)$, and $j_{n+1}(P) = q$ otherwise; in particular, all rational points over $k$ are $D$-Weierstrass points of $X$.
(iii) $j_1(P) = 1$ for all points $P \in X$; in particular, $\epsilon_1 = 1$.
(iv) If $n \geq 2$, then $\nu_1 = \epsilon_1 = 1$.

Proof. Statement (iii), for $P \in X(k)$, follows from (i), (ii) and the second inequality in (1.3). From Corollary 1.2 it follows the assertion (ii) and $\epsilon_{n+1} = q$. Furthermore, it also follows that $j_1(P) = 1$ for $P \notin X(k)$: in fact, let $P' \in X$ be such that Fr($P'$) = $P$; then $P + qP' = \text{Fr}(P') + qP' \sim (q + 1)P_0$.

Now we are going to prove that $\nu_n = \epsilon_{n+1}$. Let $P \in X \setminus \{P_0\}$. Corollary 1.2 says that $\pi(\text{Fr}(P))$ belongs to the osculating hyperplane at $P$, where $\pi$ stands for the morphism associated to $D$. This morphism $\pi$ can be defined by a base $\{f_0, f_1, \ldots, f_{n+1}\}$ of $L((q + 1)P_0)$. Let $x$ be a separating variable of $k(X) | k$. Then by [S-V], Prop. 1.4(c), Corollary 1.3 the rational function below is identically zero

\[
\nu_n < \ldots < \nu_1 = \{\epsilon_0 < \ldots < \epsilon_{I-1} < \epsilon_{I+1} < \ldots < \epsilon_{n+1}\}.
\]

That $\epsilon_1 = 1$ follows from statement (iii). Suppose that $\nu_1 > 1$. Since $j_1(P) = 1$ for all points of $X$, it follows from the proof of [H-V], Thm. 1 that

\[
\# X(k) = (q + 1)(q^2 - 1) - (2g - 2).
\]

From the maximality of $X$, we then conclude $2g = (q - 1) \cdot q$. 

On the other hand, $\pi$ is a birational morphism as follows from [Sti-X, Prop. 1] (see also Proposition 1.5(iv) here). Then Castelnuovo’s genus bound for curves in projective spaces applied to the morphism $\pi$ reads:

\[
2g \leq M \cdot (q - n + e) \leq \begin{cases} 
(2q - n)^2/4n, & \text{if } n \text{ is even} \\
((2q - n)^2 - 1)/4n, & \text{if } n \text{ is odd},
\end{cases}
\]

where $M$ is the integer part of $q/n$ and $e = q - M \cdot n$. We then conclude that $n = 1$ and this finishes the proof of the theorem. 

Remark. For a maximal curve $X$ with $n = 1$, we have $\nu_1 = \epsilon_2 = q > 1$. Then the proof above shows that $2g = (q - 1) \cdot q$. It then follows from [R-Sti] that the curve $X$ is $k$-isomorphic to the Hermitian curve given by $y^q + y = x^{q+1}$. Also, if $n \geq 2$ then from Castelnuovo’s formula (1.6) we get $g \leq (q - 1)^2/4$. This is the main result of [F-T].

The next proposition gives information on $\mathcal{D}$-orders and non-gaps at points of $X$.

**Proposition 1.5.** Let $X$ be a maximal curve over $k$ (notations being as before). Then:

(i) For each point $P$ on $X$, we have $\ell(qP) = n + 1$; i.e., we have the following behaviour for the non-gaps at $P$

\[
0 < m_1(P) < \cdots < m_n(P) \leq q < m_{n+1}(P).
\]

(ii) If $P$ is not rational over $k$, the numbers below are $\mathcal{D}$-orders at the point $P$

\[
0 \leq q - m_n(P) < \cdots < q - m_1(P) < q.
\]

(iii) If $P$ is rational over $k$, the numbers below are exactly the $(\mathcal{D}, P)$-orders

\[
0 < q + 1 - m_n(P) < \cdots < q + 1 - m_1(P) < q + 1.
\]

In particular, if $j$ is a $\mathcal{D}$-order at a rational point $P$ then $q + 1 - j$ is a non-gap at $P$.

(iv) If $P \in X(\mathbb{F}_{q^4}) \setminus X(k)$, then $q - 1$ is a non-gap at $P$. If $P \notin X(\mathbb{F}_{q^4})$, then $q$ is a non-gap at $P$. If $P \in X(k)$, then $q$ and $q + 1$ are non-gaps at $P$.

(v) Let $P$ be a non-Weierstrass point of $X$ (for the canonical morphism) and suppose that $n \geq 2$, then we have for the non-gaps at $P$ that $m_{n-1}(P) = q - 1$ and $m_n(P) = q$.

**Proof.** Assertion (i) follows from Corollary 1.2. Let $m(P)$ be a non-gap at a point $P$ of $X$ with $m(P) \leq q$, then by definition there exists a positive divisor $E$ disjoint from $P$ with

\[
E \sim m(P) \cdot P.
\]

Summing up to both sides of the equivalence above the divisor $(q - m(P)) \cdot P + \text{Fr}(P)$, we get

\[
E + (q - m(P)) \cdot P + \text{Fr}(P) \sim qP + \text{Fr}(P) \sim (q + 1)P_0.
\]

This proves assertions (ii) and (iii). To prove assertion (iv) we just apply (as in [Har, IV, Ex. 2.6]) the Frobenius morphism to the equivalence in Corollary 1.2 getting

\[
\text{Fr}^2(P) + (q - 1)\text{Fr}P \sim qP.
\]

The fact that $q$ and $q + 1$ are non-gaps at any rational point follows from assertion (iii) taking $j = 0$ and $j = 1$.

Now we are going to prove the last assertion (v). From assertion (iv) we know already

\[
m_n(P) = q \quad \text{and} \quad m_{n-1}(P) \leq q - 1.
\]
Suppose that $m_{n-1}(P) < (q - 1)$. It then follows from Theorem 1.4 and the assertion (ii) above that the generic order sequence for the linear system $D$ is as given below:

$$\epsilon_0 = 0 < \epsilon_1 = 1 < \epsilon_2 = q - m_{n-1}(P) < \cdots < \epsilon_n = q - m_1(P) < \epsilon_{n+1} = q.$$  

On the other hand, we have that Equation (1.1) implies

$$m_i(Q) \leq m_i(P), \text{ for each } i \text{ and each } Q \in X.$$  

Thus at a rational point $Q \in X$, it follows from assertion (iii) that:

$$v_Q(R) \geq \sum_{i=1}^{n+1} (j_i(Q) - \epsilon_i) = 1 + \sum_{i=1}^{n-1} (m_i(P) - m_i(Q) + 1) \geq n.$$  

From the maximality of $X$, Equation (1.2) and [Hö, Thm. 1], we conclude that

$$n(q^2 + 2gq + 1) \leq \deg R \leq (n + 2)\epsilon_{n+1}(g - 1) + (n + 2)(q + 1).$$  

Using that $\epsilon_{n+1} = q$, we finally have $nq^2 + gq(n-2) \leq 2$. This contradicts the assumption that $n \geq 2$. \hfill \Box

**Example 1.6.** By Theorem 1.4, we have that all rational points of the curve are $D$-Weierstrass points. However, these sets may be different from each other as the following example shows:

Let $X$ be the hyperelliptic curve defined by $x^2 + y^5 = 1$ over $\mathbb{F}_{81}$. The curve $X$ is maximal because it is covered by the Hermitian curve $x^{10} + y^{10} = 1$ (see [Sti, Example VI.4.3]). It has genus 2 and at a generic point $P$, we have $m_2(P) = 9$. Hence we have $D = |10P_0| = g_0^n$. All the canonical Weierstrass points are trivially rational points, and since $\#X(\mathbb{F}_{81}) = 118 > \# \{\text{Weierstrass points}\} = 6$, we have two possibilities for the $(D, P)$-orders at rational points, namely:

(a) If $P$ is a rational non-Weierstrass point; then its orders are $0, 1, 2, 3, 4, 5, 6, 7, 10$.

(b) If $P$ is a Weierstrass point; then its orders are $0, 1, 2, 3, 4, 5, 6, 8, 10$.

These computations follow from Proposition 1.5(iii). From the $D$-orders in (a) above, we conclude that the generic order sequence for $D$ is $0, 1, 2, 3, 4, 5, 6, 7, 9$. Hence, $\deg(R) = 164$ and $v_P(R) = 1$ (resp. $v_P(R) = 2$) if $P$ satisfies (a) (resp. (b)) above. Since $\deg R - 112 \times 1 - 6 \times 2 = 40 > 0$, we then conclude that there exist non-rational $D$-Weierstrass points. The order sequence at such points must be $0, 1, 2, 3, 4, 5, 6, 8, 9$ and so there exist 40 non-rational $D$-Weierstrass points, namely the fixed points of $\sigma \circ \text{Fr}$, where $\sigma$ denotes the hyperelliptic involution.

By Proposition 1.5(v) we have that $q - n$ is a lower bound for the genus of a maximal curve over $\mathbb{F}_{q^2}$. We are going to show that classical (for the canonical morphism) maximal curves attain such a bound.

**Proposition 1.7.** Let $X$ be a maximal curve over $k = \mathbb{F}_{q^2}$ and let $g \geq 2$ be its genus. Then

(i) If $g > q - n$ (with $n+1 = \dim D$ as before), then $X$ is non-classical for the canonical morphism. In particular, this holds for $g \geq q - 1$.

(ii) If $X$ is hyperelliptic and the characteristic is two, then $X$ has just one Weierstrass point for the canonical morphism.
Proof. (i) If \( X \) is classical, then at a generic point \( P \) of the curve \( X \) we have
\[
m_i(P) = g + i, \quad \forall i \in \mathbb{N}.
\]
On the other hand, from Proposition 1.5(iv) we have \( m_n(P) = q \). We then conclude that \( g + n = q \). Now if \( g \geq q - 1 \) and \( X \) classical, then \( n = 1 \). Therefore from the remark after Theorem 1.4 we would have \( 2g = q(q - 1) \) and so \( g = 1 \), a contradiction.

(ii) Since \( X \) is hyperelliptic, the Weierstrass points are the fixed points of the hyperelliptic involution. Let \( P, Q \) be Weierstrass points of \( X \) (they exist because the genus is bigger than one). From 2P \( \sim \) 2Q and 2 | \( q \), we get \( qP \sim qQ \). Therefore by Corollary 1.2,
\[
qQ + \Fr(Q) \sim qP + \Fr(P) \sim qQ + \Fr(P),
\]
and so \( \Fr(P) \sim \Fr(Q) \). This implies \( \Fr(P) = \Fr(Q) \), and consequently \( P = Q \). \( \square \)

Remark. Hyperelliptic maximal curves are examples of classical curves for the canonical morphism. It would be interesting to investigate the maximal curves that are both non-hyperelliptic and classical for the canonical morphism. Examples of such curves are the one of genus 3 over \( \mathbb{F}_{25} \) listed by Serre in [5, §4], and the generalizations of Serre’s example obtained by Ibukiyama [7, Thm. 1].

Another question is whether or not the condition \( g = q - n \) characterizes classical (for the canonical morphism) maximal curves.

Now we present two non-classical (for the canonical morphism) maximal curves over \( \mathbb{F}_{q^2} \) of genus \( g < q - 1 \). These are the so-called Deligne-Lusztig curves associated to the Suzuki group and to the Ree group.

**Proposition 1.8.** (I) Let \( s \in \mathbb{N}, \ r := 2^{2s+1}, \ r_0 := 2^s, \) and consider the curve \( X \) over \( \mathbb{F}_r \), defined by
\[
y^r - y = x^{r_0}(x^r - x).
\]
Then
(i) (H, H-Sti, Se) The genus of \( X \) is \( g = r_0(r - 1) \) and this curve is maximal over \( \mathbb{F}_r^2 \).
(ii) (G-Sti) The curve \( X \) is non-classical for the canonical morphism.

(II) Let \( s \in \mathbb{N}, \ r := 3^{2s+1}, \ r_0 := 3^s, \) and consider the curve \( X \) over \( \mathbb{F}_r \) defined by
\[
y^r - y = x^{r_0}(x^r - x), \quad z^r - z = x^{2r_0}(x^r - x).
\]
Then
(i) (H, H, Se) The genus of \( X \) is \( g = 3r_0(r-1)(r+r_0+1) \) and this curve is maximal over \( \mathbb{F}_{r^6} \).
(ii) The curve \( X \) is non-classical for the canonical morphism.

Proof. We first set some notations. We write \( \Fr \) for the Frobenius morphism on \( X \) relative to \( \mathbb{F}_r \) and \( h_i(t) \) for the characteristic polynomial of the Frobenius endomorphism (relative to \( \mathbb{F}_{r^6} \)) of the Jacobian of \( X \).

(I) From [H, Prop. 4.3], [H-Sti], [Se] we know that \( g = r_0(r - 1) \) and that \( h_1(t) = (t^2 + 2r_0t + r)^3 \). If \( a_1 \) and \( a_2 \) denote the roots of \( h_1(t) \), then we have \( a_1 + a_2 = -2r_0 \) and \( a_1a_2 = r \). It then follows easily that \( (a_1a_2)^4 = r^4 \) and \( a_1^4 + a_2^4 = -2r^2 \), and hence that \( h_4(t) = (t + r^2)^2g \). This shows the maximality over \( \mathbb{F}_r^2 \).

Now by (1.4) we have \( \Fr^2J + 2r_0\Fr J + r = 0 \) on \( J \) and then by (1.3) we obtain
\[
\Fr^2(P) + 2r_0\Fr(P) + rP \sim (1 + 2r_0 + r)P_0,
\]
for all \( P \in X \), \( P_0 \in X(\mathbb{F}_r) \). Now applying \( \text{Fr} \) to the equivalence above we get
\[
\text{Fr}^3(P) + (2r_0 - 1)\text{Fr}^2(P) + (r - 2r_0)\text{Fr}(P) \sim rP.
\]
Hence we conclude that \( r \in H(P) \) at a general point \( P \in X \), and since \( g \geq r \), that \( X \) is non-classical for the canonical morphism.

(II) From [1, Prop. 5.3], [1, 5] we already know the formula for the genus and that
\[
h_1(t) = (t^2 + r)^a(t^2 + 3rt + r)^b
\]
with \( a, b \in \mathbb{N} \) and \( a + b = g \). Let \( a_1, a_2 \) denote the roots of some factor of \( h_1(t) \). Then in either case we get \( a_1a_26 = r^6 \) and \( a_1^6 + a_2^6 = -2r^3 \) and hence that \( h_0(t) = (t + r^3)^2g \). This shows the maximality of \( X \) over \( \mathbb{F}_r^g \).

Finally as in the proof of item (I) we conclude that \( r^2 \in H(P) \) for a generic \( P \in X \). Since \( g \geq r^2 \) the assertion follows.

To finish this section on maximal curves, we study some properties involving the morphism \( \pi : X \to \mathbb{P}^{n+1} \) associated to the linear system \( D = [(q + 1)P_0] \).

**Proposition 1.9.** The following statements are equivalent:

(i) The morphism \( \pi \) is a closed embedding, i.e. \( X \) is \( k \)-isomorphic to \( \pi(X) \).

(ii) For all \( P \in X(\mathbb{F}_{q^f}) \), we have that \( \pi(P) \in \mathbb{P}^{n+1}(k) \iff P \in X(k) \).

(iii) For all \( P \in X(\mathbb{F}_{q^f}) \), we have that \( q \) is a non-gap at \( P \).

**Proof.** Let \( P \in X \). Since \( j_1(P) = 1 \) (cf. Theorem [1, (iii)]), we have that \( \pi(X) \) is non-singular at all branches centered at \( \pi(P) \). Thus \( \pi \) is an embedding if and only if \( \pi \) is injective.

**Claim.** We have \( \pi^{-1}(\pi(P)) \subseteq \{ P, \text{Fr}(P) \} \) and if \( \pi \) is not injective at the point \( P \), then \( P \in X(\mathbb{F}_{q^f}) \setminus X(k) \) and \( \pi(P) \in \mathbb{P}^{n+1}(k) \).

From Corollary [1, 2] it follows that \( \pi^{-1}(\pi(P)) \subseteq \{ P, \text{Fr}(P) \} \). Now if \( \pi \) is not injective at \( P \), then \( P \notin X(k) \) and, since \( P \in \pi^{-1}(\pi(Fr(P))) \subseteq \{ Fr(P), Fr^2(P) \} \), we have \( Fr^2(P) = P \), i.e. \( P \in X(\mathbb{F}_{q^f}) \setminus X(k) \). Furthermore we have \( \pi(P) = Fr(P) = Fr(\pi(P)) \), i.e. \( \pi(P) \in \mathbb{P}^{n+1}(k) \). This proves the claim above.

From this claim the equivalence (i) \( \iff \) (ii) follows immediately. As to the implication (i) \( \Rightarrow \) (iii), we know that \( \dim |Fr(P) + qP - Fr(P)| = \dim |Fr(P) + qP| - 2 \) (Corollary [1, 2] and [Har, Prop. 3.1(b)]), i.e. \( \ell((q - 1)P) = n \) and so \( q \in H(P) \), by Proposition 1.5(i).

Finally we want to conclude from (iii) that \( \pi \) is an embedding. According to the above claim it is sufficient to show that \( \pi^{-1}(\pi(P)) = \{ P \} \), for \( P \in X(\mathbb{F}_{q^f}) \setminus X(k) \). Let then \( P \in X(\mathbb{F}_{q^f}) \). Since we have \( q \in H(P) \), there is a divisor \( D \in |qP| \) with \( P \notin \text{Supp}(D) \). In particular,
\[
\text{Fr}(P) + D \sim \text{Fr}(P) + qP \sim (q + 1)P_0,
\]
and then \( \pi^{-1}(\pi(Fr(P))) \subseteq \text{Supp}(\text{Fr}(Fr(P) + D)) \). So if \( \pi^{-1}(\pi(P)) = \{ P, \text{Fr}(P) \} \), then we would have that \( P \in \text{Supp}(D) \), a contradiction. This means altogether that \( \pi \) is injective and so indeed a closed embedding.

**Remark.** Condition (iii) above is satisfied whenever \( q \geq 2g \), and in most of the well known examples of maximal curves the morphism \( \pi \) is always an embedding. Then a natural question is whether or not \( \pi \) is an embedding for an arbitrary maximal curve. We conjecture that this property is a necessary condition for a maximal curve being covered by the Hermitian curve.
Proposition 1.10. Suppose that $\pi : X \to \mathbb{P}^{n+1}$ is a closed embedding. Let $P_0 \in X(k)$ and assume furthermore that there exist $r, s \in H(P_0)$ such that all non-gaps at $P_0$ less than or equal to $q + 1$ are generated by $r$ and $s$. Then the semigroup $H(P_0)$ is generated by $r$ and $s$. In particular, the genus of $X$ is equal to $(r - 1)(s - 1)/2$.

Proof. Let $x, y \in k(X)$ with $\text{div}_\infty(x) = sP_0$ and $\text{div}_\infty(y) = rP_0$. Since we have that $q, q + 1 \in H(P_0)$, then the numbers $r$ and $s$ are coprime. Let $\pi_2 : X \to \mathbb{P}^2$, be given by $P \mapsto (1 : x(P) : y(P))$. Then the curves $X$ and $\pi_2(X)$ are birational and the image $\pi_2(X)$ is a plane curve given by an equation of the type below:

$$x^r + \beta y^s + \sum_{i+s+jr<rs} \alpha_{ij} x^i y^j = 0,$$

where $\beta, \alpha_{ij} \in k$ and $\beta \neq 0$. We are going to prove that $\pi_2(P)$ is a non-singular point of the curve $\pi_2(X)$ for all $P \neq P_0$. From this it follows that $g = (r - 1)(s - 1)/2$ and also that $H(P_0) = \langle r, s \rangle$ (see [Ful, Ch. 7], [To]).

Let $1, f_1, \ldots, f_{n+1}$ be a basis of $L((q+1)P_0)$, where $n + 1 := \dim |(q+1)P_0|$. Then there exist polynomials $F_i(T_1, T_2) \in k[T_1, T_2]$ for $i = 1, \ldots, n + 1$, such that

$$f_i = F_i(x, y), \quad \text{for} \quad i = 1, \ldots, n + 1.$$

The existence of these polynomials follows from the hypothesis on the non-gaps at $P_0$ less than or equal to $(q + 1)$.

Consider the maps $\pi_1|\{X \setminus \{P_0\} : X \setminus \{P_0\} \to \mathbb{A}^{n+1}$ given by $P \mapsto (f_1(P), \ldots, f_{n+1}(P)); \pi_2|\{X \setminus \{P_0\} : X \setminus \{P_0\} \to \mathbb{A}^2, P \mapsto (x(P), y(P))$; and $\phi : \mathbb{A}^2 \to \mathbb{A}^{n+1}$, given by $(p_1, p_2) \mapsto (F_1(p_1, p_2), \ldots, F_{n+1}(p_1, p_2))$. Then the following diagram is commutative

Thus we have for a point $P$ of $X \setminus \{P_0\}$ and the corresponding local rings assigned to $\pi(P), \pi_2(P)$ the commutative diagram

where $h$ is injective since $k(X) = k(x, y)$, and $c$ is an isomorphism by assumption. Thus $\pi_2 X$ is non-singular at $\pi_2 P$. 

2. Certain maximal curves

The curves we have in mind in this section are the ones given by (see [G-V] and [Sch]):

$$y^q + y = x^m, \quad \text{with} \quad m \text{ being a divisor of } (q + 1).$$
These are maximal curves (with $2g = (m - 1)(q - 1)$) since they are covered by the Hermitian curve. If $P_0$ is the unique point at infinity of this curve, then the semigroup of non-gaps at $P_0$ is generated by $m$ and $q$ and we have:

$$m \cdot n = q + 1, \quad \text{where} \quad (n + 2) = \ell((q + 1)P_0). \quad (***)$$

The goal of this section is to give a proof that the above condition (***) on non-gaps at a rational point $P_0$ characterizes the curves $y^d + y = x^m$ among the maximal curves over the finite field $k$.

**Proposition 2.1.** Let $X$ be a maximal curve of genus $g$. Suppose that there exists a rational point $P_0 \in X(k)$ such that $n \cdot m = q + 1$, with $m$ being a non-gap at $P_0$. Then, we have $2g = (q - 1)(m - 1)$. Also, there are at most two types of $(\mathcal{D}, P)$-orders at rational points $P \in X(k)$:

**Type 1.** The $\mathcal{D}$-orders at $P$ are $0, 1, 2, 3, \ldots, n, q + 1$. In this case we have $v_P(R) = 1$.

**Type 2.** The $\mathcal{D}$-orders at $P$ are $0, 1, m, 2m, \ldots, (n - 1)m, q + 1$. In this case we have $w_2 := v_P(R) = n((n - 1)m - n - 1)/2 + 2$.

Moreover, the set of $\mathcal{D}$-Weierstrass points of $X$ coincides with the set of its $k$-rational points, and the order sequence for $\mathcal{D}$ is $0, 1, 2, \ldots, n, q$.

**Proof.** The morphism $\pi$ can be defined by $(1 : y : \ldots : y^{n-1} : x : y^n)$, where $x, y \in k(X)$ are functions such that

$$\text{div}_\infty(x) = qP_0 \quad \text{and} \quad \text{div}_\infty(y) = mP_0.$$ 

The set of $\mathcal{D}$-orders at $P_0$ is of Type 2, as follows from Proposition 1.5(iii).

Let $P \in X \setminus \{P_0\}$. From the proof of [S-V, Thm. 1.1] and letting $z = y - y(P)$, we have (2.1)

$$v_P(z), \ldots, nv_P(z)$$

are $(\mathcal{D}, P)$-orders. Thus, considering a non-ramified point for $y : X \to \mathbb{P}^1$, we conclude that the order sequence of the linear system $\mathcal{D}$ is given by

$$\epsilon_i = i \quad \text{for} \quad i = 1, \ldots, n, \quad \text{and} \quad \epsilon_{n+1} = q.$$ 

If $P$ is a rational point, by Theorem 1.4, we know that 1 and $(q + 1)$ are $(\mathcal{D}, P)$-orders. We consider two cases:

1. $v_P(z) = 1$: This implies that the point $P$ is of Type 1.
2. $v_P(z) > 1$: From assertion (2.2) above, it follows $n \cdot v_P(z) = q + 1$ and hence $v_P(z) = m$. Then, we have that the point $P$ is of Type 2.

If $P$ is not a rational point, by Theorem 1.4, we have that $j_{n+1}(P) = q$. If $v_P(z) > 1$ and using assertion (2.1), we get

$$n \cdot v_P(z) = q = n \cdot m - 1.$$ 

Hence $n = 1$ and the $(\mathcal{D}, P)$-orders are $0, 1, q$. This shows that $P$ is not a $\mathcal{D}$-Weierstrass point. If $v_P(z) = 1$, again from assertion (2.1), we have that

$$0, 1, 2, \ldots, n, q$$

are the $\mathcal{D}$-orders at the point $P$; i.e., $P$ is not a $\mathcal{D}$-Weierstrass point. This shows the equality of the two sets below:

$$\{\mathcal{D} - \text{Weierstrass points of } X\} = \{k - \text{rational points of } X\}.$$ 

The assertions on $v_P(R)$ follow from [S-V, Thm. 1.5].
Let \( T_1 \) (resp. \( T_2 \)) denote the number of rational points \( P \in X(k) \) whose \((D, P)\)-orders are of Type 1 (resp. Type 2). Thus we have from the equality in (1.2)
\[
\deg(R) = (n(n + 1)/2 + q)(2g - 2) + (n + 2)(q + 1) = T_1 + w_2T_2.
\]
Riemann-Hurwitz applied to \( y : X \to \mathbb{P}^1(\bar{k}) \) gives
\[
2g - 2 = -2m + (m - 1)T_2.
\]
Since \( T_1 + T_2 = \#X(k) = q^2 + 2gq + 1 \), and using the two equations above, we conclude after tedious computations that \( 2g = (m - 1)(q - 1) \). This finishes the proof of the proposition.

Now we are going to prove that maximal curves as in Proposition 2.1 are isomorphic to \( y^q + y = x^m \). To begin with we first generalize \([R-St], \text{Lemma 5}\). We will repeat their argument here for completeness. Let \( \tilde{\mathbb{F}} \) denote the genus of the field \( \bar{k} \) and then they give rise to \((q^2 - q)m[\tilde{F} : F] \) rational points of \( \bar{F} \) over \( k \).

Now the proof continues as in the proof of \([R-St], \text{Lemma 5}\). We will repeat their argument here for completeness. Let \( \tilde{F} \) be the Galois closure of the extension \( k(X) \mid k(y) \). The field \( k \) is still algebraically closed in \( \tilde{F} \) since the elements of the set \( V_1 \) split completely in \( k(X) \mid k(y) \). Moreover the extension \( \tilde{F} \mid k(X) \) is unramified, as follows from Abhyankar’s lemma \([St], \text{ch.III.8}\). Hence,
\[
2\tilde{g} - 2 = [\tilde{F} : F](2g - 2),
\]
where \( \tilde{g} \) denotes the genus of the field \( \tilde{F} \). The \((q^2 - q)\) elements of the set \( V_1 \) split completely in \( \tilde{F} \) and then they give rise to \((q^2 - q)m[\tilde{F} : F] \) rational points of \( \tilde{F} \) over \( k \).

Then, from the Hasse-Weil bound, we conclude
\[
(q^2 - q)m[\tilde{F} : F] \leq q^2 + 2q + (2\tilde{g} - 2)q = q^2 + 2q + [\tilde{F} : F](2g - 2)q.
\]
Substituting \( 2g = (m - 1)(q - 1) \) in the inequality above, we finally get:
\[
[\tilde{F} : F] \leq \frac{q + 2}{q + 1} \quad \text{and hence} \quad \tilde{F} = F.
\]
Note that the extension is cyclic since there exist rational points (those of Type 2) that are totally ramified for the morphism $y$. 

**Theorem 2.3.** Let $X$ be a maximal curve of genus $g$ such that there exists a rational point $P_0 \in X(k)$ with $m \cdot n = (q + 1)$, where $m$ is a non-gap at $P_0$. Then the curve $X$ is $k$-isomorphic to the curve given by the equation:

$$y_1^q + y_1 = a_1^m.$$  

**Proof.** We know that $k(X) \mid k(y)$ is a Galois cyclic extension of degree $m$ and moreover that the functions $1, y, y^2, \ldots, y^{n-1}$ and $x$ form a basis for $L(qP_0)$. Let $\sigma$ be a generator of the Galois group of $k(X) \mid k(y)$. Since $P_0$ is totally ramified, then $\sigma(P_0) = P_0$ and hence $\sigma(L(qP_0)) = L(qP_0)$. Note that the functions $1, y, y^2, \ldots, y^{n-1}$ form a basis for the subspace $L((n-1)mP_0)$ and that $\sigma$ acts as the identity on this subspace. Since $m$ and $q$ are relatively prime, we can diagonalize $\sigma$ on $L(qP_0)$. Take then a function $v \in L(qP_0)$, $v \notin L((n-1)mP_0)$, satisfying $\sigma(v) = \lambda v$, with $\lambda$ a primitive $m$-th root of 1.

Then denoting by $N$ the norm of $k(X) \mid k(y)$, we get $N(v) = (-1)^{m+1} \cdot v^m$. Hence $v^m \in k(y)$ and since it has poles only at $P_0$, we must have $v^m = f(y) \in k[y]$. Since $\text{div}_\infty(v) = \text{div}_\infty(x) = qP_0$, we see that $\text{deg } f(y) = q$. Now from the fact that there are exactly $(q+1)$ totally ramified points of $k(X) \mid k(y)$ and that all of them are rational, we conclude that $f(y) \in k[y]$ is separable and has all its roots in $k$. After a $k$-rational change of coordinates, we may assume that $f(0) = 0$. Then, we get the following description for the set $V_1: V_1 = \{\alpha \in k \mid f(\alpha) \neq 0\}$. Knowing that all points of $X$ above $V_1$ are rational points over $k$ and from the equation $v^m = f(y)$, we get:

$$f^n(y) \equiv f^{nq}(y) \mod (y^{q^2} - y). \quad (*)$$

**Claim.** $f(y) = a_1 y + a_q y^q$, with $a_1, a_q \in k^*$. 

We set $f(y) = \sum_{i=1}^{q} a_i y^i$ and $f^n(y) = \sum_{i=n}^{nq} b_i y^i$. Clearly, the fact that $a_1, a_q \in k^*$ follows from the fact that $f(y)$ is separable of degree $q$. Suppose that the set $I$ below is non-empty

$$I = \{2 \leq i \leq q-1 \mid a_i \neq 0\},$$

and then define

$$t = \min I \quad \text{and} \quad j = \max I.$$  

Clearly, we have $b_{(n-1)q+j} = n \cdot a_q^{n-1} \cdot a_j \neq 0$. Since the unique solution for $i$ in the congruence $iq \equiv (n-1)q + j \mod (q^2 - 1)$, $i$ being smaller than $q^2$, is the one given by $i = (n-1) + j q$, it follows from $(*)$ above that $b_{(n-1)q+j} = b_{(n-1)+j}^q \neq 0$.

It now follows that $\text{deg } (f^n(y)) = n q \geq (n-1) + j q$ and hence we get that $n - j \geq 1$ if $n \geq 2$. Note that if $n = 1$, then we get $j \leq 1$ and the proof of the claim is complete in this case. From now on we then assume $n \geq 2$. We then conclude that $t \leq j \leq (n-1)$. Note that then $(n-1) + t < q$.

Clearly, we also have $b_{n-1+t} = n \cdot q^{n-1} \cdot a_t \neq 0$. Since the unique solution for $i$ in the congruence $iq \equiv n-1 + t \mod (q^2 - 1)$, $i$ being smaller than $q^2$, is the one given by $i = (n-1 + t) q$, it follows from $(*)$ above that $b_{(n-1)+t} = b_{(n-1)+t}^q \neq 0$.

As before, it now follows that $n q \geq (n-1 + t) q$, and hence $t \leq 1$. This gives the desired contradiction and hence the set $I$ is empty, thereby proving the claim.
Now we are in a position to finish the proof of the theorem. Denoting 
\[ f(k) = \{ f(\alpha) \mid \alpha \in k \} \quad \text{and} \quad H = \{ \beta^m \mid \beta \in k \}, \]
we have that \( \mathbb{F}_q^n \) is a subgroup of \( H \setminus \{0\} \) of index equal to \( n \). Moreover, using the fact that above \( V_1 \) there are only rational points, we have:
\[ f(k) \subseteq H = \bigcup_{\ell=0}^{n-1} \xi^{\ell m} \mathbb{F}_q, \]
where \( \xi \) denotes a primitive element of the field \( k \); i.e., \( \xi \) is a generator for the multiplicative cyclic group \( k^* \). Since \( f(k) \) is a \( \mathbb{F}_q \)-linear subspace of \( k \) as follows from the above claim, we conclude that its dimension is one and hence that \( f(k) = \xi^{-m} \mathbb{F}_q \), for some \( r \). Finally, putting \( x_1 = \xi^{-v} v \) and \( y_1 = \epsilon y \), where \( \epsilon \) is the unique element of \( k^* \) satisfying
\[ \text{Tr} (\epsilon \alpha) = \xi^{-r m} f(\alpha), \quad \forall \alpha \in k, \]
we conclude the proof of the theorem (\( \text{Tr} \) being the trace operator in \( k(X) \mid k(y) \)). \( \square \)

Remark. Notations being as above. Suppose that \( m \cdot n \leq q + 1 \) ( \( m \) being a non-gap at some rational point \( P_0 \) of \( X \)). Then, we have \( q + 1 \geq m \cdot n \geq m_n(P_0) = q \), where the last equality follows from Proposition 1.5(iv). In case that \( m \cdot n = q \), we conjecture that \( 2g = (m - 1)q \) and the curve is \( \mathbb{F}_q \)-isomorphic to a curve given by
\[ F(y) = x^{q+1}, \]
where \( F(y) \) is a \( \mathbb{F}_q \)-linear polynomial of degree \( m \). We have not been able to prove this possible result yet.

We notice that if one could show that the morphism \( \pi : X \to \mathbb{P}^{m+1} \) is a closed embedding, then by Proposition 1.10 we would have the claimed formula for \( g \).

Finally we also notice that \( (m_1(P) - 1)q/2, P \in X(k) \), is an upper bound for the genus of maximal curves. This follows from [Le, Thm. 1(b)].

Example 2.4. There exist maximal curves that do not satisfy the hypothesis of Theorem 2.3. We give two such examples below:

(i) Let \( X \) be the maximal curve over \( \mathbb{F}_{25} \) and genus \( g = 3 \) listed by Serre in [Sc, §4]. Let \( m, 5, 6 \) be the first three non-gaps at \( P \in X(\mathbb{F}_{25}) \). Here we have \( 6P_0 = g_0^3 \). We claim that \( m = 4 \) (and so \( nm > q + 1 \)). Indeed, if \( m = 3 \) by Proposition 2.1 we would have \( g = 4 \).

This example also shows a maximal curve where all the rational points are non-Weierstrass points: in fact, since \( 5 = \text{char}(k) > 2g - 2 \) the curve is classical.

(ii) Let \( X \) be a maximal curve over \( \mathbb{F}_{q^2} \) of genus \( g \). Suppose that \( q \geq 2g + 2 \) (e.g. the maximal curves in Proposition 1.8 here, Thm. 3.12, Thm. 3.16, Thm. 1). Then \( X \) does not satisfy the hypothesis of Theorem 2.3. In fact, for \( P_0 \in X(k) \) we have \( m_{q+i}(P_0) = 2g + i \) and then \( n = q - g \). Therefore \( m_1(P_0)n \geq 2n \geq q + 2 \), the last inequality following from \( q \geq 2g + 2 \).

3. Maximal curves of genus \((q - 1)^2/4\).

As an interesting application of the preceding section we prove:

**Theorem 3.1.** Let \( X \) be a maximal curve over \( \mathbb{F}_{q^2} \) of genus \( g = (q - 1)^2/4 \). Then the curve \( X \) is \( \mathbb{F}_{q^2} \)-isomorphic to the one given by
\[ y^q + y = x^{q+1/2}. \]
Proof. From Equation (1.6), which is Castelnuovo’s genus bound applied to the linear system \( |(q + 1)P_0| \), we have \( n = 2 \) (see remark before Proposition 1.5). From Theorem 2.3, it suffices to prove the existence of a rational point \( P \) over \( k \) with \( m_1(P) = (q + 1)/2 \). This is clearly true for \( q = 3 \) (since \( g = 1 \) in this case) and hence we can assume \( q \geq 5 \).

We prove firstly some lemmas:

**Lemma 3.2.** Let \( P \) be a rational point over \( k \) of the curve \( X \) (hypothesis being as in Theorem 3.1). Then we have that \( \ell((2q + 2)P) = 9 \) and that either \( m_1(P) = (q - 1)/2 \) or \( m_1(P) = (q + 1)/2 \). Moreover, the divisor \( (2g - 2)P \) is a canonical divisor.

**Proof.** Let \( m_i = m_i(P) \) be the \( i \)-th non-gap at the rational point \( P \). We have the following list of non-gaps at \( P \):

\[
0 < m_1 < m_2 = q < m_3 = q + 1 < 2m_1 < m_1 + m_2 < m_1 + m_3 < 2m_2 < m_2 + m_3 < 2m_3.
\]

The inequality \( 2m_1 \geq (q + 1) \) follows from the fact that \( n = 2 \) and \( q \) odd. Clearly,

\[
m_3 = 2m_1 \quad \text{if and only if} \quad m_1 = (q + 1)/2 \quad \text{and} \quad m_1 + m_3 = 2m_2 \quad \text{if and only if} \quad m_1 = (q - 1).
\]

Since \( q \geq 5 \), one cannot have both equalities above simultaneously. From the above list of non-gaps at \( P \), it then follows that \( \ell((2q + 2)P) \geq 9 \). Moreover, after showing that \( \ell((2q + 2)P) = 9 \), it also follows that either \( m_1 = (q + 1)/2 \) or \( m_1 = (q - 1) \). Let \( \pi_2 : X \to \mathbb{P}^{r + 1} \) be the morphism associated to the linear system \( |(2q + 2)P| \); we already know that \( r \geq 7 \) and we have to show that \( r = 7 \). Castelnuovo’s bound for the morphism \( \pi_2 \) gives

\[
2g = \frac{(q - 1)^2}{2} \leq M \cdot (d - 1 - (r - e)), \tag{\ast}
\]

where \( d = 2q + 2 \), \( M = \left\lfloor \frac{d - 1}{r} \right\rfloor \), and \( d - 1 = M \cdot r + e \). Since \( (r - e) \geq 1 \) we have \( d - 1 - (r - e) \leq 2q \), and hence

\[
(q - 1)^2 \leq 4qM \quad \text{and then} \quad q^2 - q \leq 4qM,
\]

since the right hand side above is a multiple of \( q \). For \( r \geq 9 \), we now see that

\[
q - 1 \leq 4M \leq 4 \cdot \frac{2q + 1}{9}, \quad \text{and then} \quad q \leq 13.
\]

The cases \( q \leq 13 \) are discarded by direct computations in Equation (\ast) above, and hence we have \( r \leq 8 \). Now we use again Equation (\ast) to discard also the possibility \( r = 8 \). Since \( q \) is odd, we have

\[
2q + 1 \equiv 3 \pmod{8} \quad \text{or} \quad 2q + 1 \equiv 7 \pmod{8}.
\]

It then follows

\[
\begin{aligned}
\begin{cases}
M = (q - 1)/4 \\
\text{and } e = 3
\end{cases}
\quad \text{or} \quad \begin{cases}
M = (q - 3)/4 \\
\text{and } e = 7.
\end{cases}
\end{aligned}
\]

Substituting these two possibilities above in Equation (\ast), one finally gets the desired contradiction; i.e., one gets

\[
(q - 1)^2 \leq (q - 1)(q - 2) \quad \text{or} \quad (q - 1)^2 \leq (q - 3) \cdot q.
\]
Now we prove the last assertion of the lemma. One can easily check that both semigroups $H_1$ and $H_2$ below are symmetric, with exactly $g = (q - 1)^2/4$ gaps:

$$H_1 = \langle (q - 1), q, q + 1 \rangle \quad \text{and} \quad H_2 = \langle \frac{q + 1}{2}, q \rangle.$$ 

At a rational point $P$ on $X$ the Weierstrass semigroup $H(P)$ must then be equal to $H_1$ or $H_2$. Hence the semigroup $H(P)$ is necessarily symmetric and the last assertion follows.

Lemma 3.3. Let $D = \lfloor (q + 1)P \rfloor$ with $P$ being a rational point of $X$ (hypothesis as in Theorem 3.1). Then at any non-rational point $Q$ of $X$, the $(D, Q)$-orders are $0, 1, 2, q$. In particular the order sequence for $D$ is $0, 1, 2, q$, and the set of $D$-Weierstrass points is exactly the set of rational points.

Proof. Let $0, 1, j, q$ be the $(D, Q)$-orders. Consider the following set $S$:

$$S = \{0, 1, 2, j, j + 1, 2j, q, q + 1, q + j, 2q\}.$$ 

The set $S$ consists of $(2D, Q)$-orders, and hence from Lemma 3.2 we must have $\# S \leq 9$. This eliminates the possibilities

$$3 \leq j \leq \frac{q - 1}{2} \quad \text{and} \quad \frac{q + 3}{2} \leq j \leq q - 2,$$

and it then follows that $j \in \{2, (q + 1)/2, q - 1\}$. From Lemma 3.2 we know that

$$(2g - 2)P = \frac{(q + 1)(q - 3)}{2}P \quad \text{is canonical.}$$

Then the following set $S(j)$ consists of orders at $Q$ for the canonical morphism

$$S(j) = \{a + bj + cq \mid a, b, c \in \mathbb{N} \text{ with } a + b + c \leq \frac{q - 3}{2}\}.$$ 

One can check that $\# S(j) = (q - 1)^2/4$ if the value of $j$ belongs to $\{2, (q + 1)/2, q - 1\}$, and hence that $S(j)$ consists of all canonical orders at the point $Q$. Then the set $H(j)$ below is necessarily a semigroup:

$$H(j) = \mathbb{N} \setminus (1 + S(j)).$$

This semigroup property on $H(j)$ is only satisfied for the value $j = 2$, as one checks quite easily, and this finishes the proof of this lemma.

Now we turn back to the proof of Theorem 3.1. Suppose that $m_1(P) = (q - 1)$ at all rational points $P$ on the curve. It then follows from Proposition 1.5(iii) that the $(D, P)$-orders are $0, 1, 2, q + 1$ and hence $v_P(R) = 1$, where $R$ is the divisor supporting the $D$-Weierstrass points. On the other hand, we have

$$\deg R - \# X(k) = 3(2g - 2) - (q - 3)(q + 1) = \frac{1}{2}(q + 1)(q - 3).$$

Since $q \geq 5$ and $v_P(R) = 1$ for $P$ rational, we would then conclude the existence of non-rational points that are $D$-Weierstrass points. This contradicts Lemma 3.3 and hence, from Lemma 3.2, we finally conclude the existence of a rational point $P$ satisfying

$$m_1(P) = (q + 1)/2.$$
We can explore further the idea of the above proofs to obtain a partial analogue of the main result of \([F-T]\), namely

**Scholium 3.4.** Let \(X\) be a maximal curve over \(k\) whose genus \(g\) satisfies
\[
\frac{q^2 - 3q + 2}{4} < g \leq \frac{(q - 1)^2}{4}.
\]

If \(q\) is odd, neither \(q\) is a power of 3 nor \(q \not\equiv 3 \pmod{4}\), then \(g = \frac{(q - 1)^2}{4}\).

Notice that Example 2.4(i) shows that the hypothesis on \(g\) above is sharp. This Scholium is the first step toward a characterization of a maximal curve whose genus is
\[
\frac{\frac{q-1}{2}(\frac{q+1}{2} - 1)}{t} \quad \text{with} \quad t \geq 3.
\]

**References**

[ACGH] Arbarello, E.; Cornalba, M.; Griffiths, P.A. and Harris, J.: Geometry of algebraic curves, Vol. I, Springer-Verlag, New York 1985.

[C] Castelnuovo, G.: Ricerche di geometria sulle curve algebriche, Atti. R. Acad. Sci. Torino 24, 196–223 (1889).

[F-T] Fuhrmann, R.; Torres, F.: The genus of curves over finite fields with many rational points, Manuscripta Math. 89, 103–106 (1996).

[Ful] Fulton, W.: Algebraic curves. An introduction to algebraic curves (second edition). W.A. Benjamin, INC 1974.

[G-Sti] Garcia, A.; Stichtenoth, H.: Elementary abelian \(p\)-extensions of algebraic function fields, Manuscripta Math. 72, 67–79 (1991).

[G-V] Garcia, A.; Viana, P.: Weierstrass points on certain non-classical curves, Arch. Math. 46, 315–322 (1986).

[G-Vl] van der Geer, G.; van der Vlugt, M.: How to construct curves over finite fields with many points, alg-geom e-prints 9511003.

[Go] Goppa, V.D.: Algebraic-Geometric codes, Math. USRR-Izv. 21 (1), 75–91 (1983).

[H] Hansen, J.P.: Deligne-Lusztig varieties and group codes, Lect. Notes Math. 1518, 63–81 (1992).

[H-Sti] Hansen, J.P.; Stichtenoth, H.: Group codes on certain algebraic curves with many rational points, AAECC 1, 67–77 (1990).

[Har] Hartshorne, R.: Algebraic Geometry, Grad. Texts in Math. 52 Springer-Verlag 1977.

[H-V] Hefez, A.; Voloch, J.F.: Frobenius non-classical curves, Arch. Math. 54, 263–273 (1990).

[Ho] Homma, M.: Linear systems on curves with no Weierstrass points, Bol. Soc. Bras. Mat. (N.S.) 23, (1–2), 93–108 (1992).

[I] Ibukiyama, T.: On rational points of curves of genus 3 over finite fields, Tôhoku Math. J. 45, 311–329 (1993).

[Ih] Ihara, Y.: Some Remarks on the Number of Rational Points of Algebraic Curves over Finite Fields, J. Fac. Sci. Tokyo 28, 721–724 (1981).

[L] Lang, S.: Abelian Varieties, Interscience Pub., New York 1959.

[Le] Lewittes, J.: Places of degree one in function fields over finite fields, J. Pure Appl. Alg. 69, 177–183 (1990).

[P] Pedersen, J.P.: A function field related to the Ree group, Lect. Notes Math. 1518, 122–131 (1992).

[Ra] Rathmann, J.: The uniform position principle for curves in characteristic \(p\), Math. Ann. 276, 565–579 (1987).

[R-Sti] Rück, H.G.; Stichtenoth, H.: A characterization of Hermitian function fields over finite fields, J. Reine Angew. Math. 457, 185–188 (1994).

[Sch] Schmidt, F.K.: Zur arithmetischen Theorie der algebraischen Funktionen II. Allgemeine Theorie der Weierstrasspunkte, Math. Z. 45, 75–96 (1939).

[Se] Serre, J.P.: Résumé des cours de 1983-1984, Annaire du College de France, 79–83 (1984). Reprinted in Œuvres III, 701–705.

[Sti] Stichtenoth, H.: Algebraic functions fields and codes, Springer-Verlag, Berlin, 1993.
[Sti-X] Stichtenoth, H.; Xing, C.: The genus of maximal functions fields, Manuscripta Math. 86, 217–224 (1995).

[S-V] Stöhr, K.O.; Voloch, J.F.: Weierstrass points and curves over finite fields, Proc. London Math. Soc. (3) 52, 1–19 (1986).

[Ta] Tate, J.: Endomorphisms of abelian varieties over finite fields, Inventiones Math. 2, 134–144 (1966).

[To] Thomas, M.: Über das Geschlecht eines Funktionenkörpers, Diplomarbeit Universität Essen, 1994.

FACHBEREICH 6, MATHEMATIK UND INFORMATIK, UNIVERSITÄT ESSEN, D-45117, ESSEN - GERMANY
E-mail address: RAINER.FUHRMANN@ZENTRALE.DEUTSCHE-BANK.dbp.de

IMPA, ESTRADA DONA CASTORINA 110, 22460-320, RIO DE JANEIRO - BRAZIL
E-mail address: garcia@impa.br

FACHBEREICH 6, MATHEMATIK UND INFORMATIK, UNIVERSITÄT ESSEN, D-45117, ESSEN - GERMANY
E-mail address: fernando.torres@uni-essen.de