ON CURVES OVER FINITE FIELDS
WITH MANY RATIONAL POINTS

Rainer Fuhrmann\textsuperscript{1}
Fachbereich 6, Mathematik und Informatik, Universität Essen,
D-45117 Essen - Germany

and

Fernando Torres\textsuperscript{2}
International Centre for Theoretical Physics, Trieste, Italy.

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 rational points we prove that maximal curves are $\mathbb{F}_q^2$-isomorphic to $y^q + y = x^m$ for some $m \in \mathbb{Z}^+$. 

MIRAMARE – TRIESTE
March 1996

\textsuperscript{1}E-mail: 100713.3165@compuserve.com
\textsuperscript{2}E-mail: feto@ictp.trieste.it
0. Introduction

Goppa in [Go] showed how to construct linear codes from curves defined over finite fields. One of the main features of these codes is the fact that one can state a lower bound for the minimum distance of the codes. In fact, let $C_X(D,G)$ be a Goppa code defined over a curve $X$ over the finite field $\mathbb{F}_q$ with $q$ elements, where $D = P_1 + \ldots + P_n$, $P_i \in X(\mathbb{F}_q)$ for each $i$ and $G$ is a $\mathbb{F}_q$-rational divisor on $X$. Then it is known that the minimum distance $d$ of $C_X(D,G)$ satisfies

$$d \geq n - \deg(G).$$

Certainly this bound is meaningful only if $n$ is large enough. This provides motivation for the study of curves over finite fields with many rational points.

The purpose of this paper is to study maximal curves, that is, curves $X$ over $\mathbb{F}_q$ whose number of rational points $\#X(\mathbb{F}_q)$ reaches the Hasse-Weil upper bound. In this case one knows that $q$ must be a square.

Let $k$ be the finite field with $q^2$ elements, where $q$ is a power of a prime $p$. Let $X$ be a projective, connected, non-singular algebraic curve defined over $k$ which is maximal, that is, $\#X(k)$ satisfies

$$\#X(k) = q^2 + 2gq + 1. \quad (0.1)$$

Let $P \in X(k)$ and set $\mathcal{D} = g_{q+1}$ the $k$-linear system on $X$ defined by the divisor $(q+1)P$. Then $n \geq 1$, and $\mathcal{D}$ is independent of $P$. In fact $\mathcal{D}$ is a simple base-point-free linear system on $X$ (Corollary 1.2.3, Remark 1.2.5 (ii)). This allows us to apply Stöhr-Voloch’s approach concerning Weierstrass point theory over finite fields [S-V]. Moreover, the dimension $n+1$ of $\mathcal{D}$ and the genus $g$ are related by Castelnuovo’s genus bound for curves in projective spaces ([C], [ACGH, p.116], [Ra, Corollary 2.8]).

It is known that $2g \leq (q-1)q$ ([Sti, V.3.3]), and that the Hermitian curve is the unique maximal curve whose genus is $(q-1)q/2$ [R-Sti]. Furthermore in [F-T] we proved the following stronger bounds for the genus, namely

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

Moreover by using the already mentioned Castelnuovo’s bound one can prove that $4g > (q-1)^2$ if and only if $n = 1$. Therefore, we assume from now on that $n \geq 2$.

The Hermitian curve is a particular case of the following type of curves. Let $m$ be a positive divisor of $q+1$, and let consider

$$y^q + y = x^m. \quad (H_{m,q})$$

These curves are maximal ([G-V, Thm. 1]) and have very remarkable properties (see e.g [G-V], [Sch]).

Under a hypothesis on non-gaps at rational points we prove that maximal curves are $k$-isomorphic to $H_{m,q}$ for some $m \in \mathbb{Z}^+$. 

**Theorem 0.1.** Let $X$ be a maximal curve of genus $g > 0$. Assume that there exists $P_0 \in X(k)$ such that the first non-gap $m_1$ at $P_0$ satisfies

$$nm_1 \leq q+1,$$

where $n + 1$ is the dimension of the complete linear system defined by $(q + 1)P_0$. Then one of the following possibilities is satisfied

(i) $nm_1 = q + 1$, $2g = (m_1 - 1)(q - 1)$, and $X$ is $k$-isomorphic to $H_{m_1,q}$.

(ii) $nm_1 = q$. 

From this theorem and a result due to Lewittes (see inequality 1.6) we obtain an analogous of the main result in [F-T]:

**Corollary 0.2.** Let $X$ be a curve satisfying the hypotheses of Theorem 0.1. Let $t \geq 1$ be an integer, and suppose that the genus $g$ of $X$ satisfies

$$(q - 1)(\frac{t + 1}{t} - 1) < 2g \leq (q - 1)(\frac{t + 1}{t} - 1).$$

Then one of the following conditions is satisfied

(i) $t = n$, $2g = (q - 1)(\frac{q + 1}{t} - 1) = (q - 1)(m_1 - 1)$.

(ii) $t > n$, $2g \leq (q - 1)(\frac{q + 1}{n} - 1) = (q - 1)(\frac{m_1(q+1)}{q} - 1)$.

**Remark 0.3.** In case $nm_1 = q$ the authors actually conjecture that then $2g = (m_1 - 1)q$, and $X$ is $k$-isomorphic to a curve whose plane model is given by $F(y) = x^{q+1}$, where $F(y)$ is a $\mathbb{F}_q$-linear polynomial of degree $m_1$. But we have not yet been able to prove this. We notice that the veracity of this conjecture implies $t = n$ and $2g = (\frac{q}{t} - 1)q = (m_1 - 1)q$ in the statement (ii) of the above corollary.

### 1. Preliminaries

Throughout this paper we use the following notation:

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

$$L(D) := \{ f \in k(X) : \text{div}(f) + D \succeq 0 \};$$

and $\ell(D) := \dim_k L(D)$. The symbol "~" denotes module linear equivalence.
- The symbol $g^r_d$ stands for a linear system of dimension $r$ and degree $d$.

#### 1.1. Weierstrass points

We summarize some results from [S-V]. Let $X$ be a curve of genus $g$, $\mathcal{D} = g^r_d$ a base-point-free $k$-linear system on $X$. Then associated to $P \in X$ we have the hermitian $P$-invariants $j_0(P) = 0 < j_1(P) < \ldots < j_r(P) \leq d$ of $\mathcal{D}$ (or simply the $(\mathcal{D}, P)$-orders). This sequence is the same for all but finitely many points. These finitely many points $P$, where exceptional $(\mathcal{D}, P)$-orders occur, are called the $\mathcal{D}$-Weierstrass points of $X$. (If $\mathcal{D}$ is generated by a canonical divisor, we obtain the usual Weierstrass points of $X$.) Associated to $\mathcal{D}$ there exists a divisor $R$ supporting the $\mathcal{D}$-Weierstrass points of $X$. Let $\epsilon_0 < \epsilon_1 < \ldots < \epsilon_r$ denote the $(\mathcal{D}, P)$-orders for a generic $P \in X$. Then

$$\epsilon_i \leq j_i(P),$$

for $P \in X$, for each $i$, and

$$\deg(R) = (\epsilon_1 + \ldots + \epsilon_r)(2g - 2) + (r + 1)d.$$
Associated to $\mathcal{D}$ we also have a divisor $S$ whose support contains $X(k)$. Its degree is given by
\[ \deg(S) = (\nu_1 + \ldots + \nu_r)(2g - 2) + (q^2 + r)d, \]
where the $\nu_i$'s is a subsequence of the $e_i$'s. More precisely there exists an integer $I$ with $0 < I \leq r$ such that $\nu_i = e_i$ for $i < I$ and $\nu_i = e_{i+1}$ otherwise. Moreover for $P \in X(k)$ we have
\[ v_P(S) \geq \sum_{i=1}^{r} (j_i(P) - \nu_{i-1}), \]
and
\[ \nu_i \leq j_{i+1}(P) - j_i(P), \]
for each $i$. 

1.2. Maximal curves. Let $X$ be a maximal curve of genus $g$. In this section we study some arithmetical and geometrical properties of $X$. To begin with we have the following basic result which is containing in the proof of [R-Sti, Lemma 1]. For the sake of completeness we state a proof of it.

**Lemma 1.2.1.** The Frobenius map $Fr_\mathcal{J}$ (relative to $k$) of the Jacobian $\mathcal{J}$ of $X$ acts just as multiplication by $(-q)$ on $\mathcal{J}$.

**Proof.** All the facts concerning Jacobians can be found in [L, VI, §3]. Let $\ell \neq p$ be a prime and let $T_\ell(\mathcal{J})$ be the Tate module of $\mathcal{J}$. Then the characteristic polynomial $P(Fr_\mathcal{J})(t)$ of the action $Fr_\mathcal{J}$ on $T_\ell(\mathcal{J})$ is equal to $\ell^g L(1/\ell)$ where $L(t)$ denotes the numerator of the Zeta function of $X$. Since $X$ satisfies (0.1), $L(t) = \prod_{i=1}^{2g} (1 + qt)$ and thus $P(Fr_\mathcal{J})(t) = (t + q)^{2g}$. Now we know that $Fr_\mathcal{J}$ is diagonalizable [Ta, Thm. 2] and all its eigenvalues are $-q$. This means that $Fr_\mathcal{J}$ acts just as multiplication by $-q$ on $T_\ell(\mathcal{J})$. Finally since the natural homomorphism of $\mathbb{Z}$-algebras
\[ \text{End}(\mathcal{J}) \to \text{End}(T_\ell(\mathcal{J})) \]
is injective, the proof follows. \qed

Now fix $P_0 \in X(k)$, and consider the map $f = f^{P_0} : X \to \mathcal{J}$ given by $P \to [P - P_0]$. We have
\[ f \circ Fr_X = Fr_\mathcal{J} \circ f, \]
where $Fr_X$ denotes the Frobenius morphism of $X$ relative to $k$. Hence from the above equality and Lemma 1.2.1 we get

**Corollary 1.2.2.**
\[ Fr_X(P) + qP \sim (q + 1)P_0. \]

From this corollary it follows immediately the following:

**Corollary 1.2.3 ([R-Sti, Lemma 1]).** Let $P_0, P_1 \in X(k)$. Then $(q + 1)P_1 \sim (q + 1)P_0$.

Now, let consider the linear system $\mathcal{D} = g^{n+1}_{P_0} := |(q + 1)P_0|$. Corollary 1.2.3 says that $\mathcal{D}$ is a $k$-invariant of the curve. In particular its dimension $n + 1$ is independent of $P \in X(k)$. Moreover from Corollary 1.2.3 we have that $q + 1 \in H(P_0)$ and hence $\mathcal{D}$ is base-point-free. Consequently we can apply [S-V] to $\mathcal{D}$.

**Theorem 1.2.4.** With notation as in §1.1 (for $\mathcal{D}$) we have:
Proof. Statement (iii) for $P \in X(k)$ follows from (i), (ii) and inequality (1.4). From Corollary 1.2.2 it follows (ii) and $e_{n+1} = q$. Furthermore it also follows that $j_1(P) = 1$ for $P \notin X(k)$: for let $P' \in X$ such that $F_{rX}(P') = P$; then $P + qP' = F_{rX}(P') + qP' \sim (q + 1)P_0$.

Now we are going to prove that $\nu_n = e_{n+1}$. Let $P \in X \setminus \{P_0\}$. Corollary 1.2.2 says that $\pi(F_{rX}(P))$ belongs to the osculating hyperplane at $P$, where $\pi$ stands for the morphism associated to $\mathcal{D}$. $\pi$ can be defined by a base $\{f_0, f_1, \ldots, f_{n+1}\}$ of $L((q + 1)P_0)$, where $v_P(f_i) \geq 0$ for each $i$. Let $x$ be a separating variable of $k(X) \mid k$. Then by [S-V, Prop. 1.4(c), Corollary 1.3] the rational function

$$w := \det \begin{pmatrix} f_0 \circ F_{rX} & \cdots & f_{n+1} \circ F_{rX} \\ D_x^0 f_0 & \cdots & D_x^{n+1} f_{n+1} \\ \vdots & \vdots & \vdots \\ D_x^0 f_0 & \cdots & D_x^{n+1} f_{n+1} \end{pmatrix}$$

satisfies $w(P) = 0$ for each generic point $P$. Let $I$ be the smallest integer such that the row $(f_0 \circ F_{rX}, \ldots, f_{n+1} \circ F_{rX})$ is a linear combination of the vectors $(D_x^0 f_0, \ldots, D_x^{n+1} f_{n+1})$ with $i = 0, \ldots, I$. Then according to [S-V, Prop. 2.1] we find

$$\{\nu_0 < \ldots < \nu_n\} = \{\epsilon_0 < \ldots < \epsilon_{I-1} < \epsilon_I < \ldots < \epsilon_{n+1}\}.$$  

This concludes the proof. \qed
We can also bound \( g \) by using non-gaps at \( P_0 \) in \( X(k) \). In fact, Lewittes [Le, Thm. 1(b)] proved that
\[
\#X(k) \leq q^2m_1(P) + 1,
\]
and hence from (0.1) we conclude that
\[
(1.6) \quad 2g \leq q(m_1(P) - 1).
\]

**Proposition 1.2.6.** The following statements are equivalent:

(i) \( \pi : X \to \mathbb{P}^{n+1} \) is a closed embedding, i.e. \( X \) is \( k \)-isomorphic to \( \pi(X) \).

(ii) \( \forall P \in X(\mathbb{F}_{q^4}) : \pi(P) \in \mathbb{P}^{n+1}(k) \Leftrightarrow P \in X(k) \).

(iii) \( \forall P \in X(\mathbb{F}_{q^4}) : q \in H(P) \).

**Proof.** Let \( P \in X \). Since \( j_1(P) = 1 \) (cf. Theorem 1.2.4 (iii)) we know already that \( \pi(X) \) is non-singular at all the branches centered at \( P \). Thus \( \pi \) is an embedding if and only if \( \pi \) is injective.

**Claim.** If \( \#\pi^{-1}(\pi(P)) \geq 2 \), then \( P \in X(\mathbb{F}_{q^4}) \setminus X(k) \) and \( \pi(P) \in \mathbb{P}^{n+1}(k) \).

**Proof.** From Corollary 1.2.2 it follows that \( \pi^{-1}(\pi(P)) \subseteq \{P, \pi(P)\} \). Analogically we have \( \pi^{-1}(\pi(F \times \pi(P))) \subseteq \{F \times \pi(P), \pi^2(X)(P)\} \). Thus if \( \#\pi^{-1}(\pi(P)) \geq 2 \), then \( P \) cannot be rational and \( F \times \pi(P) = P \), i.e. \( P \in X(\mathbb{F}_{q^4}) \setminus X(k) \). Furthermore we have \( \pi(P) = \pi(F \times \pi(P)) = \pi^2(X)(P) \), i.e. \( \pi(P) \in \mathbb{P}^{n+1}(k) \).

From this claim the equivalence (i) \( \Leftrightarrow \) (ii) follows immediately. As to the implication (i) \( \Rightarrow \) (iii) we know that \( \dim \left| F \times \pi(X) + qP - P - F \times \pi(X) \right| = \dim \left| F \times \pi(X) + qP \right| - 2 \) (Corollary 1.2.2 and [Har, Prop.3.1(b)]), i.e. \( q \in H(P) \). Finally we want to conclude that \( \pi \) is an embedding from (iii). According to the above claim it is sufficient to show that \( \pi^{-1}(\pi(P)) = \{P\} \) for \( P \in X(\mathbb{F}_{q^4}) \). Let \( P \in X(\mathbb{F}_{q^4}) \). Because of Corollary 1.2.2 we know that \( \pi^{-1}(\pi(P)) \subseteq \{P, F \times \pi(X)\} \). Since \( q \in H(P) \), there is a divisor \( D \in |qP| \) with \( P \notin \text{Supp}(D) \). In particular
\[
F \times \pi(X) + D \sim F \times \pi(X) + qP \sim (q + 1)P_0.
\]
Thus \( \pi^{-1}(\pi(F \times \pi(X))) \subseteq \text{Supp}(F \times \pi(X) + D) \). So either \( \pi(P) \neq \pi(F \times \pi(X)) \) or \( P = F \times \pi(X) \). In both cases we have \( \pi^{-1}(\pi(P)) = \{P\} \). This means altogether that \( \pi \) is injective and so indeed a closed embedding. \( \Box \)

**Proposition 1.2.7.** Suppose that \( \pi : X \to \mathbb{P}^{n+1} \) is a closed embedding. 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 \( H(P_0) \) 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 \( q, q + 1 \in H(P_0) \), the numbers \( r \) and \( s \) are coprime. Let \( \pi_2 : X \to \mathbb{P}^2, P \mapsto (1 : x(P) : y(P)) \). Then the curves \( X \) and \( \pi_2(X) \) are birational and \( \pi_2(X) \) is a plane curve given by an equation of type
\[
x^r + \beta y^s + \sum_{i+j+r<s+r} \alpha_{ij}x^iy^j = 0,
\]
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 \( \pi_2(X) \) for \( P \neq P_0 \). From this follows by [Ful, Ch. 7] that \( g = 1/2(r - 1)(s - 1) \). Then by Jenkins [J] we have \( H(P_0) = (r, s) \).

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
\[
f_i = F_i(x, y) \quad \text{on} \quad X \quad \text{for} \quad i = 1, \ldots, n + 1.
\]
Consider the maps \( \pi \mid (\mathcal{X} \setminus \{P_0\}) : \mathcal{X} \setminus \{P_0\} \to \mathbb{A}^{n+1} \) given by \( P \mapsto (f_1(P), \ldots, f_{n+1}(P)) \); \( \pi_2 \mid (\mathcal{X} \setminus \{P_0\}) : \mathcal{X} \setminus \{P_0\} \to \mathbb{A}^2 \); \( P \mapsto (x(P), y(P)) \); 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 commuting

\[
\begin{array}{ccc}
\mathcal{X} \setminus \{P_0\} & \xrightarrow{\pi_2} & \mathbb{A}^2 \\
\downarrow{\pi} \quad & & \downarrow{\phi} \\
\mathcal{X} & \xrightarrow{\phi} & \mathbb{A}^{n+1}
\end{array}
\]

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

\[
\begin{array}{ccc}
O_{\pi_2(X), \pi_2(P)} & \xrightarrow{f} & O_{\pi_2(X), \pi_2(P)} \\
\downarrow{h} & & \downarrow{c} \\
O_{\pi(X), \pi(P)} & & O_{\pi(P)}
\end{array}
\]

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. Proofs of Theorem 0.1 and Corollary 0.2

Set \( m := m_1 \). Recall that \( n + 1 \) is by definition the dimension of \( \mathcal{D} := \{(q + 1)P\} \) for any \( P \in \mathcal{X}(k) \). Let \( \pi \) be the morphism associated to \( \mathcal{D} \). By Remark 1.2.5 (ii) we have \( nm \geq q \), and hence by the hypothesis on \( m \) we get

\[ nm \in \{q, q + 1\} \]

2.1. Case: \( nm = q + 1 \).

**Proposition 2.1.1.** Let \( X \) be a maximal curve of genus \( g \). Assume there exists \( P_0 \in X \) such that \( nm_1(P_0) = q + 1 \). Then

\[ 2g = (q - 1)(m_1 - 1) \]

**Proof.** Since \( m, q \in H(P_0) \) and \( \gcd(m, q) = 1 \), then \( 2g \leq (m - 1)(q - 1) \) (see e.g. Jenkins [J]). Now, \( \pi \) can be defined by \((1 : y : \ldots : y^{n-1} : x : y^n)\) where \( x, y \in k(X) \) such that

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

Let \( P \in \mathcal{X} \setminus \{P_0\} \). From the proof of [S-V, Thm. 1.1], we have that

\[ v_P(y), \ldots, nv_P(y) \]

are \((\mathcal{D}, P)\)-orders. Thus by considering a non-ramified point for \( y : \mathcal{X} \to \mathbb{P}^1 \), and by (1.1) we find

\[ \epsilon_i = i, \quad \text{for} \quad i = 1, \ldots, n \]

**Lemma 2.1.2.** There are at most two types of \((\mathcal{D}, P)\)-orders for \( P \in \mathcal{X}(k) \):

(i): \( 0, 1, m, \ldots, (n - 1)m, q + 1 \). Hence \( w_1 := v_P(R) = \frac{n(n - 1)m - n - 1}{2} + 2 \).

(ii): \( 0, 1, \ldots, n, q + 1 \). Hence \( w_2 := v_P(R) = 1 \).

Moreover, the set of the \( \mathcal{D} \)-Weierstrass points of \( X \) coincides with the set of \( k \)-rational points.
Proof. The statement on $v_P(R)$ follows from [S-V, Thm. 1.5]. Let $P \in X(k)$. By Theorem 1.2.4 we know that 1 and $q + 1$ are $(D, P)$-orders. We consider two cases:

(1) $v_P(y) = 1$: With (2.2) this implies statement (ii).

(2) $v_P(y) > 1$: From (2.2) it follows $n v_P(y) = q + 1$ and then we obtain statement (i).

Let $P \not\in X \setminus X(k)$. By Theorem 1.2.4 we have that $j_{n+1}(P) = q$. If $v_P(y) > 1$, then from (2.2) we get $n v_P(x) = q = mn - 1$ and hence $n = 1$. Since by hypothesis $n > 1$ then $v_P(y) = 1$. This finish the proof of the lemma.

Let $T_1$ (resp. $T_2$) denote the number of points $P \in X(k)$ whose $(D, P)$-orders are of type (i) (resp. type (ii)) in Lemma 2.1.2. Thus by (1.2) we have

$$\deg(R) = (n(n + 1)/2 + q)(2g - 2) + (n + 2)(q + 1) = w_1 T_1 + T_2,$$

and by Riemann-Hurwitz applied to $y : X \to \mathbb{P}^1$

$$2g - 2 = -2m + (m - 1) T_1.$$

Consequently, since $T_1 + T_2 = \#X(k) = q^2 + 2gq + 1$, from the above two equations we obtain Proposition 2.1.1.

Now we are going to prove the uniqueness part of the result. To begin with we generalize [R-Sti, Lemma 5].

Lemma 2.1.3. Let $X$ be a curve satisfying the hypotheses of Proposition 2.1.1. Take $y$ as in (2.1). Then $k(X) \mid k(y)$ is a Galois cyclic extension.

Proof. Consider $y : X \to \mathbb{P}^1(\bar{k})$ as a map of degree $m = m_1$. From the proof of Lemma 2.1.2 we see that $y$ has $(q + 1)$ ramified points. Moreover, all of them are rational and totally ramified.

Claim. Let $P \in k \cup \{\infty\}$ such that $\#y^{-1}(P) = m$. Then $y^{-1}(P) \subseteq X(k)$.

Proof (Claim). Let $P_1, \ldots, P_r \in k \cup \{\infty\}$ which are not ramified for $y$. Then $r \leq q^2 - q$. Let $n_i = \#y^{-1}(P_i) \leq m$. Since $2g = (q - 1)(m - 1)$ by Proposition 2.1.1, then we have

$$(q^2 - q)m = \#X(k) - q - 1 = \sum_{i=1}^{r} n_i,$$

from where it follows that $r = q^2 - q$ and $n_i = m$ for each $i$.

Now it follows that $k(X) \mid k(y)$ is Galois as in the proof of [R-Sti, Lemma 5]. It is cyclic because there exists rational points that are totally ramified for $y$.

Proposition 2.1.4. Let $X$ be a curve as in Proposition 2.1.1. Then $X$ is $k$ isomorphic to $\mathcal{H}_{m_1, q}$.

Proof. Let $y$ be as in (2.1).

Claim 1. $X$ has a model plane given by an equation of type

$$f(y) = v^m,$$

where $f \in k[T]$ with $\deg(f) = q$, $f(0) = 0$, and $v \in L(q P_0)$. 

Proof. (Claim 1.) We know that $k(X)/k(y)$ is cyclic (Lemma 2.1.3). Let $\sigma$ be a generator of $k(X)/k(y)$. Set $V := \text{L}(qP_0)$, $U := \text{L}((n-1)mP_0)$. Then $\sigma | V \in \text{Aut}(V)$ and $\sigma | U = \text{id} | U$. Since $p \nmid m$ we then have that $\sigma | V$ is diagonalizable with an eigenvalue $\lambda$ a primitive $m$-root of unity in $k$. Let $v \in V \setminus U$ be the corresponding eigenvector for $\lambda$. Now since $\text{Norm}_{k(X)/k(y)}(v) = -v^m$ and since $v \in \text{L}(qP_0)$ we conclude the existence of $f \in k[T]$ such that $f(y) = v^m$ and $\deg(f) = q$. Finally from the fact that $y$ has exactly $(q+1)$ rational points as totally ramified points, it follows that $f$ splits into linear factors in $k[T]$. Hence we can assume $f(0) = 0$.

Now from the claim in the proof of Lemma 2.1.3, Claim 1 and $nm = q + 1$ it follows that $f^n(\alpha) - f^{aq}(\alpha) = 0$ for $\alpha \in k$, and hence we obtain

$$(*) \quad f^n(T) \equiv f^{aq}(T) \pmod{T^{q^2} - T}.$$ 

Set $f(T) = \sum_{i=1}^{q^2} a_i T^i$, $f^n(T) = \sum_{i=1}^{q^2} b_i T^i$.

Claim 2. $a_1 \neq 0$, $a_i = 0$ for $2 \leq i \leq q - 1$.

Proof. (Claim 2). $a_1 \neq 0$ follows from $(*)$ and $f(0) = 0$. Suppose that $\{2 \leq i \leq q - 1 : a_i \neq 0\} \neq \emptyset$. Set $t := \min\{1 \leq i \leq q - 1 : a_i \neq 0\}$ and $j := \max\{1 \leq i \leq q - 1 : a_i \neq 0\}$. Due to the facts: multiplication by $q$ gives an automorphism of $\mathbb{Z}/(q^2-1)\mathbb{Z}$, and $n-1+t < q^2$ we then get $b_{n-1+qj} = b_{n+1}^{qj} = na_n^{-1}a_j \neq 0$. Then $nq = \deg(f) \geq n - 1 + qj$ implies together with $2n \leq q + 1$ that

\[(\dagger) \quad j + n - 1 < q.\]

Then from $(*)$ we have $b_{t+n-1} = na_n^{-1}a_1 \neq 0$. Then again by $(*)$ and by $(\dagger)$ it follows that $b_{q(t+n-1)} = b_{t+n-1}^{q} \neq 0$ which implies $nq = \deg(f^n) \geq q(t+n-1)$. But this contradicts to $t \geq 2$. Thus $a_i = 0$ for $2 \leq i \leq q - 1$ and we are done.

Write $f(T) = aT^q + bT$, $a, b \in k^*$. By Claim 1 we have that

$$f(k) \subseteq \{\beta^m : \beta \in k\} = \cup q^{-1} \xi^m F_q,$$

where $\xi$ is a primitive element of $k$. Now since $f(k)$ is a one dimensional $k$- space, it follows that there exists $i \in \{0, \ldots, n-1\}$ such that $f(k) = \xi^m F_q$. Set $x_1 := \xi^{-t}x$, $y_1 := ey$, with $e$ being the unique element of $k^*$ such that

$$\text{Trace}_{F_q}^k(\epsilon \alpha) = \xi^{-im}f(\alpha) \forall \alpha \in k.$$ 

These functions fulfill $y^q_1 + y_1 = x^m_1$ and we finish the proof of Proposition 2.1.1.

Now the proof of Theorem 0.1 (i) follows from the last two propositions.

Proof. (Corollary 0.2). By Theorem 0.1 we have two possibilities:

(1) $nm_1 = q + 1$: Then $2g = (m_1-1)(q-1)$ and statement (i) follows from the hypothesis on $g$.

(2) $nm_1 = q$: Here from $(q-1)(q+1)/(q+1) - 1 < 2g$, (1.6) and $n < q$ we found $t \geq n$. The remaining part of (ii) follows from $2g \leq (q-1)(q+1)/2 - 1$.

Corollary 2.1.5. Let $X$ be a maximal curve with genus $g = (q-1)^2/4$. Then one of the following possibilities is satisfied:

(i) $X$ is $k$-isomorphic to $H_{q+1,q}$ or

(ii) For every point $P \in X(k)$ the first three non-gaps at $P$ are $\{q-1, q, q+1\}$. 
Proof. From the hypothesis on \( g \) and from (1.5) (applied to \( g_{n+1}^{n+1} \)) we conclude \( n + 1 \leq 3 \). Then by [F-T] we must have \( n + 1 = 3 \). Let \( P \in X(k) \) and let \( m,q,q + 1 \) be the first three non-gaps. Then \( 2m \geq q + 1 \) due to (1.6). Moreover, \( g \leq g' \), where \( g' \) is the genus of the semigroup \( \langle m,q,q + 1 \rangle \). We bound from above \( g' \) according to Selmer [Sel, §3.II]. From that reference it follows that \( g' \) will be larger if \( \gcd(m,q) = 1 \). So let assume this. Define \( s,t \) by \( q + 1 = sq - tm, 1 \leq s < m, t > 0 \). Write \( m = us + r, 0 \leq r < s \). Then we have ([p.6 loc. cit.])

\[
2g' = (m - 1)(q - 1) - ut(m - s + r).
\]

Hence by the hypothesis on \( g \) we then have

\[
2ut(m - s + r) \leq (q - 1)(2m - q - 1),
\]

and now it is easy to see that \( 2m = (q + 1) \) or \( m = q - 1 \). The first case for some point \( P \in X(k) \), and Theorem 0.1 (i) imply the result.

2.2. Case: \( nm_1 = q \). As in the proof of Lemma 2.1.2 here one also has \( \epsilon_i = \nu_i \) for \( i = 0,1, \ldots, n - 1; \epsilon_n = n \). However we cannot apply [S-V, Thm. 1.5] to compute \( v_p(R) \) for \( P \in X(k) \).

If one can show that \( \pi : X \to \mathbb{P}^{n+1} \) is a closed embedding, then from Proposition 1.2.7 we would have \( 2g = q(m_1(P) - 1) \) for \( P \in X(k) \).

Remark 2.2.1. The hypothesis on the first non-gap of Theorem 0.1 is necessary. In fact, consider the curve from Serre’s list (see [Se, §4]) over \( \mathbb{F}_{25} \), \( g = 3 \). Then it is maximal. Let \( m,5,6 \) be the first non-gaps at \( P \in X(\mathbb{F}_{25}) \). If \( m = 3 \) from Theorem 0.1 (i) we would have \( g = 4 \). Thus \( m = 4 \).

Acknowledgments. The paper was written while the first author was visiting the Instituto de Matematica Pura e Aplicada, Rio de Janeiro (Oct. 1995 - Jan. 1996). This visit was supported by Cnpq. The second author is supported by a grant from the International Atomic Energy Agency and UNESCO.

REFERENCES


