BULLETIN OF THE BRAZILIAN MATHEMATICAL SOCIETY

Bull Braz Math Soc, New Series 36(1), 39-58
© 2005, Sociedade Brasileira de Matemática

Eventually minimal curves

Paulo H. Viana and Jaime E. A. Rodriguez

Abstract. A curve defined over a finite field is maximal or minimal according to whether the number of rational points attains the upper or the lower bound in Hasse-Weil's theorem, respectively. In the study of maximal curves a fundamental role is played by an invariant linear system introduced by Rück and Stichtenoth in [6]. In this paper we define an analogous invariant system for minimal curves, and we compute its orders and its Weierstrass points. In the last section we treat the case of curves having genus three in characteristic two.

Keywords: Hasse-Weil bound, rational point, Weierstrass point, minimal curve, gap, genus, zeta funtion.

Mathematical subject classification: 11G20, 14H45.

1 Zeta functions of eventually minimal curves

The study of an algebraic curve C defined over finite field $\mathbf{F}_q$ is centered around its *zeta function*, introduced by Emil Artin in analogy with the classical Riemann zeta function. It may be defined as the enumerating function of the set of positive divisors of $C/\mathbf{F}_q$ counted by degree,

$$Z_{C/\mathbf{F}_q}(t) = \sum_{n\geq 0} A_{n,\mathbf{F}_q} t^n, \qquad \text{where} \qquad A_{n,\mathbf{F}_q} := card\ \mathcal{D}^n_{\mathbf{F}_q},$$

$\mathcal{D}^n_{\mathbf{F}_q}$ denoting the set of positive divisors of degree n defined over $\mathbf{F}_q$. For the function field of the curve the function $\zeta_{C/\mathbf{F}_q}(s) := Z_{C/\mathbf{F}_q}(q^{-s})$ is the analogue of the classical zeta function $\zeta(s) = \sum_{n\geq 1} n^{-s}$.

It is known that $Z_{C/\mathbf{F}_q}(t)$ is a rational function given by

$$Z_{C/\mathbf{F}_q}(t) = \frac{L_{C/\mathbf{F}_q}(t)}{(1-t)(1-qt)},$$

Received 12 July 2004.

where $L_{C/\mathbf{F}_q}(t)$ is a polynomial with integer coefficients having degree twice the genus g of the curve. The theorem of Riemann-Roch is expressed as the *functional equation*

$$\begin{aligned} Z_{C/\mathbf{F}_q}(t) &= q^{g-1}t^{2g-2}Z_{C/\mathbf{F}_q}\left(\frac{1}{qt}\right) \quad \text{or also} \\ L_{C/\mathbf{F}_q}(t) &= q^g t^{2g} L_{C/\mathbf{F}_q}\left(\frac{1}{qt}\right). \end{aligned} \tag{1.1}$$

The analogue of the Riemann hypothesis for the function $\zeta_{C/\mathbf{F}_q}(s)$ was proved by Helmut Hasse in case of genus 1 and in general by André Weil, and may be stated as

Theorem 1.2 (Hasse-Weil).

$$\textit{If} \quad L_{C/\mathbf{F}_q}(t) = \prod_{i=1}^{2g}(1-\alpha_i t) \quad \textit{then} \quad |\frac{\alpha_i}{\sqrt{q}}| = 1. \tag{1.2}$$

As a consequence one has the bound of Hasse-Weil

$$|A_{1,\mathbf{F}_q} - (q+1)| \leq 2g\sqrt{q}. \tag{1.3}$$

All this is established in a quite elementary and elegant setup in [7]. The curve C is maximal *or* minimal *if*

$$A_{1,\mathbf{F}_q} - (q+1) = 2g\sqrt{q} \qquad \textit{or} \qquad A_{1,\mathbf{F}_q} + (q+1) = 2g\sqrt{q},$$

respectively. It is immediate that $C/\mathbf{F}_q$ is maximal or minimal according to whether

$$L_{C/\mathbf{F}_q}(t) = (1+\sqrt{q}t)^{2g} \qquad \textit{or} \qquad L_{C/\mathbf{F}_q}(t) = (1-\sqrt{q}t)^{2g}, \tag{1.4}$$

respectively.

Maximal curves were used in the construction of good Goppa codes, and their study was renewed on account of this surprising source of applications. Minimal curves have had much less attention. But from the *constant field extension formula* [7, Theo. V.1.15, p. 166]: with notations as in (1.2)

$$L_{C/\mathbf{F}_{q^r}}(t) = \prod_{i=1}^{2g}(1-\alpha_i^r t), \tag{1.5}$$

it follows that for a maximal curve $C/\mathbf{F}_q$ the constant field extensions $C/\mathbf{F}_{q^r}$ are maximal or minimal according to whether r is even or odd, while for a minimal curve $C/\mathbf{F}_q$ the constant field extensions $C/\mathbf{F}_{q^r}$ are always minimal. If one plans to use the tool of constant field extensions it seems thus unwise to study only maximal curves. A curve $C/\mathbf{F}_q$ is *eventually minimal* or *eventually maximal* if for some integer r it happens that $C/\mathbf{F}_{q^r}$ is minimal or maximal; from what was just seen, a eventually maximal curve is eventually minimal. Examples below show that the converse is not true.

Equations (1.4) and (1.5) have other easy consequences. For instance,

Proposition 1.6. *Let C be a curve defined over $\mathbf{F}_q$. The curve $C/\mathbf{F}_{q^2}$ is maximal if and only if*

$$L_{C/\mathbf{F}_q}(t) = (1+qt^2)^g.$$

If q is not a perfect square then the curve $C/\mathbf{F}_{q^2}$ is minimal if and only if

$$L_{C/\mathbf{F}_q}(t) = (1-qt^2)^g.$$

Proof. Sufficiency is a direct application of (1.5). For necessity, if the numerator of the zeta function of $C/\mathbf{F}_q$ is given as in (1.2) then $C/\mathbf{F}_{q^2}$ is maximal (resp. minimal) only if for all $i = 1, \cdots, 2g$ one has $\alpha_i = \pm\sqrt{-q}$ (resp., $\alpha_i = \pm\sqrt{q}$), with, say, N choices of $+$ and $2g-N$ choices of $-$. Hence,

$$L_{C/\mathbf{F}_q}(t) = (1-\sqrt{-q}t)^N(1+\sqrt{-q}t)^{2g-N},$$

(resp., $L_{C/\mathbf{F}_q}(t) = (1-\sqrt{q}t)^N(1+\sqrt{q}t)^{2g-N}$). Now the coefficient of t^{2g-1},

$$(-1)^N 2(N-g)(\sqrt{-q})^{2g-1}, \qquad (\text{resp., } (-1)^N 2(N-g)(\sqrt{q})^{2g-1}),$$

is an integer, and thus one certainly has $N = g$ in the maximal case or in the minimal case if q is not a perfect square.

Corollary 1.7. *Let C be a minimal curve of odd genus g defined over $\mathbf{F}_q$. If $C/\mathbf{F}_{q^2}$ is minimal then q is a square.*

Proof. This is a consequence of the fact that

$$(1-qt^2)^g = 1 - \cdots + (-q)^g t^{2g},$$

and the fact that the coefficient of t^{2g} is always q^g.

Corollary 1.8. *Let C be a curve defined over $\mathbf{F}_q$. Then $C/\mathbf{F}_{q^2}$ is maximal if and only if*

$$L_{C/\mathbf{F}_{q^{2r}}}(t) = \begin{cases} (1+q^r t)^{2g} & \textit{for odd } r \\ (1-(-q)^{r/2}t)^{2g} & \textit{for even } r. \end{cases}$$

If q is not a perfect square then the curve $C/\mathbf{F}_{q^2}$ is minimal if and only if

$$L_{C/\mathbf{F}_{q^{2r}}}(t) = \begin{cases} (1-q^r t)^{2g} & \textit{for odd } r \\ (1-q^{r/2}t)^{2g} & \textit{for even } r. \end{cases}$$

Proof. Direct consequence of (1.5).

A consequence of the Riemann hypothesis (1.2) is that the essential information of a zeta function $L_{C/\mathbf{F}_q}(t)$ is contained in the arguments θ_j of the inverses $\alpha_j = \sqrt{q}e^{i\theta_j}$ of its roots. It seems natural then to consider, through the change of variables $u = \sqrt{q}t$, the *normalized polynomial*

$$\Lambda_{C/\mathbf{F}_q}(u) = L_{C/\mathbf{F}_q}(q^{-1/2}u);$$

now Riemann-Roch duality is expressed as

$$\Lambda_{C/\mathbf{F}_q}(u) = u^{2g}\Lambda_{C/\mathbf{F}_q}(u^{-1}),$$

and $\Lambda_{C/\mathbf{F}_q}(u)$ has all roots in the complex unitary circle $\{|u| = 1\}$. The normalized polynomial for maximal and minimal curves $C/\mathbf{F}_q$ are given by

$$\Lambda_{C/\mathbf{F}_q}(u) = (1+u)^{2g} \qquad \text{and} \qquad \Lambda_{C/\mathbf{F}_q}(u) = (1-u)^{2g},$$

respectively. The constant field extension formula for normalized polynomials states that

$$\Lambda_{C/\mathbf{F}_q}(u) = \prod(u-u_i) \qquad \text{implies} \qquad \Lambda_{C/\mathbf{F}_{q^r}}(u) = \prod(u-u_i^r).$$

Theorem 1.9. *Suppose q is a perfect square. For a curve $C/\mathbf{F}_q$ the following are equivalent:*

(a) *$C/\mathbf{F}_q$ is eventually minimal.*

(b) *Any root of $\Lambda_{C/\mathbf{F}_q}(u)$ is cyclotomic.*

(c) *The normalized polynomial has integer coefficients:*

$$\Lambda_{C/\mathbf{F}_q}(u) \in \mathbf{Z}[u].$$

Proof. As q is a square by hypothesis, the normalized polynomial $\Lambda_{C/\mathbf{F}_q}(u)$ has rational coefficients.

A curve $C/\mathbf{F}_q$ is eventually minimal if and only if $\Lambda_{C/\mathbf{F}_{q^r}}(u) = (1-u)^{2g}$ for some r, and from the constant field extension formula this implies that any root of its normalized polynomial is cyclotomic. That any algebraic integer which, along with all of its conjugates, lies on the unit circle, is a cyclotomic root is a standard fact (for example, [10]). This establishes the equivalence of (a) and (b).

That (c) implies (b) is clear. If $\Lambda_{C/\mathbf{F}_q}(u)$ does not have integer coefficients then in its prime factorization in $\mathbf{Q}[u]$ there will be some prime factor not in $\mathbf{Z}[u]$, whose roots will not be algebraic integers, and hence not cyclotomic. This finishes the proof.

2 The invariant system of minimal curves

Let C be a curve of genus g and $\mathcal{D} = g^r_d$ be a base-point-free system on C. Then associated to a point $P \in C$ we have the Hermitian P-invariants $j_0(P) = 0 < j_1(P) < \ldots < j_r(P) \leq d$ of $\mathcal{D}$ (also called the $(\mathcal{D}, P)$-orders). This sequence is the same for all but finitely many points. These finitely points P, where exceptional $(\mathcal{D}, P)$-orders occur, are called the $\mathcal{D}$-Weierstrass points of C. The Weierstrass points of the curve are those exceptional points obtained from the canonical linear system. A curve is called *nonclassical* if the generic order sequence (for the canonical linear system) is different from $\{0, 1, \ldots, g-1\}$.

Associated to the linear system $\mathcal{D}$ there exists a divisor R supporting exactly the $\mathcal{D}$-Weierstrass points. Let $\epsilon_0 < \epsilon_1 < \ldots < \epsilon_r$ denote the $(\mathcal{D}, Q)$-orders for a generic point $Q \in C$. Then we have $\epsilon_i \leq j_i(P)$, for each $i = 0, 1, 2, \ldots, r$ and for any point P, and also that

$$\deg(R) = (\epsilon_1 + \cdots + \epsilon_r)(2g-2) + (r+1)d.$$

Now, in the study of a maximal curve $C/\mathbf{F}_{q^2}$ a decisive role is played by the *invariant linear system*, defined as:

$$\mathcal{D} := |(q+1)P_0|.$$

Here $P_0 \in C(\mathbf{F}_{q^2})$ is any rational point: it is an important fact that $\mathcal{D}$ is independent of P_0. See, for instance, [6], [2], [3], [1]. The importance of this system is a consequence of the following linear equivalence

$$qP + \mathcal{F}_{q^2}(P) \sim (q+1)P_0,$$

valid for any point P in the maximal curve $C/\mathbf{F}_{q^2}$. Here $\mathcal{F}_{q^2}$ denotes the Frobenius on the curve. This comes from the fact [6, proof of lemma 1, p. 185] that the Frobenius (relative to $\mathbf{F}_{q^2}$) acts on the Jacobian $\mathcal{J}_C$ of C as multiplication by $-q$. It follows that in any maximal curve the *Hasse-Witt invariant* vanishes.

For a minimal curve $C/\mathbf{F}_{q^2}$ one has, *mutatis mutandis*, perfect analogues of these concepts: the Frobenius (relative to $\mathbf{F}_{q^2}$) acts on the Jacobian $\mathcal{J}_C$ of C as multiplication by q, one has the *fundamental linear equivalence*

$$qP - \mathcal{F}_{q^2}(P) \sim (q-1)P_0,$$

valid for any point P in the minimal curve $C/\mathbf{F}_{q^2}$, and the linear system

$$\mathcal{E}_{q^2} := |(q-1)P_0|$$

is an invariant of the minimal curve $C/\mathbf{F}_{q^2}$ in the sense that it does not depend on P_0. As a consequence, in any minimal curve the Hasse-Witt invariant also vanishes.

This section is modelled on the theory developped in [2], where the authors apply the Stöhr-Voloch theory of Weierstrass points ([8]) to the invariant system of a maximal curve. Here we fix a minimal curve $C/\mathbf{F}_{q^2}$ and consider the above invariant system $\mathcal{E}_{q^2} = |(q-1)P_0|$.

The study of possible genera of maximal curves is very rich: for instance, it is known that for $C/\mathbf{F}_{q^2}$ maximal its genus g is bounded by $g \leq q(q-1)/2$, with equality only for the Hermitian curves ([4], [6]).

For minimal curves the following genus bound was found by Arnaldo Garcia.

Theorem 2.1. *Let $C/\mathbf{F}_{q^2}$ be a minimal curve having genus g. Then*

$$g \leq \frac{q}{2}.$$

The invariant system $\mathcal{E}_{q^2}$ is non-special, i.e, the index of speciality is zero.

Proof. A minimal curve $C/\mathbf{F}_{q^2}$ has necessarily at least one rational point over $\mathbf{F}_{q^2}$, as

$$card(C(\mathbf{F}_{q^2})) = q^2 + 1 - 2gq = q(q-2g) + 1 > 0$$

as follows from taking the remainder mod q. The upper bound then follows, and as it implies $2g - 1 \leq q - 1$, the statement about the invariant system is a consequence of the Riemann-Roch theorem. This finish the proof.

This bound is sharp, as the hyperelliptic curve $y^2+y+x^5+\delta^3 = 0$ has genus 2 and is minimal over $\mathbf{F}_{q^2} = \mathbf{F}_{16}$, having just one rational point over $\mathbf{F}_{16} = \mathbf{F}_2[\delta]$, for $\delta^4 = \delta+1$. The unique rational point is the place corresponding to the unique branch at the singular infinite point.

In [3] the case of maximal curves with classical Weierstrass gaps is treated; because of the Prop. 1.7 (i) in [2, p. 37], in this case the invariant system $\mathcal{D}$ is non-special.

On what follows let

$$l = q - g$$

be the dimension of the invariant system $\mathcal{E}_{q^2}$.

Theorem 2.2. *Let $C/\mathbf{F}_{q^2}$ be a minimal curve having positive genus $g > 0$. Any rational point over $\mathbf{F}_{q^2}$ is a Weierstrass point for $\mathcal{E}_{q^2}$.*

Proof. Denoting by $\{j_0, \dots , j_{l-1}\}$ the orders of $\mathcal{E}_{q^2}$ at the rational point P_0, it follows from the fundamental linear equivalence that $j_{l-1} = q - 1$.

Denote by $\{\epsilon_0, \dots , \epsilon_{l-1}\}$ the generic orders of $\mathcal{E}_{q^2}$. If P_0 were a generic point of $\mathcal{E}_{q^2}$ then $\epsilon_{l-1} = j_{l-1} = q - 1$, and as $q = p^m$ any integer $\epsilon < q - 1$ is p-adically smaller than

$$q - 1 = p^m - 1 = (p - 1)p^{m-1} + (p - 1)p^{m-2} + \cdots + (p - 1)p + (p - 1),$$

and the corollary 1.9 in [8, p. 7] assures that $\epsilon_i = i$ for $i = 0, \dots , l - 1$, and hence that

$$q - 1 = \epsilon_{l-1} = l - 1 = q - g - 1,$$

but then it follows that $g = 0$, a contradiction. The theorem is proved.

The notation in the proof will be used on what follows. Also, the *Weierstrass semigroup*, or semigroup of non-gaps, at a point $P \in C$ is defined to be

$$\begin{aligned}\mathcal{W}_P &:= \{\, m \in \mathbf{N} \mid \text{there is a function } f \in \overline{\mathbf{F}_{q^2}}(C) \text{ such that } \operatorname{div}_\infty(f) = mP \,\} \\ &= \{\, 0 = m_0(P) < m_1(P) < m_2(P) < \cdots \},\end{aligned}$$

so that

$$\dim \mathcal{L}(dP) = card\{\, i \geq 0 \mid m_i(P) \leq d \,\}.$$

As a consequence of the fundamental linear equivalence the invariant system $\mathcal{I}_{q^2} = |(q-1)P_0|$ has no base point. The system $|qP_0|$ may have P_0 as a base point. Define

$$s := \dim \mathcal{L}(qP_0) = \begin{cases} l & \text{if } q \text{ is a gap at } P_0, \\ l+1 & \text{if } q \text{ is a non-gap at } P_0. \end{cases}$$

Then

$$0 < m_1(P_0) < \cdots < m_{s-1}(P_0) \leq q < m_s(P_0),$$

with $m_{s-1}(P_0) = q = m_l(P_0)$ if and only if q is a non-gap at P_0. In any case, if $m(P_0) \in \mathcal{W}_{P_0}$ is a non-gap at P_0 satisfying $m(P_0) < q$ then

$$m(P_0) \in \{\, 0, m_1(P_0), \cdots, m_{l-1}(P_0) \,\}.$$

By definition of a non-gap there is a positive divisor E not having P_0 in its support such that $E \sim m(P_0)P_0$.

Adding the divisor $(q - m(P_0) - 1)P_0$ to this linear equivalence yields

$$E + (q - m(P_0) - 1)P_0 \sim (q-1)P_0,$$

and thus the following are orders of $\mathcal{I}_{q^2}$ at P_0:

$$0 \leq q - m_{l-1}(P_0) - 1 < \cdots < q - m_1(P_0) - 1 < q - 1.$$

As there are exactly l orders of $\mathcal{I}_{q^2}$ at any point, the following are exactly the orders of $\mathcal{I}_{q^2}$ at P_0:

$$\{j_0, \cdots, j_{l-1}\} = \{q - m_{l-1}(P_0) - 1, \cdots, q - m_1(P_0) - 1, q - 1\}.$$

From the fact that P_0 is not a base point of $\mathcal{I}_{q^2}$ it follows that $j_0 = 0$, and thus $m_{l-1}(P_0) = q - 1$.

As a result,

Theorem 2.3. *Let $C/\mathbf{F}_{q^2}$ be a minimal curve, and let P_0 be a rational point. The canonical sequence of orders at P_0 determines the order sequence of $\mathcal{I}_{q^2}$ at P_0 in the following way: if*

$$0 < m_1(P_0) < \cdots < m_{l-1}(P_0)$$

are the first non-gaps then the orders of $\mathcal{E}_{q^2}$ at P_0 are

$$0 = q - m_{l-1}(P_0) - 1 < \cdots < q - m_1(P_0) - 1 < q - 1.$$

If j is an order of $\mathcal{E}_{q^2}$ at a rational point then $q - j - 1$ is a non-gap at this point, and in particular $q - 1$ is a non-gap at the point.

Now let P be a non rational point. The space $\mathcal{L}(qP)$ always has a function f which does not vanish at $\mathcal{F}_{q^2}(P)$, so that the inclusion

$$\mathcal{L}(qP - \mathcal{F}_{q^2}(P)) \subset \mathcal{L}(qP)$$

is proper, and hence

$$\dim \mathcal{L}(qP) = l + 1.$$

Thus,

Theorem 2.4. *Let $C/\mathbf{F}_{q^2}$ be a minimal curve and let $P \notin C(\mathbf{F}_{q^2})$ be a non-rational point. The first $l + 1$ non-gaps at P satisfy*

$$0 < m_1(P) < \cdots < m_l(P) \leq q < m_{l+1}(P).$$

For a non-gap $m(P) \in \mathcal{W}_P$ at P there exists, by definition of gap, a positive divisor E not having P in its support such that

$$E \sim m(P) \cdot P.$$

As for any positive non-gap one has $\dim \mathcal{L}(m(P)P) > 1$, it is possible to choose the positive divisor E having $\mathcal{F}_{q^2}(P)$ in its support, and then, adding to the above linear equivalence relation the divisor $(q - m(P))P - \mathcal{F}_{q^2}(P)$ (as in [2, Prop. 1.5, p. 35]) one has

$$E + (q - m(P))P - \mathcal{F}_{q^2}(P) \sim qP - \mathcal{F}_{q^2}(P) \sim (q-1)P_0,$$

where the divisor at the left-hand side is positive, and therefore $q - m(P)$ is an order of $\mathcal{E}_{q^2}$ at P. As there are exactly l orders of $\mathcal{E}_{q^2}$ at any point, these are precisely the orders of $\mathcal{E}_{q^2}$ at P. This may be stated as

Theorem 2.5. *Let $C/\mathbf{F}_{q^2}$ be a minimal curve and let $P \notin C(\mathbf{F}_{q^2})$ be a non-rational point. The order sequence of $\mathcal{E}_{q^2}$ at P is*

$$\{\, j_0, \cdots, j_{l-1} \,\} = \{\, q - m_l(P), \cdots, q - m_1(P) \,\}.$$

In particular, from $j_0 = 0$ it follows that $m_l(P) = q$. So if j is an order of $\mathcal{E}_{q^2}$ at P then $q - j$ is a non-gap at P.

The Theorems 2.2–2.5 give a description of the Weierstrass points for the invariant system $\mathcal{E}_{q^2}$ of a minimal curve which is more complete than the corresponding available for a maximal curve ([2, Theo. 1.4 and Prop. 1.5]).

Theorem 2.6. *Let $C/\mathbf{F}_{q^2}$ be a minimal curve of genus g. Then the Weierstrass points of $\mathcal{E}_{q^2}$ are exactly the rational points over $\mathbf{F}_{q^2}$ and the canonical Weierstrass points. The invariant system $\mathcal{E}_{q^2}$ is classical if and only if the canonical system is so.*

If the canonical system is classical then there will be a non-rational point P which is a generic point for the canonical system, and then

$$m_i(P) = g + i \quad \text{for} \quad i \geq 1,$$

and thus

$$j_{i-1} = q - g - i \quad \text{for} \quad i = 1, \dots, l,$$

from Theorem 2.5, so that the invariant system is classical.

For a point $P \in C(\mathbf{F}_{q^4}) \setminus C(\mathbf{F}_{q^2})$, applying the Frobenius morphism $\mathcal{F}_{q^2}$, as in [2, Prop. 1.5 (iv), p. 35], to the fundamental linear equivalence relation yields

$$q\mathcal{F}_{q^2}(P) - \mathcal{F}^2_{q^2}(P) \sim (q-1)P_0 \sim qP - \mathcal{F}_{q^2}(P),$$

or

$$(q+1)\mathcal{F}_{q^2}(P) \sim (q+1)P.$$

As a consequence,

Proposition 2.7. *In any minimal curve $C/\mathbf{F}_{q^2}$ a point $P \in C(\mathbf{F}_{q^4}) \setminus C(\mathbf{F}_{q^2})$ has $q + 1$ as a non-gap.*

3 The case of genus three and characteristic two

The connections shown above between the invariant and the canonical systems of a minimal curve suggest that even though minimality and maximality are arithmetical conditions, they are bound to have strong geometrical consequences. In this section these arithmetical-geometrical relations are explored in the situation of curves having genus three and characteristic two. This case is extremely rich, for a number of reasons: In the first place, it is known that these curves are canonically classical ([5]). Also, such a curve is canonically a smooth plane quartic, and the Riemann-Roch duality is just the classical projective duality in the projective plane. Finally, in characteristic two the theory of theta characteristics is totally different. This theory, given in [9], will be very important on what follows.

An example of the interplay between Algebra and Geometry in this situation is given by

Theorem 3.1. *An eventually minimal curve $C/\mathbf{F}_{q^2}$ having genus three and defined over a field of characteristic two is given as a smooth quartic with exactly one hyperflex.*

Proof. The conclusion is a geometrical statement which may be checked over the algebraic closure of the constant field, and so the curve $C/\mathbf{F}_{q^2}$ may be assumed already minimal. Canonical order sequences in genus three and characteristic two may be the classical one 0,1,2 (for a generic point), 0,1,3 (for a simple flex) or 0,1,4 (for a hyperflex). From the Theorem 1.5 in [8] it follows that the Weierstrass weight if these points is 0,1 or greater than 2, respectively. The total number of Weiertrass points, counted with weights, is 24. On the other hand, the number of bitangents is 7,4,2 and 1 depending on the values 3,2,1 or 0 of the Hasse-Witt invariant, respectively ([9, Sect. 3]).

For a minimal curve $C/\mathbf{F}_{q^2}$ the Hasse-Witt invariant vanishes, and thus C has only one bitangent. Also, a hyperflex P has a tangent which has intersection divisor $4P$ with the curve, and so it is a bitangent, and thus the uniqueness in the statement is proved. If the minimal curve C has no hyperflex then C has a unique bitangent whose intersection divisor has the form

$$2(P_0 + Q_0) \qquad \text{with} \qquad P_0 \neq Q_0.$$

The curve will then have 24 Weierstrass points, all of them with order sequence 0,1,3. Using a minimality preserving constant field extension, if necessary, P_0, Q_0 and all Weierstrass points may be assumed rational.

For a minimal curve the numerator of the zeta function is given by

$$L_{C/\mathbf{F}_{q^2}}(t) = (1-qt)^6 = 1 - 6qt + 15q^2t^2 - 20q^3t^3 + 15q^4t^4 - 6q^5t^5 + q^6t^6,$$

and it follows from the constant field extension formula (1.5) that

$$\begin{aligned} A_{1,\mathbf{F}_{q^2}} &= q^2 - 6q + 1 \\ A_{2,\mathbf{F}_{q^2}} &= q^4 - 6q^3 + 16q^2 - 6q + 1. \end{aligned}$$

Now each of the $q^4 + q^2 + 1$ lines L of the projective plane $\mathbf{P}(\mathbf{F}_{q^2})$ falls into ten exclusive types according to the intersection divisor $C \cdot L$. These ten types are labelled and counted as follows: $\kappa_{1,1,1,1}$ is the number of positive canonical divisors K of the form $\sum_i P_i$ for $P \in C(\mathbf{F}_{q^2})$ rational and *distinct*:

$$\kappa_{1,1,1,1} := card\Big\{ \sum_i P_i \mid P_i \text{ rational, distinct and collinear} \Big\}.$$

Similarly,

$$\kappa_{2,1,1} := card\Big\{ 2P_1 + P_2 + P_3 \mid P_i \text{ rational, distinct and collinear} \Big\},$$

$$\kappa_{3,1} := card\Big\{ 3P_1 + P_2 \mid P_i \text{ rational, distinct and collinear} \Big\},$$

and

$$\kappa_4 := card\Big\{ 4P \mid P \text{ rational} \Big\}.$$

Here it is undestood that in the divisors $3P_1 + P_2$ counted by $\kappa_{3,1}$ the rational point P_1 is a flex, and similarly for the other cases. Also,

$$\begin{aligned} \kappa_{d,1,1} := card\{ D + P_2 + P_3 \mid P_i &\text{ rational, distinct and} \\ &D = P + \mathcal{F}_{q^2}(P) \text{ for } P \in C(\mathbf{F}_{q^4}) \setminus C(\mathbf{F}_{q^2}) \}, \end{aligned}$$

$$\kappa_{2,2} := card\{ 2(P_1 + P_2) \mid P_i \text{ rational, distinct} \},$$

$$\begin{aligned} \kappa_{2,d} := card\{ D + 2P \mid P &\text{ rational and} \\ &D_i = P_i + \mathcal{F}_{q^2}(P_i) \text{ for } P_i \in C(\mathbf{F}_{q^4}) \setminus C(\mathbf{F}_{q^2}) \}, \end{aligned}$$

$$\begin{aligned} \kappa_{d,d} := card\{ D_1 + D_2 \mid D_i &\text{ distinct and} \\ &D_i = P_i + \mathcal{F}_{q^2}(P_i) \text{ for } P_i \in C(\mathbf{F}_{q^4}) \setminus C(\mathbf{F}_{q^2}) \}, \end{aligned}$$

$$\begin{aligned} \kappa_{t,1} := card\{ D + P \mid P &\text{ rational and} \\ &D = Q + \mathcal{F}_{q^2}(Q) + \mathcal{F}_{q^2}^2(Q) \text{ for } Q \in C(\mathbf{F}_{q^6}) \setminus C(\mathbf{F}_{q^2}) \}, \end{aligned}$$

and finally,

$$\kappa_q := card\big\{D \mid D = Q + \mathcal{F}_{q^2}(Q) + \mathcal{F}_{q^2}^2(Q) + \mathcal{F}_{q^2}^3(Q) \\ \text{for } \; Q \in C(\mathbf{F}_{q^8}) \setminus C(\mathbf{F}_{q^2})\big\}.$$

(The subscripts d, t, q should recall *d*ouble, *t*riple and *q*uadruple). By way of contradiction it is assumed

$$\kappa_4 = 0, \qquad \kappa_{2,2} = 1, \quad \text{and} \quad \kappa_{3,1} = 24.$$

Denote by $\mathcal{D}^n_{C/\mathbf{F}_{q^2}}$ the set of positive divisors having degree n defined over $\mathbf{F}_{q^2}$, so that $\mathcal{D}^1_{C/\mathbf{F}_{q^2}} = C(\mathbf{F}_{q^2})$. The application

$$\delta : \mathcal{D}^1_{C/\mathbf{F}_{q^2}} = C(\mathbf{F}_{q^2}) \longrightarrow \mathcal{D}^2_{C/\mathbf{F}_{q^2}} \\ P \mapsto D_P \quad \text{for} \quad 2P + D_P \text{ canonical}$$

defines an injection. Similarly, for $D \in \mathcal{D}^2_{C/\mathbf{F}_{q^2}}$ let L_D be the unique line of $\mathbf{P}(\mathbf{F}_{q^2})$ such that $K_D = C \cdot L_D$ is the unique positive canonical divisor greater than D:

$$K_D = C \cdot L_D = D + E_D, \quad \text{with} \quad K_D \geq E_D \geq 0.$$

Now residuation

$$\iota : \mathcal{D}^2_{C/\mathbf{F}_{q^2}} \longrightarrow \mathcal{D}^2_{C/\mathbf{F}_{q^2}} \\ D \mapsto K_D - D = E_D$$

defines an involution satisfying

$$\iota(2P) = \delta(P) \quad \text{for} \quad P \in \mathcal{D}^1_{C/\mathbf{F}_{q^2}} = C(\mathbf{F}_{q^2}).$$

The divisor $P_0 + Q_0$ is the unique fixed point of this involution:

$$\iota(D) = D \quad \text{implies} \quad D = P_0 + Q_0.$$

It follows that there are exactly

$$\frac{A_{2,\mathbf{F}_{q^2}} - 1}{2} + 1 = \frac{q^4 - 6q^3 + 16q^2 - 6q}{2} + 1 \qquad (C_{2+2})$$

ordered pairs of divisors of degree two $D, \iota(D) = E$ with $D + E$ canonical. Geometrically such a pair of divisors determines a unique line L with intersection divisor

$$C \cdot L = D + E \qquad \text{with} \qquad D, E \in \mathcal{D}^2_{C/\mathbf{F}_{q^2}}.$$

This value counts

$$\frac{q^4 - 6q^3 + 16q^2 - 6q}{2} + 1 = \tag{$R_{2,2}$}$$
$$3\kappa_{1,1,1,1} + 2\kappa_{2,1,1} + \kappa_{2,d} + \kappa_{d,d} + \kappa_{d,1,1} + \kappa_{2,2} + \kappa_{3,1}.$$

For example, the coefficient $3 = \frac{1}{2}\binom{4}{2}$ of $\kappa_{1,1,1,1}$ counts the possible ways of forming an ordered pair of order two divisors out of four distinct rational points.

Among the $A_{3,\mathbf{F}_{q^2}}$ positive divisors of degree three there are exactly $A_{1,\mathbf{F}_{q^2}} \cdot (q^2 + 1)$ which are special. This is seen as such a divisor D is special exactly when there is a canonical divisor (necessarily uniquely determined) K_D with $K_D \geq D$, that is, geometrically a line L_D such that

$$K_D = C \cdot L_D = D + P_D.$$

Then clearly $P_D \in \mathcal{D}^1_{C/\mathbf{F}_{q^2}} = C(\mathbf{F}_{q^2})$. On the other hand the association $D \mapsto P_D$ has degree $q^2 + 1$, which is the number of lines passing through P_D. As a consequence there are exactly

$$\begin{aligned} A_{1,\mathbf{F}_{q^2}} \cdot (q^2 + 1) &= (q^2 - 6q + 1) \cdot (q^2 + 1) \\ &= q^4 - 6q^3 + 2q^2 - 6q + 1 \end{aligned} \tag{C_{3+1}}$$

lines L with intersection divisor of the form $C \cdot L = D + P$ with $D \in \mathcal{D}^3_{C/\mathbf{F}_{q^2}}$. This value counts

$$\begin{aligned} q^4 - 6q^3 + 2q^2 - 6q + 1 &= 4\kappa_{1,1,1,1} + 3\kappa_{2,1,1} + 2\kappa_{d,1,1} + \kappa_{t,1} \\ &\quad + 2 \cdot \kappa_{3,1} + 2\kappa_{2,2} + \kappa_{2,d} \\ &= 4\kappa_{1,1,1,1} + 3\kappa_{2,1,1} + 2\kappa_{d,1,1} + \kappa_{t,1} \\ &\quad + 2 \cdot 24 + 2 + \kappa_{2,d}. \end{aligned} \tag{$R_{3,1}$}$$

As each rational point has a unique tangent,

$$\begin{aligned} A_{1,\mathbf{F}_{q^2}} = q^2 - 6q + 1 &= \kappa_{3,1} + \kappa_{2,1,1} + \kappa_{2,d} + 2\kappa_{2,2} \\ &= 24 + \kappa_{2,1,1} + \kappa_{2,d} + 2. \end{aligned} \tag{R_2}$$

As for each pair of distinct rational points there is a unique secant,

$$\begin{aligned}\binom{A_{1,\mathbf{F}_{q^2}}}{2} &= \frac{(q^2-6q)(q^2-6q+1)}{2} = \frac{q^4-12q^3+37q^2-6q}{2}\\ &= \binom{4}{2}\kappa_{1,1,1,1} + \kappa_{3,1} + \binom{3}{2}\kappa_{2,1,1} + \kappa_{d,1,1} + \kappa_{2,2} \qquad (R_{1,1})\\ &= 6\kappa_{1,1,1,1} + 24 + 3\kappa_{2,1,1} + \kappa_{d,1,1} + 1.\end{aligned}$$

As for each point rational over $\mathbf{F}_{q^4}$ but not over $\mathbf{F}_{q^2}$ there is a unique secant,

$$\frac{A_{1,\mathbf{F}_{q^4}} - A_{1,\mathbf{F}_{q^2}}}{2} = \frac{q^4-7q^2+6q}{2} = \kappa_{d,1,1} + 2\kappa_{d,d} + \kappa_{2,d}. \qquad (R_d)$$

From having taking, without repetition or omission, each line in the projective plane $\mathbf{P}(\mathbf{F}_{q^2})$ it follows that

$$\begin{aligned}q^4+q^2+1 &= \kappa_{1,1,1,1} + \kappa_{2,1,1} + \kappa_{2,d} + \kappa_{d,1,1} + \kappa_{d,d} + \kappa_{2,2}\\ &\quad + \kappa_{3,1} + \kappa_{t,1} + \kappa_q + \kappa_4 \qquad (R_0)\\ &= \kappa_{1,1,1,1} + \kappa_{2,1,1} + \kappa_{2,d} + \kappa_{d,1,1} + \kappa_{d,d}\\ &\quad + 1 + 24 + \kappa_{t,1} + \kappa_q.\end{aligned}$$

Taking these relations mod 2 yields

$$\begin{aligned}(R_{2,2}) &\qquad 1 \equiv \kappa_{1,1,1,1} + \kappa_{2,d} + \kappa_{d,d} + \kappa_{d,1,1} + 1\\ (R_{3,1}) &\qquad 1 \equiv \kappa_{2,1,1} + \kappa_{t,1} + \kappa_{2,d}\\ (R_2) &\qquad 1 \equiv \kappa_{2,1,1} + \kappa_{2,d}\\ (R_{1,1}) &\qquad 0 \equiv \kappa_{2,1,1} + \kappa_{d,1,1} + 1\\ (R_d) &\qquad 0 \equiv \kappa_{d,1,1} + \kappa_{2,d}\\ (R_0) &\qquad 1 \equiv \kappa_{1,1,1,1} + \kappa_{2,1,1} + \kappa_{2,d} + \kappa_{d,1,1} + \kappa_{d,d} + 1 + \kappa_{t,1} + \kappa_q.\end{aligned}$$

It follows from this that

$$\kappa_{t,1} \equiv 0 \qquad \kappa_{2,d} \equiv \kappa_{d,1,1} \not\equiv \kappa_{2,1,1} \equiv \kappa_q \qquad \text{and} \qquad \kappa_{1,1,1,1} \equiv \kappa_{d,d} \bmod 2.$$

Taking these relations mod 4, and using that a minimal curve $C/\mathbf{F}_{q^2}$ having odd genus is possible only if q is a square, and hence a multiple of 4, yields

$$\begin{aligned}
(R_{2,2}) \qquad & 1 \equiv 3\kappa_{1,1,1,1} + 2\kappa_{2,1,1} + \kappa_{2,d} + \kappa_{d,d} + \kappa_{d,1,1} + 1 \\
(R_{3,1}) \qquad & 1 \equiv 3\kappa_{2,1,1} + 2\kappa_{d,1,1} + \kappa_{t,1} + 2 + \kappa_{2,d} \\
(R_2) \qquad & 1 \equiv \kappa_{2,1,1} + \kappa_{2,d} + 2 \\
(R_{1,1}) \qquad & 0 \equiv 2\kappa_{1,1,1,1} + 3\kappa_{2,1,1} + \kappa_{d,1,1} + 1 \\
(R_d) \qquad & 0 \equiv \kappa_{d,1,1} + 2\kappa_{d,d} + \kappa_{2,d} \\
(R_0) \qquad & 1 \equiv \kappa_{1,1,1,1} + \kappa_{2,1,1} + \kappa_{2,d} + \kappa_{d,1,1} + \kappa_{d,d} + 1 + \kappa_{t,1} + \kappa_q .
\end{aligned}$$

On the other hand, taking (R_2) in $(R_{1,1})$ yields

$$\begin{aligned}
0 &\equiv 2\kappa_{1,1,1,1} + 3(3 + 3\kappa_{2,d}) + \kappa_{d,1,1} + 1 \\
&\equiv 2\kappa_{1,1,1,1} + 2 + \kappa_{2,d} + \kappa_{d,1,1} \bmod 4
\end{aligned}$$

and, using (R_d),

$$2 \equiv 2(\kappa_{1,1,1,1} + \kappa_{d,d}) \bmod 4.$$

It follows that $\kappa_{1,1,1,1} \not\equiv \kappa_{d,d} \bmod 2$, which contradicts the relations obtained with $p = 2$, and the Theorem is proved.

It follows that $\kappa_4 = 1$ and $\kappa_{2,2} = 0$. It may be proved that $\kappa_{3,1} = 4$ or 16.

From Komiya's Theorem [5] the canonical system is classical, and from Theorem 2.6 above the invariant system $\mathcal{E}_{q^2}$ is also classical. After an eventual minimality preserving constant field extension it may be assumed that all canonical Weierstrass points are rational over $\mathbf{F}_{q^2}$, and then there are four possible situations of points with respect to the invariant system $\mathcal{E}_{q^2}$:

(a) Non-rational points of C are by hypothesis canonically generic, and they are also generic for $\mathcal{E}_{q^2}$ because of Theorem 2.6 above. They have the classical sequence:

$$\{\, \epsilon_0, \cdots, \epsilon_{l-1} \,\} = \{0, \cdots, q-4\}.$$

(b) Rational points of $C/\mathbf{F}_{q^2}$ which are canonically generic have from Theorem 2.3 the order sequence:

$$\{\, j_0, \cdots, j_{l-1} \,\} = \{0, \cdots, q-5, q-1\}.$$

(c) Canonical Weierstrass points of C with canonical orders 0,1,3 are rational, and have from Theorem 2.3 the order sequence:

$$\{\, j_0, \cdots, j_{l-1}\,\} = \{0, \cdots, q-6, q-4, q-1\}.$$

(d) Canonical Weierstrass points of C with canonical orders 0,1,4 are rational, and have from Theorem 2.3 the order sequence:

$$\{\, j_0, \cdots, j_{l-1}\,\} = \{0, \cdots, q-7, q-5, q-4, q-1\}.$$

From the Stöhr-Voloch theory it is known that Weierstrass points of $\mathcal{E}_{q^2}$ contribute for the ramification divisor $R_{\mathcal{E}_{q^2}}$ with weight given by

$$v_{R_{\mathcal{E}_{q^2}}} \geq \sum_{0 \leq i \leq l-1} (j_i - \epsilon_i),$$

where equality holds if and only if

$$\det(\binom{j_i}{\epsilon_i}) \not\equiv 0 \bmod p.$$

See [8, Theo. 1.5, p. 6]. For canonically generic rational points (the situation in (b)), and with $q = 2^m$, this determinant is

$$\det\begin{pmatrix} \binom{0}{0} & \binom{0}{1} & \cdots & \binom{0}{q-4} \\ \binom{1}{0} & \binom{1}{1} & \cdots & \binom{1}{q-4} \\ \cdot & \cdot & \cdot & \cdot \\ \binom{q-5}{0} & \binom{q-5}{1} & \cdots & \binom{q-5}{q-4} \\ \binom{q-1}{0} & \binom{q-1}{1} & \cdots & \binom{q-1}{q-4} \end{pmatrix} = \binom{q-1}{q-4} \equiv \frac{q-2}{2} = 2^{m-1} - 1 \bmod 2$$

and so it is odd, and these points have weight $v_{R_{\mathcal{E}_{q^2}}}(P) = \sum_{0 \leq i \leq l-1} (j_i - \epsilon_i) = 3$.

For canonical Weierstrass points with canonical orders 0,1,3. This determinant is

$$\det\begin{pmatrix} \binom{0}{0} & \binom{0}{1} & \cdots & \binom{0}{q-4} \\ \binom{1}{0} & \binom{1}{1} & \cdots & \binom{1}{q-4} \\ \cdot & \cdot & \cdot & \cdot \\ \binom{q-6}{0} & \binom{q-6}{1} & \cdots & \binom{q-6}{q-4} \\ \binom{q-4}{0} & \binom{q-4}{1} & \cdots & \binom{q-4}{q-4} \\ \binom{q-1}{0} & \binom{q-1}{1} & \cdots & \binom{q-1}{q-4} \end{pmatrix} = \det\begin{pmatrix} q-4 & 1 \\ \binom{q-1}{4} & \binom{q-1}{3} \end{pmatrix} \equiv 2^{m-2} - 1 \bmod 2,$$

and so it is odd, and these points are have weight

$$v_{R_{\mathfrak{L}_{q^2}}}(P) = \sum_{0 \leq i \leq l-1} (j_i - \epsilon_i) = 4.$$

The unique point P with canonical orders 0,1,4 has greater Weierstrass weight, which can be computed as the total Weierstrass weight is known to be ([8], p. 6):

$$\deg(R_{\mathfrak{L}_{q^2}}) = (2g-2)\sum_{i \leq l-1} \epsilon_i + l(q-1) = 3(q-3)^2.$$

This yields

$$v_{R_{\mathfrak{L}_{q^2}}}(P) = 3(q-3)^2 - 3(q^2 - 6q - \kappa_{3,1}) - 4\kappa_{3,1} = 27 - \kappa_{3,1}.$$

As a result one has the following equality of divisors

$$R_{\mathfrak{L}_{q^2}} = 3 \sum_{P \in C(\mathbf{F}_{q^2})} P + R_{K_C},$$

where K_C is the canonical divisor of C.

This equality should be compared to the equality conjectured in [3]

$$S_{\mathfrak{D}} = (n+1) \sum_{P \in C(\mathbf{F}_{q^2})} P + R_{K_C},$$

for maximal curves which are canonically classical.

We conclude with some examples. From the Theorem 3.1 there is exactly one hyperflex Q_0. That 4 is a canonical order at Q_0 means that the intersection divisor of the curve C with the tangent L at Q_0 is $4P$, that is, L is a bitangent, and it is necessarily the bitangent associated to the *canonical theta characteristic* ([9], p. 59). Geometrically it is interesting to know if there are Weierstrass points Q_1 and Q_2 — which from the theorem have to be necessarily simple flexes — such that their tangents intersect the curve along the divisors $3Q_i + Q_0$, for $i = 1, 2$.

This simple moduli problem is easily solved: the existence of these two points Q_1 and Q_2 implies that the curve is given by

$$C_{a,b,c} \quad : \quad f = x + y + ax^3y + bx^2y^2 + cxy^3 = 0, \qquad abc \neq 0.$$

One can easily show that these curves are smooth iff $a + b + c \neq 0$, that the origin Q_0 is the hyperflex and that the four distinct points Q_1, Q_2, Q_3, Q_4 in the infinite line are Weierstrass points. Incidentally, the points Q_3 and Q_4 also have tangents cutting the curve along divisors $3Q_i + Q_0$. The Hasse-Witt invariant of $C_{a,b,c}$ is 2 or 0 according to whether $a \neq c$ or $a = c$, so that among curves of this type only curves $C_{a,b,a}$ can be minimal (or maximal).

The curve $C_{1,1,1}/\mathbf{F}_8$ has zeta function

$$Z_{C_{1,1,1}/\mathbf{F}_8}(t) = \frac{1 + 24t^2 + 192t^4 + 512t^6}{(1-t)(1-8t)},$$

and as a consequence of the constant field extension formula for zeta functions $C_{1,1,1}/\mathbf{F}_{64}$ is maximal and $C_{1,1,1}/\mathbf{F}_{4096}$ is minimal. Its invariant system has ramification divisor

$$R_{\mathcal{L}_{q^2}} = 20Q_0 + Q_1 + Q_2 + Q_3 + Q_4 + 3 \sum_{P \in C_{1,1,1}(\mathbf{F}_{q^2})} P.$$

Given that $\mathbf{F}_8 = \mathbf{F}_2(\beta)$ with $\beta^3 = \beta + 1$ the curve $C_{\beta,1,\beta}/\mathbf{F}_8$ has zeta function

$$Z_{C_{\beta,1,\beta}/\mathbf{F}_8}(t) = \frac{1 + 24t^2 + 192t^4 + 512t^6}{(1-t)(1-8t)},$$

and thus it is maximal over $\mathbf{F}_{8^2}$ and minimal over $\mathbf{F}_{8^4}$. The curve $C_{\beta^3,1,\beta^3}/\mathbf{F}_8$ has zeta function

$$Z_{C_{\beta^3,1,\beta^3}/\mathbf{F}_8}(t) = \frac{1 + 512t^6}{(1-t)(1-8t)}$$

and thus it is maximal over $\mathbf{F}_{8^6}$ and minimal over $\mathbf{F}_{8^{12}}$.

If $\alpha \in \mathbf{F}_4 \setminus \mathbf{F}_2$ then the curve $C_{\alpha,1,\alpha}/\mathbf{F}_4$ has normalized polynomial

$$\begin{aligned}\Lambda_{C_{\alpha,1,\alpha}/\mathbf{F}_4}(u) = L_{C_{\alpha,1,\alpha}/\mathbf{F}_4}(u/2) &= 1 - u + 2u^2 - u^3 + 2u^4 - u^5 + u^6 \\ &= \left[\left(u - \frac{1+\sqrt{-3}}{2}\right)\left(u - \frac{1-\sqrt{-3}}{2}\right)\right]^2 \\ &\quad \left(u - \frac{-1+\sqrt{-3}}{2}\right)\left(u - \frac{-1-\sqrt{-3}}{2}\right).\end{aligned}$$

The last two roots do not satisfy $x^n + 1 = 0$ for any value of n, and thus no constant field extension of this curve is maximal. However, from Theorem 1.9 this curve is eventually minimal, and indeed $C_{\alpha,1,\alpha}/\mathbf{F}_{2^{12}}$ is minimal.

Acknowledgments. The authors wish to thank Arnaldo Garcia for some interesting discussions on this subject.

References

[1] M. Abdón and F. Torres, On maximal curves in characteristic two, Manuscripta Math., **99** (1999), 39–53.

[2] R. Fuhrmann, A. Garcia and F. Torres, On maximal curves, Journal of Number Theory, **67** (1997), 29–51.

[3] A. Garcia and F. Torres, On maximal curves having classical Weierstrass gaps, Contemp. Math., **245** (1999), 49–59.

[4] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Tokyo, **28** (1981), 721–724.

[5] K. Komiya, Algebraic curves with non classical types of gap sequences for genus three and four, Hiroshima Math. J., **8** (1978), 371–400.

[6] H-G. Rück and H. Stichtenoth, A characterization of Hemitian function fields over finite fields, J. reine angew. Math., **457** (1994), 185–188.

[7] H. Stichtenoth, Algebraic Function Fields and Codes, Universitext, Springer-Verlag, 1993.

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

[9] K-O. Stöhr and J.F. Voloch, A formula for the Cartier operator on plane algebraic curves, Journal für die Reine und Ang. Math., **377** (1986), 49–64.

[10] L. Washington, Introduction to Cyclotomic Fields, Springer-Verlag, 1982.

Paulo Henrique Viana de Barros
Universidade Federal de Santa Catarina
Departamento de Matemática
Campus Trindade
88040-900 Florianópolis – SC
BRASIL

E-mail: pviana@mtm.ufsc.br

Jaime Edmundo Apaza Rodriguez
Universidade Estadual Paulista - UNESP
Departamento de Matemática
Campus de Ilha Solteira
Caixa Postal 31, 15385-000 Feis – SP
BRASIL

E-mail: jaime@fqm.feis.unesp.br