Certain maximal curves and Cartier operators

by

ARNALDO GARCIA and SAEED TAFAZOLIAN (Rio de Janeiro)

1. Introduction. More than half a century ago, André Weil proved a formula for the number $N = \#\mathcal{C}(\mathbb{F}_q)$ of rational points on a smooth geometrically irreducible projective curve $\mathcal{C}$ of genus $g$ defined over a finite field $\mathbb{F}_q$. This formula provides upper and lower bounds on the number of rational points possible. It states that

$$q + 1 - 2g\sqrt{q} \leq N \leq q + 1 + 2g\sqrt{q}.$$ 

In general, this bound is sharp. In fact, if $q$ is a square, there exist several curves that attain the above upper bound (see [4], [5], [14] and [23]). We say a curve is maximal (resp. minimal) if it attains the above upper (resp. lower) bound.

There are however situations in which the bound can be improved. For instance, if $q$ is not a square there is a nontrivial improvement due to Serre (see [17, Section V.3]):

$$q + 1 - g[2\sqrt{q}] \leq N \leq q + 1 + g[2\sqrt{q}],$$

where $[a]$ denotes the integer part of the real number $a$.

Ihara showed that if a curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$ then its genus satisfies

(1.1) $$g \leq \frac{q^2 - q}{2}.$$ 

There is a unique maximal curve over $\mathbb{F}_{q^2}$ which attains the above genus bound, and it can be given by the affine equation (see [14])

(1.2) $$y^q + y = x^{q+1}.$$ 

This is the so-called Hermitian curve over $\mathbb{F}_{q^2}$.

In this paper, we consider maximal (and also minimal) curves over a finite field with $q^2$ elements. We give a characterization of certain ma-
mal and minimal curves of the following types: Fermat, Artin–Schreier or hyperelliptic. The main tool is the Cartier operator, which is a nilpotent operator in the case of maximal (or minimal) curves over finite fields. We give generalizations of results from [1], [7], [9], [22] and [23].

In Section 2 we review some important properties of the curves in question. Of special interest is Proposition 2.9 which is used to prove in Section 3 that \( C^n = 0 \) for a maximal or a minimal curve over \( \mathbb{F}_{q^2} \) with \( q = p^n \), where \( C \) denotes the Cartier operator (see Theorem 3.3). In Section 4 we consider the Fermat curve \( C(m) \) over \( \mathbb{F}_{q^2} \), defined by the affine equation \( y^m = 1 - x^m \). We show that \( C(m) \) is maximal over \( \mathbb{F}_{q^2} \) if and only if \( m \) divides \( q + 1 \). This generalizes [1, Corollary 3.5] which deals with the particular case when \( m \) belongs to the set of values of the polynomial \( T^2 - T + 1 \), and it also generalizes [9, Corollary 1] which deals with the case of \( q = p \) prime (see Remark 4.3).

In Section 5 we consider maximal curves \( C \) over \( \mathbb{F}_{q^2} \) given by an affine equation \( y^q - y = f(x) \), where \( f(x) \) is a polynomial in \( \mathbb{F}_{q^2}[x] \) with degree \( d \) prime to the characteristic \( p \). We show that \( d \mid q + 1 \) and that the maximal curve \( C \) is isomorphic to the curve given by \( y^q + y = x^d \) (see Theorem 5.4). In particular, this result shows that the hypothesis that \( d \mid q + 1 \) in Proposition 5.2 is superfluous and that the maximal curves \( C \) in Theorem 5.4 are covered by the Hermitian curve over \( \mathbb{F}_{q^2} \) given by (1.2) (see Remark 5.5). The main ideas here come from [7] which deals with the case of \( q = p \) prime.

In Section 6 we deal with maximal hyperelliptic curves \( C \) over \( \mathbb{F}_{q^2} \) in characteristic \( p > 2 \). The genus of \( C \) satisfies \( g(C) \leq (q - 1)/2 \) and we show that the curve \( C \) given by the affine equation

\[
y^2 = x^q + x
\]

is the unique maximal hyperelliptic curve over \( \mathbb{F}_{q^2} \) with genus \( g = (q - 1)/2 \) (see Theorem 6.1). The main ideas here come from [22] which deals with hyperelliptic curves with zero Hasse–Witt matrix (see Remark 6.2).

In this paper the word "curve" will mean a projective nonsingular and geometrically irreducible algebraic curve defined over a perfect field of characteristic \( p > 0 \).

2. Maximal curves. In this section we review some well-known properties of maximal curves.

Let \( C \) be a curve of genus \( g > 0 \) over the finite field \( k = \mathbb{F}_q \) with \( q \) elements. The zeta function of \( C \) is a rational function of the form

\[
Z(C/k) = \frac{L(t)}{(1 - t)(1 - qt)},
\]

where \( L(t) \in \mathbb{Z}[t] \) is a polynomial of degree \( 2g \) with integral coefficients. We call this polynomial the \( L \)-polynomial of \( C \) over \( k \).
Let $K/k$ be the function field of $C$ over $k$. Then the divisor class group $C^0(K)$ is finite and it is isomorphic to the group of $k$-rational points of the Jacobian $J$ of $C$,

$$C^0(K) = J(k).$$

It is well-known that the class number $h = \text{ord}(C^0(K))$ of $K/k$ is given by $h = L(1)$. We have

$$L(t) = 1 + a_1 t + \cdots + a_{2g-1} t^{2g-1} + q^g t^{2g} = \prod_{i=1}^{2g} (1 - \alpha_i t),$$

where $a_{2g-i} = q^{g-i} a_i$ for $i = 1, \ldots, g$, and moreover the $\alpha_i$'s are complex numbers with absolute value $|\alpha_i| = \sqrt{q}$ for $1 \leq i \leq 2g$.

We recall the following fact about maximal curves (see [21]):

**Proposition 2.1.** Suppose $q$ is a square. For a smooth projective curve $C$ of genus $g$, defined over $k = \mathbb{F}_q$, the following conditions are equivalent:

- $C$ is maximal (minimal, respectively).
- $L(t) = (1 + \sqrt{q} t)^{2g}$ ($L(t) = (1 - \sqrt{q} t)^{2g}$, respectively).
- The Jacobian of $C$ is $k$-isogenous to the $g$th power of a supersingular elliptic curve, all of whose endomorphisms are defined over $k$.

Let $h(t) = t^{2g} L(t^{-1})$. Then $h(t)$ is the characteristic polynomial of the Frobenius action on the Jacobian variety $J/k$.

**Remark 2.2.** As shown by J.-P. Serre, if there is a morphism defined over the field $k$ between two curves $f : C \to D$, then the $L$-polynomial of $D$ divides the one of $C$. Hence a subcover $D$ of a maximal curve $C$ is also maximal (see [10]). So one way to construct explicit maximal curves is to find equations for subcovers of the Hermitian curve (see [1] and [4]).

**Definition.** The $p$-rank of an abelian variety $A/k$ is denoted by $\sigma(A)$; it is the number of copies of $\mathbb{Z}/p\mathbb{Z}$ in the group of points of order $p$ in $A(k)$. The $p$-rank $\sigma(C)$ of a curve $C/k$ is the $p$-rank of its Jacobian. We also call it the Hasse–Witt invariant of the curve.

If we have the $L$-polynomial of a curve $C$, we can use the following result to determine its Hasse–Witt invariant (see [16]):

**Proposition 2.3.** Let $C$ be a curve defined over $k = \mathbb{F}_q$. If the $L$-polynomial is $L = 1 + a_1 t + \cdots + a_{2g-1} t^{2g-1} + q^g t^{2g}$, then the Hasse–Witt invariant satisfies

$$\sigma(C) = \max\{i \mid a_i \not\equiv 0 \pmod{p}\}.$$

**Remark 2.4.** Since $a_{2g-i} = q^{g-i} a_i$, $i = 0, 1, \ldots, g$, we have $0 \leq \sigma(C) \leq g$. If $\sigma(C) = g$ the curve is called ordinary.
Corollary 2.5. If a curve $C$ is maximal (or minimal) over a finite field, then the Hasse–Witt invariant satisfies $\sigma(C) = 0$.

Proof. This follows from the above proposition and Proposition 2.1. □

Remark 2.6. In fact, the $p$-rank of an abelian variety is equal to the number of zero slopes in its $p$-adic Newton polygon and this number is not greater than the dimension. So in general we have $0 \leq \sigma(C) \leq g(C)$. From Proposition 2.1 a maximal (or minimal) curve $C$ is supersingular, so all slopes of its Newton polygon are equal to 1/2. On the other hand, if a curve $C$ defined over a finite field $k = \mathbb{F}_q$ is supersingular, then $C$ is minimal over some finite extension of $k$ (see [18, Proposition 1]). For additional information about Newton polygons, see [12].

We recall the following basic result concerning Jacobians. Let $C$ be a curve, $\mathcal{F}$ the Frobenius endomorphism (relative to the base field) of the Jacobian $J$ of $C$, and $h(t)$ the characteristic polynomial of $\mathcal{F}$. Let $h(t) = \prod_{i=1}^{T} h_i(t)^{r_i}$ be the irreducible factorization of $h(t)$ over $\mathbb{Z}[t]$. Then

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

This follows from the semisimplicity of $\mathcal{F}$ and the fact that the representation of endomorphisms of $J$ on the Tate module is faithful (cf. [21, Theorem 2] and [11, VI, Section 3]). In the case of a maximal curve over $\mathbb{F}_{q^2}$, we have $h(t) = (t + q)^{2g}$. Therefore from (2.1) we obtain the following result, which is contained in the proof of [14, Lemma 1].

Lemma 2.7. The Frobenius map $\mathcal{F}$ (relative to $\mathbb{F}_{q^2}$) of the Jacobian $J$ of a maximal (resp. minimal) curve over $\mathbb{F}_{q^2}$ acts as multiplication by $-q$ (resp. by $+q$).

Remark 2.8. Let $A$ be an abelian variety defined over $\mathbb{F}_{q^2}$, of dimension $g$. Then

\[(q-1)^{2g} \leq \#A(\mathbb{F}_{q^2}) \leq (q+1)^{2g}.\]

But if $C$ is a maximal (resp. minimal) curve over $\mathbb{F}_{q^2}$, then by the above lemma we have $J(\mathbb{F}_{q^2}) = (\mathbb{Z}/(q+1)\mathbb{Z})^{2g}$ (resp. $J(\mathbb{F}_{q^2}) = (\mathbb{Z}/(q-1)\mathbb{Z})^{2g}$). So the Jacobian of a maximal (resp. minimal) curve is maximal (resp. minimal) in the sense of the above bounds.

The following proposition is crucial for us (see [2, Proposition 1.2]):

Proposition 2.9. Let $A$ be an abelian variety defined over $\mathbb{F}_{q^2}$, where $q = p^n$. If the Frobenius $\mathcal{F}$ relative to $\mathbb{F}_{q^2}$ acts on the abelian variety $A$ as multiplication by $\pm q$, then $\mathcal{F}^n = 0$ on $H^1(A, \mathcal{O}_A)$. 
3. Cartier operator. Let $C$ be a curve defined over a perfect field $k$ of characteristic $p > 0$. Let $\Omega^1$ be the sheaf of differential 1-forms on $C$. Then there exists a unique operation $\mathcal{C}: \Omega^1 \rightarrow \Omega^1$, called the Cartier operator, such that

(i) $\mathcal{C}$ is $1/p$-linear, i.e., $\mathcal{C}(f^p \omega) = f \mathcal{C}(\omega)$,
(ii) $\mathcal{C}$ vanishes on exact differentials, i.e., $\mathcal{C}(df) = 0$,
(iii) $\mathcal{C}(f^{p-1} df) = df$,
(iv) a differential $\omega \in \Omega^1$ is logarithmic (i.e., there exists a section $f \neq 0$ such that $\omega = df/f$) if and only if $\omega$ is closed and $\mathcal{C}(\omega) = \omega$,

where $f$ (resp. $\omega$) is a local section of $\mathcal{O}$ (resp. $\Omega^1$). This operator induces a $1/p$-linear map $\mathcal{C}: H^0(C, \Omega^1) \rightarrow H^0(C, \Omega^1)$, acting on the space of regular differential forms.

Remark 3.1. Moreover, for a given natural number $n$, one can easily show that

$$\mathcal{C}^n(x^j dx) = \begin{cases} 0 & \text{if } p^n \nmid j + 1, \\ x^{s-1}dx & \text{if } j + 1 = p^n s. \end{cases}$$

We mention here the following theorem of Hasse–Witt ([6]):

Theorem 3.2. Let $V$ be a finite-dimensional vector space over an algebraically closed field of characteristic $p > 0$. Let $\psi: V \rightarrow V$ be a $1/p$-linear map. Then there are two subspaces $V^s$ and $V^0$ of $V$ satisfying the following conditions:

- $V^s$ is spanned by $\psi$ invariant elements.
- Each $y$ in $V^0$ is killed by an iterate of $\psi$.
- $V = V^s \oplus V^0$.

Definition. For a basis $\omega_1, \ldots, \omega_g$ of $H^0(C, \Omega^1)$ let $(a_{ij})$ denote the associated matrix of the Cartier operator $\mathcal{C}$, i.e.,

$$\mathcal{C}(\omega_j) = \sum_{i=1}^g a_{ij} \omega_i.$$

The corresponding Hasse–Witt matrix $\mathcal{A}(\mathcal{C})$ is obtained by taking $p$th powers, i.e.,

$$\mathcal{A}(\mathcal{C}) = (a_{ij}^p).$$

Because of $1/p$-linearity, the operator $\mathcal{C}^n$ is represented with respect to the basis $\omega_1, \ldots, \omega_g$ by the product of the matrices below:

$$(a_{ij}^{1/p^n - 1}) \cdots (a_{ij}^{1/p}) \cdot (a_{ij}).$$

By raising the coefficients to $p^n$th powers we get the matrix

$$\mathcal{A}(\mathcal{C})^{[n]} = (a_{ij}^p) \cdot (a_{ij}^{p^2}) \cdots (a_{ij}^{p^n}).$$
It is remarkable that if \( n \geq g \) then the rank of the matrix \( \mathcal{A}(C)^{[n]} \) does not depend on \( n \) and it is equal to the Hasse–Witt invariant of \( C \).

**Theorem 3.3.** Let \( C \) be an algebraic curve defined over a finite field with \( q^2 \) elements, where \( q = p^n \) for some \( n \in \mathbb{N} \). If the curve \( C \) is maximal (or minimal) over \( \mathbb{F}_{q^2} \), then \( \mathcal{C}^n = 0 \).

**Proof.** From Lemma 2.7 we know that the Frobenius acting on the Tate module of the Jacobian of \( C \) acts as multiplication by \( \pm q \). Then one may apply Proposition 2.9 to conclude that \( \mathcal{F}^n = 0 \). Finally, since the Cartier operator acting on \( H^0(C, \Omega^1) \) is dual to the Frobenius acting on \( H^1(C, \mathcal{O}_C) \) by the Serre duality, one concludes that also \( \mathcal{C}^n = 0 \). ■

The next result (see [19, Corollary 2.7]) relates the Hasse–Witt matrix and the Weierstrass gap sequence at a rational point.

**Proposition 3.4.** Let \( C \) be a curve defined over a perfect field and \( n \in \mathbb{N} \). Let \( \mathcal{A}(C) \) denote the Hasse–Witt matrix of the curve \( C \). If \( P \) is a rational point on \( C \), then the rank of \( \mathcal{A}(C)^{[n]} \) is no smaller than the number of gaps at \( P \) divisible by \( p^n \).

**Corollary 3.5.** Let \( C \) be a curve defined over \( \mathbb{F}_{q^2} \). Let \( P \) be a rational point on the curve \( C \). If \( C \) is maximal over \( \mathbb{F}_{q^2} \) then \( q \) is not a gap number of \( P \).

**Proof.** If \( q = p^n \) for some integer \( n \) and \( C \) is a maximal curve over \( \mathbb{F}_{q^2} \) then Theorem 3.3 yields \( \mathcal{A}(C)^{[n]} = 0 \). Thus the result follows from Proposition 3.4. ■

**Corollary 3.6.** Let \( C \) be a hyperelliptic curve over \( \mathbb{F}_{q^2} \) where \( q = p^n \) and \( p > 2 \). If \( \mathcal{C}^n = 0 \), then

\[
g(C) \leq \frac{q - 1}{2}.
\]

**Proof.** As the genus is fixed under a constant field extension, we can suppose that \( k \) is algebraically closed. We know that a Weierstrass point on a hyperelliptic curve has the gap sequence \( 1, 3, 5, \ldots, 2g - 1 \), so the result follows from Proposition 3.4. ■

**Remark 3.7.** If \( C \) is maximal over \( \mathbb{F}_{p^2} \) then \( \mathcal{C} = 0 \). On the other hand, the Cartier operator on a curve is zero if and only if the Jacobian of the curve is the product of supersingular elliptic curves (see [13, Theorem 4.1]). Now by Theorem 1.1 of [2] we also have

- \( g(C) \leq (p^2 - p)/2 \).
- \( g(C) \leq (p - 1)/2 \) if \( C \) is hyperelliptic and \( (p, g) \neq (2, 1) \).
4. Fermat curves. In this section we give a characterization of maximal Fermat curves.

Let $k$ be a finite field with $q^2$ elements, where $q = p^n$ for some integer $n$. Let $C(m)$ be the Fermat curve defined over $k$ by

$$x^m + y^m = z^m,$$

where $m$ is an integer such that $m \geq 3$ and $\gcd(m, p) = 1$.

As is well-known, the genus $g$ of $C(m)$ is $g = (m - 1)(m - 2)/2$. The affine model of $C(m)$ is given by $x^m_1 + y^m_1 = 1$ ($x_1 = x/z$, $y_1 = y/z$). Let $\mu_m$ denote the set of $m$th roots of unity. If $m$ divides $q^2 - 1$, then the group $\mu_m \times \mu_m$ operates on rational points of $C(m)$ by

$$(\xi, \zeta)(x_1, y_1) = (\xi x_1, \zeta y_1) \quad \text{with} \quad \xi, \zeta \in \mu_m.$$

Remark 4.1. If $C$ is maximal over $\mathbb{F}_{q^2}$, then $m$ divides $q^2 - 1$ (see the proof of Lemma 4.5 in [5]).

Lemma 4.2. With notation and hypotheses as above, if $C(m)$ is maximal over $\mathbb{F}_{q^2}$, then $m \leq q + 1$.

Proof. Since the genus is $g = (m - 1)(m - 2)/2$ and the curve $C(m)$ is maximal over $\mathbb{F}_{q^2}$, then

$$\#C(m)(\mathbb{F}_{q^2}) = 1 + q^2 + (m - 1)(m - 2)q.$$

Looking at the function field extension $\mathbb{F}_{q^2}(x, y)/\mathbb{F}_{q^2}(x)$, where $y^m = 1 - x^m$, we see that the points with $x^m = 1$ are totally ramified. Hence we also have

$$\#C(m)(\mathbb{F}_{q^2}) \leq m + (q^2 + 1 - m)m.$$

From (4.2) and (4.3) we conclude that $m \leq q + 1$. ■

If $m = q + 1$ then $C(q + 1)$ is the Hermitian curve over $\mathbb{F}_{q^2}$. Suppose $m$ divides $q + 1$, i.e., $q + 1 = mr$ for some integer $r$. Then we can define the following morphism:

$$C(q + 1) \to C(m), \quad (x, y) \mapsto (x^r, y^r).$$

Hence $C(m)$ is covered by $C(q + 1)$. Thus by Remark 2.2 if $m$ divides $q + 1$, then $C(m)$ is maximal over $\mathbb{F}_{q^2}$. Now we want to show the converse. We start with a remark:

Remark 4.3. Assume $q = p$ is a prime number. If the curve $C(m)$ is maximal over $\mathbb{F}_{p^2}$, then Theorem 3.3 implies that the Hasse–Witt matrix of $C(m)$ is zero. Hence from [9, Corollary 1] we find that $m \mid p + 1$. The next theorem generalizes this result.

Theorem 4.4. Let $C(m)$ be the Fermat curve of degree $m$ prime to the characteristic $p$ defined over $\mathbb{F}_{q^2}$. Then $C(m)$ is maximal over $\mathbb{F}_{q^2}$ if and only if $m$ divides $q + 1$. 
Proof. If $m \mid q+1$, then the above discussion shows that $\mathcal{C}(m)$ is maximal over $\mathbb{F}_{q^2}$. Conversely, let $\mathcal{C}(m)$ be a maximal curve over $\mathbb{F}_{q^2}$. By Remark 4.1 we know that $m$ divides $q^2 - 1$. As in the proof of the lemma above, looking at the function field extension $\mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}(x)$ we find that

$$\#\mathcal{C}(m)(\mathbb{F}_{q^2}) = m + \lambda m$$

for some integer $\lambda$. In fact, $\mathcal{C}(m)$ has $m$ rational points which correspond to the totally ramified points with $x^m = 1$ and some others that are completely splitting. On the other hand, from the maximality of $\mathcal{C}(m)$ we have

$$\#\mathcal{C}(m)(\mathbb{F}_{q^2}) = 1 + q^2 + (m - 1)(m - 2)q.$$  

Comparing (4.4) and (4.5) we deduce that $m \mid (q+1)^2$. Hence $m \mid 2(q+1)$, since $m \mid q^2 - 1$. Now we have two cases:

Case 1: $p = 2$. In this case since $\gcd(m, p) = 1$, we see that $m$ is odd and hence it divides $q + 1$, since it divides $2(q+1)$.

Case 2: $p = odd$. In this case $\gcd(q + 1, q - 1) = 2$. Reasoning as for $p = 2$, we find that if $d$ is an odd divisor of $m$, then $d \mid q + 1$. The only situation still to be investigated is the following: $q + 1 = 2^rs$ with $s$ an odd integer and $m = 2^{r+1}s_1$ with $s_1 \mid s$. But according to Remark 2.2 and the following lemma, this situation does not occur.

Lemma 4.5. Assume that the characteristic $p$ is odd and write $q+1 = 2^rs$ with $s$ an odd integer. Set $m := 2^{r+1}$. Then the Fermat curve $\mathcal{C}(m)$ is not maximal over $\mathbb{F}_{q^2}$.

Proof. Writing $q = p^n$ we consider three cases:

Case 1: $p \equiv 1 \pmod{4}$. In this case we have $q + 1 = 2s$ with $s$ odd. So we must show that the curve $\mathcal{C}(4)$ is not maximal over $\mathbb{F}_{q^2}$. But it follows from [9, Theorem 2] that $\mathcal{C}(4)$ with $p \equiv 1 \pmod{4}$ is ordinary and so it is not maximal.

Case 2: $p \equiv 3 \pmod{4}$ and $n$ even. In this case we have again $q + 1 = 2s$ with $s$ odd and we must show that the curve $\mathcal{C}(4)$ is not maximal over $\mathbb{F}_{q^2}$. Since $4 \mid p + 1$, the curve $\mathcal{C}(4)$ is maximal over $\mathbb{F}_{p^2}$. Hence $\mathcal{C}(4)$ is minimal over $\mathbb{F}_{q^2}$ because $n$ is even.

Case 3: $p \equiv 3 \pmod{4}$ and $n$ odd. As $n$ is odd, we have $q + 1 = 2^rs$ with $r \geq 2$ and $s$ odd. Here we can assume that $r \geq 3$. In fact, for $r = 2$ according to [8, p. 204], the curve $\mathcal{C}(8)$ is not supersingular and hence cannot be maximal. Note that $r = 2$ implies $p \equiv 3 \pmod{8}$.

Consider now the curve $\mathcal{C}(m)$ with $m = 2^{r+1}$ and $r \geq 3$. As $m = 2^{r+1}$ is the largest power of 2 that divides $q^2 - 1$, $-1$ is not an $m$th power in $\mathbb{F}_{q^2}^*$. Hence the points at infinity on $y^m = 1 - x^m$ are not rational. This implies
that (see (4.1))

\[ \#C(m)(\mathbb{F}_{q^2}) = m + \lambda_1 m^2 \]  

for some integer \( \lambda_1 \).

Then from (4.5) and (4.6) we get

\[ q^2 + 1 + 2q - 3mq - m \equiv 0 \pmod{m^2}. \]

Hence \((q+1)^2 - m(2q+2) - m(q-1) \equiv 0 \pmod{4m^2}\). Since \(m \mid 4(q-1)\), and this is impossible as \( r \geq 3 \) and \(4(q-1) = 8s_1 \) with \(s_1\) odd. This completes the proofs of Lemma 4.5 and of Theorem 4.4. ■

**Remark 4.6.** The particular case of Theorem 4.4 when \( m \) is of the form \( m = t^2 - t + 1 \) with \( t \in \mathbb{N} \) was proved in Corollary 3.5 of [1].

**5. Artin–Schreier curves.** In this section we consider curves \( C \) over \( k = \mathbb{F}_{q^2} \) given by an affine equation

\[ y^q - y = f(x), \]  

where \( f(x) \) is an admissible rational function in \( k(x) \), i.e., a rational function such that every pole of \( f(x) \) in the algebraic closure \( \overline{k} \) occurs with a multiplicity relatively prime to the characteristic \( p \). If \( C \) is a maximal curve over \( \mathbb{F}_{q^2} \), from [5, Remark 4.2] we can assume that \( f(x) \) is a polynomial of degree \( \leq q + 1 \). In the following we apply results introduced in the preceding sections to characterize maximal curves given by (5.1).

The following remark is due to Stichtenoth:

**Remark 5.1.** Suppose that \( q = p \) in (5.1) considered over a perfect field \( k \). Then we can change variables to assume that the curve \( C \) is given by (5.1) with an admissible rational function \( f(x) \). This follows from the partial fraction decomposition and from arguments similar to the proof of [17, Lemma III.7.7]. In fact, let \( u(x) \) in \( k[x] \) be an irreducible polynomial and suppose that the rational function \( f(x) \) involves a partial fraction of the form \( c(x)/u(x)^l \), with \( c(x) \) a polynomial in \( k[x] \) prime to \( u(x) \) and with \( l \) a natural number. Since the quotient field \( k[x]/(u(x)) \) is perfect, we can find polynomials \( a(x) \) and \( b(x) \) in \( k[x] \) such that \( c(x) = a(x)^p + b(x)u(x) \). Setting \( z = a(x)/u(x) \) we get

\[ c(x)/u(x)^l - (z^p - z) = z + b(x)/u(x)^{l-1}. \]

Performing the substitution \( y \mapsto y - z \) and repeating this argument as in the proof of [17, Lemma III.7.7], we get the desired result.

Denote by \( \text{tr} \) the trace of \( \mathbb{F}_{q^2} \) over \( \mathbb{F}_q \). We have (see [23]):

**Proposition 5.2.** Let \( C \) be a curve defined over \( \mathbb{F}_{q^2} \) by the equation

\[ y^q - y = ax^d + b \]
where \( a, b \in \mathbb{F}_{q^2}, a \neq 0 \) and \( d \) is any positive integer relatively prime to the characteristic \( p \). Suppose \( d \) divides \( q + 1 \) and define \( v \) and \( u \) by \( vd = q^2 - 1 \) and \( ud = q + 1 \). Then

(i) If \( C \) is maximal over \( \mathbb{F}_{q^2} \), then \( \text{tr}(b) = 0 \) and \( a^v = (-1)^u \).

(ii) If \( C \) is minimal over \( \mathbb{F}_{q^2} \) and \( q \neq 2 \), then \( d = 2, \text{tr}(b) = 0 \) and \( a^v \neq (-1)^u \).

Remark 5.3. Let \( q = 2 \) and \( b \in \mathbb{F}_4 \setminus \mathbb{F}_2 \); apart from the curves listed in item (ii) of the above proposition, we have another minimal one of the form (5.1): the minimal elliptic curve over \( \mathbb{F}_4 \) given by the affine equation \( y^2 + y = x^3 + b \).

Suppose \( q = p \) is a prime. Then a curve given by (5.1) is a \( p \)-cyclic extension of \( \mathbb{P}^1 \). In [7] we have a characterization of such curves, defined over an algebraically closed field, with zero Hasse–Witt matrix. Here we generalize their argument, and we characterize such curves in the general case \( q = p^n \) with nilpotent Cartier operator, \( \mathcal{C}^n = 0 \).

We now state the main result of this section:

**Theorem 5.4.** Let \( C \) be a curve defined by the equation \( y^q - y = f(x) \), where \( f(x) \in \mathbb{F}_{q^2}[x] \) has degree \( d \) prime to \( p \). If the curve \( C \) is maximal over \( \mathbb{F}_{q^2} \), then \( C \) is isomorphic to the projective curve defined over \( \mathbb{F}_{q^2} \) by the affine equation \( y^q + y = x^d \) with \( d \mid q + 1 \).

**Proof.** Write \( q = p^n \). As \( C \) is maximal over \( \mathbb{F}_{q^2} \), from Theorem 3.3 we know that \( \mathcal{C}^n = 0 \).

A basis for \( H^0(C, \Omega^1) \) is

\[
\mathcal{B} = \{y^r x^a dx \mid 0 \leq a, r \text{ and } a p^n + rd \leq (p^n - 1)(d - 1) - 2\}.
\]

Since \( y = y^q - f(x) \) we have

\[
\mathcal{C}^n(y^r x^a dx) = \mathcal{C}^n((y^q - f)^r x^a dx).
\]

From Remark 3.1 we get

\[
\mathcal{C}^n(y^r x^a dx) = \sum_{h=0}^{r} \binom{r}{h} (-1)^h y^{r-h} \mathcal{C}^n(f^h x^a dx).
\]

Hence

\[
\mathcal{C}^n(f^h x^a dx) = 0
\]

for all \( h, r \) and \( a \) such that \( 0 \leq h \leq r, \binom{r}{h} \) is prime to \( p \) and

\[
ap^n + rd \leq (p^n - 1)(d - 1) - 2.
\]
First we show again that the degree of $f(x)$ is at most $q + 1$. In fact, if $d = \deg(f(x)) \geq q + 2$, then $x^{q-1}dx \in \mathcal{B}$, because

$$q(q - 1) \leq (q - 1)(q + 1) - 2.$$ 

From Remark 3.1 we get $\mathcal{C}^n(x^{p^n-1}dx) = dx$ and this contradicts $\mathcal{C}^n = 0$.

Now if $d = q + 1$, then the genus of the curve $C$ is $g = q(q - 1)/2$. Hence according to [14], $C$ is the Hermitian curve given by

$$y^q + y = x^{q+1}.$$ 

Hence we can assume $d \leq q$, and so $d \leq q - 1$. Then there exists $l \geq 1$ such that

$$ld + 1 \leq q < (l + 1)d + 1.$$ 

Again since $\gcd(p, d) = 1$, we have

(5.6) $$ld + 1 \leq q \leq (l + 1)d - 1.$$ 

For $r \in \mathbb{N}$ satisfying

$$(q - 1 - r)d \geq q + 1$$ 

we define

$$a(r) := \left\lfloor d - 1 - \frac{(r + 1)d + 1}{q} \right\rfloor,$$

which is the largest possible $a \in \mathbb{N}$ satisfying (5.5).

From (5.6) and $d \leq q - 1$, we find that $a(l) = d - 3$ and therefore

(5.7) $$\deg(f^l x^{a(l)}) = ld + a(l) = (l + 1)d - 3.$$ 

Suppose that $q - 1 = ld + a$ with $0 \leq a \leq a(l)$. Then the polynomial $f^l x^a$ has degree $q - 1$ and it follows from Remark 3.1 that

$$\mathcal{C}^n(f^l x^a dx) = a_d^{l/q} dx$$

where $a_d$ denotes the leading coefficient of $f(x)$. But this contradicts (5.4) with $r = h = l$.

Therefore (5.7) implies that

(5.8) $$q - 1 \geq ld + a(l) + 1 = (l + 1)d - 2.$$ 

By (5.6) and (5.8), we have

(5.9) $$q + 1 = sd \quad \text{with } s := l + 1 \geq 2.$$ 

Since $\gcd(p, d) = 1$, we can change variable $x \mapsto x + \alpha$, for a suitable $\alpha \in \mathbb{F}_{q^2}$, so that

$$f(x) = a_d x^d + a_i x^i + \cdots + a_0 \quad \text{with } i \leq d - 2.$$ 

Therefore

$$f(x)^s = a_d^s x^{sd} + sa_d^{s-1}a_i x^{i+(s-1)d} + \cdots + a_0^s.$$
Suppose $d \geq 3$. In this case if $1 \leq i \leq d - 2$, then
$$0 \leq d - i - 2 \leq d - 3 = a(s).$$
We stress here that $a(l) = a(l + 1) = d - 3$. Therefore
$$i + (s - 1)d + d - i - 2 = sd - 2 = q - 1,$$
and we get
$$\mathcal{C}^n(f^s x^{d-i-2} dx) = s(a^{s-1}_d a_i)^{1/q} dx = 0.$$ 
This implies $a_i = 0$ since $s$ is prime to $p$ by (5.9). Hence $f(x)$ must be of the form (the case $d = 2$ is trivial)
$$f(x) = ax^d + b \quad \text{with } d \mid q + 1.$$ 
Now if the curve is maximal, from Proposition 5.2 we know that $\text{tr}(b) = 0$ and $a^v = (-1)^u$ where $u = (q + 1)/d$ and $v = (q^2 - 1)/d$. By Hilbert’s 90 Theorem, there exists $\gamma \in \mathbb{F}_{q^2}$ such that $\gamma^q - \gamma = b$ and by changing variable $y \mapsto y + \gamma$ we can assume $b = 0$.

Now we have two cases:

**Case 1: $u$ is even.** In this case $a^v = 1$ and hence $a = c^d$ for some $c \in \mathbb{F}_{q^2}^*$. Changing variable $x \mapsto c^{-1}x$ we have
$$y^q - y = x^d \quad \text{with } d \mid q + 1.$$ 
Pick $\alpha \in \mathbb{F}_{q^2}$ with $\alpha^{q-1} = -1$. Substituting $y \mapsto \alpha^{-1}y$ we have $y^q + y = \alpha x^d$.
Again here $\alpha^v = \alpha^{(q-1)u} = (-1)^u = 1$ and hence $\alpha = \theta^d$ for some $\theta \in \mathbb{F}_{q^2}^*$, and we conclude that the curve is isomorphic to $y^q + y = x^d$.

**Case 2: $u$ is odd.** In this case $a^v = -1$ and hence $(-a^{q-1})^u = 1$. So $-a^{q-1} = \beta^d(q-1)$ for some $\beta \in \mathbb{F}_{q^2}^*$. Set $\mu := a \beta^{-d}$; then $\mu^{q-1} = -1$. Now by changing variables $x \mapsto \beta^{-1}x$ and $y \mapsto -\mu y$ we conclude that the curve $C$ is equivalent to
$$y^q + y = x^d \quad \text{with } d \mid q + 1.$$ 

**Remark 5.5.** Most of the argument above just uses the property $\mathcal{C}^n = 0$, and we see that the hypothesis that $d \mid q + 1$ in Proposition 5.2 is superfluous. We also infer that all maximal curves over $\mathbb{F}_{q^2}$ given by $y^q - y = f(x)$ as in Theorem 5.4 are covered by the Hermitian curve.

We can also classify minimal Artin–Schreier curves over $\mathbb{F}_{q^2}$:

**Theorem 5.6.** Let $C$ be a curve defined by the equation $y^q - y = f(x)$, where $f(x) \in \mathbb{F}_{q^2}[x]$ has degree prime to $p$ and $p \neq 2$. If $C$ is minimal over $\mathbb{F}_{q^2}$ and $g(C) \neq 0$, then $C$ is equivalent to the projective curve defined by the equation
$$y^q - y = ax^2 \quad \text{where } a \in \mathbb{F}_{q^2}, a \neq 0, \text{ and } a^{(q^2-1)/2} \neq (-1)^{(q+1)/2}.$$
Proof. We know that if a curve is minimal over $F_{q^2}$, with $q = p^n$, then again the operator $C^n$ is zero. So by the above proof, the curve can be defined by $y^q - y = ax^d + b$ where $d \mid q + 1$. Now we can use again Proposition 5.2; it yields $d = 2$, $\text{tr}(b) = 0$ and $a^{(q^2-1)/2} \neq (-1)^{(q+1)/2}$. □

Remark 5.7. In the above theorem, if $q \equiv 1 \pmod{4}$, then on changing variable $x \mapsto \alpha^{-1}x$, where $a = \alpha^2$, the minimal curve $C$ is equivalent to

$$y^q - y = x^2.$$ 

Clearly, this last curve is maximal over $F_{q^2}$ if $q \equiv 3 \pmod{4}$.

Let $\pi : C \to D$ be a $p$-cyclic covering of projective nonsingular curves over the algebraic closure $\overline{k}$. Then we have the so-called Deuring–Shafarevich formula:

$$(5.10) \quad \sigma(C) - 1 + r = p(\sigma(D) - 1 + r),$$

where $r$ is the number of ramification points of the covering $\pi$.

Corollary 5.8. Let $C$ be a curve defined over $k = \mathbb{F}_{p^2}$ such that there exists a cyclic covering $C \to \mathbb{P}^1$ of degree $p$ which is also defined over $k$. If the curve $C$ is maximal over $\mathbb{F}_{q^2}$, then $C$ is isomorphic to the curve given by the affine equation $y^p + y = x^d$, where $d$ divides $p + 1$.

Proof. From Remark 5.1 we can assume that $C$ is given by

$$y^p - y = f(x),$$

where every pole of $f(x)$ in $\overline{k}$ occurs with a multiplicity relatively prime to $p$. Now if $C$ is maximal, then $\sigma(C) = 0$ by Corollary 2.5. Note that from (5.10) we must have $r = 1$ and we can put this unique ramification point at infinity; hence we can assume that $f(x) \in k[x]$. Note here that the unique ramification point is $k$-rational. The result now follows from Theorem 5.4. □

6. Hyperelliptic curves. Let $k = \mathbb{F}_{q^2}$ be a finite field of characteristic $p > 2$. Let $C$ be a projective nonsingular hyperelliptic curve over $k$ of genus $g$. Then $C$ can be defined by an affine equation of the form

$$y^2 = f(x),$$

where $f(x)$ is a polynomial over $k$ of degree $2g + 1$, without multiple roots. If $C$ is maximal over $\mathbb{F}_{q^2}$ then by Corollary 3.6 we have an upper bound on the genus, namely

$$g(C) \leq \frac{q - 1}{2}.$$ 

In the next theorem we establish a characterization of maximal hyperelliptic curves in characteristic $p > 2$ that attain this upper bound.
Theorem 6.1. Suppose that $p > 2$. There is a unique maximal hyperelliptic curve over $\mathbb{F}_{q^2}$ with genus $g = (q - 1)/2$. It can be given by the affine equation

$$y^2 = x^q + x.$$ 

Before proving this theorem, we need to explain how the matrix associated to $\mathcal{C}^n$, where $q = p^n$, is determined from $f(x)$.

The differential 1-forms of the first kind on $\mathcal{C}$ form a $k$-vector space $H^0(\mathcal{C}, \Omega^1)$ of dimension $g$ with basis $B = \{\omega_i = x^{i-1}dx/y \mid i = 1, \ldots, g\}$.

The images under the operator $\mathcal{C}^n$ are determined in the following way. Rewrite

$$\omega_i = \frac{x^{i-1}dx}{y} = x^{i-1}y^{-q}y^{q-1}dx = y^{-q}x^{i-1} \sum_{j=0}^{N} c_j x^j dx,$$

where the coefficients $c_j \in k$ are obtained from the expansion

$$y^{q-1} = f(x)^{(q-1)/2} = \sum_{j=0}^{N} c_j x^j \quad \text{with} \quad N = \frac{q-1}{2}(2g+1).$$

Then for $i = 1, \ldots, g$ we get

$$\omega_i = y^{-q} \left( \sum_{i+j \not\equiv 0 \pmod{q}} c_j x^{i+j-1} dx \right) + \sum_l c_{(l+1)q-i} x^{(l+1)q-1} \frac{dx}{yq} \frac{x^l}{x}.$$ 

Note here that $0 \leq l \leq (N+i)/q - 1 < g - 1/2$. On the other hand, we know from Remark 3.1 that if $\mathcal{C}^n(x^{r-1}dx) \neq 0$ then $r \equiv 0 \pmod{q}$. Thus we have

$$\mathcal{C}^n(\omega_i) = \sum_{l=0}^{g-1} (c_{(l+1)q-i})^{1/q} \cdot x^{l/q} \cdot \frac{x^l}{y} \cdot dx.$$ 

If we write $\omega = (\omega_1, \ldots, \omega_g)$ as a row vector we have

$$\mathcal{C}^n(\omega) = \omega M^{1/q},$$

where $M$ is the $(g \times g)$ matrix with elements in $k$ given as

$$M = \begin{pmatrix}
  c_{q-1} & c_{q-2} & \cdots & c_{q-g} \\
  c_{2q-1} & c_{2q-2} & \cdots & c_{2q-g} \\
  \vdots & \vdots & \ddots & \vdots \\
  c_{gq-1} & c_{gq-2} & \cdots & c_{gq-g}
\end{pmatrix}.$$ 

Remark 6.2. In [22] the author found a characterization for hyperelliptic curves defined over an algebraically closed field whose Hasse–Witt matrix
is zero. In the proof below we use his ideas to classify hyperelliptic curves with a nilpotent Cartier operator.

Proof of Theorem 6.1. Let $\mathcal{C}$ be a hyperelliptic curve of genus $g = (q - 1)/2$. Then $\mathcal{C}$ can be defined by the equation $y^2 = f(x)$ with a square-free polynomial

$$f(x) = a_q x^q + a_{q-1} x^{q-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x] \quad \text{and} \quad a_q \neq 0.$$ 

As $\mathcal{C}$ is maximal over $\mathbb{F}_q^2$, it has $1 + q^2 + q(q - 1)$ rational points. On the other hand, if we consider $\mathcal{C}$ as a double cover of $\mathbb{P}^1$, the ramification points are the roots of $f(x)$ and the point at infinity. As the latter is a rational point and $1 + q^2 + q(q - 1)$ is an even number, $f(x)$ must have an odd number of rational roots. Hence $f(x)$ has at least one rational root in $\mathbb{F}_q^2$, say $\theta$. By substituting $x + \theta$ for $x$, we can assume that $\mathcal{C}$ is defined by the equation $y^2 = f(x)$ with $f(0) = 0$. We then write

$$f(x) = a_q x^q + a_{q-1} x^{q-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x] \quad \text{and} \quad a_1 a_q \neq 0.$$ 

Now as the curve $\mathcal{C}$ is maximal over $\mathbb{F}_q^2$, with $q = p^n$ for some integer $n$, it follows that $\mathcal{C}^n = 0$. So the above matrix $M$ is the zero matrix. Hence looking at the last row of $M$, we see that

$$c_{gq-1} = c_{gq-2} = \cdots = c_{gq-g} = 0.$$ 

We will show by induction that this means

$$a_{q-1} = a_{q-2} = \cdots = a_{q-g} = 0.$$ 

First we observe that

$$c_{gq-1} = g a_q^{q-1} a_{q-1}.$$ 

So $c_{gq-1} = 0$ implies $a_{q-1} = 0$. Now assume $a_{q-i} = 0$ for all $1 \leq i < m \leq g$. We want to show that $a_{q-m} = 0$. Under the assumption above, $f(x)$ reduces to

$$f(x) = a_q x^q + a_{q-m} x^{q-m} + \cdots + a_1 x.$$ 

Thus $c_{gq-m} = g a_q^{q-1} a_{q-m}$. So $c_{gq-m} = 0$ implies that $a_{q-m} = 0$. By induction, $f(x)$ reduces to

$$f(x) = a_q x^q + a_g x^g + \cdots + a_2 x^2 + a_1 x.$$ 

Now we want to show that $a_t = 0$ for all $2 \leq t \leq g$. Looking at the first row of the matrix $M$, we see that

$$c_{q-1} = c_{q-2} = \cdots = c_{g+1} = 0.$$ 

By induction we can show that this means

$$a_2 = a_3 = \cdots = a_g = 0.$$ 

In fact, we first observe that $c_{g+1} = g a_1^{g-1} a_2$. Because $a_1 \neq 0$, $c_{g+1} = 0$ implies $a_2 = 0$. Now assume that $a_i = 0$ for all $i$ with $2 \leq i < m \leq g$. We
want to show that \( a_m = 0 \). Under the above assumption,

\[
    f(x) = a_q x^q + a_g x^g + \cdots + a_m x^m + a_1 x.
\]

Therefore \( c_{g-1+m} = g a_1^{q-1} a_m \). Again because \( a_1 \neq 0 \), we see that \( c_{g-1+m} = 0 \) implies \( a_m = 0 \). Thus by induction we have shown that

\[
    f(x) = a_q x^q + a_1 x \quad \text{with } a_1 a_q \neq 0.
\]

Now we can write the equation of the curve \( C \) as

\[
    x^q + \mu x = \lambda y^2
\]

for some \( \mu, \lambda \in \mathbb{F}_{q^2}^* \).

Since \( C \) is maximal over \( \mathbb{F}_{q^2} \), one can show easily that the additive polynomial

\[
    A(x) := x^q + \mu x
\]

has a nonzero root \( \beta \in \mathbb{F}_{q^2}^* \). In fact, more is true: it follows from [5, Theorem 4.3] that all roots of \( A(x) \) belong to \( \mathbb{F}_{q^2} \).

Set \( \alpha := \beta^q \) and \( x_1 := \alpha x \). Then

\[
    A(x) = \alpha^{-q} (\alpha x)^q + (\mu \alpha^{-1})(\alpha x).
\]

Hence

\[
    A(x) = \alpha^{-q} (x_1^q + \mu \alpha^{-1} x_1)
\]

has the root \( x_1 = \alpha \beta = \beta^{q+1} \in \mathbb{F}_q^* \). So \( \mu \alpha^{q-1} = -1 \), and this means that \( C \) is equivalent to the curve given by the equation

\[
    x_1^q - x_1 = ay^2, \quad \text{where} \quad a := \alpha^q \lambda.
\]

Now as we have seen at the end of the proof of Theorem 5.4, this curve is isomorphic to the curve given by the equation

\[
    y^2 = x^q + x.
\]

In the next theorem we also classify minimal hyperelliptic curves over \( \mathbb{F}_{q^2} \) in characteristic \( p > 2 \) with genus satisfying \( g = (q - 1)/2 \):

**Theorem 6.3.** Suppose that \( p > 2 \). There is a unique curve \( C \) which is a minimal hyperelliptic curve over \( \mathbb{F}_{q^2} \) with genus \( g = (q - 1)/2 \); it can be given by the affine equation

\[
    ay^2 = x^q - x \quad \text{with } a \in \mathbb{F}_{q^2}^* \text{ such that } a^{(q^2-1)/2} \neq (-1)^{(q+1)/2}.
\]

**Proof.** The curve \( C \) can be given by \( y^2 = f(x) \) with \( f(x) \) a square-free polynomial in \( \mathbb{F}_{q^2}[x] \) of degree \( \deg(f(x)) = q = p^n \). We have

\[
    \#C(\mathbb{F}_{q^2}) = q^2 + 1 - (q - 1)q = q + 1
\]

and in particular \( \#C(\mathbb{F}_{q^2}) \) is an even number. As in the proof of Theorem 6.1 we can assume that \( f(0) = 0 \), and from \( C^n = 0 \) we then conclude that

\[
    f(x) = a_q x^q + a_1 x \quad \text{with } a_1 a_q \neq 0.
\]

Hence the minimal curve \( C \) can be defined by

\[
    x^q + \mu x = \lambda y^2 \quad \text{for some } \mu, \lambda \in \mathbb{F}_{q^2}^*.
\]
The polynomial \( A(x) = x^q + \mu x \) must have a nonzero root in \( \mathbb{F}_{q^2} \); otherwise the map sending \( x \) to \( A(x) \) would be an additive automorphism of \( \mathbb{F}_{q^2} \) and hence the cardinality of rational points would satisfy
\[
\#C(\mathbb{F}_{q^2}) = 1 + q^2.
\]

Having such a nonzero root \( \beta \in \mathbb{F}_{q^2}^* \), we conclude as in the proof of Theorem 6.1 that the curve \( C \) can be given by the equation
\[
x_1^q - x_1 = ay^2 \quad \text{with } a \in \mathbb{F}_{q^2}^*.
\]

It now follows from Proposition 5.2 that
\[
a^v \neq (-1)^u \quad \text{with } u = \frac{q + 1}{2} \text{ and } v = \frac{q^2 - 1}{2}.
\]

The element \( a \in \mathbb{F}_{q^2}^* \) satisfies \( a^v = \pm 1 \). Consider two curves over \( \mathbb{F}_{q^2} \) given by \( a_1 y^2 = x^q - x \) and \( a_2 y^2 = x^q - x \) respectively, with \( a_1^v \neq (-1)^u \) and \( a_2^v \neq (-1)^u \). Hence \( a_1^v = a_2^v \) and \( a_2 = a_1 c^2 \) for some \( c \in \mathbb{F}_{q^2}^* \). The substitution \( y \mapsto cy \) shows that the two curves above are isomorphic to each other.

The theorem below is the analogue of Theorem 6.1 in characteristic \( p = 2 \):

**Theorem 6.4.** Suppose that \( p = 2 \). There exists a unique maximal hyperelliptic curve over \( \mathbb{F}_{q^2} \) with genus \( g = q/2 \). It can be given by the affine equation
\[
y^2 + y = x^{q+1}.
\]

**Proof.** With arguments as in the proof of Corollary 5.8, we find that the curve can be given by \( y^2 + y = f(x) \) with \( f(x) \in \mathbb{F}_{q^2}[x] \) of degree \( q + 1 \). The result now follows from item 3) of Theorem 2.3 of [3].

**7. Serre maximal curves.** In this section we consider curves \( C \) that attain the Serre upper bound (we call them SW-maximal curves), i.e., curves \( C \) defined over \( \mathbb{F}_q \) such that
\[
\#C(\mathbb{F}_q) = q + 1 + [2\sqrt{q}]g(C).
\]

**Proposition 7.1.** Let \( k \) be a field with \( q \) elements and set \( m = [2\sqrt{q}] \). For a smooth projective curve \( C \) of genus \( g \) defined over \( k = \mathbb{F}_q \), the following conditions are equivalent:

- The curve \( C \) is SW-maximal.
- The L-polynomial of \( C \) satisfies \( L(t) = (1 + mt + qt^2)^g \).

**Proof.** See [10] and [17, p. 180].

**Corollary 7.2.** Let \( C \) be a smooth projective curve of genus \( g \) defined over \( k = \mathbb{F}_q \) which attains the Serre upper bound. Then its Hasse–Witt
invariant satisfies
\[ \sigma(C) = \begin{cases} g & \text{if } \gcd(p, m) = 1, \\ 0 & \text{if } p \mid m. \end{cases} \]

**Proof.** Since \( C \) is SW-maximal, from Proposition 7.1 we have

\[
L(t) = (1 + mt + qt^2)^g = 1 + \sum_{i=1}^{g} \binom{g}{i} t^i (m + qt)^i
\]

\[= 1 + \sum_{i=1}^{g} \left( \binom{g}{i} t^i \sum_{j=0}^{i} \binom{i}{j} m^{i-j} q^j t^j \right).\]

If \( p \mid m \), then it is clear from Proposition 2.3 that \( \sigma(C) = 0 \). Now suppose that \( \gcd(p, m) = 1 \). We have to show that the coefficient of \( t^g \) in the \( L \)-polynomial \( L(t) \) is not divisible by \( p \). Denote it by \( a_g \). From the last equality above, we then obtain

\[ a_g \equiv m^g \pmod{p}. \]

We recall that an admissible rational function \( f(x) \in \mathbb{k}(x) \) is such that every pole of \( f(x) \) in the algebraic closure \( \overline{k} \) occurs with a multiplicity prime to the characteristic \( p \). We then have:

**Theorem 7.3.** Let \( C \) be an SW-maximal curve over \( \mathbb{F}_q \) given by an affine equation of the form

\[(7.1) \quad A(y) = f(x),\]

where \( A(y) \in \mathbb{F}_q[y] \) is an additive and separable polynomial and where \( f(x) \) is an admissible rational function. Set \( m = [2\sqrt{q}] \) and suppose that \( \gcd(p, m) = 1 \). Then all poles of \( f(x) \) are simple.

**Proof.** We know that a curve \( C \) given by (7.1) is ordinary if and only if the rational function \( f(x) \) has only simple poles (see [20, Corollary 1]). Thus Theorem 7.3 follows directly from Corollary 7.2.

**Corollary 7.4.** Let \( C \) be an SW-maximal curve as in the above theorem with \( \gcd(p, m) = 1 \). Then its genus satisfies \( g(C) = (\deg A - 1)(s - 1) \), where \( s \) denotes the number of poles of \( f(x) \).

We finish with two examples of SW-maximal Artin–Schreier curves. In the first example \( p \mid m \) and the rational function \( f(x) \) has a nonsimple pole; in the second, \( \gcd(p, m) = 1 \) and \( f(x) \) has only simple poles, as follows from Theorem 7.3.

**Example 7.5.** Let \( k = \mathbb{F}_2 \). So \( m = [2\sqrt{2}] = 2 \) and \( p \mid m \). Let \( C \) be the elliptic curve over \( \mathbb{F}_2 \), given by the affine equation

\[ y^2 + y = x^3 + x. \]
One can easily see that $C$ has five $k$-rational points, which means that $C$ is SW-maximal over $k$. Note that $f(x) = x^3 + x$ has a pole of order 3 at infinity.

**Example 7.6.** Let $k = \mathbb{F}_8$. So $m = [2\sqrt{8}] = 5$ and $\gcd(p, m) = 1$. Let $C$ be the elliptic curve over $\mathbb{F}_8$, given by the affine equation

$$y^2 + y = \frac{x^2 + x + 1}{x}.$$  

Then the curve $C$ is SW-maximal since it has 14 $k$-rational points. In fact, the two simple poles of $(x^2 + x + 1)/x$ are totally ramified in the extension $k(x,y)/k(x)$ and they correspond to two $k$-rational points on $C$. By Hilbert’s 90 Theorem, we have

$$\#C(\mathbb{F}_8) = 2 + 2B,$$

where $B := \#\{\alpha \in \mathbb{F}_8 \mid \text{tr}_{\mathbb{F}_8|\mathbb{F}_2}(\alpha^2 + \alpha + 1) = 0\}$. But one can show that $B = 6$; in fact, the points $x = \alpha \in \mathbb{F}_8 \setminus \mathbb{F}_2$ are completely splitting in $k(x,y)/k(x)$.

**References**


218 A. Garcia and S. Tafazolian


IMPA-Instituto Nacional de Matemática Pura e Aplicada
Estrada Dona Castorina 110, Jardim Botânico
22460-320, Rio de Janeiro, Brazil
E-mail: garcia@impa.br
saeed@impa.br

Received on 8.10.2007