A family of maximal hyperelliptic function fields of genus 2

Tadashi WASHIO and Tetsuo KODAMA*

Department of Mathematics, Faculty of Education
Nagasaki University, Nagasaki 852-8521, Japan
(Received October 31, 2006)

Abstract
This note is devoted to studying certain maximal hyperelliptic function fields of genus two defined over a finite field.

1. Introduction
A function field $K$ of one variable over a finite field $\mathbb{F}_q$ of order $q$ is said to be maximal if the number $N$ of degree one prime divisors of $K$ is given by the Weil upper bound as

$$N = 1 + q + 2g\sqrt{q},$$

where $g$ means the genus of $K$.

The maximal function fields or maximal curves have been studied extensively by Shparlinski[5], Stepanov[6] and Stichtenoth[7,8] and we have also obtained the explicit examples in the case of maximal hyperelliptic function fields whose defining equations are of the form

$$Y^2 = X^{2g+1} + a \text{ or } Y^2 = X(X^{2g} + a), \text{ (see [2,3]).}$$

For the general theory of algebraic function fields of one variable, refer to Deuring[1] and Stichtenoth[7]. "Prime divisor" is synonymous with "place".

*Professor emeritus, Kyushu University, Fukuoka 810-8560, Japan.
In the present note we want to consider a function field with genus two whose defining equation is of the form

\[ Y^2 = X(X^2 + X + s)(X^2 + X + t) \]

and we will prove the following result.

Assume that \( p \) is a prime number satisfying \( p \equiv 9 \pmod{16} \) and denote by \( r \) the element in \( \mathbb{F}_p \) satisfying \( 8r = 1 \). Moreover denote by \( s \) and \( t \) two distinct solutions in \( \mathbb{F}_p \) of the quadratic equation

\[ X^2 - 2rX + 4r^3 = 0. \]

Then the hyperelliptic function field defined by \( Y^2 = X(X^2 + X + s)(X^2 + X + t) \) over \( \mathbb{F}_{p^2} \) is maximal.

Our proof is based on the theory of Gauss and Jacobi sums.

2. Roots of biquadratic equations

Throughout this section we assume that \( p \) is a prime number satisfying \( p \equiv 9 \pmod{16} \) and denote by \( r \) the element in \( \mathbb{F}_p \) satisfying \( 8r = 1 \). Moreover denote by \( s \) and \( t \) two distinct solutions in \( \mathbb{F}_p \) of the quadratic equation

\[ X^2 - 2rX + 4r^3 = 0. \]

In our case we have known that two polynomials \( X^2 + X + s \) and \( X^2 + X + t \) are irreducible over \( \mathbb{F}_p \), (see [9]).

Now we put

\[ f(X) = (X^2 + X + s)(X^2 + X + t) \]

and discuss properties of the roots of the biquadratic equation \( f(X) = \alpha \) for an element \( \alpha \in \mathbb{F}_{p^2} \).
Let $F = \mathbb{F}_{p^2}$, $F^* = F \setminus \{0\}$ and $F^{*4} = \{ \lambda^4 \mid \lambda \in F^* \}$. Furthermore we denote by $\theta$ a generator of the cyclic group $F^*$ and fix it. Also put $\iota = \theta^{(p^2-1)/16}$ and $i = i^4$. Clearly $\iota$ is a primitive 16-th root of unity and $i$ is a primitive 4-th root of unity.

Moreover, for $\alpha \in F$, we denote by $\Lambda(\alpha)$ and $\Lambda'(\alpha)$ two roots of the quadratic equation

$$X^2 - 4\alpha X + r^4 = 0.$$ 

Then, because of $\Lambda(\alpha)\Lambda'(\alpha) = r^4$, it is clear that $\Lambda(\alpha) \in F^{*4}$ is equivalent to $\Lambda'(\alpha) \in F^{*4}$. Clearly $\alpha = \pm 4r^3$ if and only if $\Lambda(\alpha) = \Lambda'(\alpha)$ and then $\Lambda(\alpha) = \pm r^2$.

Furthermore let $\chi$ be the multiplicative quadratic character of $F$. Then, from our assumption $p \equiv 9 \pmod{16}$, we have $(p^2 - 1)/16 \equiv 1 \pmod{2}$ and so $\chi(\iota) = -1$. The Legendre symbol $\left(\frac{2}{p}\right) = 1$ gives us $\chi(\sqrt{2}) = \chi(\sqrt{r}) = 1$.

**Lemma 1.** (1) There exists an $x$ in $F$ satisfying $\Lambda(f(x)) = \Lambda'(f(x)) = r^2$ and then the roots of the equation $f(X) = f(x)$ are given by $0, -1$ and $-4r$. Clearly $r^2 \in F^{*4}$, $f(x) = 4r^3$ and $\chi(-4r) = \chi(-4r + 1) = 1$.

(2) There exists an $x$ in $F$ satisfying $\Lambda(f(x)) = \Lambda'(f(x)) = -r^2$ and then the roots $a$’s of the equation $f(X) = f(x)$ are given by $-4s$ and $-4t$. Clearly $-r^2 \in F^{*4}$, $f(a) = -4r^3$ and $\chi(a) = \chi(a + 1) = 1$.

(3) If $\mu \in F^*$ and $\mu^4 \neq \pm r^2$, then there exists an $x$ in $F$ satisfying $\Lambda(f(x)) = \mu^4$ or $\Lambda'(f(x)) = \mu^4$. In this case, the equation $f(X) = f(x)$ has four distinct roots $a$’s in $F$ and $\chi(a(a + 1)) = 1$ holds. Clearly $f(a) = \lambda^4 + 4r^6/\lambda^4$, where $\lambda^4 = 2r\mu^4$. 
PROOF. It is clear that $\pm r^2 \in F^*4$, $\Lambda(4r^3) = \Lambda'(4r^3) = r^2$ and $\Lambda(-4r^3) = \Lambda'(-4r^3) = -r^2$. Therefore the assertions (1) and (2) follow at once from

$$f(X) - 4r^3 = X(X + 1)(X + 4r)^2,$$

$$f(X) + 4r^3 = \{(X + 4s)(X + 4t)\}^2.$$

To prove the assertion (3) let us assume that $\mu \in F^*$ and $\mu^4 \neq \pm r^2$. Moreover we put $\lambda^4 = 2r\mu^4$ and $\alpha = \lambda^4 + 4r^6/\lambda^4$. Then it is clear that

$$(4\lambda^4)^2 - 4\alpha(4\lambda^4) + r^4 = 0$$

and so we have $\Lambda(\alpha) = \mu^4$ or $\Lambda'(\alpha) = \mu^4$.

Since $f(X)$ has an expression as

$$f(X) = (X^2 + X + r)^2 - 4r^3$$

and $\alpha$ has two ways of expressions as

$$\alpha = (\lambda^2 i^{2n} + \frac{2r^3}{\lambda^2 i^{2n}})^2 - 4r^3 \quad (n = 0, 1)$$

we see

$$f(X) - \alpha = \prod_{n=0,1} \{X^2 + X + r - (\lambda^2 i^{2n} + \frac{2r^3}{\lambda^2 i^{2n}})\}.$$  

Here, for $n = 0$ or $1$, the quadratic equation

$$X^2 + X + r - (\lambda^2 i^{2n} + \frac{2r^3}{\lambda^2 i^{2n}}) = 0$$

has the discriminant

$$4(\lambda i^n + \frac{4r^2}{\lambda i^n})^2 \neq 0$$

and hence it has distinct roots in $F$. 
Therefore the equation $f(X) - \alpha = 0$ has four distinct roots $a$'s in $F$. In this case it is clear that

$$a^2 + a = (\lambda i^n - \frac{4r^2}{\lambda i^n})^2 \neq 0$$

for some $n$ and so we get $\chi(a(a+1)) = 1$. Lemma 1 is thereby proved.

**Lemma 2.** Let $a \in F$. If $a = 0, -1$ or $\chi(a(a+1)) = 1$, then

$$\Lambda(f(a)), \Lambda'(f(a)) \in F^{*4}$$

holds. In this case, if we put $\Lambda(f(a)) = \mu^4 (\mu \in F^*)$, then

$$\chi(\mu) = \begin{cases} 
1 & \text{if } a = 0, -1 \text{ or } \chi(a) = \chi(a+1) = 1, \\
-1 & \text{if } \chi(a) = \chi(a+1) = -1.
\end{cases}$$

**Proof.** To begin with, we assume that $a = 0, -1$ or $\chi(a) = \chi(a+1) = 1$. In this case, $F$ contains $\sqrt{a}$ and $\sqrt{a+1}$. So we put

$$\nu = \sqrt{a} + \sqrt{a+1},$$

$$\nu' = \sqrt{a} - \sqrt{a+1}.$$

Then calculation shows that

$$r^2\nu^8 + r^2\nu'^8 = 4f(a),$$

$$(r^2\nu^8)(r^2\nu'^8) = r^4,$$

and so that

$$\{ \Lambda(f(a)), \Lambda'(f(a)) \} = \{ r^2\nu^8, r^2\nu'^8 \}.$$
It is clear that $r^2\nu^8, r^2\nu'^8 \in F^{*4}$. If we put $\Lambda(f(a)) = \mu^4 (\mu \in F^*)$ then $\mu$ has an expression of $\mu = i^n\sqrt{r\nu^2} \text{ or } \mu = i^n\sqrt{r\nu'^2}$ for some $0 \leq n \leq 3$. This leads to $\chi(\mu) = 1$.

We next assume that $\chi(a) = \chi(a + 1) = -1$. In this case, because of $\chi(\theta) = -1$, $F$ contains $\sqrt{a\theta}$ and $\sqrt{(a + 1)\theta}$. So we put

$$\nu = \sqrt{a\theta} + \sqrt{(a + 1)\theta},$$
$$\nu' = \sqrt{a\theta} - \sqrt{(a + 1)\theta}.$$

Then calculation also shows that

$$r^2\nu^8\theta^{-4} + r^2\nu'^8\theta^{-4} = 4f(a),$$
$$(r^2\nu^8\theta^{-4})(r^2\nu'^8\theta^{-4}) = r^4,$$

and so that

$$\{\Lambda(f(a)), \Lambda'(f(a))\} = \{r^2\nu^8\theta^{-4}, r^2\nu'^8\theta^{-4}\}.$$

It is clear that $r^2\nu^8\theta^{-4}, r^2\nu'^8\theta^{-4} \in F^{*4}$. If we put $\Lambda(f(a)) = \mu^4 (\mu \in F^*)$, then $\mu$ has an expression of $\mu = i^n\sqrt{r\nu^2}\theta^{-1} \text{ or } \mu = i^n\sqrt{r\nu'^2}\theta^{-1}$ for some $0 \leq n \leq 3$. This leads to $\chi(\mu) = -1$. This completes the proof.

We now define the rational expressions $\Delta(X)$ and $\nabla(X)$ over $F$ by

$$\Delta(X) = X + \frac{1}{X} \in F(X),$$
$$\nabla(X) = X - \frac{1}{X} \in F(X).$$

Then using $\Delta(X)$ and $\nabla(X)$ we can summarise Lemmas 1 and 2 as follows.
There exists $\alpha \in F$ such that $\Lambda(\alpha) = \mu^4$ for each $\mu$ in $F^*$. From this, we have $\alpha = 2r(\mu^4 + r^4/\mu^4)$. First, if $\chi(\mu) = 1$, then we can put $\mu = \sqrt{r}\lambda^2$ for some $\lambda \in F^*$ and so we get $\alpha = 2r^3\Delta(\lambda^8)$. Secondly, if $\chi(\mu) = -1$, then we can put $\mu = i\sqrt{r}\lambda^2$ for some $\lambda \in F^*$ and so we get $\alpha = 2ir^3\nabla(\lambda^8)$.

Conversely first, if we put $\alpha = 2r^3\Delta(\lambda^8)$ for each $\lambda$ in $F^*$, then we get $\Lambda(\alpha) = r^2\lambda^8$ or $\Lambda'(\alpha) = r^2\lambda^8$ with $\chi(\sqrt{r}\lambda^2) = 1$. Secondly, if we put $\alpha = 2ir^3\nabla(\lambda^8)$ for each $\lambda$ in $F^*$, then we get $\Lambda(\alpha) = i^4r^2\lambda^8$ or $\Lambda'(\alpha) = i^4r^2\lambda^8$ with $\chi(i\sqrt{r}\lambda^2) = -1$.

Therefore Lemmas 1 and 2 lead to the following theorem.

**Theorem 1.** (1) If $a \in F$ and $a = 0, -1$ or $\chi(a) = \chi(a + 1) = 1$, then there exists $\lambda \in F^*$ such that

$$f(a) = 2r^3\Delta(\lambda^8).$$

Conversely, if $\lambda \in F^*$, then there exists $a \in F$ such that $f(a) = 2r^3\Delta(\lambda^8)$ and then $a = 0, -1$ or $\chi(a) = \chi(a + 1) = 1$. Especially, for each powers $\lambda^8$, we can select such $a$’s above in four different ways besides $\lambda^8 = \pm r^2$.

(2) If $a \in F$ and $\chi(a) = \chi(a + 1) = -1$, then there exists $\lambda \in F^*$ such that

$$f(a) = 2ir^3\nabla(\lambda^8).$$

Conversely, if $\lambda \in F^*$ then there exists $a \in F$ such that $f(a) = 2ir^3\nabla(\lambda^8)$ and then $\chi(a) = \chi(a + 1) = -1$. Especially, for each powers $\lambda^8$, we can also select such $a$’s above in four different ways.
3. An application of Jacobi sums

Let $\mathbb{F}$ be a finite field and denote by $\psi$ and $\chi$ two multiplicative characters of $\mathbb{F}$. Then we define a Jacobi sum

$$J(\psi, \chi) = \sum_{\alpha \in \mathbb{F}} \psi(\alpha) \chi(1 - \alpha).$$

For the general theory of Jacobi sums and Gaussian sums, refer to Lidl and Niederreiter[4].

**Lemma 3.** Let $p$ be a prime number satisfying $p \equiv 9 \pmod{16}$ and put $F = \mathbb{F}_{p^2}$. Moreover denote by $\chi$ and $\mu$ two multiplicative characters of $F$ such that $\chi$ is quadratic and $\mu$ is of degree 16. Then,

$$J(\mu^j, \chi) = -p$$

holds for any odd integer $j$ satisfying $1 \leq j \leq 15$.

**Proof.** For a multiplicative character $\psi$ and the canonical character $\phi$ of $F$ we define a Gaussian sum

$$G(\psi, \phi) = \sum_{\alpha \in F^*} \psi(\alpha) \phi(\alpha).$$

Then it is well-known that the Jacobi sum $J(\mu^j, \chi)$ is written of the form

$$J(\mu^j, \chi) = \frac{G(\mu^j, \phi)G(\chi, \phi)}{G(\mu^j \chi, \phi)}$$

where $j$ is an odd integer satisfying $1 \leq j \leq 15$.

Since $\chi$ is quadratic the congruence $p \equiv 1 \pmod{4}$ leads to

$$G(\chi, \phi) = -p.$$
Moreover we can get easily

\[ G(\mu^j, \phi) - G(\mu^j \chi, \phi) = \sum_{\alpha \in F^*, \chi(\alpha) = -1} \{ \mu^j(\alpha) + \mu^j(\alpha^p) \} \phi(\alpha). \]

because \( j \) is odd and \( \phi(\alpha) = \phi(\alpha^p) \).

Thus we have

\[ G(\mu^j, \phi) - G(\mu^j \chi, \phi) = \sum_{\alpha \in F^*, \chi(\alpha) = -1} \{ 1 + \mu^j(\alpha^{p-1}) \} \mu^j(\alpha) \phi(\alpha). \]

It follows from \( \chi(\alpha) = -1 \) and \( p \equiv 9 \pmod{16} \) that we see \( \mu^j(\alpha^{p-1}) = -1 \) and so \( G(\mu^j, \phi) - G(\mu^j \chi, \phi) = 0 \). Therefore, from

\[ G(\mu^j, \phi) = G(\mu^j \chi, \phi), \]

we obtain \( J(\mu^j, \chi) = -p \) which is the requested assertion.

**Theorem 2.** Let \( p \) be a prime number and put \( F = \mathbb{F}_{p^2} \). Furthermore denote by \( \theta \) a primitive root of \( F \) and fix it. Moreover put

\[ M_1 = \{ (x, y) \in F \times F \mid -x^{16} + y^2 = 1 \}, \]
\[ M_2 = \{ (x, y) \in F \times F \mid x^{16} + y^2 = 1 \}, \]
\[ M_3 = \{ (x, y) \in F \times F \mid -x^{16} + \theta y^2 = 1 \}, \]
\[ M_4 = \{ (x, y) \in F \times F \mid x^{16} + \theta y^2 = 1 \}. \]

If \( p \equiv 9 \pmod{16} \) then

1. \( \#M_1 - \#M_2 = 16p, \)
2. \( \#M_3 - \#M_4 = -16p, \)

where \( \# \) means the cardinal number of a set.
PROOF. Denote by \( \chi \) and \( \mu \) two multiplicative characters of \( F \) such that \( \chi \) is quadratic and \( \mu \) is of degree 16.

Then, by making use of the general theory of Jacobi sums, we have

\[
\#M_1 = p^2 + \sum_{j=1}^{15} \mu^j(-1)J(\mu^j, \chi),
\]

\[
\#M_2 = p^2 + \sum_{j=1}^{15} J(\mu^j, \chi),
\]

\[
\#M_3 = p^2 - \sum_{j=1}^{15} \mu^j(-1)J(\mu^j, \chi),
\]

\[
\#M_4 = p^2 - \sum_{j=1}^{15} J(\mu^j, \chi).
\]

and so we get

\[
\#M_1 - \#M_2 = \sum_{j=1}^{15} \{\mu^j(-1) - 1\}J(\mu^j, \chi),
\]

\[
\#M_3 - \#M_4 = \sum_{j=1}^{15} \{1 - \mu^j(-1)\}J(\mu^j, \chi).
\]

Furthermore we put \( \iota = \theta^{(p^2-1)/16} \). Then \( \iota \) is a primitive 16-th root of unity and \( (p^2 - 1)/16 \equiv 1 \pmod{2} \). So we have \( \mu(-1) = \mu(\iota^8) = \chi(\iota) = -1 \).

Therefore, our assertions follow at once from Lemma 3.
4. The main result

Our main result is stated as follows.

**Theorem 3.** Let $p$ be a prime number satisfying $p \equiv 9 \pmod{16}$ and denote by $r$ the element in $\mathbb{F}_p$ satisfying $8r = 1$. Moreover denote by $s$ and $t$ two distinct solutions in $\mathbb{F}_p$ of the equation $X^2 - 2rX + 4r^3 = 0$. Then the hyperelliptic function field defined by

$$Y^2 = X(X^2 + X + s)(X^2 + X + t)$$

over $\mathbb{F}_p^2$ is maximal function field of genus two.

In this section we discuss under the same assumptions for $p, r, s$ and $t$ as in Theorem 3. We put $F = \mathbb{F}_p^2$ and denote by $\chi$ the multiplicative quadratic character of $F$ with $\chi(0) = 0$. We denote by $\theta$ a generator of the cyclic group $F^*$ and put $i = \theta^{(p^2-1)/4}$.

In order to prove Theorem 3, we prepare the following notations:

$$A_1 = \{ \lambda^8 | \lambda \in F^*, \lambda^8 \neq \pm 1, \chi(2r^3\Delta(\lambda^8)) = 1 \},$$

$$A_2 = \{ \lambda^8 | \lambda \in F^*, \lambda^8 \neq \pm 1, \chi(2ir^3\nabla(\lambda^8)) = 1 \},$$

$$A_3 = \{ \lambda^8 | \lambda \in F^*, \lambda^8 \neq \pm 1, \chi(2r^3\Delta(\lambda^8)) = -1 \},$$

$$A_4 = \{ \lambda^8 | \lambda \in F^*, \lambda^8 \neq \pm 1, \chi(2ir^3\nabla(\lambda^8)) = -1 \}.$$  

where $\Delta(X) = X + 1/X$ and $\nabla(X) = X - 1/X$.

**Lemma 4.** Let notations $M_1, M_2, M_3, M_4$ be same as in Theorem 2. Then the following equalities hold:

1. $\#M_1 = 16 \#A_1 + 34$.
2. $\#M_2 = 16 \#A_2 + 18$.
(3) \(\#M_3 = 16 \#A_3\).

(4) \(\#M_4 = 16 \#A_4 + 16\).

**Proof.** Since \(\chi(2r^3) = \chi(2ir^3) = 1\), we have

\[
A_1 = \{ \lambda^8 \mid \lambda \in F^*, \lambda^8 \neq \pm 1, \chi(\Delta(\lambda^8)) = 1 \},
\]

\[
A_2 = \{ \lambda^8 \mid \lambda \in F^*, \lambda^8 \neq \pm 1, \chi(\nabla(\lambda^8)) = 1 \},
\]

\[
A_3 = \{ \lambda^8 \mid \lambda \in F^*, \lambda^8 \neq \pm 1, \chi(\Delta(\lambda^8)) = -1 \},
\]

\[
A_4 = \{ \lambda^8 \mid \lambda \in F^*, \lambda^8 \neq \pm 1, \chi(\nabla(\lambda^8)) = -1 \}.
\]

First we will prove the assertion (1). Take \(\lambda^8 \in A_1\). Then \(\chi(\Delta(\lambda^8)) = 1\) leads to that there exists \(z \in F^*\) satisfying \(\lambda^8 + 1/\lambda^8 = z^2\), i.e., \(\lambda^{16} + 1 = z^2\lambda^8\) and so if we put \(x = \lambda\) and \(y = z\lambda^4\), then \((x, y) \in M_1\). Clearly this \((x, y)\) yields 16 solutions of the equation \(-X^{16} + Y^2 = 1\). In addition to such solutions, \(M_1\) contains \((0,1), (0,-1)\) and 32 solutions \((x, y)\) such that \(x^{16} = 1\) and \(y^2 = 2\). Thus we obtain \(\#M_1 = 16 \#A_1 + 34\).

In order to prove the assertion (2), take \(\lambda^8 \in A_2\). Then \(\chi(\nabla(\lambda^8)) = 1\) leads to that there exists \(z \in F^*\) satisfying \(\lambda^8 - 1/\lambda^8 = z^2\), i.e., \(\lambda^{16} - 1 = z^2\lambda^8\) and so if we put \(x = \lambda\) and \(y = iz\lambda^4\), then \((x, y) \in M_2\). Clearly this \((x, y)\) yields 16 solutions of the equation \(X^{16} + Y^2 = 1\). In addition to such solutions, \(M_2\) contains \((0,1), (0,-1)\) and 16 solutions \((x, 0)\) such that \(x^{16} = 1\). So we have \(\#M_2 = 16 \#A_2 + 18\).

To prove the assertion (3) we use \(\chi(\theta) = -1\). We also take \(\lambda^8 \in A_3\). Then \(\chi(\Delta(\lambda^8)) = -1\) leads to that there exists \(z \in F^*\) satisfying \(\lambda^8 + 1/\lambda^8 = \theta z^2\), i.e., \(\lambda^{16} + 1 = \theta z^2\lambda^8\) and so if we put \(x = \lambda\) and \(y = z\lambda^4\), then \((x, y) \in M_3\). Clearly this \((x, y)\) yields 16 solutions of the equation \(-X^{16} + \theta Y^2 = 1\). Since \(M_3\) contains no solutions except for such solutions we get \(\#M_3 = 16 \#A_3\).
Finally we will prove the assertion (4). Take \( \lambda^8 \in A_4 \). Then \( \chi(\nabla(\lambda^8)) = -1 \) leads to that there exists \( z \in F^* \) satisfying \( \lambda^8 - 1/\lambda^8 = \theta z^2 \), i.e., \( \lambda^{16} - 1 = \theta z^2 \lambda^8 \) and so if we put \( x = \lambda \) and \( y = iz\lambda^4 \), then \( (x, y) \in M_4 \). This \( (x, y) \) also yields 16 solutions of the equation \( X^{16} + \theta Y^2 = 1 \). In addition to such solutions, \( M_4 \) contains 16 solutions \( (x, 0) \) such that \( x^{16} = 1 \). So we have \( \#M_4 = 16 \#A_4 + 16 \). This completes the proof.

From now on, we will prove Theorem 3.

**Proof of Theorem 3.** Let \( K \) be the hyperelliptic function field defined by \( Y^2 = X f(X) \) over \( F = \mathbb{F}_{p^2} \) where

\[
f(X) = (X^2 + X + s)(X^2 + X + t) \in \mathbb{F}_p[X].
\]

Let \( N \) be the number of places of degree one of \( K \). Then it is well-known that \( N \) is written by

\[
N = p^2 + 1 + S
\]

with

\[
S = \sum_{a \in F} \chi(af(a)),
\]

where \( \chi \) means the multiplicative quadratic character of \( F \).

Since the genus of \( K \) is equal to 2, we have to show \( S = 4p \). It is obvious that \( \chi(a(a + 1)) = \chi(a(-a - 1)) \) and \( f(a) = f(-a - 1) \) for any \( a \in F \).

So, if we put

\[
V^+ = \{ 2r^3 \Delta(\lambda^8) \mid \lambda \in F^*, \lambda^8 \neq \pm 1 \},
\]

\[
V^- = \{ 2ir^3 \nabla(\lambda^8) \mid \lambda \in F^*, \lambda^8 \neq \pm 1 \},
\]
then, by making use of Theorem 1, we get

\[ S = \chi(-f(-1)) + \chi(-4rf(-4r)) + \chi(-4sf(-4s)) + \chi(-4tf(-4t)) \]
\[ + 4 \sum_{\alpha \in V^+} \chi(\alpha) - 4 \sum_{\alpha \in V^-} \chi(\alpha) \]
\[ = 4 + 4 \sum_{\alpha \in V^+} \chi(\alpha) - 4 \sum_{\alpha \in V^-} \chi(\alpha). \]

Furthermore it is clear for different values \( \lambda^8 \) and \( \mu^8 \) that \( \Delta(\lambda^8) = \Delta(\mu^8) \), iff \( \lambda^8 \mu^8 = 1 \) and that \( \nabla(\lambda^8) = \nabla(\mu^8) \), iff \( \lambda^8 \mu^8 = -1 \). This yields

\[ 2 \sum_{\alpha \in V^+} \chi(\alpha) = \#A_1 - \#A_3, \]
\[ 2 \sum_{\alpha \in V^-} \chi(\alpha) = \#A_2 - \#A_4, \]

and so we have

\[ S = 4 + 2(\#A_1 - \#A_3) - 2(\#A_2 - \#A_4) \]
\[ = 4 + 2(\#A_1 - \#A_2) - 2(\#A_3 - \#A_4). \]

Using Lemma 4, we get

\[ S = 4 + \frac{1}{8}(\#M_1 - \#M_2 - 16) - \frac{1}{8}(\#M_3 - \#M_4 + 16). \]

It follows immediately from Theorem 2 that we obtain \( S = 4p \). Theorem 3 is thereby proved.

**Remark:** We have proved in [9] that the hyperelliptic function field defined by \( Y^2 = X(X^2 + X + s)(X^2 + X + t) \) over \( \mathbb{F}_p \) has just \( p + 1 \) places of degree one.
References


