On Class Numbers of Hyperelliptic Function Fields

Tadashi Washio

Department of Mathematics, Faculty of Education, Nagasaki University, Nagasaki

(Received Oct. 31, 1977)

Abstract. Let \( F=\text{GF}(p) \) be a finite prime field of characteristic \( p\neq 2 \). Let \( K=F(x,y) \) be a hyperelliptic function field over \( F \) defined by an equation \( y^2=x^n+a \) (\( a\neq 0, a\in F \)), where \( n \) denotes an odd number such that \( n>1 \) and \( p\nmid n \). Let \( h \) be the class number of \( K \) and \( g \) the genus of \( K \). Then, we have proved that \( h=p+1 \) if \( n=3 \) and \( p\equiv 2 \) mod 3. ([4], Theorem 1 (i)). This particular fact can be generally expressed as follows:

Given \( n \), there exists an integer \( c \) such that \( h=p^g+1 \) whenever \( p\equiv c \) mod \( n \). In this note, it is shown that this generalization is true in the particular case of \( n=5 \) and of \( n=7 \).

1. Introduction. Let \( F=\text{GF}(p) \) be a finite prime field of characteristic \( p\neq 2 \). Let \( K=F(x,y) \) be a hyperelliptic function field over \( F \) defined by an equation \( y^2=x^n+a \) (\( a\neq 0, a\in F \)), where \( n \) denotes an odd number such that \( n>1 \) and \( p\nmid n \). Let \( h \) be the class number of \( K \) and \( g \) the genus of \( K \). It is obvious that \( g=(n-1)/2 \). (M. Deuring[1], §17). We will then discuss the following question;

Does there exist an integer \( c \) which depends only on \( n \) such that \( h=p^g+1 \) whenever \( p\equiv c \) mod \( n \)?

In the case where \( n=3 \), we had an answer in the affirmative. ([4], Theorem 1 (i)). In this note, we will give an affirmative answer only in the case of \( n=5 \) and of \( n=7 \).

2. Preliminary. In this section, we will state a method of estimating for class numbers of algebraic function fields without proof but with references. Let \( K \) be an algebraic function field of one variable having Galoisfield \( GF(q) \) as its exact field of constants. The order of the finite group of divisor classes of degree zero is called the class number of \( K \).

Then, with the \( L \)-function of \( K \), it is well known that the class number \( h \) is given by

\[
(1) \quad h = L(1) \quad \text{where} \quad L(u) = 1 + a_1u + a_2u^2 + \cdots + a_{g+1}u^{g+1} + \cdots + q^{g-2}a_{2g^{g-2}} + q^{g-1}a_1u^{g-1} + q^gu^{2g} \in \mathbb{Z}[u]
\]

\( g \) being the genus of \( K \). (M. Eichler [2], p. 305).
Moreover, the explicit expression for coefficients $a_1$, $a_2$, $a_3$ is given by

\begin{equation}
\begin{align*}
2a_2 &= N_1^2 - (2q+1)N_1 + 2N_2 + 2q \\
6a_3 &= N_1^3 - 3qN_1^2 + (3q-1)N_1 - 6(q+1)N_2 + 6N_1N_2 + 6N_3
\end{align*}
\end{equation}

where $N_i$ denotes the number of prime divisors of degree $i$ of $K$. (M. L. Madan and C. S. Queen [31, p. 427). Thus, for our purpose, it is enough to compute the number of prime divisors of degree $i$.

3. Results. Let us now answer the question in Section I of this note only in the case of $n=5$ and of $n=7$. Since we need to estimate the number of prime divisors of degree one, we will start by proving the following theorem.

**Theorem 1.** Let $F$ be a finite field $GF(q)$ of characteristic $\neq 2$. Given an odd number $n>1$, let $K$ be a hyperelliptic function field over $F$ defined by an equation $y^2=x^n+a$ ($a \neq 0, a \in F$). Let $N_1$ denote the number of prime divisors of degree one. Then, we have $N_1=q+1$ if $n$ and $q-1$ are coprime.

**Proof.** Since $n$ is odd, there exists only one infinite prime divisor of $K$. So we get the formula as follows;

\begin{equation}
N_1 = 1 + \#\{(\alpha, \beta) \in F \times F \mid \beta^2 = \alpha^n + a\}
\end{equation}

where $\#S$ means the number of elements in $S$.

Moreover, for the sake of convenience, we will denote by $F^*$ the multiplicative group of non-zero elements of $F$. Then it is easy to verify that $\{\alpha^n \mid \alpha \in F^*\} = F^*$. This is due to the assumption $(q-1, n) = 1$ and to the fact that $F^*$ is a cyclic group of order $q-1$. Therefore, we have $\{\alpha^n \mid \alpha \in F\} = F$, so we see $\{\alpha^n + a \mid \alpha \in F\} = F$.

This equality means that

\begin{equation}
\begin{align*}
\#\{(\alpha, 0) \in F \times F \mid \alpha^n + a = 0\} &= 1 \\
\#\{(\alpha, \beta) \in F \times F \mid \beta^2 = \alpha^n + a, \beta \neq 0\} &= q-1
\end{align*}
\end{equation}

because of the fact that the number of elements of the form $\beta^2$ ($\beta \in F^*$) equals to $(q-1)/2$ and that we can associate such a element $\beta^2$ with two prime divisors of degree one of $K$. Thus, by making use of the formula (3) above, we obtain $N_1 = 1 + 1 + (q-1) = q+1$. Theorem 1 is thereby proved.

Now let us turn to our question in Section I. As an application of Theorem 1, we can easily answer our question for $n=5$ in the affirmative. In fact, we will prove the following theorem.

**Theorem 2.** Let $F=GF(p)$ be a finite prime field of characteristic $p \neq 2$. Let $K=F(x, y)$ be a hyperelliptic function field over $F$ defined by an equation $y^2=x^5+a$ ($a \neq 0, a \in F$). Denote by $h$ the class number of $K$. Then we have $h=p^2+1$ and $L(u)=1+p^2u^4$ if $p \equiv 2$ or 3 mod 5.
Proof. We will indicate by \( N_i \) (\( i=1,2 \)) the number of prime divisors of degree \( i \) in \( K \). Moreover we will denote a constant field extension of \( K \) of degree two by \( \overline{K} \) and also the number of prime divisors of degree one of \( \overline{K} \) by \( \overline{N}_1 \). By means of our assumption \( p \equiv 2 \) or \( 3 \mod 5 \), it is obvious that \( (p-1,5)=1 \) and \( (p^2-1,5)=1 \).

Then, applying Theorem 1 to \( K \) and \( \overline{K} \), we have \( N_1=p+1 \) and \( \overline{N}_1=p^2+1 \). Thus we see \( N_2=p(p-1)/2 \) in view of the fact that the relation among \( N_1, N_2, \overline{N}_1 \) is given by \( \overline{N}_1 = N_1+2N_2 \). Hence we can easily obtain \( a_1 = a_2 = 0 \) because of the formula (2). In particular \( L(u)=1+p^2u^4 \). Therefore the formula (1) leads to \( h=p^2+1 \). This completes the proof of Theorem 2.

Finally we will give an affirmative answer to our question in the case of \( n=7 \).

**Theorem 3.** Let \( F=GF(p) \) be a finite prime field of characteristic \( p \neq 2 \). Let \( K=F(x,y) \) be a hyperelliptic function field over \( F \) defined by an equation \( y^2=x^7+a (a \neq 0, a \in F) \). Denote by \( h \) the class number of \( K \). Then we have \( h=p^3+1 \) and \( L(u)=1+p^3u^6 \) if \( p \equiv 3 \) or \( 5 \mod 7 \).

Proof. We will denote by \( N_i \) (\( i=1,2,3 \)) the number of prime divisors of degree \( i \) of \( K \). Let \( \overline{K} \) and \( \overline{\overline{K}} \) be constant field extensions of \( K \) of degree two and of three respectively. Moreover, denote by \( \overline{N}_1 \) and \( \overline{N}_1 \) the numbers of prime divisors of \( \overline{K} \) and of \( \overline{\overline{K}} \) respectively. Then \( N_2 \) and \( N_3 \) are explicitly given by

\[
\overline{N}_1 = N_1 + 2N_2 \quad \text{and} \quad \overline{N}_1 = N_1 + 3N_3.
\]

By means of our assumption \( p \equiv 3 \) or \( 5 \mod 7 \), we can obviously obtain \( (p-1,7)=1 \), \( (p^2-1,7)=1 \) and \( (p^3-1,7)=1 \). Therefore, as applications of Theorem 1 to \( K, \overline{K} \) and \( \overline{\overline{K}} \), we have \( N_1=p+1, \overline{N}_1=p^2+1 \) and \( \overline{N}_1=p^3+1 \). It follows from the formula (4) above that \( N_2=p(p-1)/2 \) and \( N_3=p(p^2-1)/3 \). Thus, by making use of the formulas (2), it is easy to get that \( a_1=a_2=a_3=0 \). Hence we see \( L(u)=1+p^3u^6 \) and \( h=p^3+1 \) in view of the formula (1). Therefore Theorem 3 is completely proved.

References