Finite Fields and Their Applications **5,** 188–205 (1999)
Article ID ffta.1998.0241, available online at http://www.idealibrary.com on IDEAL®

# Codes on Fibre Products of Some Kummer Coverings

F. Özbudak

*Department of Mathematics, Middle East Technical University, Inonu Bulvari, Ankara, 06531 Turkey*

*Communicated by Michael Tsfasman*

Received July 8, 1996; revised June 21, 1997

The purpose of this paper is to construct fairly long geometric Goppa codes over $F_q$ with rather good parameters by fibre products of some Kummer coverings. This paper also extends the results of Stepanov [1] and Stepanov and Özbudak [2]. © 1999 Academic Press

## 1. INTRODUCTION

Let $F_p \subset F_q$ be a Galois extension of prime field $F_p$. Weil [18] proved that if $F(x, y) \in F_q[x, y]$ is an absolutely irreducible polynomial and if $N_q$ denotes the number of $F_q$-rational points of the curve defined by the equation $F(x, y) = 0$, then

$$|N_q - (q+1)| \leq 2gq^{1/2},$$

where $g$ is the genus of the curve. Now let $F(x, y) = y^s - f(x)$, where $f$ is a polynomial in $F_q[x]$. As a corollary we have that if $m$ is the number of distinct roots of $f$ in its splitting field over $F_q$, $\chi$ is a non-trivial multiplicative character of exponent $s$, and $f$ is not an $s$th power of a polynomial, then

$$\left| \sum_{x \in F_q} \chi(f(x)) \right| \leq (m-1)q^{1/2}.$$

By Goppa construction (see, for example, [8, 9]) we get linear $[n, k, d]_q$ codes associated to a smooth projective curve $X$ of genus $g = g(X)$ defined over a finite field $F_q$. Let $\mathscr{P} = \{P_1, \ldots, P_n\}$ be a set of $F_q$-rational points of



1071-5797/99 $30.00

$X$ and set

$$D_0 = P_1 + \cdots + P_n.$$

Let $D$ be a $F_q$-rational divisor on $X$ whose support is disjoint from $D_0$. Consider the following vector $F_q$-space of rational functions on $X$,

$$L(D) = \{h \in F_q(X)^* \mid (h) + D \geq 0\} \cup \{0\},$$

and denote its dimension over $F_q$ by $l(D)$. The linear $[n, k, d]$ code $C = C(D_0, D)$ associated to the pair $(D_0, D)$ is the image of the linear evaluation map

$$Ev: L(D) \to F_q^n, \qquad h \mapsto (h(x_1), \ldots, h(x_n)).$$

Such a $q$-ary linear code is called a geometric Goppa code. If $\deg D < n$ then $Ev$ is an embedding, and hence $k = \dim C = l(D)$ and by the Riemann–Roch theorem,

$$k \geq \deg D - g + 1;$$

in particular, if $2g - 2 < \deg D < n$, then

$$k = \deg D - g + 1.$$

Moreover we have

$$d \geq n - \deg D.$$

Stepanov [3] proved the existence of a square-free polynomial $f(x) \in F_p[x]$ of degree $\geq 2((N+1)\log 2/\log p + 1)$ for which

$$\sum_{i=1}^{N} \left(\frac{f(x)}{p}\right) = N,$$

where $\{1, \ldots, N\} \subset F_p$ and $(\frac{\cdot}{p})$ is the Legendre symbol and $(p, 2) = 1$. Later, Özbudak [4] extended this to arbitrary non-trivial characters of arbitrary finite fields. Let $\chi$ be a multiplicative character of exponent $s$. Considering only the irreducible monic polynomials and applying Dirichlet's pigeonhole principle as in [3] or [4], we get the existence of square-free polynomial $f \in F_q[x]$ of degree on the order of $sq \log s/\log q$ where $\chi(f(a)) = 1$ for each

$a \in F_q$. Application of Goppa's construction to the curve

$$y^s = f(x)$$

providing a Kummer covering of the affine line $\mathbb{A}^1_{F_q}$ gives the following result which is valid for any finite field.

THEOREM 1. *Let $F_q$ be a finite field of characteristic $p$, $s$ be an integer $s \geq 2$, $s|(q-1)$, and $c$ be the infimum of the set*

$$C = \left\{ x : \text{a non-negative real number} \,|\, \text{there exists an integer } n \text{ such that} \right.$$
$$\left. \frac{q^x(q-2)}{(q-1)(s-1)(1+1/s^q(s-1))} \geq n \geq \frac{q \log s}{\log q} + x \right\}.$$

*Let $r$ be an integer satisfying*

$$s(s-1)\left\lceil \frac{q \log s}{\log q} + c \right\rceil - 2s < r < sq.$$

*Then there exists a linear code $[n, k, d]_q$ with parameters*

$$n = sq,$$
$$k = r - \frac{s(s-1)}{2}\left\lceil \frac{q \log s}{\log q} + c \right\rceil + s,$$
$$d \geq sq - r.$$

*Therefore the relative parameters $R = k/n$ and $\delta = d/n$ satisfy*

$$R \geq 1 - \delta - \frac{\frac{s(s-1)}{2}\left\lceil \frac{q \log s}{\log q} + c \right\rceil - s}{sq}.$$

*Remark* 1. This result is significant especially when $q$ is prime. The number of $F_q$-rational affine points in $\mathbb{A}^2_{F_q}$ of the curve $y^s = f(x)$ is $N_q = sq$; the genus of the curve is

$$g = \frac{s(s-1)}{2}\left\lceil \frac{q \log s}{\log q} + c \right\rceil - s + 1 \qquad \text{and} \qquad \frac{N_q}{g} \sim \frac{2 \log q}{(s-1)\log s}.$$

If $F_q$ is not a prime field, using Galois structure of $F_q$ over a proper subfield $F_{q'} \subsetneq F_q$, we get much larger $N_q/g$ ratios (see Theorem 2). Note that the length of the codes are $sq > q$.

In [5] Stepanov introduced some special sums $S_v(s) = \sum_{a \in F_{q^v}} \chi(f(a))$ with a non-trivial quadratic character $\chi$ whose absolute values are very close to Weil's upper bound by explicitly representing the polynomial $f(x)$. Later, Gluhov [6, 7] generalized Stepanov's approach to the case of arbitrary multiplicative characters.

Applying similar polynomials for the corresponding fields to the fibre products of Kummer coverings

$$y_i^{\mu} = f_i(x), \qquad 1 \leq i \leq s, \tag{1}$$

where $\mu | (q-1)$, we obtain the following result. Namely the polynomials we apply are $f_i(x) = f_1(x+c)$, $c \in A$, a corresponding subset of $F_{q^v}$, where $f_1$ is given in Table I for the corresponding cases below.

THEOREM 2. *Let $v > 2$ be a positive integer, $F_{q^v}$ a finite field of characteristic $p$, $\mu$ an integer $\mu \geq 2$, $\mu | (q-1)$. If $s$ is an integer satisfying the corresponding conditions given in Table II, then there exists $A_j \subset F_{q^v}$ for the respective cases $j = 1, \dots, 6$ such that the affine curves given by* (1) *and Table I have $N_{q^v} = \mu^s q^v$ many $F_{q^v}$-rational points and genera $g_j$ as given in Table II, respectively.*

*Therefore if $r$ is an integer satisfying the conditions given in Table III, we get linear $[n, k, d]_{q^v}$ codes with the corresponding parameters given in Table III. Moreover the relative parameters $R = \frac{k}{n}$ and $\delta = \frac{d}{n}$ satisfy*

$$R \geq 1 - \delta - J(n, s, \mu, q),$$

*where $J(n, s, \mu, q)$ is given in Table IV.*

*Remark* 2. The parameters of the codes of Theorem 2 are rather good. First of all the lengths are in the order of $\mu^s q^v$, which are far larger than $q^v$ = the number of elements of the field, and the parameters are near to Singleton bound at the same time. It is possible to calculate the minimum distance in some cases directly. For example we have such codes:

(i) Over $F_{27} \supset F_3$ if $6 < r < 54$, then it gives $[54, r-3, d]_{27}$ code, where $d \geq 54 - r$. If $r$ is even, then $d = 54 - r$ (see Stichtenoth [12, Remark 2.2.5]).

(ii) Over $F_{64} \supset F_4$ if $18 < r < 192$, then it gives $[192, r-9, d]_{64}$ code, where $d \geq 192 - r$. If $r \equiv 0 \bmod 3$, then $d = 192 - r$.

(iii) Over $F_{1331} \supset F_{11}$ if $11600 < r < 133100$, then it gives $[133100, k, d]_{1331}$ code, where $k \geq r - 11600$ and $d \geq 133100 - r$.

**TABLE I**

| | | |
|---|---|---|
| Case 1: | $p > 2$, $v$: odd | $f_1(x) = (1 + x^{q^{(v-1)/2}-1})^{\mu_1}(1 + x^{q^{(v+1)/2}-1})^{\mu_2}$ |
| Case 2: | $p > 2$, $v \equiv 2 \bmod 4$ | $f_1(x) = (1 + x^{q^{v/2-1}-1})^{\mu_1}(1 + x^{q^{v/2+1}-1})^{\mu_2}$ |
| Case 3: | $p > 2$, $v \equiv 0 \bmod 4$ | $f_1(x) = \left(\frac{1 + x^{q^{v/2-1}-1}}{1 + x^{q-1}}\right)^{\mu_1}\left(\frac{1 + x^{q^{v/2+1}-1}}{1 + x^{q-1}}\right)^{\mu_2}$ |
| Case 4: | $p = 2$, $v$: odd | $f_1(x) = \left(\frac{1 + x^{q^{(v-1)/2}-1}}{1 + x^{q-1}}\right)^{\mu_1}\left(\frac{1 + x^{q^{(v+1)/2}-1}}{1 + x^{q-1}}\right)^{\mu_2}$ |
| Case 5: | $p = 2$, $v \equiv 2 \bmod 4$ | $f_1(x) = \left(\frac{1 + x^{q^{v/2-1}-1}}{1 + x^{q^2-1}}\right)^{\mu_1}\left(\frac{1 + x^{q^{v/2+1}-1}}{1 + x^{q^2-1}}\right)^{\mu_2}$ |
| Case 6: | $p = 2$, $v \equiv 0 \bmod 4$ | $f_1(x) = \left(\frac{1 + x^{{}^{v/2-1}-1}}{1 + x^{q-1}}\right)^{\mu_1}\left(\frac{1 + x^{q^{v/2+1}-1}}{1 + x^{q-1}}\right)^{\mu_2}$ |

*Note*. The field $F_{q^v}$, $v > 2$, $p$: the characteristic of the field, $\mu$: a positive integer such that $\mu | (q-1)$, $\mu = \mu_1 + \mu_2$, where $\mu_1$, $\mu_2$ are positive integer with $gcd(\mu, \mu_1) = 1$.

**TABLE II**

| Case $j = 1, \ldots, 6$ | Conditions on $s$ | Genus, $g_j$, $j = 1, \ldots, 6$ |
|---|---|---|
| Case 1<br>$p > 2$<br>$v$: odd | $1 \le s \le \frac{2\mu(q^v + 1)}{(\mu-1)(q^{(v-1)/2}(q+1) - 2)}$ | $\frac{\mu^{s-1}}{2}((\mu-1)s(q^{(v-1)/2}(q+1) - 2) - 2\mu) + 1$ |
| Case 2<br>$p > 2$<br>$v \equiv 2 \bmod 4$ | $1 \le s \le \frac{2\mu(q^v + 1)}{(\mu-1)(q^{v/2-1}(q^2+1) - 2)}$ | $\frac{\mu^{s-1}}{2}((\mu-1)s(q^{v/2-1}(q^2+1) - 2) - 2\mu) + 1$ |
| Case 3<br>$p > 2$<br>$v \equiv 2 \bmod 4$ | $1 \le s \le \frac{2\mu(q^v + 1)}{(\mu-1)(q^{v/2-1}(q^2+1) - 2q)}$ | $\frac{\mu^{s-1}}{2}((\mu-1)s(q^{v/2-1}(q^2+1) - 2q) - 2\mu) + 1$ |
| Case 4<br>$p = 2$<br>$v$: odd | $1 \le s \le \frac{2\mu(q^v + 1)}{(\mu-1)(q^{(v-1)/2}(q+1) - 2q)}$ | $\frac{\mu^{s-1}}{2}((\mu-1)s(q^{(v-1)/2}(q+1) - 2q) - 2\mu) + 1$ |
| Case 5<br>$p = 2$<br>$v \equiv 2 \bmod 4$ | $1 \le s \le \frac{2\mu(q^v + 1)}{(\mu-1)(q^{v/2-1}(q^2+1) - 2q^2)}$ | $\frac{\mu^{s-1}}{2}((\mu-1)s(q^{v/2-1}(q^2+1) - 2q^2) - 2\mu) + 1$ |
| Case 6<br>$p = 2$<br>$v \equiv 0 \bmod 4$ | $1 \le s \le \frac{2\mu(q^v + 1)}{(\mu-1)(q^{v/2-1}(q^2+1) - 2q)}$ | $\frac{\mu^{s-1}}{2}((\mu-1)s(q^{v/2-1}(q^2+1) - 2q) - 2\mu) + 1$ |

**TABLE III**

| Case | Condition on $r$ | $[n, k, d]_{q^v}$ |
|---|---|---|
| Case 1<br>$p > 2$<br>$v$: odd | $\frac{\mu^{s-1}}{2}((\mu-1)s(q^{(v-1)/2}(q+1)-2)-2\mu)$<br>$< r < \mu^s q^v$ | $r < n \leq \mu^s q^v$<br>$k \geq r - \frac{\mu^{s-1}}{2}((\mu-1)s(q^{(v-1)/2}(q+1)-2)-2\mu)$<br>$d \geq n - r$ |
| Case 2<br>$p > 2$<br>$v \equiv 2 \bmod 4$ | $\frac{\mu^{s-1}}{2}((\mu-1)s(q^{v/2-1}(q^2+1)-2)-2\mu)$<br>$< r < \mu^s q^v$ | $r < n \leq \mu^s q^v$<br>$k \geq r - \frac{\mu^{s-1}}{2}((\mu-1)s(q^{v/2-1}(q^2+1)-2)-2\mu)$<br>$d \geq n - r$ |
| Case 3<br>$p > 2$<br>$v \equiv 0 \bmod 4$ | $\frac{\mu^{s-1}}{2}((\mu-1)s(q^{v/2-1}(q^2+1)-2q)-2\mu)$<br>$< r < \mu^s q^v$ | $r < n \leq \mu^s q^v$<br>$k \geq r - \frac{\mu^{s-1}}{2}((\mu-1)s(q^{v/2-1}(q^2+1)-2q)-2\mu)$<br>$d \geq n - r$ |
| Case 4<br>$p = 2$<br>$v$: odd | $\frac{\mu^{s-1}}{2}((\mu-1)s(q^{(v-1)/2}(q+1)-2q)-2\mu)$<br>$< r < \mu^s q^v$ | $r < n \leq \mu^s q^v$<br>$k \geq r - \frac{\mu^{s-1}}{2}((\mu-1)s(q^{(v-1)/2}(q+1)-2q)-2\mu)$<br>$d \geq n - r$ |
| Case 5<br>$p = 2$<br>$v \equiv 2 \bmod 4$ | $\frac{\mu^{s-1}}{2}((\mu-1)s(q^{v/2-1}(q^2+1)-2q^2)-2\mu)$<br>$< r < \mu^s q^v$ | $r < n \leq \mu^s q^v$<br>$k \geq r - \frac{\mu^{s-1}}{2}((\mu-1)s(q^{v/2-1}(q^2+1)-2q^2)-2\mu)$<br>$d \geq n - r$ |
| Case 6<br>$p = 2$<br>$v \equiv 0 \bmod 4$ | $\frac{\mu^{s-1}}{2}((\mu-1)s(q^{v/2-1}(q^2+1)-2q)-2\mu)$<br>$< r < \mu^s q^v$ | $r < n \leq \mu^s q^v$<br>$k \geq r - \frac{\mu^{s-1}}{2}((\mu-1)s(q^{v/2-1}(q^2+1)-2q)-2\mu)$<br>$d \geq n - r$ |

If $q^v = p^{v'}$, where $p$ is the characteristic of the field and $v'$ is even, there exist better codes in some respects, for instance, Hermitian codes (see, for example, [12, Ex. 6.4.2]), which are maximal codes. Moreover the codes of Stepanov [1] are also better in this case if $p \neq 2$ and longer than Hermitian codes. However, the codes of Theorem 2 are even longer than the codes of [1] if $\mu > 2$ and also include the case $p = 2$.

If $q^v = p^{v'}$, where $v'$ is odd, there are no maximal codes as Hermitian codes of the case $v'$ even. Van der Geer and van der Vlugt found independently good codes by fibre products of Artin–Schreier curves [14]. The results of Theorem 2 are compatible with their results. Moreover we have one more parameter $\mu$, and our codes are much longer than their codes while near to Singleton bound as close as their codes.

Theorem 2 also extends the results of [2] since $\mu = 2$ was fixed in that case. Moreover in this way we get similar results also for characteristic $p = 2$ fields.

**TABLE IV**

| Case | $J(n, s, \mu, q)$ |
|---|---|
| Case 1<br>$p > 2$<br>$v$: odd | $\dfrac{\mu^{s-1}((\mu-1)s(q^{(v-1)/2}(q+1)-2)-2\mu)}{2n}$ |
| Case 2<br>$p > 2$<br>$v \equiv 2 \bmod 4$ | $\dfrac{\mu^{s-1}((\mu-1)s(q^{v/2-1}(q^2+1)-2)-2\mu)}{2n}$ |
| Case 3<br>$p > 2$<br>$v \equiv 0 \bmod 4$ | $\dfrac{\mu^{s-1}((\mu-1)s(q^{v/2-1}(q^2+1)-2q)-2\mu)}{2n}$ |
| Case 4<br>$p = 2$<br>$v$: odd | $\dfrac{\mu^{s-1}((\mu-1)s(q^{(v-1)/2}(q+1)-2q)-2\mu)}{2n}$ |
| Case 5<br>$p = 2$<br>$v \equiv 2 \bmod 4$ | $\dfrac{\mu^{s-1}((\mu-1)s(q^{v/2-1}(q^2+1)-2q^2)-2\mu)}{2n}$ |
| Case 6<br>$p = 2$<br>$v \equiv 0 \bmod 4$ | $\dfrac{\mu^{s-1}((\mu-1)s(q^{v/2-1}(q^2+1)-2q)-2\mu)}{2n}$ |

It is known that by fibre products of Kummer coverings of the affine line, one cannot get asymptotically good curves (see [13]). This explains why $s$ and therefore the length of the codes in Theorem 2 and the codes given by van der Geer and van der Vlugt are bounded. Recently Garcia and Stichtenoth gave a sequence of curves of arbitrarily large genera with good parameters over square finite fields using Artin–Schreier coverings [15].

## 2. NOTATION AND THE CALCULATION OF THE GENUS

Let $\bar{F}_{q^v}$ be an algebraic closure of the field $F_{q^v}$ and $\mathbb{A}^{s+1}$ be $(s+1)$-dimensional affine space over $\bar{F}_{q^v}$.

Let $\theta : F_{q^v} \to F_{q^v}$ be the Frobenius automorphism of $F_{q^v}$ over $F_q : \theta(x) = x^q$. The multiplicative homomorphism

$$norm_v(x) = x \cdot \theta(x) \cdot \theta^2(x) \cdots \theta^{v-1}(x) = x \cdot x^q \cdots x^{q^{v-1}}$$

of the field $F_{q^v}$ onto $F_q$ is the relative norm of $x \in F_{q^v}$ with respect to $F_q$. Let $\chi_\mu$ be a non-trivial multiplicative character of $F_q$ of exponent $\mu$, so $\mu > 1$. We denote by $\chi_{v,\mu}$ the multiplicative character of $F_{q^v}$ induced by $\chi_\mu$:

$$\chi_{v,\mu}(x) = \chi_\mu(norm_v(x)).$$

For $f(x) \in F_{q^v}[x]$ we denote by $S_{v,\mu}(f)$ the sum

$$S_{v,\mu}(f) = \sum_{x \in F_{q^v}} \chi_{v,\mu}(f(x)).$$

LEMMA 1. *Let $f_{1,i}, f_{2,i}, \ldots, f_{s,i} \in F_q[x]$ be square-free monic polynomials of the same degree $m_i$ for $i = 1, 2$. Let $\mu_1, \mu_2$ be positive integers, $\mu \geq 2$ a positive integer with $\mu | q - 1$, $gcd(\mu, \mu_1) = 1$, and $m_1\mu_1 + m_2\mu_2 \geq \mu + 1$. Assume $f_{i,j}$, $i = 1, 2, \ldots, s$, $j = 1, 2$ are pairwise coprime polynomials in $F_q[x]$. Let $Y$ be the fibre product in $\mathbb{A}^{s+1}$ given over $F_q[x]$ via*

$$Y : \begin{aligned} z_1^\mu &= (f_{1,1}(x))^{\mu_1}(f_{1,2}(x))^{\mu_2}, \\ z_2^\mu &= (f_{2,1}(x))^{\mu_1}(f_{2,2}(x))^{\mu_2}, \\ &\vdots \\ z_s^\mu &= (f_{s,1}(x))^{\mu_1}(f_{s,2}(x))^{\mu_2}. \end{aligned}$$

*Moreover let $m = m_1\mu_1 + m_2\mu_2$ and assume $(m, \mu) = 1$ or $(m, \mu) = \mu$. Then the genus $g = g(Y)$ of the curve $Y$ is*

$$g = \begin{cases} \dfrac{\mu^{s-1}}{2}((\mu - 1)s(m_1 + m_2) - (\mu + 1)) + 1 & \text{if } (m, \mu) = 1 \\ \dfrac{\mu^{s-1}}{2}((\mu - 1)s(m_1 + m_2) - (2\mu)) + 1 & \text{if } (m, \mu) = \mu. \end{cases}$$

*Proof.* The plan of the proof is as follows. First we consider the curve with $\mu_1 = \mu_2 = 1$:

$$Y : \begin{aligned} z_1^\mu &= f_{1,1}(x) f_{1,2}(x), \\ &\vdots \\ z_s^\mu &= f_{s,1}(x) f_{s,2}(x). \end{aligned}$$

Note the affine curve $Y$ is non-singular and we compute the genus using the same methods of Lemma 1 [2]. Then we consider for general $\mu_1$, $\mu_2$. In this case the affine curve is singular in general. We add contributions of these singularities to the genus using Riemann–Hurwitz formula.

Now let $\mu_1 = \mu_2 = 1$. Let $I$ be the ideal of the curve $Y$ over $\bar{F}_q$ and $\bar{Y}$ be the projective closure of $Y$ in $\mathbb{P}^{s+1}$. The homogeneous ideal of $\bar{Y}$ in $\bar{F}_q[x_0, x, z_1, \dots, z_s]$ has the form $I_h = \{ f(x/x_0,\ z_1/x_0, \dots, z_s/x_0) x_0^{\deg f} \mid f \in I \}$. Thus $\bar{Y} = Y \cup \{[0{:}0{:}\xi_1{:}\cdots{:}\xi_s]\}$, where $\xi^\mu = 1$ for $i = 1, \dots, s$ and the curve $\bar{Y}$ is singular at $\mu^{s-1}$ points $P_i \in \{[0{:}0{:}\xi_1{:}\cdots{:}\xi_s]\}$ in general.

Let $X$ be normalization of $\bar{Y}$. There exists a finite regular morphism $\phi_1 : X \to \bar{Y}$. Let $\phi_2 : \bar{Y} \to \mathbb{P}^1$ be the projection $[x_0, x{:}z_1{:}\cdots{:}z_s] \to [x_0{:}x]$. Then $\phi : X \to \mathbb{P}^1$ is a finite regular surjective morphism of degree $\mu^s$, where $\phi = \phi_2 \circ \phi_1$. Since $\bar{Y}$ has already $\mu^{s-1}$ points, $P_i$, $1 \le i \le \mu^{s-1}$ at the hypersurface $x_0 = 0$, $\phi^{-1}([0{:}1])$ consists of $\mu^s$ or $\mu^{s-1} l$, $1 < l$, $l \mid \mu$ points call $\{Q_i\} \subset X$, by symmetry.

Let $\Omega[Y]$ be the $\bar{F}_q[x, z_1, \dots, z_s]$ module of regular differential forms generated by $dx$ and $dz_i$, $1 \le i \le s$. Since $z_i^\mu = f_i(x)$ for $i = 1, 2, \dots, s$ we have

$$\Omega[Y] = \left\langle \frac{dx}{z_{i_1}^{n_{i_1}} \cdots z_{i_\sigma}^{n_{i_\sigma}}} \middle| 1 \le i_1 < i_2 \cdots < i_\sigma \le s,\ 0 \le n_{i_j} \le \mu - 1,\ j = 1, \dots, \sigma \right\rangle_{\bar{F}_q[x]}$$

since the affine curve $Y$ is non-singular. Therefore $\Omega[X]$ is an $\bar{F}_q[x]$ submodule of $\Omega[Y]$ since $\phi$ is regular. Hence any differential form $\omega \in \Omega[X]$ has the form

$$\omega = F_{(i_1, n_{i_1}), \dots, (i_\sigma, n_{i_\sigma})}(x) \frac{dx}{z_{i_1}^{n_{i_1}} \cdots z_{i_\sigma}^{n_{i_\sigma}}},$$

where $F_{(i_1, n_{i_1}), \dots, (i_\sigma, n_{i_\sigma})}(x) \in \bar{F}_q[x]$. Note that any differential form $\omega \in \Omega[X]$ is non-singular at any point of $X$ except $Q \in \phi^{-1}\{[0{:}1]\}$.

Let $x$ be the coordinate on $\mathbb{P}^1$; then $u = x^{-1}$ is a local parameter at the infinity point $[0{:}1] \in \mathbb{P}^1$. Since $x$ is a rational function on $\mathbb{P}^1$, it defines the divisor $(x) \in Div(\mathbb{P}^1)$. Denoting $\phi^{-1}(x) \in \overline{F_{q^v}}(X)$ a rational function on $X$ by $x$ and its divisor by $(x)$ again, we get the pullback divisor $(x) \in Div(X)$.

If $|\{Q_i\}| = |\phi^{-1}([0{:}1])| = \mu^s$, then $v_{Q_i}(u) = 1$. If $|\{Q_i\}| = \mu^{s-1} l$, then $v_{Q_i}(u) = d$ and $d \mid \mu$ since $\mu^s = d\mu^{s-1} l$ using the formula $\deg \phi \cdot v_{[0:1]}(u) = \sum_{Q_i} v_{Q_i}(u)$. Now there are two cases to consider in our lemma: $(\mu, m) = 1$ and $\mu \mid m$. Let $Q \in \{Q_i\}$.

*Case* $(\mu, m) = 1$. If $v_Q(u) = 1$, then $v_Q(x) = -1$, $v_Q(z_i^\mu) = -m$, and $v_Q(z_i) = -m/\mu \notin \mathbb{Z}$, a contradiction. Thus $v_Q(u) = d$ and $d \mid \mu$. Hence

$v_Q(z_i) = -md/\mu$ and $\mu | d$, so $\mu = d$. In short we have

(1) $v_Q(x) = -\mu$,

(2) $v_Q(z_i) = -m$ for $i = 1, \ldots, s$,

(3) $v_Q(dx) = -(\mu + 1)$.

In this case

$$\omega = F_{(i_1, n_{i_1}), \ldots, (i_\sigma, n_{i_\sigma})}(x) \frac{dx}{z_{i_1}^{n_{i_1}} \cdots z_{i_\sigma}^{n_{i_\sigma}}} \in \Omega[X]$$

if and only if $v_Q(\omega) \geq 0$. This means

$$\deg F_{(i_1, n_{i_1}), \ldots, (i_\sigma, n_{i_\sigma})}(x) \leq \frac{m(n_1 + \cdots + n_{i_\sigma}) - (\mu + 1)}{\mu}.$$

If $m(n_{i_1} + \cdots + n_{i_\sigma}) - 1 \equiv k \bmod \mu$, where $k = 0, 1, \ldots, \mu - 1$, then

$$\left[ \frac{m(n_{i_1} + \cdots + n_{i_\sigma}) - (\mu + 1)}{\mu} \right] = \frac{m(n_{i_1 + \cdots + n_{i_\sigma}}) - (\mu + 1) - k}{\mu},$$

where $[\cdot]$ is the greatest integer function. Therefore we have

$$\dim_{\overline{F_{q^v}}} \left\{ F_{(i_1, n_{i_1}), \ldots, (i_\sigma, n_{i_\sigma})}(x) \frac{dx}{z_{i_1}^{n_{i_1}} \cdots z_{i_\sigma}^{n_{i_\sigma}}} \,\middle|\, m(n_{i_1} + \cdots + n_{i_\sigma}) \equiv k + 1 \bmod \mu \right\}$$
$$= \frac{m(n_{i_1} + \cdots + n_{i_\sigma}) - (\mu + 1)}{\mu}.$$

To calculate genus we use a generating function for partitions. Let

$$u(x) = (1 + x + \cdots + x^{\mu - 1})^s = 1 + c_1 x + c_2 x^2 + \cdots + c_{(\mu - 1)s} x^{(\mu - 1)s}$$
$$= 1 + x(c_1 + c_{\mu + 1} x^\mu + \cdots) + x^2(c_2 + c_{\mu + 2} x^\mu + \cdots)$$
$$+ \cdots + x^\mu (c_\mu + c_{2\mu} x^\mu + \cdots).$$

Let

$$L_1 = c_1 + c_{\mu + 1} + \cdots,$$
$$L_2 = c_2 + c_{\mu + 2} + \cdots,$$
$$\vdots$$
$$L_\mu = c_\mu + c_{2\mu} + \cdots.$$

Let $\theta = e^{2\pi i/\mu}$. Then we have

$$\begin{aligned} u(1) - 1 &= L_1 + L_2 + \cdots + L_\mu, \\ u(\theta) - 1 &= L_1\theta + L_2\theta^2 + \cdots + L_\mu\theta^\mu, \\ &\vdots \\ u(\theta^{\mu-1}) - 1 &= L_1\theta^{(\mu-1)} + L_2\theta^{2(\mu-1)} + \cdots + L_\mu\theta^{\mu(\mu-1)}. \end{aligned}$$

In matrix form

$$\underbrace{\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \theta & \theta^2 & \cdots & \theta^\mu \\ \theta^2 & \theta^4 & \cdots & \theta^{2\mu} \\ \vdots & \vdots & & \vdots \\ \theta^{(\mu-1)} & \theta^{2(\mu-1)} & \cdots & \theta^{\mu(\mu-1)} \end{bmatrix}}_{A} \begin{bmatrix} L_1 \\ L_2 \\ L_3 \\ \vdots \\ L_\mu \end{bmatrix} = \begin{bmatrix} \mu^s - 1 \\ -1 \\ -1 \\ \vdots \\ -1 \end{bmatrix}.$$

Note that $A = [A_{ij}]_{\mu\times\mu} = [\theta^{(i-1)j}]$. Then $L_i = \Delta_i/\Delta$, where $\Delta = \det A$, $\Delta_i = \det A_i$, and $A_i$ is the matrix whose $i$th column is interchanged with $[\mu^s - 1, \quad -1, \ldots, -1]^T$. We have $L_1 = L_2 = \cdots = L_{\mu-1} = \mu^{s-1}$ and $L_\mu = \mu^{s-1} - 1$. Similarly let

$$\begin{aligned} v(x) &= \frac{d}{dx}u(x) \\ &= s(1 + x + \cdots + x^{\mu-1})^{s-1}(1 + 2x + 3x^2 + \cdots + (\mu-1)x^{\mu-2}), \\ &= c_1 + 2c_2x + 3c_3x^2 + \cdots, \\ &= (c_1 + (\mu+1)c_{\mu+1}x^\mu + \cdots) + x(2c_2 + (\mu+2)c_{\mu+2}x^\mu + \cdots) + \cdots, \end{aligned}$$

and

$$\begin{aligned} \tilde{L}_1 &= c_1 + (\mu+1)c_{\mu+1} + \cdots, \\ \tilde{L}_2 &= 2c_2 + (\mu+2)c_{\mu+2} + \cdots, \\ &\vdots \\ \tilde{L}_\mu &= \mu c_\mu + (2\mu)c_{2\mu} + \cdots. \end{aligned}$$

Then we have

$$\tilde{L}_1 + \tilde{L}_2 + \cdots + \tilde{L}_\mu = v(1) = s\mu^{s-1}\frac{\mu(\mu-1)}{2}.$$

Note that

$$L_k = \sum_{\sigma=1}^{s} \sum_{1 \le i_1 < i_2 < \cdots < i_\sigma \le s} \sum_{\substack{0 \le n_{i_1} \le \mu-1 \\ 0 \le n_{i_2} \le \mu-1 \\ \vdots \\ 0 \le n_{i_\sigma} \le \mu-1}} \delta_k(n_{i_1}, \ldots, n_{i_\sigma})$$

and

$$\tilde{L}_k = \sum_{\sigma=1}^{s} \sum_{1 \le i_1 < i_2 < \cdots < i_\sigma \le s} \sum_{\substack{0 \le n_{i_1} \le \mu-1 \\ 0 \le n_{i_2} \le \mu-1 \\ \vdots \\ 0 \le n_{i_\sigma} \le \mu-1}} (n_{i_1} + \cdots + n_{i_\sigma})\delta_k(n_{i_1}, \ldots, n_{i_\sigma}),$$

where

$$\delta_k(n_{i_1}, \ldots, n_{i_\sigma}) = \begin{cases} 1 & \text{if } n_{i_1} + \cdots + n_{i_\sigma} \equiv k \bmod \mu, \\ 0 & \text{else.} \end{cases}$$

Therefore the genus of $Y$ $g = g(Y)$ is

$$\begin{aligned} g &= \frac{m}{\mu}\sum_{k=1}^{\mu-1}\tilde{L}_k - \frac{1}{\mu}\sum_{k=1}^{\mu-1}kL_k + \frac{m}{\mu}\tilde{L}_\mu - \frac{\mu}{\mu}L_\mu \\ &= \frac{m}{\mu}s\mu^s\frac{\mu-1}{2} - \frac{1}{\mu}\sum_{k=1}^{\mu-1}k\mu^{s-1} - \frac{\mu}{\mu}(\mu^{s-1}-1) \\ &= \frac{ms\mu^{s-1}(\mu-1)}{2} - \frac{1}{\mu}\sum_{k=1}^{\mu}k\mu^{s-1} + 1 \\ &= \frac{ms\mu^{s-1}(\mu-1)}{2} - \frac{1}{\mu}\mu^{s-1}\frac{\mu(\mu+1)}{2} + 1 \\ &= \frac{\mu^{s-1}}{2}(ms(\mu-1) - (\mu+1)) + 1. \end{aligned}$$

Case $\mu|m$. In this case we have

(1) $v_Q(x) = \dfrac{-\mu}{l}$,

(2) $v_Q(z_i) = \dfrac{-m}{l}$ for $i = 1, 2, \ldots, s$,

(3) $v_Q(dx) = -\left(\dfrac{\mu}{l} + 1\right)$,

where $l = \mu/d$. Therefore

$$F_{(i_1, n_{i_1}), \ldots, (i_\sigma, n_{i_\sigma})}(x) \frac{dx}{z_{i_1}^{n_{i_1}} \cdots z_{i_\sigma}^{n_{i_\sigma}}} \in \Omega[X]$$

if and only if

$$\deg F_{(i_1, n_{i_1}), \ldots, (i_\sigma, n_{i_\sigma})}(x) \leq \frac{m}{\mu}(n_{i_1} + \cdots + n_{i_\sigma}) - 2.$$

Thus

$$\dim_{\overline{F_{q^v}}} \left\{ F_{(i_1, n_{i_1}), \ldots, (i_\sigma, n_{i_\sigma})}(x) \frac{dx}{z_{i_1}^{n_{i_1}} \cdots z_{i_\sigma}^{n_{i_\sigma}}} \in \Omega[x] \right\} = \frac{m}{\mu}(n_{i_1} + \cdots + n_{i_\sigma}) - 1$$

Therefore the genus $g = g(Y)$ is

$$g = \frac{m}{\mu} \sum_{k=1}^{\mu} \tilde{L}_k - \sum_{k=1}^{\mu} L_k$$

$$= \frac{m}{\mu}\left(s \frac{\mu^s(\mu - 1)}{2}\right) - (\mu\mu^{s-1} - 1)$$

$$= \frac{\mu^{s-1}}{2}(ms(\mu - 1) - 2\mu) + 1.$$

Now we can compute the genus for general $(\mu_1, \mu_2)$ using the Riemann–Hurwitz formula. Recall that if $\phi : X \to \mathbb{P}^1$ is a finite regular morphism of projective irreducible curves, then

$$g(X) = 1 + \frac{1}{2} \sum_{P \in X \setminus \phi^{-1}([0:1])} (e_P - 1) + \frac{1}{2} \sum_{Q \in \phi^{-1}([0:1])} (e_Q - 1) - \deg \phi,$$

where $e_P$ and $e_Q$ are ramification indices of $\phi$ at $P$ and $Q$, respectively. Let

$$Y_1: \quad \begin{aligned} z_1^{\mu} &= f_{1,1}(x)^{\mu_1} f_{1,2}(x)^{\mu_2} \\ &\vdots \\ z_s^{\mu} &= f_{s,1}(x)^{\mu_1} f_{s,2}(x)^{\mu_2} \end{aligned}$$

be the general form of the curve whose genus we want to calculate. Let

$$Y_2: \quad \begin{aligned} z_1^{\mu} &= f_1 \\ &\vdots \\ z_s^{\mu} &= f_s \end{aligned}$$

be the curve where $\mu_1 = \mu_2 = 1$ and $m = \deg f_i$ for $i = 1, \ldots, s, f_i$ are pairwise coprime. If $X_i$ is the normalization of the projectivization of $Y_i$ and $\phi_i \to \mathbb{P}^1$ the corresponding maps, then deg $\phi_i = \mu^s$, $i = 1, 2$. Moreover

$$\sum_{Q \in \phi_1^{-1}([0:1])} (e_Q - 1) = \sum_{Q \in \phi_2^{-1}([0:1])} (e_Q - 1)$$

since $m = \deg f_i$, $i = 1, \ldots, s$. Consider the curve $Y_1$. If $\phi_1(P) = [1, t]$, $t \in \bar{F}_{q^v}$, and $(f_{1,1}(t) f_{1,2}(t)) \cdots (f_{s,1}(t) f_{s,2}(t)) \neq 0$, then $|\phi_1^{-1}([1, t])| = \mu^s$ and $e_P = 1$ for each $P \in \phi_1^{-1}([1:t])$. If $\phi_1(P) = [1, t]$ and $f_{1,1}(t) = 0$, then $(f_{1,2}(t))(f_{2,1}(t) f_{2,2}(t)) \cdots (f_{s,1}(t) f_{s,2}(t)) \neq 0$ since they are relatively prime polynomials. Therefore $|\phi_1^{-1}([1:t])| = \mu^{s-1}$ and $e_P = \mu$ for each $P \in \phi^{-1}([1:t])$. This holds for other polynomials also. Therefore

$$\sum_{P \in X_1 \setminus \phi_1^{-1}([0:1])} (e_P - 1) = s(m_1 + m_2)(\mu - 1)\mu^{s-1}.$$

Similarly for $Y_2$ we have

$$\sum_{P \in X_2 \setminus \phi_2^{-1}([0:1])} (e_P - 1) = sm(\mu - 1)\mu^{s-1}.$$

Therefore if we denote the genus of $Y_i$ by $g_i$, $i = 1, 2$, we have

$$g_1 = g_2 + \frac{s(m_1 + m_2)(\mu - 1)\mu^{s-1}}{2} - \frac{sm(\mu - 1)\mu^{s-1}}{2}.$$

But we know

$$g_2 = \begin{cases} \frac{\mu^{s-1}}{2}((\mu-1)sm - (\mu+1)) + 1 & \text{if } (m,\mu)=1, \\ \frac{\mu^{s-1}}{2}((\mu-1)sm - 2\mu) + 1 & \text{if } (m,\mu)=\mu. \end{cases}$$

Adding the difference we prove the lemma. ■

*Remark* 3. One of the anonymous referees remarked that there exists a different method to calculate the genus given by Xing [16]. Our method, which is a generalization of that of Stepanov, allows us to find explicitly a basis for regular differential forms on the curve. Moreover this provides a fast decoding algorithm following the arguments of the proof of Lemma 1 after the resolution of affine singularities.

## 3. THE CALCULATION OF THE NUMBER OF $F_{q^v}$-RATIONAL POINTS

LEMMA 2. *Let $v > 1$ be an integer, $F_{q^v}$ a finite field of characteristic $p$, $\mu \geq 2$ an integer, $\mu | (q-1)$, $\mu_1$, $\mu_2$ positive integers with $\mu_1 + \mu_2 = \mu$, and $gcd(\mu, \mu_1) = 1$. Then there exist $A_j \subset F_{q^v}$ for the cases $j = 1, \ldots, 6$ corresponding to Table I such that the curve $Y$ defined by*

$$Y : z_i^{\mu} = f_1(x + c_i), \qquad 1 \leq i \leq s,$$

*where $f_1$ is defined in Table I, and $s \leq |A_j|$ is absolutely irreducible and it has $\mu^s q^v$ many $F_{q^v}$-rational affine points in $\mathbb{A}^{s+1}_{F_{q^v}}$. Moreover $|A_j| = q^v$ for $j = 1, 2$, $|A_4| = q^{v-1}$, and $|A_j| = q^{v-2}$ for $j = 3, 5, 6$.*

*Proof.* The proofs are similar for all six cases. We give the proof for the Case 3, i.e., $p > 2$, $v \equiv 0 \bmod 4$:

$$f_1(x) = \left(\frac{1 + x^{q^{v/2-1}-1}}{1 + x^{q-1}}\right)^{\mu_1} \left(\frac{1 + x^{q^{v/2+1}-1}}{1 + x^{q-1}}\right)^{\mu_2}$$

in this case.

Let $g_1(x) = (x^{q^{v/2-1}} + x)$ and $H_1 = \{c \in F_{q^v} | c^{q^{v/2-1}} + c = 0\}$. Observe that $H_1$ is an additive subgroup of $F_{q^v}$ with $H_1 = \{0\} \cup \{g^{((2s+1)/2)(q+1)} | 0 \leq s \leq q-2$, $g$ is a generator of $F^*_{q^2}\}$ and $gcd(g_1(x), g_1(x+c)) = 1$ for $c \in F_{q^v} \setminus H_1$.

Let $g_2(x) = (x^{q^{v/2+1}} + x)$. Then $gcd(g_2(x), g_2(x+c)) = 1$ for $c \in F_{q^v} \setminus H_1$ similarly.

Let $\delta = \frac{v}{2} - 1$ and $I$ be the ideal of $F_{q^v}[x]$ defined by $I = (g_2(x+c), g_1(x))$, where $c \in F_{q^v}$. Using the Euclidean algorithm we get $I = (x^{q^\delta} + x, -x^{q^2} + x + c^{q^{\delta+2}} + c)$ (see the proof of Lemma 2 in [2]. Moreover if $J = (x^{q^\delta} + x, -x^{q^{\delta+2}} + x^{q^\delta} + c_1^{q^{\delta+2}} + c_1)$, where $c_1 = c^{q^\delta}$, then

$$I \supset J = (x^{q^\delta} + x, x^{q^{\delta+2}} + x - c_1^{q^{\delta+2}} - c_1).$$

Since $g_2(x+c) \in I$, if

$$c^{q^{\delta+2}} + c + c_1^{q^{\delta+2}} + c_1 \neq 0, \tag{2}$$

then $I = (1)$. But (2) holds iff

$$(c^{q^{\delta+2}} + c + c_1^{q^{\delta+2}} + c_1)^{q^\delta} = (c^{q^\delta} + c)^{q^\delta} + (c^{q^\delta} + c) \neq 0. \tag{3}$$

Let $\tau$ be the additive homomorphism defined by

$$\tau : F_{q^v} \to F_{q^v}, \qquad \tau(c) = c^{q^\delta} + c.$$

The $ker\,\tau = H_1$. Let $H_2 = \tau^{-1}(H_1)$ be the inverse image of $H_1$. $H_2$ is again an additive subgroup of $F_{q^v}$ and $|H_2| = |H_1||ker\,\tau| = q^2$. Inequality (3) is satisfied when $c \notin F_{q^v} \backslash H_2$. Then $A_3$ is a complete set of representatives of $F_{q^v}/H_2$. Therefore $gcd(f_1(x+c), f_1(x)) = 1$ over $F_{q^v}[x]$ in this case and $Y$ is absolutely irreducible.

By similar arguments we find $A_1 = A_2 = F_{q^v}^*$, $A_4$ as a complete set of representatives of $F^{q^v}/F_q$, and $A_5 = A_6$ as a complete set of representatives of $F_{q^v}/F_{q^2}$.

Let $\chi$ be any non-trivial multiplicative character of $F_{q^v}$ of exponent $\mu$ and $\chi_{v,\mu}$ be the multiplicative character of $F_{q^v}$ induced by $\chi$. It follows that

$$\chi_{v,\mu}(f_1(a)) = 1, \qquad \text{for all } a \in F_{q^v}$$

in each case (see [7]). Moreover the number of $F_{q^v}$-rational affine points of the curve $Y$ (see for example [10, 11]) is

$$\begin{aligned} N_{q^v} &= \sum_{x \in F_{q^v}} \prod_{i=1}^{s} \left(1 + \sum_{\substack{\chi:\text{non-trivial multiplicative} \\ \text{character of exponent } \mu}} \chi_{v,\mu}(f(x+c_i))\right) \\ &= \sum_{x \in F_{q^v}} \prod_{i=1}^{s} \mu \\ &= \mu^s q^v. \quad \blacksquare \end{aligned}$$

## 4. PROOF OF THEOREM 2

Note that $f_1$ satisfies the conditions of Lemma 1 in the respective cases. Therefore the genera of the curves $g_j$ are as given in Table II. By Lemma 2 it has $\mu^s q^v$ many $F_{q^v}$-rational affine points. By normalization of the curve $Y$ we get a non-singular model $\tilde{Y}$ without losing $F_{q^v}$-rationality of these points (see for example [17, Sect. 5.3]). Let $S$ be the corresponding set of $F_{q^v}$-rational points of $\tilde{Y}$ and $S_1 \subset S$, be a subset of $S$. Applying Goppa's construction to

$$D_0 = \sum_{P \in S_1} P$$

and

$$D = rP_\infty,$$

where $r < \deg D_0 = |S_1|$ and $P_\infty$ is a point of non-singular model corresponding to a point at infinity of the projectivization of the affine model $Y$, we get $r < n \leq \mu^s q^v$, $k \geq r + 1 - g$, $d \geq n - r$. Moreover if $2g - 2 < r = \deg D < n$, then $k = r + 1 - g$.

## ACKNOWLEDGMENTS

I am grateful to S.A. Stepanov, who introduced me to the problem. He provided marvelous ideas, comments, and suggestions. I also thank the referees for their suggestions and remarks.

## REFERENCES

1. S. A. Stepanov, Codes on fibre products of hyperelliptic curves, *Discrete Math. Appl.* **7** (1997), 77–88.
2. S. A. Stepanov and F. Özbudak, Fibre products of hyperelliptic curves and geometric Goppa codes, *Discrete Math. Appl.* **7** (1997) 223–229.
3. S. A. Stepanov, On lower estimates of incomplete character sums of polynomials, Proc. *Steklov Inst. Math.* **1** (1980), 187–189.
4. F. Özbudak, On lower bounds for incomplete character sums over finite fields, *Finite Fields Appl.* **2** (1996), 173–191.
5. S. A. Stepanov, On lower bounds of sums of characters over finite fields, *Discrete Math. Appl.* **2** (1992), 523–532.
6. M. M. Gluhov, Lower bounds for character sums over finite fields, *Diskret. Math.*, **6** (1994), 136–142. [In Russian]
7. M M. Gluhov, On lower bounds for character sums over finite fields, preprint.
8. V. G. Goppa, Codes on algebraic curves, *Soviet Math. Dokl.* **24** (1981), 170–172.

9. S. A. Stepanov, “Error-Correcting Codes and Algebraic Curves,” CRC Press, Boca Raton, FL, in press.
10. S. A. Stepanov, “Arithmetic of Algebraic Curves,” Plenum, New York, 1994.
11. W. Schmidt, “Equations over Finite Fields—An Elementary Approach,” Lecture Notes in Mathematics, Vol. 536, Springer-Verlag, Berlin/New York, 1976.
12. H. Stichtenoth, “Algebraic Function Fields and Codes,” Springer-Verlag, Berlin/New York, 1993.
13. G. Frey, M. Perret, and H. Stichtenoth, On the different of Abelian extensions of global fields, *in* “Coding Theory and Algebraic Geometry Proceeding, Luminy 1991,” pp. 26–32, Lecture Notes in Mathematics, Vol. 1518, Springer-Verlag, Berlin/New York, 1992.
14. G. van der Geer and M. van der Vlugt, Fiber products of Artin–Schreier curves and generalized Hamming weights of codes, *J. Combin. Theory Sec A* **70** (1995), 337–348.
15. A. Garcia and H. Stichtenoth, A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound, *Invent. Math.* **121** (1995), 211–222.
16. C. Xing, Multiple Kummer extensions and the number of prime divisors of degree one in function fields, *J. Pure Appl. Algebra* **84** (1993), 85–93.
17. I. R. Shafarevich, “Basic Algebraic Geometry 1,” Springer-Verlag, Berlin/New York, 1994.
18. A. Weil, Numbers of solutions of equations in finite fields, *Bull. Amer. Math. Soc.* **55** (1949), 497–508.