Codes on fibre products of Artin–Schreier curves*

S. A. STEPANOV and M. H. SHALALFEH

Abstract — The purpose of this paper is to construct a new family of smooth projective curves over a finite field F_q with many F_q -rational points using fibre products of Artin–Schreier curves. We show that for any curve X in this family the ratio $g(X)/N_q(X)$, where $g(X)$ is the genus and $N_q(X)$ is the number of F_q -rational points, is small enough to get geometric Goppa codes with good parameters. This paper extends the results of Stepanov and Özbudak concerning the construction of long codes.

1. INTRODUCTION

Let p be a prime number, and let F_q be a finite field with $q = p^\nu$ elements. A linear $[n, k, d]_q$ -code C is a subspace of F_q^n , where n is the length of the code C , $k = \dim_{F_q} C$ is the dimension of C , and d is the minimum Hamming distance between the non-zero elements of C . Each linear $[n, k, d]$ -code C defines a pair of its relative parameters (δ, R) , where $\delta = d/n$ is the relative minimum distance and $R = k/n$ is the transmission rate of the code C .

Using the Goppa construction for linear codes associated with smooth projective curves over finite fields, one can prove the existence of long linear codes. Although the geometric Goppa codes associated with maximal curves are interesting codes since they have quite good relative parameters, the length of these codes is bounded by $1 + q^3$. This is a direct consequence of Hasse–Weil bound and the fact that the genus of a maximal curve X satisfies the inequality $g(X) \leq q(q-1)/2$ (see [10]).

In [7], Stepanov constructed long geometric Goppa codes using fibre products of hyperelliptic curves over a finite field F_q , where $q = p^\nu$ and ν is even. In [8], Stepanov and Özbudak extended this result to the case where ν is odd. In [4], Özbudak constructed longer codes than those in [7] and [8] using fibre product of Kummer coverings. The aim of this paper is to construct geometric Goppa codes which are much longer than those in [6], [7], [8], and [4] using fibre products of Artin–Schreier curves.

Throughout this paper, $F_q(x)$ denotes the space of rational functions of the projective line P^1 . An element $f(x) \in F_q(x)$ is said to be degenerated if there exists $g(x) \in F_q(x)$ such that $f = g^p - g + a$, where $a \in F_q$, otherwise f is called non-degenerated.

If C is a code over F_q and $\text{Tr}_\nu: F_q \rightarrow F_p$ denotes the trace map from F_q to F_p , then

$$\text{Tr}(C) = \{\text{Tr}_\nu(c) \mid c \in C\}$$

is a code over F_p , which is called the trace code of C .

The relation $\text{Tr}_v(\alpha) = 0$ if and only if there exists $\beta \in F_q$ such that $\beta^p - \beta = \alpha$ connects trace codes with Artin–Schreier curves X_f with defining equation

$$y^p - y = f(x) \in F_q(x). \quad (1)$$

The curve (1) is absolutely irreducible if and only if $f(x)$ is non-degenerated, (cf. [3]). It is known that if $f(x) \in F_q[x]$, $\deg f(x) = m$, and $(m, p) = 1$, then $f(x)$ is non-degenerated, (cf. [5], p. 55).

The number $N_q(X_f)$ of F_q -rational points of the smooth projective model of (1) is equal to

$$N_q(X_f) = pN + 1,$$

where $N = |\{x \in F_q : \text{Tr}_v f(x) = 0\}|$.

Let A be F_q -linear subspace of $F_q[x]$; A is called non-degenerated if each $f(x) \in A$ is non-degenerated. If we regard A as a vector space over F_p , then we see that there is a basis $\{f_1(x), \dots, f_s(x)\}$ of A over F_p and can write

$$A = F_p f_1(x) + \dots + F_p f_s(x).$$

We call such a basis a canonical basis if any subset of this basis consisting of equal degree polynomials has F_p -linearly independent leading coefficients. Then the system of equations over $\bar{F}_q$

$$\begin{aligned} y_1^p - y_1 &= f_1(x), \\ y_2^p - y_2 &= f_2(x), \\ &\dots \\ y_s^p - y_s &= f_s(x) \end{aligned} \quad (2)$$

defines an irreducible curve in the $(s+1)$ -dimensional projective space P^{s+1} (cf. [3]).

In [9], G. van der Geer and M. van der Vlugt considered the fibre products

$$y_i^p - y_i = a_i x^{\sqrt{q}+1},$$

where $a_i \in F_q^*$ satisfies the equality $a_i^{\sqrt{q}} + a_i = 0$ if $q = p^\nu$ and ν even, and

$$y_i^p - y_i = a_i x^{p^{(\nu+1)/2}+1} - a_i^{(\nu-1)/2} x^{p^{(\nu-1)/2}+1},$$

where $a_i \in F_q^*$ if $q = p^\nu$ and ν odd.

As a result, they got smooth projective curves X_r such that

$$g(X_r) = \begin{cases} (p^r - 1)\sqrt{q}/2, & 1 \leq r \leq \nu/2, \nu \text{ is even,} \\ (p^r - 1)\sqrt{pq}/2, & 1 \leq r \leq \nu, \nu \text{ is odd,} \end{cases}$$

and the number of F_q -rational points of the curve X_r is

$$N_q(X_r) = \begin{cases} p^r q + 1, & 1 \leq r \leq \nu/2, \nu \text{ is even,} \\ p^r q + 1, & 1 \leq r \leq \nu, \nu \text{ is odd.} \end{cases}$$

Remark 1. For even ν , the curve X_r is a maximal curve for any r , $1 \leq r \leq \nu/2$.

In this paper, we construct a family $f_i(x) \in F_q[x]$ of non-degenerated polynomials, which form a canonical basis for a linear subspace of $F_q[x]$, and we apply the fibre product (2) to this family of polynomials to obtain smooth projective curves defined over finite fields with many rational points and considerably small ratio $g(X)/N_q(X)$. We obtain the following results.

Theorem 1. *Let $q = p^\nu$ and F_{q^2} be a finite field with q^2 elements. Then for any integer s such that $1 \leq s < q$, $(s, p) = 1$, there exists a smooth projective curve X_s with the genus $g(X_s)$ and the number of F_{q^2} -rational points $N_q(X_s)$, which satisfy the relations*

$$g(X_s) \leq \frac{1}{2}(q^{N_1(s)} - 1)(s(q+1) - 1), \quad N_q(X_s) = q^{N_1(s)+2} + 1,$$

where $N_1(s) = s - [s/p] + 2[\log_p((s(q+1) - 1)/q)]$.

Theorem 2. *Let $q = p^{2\nu+1}$ and F_q be a finite field with q elements. Then for any integer s such that $1 \leq s < p^{\nu-1}$, $(s, p) = 1$, there exists a smooth projective curve X_s with the genus $g(X_s)$ and the number of F_q -rational points, which satisfy the relations*

$$g(X_s) < \frac{1}{2}(p^{N_2(s)} - 1)(s(p^{\nu+1} + 1) - 1), \quad N_q(X_s) = qp^{N_2(s)} + 1,$$

where $N_2(s) = (2\nu + 1)(s - [s/p])$.

We apply Goppa's construction to the family of curves of these theorems to obtain the following result.

Corollary 1. *Let F_{q^2} , s , $N_1(s)$ be such as in Theorem 1. Then for any*

$$l > \frac{1}{2}(q^{N_1(s)} - 1)(s(q+1) - 1)$$

there exists a geometric Goppa $[n, k, d]_{q^2}$ -code $C(D_0, D)$ with parameters

$$\begin{aligned} l &< n \leq q^{N_1(s)+2}, \\ k &\geq l - \frac{1}{2}(q^{N_1(s)} - 1)(s(q+1) - 1) + 1, \\ d &\geq n - l. \end{aligned}$$

Corollary 2. *Let F_q , s , $N_2(s)$ be such as in Theorem 2. Then for any*

$$l > \frac{1}{2}(p^{N_2(s)} - 1)(s(p^{\nu+1} + 1) - 1)$$

there exists a geometric Goppa $[n, k, d]_q$ -code $C(D_0, D)$ with parameters

$$\begin{aligned} l &< n \leq qp^{N_2(s)}, \\ k &\geq l - \frac{1}{2}(p^{N_2(s)} - 1)(s(p^{\nu+1} + 1) - 1) + 1, \\ d &\geq n - l. \end{aligned}$$

Remark 2. The longest code in Corollary 1 has the length $p^{2\nu} p^{\nu((p-1)p^{\nu-1}+\nu)}$, and the longest code in Corollary 2 has the length $p^{(2\nu+1)(p-1)p^{\nu-2}}$, these codes are much longer than those in [4], which had already extended the results in [7] and [8]. The longest code obtained in [4] has the length $(p-1)p^\nu p^\nu$.

Remark 3. The relative parameters $R = k/n$ and $\delta = d/n$ of the codes in Corollaries 1 and 2 satisfy, respectively, the inequalities

$$R \geq 1 - \delta - \frac{(q^{N_1(s)} - 1)(s(q+1) - 1) - 1}{q^{N_1(s)+2} + 1},$$

$$R \geq 1 - \delta - \frac{(p^{N_2(s)} - 1)(s(p^{\nu+1} + 1) - 1) - 1}{qp^{N_2(s)} + 1}.$$

The proof of the main results in this paper are arranged as follows. In Section 2, we give an explicit formula for the genus of the curve (2). In Section 3, we construct a canonical basis for a non-degenerate subspace from $F_q[x]$ of special form and then we calculate the number of F_q -rational points of the curve defined by (2) for this canonical basis. In the last section, we prove Theorem 1, Theorem 2, and their corollaries.

2. THE GENUS CALCULATION

Let F_q be a finite field of characteristic p with $q = p^\nu$ elements. Let $f(x) \in F_q[x]$ be a polynomial of degree m with $(m, p) = 1$. Then the curve X defined over $\bar{F}_q$ by the equation

$$y^p - y = f(x) \quad (3)$$

is irreducible. The following lemma is well known, but we include the proof because a part of it will be used in the proof of Theorem 3.

Lemma 1. *The genus of the curve X is*

$$g(X) = \frac{1}{2}(p-1)(m-1).$$

Proof. The curve X provides a covering $\phi: X \rightarrow P^1$ of degree p of the projective line P^1 . The only ramification point of ϕ is the point at infinity. Let $p_\infty = [0 : 1]$ be the point at infinity and x be the coordinate in A^1 . If we take $t = 1/x$ as a local parameter at p_∞ , then the inverse image of p_∞ is the point x_∞ in the curve X which corresponds to the discrete valuation v_{x_∞} with $v_{x_\infty}(x) = -p$ and $v_{x_\infty}(y) = -m$. A local parameter at x_∞ is $s = 1/(x^a y^b)$, where $ap + bm = 1$. Since $v_{x_\infty}(1/(x^a y^b)) = 1$,

$$v_{x_\infty} \left(d \left(\frac{1}{x^a y^b} \right) \right) = v_{x_\infty} \left(\frac{bx^a y^{b-1} dy + ax^{a-1} y^b dx}{x^{2a} y^{2b}} \right) = 0.$$

Using $d(y^p - y) = df(x)$, or equivalently, $dy = -f'(x)dx$, we get

$$v_{x_\infty} \left(\frac{(bx f'(x) + ay)dx}{x^{a+1} y^{b+1}} \right) = 0.$$

Since

$$\begin{aligned} v_{x_\infty}(bxf'(x) + ay) &= \min\{v_{x_\infty}(bxf'(x)), v_{x_\infty}(ay)\} \\ &= v_{x_\infty}(bxf'(x)) = -mp, \end{aligned}$$

we deduce that the degree of the canonical divisor is

$$v_{x_\infty}(dx) = mp - m - p - 1.$$

Thus, $2g(X) - 2 = mp - m - p - 1$, which gives

$$g(X) = \frac{1}{2}(p-1)(m-1).$$

Since ϕ is a covering of degree p of the projective line P^1 , we have

$$2g(X) - 2 = p(2g(P^1) - 2) + \deg R_\phi, \quad (4)$$

where R_ϕ is the ramification divisor of ϕ .

Since the only ramification point of ϕ is x_∞ , $R_\phi = a_{x_\infty}x_\infty$. Combining equation (4) and the value of the genus, we get $a_{x_\infty} = (p-1)(m+1)$.

Now let A be a linear subspace of $F_q[x]$. Let $\{f_1, \dots, f_s\}$ be a canonical basis of A such that $\deg f_i(x) = m_i$ and $(m_i, p) = 1$. Assume that m_i are ordered such that $m_1 \leq \dots \leq m_s$. Let X_s be the curve given over $\bar{F}_q$ by the fibre product

$$\begin{aligned} y_1^p - y_1 &= f_1(x), \\ y_2^p - y_2 &= f_2(x), \\ &\vdots \\ y_s^p - y_s &= f_s(x). \end{aligned} \quad (5)$$

Theorem 3. *The genus of the curve X_s given by (5) is*

$$g(X_s) = p^{s-1} \frac{(p-1)(m_s-1)}{2} + \dots + p \frac{(p-1)(m_2-1)}{2} + \frac{(p-1)(m_1-1)}{2}.$$

Proof. For $1 \leq r \leq s$, let X_r be the curve in P^{s-r+1} defined by removing the first $r-1$ equations in (5). Then for any $2 \leq r \leq s$, X_{r-1} is a covering of X_r and X_s is a covering of the projective line P^1 , each of the covering is of degree p . Thus, we have the coverings

$$X_1 \rightarrow X_2 \rightarrow \dots \rightarrow X_s \rightarrow P^1.$$

To prove the formula of the genus, we use induction on s . For $s = 1$, the result is contained in Lemma 1. Suppose that the result holds true for $s-1$, then

$$g(X_2) = p^{s-2} \frac{(p-1)(m_{s-1}-1)}{2} + \dots + p \frac{(p-1)(m_2-1)}{2} + \frac{(p-1)(m_1-1)}{2}.$$

Since X_1 is a covering of degree p of X_2 , we have

$$2g(X_1) - 2 = p(2g(X_2) - 2) + \deg R_{\phi_2} \quad (6)$$

where R_{ϕ_2} is the ramification divisor of the covering $\phi_2: X_1 \rightarrow X_2$. If we bear in mind that the only ramification point of ϕ_2 is the point at infinity and the (smooth projective) curve X_2 near the point at infinity looks like the projective line P^1 , then by the arguments of Lemma 1 we see that

$$\deg R_{\phi_2} = (p-1)(m_1+1).$$

Thus (6) implies that

$$g(X_1) = pg(X_2) + \frac{1}{2}(p-1)(m_1-1),$$

which is the required result.

We emphasise that the ordering $m_1 \leq \dots \leq m_s$ of the degrees of the polynomials $f_1(x), \dots, f_s(x)$ is crucial. Indeed, if we regard each equation $y_i^p - y_i = f_i(x)$ in (5) separately as a covering of the projective line and $x_{i\infty}$ as the inverse image of the infinity point $[0:1] \in P^1$, then $x_{i\infty}$ corresponds to the discrete valuation $v_{x_{i\infty}}$ such that $v_{x_{i\infty}}(x) = -m_i$. Thus, we first have to consider the covering with the minimum valuation of x and this is clearly the covering with maximum m_i , say m_s . Repeating the same thing with the projective line replaced by the curve $y_s^p - y_s = f_s(x)$ and bearing in mind that the smooth projective model of this curve near the point at infinity looks like the projective line, we see the necessity of the ordering.

It is worth pointing out that one could use the genus formula for elementary Abelian p -extensions given in [1] or Theorem 2.2 in [3] to prove Theorem 3, but the advantage of our proof lies in its simplicity and closeness, in spirit, to the geometry of the curve X_s .

Remark 4. It is important to note that the value of the genus given in Theorem 3 is bounded by $(p^s - 1)(m_s - 1)/2$.

3. THE NUMBER OF F_q -RATIONAL POINTS

Let p be a prime number and F_q be a finite field with $q = p^v$ elements. We denote by $\text{Tr}_v: F_q \rightarrow F_p$ the trace map. The number N of solutions of the equation

$$y^p - y = f(x) \in F_q(x)$$

in $F_q \times F_q$ is given by

$$N = p|\{x \in F_q: \text{Tr}_v f(x) = 0\}|.$$

Using this well-known fact, we obtain the following assertion.

Lemma 2. *Let p be a prime number, $q = p^v$, where v is a positive integer, and let F_{q^2} be a finite field with q^2 elements. Then for any $a \in F_{q^2}^*$ such that $a + a^q = 0$ and any integer $j \geq 1$, the number of F_{q^2} -rational points of the affine curve*

$$y^p - y = ax^{j(1+q)}$$

is equal to $q^2 p$.

Proof. It is clear that

$$\begin{aligned}
 \text{Tr}_{2\nu}(ax^{j(1+q)}) &= \sum_{k=0}^{2\nu-1} (ax^{j(1+q)})^{p^k} \\
 &= \sum_{k=0}^{\nu-1} a^{p^k} x^{jp^k(1+q)} + \sum_{k=\nu}^{2\nu-1} a^{p^k} x^{jp^k(1+q)} \\
 &= \sum_{k=0}^{\nu-1} a^{p^k} x^{jp^k(1+q)} + \sum_{k=0}^{\nu-1} a^{p^{k+\nu}} x^{jp^{k+\nu}(1+q)} \\
 &= \sum_{k=0}^{\nu-1} a^{p^k} x^{jp^k(1+q)} + \sum_{k=0}^{\nu-1} -a^{p^k} x^{jp^k(q+q^2)}.
 \end{aligned}$$

Since $x^{q^2} = x$ for $x \in F_{q^2}$, we have $\text{Tr}_{2\nu}(ax^{j(1+q)}) = 0$ for any $x \in F_{q^2}$. This gives the result.

Lemma 3. *Let F_{q^2} be as in Lemma 2. Then for any $a \in F_{q^2}^*$ and any integer j , $0 < j \leq \nu - 1$, the number of F_{q^2} -rational points of the affine curve $y^p - y = ax^{1+p^{v+j}} - a^{p^{v-j}} x^{1+p^{v-j}}$ is equal to $q^2 p$.*

Proof. It is clear that

$$\begin{aligned}
 &\text{Tr}_{2\nu}(ax^{1+p^{v+j}} - a^{p^{v-j}} x^{1+p^{v-j}}) \\
 &= \sum_{k=0}^{2\nu-1} (ax^{1+p^{v+j}})^{p^k} - \sum_{k=0}^{2\nu-1} (a^{p^{v-j}} x^{1+p^{v-j}})^{p^k} \\
 &= \sum_{k=0}^{\nu-j-1} (ax^{1+p^{v+j}})^{p^k} + \sum_{k=\nu-j}^{2\nu-1} (ax^{1+p^{v+j}})^{p^k} \\
 &\quad - \sum_{k=0}^{\nu+j-1} (a^{p^{v-j}} x^{1+p^{v-j}})^{p^k} - \sum_{k=\nu+j}^{2\nu-1} (a^{p^{v-j}} x^{1+p^{v-j}})^{p^k} \\
 &= \sum_{k=0}^{\nu-j-1} a^{p^k} x^{p^k(1+p^{v+j})} + \sum_{k=0}^{\nu+j-1} a^{p^{v-j+k}} x^{p^k(p^{v-j}+q^2)} \\
 &\quad - \sum_{k=0}^{\nu+j-1} a^{p^{v-j+k}} x^{p^k(1+p^{v-j})} - \sum_{k=0}^{\nu-j-1} a^{p^{2v+k}} x^{p^k(p^{v+j}+q^2)} \\
 &= \sum_{k=0}^{\nu-j-1} a^{p^k} x^{p^k(1+p^{v+j})} - \sum_{k=0}^{\nu-j-1} a^{p^{2v+k}} x^{p^k(p^{v+j}+q^2)} \\
 &\quad + \sum_{k=0}^{\nu+j-1} a^{p^{v-j+k}} x^{p^k(p^{v-j}+q^2)} - \sum_{k=0}^{\nu+j-1} a^{p^{v-j+k}} x^{p^k(1+p^{v-j})}.
 \end{aligned}$$

Using the fact that $a^{q^2} = a$ and $x^{q^2} = x$ for $x \in F_{q^2}$, we obtain

$$\text{Tr}_{2\nu}(ax^{1+p^{\nu+j}} - a^{p^{\nu-j}}x^{1+p^{\nu-j}}) = 0$$

for any $x \in F_{q^2}$. This gives the result.

Let $S_1, S_2 \subset F_q[x]$ be the sets of polynomials having, respectively, the forms

$$f_1(x) = a_i x^{j(1+q)},$$

where $a_i \in F_{q^2}$ are such that $a_i^q + a_i = 0$, a_i are F_p -linearly independent, and $1 \leq j < q$, $(j, p) = 1$; and

$$f_2(x) = a_i x^{1+p^{\nu+j}} - a_i^{p^{\nu-j}} x^{1+p^{\nu-j}},$$

where $a_i \in F_{q^2}$ are F_p -linearly independent and $1 \leq j \leq \nu - 1$.

Using these sets of polynomials and Lemmas 2, 3, we arrive at the following result.

Lemma 4. *Let F_{q^2} be as in Lemmas 2, 3. Let $1 \leq s < q$ be an integer such that $(s, p) = 1$, and let X_s be the affine curve defined over $\bar{F}_{q^2}$ by the fibre product*

$$y_1^p - y_1 = f_1(x),$$

$$y_2^p - y_2 = f_2(x),$$

...

$$y_s^p - y_s = f_s(x),$$

where $f_i(x) \in S_1 \cup S_2$ are such that $\deg f_i(x) \leq s(q+1)$, $i = 1, \dots, s$.

Then the number $N_{q^2}(X_s)$ of F_{q^2} -rational points of X_s is

$$N_{q^2}(X_s) = q^{N_1(s)+2},$$

where $N_1(s) = s - [s/p] + 2[\log_p((s(q+1) - 1)/q)]$.

Proof. The family of polynomials $S_1 \cup S_2$ forms a canonical basis for a non-degenerate linear subspace of $F_q[x]$, hence the given system of equations defines a curve. By virtue of Lemmas 2 and 3, for any $x \in F_{q^2}$, the fibre over x on the curve X_s contains $p^{N(s)}$ F_{q^2} -rational points, where $N(s)$ is the number of the defining equations of the curve. Writing s in the form $s = np + r$, $1 \leq r \leq p - 1$, we see that the number of integers j such that $1 \leq j \leq s$ and $(j, p) = 1$ is equal to

$$n(p-1) + r = np + r - n = s - n = s - [s/p].$$

Thus, the number of the defining equations with polynomials coming from S_1 is equal to $\nu(s - [s/p])$. The number of the defining equations with polynomials coming from S_2 is equal to $2\nu m$, where m is the largest integer such that

$$p^{\nu+m} + 1 \leq s(p^\nu + 1).$$

Thus,

$$m = [\log_p((s(q+1) - 1)/q)],$$

and hence

$$N(s) = v((s - [s/p]) + 2[\log_p((s(q+1) - 1)/q)]) = vN_1(s),$$

which completes the proof.

The following two lemmas concern the case of F_q , $q = p^{2v+1}$.

Lemma 5. *Let p be a prime number, $q = p^{2v+1}$, where v is a positive integer, and let F_q be a finite field with q elements. Then for any $a_i \in F_q^*$ and any integer $j \geq 1$, the number of F_q -rational points of the affine curve*

$$y^p - y = a_i x^{j(p^{v+1}+1)} - a_i^{p^v} x^{j(p^v+1)}$$

is equal to qp .

Proof. It is clear that

$$\begin{aligned} & \text{Tr}_{2v+1}(ax^{j(p^{v+1}+1)} - a^{p^v}x^{j(p^v+1)}) \\ &= \sum_{k=0}^{2v} (ax^{j(p^{v+1}+1)})^{p^k} - \sum_{k=0}^{2v} (a^{p^v}x^{j(p^v+1)})^{p^k} \\ &= \sum_{k=0}^{v-1} a^{p^k} x^{jp^k(p^{v+1}+1)} + \sum_{k=v}^{2v} a^{p^k} x^{jp^k(p^{v+1}+1)} \\ &\quad - \sum_{k=0}^v a^{p^{v+k}} x^{jp^k(p^v+1)} - \sum_{k=v+1}^{2v} a^{p^{v+k}} x^{jp^k(p^v+1)} \\ &= \sum_{k=0}^{v-1} a^{p^k} x^{jp^k(p^{v+1}+1)} + \sum_{k=0}^v a^{p^{v+k}} x^{jp^{v+k}(p^{v+1}+1)} \\ &\quad - \sum_{k=0}^v a^{p^{v+k}} x^{jp^k(p^v+1)} - \sum_{k=0}^{v-1} a^{p^{2v+k+1}} x^{jp^{v+k+1}(p^v+1)} \\ &= \sum_{k=0}^{v-1} a^{p^k} x^{jp^k(p^{v+1}+1)} + \sum_{k=0}^v a^{p^{v+k}} x^{jp^k(p^{2v+1}+p^v)} \\ &\quad - \sum_{k=0}^v a^{p^{v+k}} x^{jp^k(p^v+1)} - \sum_{k=0}^{v-1} a^{p^{2v+k+1}} x^{jp^k(p^{2v+1}+p^v+1)}. \end{aligned}$$

Using the fact that $a^q = a$ and $x^q = x$ for $x \in F_q$, we obtain

$$\text{Tr}_{2v+1}(ax^{j(p^{v+1}+1)} - a^{p^v}x^{j(p^v+1)}) = 0$$

for any $x \in F_q$, which completes the proof.

If we take a_i in the previous lemma to be a basis of F_q over F_p and argue as in the proof of Lemma 4, we get the following assertion.

Lemma 6. *Let F_q be as in Lemma 5. Then for any integer s , $1 \leq s < p^{\nu-1}$, $(s, p) = 1$, the fibre product*

$$y_{ij}^p - y_{ij} = a_i x^{j(p^{\nu+1}+1)} - a_i^p x^{j(p^{\nu}+1)}$$

where $1 \leq j \leq s$, $(j, p) = 1$, has

$$qp^{(2\nu+1)(s-[s/p])}$$

F_q -rational points.

4. PROOF OF THE THEOREMS

In this section, we prove Theorem 1 and Corollary 1. The proofs of Theorem 2 and Corollary 2 are completely similar.

Proof of Theorem 1. Let F_{q^2} be a finite field consisting of $q^2 = p^{2\nu}$ elements, and let $1 \leq s < q$, $(s, p) = 1$. Let X_s be the affine curve defined in Lemma 4. By that lemma X_s has $q^{N_1(s)+2}$ F_{q^2} -rational points, where

$$N_1(s) = s - [s/p] + 2[\log_p((s(q+1)-1)/q)].$$

By normalization of the curve X_s , we obtain a non-singular model $\tilde{X}_s$ without losing F_{q^2} -rationality of these points. Taking into account the point at infinity p_∞ of the curve $\tilde{X}_s$, we obtain

$$N_{q^2}(\tilde{X}_s) = q^{N_1(s)+2} + 1.$$

By Theorem 3 and Remark 4 the genus of $\tilde{X}_s$ is less than

$$\frac{1}{2}(q^{N_1(s)} - 1)(s(q+1) - 1).$$

The proof is complete.

Before giving the proof for Corollary 1, we recall the well-known Goppa construction of the linear $[n, k, d]_q$ -codes associated to a smooth projective curve X over a finite field F_q , where $q = p^\nu$ (see [2]).

Let X be an absolutely irreducible smooth projective curve of genus g over F_q . Let $\{p_1, \dots, p_n\}$ be a set of distinct F_q -rational points on X and $D_0 = p_1 + \dots + p_n$. Let D be a F_q -rational divisor on X such that the supports of D and D_0 are disjoint. The linear space

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

yields the linear evaluation map

$$Ev: L(D) \rightarrow F_q^n, \quad f \rightarrow (f(p_1), \dots, f(p_n)).$$

The image of this map is the linear $[n, k, d]_q$ -code $C = C(D_0, D)$, which is called a geometric Goppa code associated to the pair (D_0, D) .

If $\deg D < n$, then Ev is an embedding, hence $k = \dim C = l(D)$. By the Riemann–Roch theorem,

$$k = l(D) \geq \deg D - g + 1.$$

In particular, if $2g - 2 < \deg D < n$, then $k = \deg D - g + 1$.

The minimum distance d of the code $C = C(D, D_0)$ satisfies the inequality

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

Hence it follows that the relative parameters $R = k/n$ and $\delta = d/n$ of the linear $[n, k, d]_q$ -code $C = C(D_0, D)$ satisfy the relation

$$R \geq 1 - \delta - \frac{g-1}{n}.$$

Now, applying Goppa's construction to the curves of Theorem 1, we prove Corollary 1.

Proof of Corollary 1. Let X_s be the (smooth projective) curve defined in Theorem 1. Let S be the set of F_{q^2} -rational points of X_s at the finite part of it, and let p_∞ denote the point of X_s at infinity. By Lemma 4 $|S| = q^{N_1(s)+2}$. Let $n \leq q^{N_1(s)+2}$ and

$$D_0 = p_1 + \dots + p_n, \quad D = lp_\infty.$$

Applying Goppa's construction to these F_{q^2} -divisors on X_s for any integer l such that

$$\frac{1}{2}(q^{N_1(s)} - 1)(s(q+1) - 1) < l < n,$$

we get the required code.

REFERENCES

1. A. Garcia and H. Stichtenoth, Elementary Abelian p -extensions of algebraic function fields. *Manuscr. Math.* (1991) **72**, 67–79.
2. V. G. Goppa, Codes on algebraic curves. *Soviet Math. Dokl.* (1981) **24**, 170–172.
3. G. Lachaud, Artin–Schreier curves, exponential sums, and the Carlitz–Uchiyama bound for geometric codes. *J. Number Theory* (1991) **39**, 18–40.
4. F. Özbudak, Codes on fibre products of some Kummer coverings. *Finite Fields and their Appl.* (1999) **5**, 188–205.
5. S. A. Stepanov, *Arithmetic of Algebraic Curves*. Plenum, New York, 1994.
6. S. A. Stepanov, *Codes on Algebraic Curves*. Plenum, New York, 1999.
7. S. A. Stepanov, Codes on fibre products of hyperelliptic curves. *Discrete Math. Appl.* (1997) **7**, 77–88.
8. S. A. Stepanov and F. Özbudak, Fibre products of hyperelliptic curves and geometric Goppa codes. *Discrete Math. Appl.* (1997) **7**, 223–229.
9. G. van der Geer and M. van der Vlugt, How to construct curves over finite fields with many points. In: *Algebraic Geometry E-prints*, alg-geom/9511005, 1995.
10. C. Xing and H. Stichtenoth, The genus of maximal function fields. *Manuscr. Math.* (1955) **86**, 217–224.