Chin. Ann. of Math.
15B: 3(1994),311-320.

GOPPA CODES FROM ARTIN-SCHREIER FUNCTION FIELDS

HAN WENBAO*

Abstract

A class of Goppa codes is constructed by using Artin-Schreier function fields, of which the number of prime divisors of degree one is obtained for some cases, and their minimum distance, duality and self-duality are discussed. At last the subfield subcode of Artin-Schreier code is investigated, the true dimension under certain conditions is given and the covering radius and minimum distance are estimated.

Keywords Artin-Schreier function field, Goppa code, Self-duality.
1991 MR Subject Classification 11T, 94B.

§0. Introduction

Algebraic geometric codes, which we always call Goppa codes, were first introduced by Goppa and proved to be better than the Gilber-Varshamov bound. Many good expositions about this topic can be found in [5,6,7,24,25]. New codes were constructed from Goppa's idea by using special curves such as elliptic curves. Hermitian curves, and their parameters can be given for partial cases.

In the present paper, we investigate the parameters of the algebraic geometric codes from Artin-Schreier curves first introduced by Stichtenoth[19]. The arrangement follows on this line. Section 1 gives the basic facts about Artin-Schreier function fields, e.g. the number of the prime divisors of degree one, the base and dimension of the function space $L(mQ)$, etc. In Section 2, we construct Artin-Schreier codes and obtain their parameters for many cases which generalize the results of [20]. In Section 3, we discuss the parameters of the subfield subcodes of Artin-Schreier codes using Bombier's reults about exponential sums. This method was used by Helleseth, Teitavainen, Moreno and Moreno to get the parameters of long BCH codes and Goppa codes such as their precise dimension and bounds on the covering radius and minimum distance.

§1. Basic Facts About Artin-Schreier Function Fields

Suppose $f(x) = \sum_{i=0}^{n} a_i x^i \in GF(p)(x)$. We associate it with a polynomial of the form $f^*(x) = \sum_{i=0}^{n} a_i x^{p^i}$, the so-called p-polynomial, $f(x)$ and $f^*(x)$ are called p-associated of each other. The polynomial $F(x,y) = x^r - f^*(y)$ is absolutely irreducible and the affine curve $C : x^r = f^*(x)$ is called Artin-Schreier curve. For our consideration, C is defined over

Manuscript received March 23, 1992.
*Department of Mathematics, Sichuan University, Chengdu 610064, Sichuan, China.

$K = GF(p^{2ab})$, $r|p^a+1$ and $f(x)|x^{2ab}-1$. The function field $K(C)$ of C is the finite seperate extension $K(x,y)$ of the single variable rational function field $K(x)$. $K(C)$ is called Artin-Schreier function field. The genus of $K(C)$ is $g(K(C)) = (r-1)(p^n-1)/2$.

In this section, we alway assume $f(x) = (x^{2ab}-1)/G(x)$. In [8], the author obtained the number of the roots $g^*(x^r)$ in K if $r|p^a+1$. From this result we can get the number of the K-rational points of Artin-Schreier curve. For this reason, we need the following lemma.

Lemma 1.1.[8] *$R(g^*(x)) = f^*(K)$. Here $R(g^*(x))$ is the root set of $g^*(x)$ in K; $f^*(K)$ is the image set of $f^*(x)$ over K.*

Later we suppose $R_r(g^*(x)) = \{\alpha \in K | \text{there exists } \beta \in R(g^*(x)) \text{ such that } \beta = \alpha^r\}$.

Theorem A.[8] *Suppose $\deg(f(x)) = n$, the order of $f(x)$ is e, i.e., the least integer such that $f(x)|x^e-1$, $(f(x),g(x))=1$, $r|p^a+1$. If $r|p^{2ab}-1/p^*-1$, then the number of the roots $g^*(x^r)$ in K is*

$$\#R_r(g^*(x)) = p^{2ab-n} + (-1)^{b-1}\delta(r,b)p^{ab-n}(p^n-1),$$

where

$$\delta(r,b) = \begin{cases} r-1 & \text{if } r \text{ odd or } p^a+1/r \text{ even or } b \text{ even,} \\ -1 & \text{if } r \text{ even, } p^a+1/r \text{ odd and } b \text{ odd.} \end{cases}$$

Theorem B.[8] *Suppose $\deg(f(x)) = n$, the suborder of $f(x)$ is e, i.e., the least integer such that $f(x)|x^e-1$, $(f(x),g(x))=1$, $r|p^a+1$. If $r|p^{2ab}-1/p^e-1$, then the number of the roots $g^*(x^r)$ in K is*

$$\#R_r(g^*(x)) = p^{2ab-n} + (-1)^{b-1}\varepsilon(r,b)p^{ab-n}(p^n-1),$$

where if $r|p^{2ab}-1/2(p^e-1)$, $\varepsilon(r,b) = \delta(r,b)$; if $r \nmid p^{2ab}-1/2(p^e-1)$,

$$\varepsilon(r,b) = \begin{cases} -1 & \text{if } r \text{ odd or } p^a+1/r \text{ even or } b \text{ even,} \\ r-1 & \text{if } r \text{ even, } p^a+1/r \text{ odd and } b \text{ odd.} \end{cases}$$

Now we can get the number of the rational points of Artin-Schreier curve from the above two theorems. If (x,y) is a sulotion of the equation $x^r = f^*(y)$, then $g^*(x^r) = 0$ by Lemma 1.1. For one such x, there are $p^{2ab-n}y'$s such that $x^r = g^*(y)$. Therefore $\#C = p^n\#R_r(g^*(x))$. From this we prove the following two theorems analogus to Theorems A and B.

Theorem 1.1. *Let the affine curve $C: x^r = f^*(y)$ be Artin-Schreier curve defined over K, $f(0) \neq 0$, the order of $f(y)$ be e, $(f(y),g(y)) = 1$, $f(y)g(y) = y^{2ab}-1$, $r|p^a+1$. If $r|p^{2ab}-1/p^e-1$, then the number of the rational points of C over K is*

$$\#C = p^{2ab} + (-1)^{b-1}\delta(r,b)p^{ab}(p^n-1),$$

where

$$\delta(r,b) = \begin{cases} r-1 & \text{if } r \text{ odd or } p^a+1/r \text{ even or } b \text{ even,} \\ -1 & \text{if } r \text{ even, } p^a+1/r \text{ odd and } b \text{ odd.} \end{cases}$$

Theorem 1.2. *Let the affine curve $C: x^r = f^*(y)$ be Artin-Schreier curve defined over K, $f(0) \neq 0$, the suborder of $f(y)$ be e, $(f(y),g(y)) = 1$, $f(y)g(y) = y^{2ab}-1$, $r|p^a+1$. If $r|p^{2ab}-1/p^e-1$, then the number of the rational points of C over K is*

$$\#C = p^{2ab} + (-1)^{b-1}\varepsilon(r,b)p^{ab}(p^n-1),$$

where if $r|p^{2ab}-1/2(p^e-1)$, $\varepsilon(r,b)=\delta(r,b)$; *if* $r\nmid p^{2ab}-1/2(p^e-1)$,

$$\varepsilon(r,b)=\begin{cases}-1 & \text{if } r \text{ odd or } p^a+1/r \text{ even or } b \text{ even},\\ r-1 & \text{if } r \text{ even, } p^a+1/r \text{ odd and } b \text{ odd}.\end{cases}$$

Remark 1.1. Later we always denote the number of the rational points of (affine curve) C by N which can be obtained from the above two theorems.

Since in $K(C)$ the infinite prime divisor of $K(x)=\infty=(1/x)$ is totally ramified, $K(C)$ has only one infinie prime divisor Q of degree one and we have $(1/x)=p^nQ$. Hence there are $N+1$ prime divisors of degree one in $K(C)$ and we can conclude for which r and f, $K(C)$ has the maximal number (attaining the Hasse-Weil bound) of prime divisors of degree one from Theorem 1.1 and Theorem 1.2.

Let $(\alpha,\beta)\in C$, and $P_{(\alpha,\beta)}$ be the prime divisor of degree one of $K(C)$ which is corresponding to the common zero of $x-\alpha$ and $y-\beta$. Every finite prime divisors of degree one of $K(C)$ has the form $P_{(\alpha,\beta)}$ and we can get the following decompositions of the principal divisors.

$$(x-\alpha)=\sum_{a^r=f^*(\beta)}P_{(\alpha,\beta)}-p^nQ,$$

$$(y-\beta)=\begin{cases}rP_0-rQ & \text{if } f^*(\beta)=0,\\ \displaystyle\sum_{a^r=f^*(\beta)}P_{(\alpha,\beta)}-rQ & \text{if } f^*(\beta)\neq 0.\end{cases}$$

Given a divisor G defined over K, the function space $L(G)$ is defined by $L(G)=\{t\in K(C)|(t)\geq -G\}$. It is well known that $L(G)$ is a finite dimensional vector space over K; the dimension is denoted by $l(G)$. For Artin-Schreier function field, we have the following result.

Proposition 1.1. *Let* m *be an intger greater than or equal to* 0.

(i) *The set* $\{h_i(x)k_j(y)|0\leq i;\ 0\leq j\leq p^n-1;\ ip^n+jr\leq m,\ h_i(x)\in K(x),\ \deg(h_i)=i,\ k_j(y)\in K(y),\ \deg(k_j)=j\}$ *is a base of* $L(mQ)$ *over* K.

(ii)

$$l(mQ)=\begin{cases}m-g+1 & \text{if } N>m>2g-2,\\ \displaystyle\sum_{j=0}^{c}((m-jr)/p^n)+c & \text{if } m\leq 2g-2,\end{cases}$$

where $c=[m/r]$, $[\ ]$ *denotes the integer part.*

Proof. Since $\{x^iy^j|0\leq i;\ 0\leq j\leq p^n-1;\ ip^n+jr\leq m\}$ is a base of $L(mQ)$, it is easily seen that (i) holds. For (ii), the first is by Riemman-Roch theorem and the second by counting the base set of (i).

Let Ω be the differential space of $K(C)$ over K, G a divisor of $K(C)$. The subspace of $\Omega(G)$ is defined by $\Omega(G)=\{\omega\in\Omega|(\omega)\geq G\}$. Let $z=g^*(x^r)/x^{r-1}$. Then $(z)=D-(N)Q$, where $D=\sum P_i$ is the sum of all finite prime divisors $P_i\,(i=1,2,\cdots,N)$ of degree one of $K(C)$. Thus $dz=(2g-2)Q$. For differential $\eta=dz/z$, we have

$$(\eta)=(dz)-(z)=(2g-2)Q-D+(N)Q=(N+2g-2)Q-D.$$

If P is a simple zero, then P is a simple pole of dz/z and the residue is 1. We have

Proposition 1.2. *The conditions as above,* $\mathrm{Res}_{P_i}(\eta) = 1,\ i = 1, 2, \cdots, N.$

§2. Construction of Goppa Codes by Artin-Schreier Function Fields

Let $D = P_1 + P_2 + \cdots + P_s$ be a divisor of $K(C)$ over K, where P_i is the prime divisor of degree one of $K(C)$. Let G be an arbitrary divisor of $K(C)$, whose support is disjoint from that of D. Then the codes $C(G, D)$ and $C^*(G, D)$ are defined by

$$C(G, D) = \{(f(P_1), f(P_2), \cdots, f(P_s)) | f \in L(G)\},$$

$$C^*(G, D) = \{(\mathrm{Res}_{P_1}(\omega), \mathrm{Res}_{P_2}(\omega), \cdots, \mathrm{Res}_{P_s}(\omega)) | \omega \in \Omega(D - G)\}.$$

Later we assume $G = mQ$ and $D = \sum P_i$. Now we can obtain the following results which is a modification of [5].

Theorem 2.1. *$C(mQ, D)$ and $C((N + 2g - 2 - m)Q, D)$ are dual to each other for any $m \in Z$. In particular, if $p = 2$ and $m = (N + 2g - 2)/2$, $C(mQ, D)$ is self-dual.*

Proof. We know that $C(mQ, D)$ and $C^*(mQ, D)$ are dual to each other. Since η is a base of Ω, we have

$$\begin{aligned} u\eta \in \Omega(D - G) &\Leftrightarrow (u) + (\eta) \geq D - G \\ &\Leftrightarrow (u) \geq D - G - (\eta) = (N + 2g - 2)Q \\ &\Leftrightarrow u \in L(N + 2g - 2)Q). \end{aligned}$$

By Proposition 1.2, we have

$$\begin{aligned} &(\mathrm{Res}_{P_1}(u\eta), \mathrm{Res}_{P_2}(u\eta), \cdots \mathrm{Res}_{P_s}(u\eta)) \\ &= (u(P_1)\mathrm{Res}_{P_1}(\eta), u(P_2)\mathrm{Res}_{P_2}(\eta), \cdots u(P_N)\mathrm{Res}_{P_s}(\eta)) \\ &= (u(P_1), u(P_2), \cdots, u(P_N)). \end{aligned}$$

Hence $C(mQ, D) = C((N + 2g - 2)Q, D)$. The theorem is proved.

Next we consider the dimension of $C(mQ, D)$. It is easily seen that $\dim C(mQ, D) = 0$ if $m < 0$ and $\dim C(mQ, D) = N - 1$ if $m > N + 2g - 2$. For other m, we have

Theorem 2.2. *Suppose $0 \leq m \leq N + 2g - 2$. Then*

$$\dim C(mQ, D) = \begin{cases} l(mQ) & if\ m \leq 2g - 2, \\ m + l - g & if\ 2g - 2 < m < N, \\ N - l((N + 2g - 2)Q) & if\ m \geq N. \end{cases}$$

Here $l(mQ)$ is given by Proposition 1.1.

Proof. The first is by Proposition 1.1, the second by Riemman-Roch theorem, the last by Theorem 2.1.

Now we discuss the minimum distance of $C(mQ, D)$. As in [18], we define

$$A(m) = \{0 \leq l \leq m | \text{ there are } i \geq 0 \text{ and } 0 \leq j \leq p^n - 1 \text{ such that } l = ip^n + jr\},$$

$$m^\sim = \max\{l | l \in A(m)\}.$$

Then we have $A(m) = A(m^\sim)$ and $C(mQ, D) = C(m^\sim Q, D)$. For the general minimum distance $d(C(mQ, D))$ of Goppa code $C(mQ, D))$, from [7,20] we have

Theorem 2.3. *Let $0 \leq m \leq N$. $d(C(mQ, D)) \geq N - m^\sim$.*

In general, the bound above is not tight, but we can try to obtain some cases with equlity. For this reason, we construct some special rational functions in $L(mQ)$ which have the zeros in C as many as possible.

Proposition 2.1. *If one of the following conditions holds, then there exists a rational function $u \in L(mQ)$ with exactly m distinct zeros.*

(i) $m = ip^n \leq N$.

(ii) $m = ip^n + jr < N - (r-1)p^n$, $0 \leq i$, $0 \leq j \leq p^n - 1$.

Proof. (i) Let S be a subset of $R_r(g^*(x))$ such that $\#S = i$. Then $\prod\limits_{\alpha \in S}(x-\alpha) \in L(mQ)$ and $\prod(x-\alpha)$ has ip^n zeros.

(ii) Let $\lambda \in R_r(g^*(x))\backslash\{0\}$,

$$A(\lambda) = \{\beta \in K | f^*(\beta) = \lambda^r\} \text{ and } A = \{\alpha \in K | \alpha^r \neq \lambda^r\}.$$

Then $\#A(\lambda) = p^n$ and $\#A = \#(R_r(g^*(x)) - r)$. Since $m < N - (r-1)p^n$ and $N = p^n \#R_r(g^*(x))$, $i \leq \#A$. Take a subset S_1 of $A(\lambda)$ such that $\#S_1 = j$ and a subset S_2 of A such that $\#S_2 = i$. The rational function $t_1 = \prod\limits_{\beta \in S_1}(y-\beta)$ has jr different zeros; $t_2 = \prod\limits_{\alpha \in S_2}(x-\alpha)$ has ip^n different zeros. We see that the zeros of t_1 are different from those of t_2. Hence $t_1 t_2$ has $ip^n + jr$ distinct zeros.

Theorem 2.4. *Let $m = ip^n + jr \leq N-1$, $0 \leq i$, $0 \leq j \leq p^n - 1$. If $j = 0$ or $m < N - (r-1)p^n$, then $d(C(mQ, D))) = N - m$.*

Proof. Take $t \in L(mQ)$ such that t has m distinct zeros. The weight of the vector $(u(P_1), u(P_2), \cdots, u(P_N))$ is $N - m$. By Theorem 2.1, $d(C(mQ, D)) = N - m$.

Corollary 2.1. *If $(p^n - 1)r \leq m < N - (r-1)p^n$, then $d(C(mQ, D)) = N - m$.*

Proof. Since $(r, p^n) = 1$, $\{m - jr | 0 \leq j \leq p^n - 1\}$ is a residue system modula p^n. Hence there exists j such that $p^n | m - jr$. Let $i = (m - jr)/p^n$. Then $i \geq 0$ and $m = ip^n + jr$. By Theorem 2.4, the corollary holds.

At last we give a generator matrix and a parity check matrix of C_m. Let $\{h_i(x)g_j(y)\}$ be a base of $L(mQ)$ from Proposition 1.1 and u_{ij} be the row vector $(h_i(\alpha)g_j(\beta))$ where (α, β) runs through all rational points of C. We use the M_n to denote the matrix with row vector u_{ij}. Then we have

Theorem 2.5. (i) *If $0 \leq m \leq N-1$, M_m is a generator matrix of $C(mQ, D)$.*

(ii) *If $2g - 2 < n \leq N + 2g - 2$, M_{N+2g-2} is a parity check matrix of $C(mQ, D)$.*

Remark 2.1. By the proof of Proposition 2.1, we can use Proposition 1.1 to make M_m simpler.

Proof. Directly by Proposition 1.1 and Theorem 2.1.

§3. Subfield Subcode of Artin-Schreier Code Over $GF(p)$

In thgis second, we discuss the parameters of the subfield subcode, which is denoted by $C_p^*(mQ, D)$, of $C^*(mQ, D)$ over $GF(p)$. First of all, we give a generalization of Delsarte's result about the dual of the subfield subcode of Goppa code.

Theorem 3.1.[2] *The dual of the subfield subcode of $C^*(mQ, G)$ is given by $C_p^*(mQ, D) = \sigma(C(mQ, D))$ where $\sigma(x) = x + x^p + x^{p^2} + \cdots + x^{p^{2ab-1}}$ for $x \in K$ is the absolute trace function*

of K to $GF(p)$ and

$$\sigma(C(mQ,D)) = \{(\sigma(f(P_1)),\sigma(f(P_2)),\cdots,\sigma(f(P_s)))|f \in L(mQ)\}.$$

In [17], [27], a few estimates about the parameters of the subfield subcode of Goppa code are obtained, which have been generalized in [9]. Now we use the method of [9], which is a combination of [17] and [27], to get the parameters of $C_p^*(G,D)$. First we need the following estimate based on Bombieri's results[1].

We say $f \in K(C)$ satisfies condition (B) if

(B) $f \neq h^p - h$ for any $h \in K(C)$, where $\overline{K}$ is the algebraic closure of K.

Theorem 3.2. *If $f \in L(mQ)$ and f satisfies condition* (B), *then*

$$\left|\sum_{i=1}^{N} \Psi(\sigma(f(P_i)))\right| \leq (m+2g-1)p^{ab},$$

where $\Psi(x) = e^{2\pi x/p}$ is the canonical additive character of $GF(p)$.

Remark 3.1. In Bombieri's original result, C is complete nonsingular. In our cases, C is not always complete nonsingular. But for the complete nonsingular model of C, the image of f under the birational isomorphism only has the possible pole corresponding to Q of order $\leq m$. Thus Bombieri's statement still holds.

Next we always assume $2g-2 \leq m \leq N-1$ and in Theorem 2.6 we take $h_i(x) = x^i$ and $g_j(y) = y^j$. Then the corresponding matrix M_T is a parity check matrix of $C^*(mQ,D)$ $(T = N+2g-2-m)$ by Theorem 2.2 and hence M_T is a parity check matrix $C_p^*(mQ,D)$. Next we want to simplify the parity check matrix M_T. For this reason let

$$A'(m) = \{(i,j) \in A(m)|p \nmid g.c.d(i,j)\} \quad \text{and} \quad A_p(m) = \{(i,j) \in A(m)\,|\,p\,|\,g.c.d(i,j)\},$$

where $g.c.d(i,j)$ denotes the greatest common divisor of i,j, $A(m) = A'(m) \cup A_p(m)$. Now we delete the rows $u_{i,j}$ of M_T such that $(i,j) \in A_p(m)$, $(i,j) \neq (0,0)$, to get a matrix M_T' and use $L'(mQ)$ to denote the subspace of $L(mQ)$ generated by $\{x^iy^j|(i,j) \in A'(m)\}$.

Theorem 3.3. (i) *M_T' is a parity check matrix of $C_p^*(mQ,D)$.*

(ii) *If $f \in L'(mQ)$, then f satisfies condition* (B) *and the dimension of $L'(mQ)$ is $l'(mQ) = l(mQ) - l([m/p]Q)$.*

Proof. (i) Let $c = (c_1,c_2,\cdots,c_{N-1}) \in C_p^*(mQ,D)$. If $i = pi', j = pj'$, $i > 0, j > 0$, then

$$u_{i,j}c^t = 0 \Leftrightarrow u_{i'j'}^p c^t = 0 \Leftrightarrow (u_{i'j'}c^t)^p = 0 \Leftrightarrow u_{i'j'}c^t = 0.$$

Therefore we can delete the row u_{ij} in M_T to get a matrix which is also a parity check matrix. From this (i) holds.

(ii) At this time we take $L(mQ)$ and $L'(mQ)$ to be the vector space over the algebraic closure $\overline{K}$ of K. It is familiar that $\{u_{ij}\}$ is still a base of $L(mQ)$. Let $f = \sum_{(i,j)\in A'(m)} f_{i'j'}x^{i'}y^{j'}$ be non-costant and in $L'(mQ)$, $f_{i'j'} \in \overline{K}$. If f does not satisfy condition (B), suppose $f = h^p - h$, $h \in \overline{K}(C)$ in $L'(mQ)$, $f_{i'j'} \in \overline{K}$. Then $h \in L'([m/p],Q)$, suppose $h = \sum h_{ij}x^iy^j$ and (i_m,j_m) be the pair such that $(i,j) \in A([m/p])$, $h_{ij} \neq 0$ and $ip^n + jr$ is largest. We have

$$f = \sum_{(i,j)\in A'(m)} f_{i'j'}x^{i'}y^{j'} = h_{i_mj_m}^p x^{pi_m}y^{pj_m} + \sum \cdots.$$

But this will produce $h_{i_m j_m} = 0$ since $\{x^i y^j | (i,j) \in A(m)\}$ is a base of $L(mQ)$.

It is a contradiction. So f satisfies condition (B).

It is easily seen that $\#A_p(m) = \#A([m/p])$, hence

$$l'(m) = \#A_p(m) = l(mQ) - l([m/p])Q).$$

Now we can give a result on the minimum distance of $\sigma(C(mQ,D))$. But we first need a simple fact: if $c \in GF(p)$, then

$$\sum_{s=0}^{p-1} e^{2\pi ics/p} = \begin{cases} p & \text{if } c = 0, \\ 0 & \text{if } c \neq 0. \end{cases}$$

From now on we denote the Hamming weight of a codeword V by $w(V)$.

Theorem 3.4. *The minimum distance of $\sigma(C(mQ,D))$ is at least*

$$\{N - (m + 2g - 1)p^{ab}\}(p-1)/p.$$

Proof. Let $V \in \sigma(C(mQ,D))$. Then $V = (\sigma(f(P_1)), \sigma(f(P_2)), \cdots, \sigma(f(P_N)))$ for $f \in L(mQ)$. If f is a constant, the weight of V is 0 or N. If $f = h^p - h$ for some $h \in K(C)$, then $V = 0$. Therefore we can assume that f is non-constant and satisfies condition (B). At this time we have

$$\begin{aligned} N - w(V) &= (1/p) \sum_{i=0}^{N} \sum_{s=0}^{p-1} \Psi(s\sigma(f(P_i))) \\ &= (1/p) \sum_{s=0}^{p-1} \sum_{i=0}^{N} \Psi(\sigma(sf(P_i))) \\ &= (1/p) \Big\{ N + \sum_{s=1}^{p-1} \sum_{i=1}^{N} \Psi(\sigma(sf(P_i))) \Big\}. \end{aligned}$$

By Theorem we have the following estimate.

$$\Big| \sum_{s=1}^{p-1} \sum_{i=1}^{N} \Psi(\sigma(sf(P_i))) \Big| \leq (p-1)(m + 2g - 1)p^{ab}.$$

So we get

$$w(V) \geq \{N - (2m + 2g)p^{ab}\}(p-1)/p.$$

Now we deal with the dimension, covering radius and minimum distance of $C_p^*(mQ,D)$. The following discussions are similar to [15]. Later we denote the base $\{u_{i'j'}\}$ of $L'(mQ)$ by $\{u_1, u_2, \cdots, u_{l'}\}$, where $l' = l'(mQ)$. Then

$$M_T' = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ u_1(P_1) & u_1(P_2) & \cdots & u_1(P_N) \\ u_2(P_1) & u_2(P_2) & \cdots & u_2(P_N) \\ \cdots & \cdots & \cdots & \cdots \\ u_{l'}(P_1) & u_{l'}(P_2) & \cdots & u_{l'}(P_N) \end{pmatrix}.$$

It is will known that we can get a parity check matrix H of $C_p^*(mQ,D)$ over $GF(p)$ from M_T'. The dimension of $C_p^*(mQ,D)$ equals to $N - r(H)$, $r(H)$ is the rank of H. For arbitary given $b_1, b_2, \cdots b_w \in K$, $c_1, c_2, \cdots, c_w \in GF(p)$, $c_i \neq 0$, $i = 1, 2, \cdots, w$, we consider the

solvability of the following system for the variable X_i in C

$$(*)\quad \begin{cases} c_1u_1(X_1)+c_2u_1(X_2)+\cdots+c_wu_1(X_w)=b_1, \\ c_1u_2(X_1)+c_2u_2(X_2)+\cdots+c_wu_2(X_w)=b_2, \\ \cdots\cdots\cdots\cdots \\ c_1u_{l'}(X_1)+c_2u_{l'}(X_2)+\cdots+c_wu_{l'}(X_w)=b_{l'}. \end{cases}$$

We can conclude that if there exists always a solution $X=(X_1,X_2,\cdots,X_w)\in C^w$ of $(*)$ for some integer $w>0$, the rank of H' must be abl', where H' is the submatrix of H corresponding to $M''T$ which is obtained by deleting the first row of M'_T.

Next we use the techniques of character sum to investigate when $(*)$ has a solution. First let $C_i=1$. We recall the following orthogonal relation

$$\sum_{\alpha\in K}\Psi(\sigma(\alpha c))=\begin{cases} p^{2ab} & \text{if } \alpha\neq 0, \\ 0 & \text{if } \alpha=0. \end{cases}$$

We use N_w to denote the number of the solutions $X=(X_1,X_2,\cdots,X_w)$ of $(*)$ in C^*. Then

$$\begin{aligned} p^{abl'}N_w &= \sum_{X\in C^w}\prod_{i=1}^{l'}\sum_{\alpha_i\in K}\Psi(\alpha_i(u_i(X_i)+u_i(X_2)+\cdots+u_i(X_w))) \\ &= \sum_{\substack{\alpha_i\in K,\\ 0\le i\le l'}}\prod_{i=1}^{w}\sum_{X_i\in K}\Psi(\alpha_1(u_1(X_i)+u_2(X_i)+\cdots+u_il'(X_i))) \\ &= \sum_{\substack{\alpha_i\in K,\\ 0\le i\le l'}}\sum_{X\in K}\Psi(\alpha_1(u_1(X)+u_2(X)+\cdots+u_il'(X)))^w. \end{aligned}$$

Because of the choice of u_i, we know that except $\alpha_1=\alpha_2=\cdots=\alpha_{l'}=0$, $u_1(X)+u_2(X)+\cdots+u_{l'}(X)$ is non-constant and satisfies condition (B). So we have the following estimate

$$|q^{l'}N_w-N^w|\le(q^{l'}-1)(A\sqrt{q})^w,$$

where $A=m+2g-1$. If $N_w=0$, then

$$N^w<q^{l'}A^w(\sqrt{q})^w \quad\text{and}\quad A>N\sqrt{q}(q^{-l'/w}).$$

Therefore if we take $A\le N\sqrt{q}(q^{-l'/w})$, $N_w>0$. But for any

$$b_1,b_2,\cdots,b_N\in K,\ \ c_1,c_2,\cdots,c_w\in GF(p),\ \ c_i\neq 0,\ \ i=1,2,\cdots,w$$

we can take arbitrary large w to get a solution $X=(X_1,X_2,\cdots,X_w)$. Hence if $A<N(\sqrt{q})-1$, $(*)$ always has a solution and $r(H')=2abl'$. At last since $c_1,c_2,\cdots,c_N$ are arbitrarily given, we must have $r(H)=r(H')+1=2abl'+1$. The following result is proved.

Theorem 3.5. *If $m+2g-1<N(\sqrt{q})-1$, the dimension of $C_p^*(mQ,D)$ is $N-2abl'-1$.*

Now we consider the covering radius. The character sum trick is used to investigate the covering radius of long BCH code first by Herlleseth, then by Tietavainen, further by Moreno and Moreno for Goppa codes. Our discussion is similar. It is well known that estimating the covering radius of a linear code with parity check matrix H' is equivalent to finding the least integer w such that the system of equation $M''_Tc^t=b^t$ is solvable with any

$$b=(b_1,b_2,\cdots,b_{l'})\in K^{l'},\ \ c=(c_1,c_2,\cdots,c_w)\in GF(p)^w,\ \ c_i\neq 0.$$

By the previous discussion, $M_T'' c^t = b^t$ is solvable if $A \le N\sqrt{q}(q^{-l'/w})$, i.e.,

$$w \ge l' \ln q / \ln(n) - \ln(A) = (\ln(q)/2).$$

At last considering the solvability of equation $c_1 + c_2 + \cdots + c_w = b_0$ for any $b_0 \in GF(p)$ such that $c_i \ne 0$, $i = 1, 2, \cdots, w$, we prove

Theorem 3.6. *Let t be the covering radius of $C_p^*(mQ, D)$. Then*

$$t \le l' \ln(q)/(\ln(N) - \ln(A) - (\ln(q)/2)) + p - 1.$$

Corollary 3.1. *If $N \ge A^{4l'+2}$, we have $t \le 2m - 2g + p - 1$.*

At last we will give an upper bound of the minimum distance of $C_p^*(mQ, D)$. To do this, in the system of equation $(*)$ let w be an integer and $c_1 = c_2 = \cdots = c_{w-1} = 1$, $c_w = -w + 1$; $\beta_1 = \beta_2 = \cdots = \beta_w = 0$. The solutions of $(*)$ may produce the trivial codeword $(0, 0, \cdots, 0)$, the number of those solution is $N^{\lceil w/p \rceil}$, where $\lceil w/p \rceil$ is the least integer which is greater than or equal to w/p. If there are only such that solutions, by the inequlity before we have

$$\left| N^w - q^{l'} N^{\lceil w/p \rceil} \right| < q^{l'} A^w q^{w/2}.$$

If W_m denotes the least integer w such that the above inequality is not satisfied, i.e.,

$$\left| N^w - q^{l'} N^{\lceil w/p \rceil} \right| \ge q^{l'} A^w q^{w/2},$$

then we have

Theorem 3.7. *Let d be the minimum distance of $C_p^*(mQ, D)$. Then*

$$m + \mu(m) - 2g + 2 \le d \le W_m,$$

where

$$\mu(m) = \begin{cases} 1, & if \quad m \equiv p - 1 \bmod p, \\ 0, & otherwise. \end{cases}$$

Remark 3.1. The first inequality is from [27].

Corollary 3.2. *If $N \ge A^{2l'+2}$, $W_m \le 2l' + 2$.*

Proof. Take $w = 2l' + 2$. Since $N > q + 1$, $N^{w-1} - q^{l'} N^{w/2} \ge q^{l'+w/2}$. Then

$$N \le (N^w - q^{l'} N^{w/2})/q^{l'+w/2} \le (N^w - q^{l'} N^{w/p})/q^{l'+w/2}.$$

Therefore if $N \ge A^{2l'+2}$,

$$N^w - q^{l'} N^{w/p} \ge N q^{l'+w/2} \ge q^{l'} A^w q^{w/2}.$$

We get $W_m \le 2l' + 2$.

Acknowledgment. The author is very grateful to Prof. Sun Qi for his kind comments.

REFERENCES

[1] Bombieri, E., On exponential sums in finite fields, *Amer. J. of Math.*, **88** (1966), 71-105.
[2] Delsarte, P., On subfields subcodes of Reed-Solommon codes, *IEEE Trans. on IT*, **21** (1975), 575-576.
[3] Driencourt, Y., Some properties of elliptic codes over a field of characteristic two, *AAECC-3, Lecture Notes in Computer Science*, **229** (1986), 185-193.
[4] Fulton, W., Algebraic curves, Reading: Benjamin Cummings, 1969.
[5] Goppa, V. D., Codes on algebraic curves, *Soviet Math Doklady*, **24** (1981), 170-172.
[6] Goppa, V. D., Algebraic-Geometric codes, *Math. of the USSR, Izvestiya*, **39:1** (1983), 75-91.
[7] Goppa, V. D., Codes and information, *Russian Math. Survrys*, **39:1** (1984), 87-141.
[8] Han, W. B., Power roots of linearized polynomials, *Proc. of Amer. Math. Soc.*, **111:4** (1991), 913-920.

[9] Han, W. B., On the dimensions of the subfield subcodes of Goppa codes(preprint).
[10] Hartshore, R. D., Algebraic geometry, GTM 52, Springer-Verlag, Berlin/Heidereberg/ New York, 1977.
[11] Helleseth, T., On the covering radius of cyclic linear codes and arithmetic codes, *Discrete Appl. Math.*, **11** (1985), 157-173.
[12] Hirschfeld, J. W. P., Linear codes and algebraic curves, in Geometrical Combinatories, Holroyd, F. C. and Wilson, R. J., Eds. Boston, MA, Pitman, 1984.
[13] Hirschfeld, J. W. P., Projective geometries over finite fields, Oxford Univ. Press, 1979.
[14] Lidl, R. & Niederreiter, H., Finite fields, Reading, M. A. Addison-Wesley, 1983.
[15] MacWilliams, F. J. & Sloane, N. J. A., The theory of error-correcting codes, North-Holland, Amsterdam, 1977.
[16] Manin, Y. I. & Vladut, S. G., Linear codes and modular curves, *J. of Sov. Math.*, **30:6** (1985), 2611-2644.
[17] Moreno, C. J. & Moreno, O., Exponential sums and Goppa codes: (I), *Proc. of Amer. Math. Soc.*, **VIII**(1991), 523-531; (II), (III), (IV), *IEEE Trans. on IT*, **38:**4(1992), 1222-1229.
[18] Moreno, C. J. & Moreno, O., An improved Bombieri-Weil bound for characteristic two and application to coding theory, (submitted to, *J. of Number Theory*).
[19] Stichtenoth, H., Self-dual Goppa codes, *J. of Pure and Appl. Algebra*, **55** (1988), 199-211.
[20] Stichtenoth, H., A note on Hermitian codes over $GF(q^2)$, *IEEE. Trans, on IT*, **34:5** (1988).
[21] Tietavainen, A., On the covering radius of long binary BCH codes, *Discrete Appl. Math.*, **16** (1987), 75-77.
[22] Tsfasman, M. A., Vladut, S. G. & Zink, T., Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound, *Math. Nachr.*, **104** (1982), 13-28.
[23] Van Lint, J. H., Introduction to coding theory, GTM 86, Springer-Verlag, Berlin/Heiderber/New York, 1982.
[24] Van Lint, J. H. & Springer, T. A., Generalized Reed-Solomon codes from algebraic geometry, *IEEE Trans. on IT*, **33:3** (1987), 305-309.
[25] Van Lint, J. H., Springer, T. A. & Van der Geer, G., Introduction to coding theory and algebraic geometry, Birkhauser Verlag, Basel, 1988.
[26] Weil, A., On some exponential sums, *P. N. Acad. Sci. USA*, **34** (1948), 204-207.
[27] Wirtz, M., On the Parameters of Goppa codes, *IEEE Trans. on IT*, **34:5** (1988), 1341-1343.