Discrete Math. Appl., Vol. 7, No. 3, pp. 223–229 (1997)

Fibre products of hyperelliptic curves and geometric Goppa codes*

S. A. STEPANOV and F. ÖZBUDAK

Abstract — The purpose of this paper is to extend the results of the first author on construction of fairly long geometric Goppa codes over F_q ($q = p^v$ and $v > 1$ is even) with rather good parameters to the case of finite fields F_q consisting of $q = p^v$ elements, where $v > 1$ is an odd integer.

The work was supported by Bilkent University, Ankara, Turkey.

The first author was partially supported by the Russian Foundation for Basic Research, grant 94-01-01206-a.

1. INTRODUCTION

Recall the basic ideas of the Goppa construction (see [2, 3]) of the linear $[n, k, d]_q$-codes associated with a smooth projective curve X of genus $g = g(X)$ defined over a finite field F_q. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a set of F_q-rational points of X and

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

Let D be a F_q-rational divisor on X whose support is disjoint with D_0. We consider the vector F_q-space of rational functions on X

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

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

$$\mathrm{Ev}\colon L(D) \to F_q^n, \qquad f \mapsto (f(x_1), \ldots, f(x_n)).$$

Such a q-ary linear code is called a geometric Goppa code. If $\deg D < n$, then the map Ev is an embedding, 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

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

*UDC 519.72. Originally published in *Diskretnaya Matematika* (1997) **9**, No. 3 (in Russian). Received August 13, 1996. Translated by the authors.

Theorem 1. *Let $v > 1$ be an odd number, F_q be a finite field of characteristic $p > 2$ consisting of $q = p^v$ elements, and let s be an integer such that*

$$1 \le s < \frac{2p^v + 4}{p^{(v-1)/2}(p+1) - 2}.$$

Moreover, let r be an integer such that

$$2^{s-2}((p^{(v-1)/2}(p+1) - 2)s - 4) < r < 2^s p^v.$$

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

$$\begin{aligned} &r < n \le 2^s p^v, \\ &k = r - 2^{s-2}((p^{(v-1)/2}(p+1) - 2)s - 4), \\ &d \ge n - r. \end{aligned}$$

Corollary 1. *Under the conditions of Theorem 1, there exists a linear $[n, k, d]_q$-code with the relative parameters $R = k/n$ and $\delta = d/n$ such that*

$$R \ge 1 - \delta - \frac{2^{s-2}((p^{(v-1)/2}(p+1) - 2)s - 4)}{n}.$$

In particular, for $n = 2^s p^v$ we have

$$R \ge 1 - \delta - \frac{(p^{(v-1)/2}(p+1) - 2)s - 4}{4p^v}.$$

2. NOTATION AND LEMMAS

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

Lemma 1. *Let $f_1, f_2, \ldots, f_s \in F_q[x]$ be pairwise coprime square-free monic polynomials of the same degree $m \ge 3$ and Y be the fibre product in A^{s+1} given over $F_q[x]$ defined by the equations*

$$\begin{aligned} z_1^2 &= f_1(x), \\ z_2^2 &= f_2(x), \\ &\cdots \\ z_s^2 &= f_s(x). \end{aligned}$$

Then the genus $g = g(X)$ of the smooth projective model X of the curve Y is

$$g = \begin{cases} (ms - 3)2^{s-2} + 1 & \text{if } m \text{ is odd}, \\ (ms - 4)2^{s-2} + 1 & \text{if } m \text{ is even}. \end{cases}$$

Proof. Let I be the ideal of the curve Y in $\bar{F}_q[x, z_1 \ldots, z_s]$ and $\bar{Y}$ be the projective closure of Y in P^{s+1}. The homogeneous ideal of $\bar{Y}$ in $\bar{F}_q[x_0, x, z_1, \ldots, z_s]$ has the form $I_h = \{f_h \mid f \in I\}$, where f_h is the homogenization of f, i.e.,

$$f_h(x_0, x, z_1, \ldots, z_s) = f(x/x_0, z_1/x_0, \ldots, z_s/x_0)x_0^{\deg f}.$$

Thus, $\bar{Y} = Y \cup \{(0, 0, \pm 1, \pm 1, \ldots, \pm 1)\}$ as a set, and the curve $\bar{Y}$ is singular at the 2^{s-1} points $P_i \in \{(0, 0, 1, \pm 1, \ldots, \pm 1)\}$ in general.

Let X be a normalization of $\bar{Y}$ which in the same time is a non-singular model of $\bar{Y}$ (see, for example [3], Chapter 2, 5.3). There exists a finite morphism (regular map) $\varphi_1 : X \to \bar{Y}$ and a composition of φ_1 with φ_2, where $\varphi_2 : \bar{Y} \to P^1$ via $(x_0, x, z_1, \ldots, z_s) \mapsto (x_0, x)$ gives a morphism $\varphi : X \to P^1$ of degree 2^s (see, for example [3], Chapter 2, 3.1). Since $\bar{Y}$ has 2^{s-1} points P_i, $1 \le i \le 2^{s-1}$, at the hypersurface $x_0 = 0$, the set $\varphi^{-1}(0, 1)$ consists of 2^s or 2^{s-1} points $\{Q_i\} \subseteq X$.

Let $\Omega[\bar{Y}]$ be the space of regular differential forms on $\bar{Y}$. The space $\Omega[\bar{Y}]$, considered as a $\bar{F}_q[x, z_1, \ldots, z_s]$-module, is generated by dx and dz_i, $1 \le i \le s$. Since $z_i^2 = f_i(x)$, the space $\Omega[\bar{Y}]$, considered as a $\bar{F}_q[x]$-module, is generated by dx and $dx/(z_{i_1} \ldots z_{i_\sigma})$, where $1 \le i_1 < \ldots < i_\sigma \le s$. Next, since φ_1 is a morphism, the space $\Omega[X]$ is a submodule of $\Omega[\bar{Y}]$, hence any differential form $\omega \in \Omega[X]$ has one of the form

$$\omega = F(x)dx, \qquad \omega = \frac{F_{i_1, \ldots, i_\sigma}(x)dx}{z_{i_1} \ldots z_{i_\sigma}}$$

with $F, F_{i_1, \ldots, i_\sigma} \in \bar{F}_q[x]$. Thus, any regular differential form in $\Omega[\bar{Y}]$ is regular at any point of X, possibly except $Q_i \in \varphi^{-1}(0, 1)$.

Let x be the coordinate on P^1, then $u = x^{-1}$ is a local parameter at the point $(0, 1)$ at infinity. Since x is a rational function on P^1, it defines the divisor $(x) \in \mathrm{Div}(P^1)$. Denoting $\varphi^{-1}(x) \in \bar{F}_q(X)$ by x and its divisor by (x) again, we get the pull-back divisor $(x) \in \mathrm{Div}(X)$.

Since $\varphi^{-1}(0, 1)$ consists of 2^s or 2^{s-1} points Q_i, we have $v_{Q_i}(u) = 1$ or $v_{Q_i}(u) = 2$, therefore $v_{Q_i}(x) = -1$ or $v_{Q_i}(x) = -2$. If $F(x)$ is a regular function on X, we have $v_{Q_i}(F(x)dx) = -(\deg F(x) + 2)$ or $-(2 \deg F(x) + 3)$ respectively. Thus, $F(x)dx \notin \Omega[X]$ for any $F(x) \in \bar{F}_q[X]$.

If m is even, then there are two cases:

(1) $v_{Q_i}(x) = -1$ and $v_{Q_i}(z_j) = -m/2$ for any $j = 1, \ldots, s$,

(2) $v_{Q_i}(x) = -2$ and $v_{Q_i}(z_j) = -m$ for any $j = 1, \ldots, s$.

Since

$$v_{Q_i}\left(\frac{F_{i_1, \ldots, i_\sigma}(x)dx}{z_{i_1} \ldots z_{i_\sigma}}\right) = v_{Q_i}(x) \deg F_{i_1, \ldots, i_\sigma}(x) + (v_{Q_i}(x) - 1) - \sigma v_{Q_i}(z_j)$$

for any $j = 1, \ldots, s$, we have

$$v_{Q_i}\left(\frac{F_{i_1, \ldots, i_\sigma}(x)dx}{z_{i_1} \ldots z_{i_\sigma}}\right) = \frac{m\sigma}{2} - \deg F_{i_1, \ldots, i_\sigma}(x) - 2,$$

or

$$v_{Q_i}\left(\frac{F_{i_1,\dots,i_\sigma}(x)dx}{z_{i_1}\dots z_{i_\sigma}}\right) = m\sigma - 2\deg F_{i_1,\dots,i_\sigma}(x) - 3$$

respectively. Thus,

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

if and only if

$$\deg F_{i_1,\dots,i_\sigma}(x) \le \frac{m\sigma}{2} - 2,$$

or

$$\deg F_{i_1,\dots,i_\sigma}(x) \le \frac{m\sigma}{2} - \frac{3}{2}$$

respectively. Since m is even the second inequality is equivalent to the first one.

If m is odd and $v_{Q_i}(x) = -1$, then $v_{Q_i}(z_j^2) = 2v_{Q_i}(z_j) = -m$ and we arrive at a contradiction. Thus, only one case is possible, where $v_{Q_i}(x) = -2$. In this case,

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

if only

$$\deg F_{i_1,\dots,i_\sigma}(x) \le \begin{cases} (m\sigma - 4)/2 & \text{if } \sigma \text{ is even,} \\ (m\sigma - 3)/2 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Since X is non-singular, we have

$$g = \dim_{F_q} \Omega[X].$$

Thus, if m is even, then

$$g = \frac{1}{2}\sum_{\sigma=1}^{s} \sum_{1\le i_1<i_2,\dots<i_\sigma\le s} (m\sigma - 2) = (ms - 4)2^{s-2} + 1,$$

and if m is odd, then

$$\begin{aligned} g &= \frac{1}{2}\sum_{\sigma=1}^{s} \sum_{1\le i_1<i_2,\dots<i_\sigma\le s} (m\sigma - 2) + \frac{1}{2}\sum_{\sigma=1}^{s} \sum_{1\le i_1<i_2,\dots<i_\sigma\le s} (m\sigma - 1) \\ &= (ms - 3)2^{s-2} + 1, \end{aligned}$$

where the summation is taken over odd σ only.

This completes the proof.

Lemma 2. *Let $v > 1$ be an odd number, F_q be a finite field of characteristic $p > 2$ with $q = p^v$ elements, and let $f \in F_q[x]$ be the polynomial*

$$f(x) = (x + x^{p^{(v-1)/2}})(x + x^{p^{(v+1)/2}}).$$

If c is a non-zero element of F_q, then the polynomials $f(x)$ and $f(x + c)$ are relatively prime.

Proof. Let $\mu = (\nu - 1)/2$ and $f'(x) = x^{p^\mu} + x, f''(x) = x^{p^{\mu+1}} + x$ so that $f'(x)f''(x) = f(x)$. We shall prove that $(f'(x), f'(x+c)) = (1)$ and $(f'(x), f''(x+c)) = (1)$ for any $c \in F_{p^\nu}^*$. This will imply that $(f(x), f(x+c)) = (1)$ for any $c \in F_{p^\nu}^*$.

Observe that the principal ideal I' generated by $f'(x)$ and $f'(x+c)$ is equal to

$$I' = (x^{p^\mu} + x, x^{p^\mu} + x + c^{p^\mu} + c).$$

The equation

$$\alpha^{p^\mu} + \alpha = 0 \tag{1}$$

has no solution in $F_{p^\nu}^*$. Otherwise $\alpha^{p^\mu - 1} = -1$. Then $\alpha^{p^{2\mu}-1} = 1$, since p is odd and hence $2 \mid (p^\mu + 1)$. Thus, $\alpha \in F_{p^{\gcd(2\mu+1, 2\mu)}} = F_p$. This implies that $\alpha^{p^\mu - 1} = 1 \neq -1$, and we obtain a contradiction.

Observe (using the Euclidean algorithm) that if k, l, $k \geq l$, are positive integers and $c \in F_{p^\nu}$, then the principal ideal $(x^k + x + c, x^l + x)$ in $F_{p^\nu}[x]$ satisfies the relation

$$(x^k + x + c, x^l + x) = (x^l + x, -x^{k-l+1} + x + c).$$

Similarly,

$$(-x^k + x + c, x^l + x) = (x^l + x, x^{k-l+1} + x + c).$$

Combining these relations, we find that if $k \geq 2l - 1$ and k, l are positive integers, then

$$(x^k + x + c, x^l + x) = (x^l + x, x^{k-2l+2} + x + c).$$

By induction, if $l \mid k$ and $c \in F_{p^\nu}^*$, then

$$(x^k + x + c, x^l + x) = (x^l + x, (-1)^{k/l} x^{k/l} + x + c).$$

Applying this relation for $k = p^{\mu+1}$ and $l = p^\mu$, we find for the ideal $I'' = (f''(x+c), f'(x))$ that

$$I'' = (x^{p^\mu} + x, -x^p + x + c^{p^{\mu+1}} + c).$$

Now we observe that $(g'(x), g''(x)) \supset (g'(x), (g''(x))^p)$ for any $h', h'' \in F_{p^\nu}[x]$. Therefore

$$I'' \supset J = (x^{p^\mu} + x, -x^{p^{\mu+1}} + x^{p^\mu} + \gamma^{p^{\mu+1}} + \gamma)$$

where $\gamma = c^{p^\mu}$. We can simplify the generators of J as

$$\begin{aligned} J &= (x^{p^\mu} + x, -x^{p^{\mu+1}} - x + \gamma^{p^{\mu+1}} + \gamma) \\ &= (x^{p^\mu} + x, x^{p^{\mu+1}} + x - \gamma^{p^{\mu+1}} - \gamma). \end{aligned}$$

Let us show that

$$c^{p^{\mu+1}} + c \neq -\gamma^{p^{\mu+1}} - \gamma. \tag{2}$$

Since $\gamma = c^{p^\mu}$ and $c^{p^\nu} = c \in F_{p^\nu}^*$, we can rewrite the inequality (2) in the form

$$c^{p^{\mu+1}} + c^{p^\mu} + 2c \neq 0. \tag{3}$$

The equation

$$\beta^{p^{\mu+1}} + \beta^{p^\mu} + 2\beta = 0 \tag{4}$$

has no solution in $F_{p^\nu}^*$. Indeed, raising both sides of (4) to the p^μth power, we obtain

$$\beta + \beta^{p^{2\mu}} + \beta^{p^\mu} + \beta^{p^\mu} = (\beta^{p^\mu} + \beta)^{p^\mu} + (\beta^{p^\mu} + \beta) = 0. \tag{5}$$

Since (1) has no non-zero solution, the last equation also has no solution in $F_{p^\nu}^*$.

Now since $f''(x + c) = x^{p^{\mu+1}} + x + c^{p^{\mu+1}} + c \in I''$, $x^{p^{\mu+1}} + x - \gamma^{p^{\mu+1}} - \gamma \in J \subseteq I''$, and

$$c^{p^{\mu+1}} + c \neq -\gamma^{p^{\mu+1}} - \gamma,$$

we conclude that $I'' = (1)$.

By symmetry $(f''(x), f''(x+c)) = (1)$, and $(f''(x), f'(x+c)) = (1)$. Using the uniqueness of factorization in $F_{p^\nu}[x]$, we find that

$$(f'(x), f'(x + c)f''(x + c)) = (1), \qquad (f''(x), f'(x + c)f''(x + c)) = (1),$$

and hence $(f(x), f(x + c)) = (1)$.

Let $\theta\colon F_q \to F_q$ be the Frobenius automorphism of F_q over F_p, namely, $\theta(x) = x^p$. Let χ be a multiplicative character of F_p. We denote by χ_ν the character of F_q induced by χ:

$$\chi_\nu(x) = \chi(\mathrm{norm}_\nu(x)), \qquad x \in F_q,$$

where

$$\mathrm{norm}_\nu(x) = x\theta(x)\ldots\theta^{\nu-1}(x) = xx^p\ldots x^{p^{\nu-1}}.$$

It is easy to see that if p and ν are odd numbers, χ_ν is induced by a non-trivial quadratic character of F_p, and $f(x) = (x + x^{p^{(\nu-1)/2}})(x + x^{p^{(\nu+1)/2}})$, then (see [1], Lemma 2)

$$\chi_\nu(f(x)) = \begin{cases} 1 & \text{if } x \in F_q^*, \\ 0 & \text{if } x = 0. \end{cases}$$

Let

$$\tilde{f}(x) = \frac{f(x)}{x^2} = (1 + x^{p^{(\nu-1)/2}-1})(1 + x^{p^{(\nu+1)/2}-1}).$$

Then $\chi_\nu(\tilde{f}(x)) = 1$ for all $x \in F_q$, and we have the following result.

Lemma 3. *Let $v > 1$ be an odd integer, F_q be a finite field of characteristic $p > 2$ with $q = p^v$ elements, $c_1, \ldots, c_s$ be distinct elements of F_q, and let N_q be the number of F_q-rational points of the affine curve Y defined by the equations*

$$z_1^2 = f_1(x) = \tilde{f}(x + c_1),$$
$$z_2^2 = f_2(x) = \tilde{f}(x + c_2),$$
$$\ldots$$
$$z_s^2 = f_s(x) = \tilde{f}(x + c_s).$$

Then

$$N_q = 2^s q.$$

Proof. Since $\chi_v(f_i(x)) = \chi_v(\tilde{f}(x + c_i)) = 1$ for all $x \in F_{p^v}$, $i = 1, \ldots, s$, we have

$$N_q = \sum_{x \in F_{p^v}} (1 + \chi_v(f_1(x)))\ldots(1 + \chi_v(f_s(x)))$$
$$= \sum_{x \in F_{p^v}} 2^s = 2^s p^v.$$

3. PROOF OF THE THEOREM

We consider the affine curve

$$Y: \quad z_i^2 = f_i(x) = \tilde{f}(x + c_i), \qquad 1 \le i \le s,$$

where $c_1, \ldots, c_s$ are distinct elements of F_q. The number of F_q-rational points of Y is $N_q = 2^s q$ by Lemma 3. The curve Y satisfies the conditions of Lemma 1, so the genus $g = g(X)$ of its smooth projective model X is

$$g = 2^{s-2}((p^{(v-1)/2}(p + 1) - 2)s - 4) + 1.$$

Let S be the set of rational points on 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_∞ is the point of X corresponding to the point at infinity of the projectivization $\bar{Y}$ of the affine curve Y, we get $r < n \le 2^s p^v$, $k \ge r + 1 - g$, $d \ge n - r$. Since in our case $2g - 2 < r = \deg D < n$, we obtain $k = r + 1 - g$.

REFERENCES

1. S. A. Stepanov, Codes on fibre products of hyperelliptic curves. *Discrete Math. Appl.* (1997) **7**, 77–88.
2. V. G. Goppa, Codes on algebraic curves, *Soviet Math. Dokl.* (1981) **24**, 170-172.
3. I. R. Shafarevich, *Basic Algebraic Geometry.* Springer, Berlin, 1994.