Discrete Math. Appl., Vol. 7, No. 1, pp. 77–88 (1997)

Codes on fibre products of hyperelliptic curves*

S. A. STEPANOV

Abstract — The purpose of this paper is to construct a new family of smooth projective curves over a finite field F_q with a lot of F_q-rational points. The genus in this family is considerably less than the number of rational points, so that the corresponding geometric Goppa codes have rather good parameters.

The work was supported by Bilkent University, 06533 Bilkent, Ankara, Turkey.

1. INTRODUCTION

Let X be a smooth projective curve of genus $g = g(X)$ defined over a finite field $k' = F_q$. Recall the basic ideas of the Goppa construction [3] of the linear $[n, k, d]_q$ -codes associated with the curve X. Let $\{x_1, \ldots, x_n\}$ be the set of k'-rational points of X and

$$D_0 = x_1 + \ldots + x_n.$$

Let D be a k'-rational divisor on X. We assume that D has the support disjoint from D_0, i.e., the points x_i, $i = 1, \ldots, n$, occur with multiplicity zero in D. Denote by $k'(X)$ the field of rational functions on X and consider the vector space over k'

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

The linear $[n, k, d]_q$-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 injection, so that $C \simeq L(D)$.

Dually, denote by $\Omega(X)$ the $k'(X)$-vector space of rational differential forms on X and consider the linear space over k'

$$\Omega(D_0 - D) = \{\omega \in \Omega(X)^* \mid (\omega) + D_0 - D \geq 0\} \cup \{0\}.$$

The linear map

$$\mathrm{Res}\colon \Omega(D_0 - D) \to F_q^n, \qquad \omega \mapsto (\mathrm{Res}_{x_1}(\omega), \ldots, \mathrm{Res}_{x_n}(\omega))$$

*UDC 519.72. Originally published in *Diskretnaya Matematika* (1997) **9**, No. 1, 83–94 (in Russian). Received May 12, 1996. Translated by the author.

defines the linear $[n,k,d]_q$-code $C^* = C^*(D_0,D)$ associated with the pair (D_0,D). If $\deg D > 2g-2$, then the map Res is injective, so that $C^* \simeq \Omega(D_0-D) \simeq L(K+D_0-D)$, where K is a canonical divisor on X.

Each linear $[n,k,d]_q$-code C defines a pair of its relative parameters (δ,R), where $\delta = d/n$ is the relative minimum distance and R is the transmission rate of C. The points (δ,R) form the set of code points $V_q^{\mathrm{lin}} \subseteq [0,1]^2$. Let U_q^{lin} denote the subset of limit points of V_q^{lin}. In other terms, $(\delta,R) \in U_q^{\mathrm{lin}}$ if and only if there exists an infinite sequence of different linear codes C_i with relative parameters $\delta_i = \delta(C_i)$ and $R_i = R(C_i)$ such that

$$\lim_{i\to\infty}(\delta_i,R_i) = (\delta,R).$$

If $\delta > 0$ and $R > 0$, then such a family of codes C_i is called asymptotically good. The structure of U_q^{lin} can be described as follows (see [1, 4]): there exists a continuous function $\alpha_q^{\mathrm{lin}}(\delta)$ such that

$$U_q^{\mathrm{lin}} = \{(\delta,R) \mid 0 \le R \le \alpha_q^{\mathrm{lin}}(\delta)\},$$

moreover, $\alpha_q^{\mathrm{lin}}(0) = 1$, $\alpha_q^{\mathrm{lin}}(\delta) = 0$ for $(q-1)/q \le \delta \le 1$, and $\alpha_q^{\mathrm{lin}}(\delta)$ decreases on the interval $[0,(q-1)/q]$.

It follows from the Riemann–Roch theorem that the relative parameters $R = k/n$ and $\delta = d/n$ both for L- and Ω-constructions satisfy (see [8, 10]) the inequality

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

In order to produce a family of asymptotically good geometric Goppa codes for which $R+\delta$ comes above the Gilbert-Varshamov bound

$$\alpha_q^{\mathrm{lin}}(\delta) \ge 1 - H_q(\delta),$$

where

$$H_q(\delta) = \delta\log_q(q-1) - \delta\log_q\delta - (1-\delta)\log_q(1-\delta),$$

one needs a family of smooth projective curves with a lot of k'-rational points compared to the genus. Examples of such families are provided by classical modular curves $X_0(N)$ and $X(N)$ (see [5, 9]), or by Drinfeld modular curves (see [10], Chapters 4.1 and 4.2). Thus, if $q = p^\nu$ is an even power of a prime number p, then there exists an infinite sequence of geometric Goppa codes C_i which gives the lower bound

$$\alpha_q^{\mathrm{lin}} \ge 1 - \delta - (\sqrt{q}-1)^{-1}.$$

The line $R = 1 - \delta - (\sqrt{q}-1)^{-1}$ intersects the curve $R = 1 - H_q(\delta)$ for $q \ge 49$. Much easier proof of this result based on consideration of a sequence of (modified) Artin–Schreier coverings of the projective line $P^1(\bar{k}')$ was recently proposed by Garcia and Stichtenoth [2].

In this paper we consider a new family of smooth projective curves X_s given over $k' = F_q$ by equations

$$z_i^2 = f_i(u), \qquad 1 \le i \le s, \tag{2}$$

where $f_i(u)$ are relatively prime square-free polynomials in $k'[u]$ of a special form. Every such curve is actually a fibre product of hyperelliptic curves. The main point of the paper is to calculate the genus $g(X_s)$ (Lemma 1) and determine the number $N_q(X_s)$ of k'-rational points (Lemma 4) on the curve X_s. We show that the ratio $g(X_s)/N_q(X_s)$ is small enough and deduce from (1) that the corresponding geometric Goppa codes $C(D, D_0)$ and $C^*(D, D_0)$ have rather good parameters. For small values of s, these parameters are comparable with the parameters of codes on Artin–Schreier coverings introduced by Garcia and Stichtenoth [2]. In particular, if $s = 1$, then the codes $C(D, D_0)$ and $C^*(D, D_0)$ have the same parameters as the codes on Hermitian curves (see [8], Section VII.3). Unfortunately, the parameter s in our construction is bounded by $q^{1/2}$ and as a result the genus $g(X_s)$ is bounded by

$$(q - 3)2^{(q^{1/2}-2)} + 1.$$

However, since the above upper bound is large enough for $q \ge q_0$, the curves X_s provide sufficiently long geometric Goppa codes.

A similar construction of non-singular projective curves with a lot of k'-rational points based on the use of fibre products of some Artin–Schreier curves was independently considered by van der Geer and van der Vlugt [11].

The genus $g(X_s)$ can be easily calculated using the Hurwitz genus formula. However, we prefer to use a slightly more complicated argument which allows us to find explicitly a basis of the space $\Omega(D_0 - D)$. This provides an easy way to write out the generator matrices for codes in the family and to find a fast decoding algorithm.

Applying to curves X_s the Goppa constructions, we obtain the following results.

Theorem 1. *Let $p > 2$ be a prime number, $v > 1$ be an even integer, and let F_q be a finite field consisting of $q = p^v$ elements. For any positive integers $s \le q^{1/2}$ and $l > (sq^{1/2} - 3)2^{s-2}$ there exists a geometric Goppa $[n, k, d]_q$-code $C = C(D_0, D)$ with parameters*

$$\begin{aligned} &l < n \le (2q^{1/2} - s)q^{1/2}2^{s-1}, \\ &k \ge l - (sq^{1/2} - 3)2^{s-2}, \\ &d \ge n - l. \end{aligned}$$

Theorem 2. *For p, q and s as in Theorem 1, and for any positive integer $l > (sq^{1/2} - 3)2^{s-1}$ there exists a geometric Goppa $[n, k, d]_q$-code $C^* = C^*(D_0, D)$ with parameters*

$$\begin{aligned} l - (sq^{1/2} - 3)2^{s-2} < n &\le (2q^{1/2} - s)q^{1/2}2^{s-1}, \\ k &\ge n - l + (sq^{1/2} - 3)2^{s-2}, \\ d &\ge l - (sq^{1/2} - 3)2^{s-1}. \end{aligned}$$

Corollary 1. *The relative parameters $R = k/n$ and $\delta = d/n$ of the above codes satisfy the inequality*

$$R \geq 1 - \delta - \frac{(sq^{1/2} - 3)2^{s-2}}{n}.$$

In particular, for $n = (2q^{1/2} - s)q^{1/2}2^{s-1}$

$$R \geq 1 - \delta - \frac{sq^{1/2} - 3}{2(2q^{1/2} - s)q^{1/2}}.$$

By a suitable concatenation one gets reasonably good codes over F_p. Indeed, let $k_0 > 1$ be an even number. Applying a linear $[n_0, k_0, d_0]_p$-code C_0 to an $[n, k, d]_q$-code $C = C(D_0, D)$ over F_q, where $q = p^{k_0}$, we obtain an $[n', k', d']_p$-code C' with parameters

$$n' = n_0 n, \quad k' = k_0 k, \quad d' = d_0 d.$$

Let us denote by $R_0 = k_0/n_0$ and $\delta_0 = d_0/n_0$ the relative parameters of the code C_0.

Corollary 2. *For any positive integers $n_0 > 1$, $s \leq q^{1/2}$ and $l > (sq^{1/2} - 3)2^{s-2}$ there exists a linear $[n', k', d']_p$-code C' with parameters*

$$\begin{aligned} n_0 l < n' = n_0 n &\leq n_0(2q^{1/2} - s)q^{1/2}2^{s-1}, \\ k' &\geq k_0(l - (sq^{1/2} - 3)2^{s-2}), \\ d' &\geq d_0(n - l). \end{aligned}$$

The relative parameters $R' = k'/n'$ and $\delta' = d'/n'$ of the code C' satisfy the inequality

$$R' + \delta' \geq R_0\left(\frac{l}{n} - \frac{(sq^{1/2} - 3)2^{s-2}}{n}\right) + \delta_0\left(1 - \frac{l}{n}\right).$$

Applying a linear $[n_0, k_0, d_0]_p$-code C_0 to a linear $[n, k, d]_q$-code $C^* = C_*(D_0, D)$, we obtain the following result.

Corollary 3. *For any positive integers $n_0 > 1$, $s \leq q^{1/2}$ and $l > (sq^{1/2} - 3)2^{s-2}$ there exists a linear $[n'', k'', d'']_p$-code C'' with parameters*

$$\begin{aligned} n_0(l - (sq^{1/2} - 3) < n'' = n_0 n &\leq n_0(2q^{1/2} - s)q^{1/2}2^{s-1}, \\ k'' &\geq k_0(n - l + (sq^{1/2} - 3)2^{s-2}), \\ d'' &\leq d_0(l - (sq^{1/2} - 3)2^{s-1}). \end{aligned}$$

The relative parameters $R'' = k''/n''$ and $\delta'' = d''/n''$ of the code C'' satisfy the inequality

$$R'' + \delta'' \geq R_0\left(1 - \frac{l}{n} + \frac{(sq^{1/2} - 3)2^{s-2}}{n}\right) + \delta_0\left(\frac{l}{n} - \frac{(sq^{1/2} - 3)2^{s-1}}{n}\right).$$

The results of this paper can be extended to the case of fibre products of more general form over an arbitrary finite field.

2. NOTATION AND LEMMAS

Let k'' be the algebraic closure of $k' = F_q$ and A^{s+1} be an $(s+1)$-dimensional affine space over k''. Assume that $\operatorname{char} k' > 2$.

Lemma 1. *Let $f_1, \ldots, f_s$ be pairwise coprime square-free monic polynomials in $k'[u]$ of the same odd degree $m \geq 1$ and Y be the fibre product in A^{s+1} given over k' by the equations*

$$z_i^2 = f_i(u), \qquad 1 \leq i \leq s. \tag{3}$$

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

$$g = (ms - 3)2^{s-2} + 1.$$

Proof. Let X be a smooth projective model of the curve Y. Denote by v_x the canonical valuation of the function field $k''(X)$, and by $\Omega[X]$ the space of regular differential forms on X. The affine curve Y is easily seen to be smooth. If $\bar{Y}$ is its projective closure, then X is a normalization of $\bar{Y}$ and we have the map $\psi\colon X \to \bar{Y}$ which is an isomorphism between Y and $\psi^{-1}(\bar{Y})$. Hence it follows that $g = g(X) = g(Y)$.

The rational map $(u, z_1, \ldots, z_s) \mapsto u$ of the curve Y in A^1 determines a morphism $\varphi\colon X \to P^1$ of degree 2^s, so that for $u_0 \in A^1$ either $\varphi^{-1}(u_0)$ consists of 2^s points of the form $x' = (u_0, \pm z_1, \ldots, \pm z_s)$ at each of which $v_{x'}(t) = 1$ for the local parameter t at u_0, or else $\varphi^{-1}(u_0)$ consists of 2^{s-1} points of the form $x_i'' = (u_0, \pm z_1, \ldots \pm z_{i-1}, 0, \pm z_{i+1}, \ldots, \pm z_s)$, and $v_{x_i''}(t) = 2$.

Let us consider the point at infinity $u_\infty \in P^1$. If the coordinate on A^1 is denoted by u, then $t = u^{-1}$ is the local parameter at u_∞. If $\varphi^{-1}(u_\infty)$ consisted of 2^s points $x_\infty^{(\tau)}$, then at each $x_\infty = x_\infty^{(\tau)}$ the function t would be the local parameter. Hence it would follow that $v_{x_\infty}(t) = 1$ and $v_{x_\infty}(f_i(t)) = -m$. But since m is odd, this contradicts the condition that $v_{x_\infty}(f_i(u)) = 2v_{x_\infty}(z_i)$. Thus, $\varphi^{-1}(u_\infty)$ consists of $r = 2^{s-1}$ points $x_\infty^{(\tau)}$, $1 \leq \tau \leq r$, with the projective coordinates $x_\infty^{(\tau)} = (0, 1, \pm 1, \ldots, \pm 1, 0)$. It follows that $X = Y \cup \{x_\infty^{(1)}\} \cup \ldots \cup \{x_\infty^{(r)}\}$. At any such point $x_\infty = x_\infty^{(\tau)}$ we have $v_{x_\infty}(u) = -2$ and $v_{x_\infty}(z_i) = -m$.

Let us now find a basis of the space $\Omega[X]$ over the field k''. Any element $\omega \in \Omega[Y]$ can be written as a k''-linear combination of the differential forms $\omega_0 = P_0(u)du$ and

$$\omega_{i_1,\ldots,i_\sigma} = \frac{P_{i_1,\ldots,i_\sigma}(u)du}{z_{i_1}\ldots z_{i_\sigma}},$$

where $i_1, \ldots, i_\sigma$ are integers such that $1 \leq i_1 < \ldots < i_\sigma \leq s$ and $P_{i_1,\ldots,i_\sigma}$ are polynomials in $k''[u]$. Indeed, the differential form

$$\omega'_{i_1,\ldots,i_\sigma} = \frac{du}{z_{i_1}\ldots z_{i_\sigma}}$$

is regular at any point $u_0 \in A^1$ with the condition $z_i(u_0) \neq 0$ for $i \in \{i_1, \ldots, i_\sigma\}$. Now if $z_i(u_0) = 0$ for an unique $i \in \{i_1, \ldots, i_\sigma\}$, then z_i is the local parameter at

$x_i'' = (u_0, \pm z_1, \ldots, \pm z_{i-1}, 0, \pm z_{i+1}, \ldots, \pm z_s)$, so that $v_{x_i''}(z_i) = 1$ and $v_{x_i''}(u - u_0) = 2$. Therefore $v_{x_i''}(du) = 1$ and again $\omega'_{i_1,\ldots,i_\sigma}$ is regular at u_0. The form $\omega'_0 = du$ is also regular at any point $u_0 \in A^1$. Thus, the differential forms $\omega'_0 = du$ and $\omega'_{i_1,\ldots,i_\sigma}$ form a basis of the $k''[u]$-module $\Omega[Y]$.

It remains to clarify which of the forms ω_0 and $\omega_{i_1,\ldots,i_\sigma}$ are regular at the points $x_\infty^{(1)}, \ldots, x_\infty^{(r)}$. Let x_∞ be one of these points. If t is the local parameter at x_∞, then $u = t^{-2}u'$, $z_i = t^{-m}z_i'$, where u' and z_i' are units in the local ring O_{x_∞}. Therefore $\omega'_{i_1,\ldots,i_\sigma} = t^{m\sigma-3}\eta_{i_1,\ldots,i_\sigma}dt$, where $\eta_{i_1,\ldots,i_\sigma}$ is a unit in O_{x_∞}, hence $(\omega'_{i_1,\ldots,i_\sigma}) = (m\sigma - 3)x_\infty$. Thus, the differential form

$$\omega_{i_1,\ldots,i_\sigma} = \frac{P_{i_1,\ldots,i_\sigma}(u)du}{z_{i_1}\ldots z_{i_\sigma}}$$

is regular at x_∞ if and only if

$$v_{x_\infty}(P_{i_1,\ldots,i_\sigma}(u)) \geq -(m\sigma - 3).$$

This means that $\deg P_{i_1,\ldots,i_\sigma}(u) \leq (m\sigma - 3)/2$ and hence

$$\deg P_{i_1,\ldots,i_\sigma}(u) \leq \begin{cases} (m\sigma - 4)/2, & \text{if } \sigma \equiv 0 \pmod 2, \\ (m\sigma - 3)/2, & \text{if } \sigma \equiv 1 \pmod 2. \end{cases}$$

The differential form $\omega_0 = P_0 du$ is not regular at x_∞ for any non-zero polynomial $P_0 \in k''[u]$, therefore the regular differential forms

$$\omega'_{i_1,\ldots,i_\sigma}, \quad u\omega'_{i_1,\ldots,i_\sigma}, \quad \ldots, u^n\omega'_{i_1,\ldots,i_\sigma},$$

where $1 \leq i_1 < \ldots < i_\sigma \leq s$ and

$$n = \begin{cases} (m\sigma - 4)/2, & \text{if } \sigma \equiv 0 \pmod 2 \\ (m\sigma - 3)/2, & \text{if } \sigma \equiv 1 \pmod 2, \end{cases}$$

form a basis of the space $\Omega[X]$ over k''. Therefore

$$\begin{aligned} \dim_{k''} \Omega[X] &= \frac{1}{2} \sum_{\sigma \equiv 0 \pmod 2} \sum_{1 \leq i_1 < \ldots < i_\sigma \leq s} (m\sigma - 2) + \frac{1}{2} \sum_{\sigma \equiv 1 \pmod 2} \sum_{1 \leq i_1 < \ldots < i_\sigma \leq s} (m\sigma - 1) \\ &= \frac{m}{2} \sum_{\sigma=1}^{s} \sigma \binom{s}{\sigma} - \sum_{\sigma \equiv 0 \pmod 2} \binom{s}{\sigma} - \frac{1}{2} \sum_{\sigma \equiv 1 \pmod 2} \binom{s}{\sigma} \\ &= \frac{1}{2}(ms2^{s-1} - 2^s - 2^{s-1} + 2) \end{aligned}$$

and hence

$$g = g(X) = \dim_{k''} \Omega[X] = (ms - 3)2^{s-2} + 1.$$

This completes the proof.

Let p be a prime number, v be a positive integer and let F_q be a finite field with $q = p^v$ elements. The field F_q is a Galois extension of the prime finite field F_p of degree v with the cyclic Galois group of order v. The action of a generator θ of this group on an element $x \in F_q$ is given by the rule $\theta(x) = x^p$. The map

$$\mathrm{norm}_v(x) = x\theta(x)\ldots\theta^{v-1}(x) = xx^p\ldots x^{p^{v-1}}$$

of F_q onto F_p is the norm of the element x.

Let χ be a multiplicative character of the field F_p and x an element of F_q. Set

$$\chi_v(x) = \chi(\mathrm{norm}_v(x))$$

and call χ_v a multiplicative character of the field F_q induced by the character χ.

Now let f be a square-free polynomial in the ring $F_q[u]$ of degree m and let χ be a non-trivial quadratic character of F_p. Consider the character sum

$$S_v(f) = \sum_{u\in F_q} \chi_v(f(u)) = \sum_{u\in F_q} \chi(\mathrm{norm}_v(f(u)))$$

and recall the well-known Weil bound [12] (see also [7], Chapters 1 and 5)

$$|\, S_v(f)\,| \leq 2\left[\frac{m-1}{2}\right] q^{1/2}.$$

The following result of the author (see [6], Theorem 3) shows us that the Weil bound cannot be sharpened essentially in any extension F_q of the field F_p.

Lemma 2. *Let F_q be a finite field with $q = p^v$ elements of characteristic $p > 2$ and let χ_v be the character of F_q induced by a non-trivial quadratic character χ of the field F_p. If $v > 1$, then for the square-free polynomial $f \in F_p[u]$,*

$$f(u) = \begin{cases} u + u^{p^{v/2}}, & \text{if } v \equiv 0 \pmod 2, \\ (u + u^{p^{(v-1)/2}})(u + u^{p^{(v+1)/2}}), & \text{if } v \equiv 1 \pmod 2, \end{cases}$$

we have

$$\sum_{u\in F_q} \chi_v(f(u)) = \begin{cases} (q^{1/2} - 1)q^{1/2} & \text{if } v \equiv 0 \pmod 2, \\ q - 1 & \text{if } v \equiv 1 \pmod 2. \end{cases}$$

Proof. Let $v > 1$ be an even number. Since $u^{p^v} = u$ in F_q, for any $u \in F_q$ we have

$$\begin{aligned} \mathrm{norm}_v(f(u)) &= \prod_{i=1}^{v} (u + u^{p^{v/2}})^{p^{i-1}} = \prod_{i=1}^{v} (u^{p^{i-1}} + u^{p^{v/2+i-1}}) \\ &= \prod_{i=1}^{v/2} (u^{p^{i-1}} + u^{p^{v/2+i-1}}) \prod_{j=1}^{v/2} (u^{p^{v/2+j-1}} + u^{p^{j-1}}) \\ &= \prod_{i=1}^{v/2} (u^{p^{i-1}} + u^{p^{v/2+i-1}})^2. \end{aligned}$$

Therefore

$$\sum_{u\in F_q}\chi_v(f(u)) = \sum_{u\in F_q}\chi(\mathrm{norm}_v(f(u))) = q - N,$$

where N is the number of elements of the set $A = \{u \in F_q \mid f(u) = 0\}$. Since $f(u) = u(1 + u^{p^{v/2}-1})$, we have $A = \{0\} \cup B$, where

$$B = \{u \in F_q \mid 1 + u^{p^{v/2}-1} = 0\}$$

is the set of roots of the polynomial $1 + u^{p^{v/2}-1}$ in F_q. Taking into account that the greatest common divisor of $(p^{v/2} - 1$ and $p^v - 1)$ is equal to $p^{v/2} - 1$, we obtain from the Euler criterion that the number of roots of the polynomial $1 + u^{p^{v/2}-1}$ is equal to $p^{v/2} - 1$. In that case

$$N = |A| = 1 + |B| = 1 + (p^{v/2} - 1) = q^{1/2},$$

and hence

$$\sum_{u\in F_q}\chi_v(f(u)) = (q^{1/2} - 1)q^{1/2}.$$

This proves the lemma for v an even positive integer.

Let now $v > 1$ be an odd number. In this case for any $u \in F_q$

$$\begin{aligned}
\mathrm{norm}_v(f(u)) &= \prod_{i=1}^{v}(u^{p^{i-1}} + u^{p^{(v-1)/2+i-1}})(u^{p^{i-1}} + u^{p^{(v+1)/2+i-1}}) \\
&= \prod_{i=1}^{(v-1)/2}(u^{p^{i-1}} + u^{p^{(v-1)/2+i-1}}) \prod_{i=(v+1)/2}^{v}(u^{p^{i-1}} + u^{p^{(v+1)/2+i-1}}) \\
&\times \prod_{i=1}^{(v-1)/2}(u^{p^{i-1}} + u^{p^{(v+1)/2+i-1}}) \prod_{i=(v+1)/2}^{v}(u^{p^{i-1}} + u^{p^{(v+1)/2+i-1}}) \\
&= \prod_{i=1}^{(v+1)/2}(u^{p^{i-1}} + u^{p^{(v-1)/2+i-1}}) \prod_{j=1}^{(v-1)/2}(u^{p^{(v+1)/2+j-1}} + u^{p^{j-1}}) \\
&\times \prod_{i=1}^{(v-1)/2}(u^{p^{i-1}} + u^{p^{(v+1)/2+i-1}}) \prod_{j=1}^{(v+1)/2}(u^{p^{(v-1)/2+j-1}} + u^{p^{j-1}}) \\
&= \prod_{i=1}^{(v+1)/2}(u^{p^{i-1}} + u^{p^{(v-1)/2+i-1}})^2 \prod_{i=1}^{(v-1)/2}(u^{p^{i-1}} + u^{p^{(v+1)/2+i-1}})^2
\end{aligned}$$

and hence

$$\sum_{u\in F_q}\chi_v(f(u)) = \sum_{u\in F_q}\chi(\mathrm{norm}_v(f(u))) = q - N',$$

where N' is the cardinality of the set $A = \{u \in F_q \mid f(u) = 0\}$. Clearly, $N' = 1$ and therefore

$$\sum_{u\in F_q}\chi_v(f(u)) = q - 1.$$

This completes the proof.

Lemma 3. *Let F_p be a prime finite field of characteristic $p > 2$, $F_q = F_{p^v}$ be an extension of F_p of even degree $v > 1$ and let A be the set of roots in F_q of the polynomial*

$$f(u) = u + u^{p^{v/2}}.$$

Then

(i) *A is a subgroup of the additive group F_q^+ of the field F_q;*

(ii) *if $\{A_1 = A, A_2, \ldots, A_r\}$ is the set of all cosets in F_q^+/A and $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ are distinct representatives of the cosets, then the polynomials*

$$f_i(u) = (u + \alpha_i) + (u + \alpha_i)^{p^{v/2}}, \qquad 1 \le i \le r, \tag{4}$$

are pairwise coprime in $F_q[u]$;

(iii) $r = |F_q^+/A| = p^{v/2}$.

Proof. The main point is (i). First of all we note that $f(0) = 0$. Now if α and β are zeros of $f(u)$, then

$$\begin{aligned} f(\alpha + \beta) &= (\alpha + \beta) + (\alpha + \beta)^{p^{v/2}} = \alpha + \alpha^{p^{v/2}} + (\beta + \beta^{p^{v/2}}) \\ &= f(\alpha) + f(\beta) = 0, \end{aligned}$$

so that $\alpha + \beta$ is also a root of the polynomial $f(u)$. Thus, A is a subgroup of F_q^+.

To prove (ii), let us suppose that $f_i(u)$ and $f_j(u)$ for $i \neq j$ have a common root in F_q, say $u = \theta$. In that case

$$\theta + \alpha_i + (\theta + \alpha_i)^{p^{v/2}} = \theta + \alpha_j + (\theta + \alpha_j)^{p^{v/2}}$$

and therefore

$$\theta + \alpha_i + \theta^{p^{v/2}} + \alpha_i^{p^{v/2}} = \theta + \alpha_j + \theta^{p^{v/2}} + \alpha_j^{p^{v/2}}.$$

This yields

$$\alpha_i - \alpha_j + (\alpha_i - \alpha_j)^{p^{v/2}} = 0,$$

and we find that $\alpha_i - \alpha_j$ is a root of $f(u)$, hence $\alpha_i - \alpha_j \in A$. But $\alpha_i - \alpha_j \notin A$ according to the choice of $\alpha_1, \ldots, \alpha_r$, and we arrive at a contradiction.

Finally, since $|A| = p^{v/2}$, we find that

$$r = |\, F_q^+/A \,| = p^v/p^{v/2} = p^{v/2}.$$

This completes the proof.

Lemma 4. *Let F_p be a prime finite field of characteristic $p > 2$, F_q be an extension of F_p of even degree $v > 1$ and let $s \le q^{1/2}$ be a positive integer. Let N_q be the number of F_q-rational points of the affine curve Y given by equations* (2) *with the polynomials*

$$f_i(x) = (u + \alpha_i) + (u + \alpha_i)^{p^{v/2}}, \qquad 1 \le i \le s,$$

defined by (3). *Then*

$$N_q = (2q^{1/2} - s)q^{1/2}2^{s-1}.$$

Proof. We have

$$N_q = \sum_{u \in F_q} (1 + \chi_v(f_1(u)))\dots(1 + \chi_v(f_s(u)))$$

$$= \sum_{u \in F_q} \left(1 + \sum_{\sigma=1}^{s} \sum_{1 \le i_1 < \dots < i_\sigma \le s} \chi_v(f_{i_1}(u))\dots\chi_v(f_{i_\sigma}(u))\right)$$

and hence

$$N_q = p^v + \sum_{\sigma=1}^{s} \sum_{1 \le i_1 < i_2 < \dots < i_\sigma \le s} \sum_{u \in F_q} \chi_v(f_{i_1}(u))\dots\chi_v(f_{i_\sigma}(u)).$$

It follows from Lemmas 2 and 3 that

$$\chi_v(f_i(u)) = \begin{cases} 0, & \text{if } u \in A_i, \\ 1, & \text{if } u \in F_q \setminus A_i, \end{cases}$$

and since any two distinct sets A_i and A_j have no common element, we obtain

$$N_q = p^v + \sum_{\sigma=1}^{s} \binom{s}{\sigma} (p^v - \sigma p^{v/2}) = p^v + (2^s - 1)p^v - s2^{s-1}p^{v/2}$$

$$= (2p^{v/2} - s)p^{v/2}2^{s-1} = (2q^{1/2} - s)q^{1/2}2^{s-1}.$$

This proves the lemma.

3. PROOF OF THE THEOREMS

Let $p > 2$ be a prime number, $k' = F_q$ be an extension of a prime finite field F_p of an even degree $v > 1$, and let $s \le q^{1/2}$ be a positive integer. Let $f_1, \dots, f_s$ be pairwise coprime polynomials in $k'[u]$ of the same degree $q^{1/2}$ defined by (3), and let $Y \subset A^{s+1}$ be the affine curve defined over k' by equations (2). Let $\bar{Y} \subset P^{s+1}$ be the projective closure of Y, and X be a non-singular projective model of $\bar{Y}$ over the algebraic closure k'' of the field k'.

Since the curves $\bar{Y}$ and X are birationally isomorphic, we have $g = g(Y) = g(X)$, and by Lemma 1

$$g = (sq^{1/2} - 3)2^{s-2} + 1.$$

Next, let N_q be the number of k'-rational points of Y and M_q be the number of k'-rational points of X. We have $M_q \geq N_q + 1$, and by Lemma 4

$$M_q \geq (2q^{1/2} - s)q^{1/2}2^{s-1} + 1.$$

Let $n \leq N_q$ be a positive integer, let $x_1, \ldots, x_n$ be k'-rational points of the curve X at the finite part of X, and let x_∞ be the point of X at infinity. Set

$$D_0 = x_1 + \cdots + x_n, \qquad D = lx_\infty.$$

Applying to X the L-construction for $l > (sq^{1/2} - 3)2^{s-2}$ and $n > l$, we obtain the geometric Goppa $[n, k, d]_q$-code $C = C(D_0, D)$ with parameters

$$\begin{aligned} &l < n \leq (2q^{1/2} - s)q^{1/2}2^{s-1}, \\ &k \geq l - g + 1 = l - (sq^{1/2} - 3)2^{s-2}, \\ &d \geq n - l. \end{aligned}$$

This proves Theorem 1.

Now, applying to X the Ω-construction for

$$l > (sq^{1/2} - s)q^{1/2}2^{s-1}, \qquad n > l - (sq^{1/2} - 3)2^{s-2},$$

we obtain the geometric Goppa $[n, k, d]_q$-code $C^* = C^*(D_0, D)$ with parameters

$$\begin{aligned} l - (sq^{1/2} - 3)2^{s-2} < n &\leq (2q^{1/2} - s)q^{1/2}2^{s-1}, \\ k &\geq n - l + (sq^{1/2} - 3)2^{s-2}, \\ d &\geq l - (sq^{1/2} - 3)2^{s-1}. \end{aligned}$$

This gives the result of Theorem 2.

Finally, it follows from (1) that the relative parameters $R = k/n$ and $\delta = d/n$ of the codes $C = C(D_0, D)$ and $C^* = C^*(D_0, D)$ satisfy the inequality

$$R \geq 1 - \delta - \frac{(sq^{1/2} - 3)2^{s-2}}{n}.$$

This proves Corollary 1.

REFERENCES

1. M. J. Aaltonen, Notes on the asymptotic behavior of the information rate of block codes. *IEEE Trans. Inform. Theory* (1984) **30**, 84–85.
2. A. Garcia and H. Stichtenoth, A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound. *Invent. Math.* (1995) **121**, 211–222.
3. V. G. Goppa, Codes on algebraic curves. *Soviet Math. Dokl.* (1981) **24**, 170–172.
4. Yu. I. Manin, What is the maximum of points on a curve over F_2? *J. Fac. Sci. Tokyo* (1981) **28**, 715–720.
5. C. Moreno, *Algebraic Curves over Finite Fields*. Cambridge Univ. Press, Cambridge, 1991.
6. S. A. Stepanov, On lower bounds of character sums over finite fields. *Discrete Math. Appl.* (1992) **2**, 523–532.
7. S. A. Stepanov, *Arithmetic of Algebraic Curves*. Plenum, New York, 1994.
8. H. Stichtenoth, *Algebraic Function Fields and Codes*. Springer, Berlin, 1993.
9. M. A. Tsfasman, S. G. Vladut, and Th. Zink, Modular curves, Shimura curves, and Goppa codes, better than the Varshamov–Gilbert bound. *Math. Nachr.* (1982) **109**, 21–28.
10. M. A. Tsfasman and S. G. Vladut, *Algebraic-Geometric Codes*. Kluwer Acad. Publ., Dordrecht, 1991.
11. G. van der Geer and M. van der Vlugt, Fibre products of Artin–Schreier curves and generalized Hamming weights of codes. *J. Comb. Theory* (1995) **70A**, 337–348.
12. A. Weil, Number of solutions of equations in finite fields. *Bull. Amer. Math. Soc.* (1949) **55**, 497–508.