Character Sums, Algebraic Curves and Goppa Codes

Serguei A. Stepanov

Department of Mathematics
Bilkent University
06533 Bilkent,Ankara, Turkey
&
Department of Algebra
Steklov Mathematical Institute
Vavilov St. 42
Moscow GSP-I, 117966 Russia

e-mail: stepanov@fen.bilkent.edu.tr

1 Introduction

The purpose of this paper is to demonstrate a close interconnection between Number Theory, Algebraic Geometry and Coding Theory and construct considerably long geometric Goppa codes on fibre products with very good parameters.

Let F_p be a prime finite field of characteristic p, which we identify as a set with $\{1, 2, \ldots, p\}$, and F_q be an extension of F_p of degree $\nu \geq 1$, so that $q = p^\nu$. Let $s \geq 2$ be a positive divisor of $q - 1$ and

χ (resp. ψ) be a non-trivial multiplicative character of exponent s (resp. a non-trivial additive character) of the field F_q. For any two polynomials $f, g \in F_q[x]$ of degree $l \geq 1$, $m \geq 1$ respectively, consider the following character sums

$$S_q(f) = \sum_{x \in F_q} \chi(f(x))$$

and

$$T_q(g) = \sum_{x \in F_q} \psi(g(x)).$$

If $f = f_1^{s_1} \cdots f_r^{s_r}$ is the factorization of f into distinct irreducible polynomials $f_1, \ldots f_r \in F_q[x]$ with $\deg(f_1 \cdots f_r) = \mu$ and $(s, s_1, \ldots, s_r) = 1$, the well-known Weil's result [45] (see also Stepanov [33]) provides the upper bound

$$|S_p(f)| \leq (\mu - 1)q^{1/2} \,. \tag{1}$$

Similarly, if $(m, p) = 1$, we have

$$|T_q(g)| \leq (m - 1)q^{1/2}. \tag{2}$$

The upper bounds (1), (2) are not trivial only for $\mu, m \leq q^{1/2} + 1$, and we know several cases (see Stark [32], Korobov [18], Mit'kin [23], Serre [30] and Stöhr-Voloch [41]) when these bounds can be essentially sharpened using the author's elementary method (see Stepanov [33]). Unfortunately, until now the algebraic structure of the polynomials f and g providing such improvement of the Weil bound is not clear. If $\mu, m > q^{1/2} + 1$, we do not know practically any non-trivial upper bounds for absolute values of the sums $S_q(f)$ and $T_q(g)$, except in the case of polynomials f and g of very special form. Thus we have the following problem.

Problem 1. *Determine the class of polynomials $f, g \in F_q[x]$ of degree l, m respectively, $1 \leq l, m < q$, for which the upper bounds (1), (2) can be sharpened and absolute values of the sums $S_q(f)$, $T_q(g)$ can be estimated non-trivially for $\mu, m > q^{1/2} + 1$.*

Note that the bounds (1), (2) are sequences of the Riemann hypothesis for zeta-functions $\zeta(X,s)$ and $\zeta(Y,s)$ of the smooth projective curves defined over F_q by equations

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

and

$$y^p - y = g(x).$$

According to this hypothesis all the zeros of the zeta-functions $\zeta(X,s)$ and $\zeta(Y,s)$ lie on the complex line $Re(s) = 1/2$. Under such interpretation we see that Problem 1 is related to the very deep question concerning the distribution of the zeros of $\zeta(X,s)$ and $\zeta(Y,s)$ on the critical line $Re(s) = 1/2$.

The problem becomes much more difficult if we consider the corresponding incomplete sums. Let $\omega_1, \ldots, \omega_\nu$ be a basis of F_q over F_p. Every element $x \in F_q$ can be uniquely written in the form

$$x = x_1\omega_1 + \cdots + x_\nu\omega_\nu$$

with $x_1, \ldots, x_\nu \in F_p$, and for any positive integer $N \leq p$ we can define the box $B_N \in F_q \simeq F_p^\nu$ of volume $V = N^\nu$ as

$$B_N = \{x = (x_1, \ldots, x_\nu) \in F_q \mid 1 \leq x_i \leq N, 1 \leq i \leq \nu\}.$$

Consider now the following incomplete character sums

$$S_N(f) = \sum_{x \in B_N} \chi(f(x))$$

and

$$T_N(g) = \sum_{x \in B_N} \psi(g(x)).$$

If $f(x) = x + a$ and χ is a non-trivial multiplicative character of the field F_q with $q = p^\nu$ elements, it follows from the well-known results of Burgess [4] and Davenport, Lewis [6] that for any $\varepsilon > 0$ there exists $\delta > 0$ such that for $p \geq p_0(\varepsilon)$ and $N > p^{(\nu/2(\nu+1))+\varepsilon}$ the estimate

$$|S_N(x)| < (Np^{-\delta})^\nu$$

holds. On the other hand, as was proved by Elliot [8] in the case when $q = p$ and χ is the non-trivial quadratic character of F_p, for any positive $\varepsilon < 1$ and any positive integer $N \le c(\varepsilon)\log p$, the equality

$$|S_N(x)| = |\sum_{x=1}^{N} \chi(x)| = N$$

holds for at least $y^{1-\varepsilon}$ primes $p \le y$.

In the general case when $q = p$ and $f, g \in F_p[x]$ are polynomials of degree $l > 1$, $m > 1$ respectively, we are able only to obtain upper bounds of the form (Burgess [5])

$$|S_N(f)| \le c(l)p^{1/2}\log p \tag{3}$$

and (Korobov [17])

$$|T_N(g)| \le c_0 N^{1-\frac{\gamma}{m^2}}, \tag{4}$$

where $N = p^{1/r}$, $1 \le r \le m$, $\min([r], [m - r + 1]) > \varepsilon m$ for any positive $\varepsilon < 1/2$, and the constants c_0 and γ depend only of ε. Thus we have the following problem, which is very important for many questions of analytic number theory.

Problem 2. *Extend estimates* (3), (4) *to the case of an arbitrary finite field* F_q, *and determine the class of polynomials* $f, g \in F_q[x]$ *of degree* $l \ge 1$, $m \ge 1$ *respectively, for which absolute values of the sums* $S_N(f)$ *and* $T_N(g)$ *can be estimated non-trivially for all* $N > \log^{1+\varepsilon} q$.

In view of the difficulties connected with the solution of Problems 1 and 2 there arises the problem on finding of lower (i.e. existence) bounds for absolute values of the sums $S_q(f)$ and $T_q(g)$. This problem is especially interesting in connection with its extraordinary significance for coding theory. Later on we shall consider two aspects of the problem, namely, coding theoretic and number theoretic ones. The first aspect concerns the obtaining of lower bounds for character sums by the use of concepts and results of coding theory, whilst the second one provides applications of the lower bounds for character sums, obtaining by the use of number theoretic methods, to

the problem of construction of linear codes over F_q with extremely good parameters. Now we explain a close interconnection between the problem concerning lower bounds for character sums and the problem concerning construction of good linear codes. To do this we shall recall shortly the basic idea of the Goppa construction [14] of linear $[n, k, d]_q$-codes associated with a smooth projective curve over an algebraic closure $\overline{F}_q$ of the field F_q.

Let X be a smooth projective curve of genus $g = g(X)$ defined over a finite field F_q. Let $\{x_1, \ldots, x_n\}$ be a set of F_q-rational points of X and set

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

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

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

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

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

Such a q-ary linear code is called a geometric Goppa code.

Let us estimate the parameter of the code $C = C(D_0, D)$. The kernel of the map Ev is $L(D - D_0)$, hence $C \simeq L(D)/L(D - D_0)$ and

$$k = \dim C = \dim L(D) - \dim L(D - D_0) = l(D) - l(D - D_0).$$

In particular, if $\deg D < n$ then the map Ev is an embedding, and the Riemann-Roch theorem implies

$$k \geq \deg D - g + 1; \tag{5}$$

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

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

Now, if the weight of $\mathrm{Ev}(f)$ is d then f vanishes at $n-d$ points, say, $x_{i_1}, \ldots, x_{i_{n-d}}$, so $(f) + D - x_{i_1} - \cdots - x_{i_{n-d}} \geq 0$. By taking degrees we obtain

$$d \geq n - \deg D. \tag{6}$$

It follows from (5) and (6) that the relative parameters $R = k/n$ and $\delta = d/n$ of a geometric Goppa code $C = C(D_0, D)$ satisfy

$$R \geq 1 - \delta - \frac{g-1}{n}. \tag{7}$$

Thus to construct a long geometric Goppa $[n, k, d]_q$-code with rather good parameters we need to find a smooth projective curve X of genus g with a lot of F_q-rational points which ensures the condition that the quantity $(g-1)/n$ is small enough. Recall that for any linear $[n, k, d]_q$-codes we have the Singleton upper bound

$$R \leq 1 - \delta + \frac{1}{n}$$

and for $n \to \infty$ the asymptotic Gilbert-Varshamov lower bound

$$R \geq 1 - H_q(\delta),$$

where $H_q(\delta)$ is the q-ary entropy function defined as

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

The points (δ, R) for all linear $[n, k, d]_q$-codes form the set of code points $V_q^{lin} \subseteq [0,1]^2$. Let U_q^{lin} denote the subset of limit points of V_q^{lin}. In other terms, $(\delta, r) \in U_q^{lin}$ if and only if there exists an infinite sequence of different linear codes C_i with distinct 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 $R > 0$ such a family of codes C_i is called asymptotically good. The structure of the set U_q^{lin} can be described as follows (Aaltonen [1], Manin [22]): *there exist a continuous function* $\alpha_q^{lin}(\delta)$ *such that*

$$U_q^{lin} = \{ \quad (\delta, R) \mid 0 \leq R \leq \alpha_q^{lin}(\delta) \quad \} \ ;$$

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

In order to produce a family of asymptotically good geometric Goppa codes for which $R+\delta$ comes above the Gilbert-Varshamov bound one needs an infinite family of smooth projective curves with a lot of F_q-rational points compared to the genus. Examples of such families are provided by classical modular curves $X_0(N)$ and $X(N)$ (Ihara [16], Tsfasman-Vladut-Zink [44], or by Drinfeld modular curves (Tsfasman-Vladut [43, Chapters 4.1 and 4.2]). So, if $q = p^\nu$ is an even power of a prime p, there exists an infinite sequence of geometric Goppa codes C_i which gives the lower bound

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

The line $R = 1 - \delta - (\sqrt{q} - 1)^{-1}$ intersects the curve $R = 1 - H_q(\delta)$ for $q \geq 49$. Much easier proof of this result based on construction of a sequence of Artin-Schreier coverings of the projective line $\mathbb{P}^1(\bar{F}_q)$ was recently proposed by Garcia and Stichtenoth [9].

In terms of algebraic geometry the problem on construction of asymptotically good codes can be reformulated as follows. Let $N_q(g)$ denote the maximal number of F_q-rational points on a smooth projective curve X defined over F_q of genus $g = g(X)$, and

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g} .$$

It follows from the Hasse-Weil bound [45] that

$$A(q) \leq 2\sqrt{q} .$$

The Serre bound [30]

$$|N_q - (q+1)| \leq g[2\sqrt{q}]$$

yields

$$A(q) \leq [2\sqrt{q}] .$$

Much stronger upper bound

$$A(q) \leq \sqrt{q} - 1$$

was obtained by Drinfeld and Vladut [7] . This is the best possible upper bound, and construction of asymptotically good geometric codes is reduced to construction of a family of smooth projective curves over F_q, for which $A(q)$ is close to the Drinfeld-Vladut bound. So, if $q = p^\nu$ is an even power of a prime p , the result of Ihara [16]. Tsfasman-Vladut-Zink [44] (see also Garcia-Stichtenoth [9]) implies

$$A(q) \geq \sqrt{q} - 1 \ .$$

If q is an odd power of p, the result of Serre [30] provides existence of an absolute constant $c > 0$ such that

$$A(q) \geq c \log q \ .$$

In some cases the Serre bound was improved by Perret [28] and Zink [47]. In particular, the Zink result yields

$$A(q^3) \geq \frac{2(q^2 - 1)}{q + 2} \ .$$

In this paper we construct a family of sufficiently long geometric Goppa codes coming from smooth projective curves X_s given over F_q by equations

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

Each such curve is actually a fibre product of hyperelliptic curves. For some polynomials $f_i \in F_q[u]$ of a special form the curves X_s have a lot of F_q-rational points and provide a family of linear $[n, k, d]_q$-codes with fairly good parameters and very fast construction and decoding algorithms. For small values of s, the parameters of the codes are comparable with the parameters of codes on Artin-Schreier coverings introduced by Garcia and Stichtenoth [9]. 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

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

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

A similar construction of non-singular projective curves with a lot of F_q-rational points based on the use of fibre products of some special Artin-Schreier curves was independently considered by van der Geer and van der Vlugt [10].

2 Coding Theoretic Aspects

Let $p > 2$ be a prime number, $N \leq p$ a positive integer and χ the unique non-trivial quadratic character of the prime finite field F_p, i.e. the Legendre symbol. Using simple coding-theoretic arguments we obtain the following result (Stepanov [33, p. 85] , [34]).

Theorem 1. *If m is an integer satisfying*

$$\frac{(N+1)\log 2}{\log p} + 1 < m \leq p$$

then there exists a square-free polynomial $f \in F_p[u]$ of degree $l = 2m$ for which

$$\sum_{u=1}^{N} \chi(f(u)) = N.$$

Proof. Consider the set $\{f_1(u), \ldots, f_n(u)\}$ of all distinct irreducible monic polynomials in $F_p[u]$ of degree $m > 1$ and the corresponding sequence $C = \{x_1, \ldots, x_n\}$ of vectors

$$x_i = (\chi(f_i(1)), \ldots, \chi(f_i(N))), \qquad 1 \leq i \leq n$$

with components $\chi(f_i(k)) = \pm 1$. We have

$$n = \frac{1}{m} \sum_{d|m} \mu(d) p^{m/d},$$

where $\mu(l)$ is the Möbius function, and hence $n \geq p^m/2m$. On the other hand, the supposition of the theorem implies $p^m/2m > 2^N$

and we arrive at the inequality $n > 2^N$. Since there is at most 2^N of distinct vectors x_i of length N it follows that at least two of the n vectors x_i must be equal. Let $x_i = x_{i'}$ for $i \neq i'$. The product $f = f_i(u)f_{i'}(u)$ is a square-free polynomial in $F_p[u]$ of degree $l = 2m$, and all the components of $(\chi(f(1)), \ldots, \chi(f(N)))$ are equal to 1. This proves the theorem.

Note that the sequence $C = \{x_1, \ldots, x_n\}$ can be considered as a code of cardinality n in the Hamming space $\{-1, 1\}^N$. Now, the equality $x_i = x_j$ for $i \neq j$ follows from the fact that cardinality of the code C cannot exceed cardinality 2^N of the whole space. In this way the result was slightly improved by Levenshtein [21] by the use of the presently best known universal upper bounds for codes. It follows from Theorem 1 that the upper bound (1) cannot be improved essentially, so in general we cannot obtain any inequality of the form

$$|S_p(f)| \leq c \cdot (\mu p)^{1/2} .$$

The following theorem is more arithmetic in nature and essentially extends the above mentioned result of Elliot.

Theorem 2. *Let $p > 3$ be a prime number and $m \leq p/4$ be a positive integer. If*

$$1 \leq N < \frac{\log(p/2m)}{\log 2} \leq p/2$$

then there exists a square-free polynomial $f = (u + \alpha_1) \cdots (u + \alpha_{2m})$, $\alpha_i \in F_p$, of degree $l = 2m$ for which

$$\sum_{u=1}^{N} \chi(f(u)) = N.$$

Proof. Consider polynomials $u, u + 1, \ldots, u + p - N - 1$ in $F_p[u]$ of degree 1 and the corresponding vectors

$$x_i = (\chi(i), \ldots, \chi(N + i - 1)), \qquad 1 \leq i \leq p - N$$

with components $\chi(k+i) = \pm 1$. By the assumption of the theorem,

$$1 \leq N < \frac{\log p/2m}{\log 2} \leq p/2,$$

hence $p - N > m(2^N + 1)$. Now let us consider m subsequences $C_s = \{x_{(s-1)r+1}, \ldots, x_{sr}\}, 1 \leq s \leq m$, of the sequence $C = \{x_1, \ldots, x_{p-N}\}$ consisting of $r = 2^N + 1$ elements. Each subsequence C_s contains at least two equal vectors, say $x_{(s-1)r+i_s} = x_{(s-1)r+i'_s}$ for $i_s \neq i'_s, 1 \leq i_s, i'_s \leq r$. The product

$$f(u) = \prod_{s=1}^{m} (u + (s-)r + i_s)(u + (s-1)r + i'_s) = (u + \alpha_1) \cdots (u + \alpha_{2m})$$

is a square-free polynomial in $F_p[u]$ of degree $l = 2m$, and all the components of $(\chi(f(1)), \ldots, \chi(f(N)))$ are equal to 1. This completes the proof.

Similarly, if ψ is a non-trivial character of the field F_p, we have (Stepanov [33, p. 86]) the following result.

Theorem 3. *Let $p > 2$ be a prime number, $N \leq p$ a positive integer and $\varepsilon < 1/4\pi$ a positive number. For every integer*

$$m \geq \frac{N \log(1 + \varepsilon^{-1})}{\log p},$$

there exists a non-zero polynomial $g \in F_p[u]$ of degree at most m for which

$$|\sum_{u=1}^{N} \psi(f(u))| \geq (1 - 2\pi\varepsilon)N.$$

The results of Theorems 1 and 3 (in a slightly stronger form) were recently extended by Özbudak [26] to the case of an arbitrary finite field F_q and arbitrary non-trivial characters χ and ψ. More subtle technique of the coding theory, based on using some properties of Reed-Muller codes, arrives at the following result for complete exponential sums (Bassalygo, Zinov'ev, Litsyn [3]).

Theorem 4. *Let F_p be a prime finite field of characteristic $p > 2$, let F_q be an extension of F_p of odd degree $\nu > 1$ and ψ be a non-trivial additive character of F_q. Then there exists a polynomial $g \in F_q[u]$ of degree at most $p^{(\nu-1)/2} + 1$ such that tr $g(u)$ is not a constant and*

$$|T_q(g)| \geq q^{\nu-1/2}.$$

Below we prove this result (Theorem 8) in a stronger form through elementary arithmetical means.

3 Number Theoretic Aspects

Let p be a prime number, ν a positive integer and F_q a finite field with $q = p^\nu$ elements. The field F_q is a Galois extension of the prime finite field F_p of degree ν with a cyclic Galois group of order ν. 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

$$\text{norm } (x) = x \cdot \theta(x) \cdots \theta^{\nu-1}(x) = x \cdot x^p \cdots x^{p^{\nu-1}}$$

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

$$\chi'(x) = \chi(\text{norm } (x))$$

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

Similarly, the map

$$\text{tr } (x) = x + \theta(x) + \cdots + \theta^{\nu-1}(x) = x + x^p + \cdots + x^{p^{\nu-1}}$$

is called a trace of the element $x \in F_q$. Let ψ be a non-trivial additive character of the field F_p. Set

$$\psi'(x) = \psi(\text{tr } (x))$$

and call ψ' the additive character of the field F_q induced by the character ψ.

Now let f be a square-free polynomial in the ring $F_q[u]$ of degree l and let g be a polynomial in $F_q[u]$ of degree m relatively prime to q. Let χ be the non-trivial quadratic character and ψ a non-trivial additive character of F_p. Consider the character sums

$$S_q(f) = \sum_{u \in F_q} \chi'(f(u)) = \sum_{u \in F_q} \chi(\text{norm } (f(u)),$$

and

$$T_q(g) = \sum_{u \in F_q} \psi'(g(u)) = \sum_{u \in F_q} \psi(\text{tr } (f(u)).$$

The following result of the author [35], [37] shows that the Weil bound cannot be sharpened essentially in any extension F_q of the field F_p.

Theorem 5. *Let F_q be a finite field of characteristic $p > 2$ consisting of $q = p^\nu$ elements and χ_ν be the character of F_q induced by the non-trivial quadratic character χ of the field F_p. If $\nu > 1$ then there exists a square-free polynomial $f \in F_p[u]$ of the form*

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

such that

$$S_q(f) = \begin{cases} (q^{1/2} - 1)q^{1/2} & \text{if } \nu \equiv 0 \pmod 2 \\ q - 1 & \text{if } \nu \equiv 1 \pmod 2 \end{cases}.$$

Proof. Let $\nu > 1$ be an even number. As $u^{p^\nu} = u$ for every $u \in F_q$,

we have

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

Therefore,

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

where N is the number of roots of the polynomial $f(u) = u + u^{p^{\nu}/2}$ in the field F_q. We have $f(u) = u(1+u^{p^{\nu}/2-1})$; hence taking into account the equality

$$(p^{\nu/2}-1, p^{\nu}-1) = p^{\nu/2}-1,$$

we obtain by the Euler criterion that $N = 1+(p^{\nu/2}-1) = q^{1/2}$. Thus,

$$S_q(f) = \sum_{u\in F_q}\chi'(f(u)) = (q^{1/2}-1)q^{1/2},$$

which proves the theorem for ν an even positive integer.

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

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

$$= \prod_{i=1}^{(\nu+1)/2} (u^{p^{i-1}} + u^{p^{(\nu-1)/2+i-1}}) \prod_{j=1}^{(\nu-1)/2} (u^{p^{(\nu+1)/2+j-1}} + u^{p^{j-1}})$$

$$\times \prod_{i=1}^{(\nu-1)/2} (u^{p^{i-1}} + u^{p^{(\nu+1)/2+i-1}}) \prod_{j=1}^{(\nu+1)/2} (u^{p^{(\nu-1)/2+j-1}} + u^{p^{j-1}})$$

$$= \prod_{i=1}^{(\nu+1)/2} (u(p^{i-1} + u^{p^{(\nu-1)/2+i-1}})^2 \prod_{i-1}^{(\nu-1)/2} (u^{p^{i-1}} + u^{p^{(\nu+1)/2+i-1}})^2$$

and hence

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

where N' is the number of roots in F_q of the polynomial $f(u) = (u + u^{p^{(\nu-1)/2}})(u + u^{p^{(\nu+1)/2}})$. Clearly $N' = 1$ and therefore

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

This completes the proof.

Note that the polynomial $f(u) = u + u^{p^{\nu/2}}$ has degree $l = p^{\nu/2}$; hence the Weil bound (1) is attained in any extension F_q of the field F_p of an even degree $\nu > 1$. The result of Theorem 5 can be extended as follows (Gluhov [11], [12], Gluhov, Özbudak [13]).

Theorem 6. *Let $\nu > 1$ be an integer, F_q the finite field of characteristic $p > 2$ consisting of $q = p^\nu$ elements, χ' the character of F_q induced by a non-trivial multiplicative character χ of the field F_p of exponent $s \geq 2$ and a, b positive integers satisfying $a + b = s$. Then*

(i) if $\nu \equiv 1 \pmod 2$, there exists a polynomial $f_1 \in F_p[u]$ of the form

$$f_1(u) = (u + u^{p^{(\nu-1)/2}})^a (u + u^{p^{(\nu+1)/2}})^b$$

such that

$$S_q(f_1) = \sum_{u \in F_q} \chi'(f_1(u)) = q - 1;$$

(ii) if $\nu \equiv 0 \pmod 2$, *there exists a polynomial* $f_2 \in F_p[u]$ *of the form*

$$f_2(u) = (u + u^{p^{\nu/2}-1})^a (u + u^{p^{\nu/2}+1})^b$$

such that

$$S_q(f_2) = \begin{cases} p^\nu - 1 & \text{if} \quad 4 \nmid \nu \\ p^\nu - p & \text{if} \quad 4 \mid \nu \end{cases};$$

(iii) if $\nu \equiv 0 \pmod 2$ *and* $s \equiv 0 \pmod 2$, *there exists a polynomial* $f_3 \in F_p[u]$ *of the form*

$$f_3(u) = (u + u^{p^{\nu/2}})^{s/2}$$

such that

$$S_q(f_3) = (p^{\nu/2} - 1)p^{\nu/2}.$$

Theorem 7. *Let* $\nu > 1$ *be an integer,* F_q *the finite field of characteristic* $p = 2$ *consisting of* $q = p^\nu$ *elements,* χ' *the character of* F_q *induced by a non-trivial multiplicative character of the field* F_p *of exponent* $s \geq 3$ *and* a, b *positive integers satisfying* $a + b = s$. *Then*

(i) if $\nu \equiv 1 \pmod 2$, *there exists a polynomial* $f_1 \in F_p[u]$ *of the form*

$$f_1(u) = (u + u^{p^{(\nu-1)/2}})^a (u + u^{p^{(\nu+1)/2}})^b$$

such that

$$S_q(f_1) = \sum_{u \in F_q} \chi'(f_1(u)) = p^\nu - p;$$

(ii) if $\nu \equiv 0 \pmod 2$, *there exists a polynomial* $f_2 \in F_p[u]$ *of the form*

$$f_2(u) = (u + u^{p^{\nu/2}-1})^a (u + u^{p^{\nu/2}+1})^b$$

such that

$$S_q(f_2) = \begin{cases} p^\nu - p^2 & \text{if} \quad 4 \nmid \nu \\ p^\nu - p & \text{if} \quad 4 \mid \nu \end{cases}.$$

Similar results can be obtained for the exponential sums $T_q(g)$ (Stepanov [35]).

Theorem 8. *Let $\nu > 1$ be an integer, F_q the finite field of characteristic $p > 2$ consisting of $q = p^\nu$ elements and ψ' the character of F_q induced by a non-trivial additive character ψ of the field F_p. There exists a polynomial $g \in F_p[u]$ of the form*

$$g(u) = \begin{cases} u^2 + 2\sum_{i=1}^{(\nu-2)/2} u^{p^i+1} + u^{p^{\nu/2}+1} & \text{if} \quad \nu \equiv 0 \pmod 2 \\ u^2 + 2\sum_{i=1}^{(\nu-1)/2} u^{p^i+1} & \text{if} \quad \nu \equiv 1 \pmod 2 \end{cases}$$

such that

$$|T_q(g)| = |\sum_{u \in F_q} \psi'(g(u))| = p^{\nu-1/2}.$$

Proof. Let $\omega_1, \ldots, \omega_\nu$ be a basis of the field F_q over F_p. Then every element $z \in F_q$ can be uniquely written as a linear combination

$$z = z_1\omega_1 + \cdots + z_\nu\omega_\nu$$

with coefficients z_i from F_p. Applying to both sides of the last equality the Frobenius automorphisms $\theta^j(z) = z^{p^j}$ for $j = 0, 1, \ldots, \nu - 1$ we arrive at the system of linear equations with respect to $z_1, \ldots, z_\nu$:

$$\begin{aligned} z &= z_1\omega_1 + \cdots + z_\nu\omega_\nu \\ \theta(z) &= z_1\theta(\omega_1) + \cdots + z_\nu\theta(\omega_\nu) \\ &\cdots \\ \theta^{\nu-1}(z) &= z_1\theta^{\nu-1}(\omega_1) + \cdots + z_\nu\theta^{\nu-1}(\omega_\nu). \end{aligned}$$

The determinant of the system

$$\Delta = \det(\theta^{j-1}(\omega_i))_{1 \le i,j \le \nu}$$

differs from zero, and we find

$$z_j = \Delta^{-1}(\Delta_{1j}z + \Delta_{2j}\theta(z) + \cdots + \Delta_{\nu j}\theta^{\nu-1}(z)), \qquad 1 \le j \le \nu,$$

where

$$\Delta_{ij} = (-1)^{i+j} \det(\theta^{l-1}(\omega_k))_{1 \le k,l \le \nu, k \ne i, l \ne j}.$$

It is clear that

$$\theta(\Delta) = (-1)^{\nu-1}\Delta,$$

and

$$\theta(\Delta_{i-1,j}) = (-1)^{\nu-2}\Delta_{ij}, \qquad 2 \le i \le \nu, \quad 1 \le j \le \nu.$$

Therefore

$$\Delta_{ij}/\Delta = \theta^{i-1}(\Delta_{1j}/\Delta), \qquad 1 \le i, j \le \nu$$

and hence

$$\begin{aligned} z_j &= (\alpha_j z) + \theta(\alpha_j z) + \cdots + \theta^{\nu-1}(\alpha_j z) \\ &= (\alpha_j z) + (\alpha_j z)^p + \cdots + (\alpha_j z)^{p^{\nu-1}} \\ &= \operatorname{tr}(\alpha_j z), \end{aligned}$$

where

$$\alpha_j = (-1)^{j+1}\Delta_{1j}/\Delta, \qquad 1 \le j \le \nu.$$

For $p > 2$ we have

$$z_j^2 = \operatorname{tr}(\alpha_j z)^2 + 2 \sum_{1 \le i < k \le \nu} (\alpha_j z)^{p^{i-1}} (\alpha_j z)^{p^{k-1}},$$

and setting $\alpha_j z = u$ for some $j = 1, 2, \ldots, \nu$ we obtain

$$z_j^2 = \operatorname{tr} u^2 + 2 \sum_{1 \le i < k \le \nu} u^{p^{i-1}} u^{p^{k-1}}.$$

Let $\nu > 1$ be an odd number. Represent the sum

$$\sum_{1 \le i < k \le \nu} u^{p^{i-1}} u^{p^{k-1}}$$

in the form

$$\begin{aligned} \sum_{1 \le i < k \le \nu} u^{p^{i-1}} u^{p^{k-1}} &= \sum_{i=1}^{\nu-1} \sum_{l=1}^{\nu-i} (u \cdot u^{p^l})^{p^{i-1}} \\ &= \sum_{i=1}^{(\nu-1)/2} \sum_{l=1}^{(\nu-1)/2} (u \cdot u^{p^l})^{p^{i-1}} \\ &\quad + \sum_{i=(\nu+1)/2}^{\nu-1} \sum_{l=1}^{\nu-i} (u \cdot u^{p^l})^{p^{i-1}} + \sum_{i=1}^{(\nu-1)/2} \sum_{l=(\nu+1)/2}^{\nu-i} (u \cdot u^{p^l})^{p^{i-1}}. \end{aligned}$$

Since $u^{p^\nu} = u$ for every $u \in F_q$, we have

$$\sum_{i=1}^{(\nu-1)/2} \sum_{l=(\nu+1)/2}^{\nu-i} (u \cdot u^{p^l})^{p^{i-1}} = \sum_{i-1}^{(\nu-1)/2} \sum_{l=(\nu+1)/2}^{\nu-i} u^{p^{l-1}} u^{p^{l+i-1}}$$

$$= \sum_{k=(\nu+3)/2}^{\nu} \sum_{l=(\nu+1)/2}^{k-1} u^{p^{\nu-l+k-1}} u^{p^{k-1}} = \sum_{k=(\nu+3)/2}^{\nu} \sum_{j=\nu-k+1}^{(\nu-1)/2} (u \cdot u^{p^j})^{p^{k-1}}$$

$$= \sum_{i=(\nu+3)/2}^{\nu} \sum_{l=\nu-i+1}^{(\nu-1)/2} (u \cdot u^{p^l})^{p^{i-1}}$$

and therefore

$$\sum_{1 \le i < k \le \nu} u^{p^{i-1}} u^{p^{k-1}} = \sum_{i-1}^{(\nu-1)/2} \sum_{l=1}^{(\nu-1)/2} (u \cdot u^{p^l})^{p^{i-1}}$$

$$+ \sum_{i=(\nu-1)/2}^{\nu-1} \sum_{l=1}^{\nu-i} (u \cdot u^{p^l})^{p^{i-1}} + \sum_{i=(\nu+3)/2}^{\nu} \sum_{l=\nu-i+1}^{(\nu-1)/2} (u \cdot u^{p^l})^{p^{i-1}}$$

$$= \operatorname{tr} \left(\sum_{i=1}^{(\nu-1)/2} u^{p^{l+1}} \right).$$

Put

$$g(u) = u^2 + 2 \sum_{l=1}^{(\nu-1)/2} u^{p^{l+1}}$$

For every $u \in F_q$ we have

$$z_j^2 = \operatorname{tr} g(u)$$

and, consequently,

$$\sum_{u \in F_q} \psi'(g(u)) = \sum_{z_1, \ldots, z_\nu \in F_p} \psi(z_j^2).$$

For the Gauss sum

$$\sum_{z_j \in F_p} \psi(z_j^2)$$

the equality

$$\left|\sum_{z_j \in F_p} \psi(z_j^2)\right| = p^{1/2}$$

is valid and hence

$$|T_q(g)| = \left|\sum_{u \in F_q} \psi(g(u))\right| = p^{\nu-1/2}.$$

This proves the statement for $\nu \equiv 1 \pmod 2$.

Let now $\nu > 1$ be an even number. In this case we have

$$z_j^2 = \operatorname{tr} u^2 + 2 \sum_{1 \le i < k \le \nu} u^{p^{i-1}} u^{p^{k-1}} = \operatorname{tr} u^2 + 2 \sum_{i=1}^{\nu-1} \sum_{l=1}^{\nu-i} (u \cdot u^{p^l})^{p^{i-1}}$$

$$= \operatorname{tr} u^2 + 2 \sum_{i=1}^{\nu/2} \sum_{l=1}^{(\nu-2)/2} (u \cdot u^{p^l})^{p^{i-1}} + 2 \sum_{i=(\nu+2)/2}^{\nu-1} \sum_{l=1}^{\nu-i} (u \cdot u^{p^l})^{p^{i-1}}$$

$$+ 2 \sum_{i=1}^{(\nu-2)/2} \sum_{l=(\nu+2)/2} (u \cdot u^{p^l})^{p^{i-1}} + 2 \sum_{i=1}^{\nu/2} (u \cdot u^{p^{\nu/2}})^{p^{i-1}},$$

and since

$$\sum_{i=1}^{(\nu-2)/2} \sum_{l=(\nu+2)/2}^{\nu-i} (u \cdot u^{p^l})^{p^{i-1}} = \sum_{i=1}^{(\nu-2)/2} \sum_{l=(\nu+2)/2}^{\nu-i} u^{p^{i-1}} u^{p^{l+i-1}}$$

$$= \sum_{k=(\nu+4)/2}^{\nu} \sum_{l=(\nu+2)/2}^{k-1} u^{p^{\nu-l+k-1}} u^{p^{k-1}} = \sum_{i=(\nu+4)/2}^{\nu} \sum_{l=\nu-i+1}^{(\nu-2)/2} (u \cdot u^{p^l})^{p^{i-1}}$$

and

$$2 \sum_{i=1}^{\nu/2} (u \cdot u^{p^{\nu/2}})^{p^{i-1}} = \sum_{i=1}^{\nu} (u \cdot u^{p^{\nu/2}})^{p^{i-1}}$$

for any $u \in F_q$, we find that

$$z_j^2 = \operatorname{tr} u^2 + 2\sum_{i=1}^{\nu}\left(\sum_{l-1}^{(\nu-2)/2} u \cdot u^{p^l}\right)^{p^{i-1}} + \sum_{i=1}^{\nu}(u \cdot u^{p^{\nu/2}})^{p^{i-1}}$$

$$= \operatorname{tr}\left(u^2 + 2\sum_{l=1}^{(\nu-2)/2} u^{p^l+1} + u^{p^{\nu/2}+1}\right).$$

Thus, if

$$g(u) = u^2 + 2\sum_{l=1}^{(\nu-2)/2} u^{p^l+1} + u^{p^{\nu/2}+1},$$

then for every $u \in F_q$ we have

$$z_j^2 = \operatorname{tr} g(u)$$

and therefore

$$|T_q(g)| = \left|\sum_{u \in F_q} \psi'(g(u))\right| = p^{\nu-1/2}.$$

This completes the proof.

If char $F_q = 2$ we are able to prove the following result.

Theorem 9. *Let $\nu > 1$ be an odd number, F_q the finite field of characteristic $p = 2$ consisting of $q = p^\nu$ elements and ψ' the character of F_q induced by a non-trivial additive character ψ of the field F_2. There exists a polynomial $g \in F_q[z]$ of the form*

$$g(z) = \alpha_r\alpha_s z^2 + \sum_{l=1}^{(\nu-1)/2} (\alpha_r\alpha_s^{p^l} + \alpha_r^{p^l}\alpha_s)z^{p^l+1}$$

such that

$$T_q(g) = p^{\nu-1}.$$

Proof. Using the same arguments as in the proof of Theorem 8 we find that

$$z_r z_s = \operatorname{tr}\left(\alpha_r\alpha_s z^2 + \sum_{l=1}^{(\nu-1)/2} (\alpha \cdot \alpha_s^{p^l} + \alpha_r^{p^l} \cdot \alpha_s)z^{p^l+1}\right) = \operatorname{tr} g(z)$$

for every $z \in F_q$. Now since

$$\sum_{z_1,\ldots,z_\nu \in F_2} \psi(z_r z_s) = p^{\nu-1}$$

for $r \neq s$, we obtain the equality

$$T_q(g) = p^{\nu-1},$$

which proves the theorem.

4 Applications to Coding Theory

Now we apply the results of previous section to construct rather long geometric Goppa codes with fairly good parameters.

Let F_q be a finite field of characteristic $p > 2$, let $\overline{F}_q$ be an algebraic closure of the field F_q and $\mathbb{A}^{s+1}$ be $(s+1)$-dimensional affine space over $\overline{F}_q$.

Lemma 1. *Let $f_1, \ldots, f_s$ be pairwise coprime square-free monic polynomials in F_q of the same odd degree $l \geq 1$ and Y be the fibre product in $\mathbb{A}^{s+1}$ given by*

$$z_i^2 = f_i(u), \qquad 1 \leq i \leq s. \tag{8}$$

Then the genus $g = g(Y)$ of the curve Y is

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

Proof. Let X be a smooth projective model of the curve Y. Denote by v_x the canonical valuation of the function field $\overline{F}_q(X)$, and by $\Omega[X]$ the space of regular differential forms on X. The affine curve Y is easily seen to be smooth. If $\overline{Y}$ is its projective closure, then X is a normalization of $\overline{Y}$ and we have the map $\psi : X \to \overline{Y}$, which

is an isomorphism between Y and $\psi^{-1}(Y)$. Hence it follows that $g = g(X)$.

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

Let us consider the point at infinity $u_\infty \in \mathbb{P}^1$. If the coordinate on $\mathbb{A}^1$ is denoted by u, then $t = u^{-1}$ is a local parameter at u_∞. If $\varphi^{-1}(u_\infty)$ were to consist of 2^s points $x_\infty^{(\tau)}$, then at each $x_\infty = x_\infty^{(\tau)}$ the function t would be a local parameter. Hence it would follow that $v_{x_\infty}(t) = 1$ and $v_{x_\infty}(f_i(t)) = -l$. But since l is odd, this contradicts the condition that $v_{x_\infty}(f_i(t)) = 2v_{x_\infty}(z_i)$. Thus $\varphi^{-1}(u_\infty)$ consists of $r = 2^{s-1}$ points $x_\infty^{(\tau)}, 1 \leq \tau \leq r$, with 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 $v_{x_\infty}(z_i) = -l$.

Now we shall find a basis of the space $\Omega[X]$ over the field $\overline{F}_q$. Any element $\omega \in \Omega[Y]$ can be written as a $\overline{F}_q$-linear combination of the differential forms $\omega_0 = P_0(u)du$ and

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

where $i_1, \ldots, i_\sigma$ are integers satisfying the condition $1 \leq i_1 < \cdots < i_\sigma \leq s$ and P_0, $P_{i_1,\ldots,i_\sigma}$ are polynomials in $\overline{F}_q[u]$. Indeed, the differential form

$$\omega_{i_1,\ldots,i_\sigma} = \frac{du}{z_{i_1} \cdots z_{i_\sigma}}$$

is regular at any point $u_0 \in \mathbb{A}^1$ 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 a unique $i \in \{i_1, \ldots, i_\sigma\}$, then z_i is a 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 $u_0 \in \mathbb{A}^1$. Thus, the differential forms $\omega_0 = du$ and $\omega_{i_1,\ldots,i_\sigma}$ form a basis of the $\overline{F}_q[u]$-module $\Omega[Y]$.

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

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

is regular at x_∞ if and only if

$$v_{x_\infty}(P_{i_1,\dots,i_\sigma}(u)du) \geq -(l\sigma-3).$$

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

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

The differential form $\omega_0 = P_0du$ is not regular at x_∞ for any non-zero polynomial $P_0 \in \overline{F}_q[u]$, so the regular differential forms

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

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

$$n = \begin{cases} \frac{l\sigma-4}{2} & \text{if } \sigma \equiv 0 \pmod 2 \\ \frac{l\sigma-3}{2} & \text{if } \sigma \equiv 1 \pmod 2 \end{cases},$$

form a basis of the space $\Omega[X]$ over $\overline{F}$. Therefore

$$\begin{aligned}
\dim_{\overline{F}} \Omega[X] &= \frac{1}{2} \sum_{\substack{\sigma=1 \\ \sigma \equiv 0 \pmod 2}}^{s} \sum_{1 \le i_1 < \cdots < i_\sigma \le s} (l\sigma - 2) \\
&+ \frac{1}{2} \sum_{\substack{\sigma=1 \\ \sigma \equiv 1 \pmod 2}}^{s} \sum_{1 \le i_1 < \cdots < i_\sigma \le s} (l\sigma - 1) \\
&= \frac{l}{2} \sum_{\sigma=1}^{s} \sigma \binom{s}{\sigma} - \sum_{\substack{\sigma=1 \\ \sigma \equiv 0 \pmod 2}}^{s} \binom{s}{\sigma} - \frac{1}{2} \sum_{\substack{\sigma=1 \\ \sigma \equiv 1 \pmod 2}}^{s} \binom{s}{\sigma} \\
&= \frac{1}{2}(ls2^{s-1} - 2^s - 2^{s-1} + 2)
\end{aligned}$$

and hence

$$g = g(X) = \dim_{\overline{F}_q} \Omega[X] = (ls - 3)2^{s-2} + 1.$$

This completes the proof.

Lemma 2. *Let F_p be a prime finite field of characteristic $p > 2$, let F_q be an extension of F_p of even degree $\nu > 1$ and A be the set of roots in F_q of the polynomial*

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

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 $\{\alpha_1, \ldots, \alpha_r\}$ are distinct representatives of the cosets, the polynomials

$$f_i(u) = (u + \alpha_i) + (u + \alpha_i)^{p^{\nu/2}}, \qquad 1 \le i \le r, \tag{9}$$

are pairwise coprime in $F_q[u]$;

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

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

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

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

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

and therefore

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

This yields

$$\alpha_i - \alpha_j + (\alpha_i - \alpha_j)^{p^{\nu/2}},$$

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

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

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

This finishes the proof.

Lemma 3. *Let F_p be a prime finite field of characteristic $p > 2$, let F_q be an extension of F_p of even degree $\nu > 1$ and $s \leq p^{\nu/2}$ be a positive integer. Let N_q be the number of F_q-rational points of the curve Y given by equations* (8) *with polynomials*

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

defined by (9). *Then*

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

Proof. We have

$$\begin{aligned} N_q &= \sum_{u \in F_q} (1 + \chi'(f_1(u))) \cdots (1 + \chi'(f_s(u))) \\ &= \sum_{u \in F_q} \left(1 + \sum_{\sigma=1}^{s} \sum_{1 \le i_1 < \cdots < i_\sigma \le s} \chi'(f_{i_1}(u)) \cdots \chi'(f_{i_\sigma}(u)) \right) \end{aligned}$$

and hence

$$N_q = p^\nu + \sum_{\sigma=1}^{s} \sum_{1 \le i_1 < \cdots < i_\sigma \le s} \chi'(f_{i_1}(u)) \cdots \chi'(f_{i_\sigma}(u)).$$

It follows from Theorem 5 and Lemma 2 that

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

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

$$\begin{aligned} N_q &= p^\nu + \sum_{\sigma=1}^{s} \binom{s}{\sigma} (p^\nu - \sigma p^{\nu/2}) = p_\nu + (2^s - 1)p^\nu - s2^{s-1}p^{\nu/2} \\ &= (2p^{\nu/2} - s)p^{\nu/2}2^{s-1} = (2q^{1/2} - s)q^{1/2}2^{s-1}. \end{aligned}$$

This proves the lemma.

Now we are able to prove the following result (Stepanov [36]).

Theorem 10. *Let $p > 2$ be a prime number, $\nu > 1$ be an even integer, and F_q the a finite field of characteristic p consisting of $q = p^\nu$ elements. For any positive integers $s \le q^{1/2}$ and $r > (sq^{1/2} -$*

$3)2^{s-2}$ *there exists a geometric Goppa* $[n,k,d]_q$*-code* $C = C(D_0, D)$ *with*

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

Proof. Let $f_1, \ldots, f_s$ be pairwise coprime polynomials in $F_q[u]$ of the same odd degree $l = q^{1/2}$ defined by (9), and $Y \subset \mathbb{A}^{s+1}$ be the affine curve defined over F_q by equations (8). Let $\overline{Y} \subset \mathbb{P}^{s+1}$ be the projective closure of Y and X be a non-singular projective model of $\overline{Y}$ over an algebraic closure $\overline{F}_q$ of the field F_q.

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

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

The number $N_q(X)$ of F_q-rational points of the curve X satisfies by Lemma 3 the inequality

$$N_q(X) \ge N_q + 1 = (2q^{1/2} - s)q^{1/2}2^{s-1} + 1.$$

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

$$D_0 = x_1 + \cdots + x_n \quad \text{and} \quad D = r \cdot x_\infty.$$

Applying to X the Goppa construction for $r > (sq^{1/2} - 3)2^{s-1}$, $n > r$, and taking into account (5), (6), we obtain a geometric Goppa $[n,k,d]_q$-code $C = C(D_0, D)$ with

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

This completes the proof.

Now using (7) we obtain the following result.

Corollary 11. *The relative parameters $R = k/n$ and $\delta = d/n$ of the code $C = C(D_0, D)$ satisfy*

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

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

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

Similar result is valid in the case of extension of the field F_p of an odd degree $\nu > 1$ (Stepanov, Özbudak [38]).

Theorem 12. *Let $p > 2$ be a prime number, $\nu > 1$ an odd integer and F_q the finite field of characteristic p consisting of $q = p^\nu$ elements. For any positive integers r, s satisfying*

$$s \leq \frac{2q + 4}{p^{(\nu-1)/2}(p + 1) - 2}$$

and

$$2^{s-2}((p^{(\nu-1)/2}(p + 1) - 2)s - 4) < r < 2^s q$$

there exists a geometric Goppa $[n, k, d]_q$-code with parameters

$$\begin{aligned} r &< n \leq 2^s q, \\ k &\geq r - 2^{s-2}((p^{(\nu-1)/2}(p + 1) - 2)s - 4), \\ d &\geq n - r. \end{aligned}$$

Recently these results were extended to the case of codes on fibre product of superelliptic curves (Özbudak [27], Stepanov, Özbudak [39]).

For other applications of character sums to coding theory see Barg [2], Helleseth [15], Lachaud [19], Lachaud, Wolfmann [20], C.J. Moreno, O. Moreno [24], [25], Rodier [29], Tietäväinen [42] and Wolfmann [46].

References

[1] Aaltonen M. J., Notes on the asymptotic behavior of the information rate of block codes, *IEEE Trans. Info. Theory* , 1984, **IT-30**, p. 84-85.

[2] Barg A., Exponential sums and constrained error-correcting codes, *Lect. Notes in Comp. Sciences* , **573**, Springer, 1991, p. 16-22.

[3] Bassalygo L. A., Zinov'ev V. A., Litsyn S. N., A lower estimate of complete trigonometric sums in terms of multiple sums, *Soviet Math. Dokl.*, 1988, **37**, p. 756-759.

[4] Burgess D.A., On character sums and primitive roots, *Proc. London Math. Soc.* (3), 1962, **12**, p. 179-192.

[5] Burgess D. A., On Dirichlet characters of polynomials, *Proc. London Math. Soc.* (3), 1963, **13**, p. 537-548.

[6] Davenport H., Lewis D.J., Character sums and primitive roots in finite fields, *Rend. Cird. Mat. Palermo* (2), 1963, **12**, p. 129-136.

[7] Drinfeld V. G., Vladut S. G., The number of points on an algebraic curve, *Funct. Anal. and Appl.* , 1983, **17**, p. 53-54.

[8] Elliot P.D.T.A., The distribution of primitive roots, *Can. J. Math.*, 1969, **14**, p. 822-841.

[9] Garcia A., Stichtenoth H., A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound, *Invent. Math.*, 1995, **121**, p. 211-222.

[10] van der Geer G., van der Vlugt N., Fibre products of Artin-Schreier curves and generalized Hamming weights of codes, *J. Comb. Theory* , 1995, **70**, no. **2**, p. 337-348.

[11] Gluhov M.M., Lower bounds for character sums over finite fields, *Diskr. Mat.*, 1994, **6**, no. **3**, p. 136-142 (*in Russian*).

[12] Gluhov M.M., On lower bounds for character sums over finite fields, *Preprint* , 1995.

[13] Gluhov M.M., Özbudak F., Codes on superelliptic curves, *Preprint* , 1995.

[14] Goppa V.G., Codes on algebraic curves, *Soviet Math. Dokl.*, 1981, **24**, p. 170-172.

[15] Helleseth T., On the covering radius of cyclic linear codes and arithmetic codes, *Discrete Appl. Math.* , 1985, **11**, p. 157-173.

[16] Ihara Y., Some remarks on the maximum of rational points of algebraic curves over finite fields, *J. Fac. Sci. Tokyo* , 1981, **28**, p. 721-724.

[17] Korobov N.M., Double trigonometric sums and their applications to the estimation of rational sums, *Math. Notes* , 1969, **6**, p. 472-478.

[18] Korobov N.M., Estimate of a sum of Legendre symbols, *Soviet Math. Dokl.*, 1971, **12**, p. 241-245.

[19] Lachaud G., Artin-Schreier curves, exponential sums and the Carlitz-Uchiyama bound for geometric codes, *J. Number Theory* 1991, **39**, p. 18-40.

[20] Lachaud G., Wolfmann J., Sommes de Kloosterman, courbes elliptique et codes cycliques en caracteristique 2, *C. R. Acad. Sci. Paris* , Ser. 1, 1987, **305**, p. 881-883.

[21] Levenshtein V. I., Bounds for packings of metric spaces and some their applications, *Probl. Cybern.*, **40**, Nauka, Moscow, 1983, p. 43-110 (*in Russian*).

[22] Manin Yu. I., What is the maximum of points on a curve over F_2?, *J. Fac. Sci. Tokyo* , 1A, 1981, **28**, p. 721-724.

[23] Mit'kin D.A., Estimation of the sum of Legendre symbols of polynomials of even degree, *Math. Notes* , 1973, **14**, p. 597-602.

[24] Moreno C.J., Moreno O., Exponential sums and Goppa codes I, *Proc. Amer. Math. Soc.* , 1991, **111**, p. 523-531; II, *IEEE Trans. Info. Theory* , 1992, **38**, p. 1222-1229.

[25] Moreno C.J., Moreno O., An improved Bombieri-Weil bound and application to coding theory, *J. Number Theory* , 1992, **38**, p. 32-46.

[26] Özbudak F., On lower bounds for incomplete character sums over finite fields, *Finite Fields and Applications* , 1996, **2**, p. 173-191.

[27] Özbudak F., Codes on fibre products of superelliptic curves, *Preprint* , 1996.

[28] Perret M., Tours ramifiées infininies de corps de classes, *J. Number Theory* , 1991, **38**, p. 300-322.

[29] Rodier F., Minoration de certaines sommes exponentielles binaires, *Lect. Notes in Math.* , **1518**, Springer, p. 199-209.

[30] Serre J.P., Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, *C.R. Acad. Sci. Paris* , Ser. 1, 1983, **296**, p. 397-402.

[31] Shafarevich I.R., *Basic Algebraic Geometry* I, Second Edition, Springer Verlag, Berlin, 1994.

[32] Stark H.M., On the Riemann hypothesis in hyperelliptic function fields, *Proc. Symp. Pure Math.*, **24**, p. 285-302, Amer. Math. Soc., Providence, R.I., 1973,

[33] Stepanov S.A., *Arithmetic of Algebraic Curves* , Plenum, New York, 1994.

[34] Stepanov S.A., On lower bound for incomplete character sums with polynomials, *Trudy Mat. Inst. Akad. Nauk SSSR* , 1977, **143**, p.175-177 (in Russian).

[35] Stepanov S.A., On lower bounds for character sums over finite fields, *Discr. Math. Appl.*, 1992, **2**, no. **5**, p. 523-532.

[36] Stepanov S.A., Codes on fibre products of hyperelliptic curves, *Discr. Math. Appl.* , to appear.

[37] Stepanov S.A., *Codes on Algebraic Curves* , to be published.

[38] Stepanov S.A., Özbudak F., Fibre products of hyperelliptic curves and geometric Goppa codes, *Discr. Math. Appl.* , 1995.

[39] Stepanov S. A., Özbudak F., Fibre products of superelliptic codes and codes therefrom, *Preprint*, 1996.

[40] Stichtenoth H., *Algebraic Function Fields and Codes* , Springer-Verlag, Berlin, 1993.

[41] Stöhr K.O, Voloch J.F., Weierstrass points and curves over finite fields, *Proc. London Math. Soc.* (3), 1986, **52**, p. 1-19.

[42] Tietäväinen A., Covering radius and dual distance, *Designs, Codes and Crypt.* , 1991, **1**, p. 31-36.

[43] Tsfasman M. A., Vladut S. G., *Algebraic-Geometric Codes* , Kluwer Acad. Publ, Dordrecht, 1991.

[44] Tsfasman M. A., Vladut S. G., Zink Th., Modular curves, Shimura curves, and Goppa codes, *Math. Nachr.* , 1982, **109**, p. 21-28.

[45] Weil A., On some exponential sums, *Proc. Nat. Acad. Sci. U.S.A* , 1948, **34**, p. 204-207.

[46] Wolfmann J., The number of points on certain algebraic curves over finite fields, *Comm. Algebra* , 1989, **17** (8), p. 2055-2060.

[47] Zink Th., Degeneration of Shimura surfaces and a problem in coding theory, *Lect. Notes on Comp. Sci.* , 1986, **199**, p. 503-511.