Tr. J. of Mathematics
22 (1998) , 223 – 234.

CODES ON SUPERELLIPTIC CURVES*

F. Özbudak & Glukhov

Abstract

The purpose of this paper is to apply superelliptic curves with a lot of rational points to construct rather good geometric Goppa codes.

1. Introduction

Let $F_p \subset F_q$ be a Galois extension of prime field F_p. A. Weil [9] proved that if $f(x,y) \in F_q[x,y]$ is an absolutely irreducible polynomial and if N_q denotes the number of F_q-rational points of the curve defined by the equation $f(x,y)=0$, then

$$|N_q - (q+1)| \leq 2gq^{1/2},$$

where g is genus of the curve. As a corollary we have that, if m is the number of distinct roots of f in its splitting field over F_q, χ is a non-trivial multiplicative character of exponent s and f is not an s-th power of a polynomial, then

$$|\sum_{x \in F_q} \chi(f(x))| \leq (m-1)q^{1/2}.$$

S.A. Stepenov [2] proved the existence of a square-free polynomial $f(x) \in F_p[x]$ of degree $\geq 2(\frac{(N+1)\log 2}{\log p}+1)$ for which

$$\sum_{i=1}^{N} (\frac{f(x)}{p}) = N,$$

where $\{1,\ldots,N\} \subset F_p$ and $(\frac{\cdot}{p})$ is the Legendre symbol and $(p,2)=1$. Later, F. Özbudak [8] extended this to arbitrary non-trivial characters of arbitrary finite fields by following

*The first author is now with the Department of Mathematics, Middle East Technical University, e-mail: ozbudak@mat.metu.edu.tr

Stepanov's approach. This gives a constructable proof of the fact that Weil's estimate is almost attainable for any F_q.

In [3], Stepanov introduced some special sums $S_\nu(f) = \sum_{x \in F_{q^\nu}} \chi(f(x))$ with a nontrivial quadratic character χ by explicitly representing the polynomial $f(x)$, whose, absolute values are very close to Weil's upper bound. M. Glukhov [6], [7] generalized Stepanov's approach to the case of arbitrary multiplicative characters over arbitrary finite field F_q.

Recall the basic ideas of the Goppa construction (see for example [1] or [5]) of linear $[n, k, d]_q$ codes associated to a smooth projective curve X 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 whose support is disjoint from D_0. Consider the following vector space of rational functions on X:

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

The linear $[n, k, d]$ code $C = C(D_0, D)$ associated to the pair (D_0, D) is the image of the linear evaluation map

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

Such a q-ary linear code is called a geometric Goppa code. If deg $D < n$ then Ev is an embedding, hence by Riemann-Roch theorem.

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

Moreover we have

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

In this paper we apply the Goppa construction to the curve given over F_q by

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

where $s \mid (q-1)$ and the polynomial $f(x)$ is obtained by Stepanov's approach to attain

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

where χ is a non-trivial multiplicative character of exponent s. Moreove, we apply the Goppa construction also to the polynomials $f(x)$ given in Glukhov's paper [6], [7] explicitly after some modification.

Theorem 1 *Let F_q be a finite fields of characteristic p, s an integer $s \geq 2, s|(q-1)$, and c be the infimum of the set*

$$C = \{x : \text{a non-negative real number} \mid \text{there exists an integer } n \text{ such that}$$
$$\frac{q^x(q-2)}{(q-1)(s-1)(1+\frac{1}{s^q(s-1)})} \geq n \geq \frac{q \log s}{\log q} + x\}.$$

Let r be an integer satisfying

$$s(s-1)\lceil \frac{q \log s}{\log q} \rceil - 2s < r < sq.$$

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

$$n = sq$$
$$k = r - \frac{s(s-1)}{2}\lceil \frac{q \log s}{\log q} + c \rceil + s,$$
$$d \geq sq - r.$$

Corollary 1 *Under the same conditions with Theorem 1, there exist a code with relative parameters satisfying*

$$R \geq 1 - \delta \frac{\frac{s(s-1)}{2}\lceil \frac{q \log s}{\log q} + c \rceil - s}{sq}.$$

By applying the same procedure to polynomials given explicitly by Glukhov [6], we get the following theorem.

Theorem 2 *Let F_q be a finite field of characteristic p, F_{q^ν} an extension of F_q of degree ν, s an integer $s \geq 2, s|(q-1)$. Moreover,* *i) if* $p \neq 2,\ \nu > 1$ *an odd integer and* r *an integer satisfying*

$$(s-1)(1+q)q^{\frac{\nu-1}{2}} - 4s + 2 < r < sq^{\nu},$$

then there exists a linear code $[n,k,d]_{q^{\nu}}$ *with parameters*

$$\begin{aligned} n &= sq^{\nu}, \\ k &= r + 2s - (s-1)\frac{(1+q)}{2}q^{\frac{\nu-1}{2}} - 1, \\ d &\geq sq^{\nu} - r; \end{aligned}$$

ii) if $p \neq 2,\ \nu < 2$ *an even integer and* r *an integer satisfying conditions*

a) when $4 \not| \nu$

$$(s-1)(1+q^2)q^{\frac{\nu}{2}-1} - 4s + 2 < r < sq^{\nu},$$

then there exists a linear code $[n,k,d]_{q^{\nu}}$ *with parameters*

$$\begin{aligned} n &= sq^{\nu}, \\ k &= r + 2s - (s-1)\frac{(1+q^2)}{2}q^{\frac{\nu}{2}-1} - 1, \\ d &\geq sq^{\nu} - r; \end{aligned}$$

b) when $4 \mid \nu$

$$(s-1)(1+q^2)q^{\frac{\nu}{2}-1} - 2(s-1)q - 2s < r < sq^{\nu},$$

then there exists a linear code $[n,k,d]_{q^{\nu}}$ *with parameters*

$$\begin{aligned} n &= sq^{\nu}, \\ k &= r + (s-1)q + s - (s-1)\frac{(1+q^2)}{2}q^{\frac{\nu}{2}-1}, \\ d &\geq sq^{\nu} - r; \end{aligned}$$

iii) if $p = 2,\ \nu > 1$ *on odd integer and* r *an integer satisfying*

$$(s-1)(1+q)q^{\frac{\nu-1}{2}} - 2(s-1)q - 2s < r < sq^{\nu},$$

then there exists a linear code $[n,k,d]_{q^\nu}$ *with parameters*

$$\begin{aligned} n &= sq^\nu, \\ k &= r + (s-1)q + s - (s-1)(1+q)^{\frac{q^{\frac{\nu-1}{2}}}{2}}, \\ d &\geq sq^\nu - r; \end{aligned}$$

iv) if $p = 2$, $\nu > 2$ *an even integer and* r *an integer satisfying conditions*

a) when $4 \not| \nu$

$$(s-1)(1+q^2)q^{\frac{\nu}{2}-1} - 2(s-1)q^2 - 2s < r < sq^\nu,$$

then there exists a linear code $[n,k,d]_{q^\nu}$ *with parameters*

$$\begin{aligned} n &= sq^\nu, \\ k &= r + (s-1)q^2 + s - (s-1)(1+q^2)^{\frac{q^{\frac{\nu}{2}-1}}{2}}, \\ d &\geq sq^\nu - r; \end{aligned}$$

b) when $4|\nu$

$$(s-1)(1+q^2)q^{\frac{\nu}{2}-1} - 2(s-1)q - 2s < r < sq^\nu,$$

then there exists a linear code $[n,k,d]_{q^\nu}$ *with parameters*

$$\begin{aligned} n &= sq^\nu, \\ k &= r + (s-1)q + s - (s-1)(1+q^2)^{\frac{q^{\frac{\nu}{2}-1}}{2}}, \\ d &\geq sq^\nu - r. \end{aligned}$$

Corollary 2 *Under the same conditions with Theorem 2, there exist codes with relative parameters satisfying, respectively,*

i)

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

ii.a)

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

ii.b)

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

iii)

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

iv.a)

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

iv.b)

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

Remark 1 *When $s << q$, we have for Corallary 1*

$$R \geq 1 - \delta - J_1(s,q),$$

where $J_1(s,q) \sim \frac{(s-1)\log s}{2}\frac{1}{\log q}$ and for Corollary 2

$$R \geq 1 - \delta - J_2(s,q^\nu),$$

where $J_2(s,q^\nu) \sim \frac{(s-1)}{2s}\frac{1}{q^{\frac{\nu-1}{2}}}$. Although $\frac{1}{q^{\frac{1}{2}}} << \frac{1}{\log q}$, Theorem 1 is significant especially when q is a prime. Indeed good codes are designed over $F_q, q = p^\nu, \nu > 1$ since curves with large $\frac{N_q}{2}$ ratio are obtained using the structure of Galois group of F_q over some subfield $F_{q'}$ where N_q is number of F_q rational points and g is the genus of the curve that Goppa construction is applied. Our result is an explicit construction of codes over $F_{p,p}$: prime, with good $\frac{N_q}{g}$ ratio since we have for general finite fields only Serre's lower bound: there exists $c > 0$ such that $\lim_{g\to\infty}\frac{N_q}{g} < c\log q$ for all q.

Remark 2 *The parameters of Theorem 2 are rather good. Moreover, it is possible to calculate directly the minimum distance d exactly in some cases. For example, we have such codes which are near to Singleton bound:*

i: *Over* $F_{27} \supset F_3$ *if* $6 < r < 54$, *then it gives* $[54, r-3, d]_{27}$ *code where* $d \geq 54 - r$. *If* r : *even, then* $d = 54 - r$ *(see Stichtenoth [10], Remark 2.2.5).*

ii.a: *Over* $F_{729} \supset F_3$ *if* $84 < r < 1458$, *then it gives* $[1458, r-42, d]_{729}$ *code where* $d \geq 1458 - r$. *If* r: *even, then* $d = 1458 - r$.

ii.b: *Over* $F_{81} \supset F_3$ *if* $20 < r < 162$, *then it gives* $[162, r-10, d]_{81}$ *code where* $d \geq 162 - r$. *If* r: *even, then* $d = 162 - r$.

iii: *Over* $F_{64} \supset F_4$ *if* $18 < r < 192$, *then it gives* $[192, r-9, d]_{64}$ *code where* $d \geq 192 - r$. *If* $r \equiv 0$ *mod 3, then* $d = 192 - r$.

iv.a: *Over* $F_{4096} \supset F_4$ *if* $474 < r < 12288$, *then it gives* $[12288, r-237, d]_{4096}$ *code where* $d \geq 12288 - r$. *If* $r \equiv 0$ *mod 3, then* $d = 12288 - r$.

iv.b.: *Over* $F_{256} \supset F_4$ *if* $114 < r < 768$, *then it gives* $[768, r-57, d]_{256}$ *code where* $d \geq 768 - r$. *If* $r \equiv 0$ *mod 3, then* $d = 768 - r$.

For ν: *even there are Hermitian codes (see for exmple Stichtenoth [10], section 7.4) which are maximal. Theorem 2 provides codes with parameters near to the parameters of maximal curves in these cases.*

2. Proof of Theorem 1

Let χ be a multiplicative character of exponent s of F_q. If $m \geq \frac{q \log s}{\log q} + c$, then $\frac{1}{m} q^m \frac{q-2}{q-1} \geq (s-1)s^q + 1$. Note that the number of monic irreducible polynomials of degree m over F_q is $\frac{1}{m} \sum_{d|m} \mu(d) q^{m/d} = \frac{1}{m} q^m c_m$ (see for example [11] page 93). Here $1 \geq c_m \geq 1 - \frac{q^m - q}{q^m(q-1)} \geq \frac{q-2}{q-1}$. Forming q-tuples for each irreducible monic polynomial as in Stepanov [2] or Özbudak [8], by Dirichlet's pigeon-hole principle if $\frac{1}{m} q^m \frac{q-2}{q-1} \geq (s-1)s^q + 1$, there exists a sequare-free polynomial $f \in E_q|x]$ of degree $\leq ms$ such that $\chi(f(a)) = 1$ for each $a \in F_{q.}$ Let deg $f = s\lceil \frac{2 \log s}{\log q} + c \rceil$.

Since $s \mid (q-1)$ there are s many multiplicative characters of exponent s over F_q.

Moreover for any χ of exponent $s, \chi(f(a)) = 1$ for all $a \in F_q$. Therefore we have over the curve

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

$N_q = sq$ many F_q-rational points (see Schmidt [12] page 79 or Stepanov [4], p. 51).

Using the well-known genus formulas for superelliptic curves (see for example Stichtenoth [10] p. 196), the geometric genus is given by

$$g = \frac{s(s-1)}{2}\lceil \frac{q \log s}{\log q} + c \rceil - s + 1.$$

Let D_0 be the divisor on the smooth model X of $y^s = f(x)$, where

$$D_0 = \sum_1^n x_i.$$

By tracing the normalization of a curve one see that the number of rational points of the non-singular model X of the curve $y^s = f(x)$ is not less than the number of rational points of $y^s = f(x)$ (see for example Shafarevich [13], section 5.3). Thus $n = \deg D_0 \geq N_q = sq$. Let x_∞ be a point of X at infinity, $D = rP_\infty$ be the divisor of degree r and $suppD_0 \cap suppD = \emptyset$, where r to be determined. If

$$2g - 2 < r < N_q,$$

by using the Goppa construction,

$$n = N_q, \;\; k = r + 1 - g, \;\; d \geq N_q - r.$$

3. Proof of Theorem 2

Let $\chi_{\nu,s}(x) = \chi_s(norm_\nu(x))$ where χ_s is a non-trivial multiplicative character of F_q of exponent s, $norm_\nu = x.x^q \ldots..x^{q^{\nu-1}}$. Therefore $\chi_{\nu,s}$ is a relative multiplicative character of F_{q^ν} of exponent s. For $f(x) \in F_{q^\nu}[x]$ denote by $S_\nu(f)$ the sum $S_{\nu,s}(f) = \sum_{x \in F_{q^\nu}}(f(x))$.

Case(i):

There exists a polynomial $f_1(x) \in F_{q^\nu}[x]$

$$f_1(x) = (x + x^{q^{\frac{\nu-1}{2}}})^a (x + x^{x^{\frac{\nu+1}{2}}})^b,$$

where $a+b=s, a\neq b$, and $(a,s)=1$ such that $S_{\nu,s}(f_1)=q^\nu-1$ (Glukhov [7]).

We can write

$$f_1(x)=x^s(1+x^{q^{\frac{\nu-1}{2}}-1})^a(1+x^{q^{\frac{\nu+1}{2}}-1})^b.$$

Consider $y^s=f_1(x)$. This curve is birationally isomorphic to

$$y^s=f_{1,1}(x)=(1+x^{q^{\frac{\nu-1}{2}}-1})^a(1+x^{q^{\frac{\nu+1}{2}}-1})^b,$$

and $S_{\nu,s}(1_{1,1})=q^\nu$. Moreover, we know

1. $1+x^m$ where $(m,q)=1$ is a square-free polynomial over F_{q^ν},
2. If ν is odd, then $(1+x^{q^{\frac{\nu-1}{2}}-1}, 1+x^{q^{\frac{\nu+1}{2}}-1})=1$ over F_{q^ν} for $p\neq 2$.

Therefore we can apply Hurwitz genus formula (see for example Stichtenoth ([10], p. 196); hence we get

$$g=(s-1)\frac{(1+q)}{2}q^{\frac{\nu-1}{2}}-2(s-1).$$

Over the curve $y^s=f_{1,1}(x)$ there are

$$N_{q^\nu}=\sum_{\exp\chi=s}\sum_{x\in F_{q^\nu}}\chi_s(f_{1,1}(x))=q^\nu+(s-1)S_{\nu,s}(f_{1,1})=sq^\nu$$

many F_{q^ν}-rational points (Stepanov [4], p. 51). Therefore we get the desired result as in the proof of Theorem 1.

Case(ii):

We apply the same techniques to

$$f_2(x)=x^s(1+x^{q^{\frac{\nu}{2}-1}-1})^a(1+x^{q^{\frac{\nu}{2}+1}-1})^b$$

given by Glukhov [7]. Here $S_{\nu,s}(f_2)=\begin{cases} q^\nu-1 & \text{if} \quad 4\not|\nu \\ q^\nu-q & \text{if} \quad 4\,|\,\nu\end{cases}$. Moreover, if $\nu\equiv 2 \bmod 4$, then $(1+x^{q^{\frac{\nu}{2}-1}-1}, 1+x^{q^{\frac{\nu}{2}+1}-1})=1$; and if $\nu\equiv 0 \bmod 4$, then $(1+x^{q^{\frac{\nu}{2}-1}-1}, 1+x^{q^{\frac{\nu}{2}+1}-1})=1+x^{q-1}$ over F_{q^ν} for $p\neq 2$. If $\nu\equiv 2 \bmod 4$, similarly consider the curve

$$y^s=f_{2,2,1}(x)=(1+x^{q^{\frac{\nu}{2}-1}-1})^a(1+x^{q^{\frac{\nu}{2}+1}-1})^b$$

whose genus is

$$g = (s-1)\frac{1+q^2)}{2}q^{\frac{\nu}{2}-1} - 2(s-1),$$

and $S_{\nu,s}(f_{2,2,1}) = q^\nu$. If $\nu \equiv 0 \bmod 4$ we can write $f_2(x)$ here as

$$f_2(x) = x^s(1+x^{q-1})^s(\frac{1+x^{q^{\frac{\nu}{2}-1}-1}}{1+x^{q-1}})^a(\frac{1+x^{q^{\frac{\nu}{2}+1}-1}}{1+x^{q-1}})^b.$$

The curve $y^s = f_2(x)$ is birationally isomorphic to the curve

$$y^s = f_{2,2,2}(x) = (\frac{1+x^{q^{\frac{\nu}{2}-1}-1}}{1+x^{q-1}})^a(\frac{1+x^{q^{\frac{\nu}{2}+1}-1}}{1+x^{q-1}})^b$$

whose genus is

$$g = (s-1)\frac{(1+q^2)}{2}q^{\frac{\nu}{2}-1} - (s-1)(1+q)$$

and $S_{\nu,s}(f_{2,2,2}) = q^\nu$

Case(iii):

We apply the same techniques observing that in this case we have the following additional fact that

If $p=2$, then $(1+x^k, 1+x^l) = 1+x^{(k,l)}$, where $1+x^k, 1+x^l \in F_{q^\nu}[x]$.

We can write $f_1(x)$ here as

$$f_1(x) = x^s(1+x^{q-1})^s(\frac{1+x^{q^{\frac{\nu-1}{2}}-1}}{1-x^{q-1}})^a(\frac{1+x^{q^{\frac{\nu+1}{2}}-1}}{1+x^{q-1}})^b.$$

The curve $y^s = f_1(x)$ is birationally isomorphic to the curve

$$y^s = f_{1,3}(x) = (\frac{1+x^{q^{\frac{\nu-1}{2}}-1}}{1+x^{q-1}})^a(\frac{1+x^{q^{\frac{\nu+1}{2}}-1}}{1+x^{q-1}})^b.$$

The genus is

$$g = (s-1)(1+q)\frac{q^{\frac{\nu-1}{2}}}{2} - (s-1)(1+q).$$

Moreover, $S_{\nu,s}(f_1) = q^\nu - q$ (see [7]), and hence $S_{\nu,s}(f_{1,3}) = q^\nu$.

Case (iv):
We apply the same techniques as in Case(iii). We have

$$(q^{\frac{\nu}{2}-1}-1, q^{\frac{\nu}{2}+1}-1) = \begin{cases} q^2-1 & \text{if} \quad 4 \not| \nu, \\ q-1 & \text{if} \quad 4 \,|\, \nu. \end{cases}$$

Thus when $4 \not| \nu, y^s = f_2(x)$ is birationally isomorphic to

$$y^s = f_{2,4,1}(x) = (\frac{1+x^{q^{\frac{\nu}{2}-1}-1}}{1+x^{q^2-1}})^a(\frac{1+x^{q^{\frac{\nu}{2}+1}-1}}{1+x^{q^2-1}})^b$$

and the genus is

$$g = (s-1)(1+q^2)\frac{q^{\frac{\nu}{2}-1}}{2} - (s-1)(1+q^2).$$

Moreover, $S_{\nu,s}(f_2) = q^\nu - q^2$ (see [7]), and hence $S_{\nu,s}(f_{2,4,1}) = q^\nu$.

When $4 \,|\, \nu, y^s = f_2(x)$ is birationally isomorphic to

$$y^s = f_{2,4,2}(x) = (\frac{1+x^{q^{\frac{\nu}{2}-1}-1}}{1+x^{q-1}})^a(\frac{1+x^{q^{\frac{\nu}{2}+1}-1}}{1+x^{q-1}})^b,$$

whose genus is

$$g = (s-1)(1+q^2)\frac{q^{\frac{\nu}{2}-1}}{2} - (s-1)(1+q),$$

and $S_{\nu,s}(f_2) = q^\nu - q(see[7])$, and hence $S_{\nu,s}(f_{2,4,2}) = q^\nu$.

Acknowledgment

We would like to thanks to S.A. Stepanov for his excellent guidance, comments, and suggestions in this work.

References

[1] V. G. Goppa, "Codes on algebraic curves", Soviet Math. Dokl., 1981, 24, 170-172.

[2] S. A. Stepanov, "On lower estimates of incomplete character sums of polynomials", Proceedings of the Steklov Institute of Mathematics, AMS, 1980 Issue 1, 187-189.

[3] S. A. Stepanov, "On lower bounds of sums of characters over finite fields", Discrete Math. Appl., 1992, Vol. 2, no. 5, 523-532.

[4] S. A. Stepanov, "Arithmetic of Algebraic Curves", Plenum, 1994.

[5] S. A. Stepanov, "Error-Correcting Codes and Algebraic Curves" CRC Press, to be published.

[6] M. Glukhov, "Lower bounds for character sums over finite fields", Diskrt. Math., 1994, 6, no. 3, 136-142 (in Russian).

[7] M. Glukhov, "On lower bounds for character sums over finite fields", preprint.

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

[9] A. Weil, "Numbers of solutions of equations in finite fields", Bull. of the American Math. Soc., 55 (1949), 497-508.

[10] H. Stichtenoth, "Algebraic Function Fields and Codes", Springer-Verlag, 1993.

[11] R. Lidl and H. Niederreiter, "Finite Fields", Encyclopedia of Mathematics and It's Applications vol 20, Cambridge University Press, 1984.

[12] W. Schmidt, "Equations over Finite Fields - An Elementary Approach", Lecture Notes in Mathematics, Springer-Verlag, 1976.

[13] I. R. Shafarevich, "Basic Algebraic Geometry 1", second edition, Springer-Verlag, 1994.

Ferruh ÖZBUDAK
Department of Mathematics
Bilkent University
06533, Ankara - TURKEY
&
Michael GLUKHOV
Faculty of Computer Science and Cybernetics,
Moscow State University
e-mail: mathcyb@cs.msu.su

Received 25.08.1997