Fibre Products of Superelliptic Curves and Codes Therefrom

Serguei A. Stepanov and Ferruh Özbudak

Serguei A. Stepanov: Dept. of Mathematics, Bilkent University, 06533 Ankara, Turkey and
Steklov Mathematical Institute, Vavilov st. 42, Moscow GSP-1, 117966 Russia
Email: stepanov@fen.bilkent.edu.tr
Ferruh Özbudak: Dept. of Mathematics, Bilkent University, 06533 Ankara, Turkey
Email ozbudak@fen.bilkent.edu.tr

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

Let X be a smooth projective curve of genus $g = g(X)$ defined over a finite field F_q. The Goppa construction of linear $[n,k,d]_q$-codes associated to the curve X can be briefly described as follows. Let $\{x_1,\dots,x_n\}$ be a set of F_q-rational points on X and

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

Let D be a F_q-rational divisor on X such that Supp $D_0 \cap$ Supp $D = \emptyset$, and $F_q(X)$ the field of rational functions on X. 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 to the pair (D_0, D) is the image of the linear evaluation map

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

Such a q-ary linear code is called a geometric Goppa code. If $\deg D < n$, the map Ev is an injection, so $C \simeq L(D)$. It follows from the Riemann-Roch theorem that the relative parameters $R = k/n$ and $\delta = d/n$ of the code C satisfy

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

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

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

one needs a family of smooth projective curves with a lot of F_q-rational points compared to the genus. Examples of such families are provided by modular curves (Ihara, Tsfasman-Vladut-Zink, C. Moreno), by Drinfeld modular curves (Tsfasman), and by Artin-Schreier coverings of the projective line $\mathbb{P}(F_q)$ (Garcia-Stichtenoth). As a result, one can construct an infinite sequence of geometric Goppa codes C_i over F_q (q is a square), which gives the lower bound

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

The line $R = 1 - \delta - (\sqrt{q} - 1)^{-1}$ intersects the curve $R = 1 - H_q(\delta)$ for $q \geq 49$.

Our purpose is to construct rather long geometric Goppa codes coming from fibre products of superelliptic curves X_s given over F_q by equations

$$z_i^{\mu} = f_i(u), \qquad 1 \leq i \leq s \ ,$$

where $f_i(u)$ are pairwise coprime polynomials of the same degree $m \geq 1$. We can exactly find a basis of the space of regular differential forms on X_s. This gives an easy way to calculate the genus of the smooth projective curve X_s. For example, if $\mu = 2$ and the polynomials $f_i(u)$, $1 \leq i \leq s$, are square-free, we have

$$g(X) = \begin{cases} (ms-3)2^{s-2}+1 & \text{if } m \equiv 1 \pmod 2 \\ (ms-4)2^{s-2}+1 & \text{if } m \equiv 0 \pmod 2 \end{cases} \ .$$

On the other hand, we can choose the polynomials $f_i(u)$ in such a way to provide a lot of F_q-rational points on X_s. So, if $\mu = 2$, $q = p^{\nu}$ ($p = \mathrm{char}\ F_q > 2$), then for some special polynomials $f_i(u)$, $1 \leq i \leq s$, the number $N_q = N_q(X_s)$ of F_q-rational points on X_s satisfies

$$N_q \geq \begin{cases} (2q^{1/2} - s)q^{1/2}2^{s-1} & \text{if } \nu \equiv 0 \pmod 2 \\ 2^s q & \text{if } \nu \equiv 1 \pmod 2 \end{cases} \ .$$

Setting $n = N_q$ and using the Goppa construction we obtain

$$R \geq 1 - \delta - \frac{sq^{1/2} - 3}{2(2q^{1/2} - s)q^{1/2}}, \quad \text{for} \quad \nu \equiv 0 \pmod 2$$

and

$$R \geq 1 - \delta - \frac{sq^{1/2} - 4}{4q}, \quad \text{for} \quad \nu \equiv 1 \pmod 2 \ .$$

Unfortunately, the parameter s in our construction is bounded by $q^{1/2}$, and as a result the genus $g = g(X_s)$ is bounded by

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

However, since the above upper bound is large enough for $q \geq q_0$, the curves X_s provide suffuciently long geometric Goppa codes with rather good parameters. Moreover, these codes have very easy construction and decoding algorithms. We note also, that this approach, being extended to the case $\mu > 2$, gives a possibility to construct rather good linear codes in arbitrary characteristic $p \geq 2$ (sometimes with better parameters than in the case $\mu = 2$).

0-7803-3956-8/97/$10.00