Artin–Schreier curves, exponential sums, and coding theory*

Gilles Lachaud

Équipe C.N.R.S. "Arithmétique et Théorie de l'Information", C.I.R.M., Luminy Case 916, 13288 – Marseille Cedex 9, France

Abstract


This is a survey of some results recently obtained on the distribution of the weights of some classical linear codes on the one hand, such as the dual of the Melas code, and the geometric BCH codes discovered by Goppa (subfield subcodes of Goppa codes) on the other hand. These results depend upon the properties of certain algebraic curves defined over a finite field, and the associated exponential sums, such as the Kloosterman sums.

0. Prelude

There is an organic connection between exponential sums and the number of points of curves defined over finite fields, and this connection is central in the application of algebraic geometry to coding theory. As an illustration, we recall the simple trick below, which is a particular and elementary case of the results developed in Section 1.

In what follows, we let $q$ be a power of a prime number $p$; we denote by $\mathbb{F} = \mathbb{F}_q$ the field with $q$ elements. For $x \in \mathbb{F}$ we denote the trace map of the extension $\mathbb{F}/\mathbb{F}_p$ by

$$\text{Tr}_{q/p}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{q-1}}.$$ 

If $\psi$ is an additive character of $\mathbb{F}_q$ and if $x \in \mathbb{F}$, we set

$$\psi_q(x) = \psi(\text{Tr}_{q/p}(x));$$

then $\psi_q$ is an additive character of $\mathbb{F}$.

Let $f \in \mathbb{F}[X]$ and consider the affine Artin–Schreier curve

$$X : y^p - y = f(x);$$

*This paper is mainly a summary of the results given in [13–17].
and let

\[ X(F) = \{(x, y) \in F \times F \mid y^p - y = f(x)\} \]

be the set of points of that curve which are defined over \( F \). If \( f \in F[X] \), define the exponential sum

\[ W_\psi(F, f) = \sum_{x \in F} \psi_x(f(x)). \]

**Theorem 0.1.** If \( \psi \) is nontrivial and \( K = \mathbb{Q}(e^{2i\pi/p}) \), then

\[ \# X(F) = q + \text{Tr}_{K/Q} W_\psi(F, f). \]

**Proof.** If \( w \in F \), consider

\[ \sum_{\psi} \psi_q(\text{Tr}_{q/p}(w)) = \text{Tr}_{K/Q} \psi(w), \]

where the sum is over the nontrivial additive characters of \( F \); the value of this sum is \( q \) or 0 according to whether \( \text{Tr}_{q/p}(w) = 0 \) or not by orthogonality of the characters. On the other hand, the number of \( y \in F \) with \( y^p - y = w \) is also equal to \( q \) or 0 according to whether \( \text{Tr}_{q/p}(w) = 0 \) or not by Hilbert Theorem 90. Then

\[ \# X(F) = \sum_{\psi} \sum_x \psi_q(f(x)) = \sum_{\psi} W_\psi(F, f), \]

and we are done, taking into account the trivial character. \( \square \)

1. **Artin–Schreier curves and exponential sums**

1.1. **Artin–Schreier theory**

If \( K \) is any field of characteristic \( p \), it is well-known [2, 18] that the Artin–Schreier equation

\[ T^p - T - a = 0 \]

is either irreducible, or has one root in \( K \), in which case all its roots are in \( K \). We denote by \( \varphi \) the endomorphism of \( K \) such that

\[ \varphi(x) = x^p - x. \]

Let \( \Omega \) be an algebraic closure of \( K \); if \( A \subset K \), we denote by \( K(\varphi^{-1}A) \) the extension of \( K \) generated by the \( x \in \Omega \) such that \( \varphi(x) \in A \). Now, let \( K \) be a function field in one
variable over the finite field $F$. We call a finite subgroup $A_0$ of $K$ nondegenerate if

$$A_0 \cap (\varphi K + F) = \{0\}.$$

**Proposition 1.1.** Let $A_0$ be a finite subgroup of $K$; then the extension $L = K(\varphi^{-1} A_0)$ is a regular extension of $F$ if and only if $A_0$ is nondegenerate.

Let $X$ be a smooth absolutely irreducible projective curve defined over $F$ with function field $K$. Assume that $A_0$ is a nondegenerate finite subgroup of $K$; let $Y$ be a smooth model of $L$. Take a basis $(f_1, \ldots, f_r)$ of the $F_p$ vector space $A_0$; an affine model of $Y$ is the curve on $\mathbb{A}^r \times X$, where $\mathbb{A}^r$ is the affine space of dimension $r$, given by the system of equations

$$y_i^p - y_i = f_i(x) \quad (1 \leq i \leq r).$$

The injection $K \to L$ defines an abelian $F$-covering

$$\pi: Y \to X,$$

with Galois group $G$, and we have $X = Y/G$. Under these conditions, we call $\pi: Y \to X$ an Artin–Schreier $F$-covering.

As an example, let $F_r$ be an intermediate field between $F_p$ and $F = F_q$:

$$F_p \subset F_r \subset F_q$$

(this means that $q$ is a power of $r$); the smooth model of the curve defined in $\mathbb{A}^1 \times X'$ by the equation

$$Y': y' - y = f(x),$$

where

$$X' = \{x \mid f \text{ has a pole at } x\}$$

is absolutely irreducible if and only if the subgroup $A_0 = fF_r$ is nondegenerate, i.e. if

$$f \not\in F_r, \varphi(K) + F.$$ 

1.2. Exponential sums and $L$ functions

Let $K$ be, as before, a function field of one variable over $F$ which is a regular extension of $F$, and let $X$ be a smooth model of $K$. If $f \in K$, define the exponential sum

$$W(F, f) = \sum_{x \in X(F)} \psi(f(x)).$$

The numbers $W(F, f)$ are contained in the ring $\mathbb{Z}[\zeta_p]$ of integers of the cyclotomic field $\mathbb{Q}(\zeta_p)$ of $p$th roots of unity. We now modify the preceding sum according to Deligne.
For any place \( u \) of \( K \), denote by \( \mathfrak{o}_u \) the subring of \( K \) of functions regular at \( u \). For \( f \in K \), set
\[
\nu_u(f) = \begin{cases} 
0 & \text{if } f \in \mathfrak{o}_u, \\
\text{order of the pole of } f \text{ at } u & \text{if } f \notin \mathfrak{o}_u, \\
\nu_u^*(f) = \min \{ \nu_u(f-g) \mid g \in \mathfrak{o} K \} 
\end{cases}
\]
the function \( \nu_u^* \) is defined on \( K / \mathfrak{o} K \), and \( \nu_u^*(f) = 0 \) if and only if \( f \in \mathfrak{o}_u + \mathfrak{o} K \). We call \( \nu_u^*(f) \) the reduced order of the pole of \( f \) at the place \( u \); this dates back to Artin.

We denote by \( X^* \) the open set of \( X \) containing all the \( x \in X \) which are at a place \( u \) such that \( \nu_u^*(f) = 0 \). It is clear that \( X'(F) \subset X^*(F) \). If \( x \in X^*(F) \) and if \( f = h + g^p - g \), with \( h \) regular at \( x \), we set
\[
\psi^*(f(x)) = \psi(h(x)), \quad W^*(F, f) = \sum_{x \in X^*(F)} \psi^*(f(x)),
\]
and
\[
L^*(T, f) = \exp \left( \sum_{s=1}^{\infty} \frac{T^s}{s} W^*(F(s), f) \right),
\]
where \( F(s) \) is the extension of the degree \( s \) of \( F \).

Take a nondegenerate finite subgroup \( A_0 \) of \( K \); let \( L = K(\varrho^{-1} A_0) \), let \( Y \) be the smooth model of \( L \), and consider the Artin–Schreier \( F \)-covering \( \pi: Y \rightarrow X \). Let \( A_0 = A_0 - \{0\} \); then
\[
Z_Y(T) = Z_X(T) \prod_{f \in A_0} L^*(T, f),
\]
and
\[
\# Y(F) - \# X(F) = \sum_{f \in A_0} W^*(F, f).
\]
As a corollary, we thus get that if \( f \notin \mathfrak{o} K + F \), then we have
\[
W^*(F, f) = - \sum_{i=1}^{C(f)} z_i(f),
\]
with
\[
C(f) = 2g_X - 2 + \sum_{u \in \text{U}^*(f)} (\nu_u^*(f) + 1) \deg u,
\]
where the numbers \( z_i(f) \) are algebraic integers such that \( z_i(f) \bar{z}_i(f) = \sqrt{q} \); hence, we get the following estimate of Weil [30, 31] in the case given by Deligne [4] (cf. also [26]): if \( f \notin \mathfrak{o} K + F \), then
\[
|W^*(F, f)| \leq C(f) \sqrt{q}.
\]
The following result shows that the Deligne bound can be sharpened if one groups the terms together. With the help of a trick of Serre [27], we get the following theorem.
Theorem 1.2. If $A_0$ is a nondegenerate finite subgroup of order $r$ of the function field $K$ of the absolutely irreducible curve $X$, then

$$\left| \sum_{f \in A_0} W^*(F,f) \right| \leq \frac{B(A_0)}{2} [2\sqrt{q}].$$

with

$$B(A_0) = 2(g_Y - g_X) = \sum_{f \in A_0} C(f).$$

As a consequence of this theorem, we get the following corollaries.

Corollary 1.3. Let $\pi: Y \to X$ be an Artin-Schreier $F$-covering; then

$$|\# Y(F) - \# X(F)| \leq (g_Y - g_X) [2\sqrt{q}].$$

In fact, this estimate is true for any abelian $F$-covering $\pi: Y \to X$ (the proof is the same).

Corollary 1.4. If $f \not\equiv K + F$, then

$$|\text{Tr}_{F/Q} W^*(F,f)| \leq (p - 1) \frac{C(f)}{2} [2\sqrt{q}].$$

This result is used, for instance, by Wolfmann [2] in the theory of cyclic codes; actually, his questions motivated the present work.

These results have been independently obtained, for char $F = 2$ when $X$ is the projective line $\mathbb{P}^1$, by Moreno and Moreno [22], and applied to the covering radius and the minimum distance of classical Goppa codes.

2. Kloosterman sums and codes

2.1. Kloosterman sums

The Kloosterman sum is defined by

$$W_{K1}(a) = \sum_{x \in F} \psi(\text{Tr}_{q/p}(x^{-1} + ax)) \quad (a \in F^\times).$$

The sum $W_{K1}(a)$ satisfies, on the one hand, the congruence

$$W_{K1}(a) \equiv -1 \mod (1 - \zeta_p)\mathbb{Z}[[\zeta_p]]$$

and, hence,

$$\text{Tr} W_{K1}(a) \equiv -1 \pmod{p}$$
and even

\[ \text{Tr } W_{Kl}(a) \equiv p + 1 \pmod{2p}, \]

as observed by Rolland and Smadja [23]; and, on the other hand, the classical Weil inequality

\[ |W_{Kl}(a)| \leq 2\sqrt{q}. \]

Let

\[ \mathcal{E}_q = \{ K \in \mathbb{R} \cap \mathbb{Z}[\zeta_p] \mid |W| \leq 2\sqrt{q} \text{ and } W \equiv -1 \pmod{(1 - \zeta_p)\mathbb{Z}[\zeta_p]} \}. \]

The main problem here is the following: what is the image of the map \( a \to W_{Kl}(a) \) from \( \mathbb{F}_q^* \) to \( \mathcal{E}_q \)? The answer is known when \( p = 2 \) or \( p = 3 \), as we shall see.

Let \( \mathcal{E}_{Kl}(a) \) be the smooth projective model of the Kloosterman curve

\[ \mathcal{E}_{Kl}(a): \quad y^p - y = ax + \frac{1}{x}, \quad a \in \mathbb{F}_q^*. \]

This curve is smooth if \( p = 2 \). If \( p \neq 2 \), there are two points at infinity, namely, the points \( P_1 = (0:1:0) \) and \( P_2 = (1:0:0) \); there is only one singular point, namely, the point \( P_2 \), which is of order \( p - 1 \), and there is only one point above this one in a smooth covering of that curve. Hence, \( \mathcal{E}_{Kl}(a) \) is of genus \( p - 1 \).

The computations of Section 0 show that the number of rational points of the Kloosterman curves is equal to

\[ \# \mathcal{E}_{Kl}(a)(\mathbb{F}) = q + 1 + \text{Tr } W_{Kl}(a). \]

2.2. Kloosterman sums in even characteristic

In even characteristic we have

\[ W_{Kl}(a) = \sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}(x^{-1} + ax)} \quad (a \in \mathbb{F}_q^*). \]

The following theorem has been proved by Wolfmann and the author of this paper.

**Theorem 2.1.** The image of the map \( a \to W_{Kl}(a) \) from \( \mathbb{F}_q^* \) to the ring \( \mathbb{Z} \) of integers is equal to the set

\[ \{ W \in \mathbb{Z} \mid W \equiv -1 \pmod{4} \text{ and } |W| \leq 2\sqrt{q} \}. \]

When \( p = 2 \), the curve \( \mathcal{E}_{Kl}(a) \) is elliptic. Recall that an elliptic curve \( \mathcal{C} \) defined on \( \mathbb{F} \) can be defined as the locus in \( \mathbb{P}^2 \) of a cubic homogeneous equation

\[ f(x, y, z) = 0. \]
The elliptic curve $C$ is said to be \textit{supersingular} if the coefficient of $(xyz)^{p-1}$ in $f(x, y, z)^{p-1}$ is equal to 0. If $C$ is not supersingular, the curve $C$ is said to be \textit{ordinary}.

Assume that $q$ is a power of 2; we choose an element $\tau \in F$ satisfying $\text{Tr}(\tau) = 1$. We have the following result, essentially from [6].

\textbf{Theorem 2.2.} Let $C$ be an elliptic curve defined on $F$.

(a) If $C$ is supersingular, it is isomorphic over $F$ to a curve with equation

$$
y^2 + a_3 y = x^3 + a_4 x + a_6,$$

where $a_3 \neq 0$.

(b) If $C$ is ordinary, it is isomorphic over $F$ to one of the Kloosterman curves

$$
y^2 + y = ax + \frac{1}{x}, \text{ where } a \in F_q^\times,
$$

$$
y^2 + y = ax + \frac{1}{x} + \tau, \text{ where } a \in F_q^\times.
$$

We have

$$
\# \mathcal{E}_k^\pm(a)(F) = q + 1 \pm W_k(a).
$$

We know from [9] (see also the surveys of Waterhouse [29] and Schoof [24]) that there is an ordinary elliptic curve with $q + 1 - t$ points over $F$ if and only if $|t| < 2[\sqrt{q}]$ and $t$ is odd; and the curves $\mathcal{E}_k^\pm(a)$ are all the curves such that $t \equiv 1 \pmod{4}$; hence the result.

\section*{2.3. Class number of quadratic forms}

Now the question is: How many sums with a given possible value are there? This means that we have to compute, for each $t \in \mathbb{Z}$, the number of $a \in F_q^\times$ such that $W_k(a) = t$. In order to do this we use the relation between classes of binary integral positive definite quadratic forms and classes of elliptic curves as established by Honda [9].

Let $D \in \mathbb{Z}$, with $D < 0$ and $D \equiv 0$ or 1 (mod 4); denote by

$$
\text{Quad}(D) = \{ aX^2 + bXY + cY^2 \in \mathbb{Z}[X, Y] | (a, b, c) \in \mathbb{Z}^3, a > 0 \text{ and } b^2 - 4ac = D \}
$$

the set of positive definite integral binary quadratic forms with discriminant $D$, and by

$$
\text{Cl}(D) = \text{Quad}(D)/\text{PSL}(2, \mathbb{Z})
$$

the set of classes of $\text{Quad}(D)$ under the action of $\text{PSL}(2, \mathbb{Z})$ (cf. e.g. [3] for an account of the theory). The set $\text{Cl}(D)$ is finite; denote the class number by

$$
H(D) = \# \text{Cl}(D).
$$
Following Gauss, a system of representatives of \( H(D) \) in \( \text{Quad}(D) \) is given by the set of "reduced forms": a form is a reduced one if and only if

\[
(\dagger) \quad a > 0, \; b^2 - 4ac = D, \; |b| \leq a \leq c, \; \text{and} \; b \geq 0 \; \text{whenever} \; a = |b| \; \text{or} \; a = c;
\]

in other words, \( H(D) \) is the number of triples \( (a, b, c) \in \mathbb{Z}^3 \) satisfying \((\dagger)\); so, it is straightforward to compute that integer. We know from \([9]\) that if \( N(t) \) denotes the number of classes of \( F \)-isomorphisms of elliptic curves over \( F \) such that the number of points over \( F \) is equal to \( q + 1 - t \), then

\[
N(t) = H(t^2 - 4q).
\]

We have thus established the following theorem.

**Theorem 2.3.** If \( t \equiv -1 \pmod{4} \) and \( |t| \leq 2\sqrt{q} \), then

\[
\# \{ a \in F_q^* \mid W_K(a) = t \} = H(t^2 - 4q).
\]

**2.4. Kloosterman codes**

The Kloosterman code \( C_{kl}(q) \) is of length \( n = q - 1 \) and of dimension \( 2m \), and is the image of the map

\[
c : F^2 \to F_p^n
\]
given by

\[
c(a, b) = \left\{ \text{Tr}_{q/p}(ax + b) \right\}_{x \in F^*}.
\]

The code \( C_{kl}(q) \) is the dual of the Melas code. Denote by \( w(x) \) the weight of a word \( x \in C_{kl}(q) \); then

\[
w(c(0, 0)) = 0, \quad w(c(a, 0)) = w(c(0, a)) = \frac{q}{p} \quad \text{for} \; a \in F^*;
\]
the other weights of the Kloosterman code \( C_{kl}(q) \) are the numbers

\[
w(c(a, b)) = q - 1 - \# M(a, b),
\]

with

\[
M(a, b) = \# \left\{ x \in F \mid \text{Tr}_{q/p}(ax + b) = 0 \right\}.
\]

If \( u \in F \), then \( \text{Tr} u = 0 \) if and only if there exists \( y \in F \) such that \( u = y^p - y \); since in this case there are \( p \) solutions, we have

\[
M(a, b) = \frac{1}{p} \left( \# \mathcal{E}_{kl}(ab) - 2 \right).
\]
because we need to delete the two points at infinity; hence, the weights of the Kloosterman code are the numbers
\[
w(c(a,b)) = q - 1 - \frac{\# \delta_{\text{KL}}(a) - 2}{p} = q - 1 - \frac{q - 1 + W_{\text{KL}}(a)}{p};
\]
in other words,
\[
w(c(a,b)) = \frac{p - 1}{p} (q - 1) = \frac{W_{\text{KL}}(a)}{p}.
\]
Thus, from Theorem 1.2 we see that the weights of the Kloosterman code satisfy the inequality
\[
\left| \frac{w - \frac{p - 1}{p} n}{p} \right| \leq \frac{(p - 1)}{p} \left[ 2\sqrt{q} \right].
\]
Assume now that \( p = 2 \). From the results of Section 2.3 we deduce the following theorem.

**Theorem 2.4.** (a) The weights of \( C_{\text{KL}}(q) \) are all the numbers
\[
w = \frac{q - 1 - t}{2}
\]
with \( t \equiv -1 \pmod{4} \)
which lie within the interval \([w_-, w_+]\), where
\[
w_{\pm} = \frac{q - 1 \pm 2\sqrt{q}}{2}.
\]
(b) for \( t \neq 1 \), the weight \( w_t \) has frequency \((q - 1)H(t^2 - 4q)\);
(c) the weight \( w_1 = q/2 \) has frequency \((q - 1)(H(1 - 4q) + 2)\).

These results are studied in [25] from the point of view of modular forms.

2.5. Distribution of the weights of the Kloosterman codes

Now denote by \( A(w) \) the number of words of \( C_{\text{KL}}(q) \) of weight \( w \); if \( f \) is a test function (i.e. a continuous function with compact support on the real line), then
\[
\sum_{w \in C_{\text{KL}}(q)} f(w(x)) = \sum_{w = 0}^{n} A(w)f(w).
\]
If \( x \in C_{\text{KL}}(q) \), let
\[
z(x) = \frac{2w(x) - (q - 1)}{2\sqrt{q}};
\]
then \( z(x) \in [-1, +1] \). The following theorem states that the numbers \( z(x) \) are equidistributed with respect to the density function of total mass 1, i.e.

\[
\varphi(z) = \frac{2}{\pi} \sqrt{1 - z^2}
\]

in the interval \([-1, +1]\), when \( q\to\infty \).

**Theorem 2.5.** If \( f \) is a test function, then

\[
\frac{1}{q^2} \sum_{x \in C_q, \partial} f(\tau(x)) = \int_{-1}^{+1} f(\tau) \varphi(\tau) \, d\tau + O\left(\frac{1}{\sqrt{q}}\right)
\]

when \( q\to\infty \), where the hidden constant in the remainder depends only on \( f \).

**Proof.** We have

\[
\sum_{x \in C_q, \partial} f(w(x)) = f(0) + 2(q-1) f \left(\frac{q}{2}\right) + (q-1) \sum_{a \in \mathbb{F}_q} f \left(\frac{q-1-W_{K_1}(a)}{2}\right).
\]

Since \( |W_{K_1}(a)| \leq 2\sqrt{q} \), we can write

\[
W_{K_1}(a) = 2\sqrt{q} \cos \theta(a),
\]

with \( 0 \leq \theta(a) \leq \pi \). From the results of Deligne [5] and Katz [10], we know that the numbers \( \theta(a) \) are equidistributed with respect to the Sato–Tate measure \( \sin^2 \theta \, d\theta \).

Instead of the results of Deligne and Katz, we could deduce the preceding theorem from an adaptation of those of Yoshida [34]; see also [1] for a more direct proof in the case considered here, but with a less precise remainder term.

If we perform the change of variables

\[
w = \frac{q-1-2z\sqrt{q}}{2},
\]

Theorem 2.5 states, in some sense, that in the interval \([w_-, w_+]\) the measure

\[
\sum_{x \in C_q, \partial} f(w(x))
\]

“behaves like” the distribution function

\[
\varphi_q(z) = \frac{1}{\pi q} \sqrt{4q-(q-1-2w)^2}
\]

when \( q\to\infty \); precisely, if \( f \) is a test function on \([-1, +1]\) and if we set

\[
g_q(w) = f\left(\frac{q-1-2w}{\sqrt{q}}\right) \quad \text{for } w \in [w_-, w_+],
\]
then
\[
\frac{1}{q^2} \sum_{x \in \mathbb{F}_q} g_\alpha(w(x)) = \int_{\mathbb{F}_q} g_\alpha(w) \varphi_\alpha(w) \, dw + O\left( \frac{1}{\sqrt{q}} \right)
\]
when \( q \to \infty \), where the hidden constant in the remainder depends only on \( \alpha \).

2.6. Kloosterman sums in characteristic 3

In characteristic 3 we have to consider the curve of genus 2:
\[
\mathcal{E}_K(a): y^3 - y = ax + \frac{1}{x}, \quad \text{where } a \in \mathbb{F}_3^\times.
\]
Katz and Livně [11] have observed that there is a nonconstant map
\[
\pi: \mathcal{E}_K(a) \to \mathcal{C}(b)
\]
from the Kloosterman curve
\[
\mathcal{E}_K(b): y^3 = bx + \frac{1}{x}, \quad \text{where } b \in \mathbb{F}_3^\times
\]
to the elliptic curve
\[
\mathcal{C}(b): Y^2 + XY + bY = X^3
\]
given by \((X, Y) = (xy, x')\). They deduced from this that the set of the \( W_{Kt}(a) \), where \( a \in \mathbb{F}_q^\times \), is the set of all the integers \( t \equiv q - 1 \pmod{3} \) such that \( |t| < 2[\sqrt{q}] \). By the same trick as above, we thus know the weights of the Kloosterman code in characteristic three. As a byproduct we get
\[
\# \mathcal{C}(b)(F) = q + 1 + W_{Kt}(b).
\]
The corresponding results for the Melas code are given by Wolfmann [32].

3. Geometric BCH codes

3.1. Trace equations

Now we come back to the curve defined in \( \mathbb{A}^1 \times X' \) by the equation
\[
Y': y' - y = f(x).
\]
This curve will allow us to study the number of points of a trace equation:
\[
M(f) = | \{ x \in X'(F) | \text{Tr}_{q/r} f(x) = 0 \} |.
\]
by Hilbert Theorem 90, we have
\[
\# Y'(F) = rM(f).
\]
Theorem 3.1. If \( A_0 = f F \) is nondegenerate, then
\[
|r M(f) - \# X'(F)| \leq \left( \frac{B_r(f)}{2} [2\sqrt{q}] \right) + \delta(f),
\]
where
\[
\delta(f) = \# (Y(k) - Y'(k)) - \# (X(k) - X'(k))
\]
and
\[
B_r(f) = \sum_{\lambda \in F} C(\lambda f).
\]

3.2. Geometric Goppa codes

We recall here the construction and properties of geometric Goppa codes (cf. [7, 8, 12, 28]). Let \( X \) be a smooth absolutely irreducible algebraic projective curve defined over \( F \); we denote by \( X(F) \) the set of points of \( X \) with coordinates in \( F \). Let \( K \) be the field of rational functions on \( X \) defined over \( F \). We denote by \( \text{Div}(X; F) \) the space of divisors of \( X \) defined over \( F \). If \( G \) is in \( \text{Div}(X; F) \), we set
\[
L(G) = \{ f \in K^* | (f) \geq -G \} \cup \{0\};
\]
this is a finite-dimensional vector space over \( F \).

Let \( (D, G) \) be a couple of divisors in \( \text{Div}(X; F) \). We assume that we have
\[
D = P_1 + \cdots + P_n,
\]
where \( P_1, \ldots, P_n \) are different points of \( X(F) \), and that
\[
\text{Supp} D \cap \text{Supp} G = \emptyset.
\]
We consider the code \( \Gamma_L \) (or \( \Gamma_L(D, G) \)) which is the image of the map
\[
c_L : L(G) \to F^n,
\]
defined by
\[
c_L(f) = (f(P_1), \ldots, f(P_n)).
\]
Recall that if \( \deg G < n \), then
\[
\dim \Gamma_L \geq \deg G - g + 1,
\]
with equality holding if \( \deg G \geq 2g - 2 \), and
\[
\text{dist} \Gamma_L \geq n - \deg G.
\]
We denote by \( \Omega(X) \) the vector space of differential forms of order 1 on \( X \) which are defined over \( F \), we denote by \( (\omega) \) the divisor of \( \omega \in \Omega(X) \), and if \( T \in \text{Div}(X; F) \), we let
\[
\Omega(T) = \{ \omega \in \Omega(X) | (\omega) \geq T \} \cup \{0\}.\]
This is a finite-dimensional vector space over $\mathbb{F}$; in particular, $\Omega(0)$ is the vector space of differentials of the first kind and the genus of $X$ is equal to

$$g(X) = \dim \Omega(0).$$

We now consider the code $\Gamma_\omega$ (or $\Gamma_\omega(D, G)$) which is the image of the map

$$c_\omega : \Omega(G - D) \to \mathbb{F}^n,$$

defined by

$$c_\omega(\omega) = (\text{Res}(\omega, P_1), \ldots, \text{Res}(\omega, P_n)).$$

Since $\ker c_\omega = \Omega(G)$, this map is injective if $\deg G > 2g - 2$.

Assume that $2g - 2 < \deg G < n + g - 1$. Then

$$\dim \Gamma_\omega \geq n - \deg G + g - 1,$$

with equality holding as soon as $\deg G \geq n$, and

$$\text{dist} \Gamma_\omega \geq \deg G - 2g + 2.$$

The codes $\Gamma_L$ and $\Gamma_\omega$ are duals: we call $\Gamma_L$ and $\Gamma_\omega$ the geometric Goppa codes on $X$ defined by the data $(D, G)$.

3.3. Bounds for the weights of codes

A geometric BCH code (subfield subcode of a geometric Goppa code) is the code defined on $\mathbb{F}_p$ obtained by descent by intersection from a code $\Gamma_\omega(D, G)$ defined over $\mathbb{F}$, i.e.

$$C = (\Gamma_\omega | \mathbb{F}) = \Gamma_\omega \cap \mathbb{F}_p^n.$$ 

Its designed distance is $\delta_2 = \deg G - 2g + 2$.

Example (cf. Michon [21]). The family of geometric BCH codes contains the family of geometric and classical Goppa codes, and also the primitive and narrow BCH codes. Take for instance

$$X = \text{the projective line } \mathbb{P}^1, \quad z_1 = \infty = (1 : 0), \quad G = (\delta - 1) \infty,$$

with

$$X'(\mathbb{F}) = \mathbb{F} = \{a_1, \ldots, a_Q\}.$$ 

The code $\Gamma_L(D, G)$, the dual of the code $\Gamma_\omega(D, G)$, is the image of the map

$$c : L(G) \to \mathbb{F}_p^q$$
defined by \( c(f) = (f(a_1), \ldots, f(a_q)) \). A basis of the vector space \( L(G) \) is given by the family of monomials \( 1, x, \ldots, x^{q-1} \). If we let \( a_1 = 0 \) and \( a_2 = 1 \), a parity check matrix of \( \Gamma_{\Omega}(D, G) \) is

\[
H = \begin{pmatrix}
1 & 1 & 1 & \cdots & 1 \\
0 & 1 & a_3 & \cdots & a_q \\
0 & 1 & \cdots & \cdots & \cdots \\
0 & 1 & a_3^{q-1} & \cdots & a_q^{q-1}
\end{pmatrix},
\]

hence, the geometric BCH code \( \Gamma_{\Omega}(D, G) | F_p \) is the primitive and narrow classical BCH code of designed distance \( \delta \), with an overall parity check added.

Table 1 shows the relation between the various families of codes.

<table>
<thead>
<tr>
<th>Over ( F )</th>
<th>On the line</th>
<th>Over ( F_p )</th>
<th>On the line</th>
<th>Arbitrary curve</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reed-Solomon</td>
<td>Classical Goppa</td>
<td>BCH</td>
<td>Classical Goppa</td>
<td>Geometric BCH</td>
</tr>
</tbody>
</table>

Let \( C = (\Gamma_{\Omega}(D, G) | F_p) \) be a geometric BCH code of length \( n \) over the prime field \( F_p \).

By Delsarte’s theorem we have

\[ C^\perp = (\Gamma_{\Omega} | F_p)^\perp = \text{Tr}_{q/p}(\Gamma_{\perp}) = \text{Tr}_{q/p}(\Gamma_L). \]

The code \( C^\perp \) is, thus, the image of the map

\[ c: L(G) \rightarrow F_p^n \]

defined by

\[ c(f) = (\text{Tr}_{q/p} f(x_1), \ldots, \text{Tr}_{q/p} f(x_n)). \]

For a nondegenerate \( f \in L(G) \), set

\[ M(f) = \# \{ x \in X'(F) | \text{Tr}_{q/p} f(x) = 0 \}; \]

then

\[ w(c(f)) = n - M(f) \]

and

\[ pM(f) - n = p(n - w(c(f))) - n = (p - 1)n - pw(c(f)). \]

If \( f \) is degenerate, then \( f = h^p - h + a \), with \( h \in K \); hence, \( w(c(f)) = 0 \) or \( n \), depending upon the value of \( \text{Tr}_{q/p} a \); we can thus deduce bounds for the weights of these codes from the bounds that we have obtained for \( M(f) \); in fact, we have the following result.
Theorem 3.2. The weight $w$ of any word of $C'$ satisfies $w = 0$, $w = n$, or

$$\left| w - \frac{p-1}{p} n \right| \leq \frac{(p-1)}{p} \left( \frac{2g-2 + \deg G + \kappa}{2} \right) \left( 2 \sqrt{q} \right) + \kappa,$$

with $\kappa = \# \operatorname{Supp} G$.

This theorem gives a nontrivial minoration only if

$$2n > (2g-2 + \deg G + \kappa) \left( 2 \sqrt{q} \right) + 2\kappa;$$

in that case we obtain the following bound for the minimum distance:

$$d > \frac{p-1}{p} \left( n - \kappa - \frac{2g-2 + \deg G + \kappa}{2} \right).$$

If $p = 2$, $q = 2^k$, we find

$$|w - \frac{1}{2} n| \leq \frac{1}{2} (2g-2 + \deg G + \kappa) \left( 2 \sqrt{q} \right);$$

in the case considered in Example 7.2, we recover the classical Carlitz–Uchiyama bound, cf. [20].

References