5. Classical Goppa codes

Let us recall that in (4.4) a BCH code was defined as the set of words \((c_0, c_1, \cdots, c_{n-1}) \in F_q^n\) such that \(c_0 + c_1(b^j) + c_2(b^j)^2 + \cdots + c_{n-1}(b^j)^{n-1} = 0\) where \(b\) is a primitive \(n\)th root of unity and \(1 \leq j < d\). Here \(d\) is the designed distance. We can rewrite this as follows:

\[
(z^n - 1) \sum_{i=0}^{n-1} \frac{c_i}{z - b^i} = \sum_{i=0}^{n-1} c_i \sum_{k=0}^{n-1} z^k (b^i)^{n-1-k} = 
\]

\[
= \sum_{k=0}^{n-1} z^k \sum_{i=0}^{n-1} c_i (b^k)^i = z^{d-1} p(z),
\]

i.e.

\[
(5.1) \quad \sum_{i=0}^{n-1} \frac{c_i}{z - b^i} = \frac{z^{d-1} p(z)}{z^{n-1}},
\]

for some polynomial \(p(z)\) and vice versa, i.e. \((c_0, c_1, \cdots, c_{n-1})\) is in the code if and only if the left-hand side of (5.1) written as a rational function \(a(z)/b(z)\) has a numerator divisible by \(z^{d-1}\). We now generalize this as follows.

(5.2) Definition: Let \(g(z)\) be a monic polynomial over \(F_q^n\) and let \(L := \{y_0, y_1, \cdots, y_{n-1}\} \subseteq F_q^n\) (here \(n = 1, L = 1\)). We require that \(g(y_i) \neq 0, 0 \leq i < n\). The Goppa code \(\Gamma(L, g)\) with Goppa polynomial \(g(z)\) is the set of words \((c_0, c_1, \cdots, c_{n-1})\) in \(F_q^n\) for which

\[
(5.3) \quad \sum_{i=0}^{n-1} \frac{c_i}{z - y_i} = 0 \pmod{g(z)}.
\]

Here (5.3) means that the numerator of the left-hand side, written as \(a(z)/b(z)\), is divisible by \(g(z)\). We can also make the convention that

\[
(5.4) \quad \frac{1}{z - y} := \frac{-1}{g(y)} \left[ \frac{g(z) - g(y)}{z - y} \right], \text{ where the right-hand side is the unique polynomial}
\]

\[
f(z) \mod g(z) \text{ such that } (z - y) f(z) \equiv 1 \pmod{g(z)}.
\]

From our introduction and (5.1) we see that if we take \(g(z) = z^{d-1}\) and \(L := \{b^i \mid 0 \leq i < n - 1\}\), where \(b\) is a primitive \(n\)th root of unity, then the Goppa code \(\Gamma(L, g)\) is the narrow sense BCH code of designed distance \(d\). We remark that not all BCH codes are also Goppa codes.

We can also interpret (5.2) as follows. Consider the vector space of rational functions \(f(z)\) with the following properties:

i) \(f(z)\) has zeros in all the points where \(g(z)\) has zeros, with at least the same multiplicity;

ii) \(f(z)\) has no poles, except possibly in the points \(y_0, y_1, \cdots, y_{n-1}\) and then of order 1.

Consider the code over \(F_q^n\) consisting of all the words \((\text{Res}_{y_0} f, \text{Res}_{y_1} f, \cdots, \text{Res}_{y_{n-1}} f)\).

The Goppa code \(\Gamma(L, g)\) is the "subfield subcode" consisting of all the words in the code with all coordinates in \(F_q^n\).
We shall now find a parity check matrix for \( \Gamma(L, g) \). Let \( g(z) = \sum_{i=0}^{t} g_i z^i \). Then

\[
\frac{g(z) - g(x)}{z - x} = \sum_{k+j=t-1} g_{k+j+1} x^j z^k,
\]

so we have an easy expression for the polynomials on the right-hand side of (5.4). By (5.3) we must have, with \( h_j := 1/g(\gamma_j) \),

\[
\sum_{i=0}^{n-1} c_i h_i \sum_{k+j=t-1} g_{k+j+1} (\gamma_j)^i z^k = 0,
\]

i.e. the coefficient of \( z^k \) is 0 for \( 0 \leq k \leq t - 1 \). We see that \( c \) must have inner product 0 with the rows of the following matrix.

\[
\begin{bmatrix}
    h_0 g_t & h_1 g_t & \cdots & h_{n-1} g_t \\
    h_0(g_{t-1} + g_{t} \gamma_0) & h_1(g_{t-1} + g_{t} \gamma_1) & \cdots & h_{n-1}(g_{t-1} + g_{t} \gamma_{n-1}) \\
    \vdots & \vdots & \ddots & \vdots \\
    h_0(g_1 + g_2 \gamma_0 + \cdots + g_t \gamma_0^{-1}) & \cdots & h_{n-1}(g_1 + g_2 \gamma_{n-1} + \cdots + g_t \gamma_{n-1}^{-1})
\end{bmatrix}
\]

Using elementary row operations we then find the following simple parity check matrix for \( \Gamma(L, g) \):

\[
H = \begin{bmatrix}
    h_0 & h_1 & \cdots & h_{n-1} \\
    h_0 \gamma_0 & h_1 \gamma_1 & \cdots & h_{n-1} \gamma_{n-1} \\
    \vdots & \vdots & \ddots & \vdots \\
    h_0 \gamma_0^{-1} & h_1 \gamma_1^{-1} & \cdots & h_{n-1} \gamma_{n-1}^{-1}
\end{bmatrix}
\]

(5.5)

Note that if in (4.9) we take \( v := (h_0, h_1, \cdots, h_{n-1}) \) and \( a := (\gamma_0, \gamma_1, \cdots, \gamma_{n-1}) \), \( k = t \), then the code \( GRS_k(a, v) \) has the matrix \( H \) of (5.5) as generator matrix. It follows that \( \Gamma(L, g) \) is a subfield subcode of the dual of a certain Generalized Reed Solomon code, i.e. \( \Gamma(L, g) \) is a subfield subcode of a Generalized Reed Solomon code!

Observe that in (5.5) we can again interpret each row as a set of \( m \) rows over \( \mathbb{F}_q \). So we find (using (4.9)):

\[\text{(5.6) Theorem.} \] The Goppa code \( \Gamma(L, g) \) has dimension \( \geq n - mt \) and minimum distance \( \geq t + 1 \).

The fact that the minimum distance is at least \( t + 1 \) follows directly from the definition (5.3). Since the code is linear, we can consider the weight of \( c \). If this is \( w \) then the degree of the numerator \( a(z) \) of the left-hand side of (5.3) is \( w - 1 \) (in fact less if \( \sum_{i=0}^{n-1} c_i = 0 \)). So \( w - 1 \) is at least \( t \). If \( q = 2 \) we can say a lot more.

Define \( f(z) := \prod_{i=0}^{n-1} (z - \gamma_i) \). Then \( \sum_{i=0}^{n-1} \frac{c_i}{z - \gamma_i} = f'(z)/f(z) \).

Since all exponents in \( f'(z) \) are even, this is a perfect square. If we assume that \( g(z) \) has no multiple zeros, then the fact that \( g(z) \) divides \( f'(z) \) implies that \( g^2(z) \) divides \( f'(z) \).

\[\text{(5.7) Theorem.} \] If \( g(z) \) has no multiple zeros, then the binary Goppa code \( \Gamma(L, g) \) has minimum distance at least \( 2t + 1 \) (where \( t := \deg g(z) \)).