On the Classification of Binary Goppa Codes

Michele Elia, Giorgio Taricco and Emanuele Viterbo

1Dipartimento di Elettronica
Politecnico di Torino
10129 Torino, ITALY
Email: viterbo@polito.it

Abstract
It is shown that binary Goppa codes with location set \( \mathbb{F}_q \) and separable polynomials of degree 2, 3 and 4 fall into a few equivalence classes characterized by canonical forms of these polynomials.

1. Introduction
The complexity of many cryptography systems that use Goppa codes depends on a code equivalence notion according to which codes are equivalent if they differ only in the order of the symbols, [7, p. 24]. Furthermore, it is well known that, these equivalent codes share several properties related to their performance: i) minimum distance; ii) weight distribution; iii) minimum-weight coset leader weight distribution; iv) maximum-likelihood decoding word error probability. It is an objective of this paper to specify explicitly the classification of Goppa codes induced by this equivalence. Let \( \mathcal{G}_l = \{ \Gamma(L, G(z)) \} \) denote the set of binary separable Goppa codes \( \Gamma(L, G(z)) \) with the error location set \( L = \{ \gamma_i \in \mathbb{F}_q \}_{i=0}^{n-1} \) being an ordered set of the elements of \( \mathbb{F}_q \), and Goppa polynomial \( G(z) = \prod_{i=1}^s G_i(z) \) taken from the set \( \mathcal{P}_l \) of the separable polynomials of degree \( t \), whose factors \( G_i(z) \) are distinct irreducible polynomials over \( \mathbb{F}_q \) of degree \( t \geq 2 \). Dimension \( k = 2^m - mt \) and minimum distance \( d = 2t + 1 \) of these Goppa codes are known, [8, 6]. Denoting with \( S_n = \{ \pi \} \) the symmetric group which is defined to act on \( L \) as \( \pi \Gamma(L) = \pi \{ \gamma_1, \ldots, \gamma_n \} = \{ \gamma_{\pi(1)}, \ldots, \gamma_{\pi(n)} \} \), two binary Goppa codes \( \Gamma(L, G(z)) \) and \( \Gamma(L, \hat{G}(z)) \) are equivalent if and only if a permutation \( \pi \) exists such that

\[
\Gamma(\pi(L), \hat{G}(z)) = \Gamma(L, G(z)) \quad (1)
\]

and we will write \( \equiv \gamma \colon \Gamma(L, G(z)) \sim \Gamma(L, \hat{G}(z)) \). The relation \( \equiv \gamma \) partitions the set \( \mathcal{G}_l \) of Goppa codes and \( \mathcal{P}_l \) into a set of classes that correspond one-to-one. The main theorem proved in this paper is basic to specify the partition of \( \mathcal{P}_l \), and it is essentially the converse of the following propositions whose proof is straightforward.

**Proposition 1** If \( \hat{G}(z) \) can be obtained from \( G(z) \) by the linear transformation \( z \to az + b \) then \( \Gamma(L, \hat{G}(z)) \) is equivalent to \( \Gamma(L, G(z)) \), the permutation of \( L \) being defined by the permutation polynomial \( f(z) = \frac{az+b}{a} \).

**Proposition 2** If \( \hat{G}(z) \) can be obtained from \( G(z) \) by the Tschebyscheff transformation \( z \to z^2 \) induced by the Frobenius automorphism of \( \mathbb{F}_q \), then \( \Gamma(L, \hat{G}(z)) \) is equivalent to \( \Gamma(L, G(z)) \), the permutation of \( L \) being defined by the permutation polynomial \( f(z) = z^{2^{m-1}} \).

Tschebyscheff transformations, which are known to be the most general transformations for polynomials [1], are defined as rational algebraic variable substitutions:

\[
\phi : z \to \frac{a_0 + \ldots + a_{r-1} z^{r-1}}{(b_0 + \ldots + b_{s-1} z^{s-1})}
\]

that transforms a polynomial \( G(z) \) in a polynomial \( \hat{G}(y) \) of the same degree \( t \) whose roots \( y_1 \) are related to the roots \( z_i \) of \( G(z) \) as \( y_i = \phi(z_i) \). It is shown in [1, p. 171] that any rational algebraic Tschebyscheff transformation \( \phi \) for \( G(z) \) of degree \( t \) can be reduced to a polynomial transformation of degree \( t - 1 \). In particular any Tschebyscheff transformation for \( G(z) \) can always be considered modulo \( G(z) \).

Given a permutation polynomial of \( \mathbb{F}_q \), we associate a map \( f : c \to f(c) \) from \( \mathbb{F}_q \) into \( \mathbb{F}_q \) which is a permutation \( \pi \) of \( \mathbb{F}_q \). Let \( \pi(\gamma) \) denote the image of \( \gamma \in \mathbb{F}_q \) under the permutation \( \pi \), then any permutation \( \pi \) of \( \mathbb{F}_q \) can be described by a polynomial \( f_\pi(z) \) of degree not greater than \( q - 2 \), and with this assumption the correspondence \( \pi \leftrightarrow f_\pi(z) \) is one-to-one. The composition \( \chi(z) \) of \( f_\pi(z) \) is \( \chi(z) \) of two permutation polynomials
is a permutation polynomial corresponding to the composition \( \theta = \pi \circ \sigma \) of permutations. Since every field element is a zero of \( z^q - z \), two permutation polynomials differing by a multiple of \( z^q - z \) produce the same permutation. The simplest permutation polynomials are of the form \( az + b \) with \( a, b \in \mathbb{F}_q \) and \( a \neq 0 \), and every \( z^i \), \( i = 0, 1, \ldots, (m - 1) \), whereas \( z^3 \) is a normalized permutation polynomial when \( m \) is odd. A fairly complete description of permutation polynomials is given in Lidl and Niederreiter's book [4].

2. General Results

The proof of the fundamental theorem given in this section is based on the following Lemma.

**Lemma 1** If the irreducible polynomial \( \tilde{G}(z) \) over \( \mathbb{F}_q \) is obtained from the irreducible polynomial \( G(z) \) by the Tschirnhaus transformation \( \Xi \) associated to the substitution polynomial \( y = f(z) \), where the coefficients of \( f(z) \) are in \( \mathbb{F}_q \), then \( \tilde{G}(f(z)) \) is divisible by \( G(z) \).

**Proof.** The Tschirnhaus transformation \( \Xi \) of \( G(z) \) produces a polynomial \( \tilde{G}(z) \) whose roots \( \xi \)'s are \( \xi = f(\zeta) \) where \( \zeta \)'s are the roots of \( G(z) \). Therefore \( \tilde{G}(f(z)) = 0 \) implies that \( G(z) \) divides \( \tilde{G}(z) \). \( \square \)

**Theorem 1** If \( \Gamma(\pi(\tilde{L}), \tilde{G}(z)) = \Gamma(L, G(z)) \) for some permutation \( \pi \), then a variable substitution \( y = f_\pi(z) \) exists that allows us to obtain the parity check equation

\[
\sum_{i=0}^{n-1} \frac{c_i}{z - \pi(\gamma_i)} \equiv 0 \mod \tilde{G}(z) \tag{2}
\]

that defines the code \( \Gamma(\pi(\tilde{L}), \tilde{G}(z)) \), from the parity check equation

\[
\sum_{i=0}^{n-1} \frac{c_i}{z - \gamma_i} \equiv 0 \mod G(z) \tag{3}
\]

that defines the code \( \Gamma(L, G(z)) \). The Tschirnhaus transformation \( \Xi \) such that \( \Xi(G(z)) = \tilde{G}(z) \) is specified by a substitution of the form \( y = f_\pi(z) = az^{2^i} + b \).

**Proof.** For binary separable Goppa codes equation (3) can be written as

\[
\sum_{i=0}^{n-1} \frac{c_i}{z - \gamma_i} = \frac{B(z)}{A(z)} G(z)^2 \tag{4}
\]

and equation (2) can be written as

\[
\sum_{i=0}^{n-1} \frac{c_i}{z - \pi(\gamma_i)} = \frac{\tilde{B}(z)}{\tilde{A}(z)} \tilde{G}(z)^2 \tag{5}
\]

Let \( \xi \) and \( \zeta \) denote a root of \( \tilde{G}(z) \) and \( G(z) \) respectively. A permutation polynomial \( f_\pi(z) \) with coefficients in \( \mathbb{F}_q \) exists such that \( \xi = f_\pi(\zeta) \) and

\[
f_\pi(\gamma) = \pi(\gamma) \text{ for all } \gamma \in \mathbb{F}_q
\]

Therefore, substituting \( f_\pi(z) \) for \( z \) in (5) we obtain

\[
\sum_{i=0}^{n-1} \frac{c_i}{f_\pi(z) - \pi(\gamma_i)} = \frac{\tilde{B}(f_\pi(z))}{\tilde{A}(f_\pi(z))} \tilde{G}(f_\pi(z))^2
\]

where \( G(f_\pi(z))^2 = G(z)^2 Q(z)^2 \) implies

\[
\sum_{i=0}^{n-1} \frac{1}{f_\pi(z) - \pi(\gamma_i)} \equiv 0 \mod G(z) \tag{6}
\]

Since \( f_\pi(\gamma) = \pi(\gamma) \), then \( f_\pi(z) - \pi(\gamma_i) = f_\pi(z) - f_\pi(\gamma) = (z - \gamma_i)R_\pi(z) \). Moreover equations (3) and (6) must imply one each other. Hence \( \gamma_i \) must be the only zero of \( f_\pi(z) - \pi(\gamma_i) \), which in turns forces \( f_\pi(z) \) to be of the form \( az^{2^i} + b \). This concludes the proof. \( \square \)

It follows that the only Tschirnhaus transformations \( \Xi \) relating Goppa polynomials of equivalent codes are produced compounding i) \( \Xi_1(z) = az + b \) and ii) \( \Xi_2(z) = z^2 \), and form a non-abelian group \( \mathcal{E} = \mathcal{C}_m \mathcal{L}_q \), by composition. \( \mathcal{E} \) is the semi-direct product of a cyclic group \( \mathcal{C}_m \) of order \( m \) consisting of the Frobenius transformations, and a group \( \mathcal{L}_q \) of linear transformations in one variable of order \( (q - 1)q \).

3. Classification

The Goppa code \( \Gamma(L, G(z)) \) classification consists in specifying the canonical forms of the representative Goppa polynomials. For 2, 3 and 4 error-correcting codes, it is given in the three theorems below. Theorem 2 summarizes results presented in [5, 2] for double error-correcting Goppa codes with the only addition of the Goppa polynomial canonical forms for even and odd \( m \), thus the proof is omitted.

**Theorem 2** Double-error correcting binary separable Goppa codes over \( \mathbb{F}_q \) with \( q = 2^m \) are all equivalent. The canonical form of \( G(z) \) can be expressed by

i) \( z^2 + z + g \) with \( g \in \mathbb{F}_{2^{2m}}^* \) and \( \text{Tr}(2^i)(g) = 1 \) for every \( m = 2^i(2h + 1) \), \( i \)

ii) \( z^2 + z + 1 \) for odd \( m \).

\( \text{Tr}(m)(x) \equiv \sum_{i=0}^{m-1} x^{2^i}. \)
The following theorem yields the equivalence classes for Goppa codes with irreducible $G(z)$ of degree 3. The situation is slightly more complex than for extended Goppa codes with irreducible $G(z)$ of degree 3 given in 5, Theorem 5).

**Theorem 3** Triple-error correcting binary separable Goppa codes over $F_q$ with $q = 2^m$ can be partitioned into the following equivalence classes:

For even $m = 2^{3*m}(2h+1)$ with $2h+1$ not divisible by 3, the canonical forms of $G(z)$ are two

1. $z^3 + g$, where $g$ is not a cube in $GF(2^3)$, and we have only a single class;

2. $z^3 + z + g$ where $g$ is chosen to make the polynomial irreducible. That is $Tr^{(m)}(1/g) = 0$ and the roots of $z^2 + z + \frac{1}{g^2} \neq 0$ are not cubes in $F_q^*.$

For odd $m = 3*(2h+1)$ with $2h+1$ not divisible by 3, the canonical form of $G(z)$ is $z^3 + z + g$, where $g ∈ GF(2^3)$ is chosen to make the polynomial irreducible. That is $Tr^{(m)}(1/g) = 1$ and the roots of $z^2 + z + \frac{1}{g^2} \neq 0$ are not cubes in $F_q^*.$

**Proof.** According to permutation polynomial composition the application to any Goppa polynomial $z^3 + a_1z^2 + a_2z + a_3$ of a linear transformation $y = az + b$ yields an equivalent code so that taking $b = a_1$ we have $y^3 + \frac{a_1}{a_2}y + \frac{a_3}{a_2}$ of the form $z^3 + g + y$, otherwise taking $a = \sqrt{a_1^2 + a_2}$ we obtain a polynomial of the form $z^3 + z + g.$ Now, it is necessary to deal with even and odd $m$ separately.

**Even $m$:**

1. The polynomial $z^3 + g$ is irreducible if $g$ is not a cube. In this case we have a single class because any polynomial $z^3 + g_a$ can be obtained from a single one by applying the two permitted transformations $y = az$ and $y = z^2.$

2. The polynomial $z^3 + z + g$ is irreducible if $g$ is chosen as $Tr^{(m)}(1/g) = 0$ and the roots of $z^2 + z + \frac{1}{g^2} \neq 0$ are not cubes in $F_q^*.$ [3, p.23].

**Odd $m$:** The canonical form of $G(z)$ can be of the form $z^3 + z + g$, with $g ∈ GF(2^3)$ such that $Tr^{(m)}(1/g) = 1$ and the roots of $z^2 + z + \frac{1}{g^2} \neq 0$ are not cubes in $F_q^*.$ [3, p.23]. The form $z^3 + g$ is excluded because $g$ is always a cube when $m$ is odd.

**Theorem 4** The set of four-error correcting binary separable Goppa codes over $F_q$ have associated canonical Goppa polynomials, which are irreducible or product of two irreducible polynomials of second degree. They have one of the following forms:

i) Irreducible polynomials

**even $m$:**

\[
\begin{align*}
z^4 + z^2 + g_0z + g_1 & \quad \text{with} \quad Tr^{(m)}(1/g_0) = 1 \\
z^4 + z^3 + g_0z^2 + g_1 & \quad \text{with} \quad Tr^{(m)}(1/g_0) = 1
\end{align*}
\]

**odd $m$:**

\[
\begin{align*}
z^4 + z + g & \quad \text{with} \quad Tr^{(m)}(g) = 1 \\
z^4 + z^2 + g_0z + g_1 & \quad \text{with} \quad Tr^{(m)}(1/g_0) = 1 \\
z^4 + z^3 + g_0z^2 + g_1 & \quad \text{with} \quad Tr^{(m)}(1/g_0) = 1 \\
z^4 + z^3 + g & \quad \text{with} \quad Tr^{(m)}(\sqrt[4]{g}) = 1
\end{align*}
\]

ii) Reducible polynomials

**even $m$:**

\[
\begin{align*}
z^4 + z + g_0 = (z^2 + z + \beta)(z^2 + z + 1 + \beta)
\end{align*}
\]

where $\beta$ is a root of $\beta^2 + \beta + g_0 = 0$ with $Tr^{(m)}(\beta) = 1$.

**odd $m$:**

\[
\begin{align*}
z^4 + g_0z^2 + (1 + g_0)z + g_0 = (z^2 + z + 1)(z^2 + z + g_0)
\end{align*}
\]

with $Tr^{(m)}(g_0) = 1$ and $g_0 ∈ F_{2^n}$ where $m_1$ is the smallest divisor of $m$ greater than 1.

**Proof.** In order to find canonical forms for irreducible $G(z)$ having degree 4, we note that $z^3 + g_0z + g_1$ is always reducible over $F_q$ when $m$ is even. In fact, if $\zeta$ is a root of this polynomial, then $\zeta^4 + g_0\zeta^4 + g_1 = 0,$ and its $q$-power is $\zeta^{q^4} + g_0\zeta^{q^4} + g_1 = 0.$ Summing the two expressions we get

\[
\zeta^{q^4} + g_0\zeta^{q^4} + \zeta^4 + g_0\zeta^4 = (\zeta^q + \zeta)^4 + g_0(\zeta^q + \zeta) = 0.
\]

Therefore, $(\zeta^q + \zeta)$ is a root of $x^4 + g_0x,$ and if $g_0$ is not a cube in $F_q$, the only root of this polynomial in $F_{q^4}$ is $x = 0,$ hence $\zeta^q + \zeta = 0$ implies $\zeta ∈ F_q,$ whereas if $g_0$ is a cube then we have other three roots in $F_q$ of the form $\sqrt[4]{g_0}\omega^j$, with $\omega$ a cube root of unity, but the $q$-power of $\zeta^q + \zeta = \sqrt[4]{g_0}\omega^j$ is $\zeta^{q^4} + \zeta^q = \sqrt[4]{g_0}\omega^j$. Summing the two expressions we get $\zeta^{q^4} + \zeta = 0,$ which implies that $\zeta ∈ F_q^2$, hence $z^4 + g_0z + g_1$ is product of quadratic factors.

**even $m$:** In view of the above result the irreducible polynomial can have two forms: $z^4 + z^3 + g_0z + g_1.$
and $z^4 + z^3 + g_0 z^2 + g_1$, where a necessary condition for irreducibility is $\text{Tr}^{(m)}(1/g_0) = 1$. Moreover, for $z^4 + z^2 + g_0 z + g_1$ we can assume $g_1 = g + g_0 b + b^2 + b^4$
where $g$ is a fixed elements such that $z^4 + z^2 + g_0 z + g$ is irreducible over $\mathbb{F}_2$. Whereas for $z^4 + z^3 + g_0 z^2 + g_1$
$g_1$ can still be selected as a function of $g_0$ and a fixed $g$, but the relation is more complex.

**odd $m$:** Since 4 and $m$ are relatively prime, the polynomial $z^4 + z + g$ is irreducible if $\text{Tr}^{(m)}(g) = 1$. For the two forms $z^4 + z^2 + g_0 z + g_1$ and $z^4 + z^3 + g_0 z^2 + g_1$, the same argument used for even $m$ applies. Lastly, the polynomial $z^4 + z^3 + g$ is irreducible if $\text{Tr}^{(m)}(g) = 1$.

**even $m = 2^h(2h + 1)$:** A reducible canonical Goppa polynomial is $G(z) = z^4 + z + g_0 = (z^2 + z + \beta)(z^2 + z + 1 + \beta)$ with $g_0 = \beta^2 + \beta$, $\beta \in \mathbb{F}_2$, and $\text{Tr}^{(m)}(g) = \text{Tr}^{(2^h)}(\beta) = 1$. This last condition assures that the quadratic factors are irreducible in $\mathbb{F}_2$.

**odd $m = m_1 m_2$:** A reducible canonical Goppa polynomial is

$$G(z) = z^4 + g z^2 + (1 + g) z + g = (z^2 + z + 1)(z^2 + z + g)$$

with $\text{Tr}^{(m_1)}(g) = 1$, where $g$ is taken into $\mathbb{F}_{2^m_1} \neq \mathbb{F}_2$ with $m_1 > 1$ as small as possible, and $\text{Tr}^{(m_1)}(g) = 1$ to make irreducible $z^2 + z + g$ in both $\mathbb{F}_{2^m_1}$ and $\mathbb{F}_2$.

Let us remark that when $m$ is odd, polynomials of the form $z^4 + az + b$ cannot split into quadratic irreducible factors, these polynomials are either irreducible or completely reducible.

4. Conclusions

Let us point out that, the above results apply only to codes with length $2^m$, in fact for the extended Goppa codes with length $2^m + 1$, birational Tschrhausen transformations are possible, [5]. Secondly, let us observe that, if we consider only irreducible Goppa polynomials, then $|\mathcal{P}_t| = N(t, q)$, the number of distinct monic polynomials of degree $t$ which are irreducible over $\mathbb{F}_q$ (see [4]). Thus, the number of partition subsets of $\mathcal{P}_t$ is lower bounded by $N(t, q)/[mq(q - 1)]$. When $G(z)$ factors, the computation is more complex, but similar bounds can still be found.

We have been able to specify relationships between $G(z)$ and $G'(z)$ that yield equivalent Goppa codes $\Gamma(L, G(z))$ and $\Gamma(L, G'(z))$. Therefore, the classes of $\Gamma(L, G(z))$ codes correcting 2, 3 and 4 errors, are explicitly given, distinguishing the forms of the Goppa polynomials for even and odd $m$. Note that distinct polynomials identify different classes.

---

**References**


