True Dimension of Some Quadratic Binary Trace Goppa Codes

Pascal Véron

Designs, Codes and Cryptography, 24, 81–97, 2001

True Dimension of Some Binary Quadratic Trace Goppa Codes

P. VÉRON veron@univ-tln.fr
Groupe de Recherche en Informatique et Mathématiques (GRIM), Université de Toulon-Var, B.P. 132, 83957 La Garde Cedex, France

Communicated by: R. C. Mullin

Received May 17, 2000; Accepted September 5, 2000

Abstract. We compute in this paper the true dimension over $\mathbb{F}_2$ of Goppa Codes $\Gamma(L, g)$ defined by the polynomial $g(z) = \mathrm{Tr}_{\mathbb{F}_{2^{2s}}:\mathbb{F}_{2^s}}(z)$ proving, this way, a conjecture stated in [14,16].

Keywords: Goppa codes, trace operator, redundancy equation, parameters of Goppa codes

1. Introduction

In 1970, V. D. Goppa [8] introduced a new class of linear error-correcting codes which asymptotically meet the Varshamov-Gilbert bound: the so-called $\Gamma(L, g)$ codes.

Definition 1. Let $g(z) \in \mathbb{F}_{q^m}[z]$, $L = \{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F}_{q^m}$ such that $\forall i$, $g(\alpha_i) \neq 0$. The Goppa code $\Gamma(L, g)$, of length n over $\mathbb{F}_q$, is the set of codewords, i.e., *n-tuples* $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$, satisfying

$$\sum_{i=1}^{n} \frac{c_i}{z - \alpha_i} \equiv 0 \pmod{g(z)}.$$

The dimension k of $\Gamma(L, g)$ and its minimal distance d satisfy

$$k \geq n - m \deg g(z)$$
$$d \geq \deg g(z) + 1.$$

Other basic definitions and properties of Goppa codes are to be found in [12]. It is well known that it is a hard problem to compute the true dimension (and minimal distance) of any Goppa code. A lot of work has been done on special classes of Goppa codes in order to improve the general bound on the dimension. Notably, for (classical) Goppa codes, interested readers can refer to [1–3,5,13,14,16,17].

1.1. The Trace Goppa Codes

In [11] M. Loeloeian and J. Conan described a subclass of binary ($q = 2$) Goppa codes defined by $g(z) = z^{2^s} + z$ and $L = \mathbb{F}_{2^{2s}} \backslash \mathbb{F}_{2^s}$ in order to illustrate their new lower bound on the minimum distance. In [13,14] authors studied the dimension of these codes and gave a new bound for the dimension:

$$\dim \Gamma(L, g) \geq n - 2s \deg g(z) + 3s - 1.$$

This result has been generalized in [16] where a special subclass of Goppa codes has been introduced: the Trace Goppa codes.

Definition 2. Let $a(z)$ and $b(z)$ be two arbitrary elements of $\mathbb{F}_{p^{ms}}[z]$. A Trace Goppa code is a $\Gamma(L, g)$ code where $g(z) = a(z)\mathrm{Tr}_{\mathbb{F}_{p^{ms}}:\mathbb{F}_{p^s}}(b(z))$ and $L = \mathbb{F}_{p^{ms}} \backslash \{z \in \mathbb{F}_{p^{ms}}, g(z) = 0\}$.

Depending on the value of p and m, three new bounds are given in [16] for the dimension of such codes. Moreover it is proved that these codes never reach the general known bound. In the so-called binary quadratic case ($p = 2, m = 2$) it is shown that

$$\dim \Gamma(L, g) \geq n - 2s \deg g(z) + 3s - 1.$$

For $a(z) = 1$ and $b(z) = z$, this bound corresponds to the one given in [13,14]. As mentioned in [13,16], when $g(z) = \mathrm{Tr}_{\mathbb{F}_{2^{2s}}:\mathbb{F}_{2^s}}(z)$, the bound is reached for $s = 2, 3, 4, 5$. Till now, it was an open problem to know whether it was reached for all $s \geq 2$.

In the quadratic case ($m = 2$), it is shown in [16] that:

$$\dim \Gamma(L, g) \geq n - 2s \deg g(z) + 2s - 1.$$

For $g(z) = \mathrm{Tr}_{\mathbb{F}_{p^{2s}}:\mathbb{F}_{p^s}}(z)$, it has been checked with the help of a computer that the proposed bound is reached.

The aim of this paper is to prove that the true dimension of binary Goppa codes defined by $g(z) = \mathrm{Tr}_{\mathbb{F}_{2^{2s}}:\mathbb{F}_{2^s}}(z)$ is $n - 2s \deg g(z) + 3s - 1$, proving this way a conjecture stated in [14,16].

In Section 2, we recall the trace description of Goppa codes (given by Delsarte's theorem) which makes a link between the calculation of the dimension and the number of solutions of a modular polynomial equation: the so-called redundancy equation. For the binary-quadratic case, the dimension of a trace Goppa code is equal to the number of polynomials $a(z) \in \mathbb{F}_{2^{2s}}[z]$ ($\deg a(z) < 2^s$) which satisfies a particular equation over $\mathbb{F}_{2^{2s}}[z]/(z^{2^{2s}} + z)$.

In Section 3, we rearrange the redundancy equation as a sum of monomials which vanishes over the polynomial ring $\mathbb{F}_{2^{2s}}[z]$. The corresponding coefficient of each monomial is either a linear combination of the a_i's or exactly one of the a_i's (which then must be 0).

In Section 4 we seek for monomials whose corresponding coefficient is one of the a_i's and conclude that if $a(z)$ satisfies the redundancy equation then $a(z) = a_0 + a_1 z + a_{2^{s-1}} z^{2^{s-1}}$.

In Section 5, we simplify the redundancy equation by using the reduced form of $a(z)$. This gives us three conditions over a_0, a_1 and $a_{2^{s-1}}$.

Section 6 uses all the results of Sections 4 and 5 in order to prove our main result.

2. Trace Description of Goppa Codes and Redundancy Equation

Let $\Gamma(L, g)$ be an (n, k) code over $\mathbb{F}_2$ ($L \subset \mathbb{F}_{2^m}$), it is well known (see [12]) that it is a restriction to $\mathbb{F}_2$ of a generalized $(n, n - \deg g(z))$ Reed-Solomon code $\hat{\Gamma}$ defined over $\mathbb{F}_{2^m}$. Delsarte's theorem states that $\Gamma(L, g)^{\perp} = \mathrm{Tr}(\hat{\Gamma}^{\perp})$ where

$$\begin{array}{rccc} \mathrm{Tr}: & \hat{\Gamma} & \to & \mathbb{F}_2^n \\ & (c_1, \ldots c_n) & \mapsto & \left(\mathrm{Tr}_{\mathbb{F}_{2^m}:\mathbb{F}_2}(c_1), \ldots, \mathrm{Tr}_{\mathbb{F}_{2^m}:\mathbb{F}_2}(c_n)\right) \end{array}$$

Since $\hat{\Gamma}^{\perp}$ has dimension $m \deg g(z)$ over $\mathbb{F}_2$, then

$$\begin{aligned} n - k &= \dim_{\mathbb{F}_2} \Gamma(L, g)^{\perp} \\ &= \dim_{\mathbb{F}_2} \mathrm{Im}(\mathrm{Tr}) \\ &= m \deg g(z) - \dim_{\mathbb{F}_2} \ker(\mathrm{Tr}). \end{aligned}$$

A possible way to determine the dimension of a Goppa code is to compute $\dim_{\mathbb{F}_2} \ker(\mathrm{Tr})$. From [14,16], in order to prove our main result we have only to show that for $g(z) = \mathrm{Tr}_{\mathbb{F}_{2^{2s}}:\mathbb{F}_{2^s}}(z)$ and $m = 2s$, $\dim_{\mathbb{F}_2} \ker(\mathrm{Tr}) \leq 3s - 1$.

In [13] it has been established that $\ker(\mathrm{Tr})$ is isomorphic to

$$\left\{ a(z) \in \mathbb{F}_{2^{2s}}[z] \mid g(z)^{2^{2s-1}+1} \mathrm{Tr}_{\mathbb{F}_{2^s}:\mathbb{F}_2}\left(\frac{a(z)}{g(z)} + \frac{a(z)^{2^s}}{g(z)^{2^s}}\right) \equiv 0 \pmod{z^{2^{2s}} + z} \right\},$$

with $0 \leq \deg a(z) \leq 2^s - 1$ (such an equation is obtained from the parity check matrix of the code).

Let $a(z) = \sum_{i=0}^{2^s-1} a_i z^i$ ($\forall i, a_i \in \mathbb{F}_{2^{2s}}$), and $g(z) = z^{2^s} + z$, since $g(z)^{2^s} \equiv g(z) \pmod{z^{2^{2s}} + z}$, then

$$\begin{aligned} & g(z)^{2^{2s-1}+1} \mathrm{Tr}_{\mathbb{F}_{2^s}:\mathbb{F}_2}\left(\frac{a(z)}{g(z)} + \frac{a(z)^{2^s}}{g(z)^{2^s}}\right) \equiv 0 \pmod{z^{2^{2s}}} + z \\ \Leftrightarrow\ & g(z)^{2^{s-1}+1} \sum_{i=0}^{s-1} \left(\frac{a(z) + a(z)^{2^s}}{g(z)}\right)^{2^i} \equiv 0 \pmod{z^{2^{2s}} + z} \\ \Leftrightarrow\ & \sum_{i=0}^{s-1} \left(z^{2^s} + z\right)^{2^{s-1}-2^i+1} \left(\sum_{j=0}^{2^s-1} a_j^{2^i} z^{2^i j} + a_j^{2^{s+i}} z^{j 2^{s+i}}\right) \equiv 0 \pmod{z^{2^{2s}} + z} \end{aligned}$$

PROPOSITION 1. *$\forall i \geq 0$,*

$$\left(z^{2^s} + z\right)^{2^{s-1}-2^i+1} = \sum_{k=0}^{2^{s-1-i}-1} z^{2^{s-1}-2^i+2^i k(2^s-1)+1} + \sum_{k=0}^{2^{s-1-i}-1} z^{2^{s-1}-2^i+2^i k(2^s-1)+2^s}.$$

Proof. Let us write $(z^{2^s} + z)^{2^{s-1}-2^i+1} = (z^{2^s} + z)(z^{2^s} + z)^{2^{s-1}-2^i}$.

$$\begin{aligned}\left(z^{2^s}+z\right)^{2^{s-1}-2^i} &= z^{2^{s-1}-2^i}\left(z^{2^s-1}+1\right)^{2^{s-1}-2^i}\\ &= z^{2^{s-1}-2^i}\frac{\left(z^{2^s-1}+1\right)^{2^{s-1}}}{\left(z^{2^s-1}+1\right)^{2^i}}\\ &= z^{2^{s-1}-2^i}\frac{\left(z^{2^i(2^s-1)2^{s-1-i}}+1\right)}{\left(z^{2^i(2^s-1)}+1\right)}\\ &= z^{2^{s-1}-2^i}\sum_{k=0}^{2^{s-1-i}-1} z^{2^i(2^s-1)k}\end{aligned}$$ ■

Thus equation (1) becomes (modulo $z^{2^{2s}}+z$)

$$\begin{aligned}&\sum_{i=0}^{s-1}\sum_{k=0}^{2^{s-i-1}-1}\sum_{j=0}^{2^s-1} a_j^{2^i} z^{2^{s-1}-2^i+2^ik(2^s-1)+2^ij+1}\\ &+\sum_{i=0}^{s-1}\sum_{k=0}^{2^{s-i-1}-1}\sum_{j=0}^{2^s-1} a_j^{2^{s+i}} z^{2^{s-1}-2^i+2^ik(2^s-1)+2^{s+i}j+1}\\ &+\sum_{i=0}^{s-1}\sum_{k=0}^{2^{s-i-1}-1}\sum_{j=0}^{2^s-1} a_j^{2^i} z^{2^{s-1}-2^i+2^ik(2^s-1)+2^ij+2^s}\\ &+\sum_{i=0}^{s-1}\sum_{k=0}^{2^{s-i-1}-1}\sum_{j=0}^{2^s-1} a_j^{2^{s+i}} z^{2^{s-1}-2^i+2^ik(2^s-1)+2^{s+i}j+2^s}=0. \qquad (1)\end{aligned}$$

Our main goal is to show that a necessary condition so that a polynomial $a(z)$ satisfies equation (1) is that, for all $j \neq 0, 1, 2^{s-1}$, $a_j = 0$. With this end in view, we are going first to study the different degrees of the monomials which appear in the above equation.

3. Distribution of the Degrees in the Redundancy Equation

- Let $i = 0$, since $(z^{2^s}+z)^{2^{s-1}-2^i+1} = z^{2^{2s-1}}+z^{2^{s-1}}$, the degrees which appear in equation (1) are: $2^{s-1}+j$, $2^{s-1}+j2^s$, $2^{2s-1}+j$, $2^{2s-1}+j2^s$ for $j = 0 \ldots 2^s-1$.
- Let $i \neq 0$ the degrees can be distributed in four classes: $2^{s-1}-2^i+2^ik(2^s-1)+2^ij+1$, $2^{s-1}-2^i+2^ik(2^s-1)+2^{s+i}j+1$, $2^{s-1}-2^i+2^ik(2^s-1)+2^ij+2^s$, $2^{s-1}-2^i+2^ik(2^s-1)+2^{s+i}j+2^s$, for $j = 0 \ldots 2^s-1$.

Now remember that we are working modulo $z^{2^{2s}}+z$, i.e. (unformally speaking) we have to replace 2^{2s} by 1 each time it appears.

$\forall j = 0 \ldots 2^s-1$,

– $2^{s-1}+j < 2^{2s}$, $2^{s-1}+j2^s < 2^{2s}$, $2^{2s-1}+j < 2^{2s}$, thus these degrees remain unchanged modulo $z^{2^{2s}}+z$,

– $2^{2s-1} + j2^s < 2^{2s}$ for $j = 0 \dots 2^{s-1} - 1$,

– let $j = 2^{s-1} + j'$ $(0 \le j' \le 2^{s-1} - 1)$, then

$$\begin{aligned} z^{2^{2s-1}+j2^s} &= z^{2^{2s-1}+(2^{s-1}+j')2^s} \\ &\equiv z^{j'2^s+1} \pmod{z^{2^{2s}} + z}. \end{aligned}$$

$\forall i = 1 \dots s-1, \forall k = 0 \dots 2^{s-1-i} - 1, \forall j = 0 \dots 2^s - 1$, let $\varepsilon = 1$ or 2^s,

– $2^{s-1} - 2^i + 2^i k(2^s - 1) + 2^i j + \varepsilon$
$\le 2^{s-1} - 2^i + (2^{s-1} - 2^i)(2^s - 1) + 2^{s-1}(2^s - 1) + 2^s$
$\le 2^{2s} - 2^{s+1} - 2^{s-1}$
$< 2^{2s}$.

– let $j = j' + \gamma 2^{s-i}$, $0 \le j' \le 2^{s-i} - 1$, $0 \le \gamma \le 2^i - 1$ and consider two cases:
(a) $0 \le j' < 2^{s-i} - k$, then

$$\begin{aligned} z^{2^{s-1}-2^i+2^i k(2^s-1)+2^{s+i}j+\varepsilon} &= z^{2^{s-1}-2^i+2^i k(2^s-1)+2^{s+i}(j'+\gamma 2^{s-i})+\varepsilon} \\ &\equiv z^{2^{s-1}-2^i+2^i k(2^s-1)+2^{s+i}j'+\gamma+\varepsilon} \pmod{z^{2^{2s}} + z} \end{aligned}$$

(and $2^{s-1} - 2^i + 2^i k(2^s - 1) + 2^{s+i} j' + \gamma + \varepsilon < 2^{2s}$).
(b) $2^{s-i} - k \le j' \le 2^{s-i} - 1$ (remark that this occurs only for $k \ge 1$). We can write $j' = j'' + 2^{s-i} - k$, $0 \le j'' \le k - 1$. Then

$$\begin{aligned} z^{2^{s-1}-2^i+2^i k(2^s-1)+2^{s+i}j+\varepsilon} &= z^{2^{s-1}-2^i+2^i k(2^s-1)+2^{s+i}(j''+2^{s-i}-k+\gamma 2^{s-i})+\varepsilon} \\ &\equiv z^{2^{s-1}-2^i(k+1)+2^{s+i}j''+\gamma+1+\varepsilon} \pmod{z^{2^{2s}} + z} \end{aligned}$$

(and $2^{s-1} - 2^i + 2^i(k+1) + 2^{s+i} j'' + \gamma + 1 + \varepsilon < 2^{2s}$).

In order to sum up these results Table 1 gives for i and k fixed, the different type of degrees which appear in equation (1). In the left column we have assigned a name to each category in order to simplify the rest of the paper. Since each degree is associated to a monomial in equation (1), in the right column we list the corresponding coefficient of each monomial.

Important Remark. Set $\bar{E}_{i,k,2}$ and $\bar{F}_{i,k,2}$ are defined only for $k \ge 1$ and $i \le s - 2$ (since $k \le 2^{s-i-1} - 1$).

As an example, Table 2 gives the different degres which appear in equation (1) for $s = 3$. From now on, we have reduce equation (1) to a sum of monomials whose degrees are less than 2^{2s}. Thus the sum of monomials vanishes over the polynomial ring $\mathbb{F}_{2^{2s}}[z]$ which implies that the corresponding coefficients are zeros. Clearly, all the sets in Table 1 are not pairwise disjoint, otherwise all a_j should be zeros and $\dim \ker(\mathrm{Tr}) = 0$. However, for k and i fixed, it is easy to see that each set contains distinct elements. We are now going to investigate the elements which only belong to one set for any value of i, k. Let d be such an element, then there is a single monomial of degree d in equation (1). This implies that its associated coefficient is one of the a_j's (and not a linear combination of some a_j's),

Table 1. Distribution of degrees

$i = 0$			
D_0	$2^{s-1} + j$	$j = 0 \dots 2^s - 1$	a_j
D_1	$2^{s-1} + j2^s$	$j = 0 \dots 2^s - 1$	$a_j^{2^s}$
D_2	$2^{2s-1} + j$	$j = 0 \dots 2^s - 1$	a_j
$D_{3,1}$	$2^{2s-1} + j2^s$	$j = 0 \dots 2^{s-1} - 1$	$a_j^{2^s}$
$D_{3,2}$	$j2^s + 1$	$j = 0 \dots 2^{s-1} - 1$	$a_{j+2^{s-1}}^{2^s}$
$i \neq 0, k = 0 \dots 2^{s-i-1} - 1, \gamma = 0 \dots 2^i - 1$			
$E_{i,k}$	$2^{s-1} - 2^i + 2^i k(2^s - 1) + 2^i j + 1$	$j = 0 \dots 2^s - 1$	$a_j^{2^i}$
$\bar{E}_{i,k,1}$	$2^{s-1} - 2^i + 2^i k(2^s - 1) + 2^{s+i} j + \gamma + 1$	$j = 0 \dots 2^{s-i} - k - 1$	$a_{j+\gamma 2^{s-i}}^{2^{s+i}}$
$\bar{E}_{i,k,2}$	$2^{s-1} - 2^i (k+1) + 2^{s+i} j + \gamma + 2$	$j = 0 \dots k - 1$	$a_{j+2^{s-i}-k+\gamma 2^{s-i}}^{2^{s+i}}$
$F_{i,k}$	$2^s + 2^{s-1} - 2^i + 2^i k(2^s - 1) + 2^i j$	$j = 0 \dots 2^s - 1$	$a_j^{2^i}$
$\bar{F}_{i,k,1}$	$2^s + 2^{s-1} - 2^i + 2^i k(2^s - 1) + 2^{s+i} j + \gamma$	$j = 0 \dots 2^{s-i} - k - 1$	$a_{j+\gamma 2^{s-i}}^{2^{s+i}}$
$\bar{F}_{i,k,2}$	$2^s + 2^{s-1} - 2^i (k+1) + 2^{s+i} j + \gamma + 1$	$j = 0 \dots k - 1$	$a_{j+2^{s-i}-k+\gamma 2^{s-i}}^{2^{s+i}}$

and must be zero. We will call such elements "isolated" degrees. In Table 2 bold integers correspond to "isolated" degrees.

4. Seeking "Isolated" Degrees

Here are some properties of the sets described in Table 1. We will often use them in the rest of the paper (we will suppose that $s \geq 3$).

Property 1.

$$\delta \in D_0 \Rightarrow \delta \leq 2^s + 2^{s-1} - 1 \tag{1a}$$

$$\delta \in D_1 \Rightarrow \delta \equiv 2^{s-1} \pmod{2^s} \quad \text{(and thus } \delta \text{ is even)} \tag{1b}$$

$$\delta \in D_2 \Rightarrow 2^{2s-1} \leq \delta \leq 2^{2s-1} + 2^s - 1 \tag{1c}$$

$$\delta \in D_{3,1} \Rightarrow \delta \geq 2^{2s-1} \text{ and } \delta \equiv 0 \pmod{2^i}, i = 1 \dots s - 1 \tag{1d}$$

$$\delta \in D_{3,2} \Rightarrow \delta \equiv 1 \pmod{2^s} \quad \text{(and thus } \delta \text{ is odd)} \tag{1e}$$

Proof. All these properties are obvious. ■

Property 2. $\forall i, 1 \leq i \leq s - 1, \forall k, \delta \in E_{i,k} \Rightarrow \delta \leq 2^{2s-1} - 1$ and $\delta \equiv 1 \pmod{2^i}$ (thus δ is odd).

Proof. First it is obvious that $\delta \equiv 1 \pmod{2^i}$. Since $k \leq 2^{s-i-1} - 1$ then $2^i k \leq 2^{s-1} - 2^i$. Moreover using the fact that $i \geq 1$ and $j \leq 2^s - 1$ then

Table 2. Distribution of degrees, $s = 3$

$i = 0$

D_0 : 4, 5, **6**, 7, 8, 9, 10, 11
D_1 : 4, 12, 20, 28, 36, 44, 52, 60
D_2 : 32, 33, 34, 35, 36, **37**, 38, **39**
$D_{3,1}$: 32, 40, 48, 56
$D_{3,2}$: 1, 9, 17, 25

$i = 1$

$E_{1,0}$: 3, 5, 7, 9, 11, 13, **15**, 17
$\bar{E}_{1,0,1}$: $\underbrace{3, 19, 35, 51}_{\gamma=0}\ \underbrace{4, 20, 36, 52}_{\gamma=1}$
$F_{1,0}$: 10, 12, 14, 16, 18, 20, 22, 24
$\bar{F}_{1,0,1}$: $\underbrace{10, 26, 42, 58}_{\gamma=0}\ \underbrace{11, 27, 43, 59}_{\gamma=1}$
$E_{1,1}$: 17, 19, 21, **23**, 25, 27, 29, 31
$\bar{E}_{1,1,1}$: $\underbrace{17, 33, 49}_{\gamma=0}\quad \underbrace{18, 34, 50}_{\gamma=1}$
$\bar{E}_{1,1,2}$: $\underbrace{2}_{\gamma=0}\qquad \underbrace{3}_{\gamma=1}$
$F_{1,1}$: 24, 26, 28, 30, 32, 34, 36, 38
$\bar{F}_{1,1,1}$: $\underbrace{24, 40, 56}_{\gamma=0}\quad \underbrace{25, 41, 57}_{\gamma=1}$
$\bar{F}_{1,1,2}$: $\underbrace{9}_{\gamma=0}\qquad \underbrace{10}_{\gamma=1}$

$i = 2$

$E_{2,1}$: 1, 5, 9, 13, 17, 21, 25, 29
$\bar{E}_{2,0,1}$: $\underbrace{1, 33}_{\gamma=0}\ \underbrace{2, 34}_{\gamma=1}\ \underbrace{3, 35}_{\gamma=2}\ \underbrace{4, 36}_{\gamma=3}$
$F_{2,0}$: 8, 12, 16, 20, 24, 28, 32, 36
$\bar{F}_{2,0,1}$: $\underbrace{8, 40}_{\gamma=0}\ \underbrace{9, 41}_{\gamma=1}\ \underbrace{10, 42}_{\gamma=2}\ \underbrace{11, 43}_{\gamma=3}$

$$\begin{aligned}\delta &\le 2^{s-1} - 2^i + (2^{s-1} - 2^i)(2^s - 1) + 2^i(2^s - 1) + 1\\ &\le 2^{2s-1} - 2^i + 1\\ &\le 2^{2s-1} - 1.\end{aligned}$$

■

Property 3. $\forall i, 1 \le i \le s-1,\ \forall k,\ \delta \in \bar{E}_{i,k,1} \Rightarrow \delta \equiv \delta' \pmod{2^s}$ where $\delta' = 2^{s-1} - 2^i(k+1) + \gamma + 1 \le 2^{s-1}$.

Proof. First it is obvious that $\delta \equiv 2^{s-1} - 2^i(k+1) + \gamma + 1 \pmod{2^s}$. Now since $\gamma + 1 - 2^i \le 0$ and $k \ge 0$ then $\delta' \le 2^{s-1} - 2^i k \le 2^{s-1}$. ■

Property 4. $\forall i, 1 \le i \le s-2,\ \forall k \ge 1,\ \delta \in \bar{E}_{i,k,2} \Rightarrow \delta \equiv \delta' \pmod{2^s}$ where $\delta' = 2^{s-1} - 2^i(k+1) + \gamma + 2 \le 2^{s-1} - 1$. Moreover $\delta \le 2^{2s-1} - 2^{s+2} + 2^{s-2} + 1$.

Proof. First it is obvious that $\delta \equiv 2^{s-1} - 2^i(k+1) + \gamma + 2 \pmod{2^s}$. Since $\gamma + 2 - 2^i \le 1$, $k \ge 1$ and $i \ge 1$ then $\delta' \le 2^{s-1} - 2^i k + 1 \le 2^{s-1} - 1$. Moreover, since $k \le 2^{s-i-1} - 1$, $j \le k-1$ and $1 \le i \le s-2$ then

$$\begin{aligned}\delta &\le 2^{s-1} - 2^i 2^{s-1-i} + 2^{s+i}(2^{s-i-1} - 2) + \gamma + 2\\ &\le 2^{2s-1} - 2^{s+2} + 2^i + 1\\ &\le 2^{2s-1} - 2^{s+2} + 2^{s-2} + 1.\end{aligned}$$

■

Property 5. $\forall i, 1 \le i \le s-1, \forall k, \delta \in F_{i,k} \Rightarrow 2^s \le \delta \le 2^{2s-1} + 2^s - 2$ and $\delta \equiv 0 \pmod{2^i}$ (thus δ is even).

Proof. First it is obvious that $\delta \equiv 0 \pmod{2^i}$. Now, since $k \ge 0$, $j \ge 0$ and $i \le s-1$, then $\delta \ge 2^s$. Next, since $2^i k \le 2^{s-1} - 2^i$, $i \ge 1$ and $j \le 2^s - 1$, then

$$\begin{aligned}\delta &\le 2^s + 2^{s-1} - 2^i + (2^{s-1} - 2^i)(2^s - 1) + 2^i(2^s - 1)\\ &\le 2^{2s-1} + 2^s - 2^i\\ &\le 2^{2s-1} + 2^s - 2.\end{aligned}$$

■

Property 6. $\forall i, 1 \le i \le s-1, \forall k, \delta \in \bar{F}_{i,k,1} \Rightarrow \delta \equiv \delta' \pmod{2^s}$ where $\delta' = 2^{s-1} - 2^i(k+1) + \gamma \le 2^{s-1} - 1$.

Proof. Proof is similar to the one of Property 3. ■

Property 7. $\forall i, 1 \le i \le s-2, \forall k \ge 1,\ \delta \in \bar{F}_{i,k,2} \Rightarrow \delta \equiv \delta' \pmod{2^s}$ where $\delta' = 2^{s-1} - 2^i(k+1) + \gamma + 1 \le 2^{s-1} - 2$. Moreover $\delta \le 2^{2s-1} - 2^{s+2} + 2^s + 2^{s-2}$.

Proof. Proof is similar to the one of Property 4. ■

We can now specify which degrees are "isolated."

LEMMA 1. $\forall i = 1 \ldots s-1, \forall k, \forall j, 2 \le j \le 2^{s-1} - 1,\ j$ *even*

$$2^{s-1} + j \in D_0$$

$$2^{s-1} + j \notin D_1 \cup D_2 \cup D_{3,1} \cup D_{3,2} \cup E_{i,k} \cup \bar{E}_{i,k,1} \cup \bar{E}_{i,k,2} \cup F_{i,k} \cup \bar{F}_{i,k,1} \cup \bar{F}_{i,k,2}$$

Proof. Let $\Delta = 2^{s-1} + j$, notice that

- Δ is even,
- $2^{s-1} < \Delta < 2^s$ (thus Δ remains unchanged modulo 2^s).

From Propositions 1b, 1c, 1d and 1e $\Delta \notin D_1 \cup D_2 \cup D_{3,1} \cup D_{3,2}$.

From Propositions 2 and 5, $\forall i = 1 \ldots s-1, \forall k, \Delta \notin E_{i,k} \cup F_{i,k}$.

From Propositions 3, 4 and 6, 7, $\forall i = 1 \ldots s-1, \forall k \geq 1, \Delta \notin \bar{E}_{i,k,1} \cup \bar{E}_{i,k,2} \cup \bar{F}_{i,k,1} \cup \bar{F}_{i,k,2}$. ■

LEMMA 2. *$\forall i = 1 \ldots s-1$, $\forall k$, $\forall j$, $2^{s-1}+1 \leq j \leq 2^s - 1$, j odd*

$$2^{2s-1} + j \in D_2$$

$$2^{2s-1} + j \notin D_0 \cup D_1 \cup D_{3,1} \cup D_{3,2} \cup E_{i,k} \cup \bar{E}_{i,k,1} \cup \bar{E}_{i,k,2} \cup F_{i,k} \cup \bar{F}_{i,k,1} \cup \bar{F}_{i,k,2}$$

Proof. Let $\Delta = 2^{2s-1} + j$, then:

- Δ is odd,
- $\Delta \equiv j \pmod{2^s}$, $j \geq 2^{s-1}+1$,
- $2^{2s-1} \leq \Delta \leq 2^{2s-1} + 2^s - 1$.

From Propositions 1a, 1b, 1d and 1e, $\Delta \notin D_0 \cup D_1 \cup D_{3,1} \cup D_{3,2}$.

From Propositions 2 and 5, $\forall i = 1 \ldots s-1, \forall k, \Delta \notin E_{i,k} \cup F_{i,k}$.

From Propositions 3, 4 and 6, 7, $\forall i = 1 \ldots s-1, \forall k, \Delta \notin \bar{E}_{i,k,1} \cup \bar{E}_{i,k,2} \cup \bar{F}_{i,k,1} \cup \bar{F}_{i,k,2}$. ■

LEMMA 3. *$\forall j$, $3 \leq j \leq 2^{s-2}+1$, j odd*

- $2^{s+1} + 2^{s-1} + 2j - 3 \in E_{1,1}$,
- $\forall k \neq 1$, $2^{s+1} + 2^{s-1} + 2j - 3 \notin E_{1,k}$,
- $\forall i > 1$, $\forall k$, $2^{s+1} + 2^{s-1} + 2j - 3 \notin E_{i,k}$,
- $\forall i \geq 1$, $\forall k$, $2^{s+1} + 2^{s-1} + 2j - 3 \notin D_0 \cup D_1 \cup D_2 \cup D_{3,1} \cup D_{3,2} \cup \bar{E}_{i,k,1} \cup \bar{E}_{i,k,2} \cup F_{i,k} \cup \bar{F}_{i,k,1} \cup \bar{F}_{i,k,2}$.

Proof. Let $\Delta = 2^{s+1} + 2^{s-1} + 2j - 3$, notice that:

- Δ is odd,
- $2^{s+1} + 2^{s-1} + 3 \leq \Delta \leq 2^{s+1} + 2^s - 1$.

Moreover, $\Delta \equiv 2^{s-1} + 2j - 3 \pmod{2^s}$, and

$$1 < 2^{s-1} + 3 \leq 2^{s-1} + 2j - 3 \leq 2^s - 1.$$

From Propositions 1a, 1b, 1c, 1d and 1e, $\Delta \notin D_0 \cup D_1 \cup D_2 \cup D_{3,1} \cup D_{3,2}$.

Let $i = 1$ and $k = 0$, then $\delta \in E_{1,0} \Rightarrow \exists j'$, $0 \leq j' \leq 2^s - 1$, such that $\delta = 2^{s-1} + 2j' - 1 \leq 2^{s+1} + 2^{s-1} - 3 < \Delta$. Thus $\Delta \notin E_{1,0}$.

Let $i = 1$ and $k > 1$, then $\delta \in E_{1,k} \Rightarrow \delta \geq 2^{s+2} + 2^{s-1} - 5 > \Delta$. Thus $\forall k \neq 1$, $\Delta \notin E_{1,k}$.

From Proposition 2, if $\forall i > 1$, $\Delta \not\equiv 1 \pmod{2^i}$ then $\Delta \notin E_{i,k}$ (for any value of k). Now, $\forall i > 1$, $\Delta \equiv 2j - 3 \pmod{2^i}$, thus

$$\begin{aligned} &2j - 3 \equiv 1 \pmod{2^i} \\ &\Rightarrow j \equiv 2 \pmod{2^{i-1}}, \end{aligned}$$

which is impossible since j is odd.

From Proposition 5, $\forall i = 1 \ldots s-1$, $\forall k$, $\Delta \notin F_{i,k}$.

From Propositions 3, 4 and 6, 7, $\forall i = 1 \ldots s-1$, $\forall k$, $\Delta \notin \bar{E}_{i,k,1} \cup \bar{E}_{i,k,2} \cup \bar{F}_{i,k,1} \cup \bar{F}_{i,k,2}$. ■

LEMMA 4. $\forall j$, $2^{s-2} + 3 \le j \le 2^{s-1} - 1$, *j odd*

- $2^{s+1} j + 2^{s-1} - 1 \in \bar{E}_{1,0,1}$ *(for* $\gamma = 0$*)*,
- $\forall k \neq 0$, $2^{s+1} j + 2^{s-1} - 1 \notin \bar{E}_{1,k,1}$,
- $\forall i > 1$, $\forall k$, $2^{s+1} j + 2^{s-1} - 1 \notin \bar{E}_{i,k,1}$,
- $\forall i = 1 \ldots s-1$, $\forall k$, $2^{s+1} j + 2^{s-1} - 1 \notin D_0 \cup D_1 \cup D_2 \cup D_{3,1} \cup D_{3,2} \cup E_{i,k} \cup \bar{E}_{i,k,2} \cup F_{i,k} \cup \bar{F}_{i,k,1} \cup \bar{F}_{i,k,2}$.

Proof. Let $\Delta = 2^{s+1} j + 2^{s-1} - 1$, notice that:

- Δ is odd,
- $\Delta \equiv 2^{s-1} - 1 \pmod{2^s}$,
- $2^{2s-1} + 2^{s+2} + 2^{s+1} + 2^{s-1} - 1 \le \Delta \le 2^{2s} - 2^{s+1} + 2^{s-1} - 1$,
- $\lfloor \frac{\Delta}{2^{s+1}} \rfloor = j$ is odd.

From Propositions 1a, 1b, 1c, 1d and 1e, $\Delta \notin D_0 \cup D_1 \cup D_2 \cup D_{3,1} \cup D_{3,2}$.

From Propositions 2 and 5, $\forall i = 1 \ldots s-1$, $\forall k$, $\Delta \notin E_{i,k} \cup F_{i,k}$.

Let $k \neq 0$, $\delta \in \bar{E}_{1,k,1} \Rightarrow \delta \equiv 2^{s-1} - 2k + \gamma - 1 \pmod{2^s}$. Thus if $2^{s-1} - 2k + \gamma - 1 \neq 2^{s-1} - 1$ then $\Delta \notin \bar{E}_{1,k,1}$. Now

$$2^{s-1} - 2k + \gamma - 1 = 2^{s-1} - 1 \Leftrightarrow \gamma = 2k.$$

Since $i = 1$, then $\gamma \ge 0$ and $\gamma \le 1$, hence there is a unique solution to the above equation: $k = \gamma = 0$. Thus, $\forall k \neq 0$, $\Delta \notin \bar{E}_{1,k,1}$.

Let $i \ge 2$ then, $\forall k$, $\delta \in \bar{E}_{i,k,1} \Rightarrow \exists j', \gamma$, such that

$$\frac{\delta}{2^{s+1}} = 2^{i-1}(k + j') + \frac{2^{s-1} - 2^i k + \gamma + 1 - 2^i}{2^{s+1}}.$$

Now since $\gamma + 1 - 2^i \le 0$ and $k \ge 0$, then

$$2^{s-1} - 2^i k + \gamma + 1 - 2^i \le 2^{s-1}.$$

Moreover since $2^i k \leq 2^{s-1} - 2^i$ and $\gamma \geq 0$, then

$$2^{s-1} - 2^i k + \gamma + 1 - 2^i \geq 1.$$

Hence

$$0 < \frac{2^{s-1} - 2^i k + \gamma + 1 - 2^i}{2^{s+1}} < 1.$$

Thus $\forall i \geq 2, \forall k, \delta \in \bar{E}_{i,k,1} \Rightarrow \lfloor \frac{\delta}{2^{s+1}} \rfloor$ is even. Hence $\Delta \notin \bar{E}_{i,k,1}$.
$\forall i = 1 \ldots s-1, \forall k$, let $\delta \in \bar{F}_{i,k,1}$, then $\delta \equiv \delta' \pmod{2^{s+1}}$, where $\delta' = 2^s + 2^{s-1} - 2^i (k+1) + \gamma$. Since $\gamma \geq 0$ and $k+1 \leq 2^{s-i-1}$, then $\delta' \geq 2^s$. Now $\Delta \equiv 2^{s-1} - 1 \pmod{2^{s+1}}$, hence $\Delta \notin \bar{F}_{i,k,1}$.

From Propositions 4 and 7, $\forall i = 1 \ldots s-2, \forall k \geq 1, \Delta \notin \bar{E}_{i,k,2} \cup \bar{F}_{i,k,2}$. ■

LEMMA 5. *$\forall j$, $2^{s-1} + 2 \leq j \leq 2^{s-1} + 2^{s-2}$, j even*

- $2^{s-1} + 2j - 1 \in E_{1,0}$,
- $\forall k \geq 1$, $2^{s-1} + 2j - 1 \notin E_{1,k}$,
- $\forall i > 1, \forall k$, $2^{s-1} + 2j - 1 \notin E_{i,k}$,
- $\forall i = 1 \ldots s-1, \forall k$, $2^{s-1} + 2j - 1 \notin D_0 \cup D_1 \cup D_2 \cup D_{3,1} \cup D_{3,2} \cup \bar{E}_{i,k,1} \cup \bar{E}_{i,k,2} \cup F_{i,k} \cup \bar{F}_{i,k,1} \cup \bar{F}_{i,k,2}$.

Proof. Let $\Delta = 2^{s-1} + 2j - 1$, notice that:

- Δ is odd,
- $2^s + 2^{s-1} + 3 \leq \Delta \leq 2^{s+1} - 1$,
- let us write $j = 2^{s-1} + j'$, $2 \leq j' \leq 2^{s-2}$, j' even. Then $\Delta \equiv 2^{s-1} + 2j' - 1 \pmod{2^s}$, and $2^{s-1} + 2j' - 1 \geq 2^{s-1} + 3 > 1$.

From Propositions 1a, 1b, 1c, 1d and 1e, $\Delta \notin D_0 \cup D_1 \cup D_2 \cup D_{3,1} \cup D_{3,2}$.

$\forall k \geq 1$, let $\delta \in E_{1,k}$, then $\delta \geq 2^{s-1} - 1 + 2(2^s - 1) > \Delta$, thus $\Delta \notin E_{1,k}$.

From Proposition 2, if $\forall i > 1$, $\Delta \not\equiv 1 \pmod{2^i}$ then $\Delta \notin E_{i,k}$ (for any value of k). Now $\forall i > 1$, $\Delta \equiv 2j - 1 \pmod{2^i}$, and

$$\begin{aligned} 2j - 1 &\equiv 1 \pmod{2^i} \\ \Rightarrow j &\equiv 1 \pmod{2^{i-1}}, \end{aligned}$$

which is impossible since j is even.

From Proposition 5, $\forall i, 1 \leq i \leq s-1, \forall k, \Delta \notin F_{i,k}$.

From Propositions 3, 4 and 6, 7, $\forall i, 1 \leq i \leq s-1, \forall k, \Delta \notin \bar{E}_{i,k,1} \cup \bar{E}_{i,k,2} \cup \bar{F}_{i,k,1} \cup \bar{F}_{i,k,2}$.

■

LEMMA 6. *$\forall j$, $2^{s-2} + 2 \leq j \leq 2^{s-1} - 2$, j even*

- $(j+1)2^{s+1}+2^{s-1}-2 \in \bar{E}_{1,1,1}$ *(for* $\gamma = 1$*),*
- $\forall k \neq 1$, $(j+1)2^{s+1}+2^{s-1}-2 \notin \bar{E}_{1,k,1}$,
- $\forall i > 1$, $\forall k$, $(j+1)2^{s+1}+2^{s-1}-2 \notin \bar{E}_{i,k,1}$,
- $\forall i = 1 \ldots s-1$, $\forall k$, $(j+1)2^{s+1}+2^{s-1}-2 \notin D_0 \cup D_1 \cup D_2 \cup D_{3,1} \cup D_{3,2} \cup E_{i,k} \cup \bar{E}_{i,k,2} \cup F_{i,k} \cup \bar{F}_{i,k,1} \cup \bar{F}_{i,k,2}$.

Proof. Let $\Delta = (j+1)2^{s+1}+2^{s-1}-2$, notice that:

- Δ is even,
- $\Delta \equiv 2^{s-1}-2 \pmod{2^s}$,
- $2^{2s-1}+2^{s+2}+2^{s+1}+2^{s-1}-2 \leq \Delta \leq 2^{2s}-2^{s+1}+2^{s-1}-2$,
- $\lfloor \frac{\Delta}{2^{s+1}} \rfloor = j+1$ is odd.

From Propositions 1a, 1b and 1c, $\Delta \notin D_0 \cup D_1 \cup D_2$.
Let $\delta \in D_{3,1}$, then $\delta \equiv 0 \pmod{2^s}$, thus $\Delta \notin D_{3,1}$.

From Proposition 1e, $\Delta \notin D_{3,2}$.

From Propositions 2 and 5, $\forall i = 1 \ldots s-1$, $\forall k$, $\Delta \notin E_{i,k} \cup F_{i,k}$.
Let $k \neq 1$, $\delta \in \bar{E}_{1,k,1} \Rightarrow \delta \equiv 2^{s-1}-2k+\gamma-1 \pmod{2^s}$. Thus if $2^{s-1}-2k+\gamma-1 \neq 2^{s-1}-2$ then $\Delta \notin \bar{E}_{1,k,1}$. Now

$$2^{s-1}-2k+\gamma-1 = 2^{s-1}-2 \Leftrightarrow \gamma = 2k-1.$$

Since $i = 1$, then $\gamma \geq 0$ and $\gamma \leq 1$, hence there is a unique solution to the above equation: $k = \gamma = 1$. Thus, $\forall k \neq 1$, $\Delta \notin \bar{E}_{1,k,1}$.
Let $i \geq 2$ then, $\forall k$, $\delta \in \bar{E}_{i,k,1} \Rightarrow \exists j'$, γ, such that

$$\frac{\delta}{2^{s+1}} = 2^{i-1}(k+j') + \frac{2^{s-1}-2^i k+\gamma+1-2^i}{2^{s+1}}.$$

Since

$$0 < \frac{2^{s-1}-2^i k+\gamma+1-2^i}{2^{s+1}} < 1,$$

(see proof of lemma 4), $\lfloor \frac{\delta}{2^{s+1}} \rfloor$ is even and thus $\forall i \geq 2$, $\forall k$, $\Delta \notin \bar{E}_{i,k,1}$.
$\forall i = 1 \ldots s-1$, $\forall k$, let $\delta \in \bar{F}_{i,k,1}$, then $\delta \equiv \delta' \pmod{2^{s+1}}$, where $\delta' = 2^s + 2^{s-1} - 2^i(k+1)+\gamma$. Since $\gamma \geq 0$ and $k+1 \leq 2^{s-i-1}$, then $\delta' \geq 2^s$. Now $\Delta \equiv 2^{s-1}-2 \pmod{2^{s+1}}$, hence $\Delta \notin \bar{F}_{i,k,1}$.

From Propositions 4 and 7, $\forall i = 1 \ldots s-2$, $\forall k \geq 1$, $\Delta \notin \bar{E}_{i,k,2} \cup \bar{F}_{i,k,2}$. ∎

5. The Reduced Redundancy Equation

PROPOSITION 2. *Let* $a(z) = \sum_{i=0}^{2^s-1} a_i z^i$ *be a polynomial of degree at most* $2^s - 1$. *If* $a(z)$ *satisfies the redundancy equation (1) then,* $\forall i \neq 0, 1, 2^{s-1}$, $a_i = 0$.

Proof. From Table 1:

- coefficients a_j are associated to monomials whose degree belongs to D_0, thus from Lemma 1, $\forall j, 2 \leq j \leq 2^{s-1} - 1$, j even, $a_j = 0$,
- coefficients a_j are associated to monomials whose degree belongs to D_2, thus from Lemma 2, $\forall j, 2^{s-1} + 1 \leq j \leq 2^s - 1$, j odd, $a_j = 0$,
- coefficients a_j^2 are associated to monomials whose degree belongs to $E_{1,1}$, thus from Lemma 3, $\forall j, 3 \leq j \leq 2^{s-2} + 1$, j odd, $a_j^2 = 0$, which implies $a_j = 0$
- coefficients $a_j^{2^{s+1}}$ are associated to monomials whose degree belongs to $\bar{E}_{1,0,1}$ (for $\gamma = 0$), thus from Lemma 4, $\forall j, 2^{s-2} + 3 \leq j \leq 2^{s-1} - 1$, j odd, $a_j^{2^{s+1}} = 0$, which implies $a_j = 0$,
- coefficients a_j^2 are associated to monomials whose degree belongs to $E_{1,0}$, thus from Lemma 5, $\forall j, 2^{s-1} + 2 \leq j \leq 2^{s-1} + 2^{s-2}$, j even, $a_j^2 = 0$, which implies $a_j = 0$,
- coefficients $a_{j+2^{s-1}}^{2^{s+1}}$ are associated to monomials whose degree belongs to $\bar{E}_{1,1,1}$ (for $\gamma = 1$), thus from Lemma 6, $\forall j, 2^{s-2} + 2 \leq j \leq 2^{s-1} - 2$, j even, $a_{j+2^{s-1}}^{2^{s+1}} = 0$, which implies $a_j = 0, \forall j, 2^{s-1} + 2^{s-2} + 2 \leq j \leq 2^s - 2$, j even. ■

Hence, if a polynomial $a(z)$ satisfies equation (1) then $a(z) = a_0 + a_1 z + a_{2^{s-1}} z^{2^{s-1}}$. This gives us a new distribution of degrees which appear in equation (1). We can now distribute them in 8 classes as shown in Table 3. We are now going to deduce, from this "reduced" redundancy equation, some properties over a_0, a_1 and $a_{2^{s-1}}$, in order to prove our main result.

PROPOSITION 3. *Let* $\Delta = 2^{s-1}$, *then*

- $\Delta \in D_0 \cup D_1 \cup E_{1,0,2}$,
- $\forall k \neq 0$, $\Delta \notin E_{1,k,2}$,
- $\forall i \geq 2$, $\forall k$, $\Delta \notin E_{i,k,2}$,
- $\forall i$, $1 \leq i \leq s - 1$, $\forall k$, $\Delta \notin D_2 \cup D_3 \cup E_{i,k,1} \cup F_{i,k,1} \cup F_{i,k,2}$.

Proof. Obviously, $\Delta \notin D_2 \cup D_3$. $\forall i$, $1 \leq i \leq s - 1$, $\forall k$, all elements of $E_{i,k,1}$ are odd, thus $\Delta \notin E_{i,k,1}$. ■

Let $i = 1$ and $k \neq 0$, then all elements of $E_{1,k,2}$ are greater than 2^s, hence $\Delta \notin E_{1,k,2}$.
Let $i \geq 2$, $\forall k$, all elements of $E_{i,k,2}$ are odd, thus $\Delta \notin E_{i,k,2}$.
$\forall i$, $1 \leq i \leq s - 1$, $\forall k$,

$$\delta \in F_{i,k,1} \cup F_{i,k,2} \Rightarrow \delta \geq 2^s + 2^{s-1} - 2^i \geq 2^s > \Delta$$

hence, $\Delta \notin F_{i,k,1} \cup F_{i,k,2}$.

Table 3. Reduced redundancy equation

$i = 0$		
D_0	$2^{s-1}, 2^{s-1}+1, 2^s$	$a_0, a_1, a_{2^{s-1}}$
D_1	$2^{s-1}, 2^{s-1}+2^s, 2^{s-1}+2^{2s-1}$	$a_0^{2^s}, a_1^{2^s}, a_{2^{s-1}}^{2^s}$
D_2	$2^{2s-1}, 2^{2s-1}+1, 2^{2s-1}+2^{s-1}$	$a_0, a_1, a_{2^{s-1}}$
D_3	$2^{2s-1}, 2^{2s-1}+2^s, 1$	$a_0^{2^s}, a_1^{2^s}, a_{2^{s-1}}^{2^s}$
$i \neq 0, k = 0 \ldots 2^{s-i-1}-1$		
$E_{i,k,1}$	$2^{s-1}-2^i+2^i k(2^s-1)+2^i j+1,\ j = 0, 1, 2^{s-1}$	$a_j^{2^i}$
$E_{i,k,2}$	$2^{s-1}-2^i+2^i k(2^s-1)+1,$	$a_0^{2^{s+i}}$
	$2^{s-1}-2^i+2^i k(2^s-1)+2^{s+i}+1,$	$a_1^{2^{s+i}}$
	$2^{s-1}-2^{i-1}+2^i k(2^s-1)+1$	$a_{2^{s-1}}^{2^{s+i}}$
$F_{i,k,1}$	$2^s+2^{s-1}-2^i+2^i k(2^s-1)+2^i j,\ j = 0, 1, 2^{s-1}$	$a_j^{2^i}$
$F_{i,k,2}$	$2^s+2^{s-1}-2^i+2^i k(2^s-1),$	$a_0^{2^{s+i}}$
	$2^{s+i}+2^s+2^{s-1}-2^i+2^i k(2^s-1),$	$a_1^{2^{s+i}}$
	$2^s+2^{s-1}-2^{i-1}+2^i k(2^s-1)$	$a_{2^{s-1}}^{2^{s+i}}$

COROLLARY 1. *Let $a(z)$ be a polynomial which satisfies equation (1), then*

$$a_{2^{s-1}}^{2^{s+1}} = \mathrm{Tr}_{\mathbb{F}_{2^{2s}}:\mathbb{F}_{2^s}}(a_0).$$

Proof. The sum of the coefficients of the monomials of degree 2^{s-1} which appear in equation (1) must be zero. From the above proposition there are exactly three monomials of degree 2^{s-1} in equation (1) whose corresponding coefficients are : a_0 (D_0), $a_0^{2^s}$ (D_1), $a_{2^{s-1}}^{2^{s+1}}$ ($E_{1,0,2}$). Thus, we conclude that $a_0 + a_0^{2^s} + a_{2^{s-1}}^{2^{s+1}} = 0$. ■

PROPOSITION 4. *Let $\Delta = 2^{s+1}+2^{s-1}-1$, then*

- $\Delta \in E_{1,1,1} \cup E_{1,0,2}$,
- $\forall k \neq 1,\ \Delta \notin E_{1,k,1}$,
- $\forall k \neq 0,\ \Delta \notin E_{1,k,2}$,
- $\forall i \geq 2,\ \forall k,\ \Delta \notin E_{i,k,1} \cup E_{i,k,2}$,
- $\forall i,\ 1 \leq i \leq s-1,\ \forall k,\ \Delta \notin D_0 \cup D_1 \cup D_2 \cup D_3 \cup F_{i,k,1} \cup F_{i,k,2}$.

Proof. Clearly, $\Delta \notin D_0 \cup D_1 \cup D_2 \cup D_3$.

Let $\delta \in E_{i,k,1}$, $(i,k) \neq (1,1)$,

- let $i \geq 2$, then $\delta \equiv 1 \pmod{2^i}$. Now $\Delta \equiv -1 \pmod{2^i}$,
- let $i = 1$ and $k \neq 1$, then since $\delta = 2^{s+1}k + 2^{s-1} + 2(j-k-1)$,
  - $\delta < 2^s + 2^{s-1} - 2 < \Delta$ $(k = 0)$,
  - $\delta > 2^{s+2} > \Delta$ $(k \geq 2)$.

Hence $\forall i, 1 \le i \le s-1, \forall k, i \ne 1$ or $k \ne 1$, $\Delta \notin E_{i,k,1}$.

Let $\delta \in E_{i,k,2}$, $(i,k) \ne (1,0)$, δ takes three values:

- $\delta = 2^{s-1} - 2^i + 2^i k(2^s - 1) + 1$. Then $\delta \equiv \delta' \pmod{2^s - 1}$, where $\delta' = 2^{s-1} - 2^i + 1 \le 2^{s-1} - 1$. Now $\Delta \equiv 2^{s-1} + 1 \pmod{2^s - 1}$.
- $\delta = 2^{s-1} - 2^i + 2^i k(2^s - 1) + 2^{s+i} + 1$
  - let $i = 1$ and $k \ge 1$, then $\delta = 2^{s+1} + 2^{s-1} + 2k(2^s - 1) - 1 > \Delta$,
  - let $i \ge 2$, then (since $2^i \le 2^{s-1}$) $\delta \ge 2^{s+2} + 1 > \Delta$.
- $\delta = 2^{s-1} - 2^{i-1} + 2^i k(2^s - 1) + 1$. Then $\delta \equiv \delta' \pmod{2^s - 1}$, where $\delta' = 2^{s-1} - 2^{i-1} + 1 \le 2^{s-1}$.

Hence $\forall i, 1 \le i \le s-1, \forall k, i \ne 1$ or $k \ne 0$, $\Delta \notin E_{i,k,2}$.

$\forall i, 1 \le i \le s-1, \forall k$, all elements of $F_{i,k,1}$ are even, thus $\Delta \notin F_{i,k,1}$.

$\forall i, 2 \le i \le s-1, \forall k$, all elements of $F_{i,k,2}$ are even, thus $\Delta \notin F_{i,k,2}$.

Let $i = 1, \forall k$, the first two elements of $F_{1,k,2}$ are even and the third one is equal to 2^{s-1} modulo $2^s - 1$, hence $\Delta \notin F_{1,k,2}$. ■

COROLLARY 2. *Let $a(z)$ be a polynomial which satisfies equation (1), then $a_1 \in \mathbb{F}_{2^s}$.*

Proof. The sum of the coefficients of the monomials of degree $2^{s+1} + 2^{s-1} - 1$ which appear in equation (1) must be zero. From the above proposition there are exactly two monomials of degree $2^{s+1} + 2^{s-1} - 1$ in equation (1) whose corresponding coefficients are : a_1^2 ($E_{1,1,1}$, $j = 1$) and $a_1^{2^{s+1}}$ ($E_{1,0,2}$). Thus, we conclude that

$$\begin{aligned} & a_1^{2^{s+1}} + a_1^2 = 0 \\ \Rightarrow\ & \mathrm{Tr}_{\mathbb{F}_{2^{2s}}:\mathbb{F}_{2^s}}(a_1) = 0 \\ \Rightarrow\ & a_1 \in \mathbb{F}_{2^s}. \end{aligned}$$

■

PROPOSITION 5. *Let $\Delta = 2^{s-1} + 1$, then*

- $\forall i, 1 \le i \le s-1$, $2^{s-1} + 1 \in D_0 \cup E_{i,0,1}$,
- $\forall i, 1 \le i \le s-1, \forall k \ne 0$, $2^{s-1} + 1 \notin E_{i,k,1}$,
- $\forall i, 1 \le i \le s-1, \forall k$, $2^{s-1} + 1 \notin D_1 \cup D_2 \cup D_3 \cup E_{i,k,2} \cup F_{i,k,1} \cup F_{i,k,2}$.

Proof. Clearly $\Delta \notin D_1 \cup D_2 \cup D_3$. $\forall i, 1 \le i \le s-1, \forall k \ge 1$, let $\delta \in E_{i,k,1}$ then $\delta \ge 2^{s+1} - 1 > \Delta$, hence $\Delta \notin E_{i,k,1}$.

$\forall i, 1 \le i \le s-1, \forall k$, let $\delta \in E_{i,k,2}$, then δ takes three values:

- $\delta = 2^{s-1} - 2^i + 2^i k(2^s - 1) + 1$, hence $\delta \equiv \delta' \pmod{2^s - 1}$, where $\delta' = 2^{s-1} - 2^i + 1 \le 2^{s-1} - 1 < \Delta$,
- $\delta = 2^{s-1} - 2^i + 2^i k(2^s - 1) + 2^{s+i} + 1 = \Delta + 2^{s+i} + 2^i k(2^s - 1) - 2^i > \Delta$,
- $\delta = 2^{s-1} - 2^{i-1} + 2^i k(2^s - 1) + 1$, hence $\delta \equiv \delta' \pmod{2^s - 1}$, where $\delta' = 2^{s-1} - 2^{i-1} + 1 \le 2^{s-1} < \Delta$.

Hence $\forall i,\ 1 \le i \le s-1,\ \forall k,\ \Delta \notin E_{i,k,2}$.
$\forall i,\ 1 \le i \le s-1,\ \forall k$, all elements of $F_{i,k,1}$ are even, thus $\Delta \notin F_{i,k,1}$.
$\forall i,\ 2 \le i \le s-1,\ \forall k$, all elements of $F_{i,k,2}$ are even, thus $\Delta \notin F_{i,k,2}$.
Let $i = 1, \forall k$, the first two elements of $F_{1,k,2}$ are even and the third one is equal to 2^{s-1} modulo $2^s - 1$, hence $\Delta \notin F_{1,k,2}$. ■

COROLLARY 3. *Let $a(z)$ be a polynomial which satisfies equation (1), then*

$$\mathrm{Tr}_{\mathbb{F}_{2^s}:\mathbb{F}_2}(a_1) = 0.$$

Proof. The sum of the coefficients of the monomials of degree $2^{s-1}+1$ which appear in equation (1) must be zero. From the above proposition there are exactly s monomials of degree $2^{s-1}+1$ in equation (1) whose corresponding coefficients are : a_1 (D_0) and $a_1^{2^i}$ ($E_{i,0,1}$, $j = 1$, $1 \le i \le s-1$). Thus, we conclude that:

$$\sum_{i=0}^{s-1} a_1^{2^i} = 0.$$ ■

6. The Main Result

THEOREM 1. *Let $g(z) = \mathrm{Tr}_{\mathbb{F}_{2^{2s}}:\mathbb{F}_{2^s}}(z)$ and $L = \mathbb{F}_{2^{2s}} \backslash \mathbb{F}_{2^s}$, the dimension of the Goppa code $\Gamma(L, g)$ satisfies:*

$$\dim \Gamma(L, g) = n - 2s \deg g(z) + 3s - 1.$$

Proof. From [13, 16], it is already known that $\dim \Gamma(L, g) \ge n - 2s \deg g(z) + 3s - 1$. Moreover, from trace description of Goppa codes (see §2), we know that:

$$\dim \Gamma(L, g) = n - 2s \deg g(z) + \dim_{\mathbb{F}_2} \ker(\mathrm{Tr}).$$

From [13], ker(Tr) is isomorphic to the set I equal to:

$$\{a(z) \in \mathbb{F}_{2^{2s}}[z] \mid g(z)^{2^{s-1}+1} \mathrm{Tr}_{\mathbb{F}_{2^s}:\mathbb{F}_2}\left(\frac{a(z)+a(z)^{2^s}}{g(z)}\right) \equiv 0 \pmod{z^{2^{2s}}+z}\}.$$

From Proposition 2, if $a(z) \in I$, then $a(z) = a_0 + a_1 z + a_{2^{s-1}} z^{2^{s-1}}$. From Corollary 1, $a_{2^{s-1}}$ is an element of the subfield $\mathbb{F}_{2^s}$ and for any given $a_{2^{s-1}} \in \mathbb{F}_{2^s}$, there are 2^s values of a_0 which satisfies $\mathrm{Tr}_{\mathbb{F}_{2^{2s}}:\mathbb{F}_{2^s}}(a_0) = a_{2^{s-1}}^{2^{s+1}}$. From Corollary 2, $a_1 \in \mathbb{F}_{2^s}$, and (from Corollary 3), $\mathrm{Tr}_{\mathbb{F}_{2^s}:\mathbb{F}_2}(a_1) = 0$. Therefore, there are exactly 2^{s-1} elements which satisfy such conditions. This means that I has at most $2^s 2^{s-1} 2^s$ distinct elements $a(z)$. We concluded that

$$\dim_{\mathbb{F}_2} \ker(\mathrm{Tr}) \le 3s - 1.$$ ■

In Table 4, we give for $s = 3$ and $s = 4$, the parameters of the associate trace Goppa code. First column contains n, k, d (d being the classical lower bound on the minimal distance) and $\bar{d}$ which is the minimal distance computed by a probabilistic algorithm [6]. For $s = 3$, $\bar{d}$ is the true minimal distance of the code. The middle column gives for n and k fixed the lower and upper bound on the minimum distance of a binary linear code as mentioned in [9]. The

Table 4.

$\Gamma(L, g)$	Linear	Non-Linear
$(n, k, d, \bar{d})$	$(n, k, d_{\min}, d_{\max})$	(n, r, d)
	$s = 3$	
(56, 16, 18, 20)	(56, 16, 20, 20)	(56, 17, 20)
	$s = 4$	
(240, 123, 34, 36)	(240, 123, 32, 52)	(240, 132, 30)

right column gives for n and d fixed, the value $n - r$ of the best known non-linear binary code $\mathcal{C}$ (as found in [9]) where $r = n - \log_2 \text{card}(\mathcal{C})$ is the so-called redundancy of the code.

Remark. It has been proved in [16], that codewords of trace Goppa codes have only even weight, which increases by 1 the general lower bound on the minimum distance.

References

1. S. V. Bezzateev and E. T. Mironchikov, N. A. Shekhunova, One subclass of binary Goppa codes, *Proc. XI Simp. po Probl. Izbit. v Inform. Syst.* (1986) pp. 140–141.
2. S. V. Bezzateev and N. A. Shekhunova, On the subcodes of one class Goppa Codes, *Proc. Intern. Workshop Algebraic and Combinatorial Coding Theory ACCT-1* (1988) pp. 143–146.
3. S. V. Bezzateev, E. T. Mironchikov and N. A. Shekhunova, A Subclass of Binary Goppa Code, *Problemy Peredachi Informatsii*, Vol. 25, No. 3 (1989) pp. 98–102.
4. S. V. Bezzateev and N. A. Shekhunova, Subclass of Binary Goppa Codes with Minimal Distance Equal to the Design Distance, *IEEE Trans. Info. Theory*, Vol. 41, No 2 (1995) pp. 554–555.
5. S. V. Bezzateev and N. A. Shekhunova, A subclass of binary Goppa codes with improved estimation of the code dimension, *Design, Codes and Cryptography*, Vol. 14, No. 1 (1998) pp. 23–38.
6. A. Canteaut and F. Chabaud, A new algorithm for finding minimum-weight words in a linear code: Application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511, *IEEE Trans. Info. Theory*, Vol. 44, No. 1 (1998) pp. 367–378.
7. P. Delsarte, On subfield subcodes of modified reed-solomon codes, *IEEE Trans. Info. Theory*, Vol. IT-21 (1975) pp. 575–576.
8. V. D. Goppa, A new class of linear error correcting codes, *Probl. Pered. Inform.*, Vol. 6, (1970) pp. 24–30.
9. V.S. Pless and W.C. Huffman (eds.), *Handbook of Coding Theory,* Vol. 1, North Holland, 1998.
10. J. M. Jensen, Subgroup subcodes, *IEEE Trans. Info. Theory*, Vol. 41, No. 3 (1995) pp. 781–785.
11. M. Loeloeian, J.Conan, A transform approach to goppa codes, *IEEE Trans. Info. Theory*, Vol. IT-33 (1987) pp. 105–115.
12. F. J. Mac Williams and N. J. A. Sloane, *The Theory of Error Correcting Codes,* North Holland (1983).
13. A. M. Roseiro, *The Trace Operator and Generalized Goppa Codes*, Ph.D. Dissert., Dept. of Elect. Eng., Michigan State Univ., East Lansing, MI 48823 (1989).
14. A. M. Roseiro, J. I. Hall, J. E. Hadney, M. Siegel, The trace operator and redundancy of Goppa codes, *IEEE Trans. Info. Theory.*, Vol. 38, No 3. (1992) pp. 1130–1133.
15. H. Stichtenoth, On the dimension of subfield subcodes, *IEEE Trans. Info. Theory.*, Vol. 36 (1990) pp. 90–93.
16. P. Véron, Goppa codes and trace operator, *IEEE Trans. Info. Theory*, Vol. 44, No. 1 (1998) pp. 290–295.
17. M. van der Vlugt, The true dimension of certain binary Goppa codes, *IEEE Trans. Info. Theory.*, Vol. 36, No. 2, (1990) pp. 397–398..
18. M. van der Vlugt, On the dimension of trace codes, *IEEE Trans. Info. Theory.*, Vol. 37, No. 1 (1991) pp. 196–199.