On quaternary Goppa codes

Markel Epelde[12], Xabier Larrucea[2], Ignacio F. Rúa[3]

[1]Universidad del País Vasco - Euskal Herriko Unibertsitatea, 48940 Leioa, Bizkaia, Spain

markel.epelde@tecnalia.com

[2]Tecnalia Research & Innovation, 48160 Derio, Bizkaia, Spain

[3]Departamento de Matemáticas, Universidad de Oviedo, 33007 Oviedo, Asturias, Spain

In [5], V. D. Goppa presents a new family of linear codes over finite fields. This family, now known as Goppa codes, has been studied for nearly 50 years, including efficient decoding algorithms [12] and its applications in cryptography [8]. Moreover, in [1], de Andrade and Palazzo present a generalization of Goppa codes to finite rings. Motivated by cryptographic applications, in this article we focus on Goppa codes over $\mathbb{Z}/4\mathbb{Z}$ and study some of their properties.

Keywords: Goppa codes, quaternary codes, McEliece cryptosystem.
MSC2010: 11T71, 94B05.

1 Introduction

Binary Goppa codes were chosen by Robert McEliece for his cryptosystem [8]. These codes have some interesting properties: namely, distinguishing a generator matrix of Goppa codes from a random binary matrix of the same size is an open problem, considered hard due to having been unsolved for 40 years. This property, along with the hardness of decoding an arbitrary linear code [2], provide the security of the McEliece crypstosystem. It is nowadays considered one of the main quantum-resitant schemes because it has been well-studied and understood.

In [4], Hammons, Kumar, Calderbank, Sloane and Solé proved that some nonlinear binary codes can be seen as Gray images of $\mathbb{Z}/4\mathbb{Z}$-linear codes. This discovery, along with the work of Nechaev [10] led to further research on quaternary codes, such as [3]. Namely, new codes with interesting properties have been found as extended cyclic codes over $\mathbb{Z}/4\mathbb{Z}$.

The goal of this article is to present a version of the McEliece cryptosystem over the Galois ring $\mathbb{Z}/4\mathbb{Z}$. In order to do this, we introduce Goppa codes over such a ring. We start by recalling classic Goppa codes' definition and parity-check matrix and de Andrade's and Palazzo's generalization to finite (and particularly Galois) rings in section 2. In sections 3 and 4.1 we present Goppa codes over $\mathbb{Z}/4\mathbb{Z}$ as a particular case of de Andrade's and Palazzo's definition, as well as proving some of their properties. We continue by suggesting an alternate definition of these codes in section 5, closer to Goppa's original definition. Finally, in section 6 we present a cryptosystem based on quaternary Goppa codes. We conclude with some final thoughts and open problems in section 7.

2 Preliminaries

Goppa codes are defined in [5] as follows.

Definition 1. Let $h, n \in \mathbb{N}$, $g \in \mathbb{F}_{2^h}[X]$ and $L = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{2^h}^n$ such that $\alpha_i \neq \alpha_j$ for $i \neq j$ and $g(\alpha_i) \neq 0$ for all $i = 1, \ldots, n$. The set

$$\Gamma_2(L, g) = \left\{ \boldsymbol{c} \in \mathbb{F}_2^n \mid \sum_{i=0}^{n} \frac{c_i}{X - \alpha_i} \equiv 0 \pmod{g(X)} \right\}$$

is called the binary Goppa code of parameters L and g. If g is irreducible, the code is said to be an irreducible Goppa code.

A parity-check matrix is also given in the same reference. Namely,

Lemma 1. *Let $\mathcal{C} = \Gamma_2(L, g)$ be a a binary Goppa code, with $L = (\alpha_1, \ldots, \alpha_n)$. If $r = \deg g$, then the following matrix*

$$H = \begin{pmatrix} g(\alpha_1)^{-1} & g(\alpha_2)^{-1} & \ldots & g(\alpha_n)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \alpha_2 g(\alpha_2)^{-1} & \ldots & \alpha_n g(\alpha_n)^{-1} \\ \alpha_1^2 g(\alpha_1)^{-1} & \alpha_2^2 g(\alpha_2)^{-1} & \ldots & \alpha_n^2 g(\alpha_n)^{-1} \\ \vdots & \vdots & & \vdots \\ \alpha_1^{r-1} g(\alpha_1)^{-1} & \alpha_2^{r-1} g(\alpha_2)^{-1} & \ldots & \alpha_n^{r-1} g(\alpha_n)^{-1} \end{pmatrix} \tag{1}$$

is a parity check matrix for $\mathcal{C}$, i.e., $\boldsymbol{c} \in \Gamma_2(L, g)$ if and only if $\boldsymbol{c}H^\intercal = \boldsymbol{0}$.

Strictly speaking, this is not a parity-check matrix since its entries are not necessarily in $\mathbb{F}_2$. However, substituting them by their coordinates in $\mathbb{F}_{2^h}$ with respect to a fixed $\mathbb{F}_2$-basis

and removing the redundant rows results in a classic parity-check matrix. Also note that this parity-check matrix implies that Goppa codes can be formulated as alternant codes [6]. In fact, we have that

$$\Gamma_2(L, g) = \mathrm{Alt}_r\left(L, (g(\alpha_i)^{-1})_{i=1}^n\right),$$

where $\mathrm{Alt}_m(\boldsymbol{a}, \boldsymbol{b})$ denotes the alternant code of order m and parameters $\boldsymbol{a}$ and $\boldsymbol{b}$, i.e., a binary linear code with parity-check matrix

$$\begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 b_1 & a_2 b_2 & \dots & a_n b_n \\ a_1^2 b_1 & a_2^2 b_2 & \dots & \alpha_n^2 b_n \\ \vdots & \vdots & & \vdots \\ a_1^{m-1} b_1 & a_2^{m-1} b_2 & \dots & a_n^{m-1} b_n \end{pmatrix}.$$

In [1], de Andrade and Palazzo generalize Goppa codes to finite rings based on the definition of Goppa codes as alternant codes. Namely, the following definition is introduced.

Definition 2. Let A be a local finite commutative ring with identity with residue field $\mathbb{F}_{p^m}$, R a Galois extension of A of degree $h \in \mathbb{N}$, and let G_s be the roots of $x^s - 1$ in R, where $s = p^{mh} - 1$. Let $g(X) \in R[X]$ of degree $r \in \mathbb{N}$ and $L = (\alpha_1, \dots, \alpha_n) \in G_s^n$ with $\alpha_i \neq \alpha_j$ for $i \neq j$ such that $g(\alpha_i)$ are units for $i = 1, \dots, n$. Then, the Goppa code $\Gamma_A(L, g)$ is the A-linear code with parity-check matrix (2).

Notice that when $A = \mathbb{Z}/4\mathbb{Z}$, the ring R can be taken as the Galois ring $GR(4^h, 4) = \frac{\mathbb{Z}/4\mathbb{Z}[X]}{(h(X))}$, where $h(X) \in A[X]$ is a monic polynomial such that its projection $\bar{\cdot}$ over $\mathbb{F}_2[X]$ is irreducible. In this Galois ring, the set

$$\mathcal{T}_h = \{a \in GR(4^h, 4) \mid a^{2^h} = a\}$$

is called the Teichmüler coordinate set of $GR(4^h, 4)$. This set is multiplicatively closed, and it is a field isomorphic to $\mathbb{F}_{2^h}$ with respect to the usual multuplication and the addition $a \oplus b \in \mathcal{T}_h$ such that $\overline{a + b} = \overline{a \oplus b}$ for all $a, b \in \mathcal{T}_h$.

3 Goppa codes over $\mathbb{Z}/4\mathbb{Z}$

In order to define Goppa codes over the ring $\mathbb{Z}/4\mathbb{Z}$, we consider the particular case of $A = \mathbb{Z}/4\mathbb{Z}$ in Definition 2. In this case, L will be a tuple of elements belonging to the Teichmüller coordinate set $\mathcal{T}_h$ of the extension $GR(4^h, 4)$ of $\mathbb{Z}/4\mathbb{Z}$.

Definition 3. Let $n, h \in \mathbb{N}$, $g(X) \in GR(4^h, 4)[X]$ of degree r and $L = (\alpha_1, \ldots, \alpha_n) \in \mathcal{T}_h^n$ with $\alpha_i \neq \alpha_j$ for $i \neq j$ and $g(\alpha_i)$ units. The quaternary Goppa code of length n and parameters g and L is defined as the $\mathbb{Z}/4\mathbb{Z}$-linear code with parity-check matrix (2) and it is denoted as $\Gamma_4(L, g)$.

Again, (2) is not a strict parity-check matrix but we can get one substituting its entries by their $\mathbb{Z}/4\mathbb{Z}$-coordinates with respect to a $\mathbb{Z}/4\mathbb{Z}$-basis of $GR(4^h, 4)$.

As a particular case of Definition 2, quaternary Goppa codes are guaranteed to have a minimum distance $d \geq r + 1$ and a specific decoding algorithm [1]. But this construction of Goppa codes given by the parity-check matrix allows us to prove some other properties for their use in cryptography. We will denote by ϕ the field isomophism between $\mathbb{F}_{2^h}$ and $\mathcal{T}_h$ given by $\phi(a) \in \mathcal{T}_h$ such that $\overline{\phi(a)} = a$ for all $a \in \mathbb{F}_{2^h}$, and we extend it to tuples, componentwise, and to codes, applying the function to every codeword. The bar notation will express the projection of an element in the Galois ring $GR(4^h, 4)$ over the finite field $\mathbb{F}_{2^h}$. This notation also extends to polynomials (coefficentwise), tuples and sets. Observe that $\bar{\cdot}$ restricted to $\mathcal{T}_h$ is the inverse map of ϕ.

Proposition 1. *Let $\Gamma_4(L, g)$ be a quaternary Goppa code of length n. Then,*

(i) $\overline{\Gamma_4(L, g)} \leq \Gamma_2(\overline{L}, \overline{g})$.

(ii) $\Gamma_4(L, g) \cap 2\,(\mathbb{Z}/4\mathbb{Z})^n \leq 2\phi(\Gamma_2(\overline{L}, \overline{g}))$. *If the leading coefficient of g is a unit, then the equality holds.*

(iii) If the leading coefficient of g is a unit, then $|\Gamma_4(L, g)| = |\overline{\Gamma_4(L, g)}| \cdot |\Gamma_2(\overline{L}, \overline{g})|$.

Proof. Let $L = (\alpha_1, \ldots, \alpha_n)$, $R = \deg g$ and $r = \deg \overline{g}$. First, observe that, since for any quaternary Goppa code $\Gamma_4((\alpha_i)_{i=1}^n, g)$, $g(\alpha_i)$ is a unit, $\overline{g}(\overline{\alpha_i}) \neq \overline{0}$ for $i = 1, \ldots, n$ and therefore the binary Goppa code $\Gamma_2(\overline{L}, \overline{g})$ is well-defined.

(i) Looking at its parity-check matrix (2),

$$\Gamma_4(L, g) = \left\{ \boldsymbol{c} \in (\mathbb{Z}/4\mathbb{Z})^n \;\middle|\; \sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-1} = 0,\ j = 1, \ldots, R \right\}. \tag{2}$$

Thus, since $r \leq R$,

$$\begin{aligned}\overline{\Gamma_4(L,g)} &= \left\{ \overline{\boldsymbol{c}} \in \mathbb{F}_2^n \;\mid\; \sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-1} = 0,\ j = 1, \ldots, R \right\} \\ &\leq \left\{ \overline{\boldsymbol{c}} \in \mathbb{F}_2^n \;\mid\; \overline{\sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-1}} = \overline{0},\ j = 1, \ldots, R \right\} \\ &\leq \left\{ \boldsymbol{c} \in \mathbb{F}_2^n \;\mid\; \sum_{i=1}^{n} c_i \overline{\alpha_i}^{j-1} \overline{g}(\overline{\alpha_i})^{-1} = \overline{0},\ j = 1, \ldots, r \right\} = \Gamma_2(\overline{L}, \overline{g}).\end{aligned}$$

(ii) Since $2\phi(\mathbb{F}_2) = 2(\mathbb{Z}/4\mathbb{Z})$,

$$\begin{aligned}\Gamma_4(L,g) \cap 2\left(\mathbb{Z}/4\mathbb{Z}\right)^n &= \left\{ 2\boldsymbol{c} \in 2(\mathbb{Z}/4\mathbb{Z})^n \mid \sum_{i=1}^{n} 2c_i \alpha_i^{j-1} g(\alpha_i)^{-1} = 0,\ j = 1, \ldots, R \right\} \\ &= \left\{ 2\boldsymbol{c} \in 2\phi(\mathbb{F}_2)^n \mid \overline{\sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-1}} = \overline{0},\ j = 1, \ldots, R \right\} \\ &\leq \left\{ 2\phi(\boldsymbol{c}) \in 2\phi(\mathbb{F}_2)^n \mid \sum_{i=1}^{n} c_i \overline{\alpha_i}^{j-1} \overline{g}(\overline{\alpha_i})^{-1} = \overline{0},\ j = 1, \ldots, r \right\} = 2\phi(\Gamma_2(\overline{L}, \overline{g})).\end{aligned}$$

Moreover, if $R = r$, this is, if the projection of leading coefficient over the finite field is not zero, the equality holds. This occurs when the leading coefficient of g is indeed a unit.

(iii) By (ii), if the leading coefficient of g is a unit it follows that the additive subgroup $S = \Gamma_4(L,g) \cap 2(\mathbb{Z}/4\mathbb{Z})^n \leq \Gamma_4(L,g)$ is equal to $2\phi(\Gamma_2(\overline{L}, \overline{g}))$. Thus, the order of the quotient group $\Gamma_4(L,g)/S$ is precisely $|\Gamma_4(L,g)|/|\Gamma_2(\overline{L}, \overline{g}))|$. Furthermore, as a consequence of (ii), if $\boldsymbol{c}, \boldsymbol{d} \in \Gamma_4(L,g)$, then $\overline{\boldsymbol{c}} = \overline{\boldsymbol{d}}$ if and only if their difference belongs to S, i.e. $\boldsymbol{c} + S = \boldsymbol{d} + S$. We conclude that $|\overline{\Gamma_4(L,g)}| = |\Gamma_4(L,g)|/|\Gamma_2(\overline{L}, \overline{g}))|$.

□

Example 1. Let us present some examples regarding the previous theorem. Let $u \in GR(4^5, 4)$ such that $\langle u \rangle = \mathcal{T}_5 \setminus \{0\}$. Let $g(X) = X^5 + u^2X^4 + uX^3 + u^2X^2 + uX + 1$ and

$$\begin{aligned}L = (&u, u^2, u^3, u^4, u^5, u^6, u^7, u^{26}, u^9, u^{10}, u^{11}, u^{12}, u^{13}, \\ &u^{14}, u^{15}, u^{16}, u^{17}, u^{18}, u^{19}, u^{20}, u^{21}, u^{27}, u^{23}, u^{24}, u^{25}) \in \mathcal{T}_5^{25}.\end{aligned}$$

The quaternary Goppa code defined by g and L is

$$\begin{aligned}\Gamma_4(L,g) = \langle &(2,0,2,2,2,2,0,2,2,2,0,2,2,0,2,2,0,0,0,2,2,0,0,2,2), \\ &(0,2,0,0,0,0,2,2,0,2,2,2,0,2,0,2,0,2,2,0,0,0,0,2,2)\rangle\end{aligned}$$

and the associated binary Goppa code is

$$\Gamma_2(\overline{L},\overline{g}) = \langle (1,0,1,1,1,1,0,1,1,1,0,1,1,0,1,1,0,0,0,1,1,0,0,1,1),$$
$$(0,1,0,0,0,0,1,1,0,1,1,1,0,1,0,1,0,1,1,0,0,0,0,1,1)\rangle.$$

(i) Note that the projection $\overline{\Gamma_4(L,g)} = \{\mathbf{0}\} \lneq \Gamma_2(\overline{L},\overline{g})$.

(ii) Part (ii) of Proposition 1 is satisfied, i.e. $\Gamma_4(L,g) = 2\phi(\Gamma_2(\overline{L},\overline{g}))$. However, $\Gamma_4(L, g + 2uX^9) = \{\mathbf{0}\}$ and therefore

$$\Gamma_4(L, g + 2uX^9) \lneq 2\phi(\Gamma_2(\overline{L}, \overline{g + 2uX^9})) = 2\phi(\Gamma_2(\overline{L},\overline{g})).$$

4 Change of parameters

Looking at Definition 3, one wonders whether changing parameters L and g of the quaternary Goppa codes has any effect towards the properties proved in section 3. In fact, in this section we propose modifying the values of L and g modulo 2, thus adding random elements from the ideals $2GR(4^h,4)$ and $2GR(4^h,4)[X]$ to the elements of L and g, respectively.

4.1 Invariance of g modulo 2

We want to prove that, in most of the cases, if we add a polyonomial in $2GR(4^h,4)[X]$ to the defining polynomial of a quaternary Goppa code, the code remains the same. First, let us present the following known lemma, which can be found in Chapter 12 of [6].

Lemma 2. *Let $h,n \in \mathbb{N}$, $L = (\alpha_1,\ldots,\alpha_n) \in \mathbb{F}_{2^h}^n$ where $\alpha_i \neq \alpha_j$ for $i \neq j$ and let $g \in \mathbb{F}_{2^h}[X]$ be a square free polynomial such that $g(\alpha_i) \neq 0$ for all $i = 1,\ldots,n$. Then, $\Gamma_2(L,g) = \Gamma_2(L,g^2)$.*

With this result we can present the following theorem.

Theorem 1. *Let $\Gamma_4(L,g)$ be a quaternary Goppa code, where $\overline{g}$ is a square free polynomial and $\deg g = \deg \overline{g} = r$, and let $\mathcal{P} = \{p \in GR(4^h,4)[X] \mid \deg p \leq r\}$. Then,*

$$\Gamma_4(L,g) = \Gamma_4(L, g + 2g_2),$$

for all $g_2 \in \mathcal{P}$.

Proof. By hyphotesis $\overline{g}$ is square free and therefore, by Lemma 2, $\Gamma_2(\overline{L},\overline{g}) = \Gamma_2(\overline{L},\overline{g}^2)$. Also, by part (i) of Proposition 1, $\overline{\Gamma_4(L,g)} \subseteq \Gamma_2(\overline{L},\overline{g}^2)$. This implies that, if $\boldsymbol{c} \in \Gamma_4(L,g)$, then

$\overline{\boldsymbol{c}} \in \Gamma_2(\overline{L}, \overline{g}^2)$. This last condition can be written using the parity-check matrix (2), as

$$\overline{\sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-2}} = \overline{0}, \qquad j = 1, \ldots, 2r.$$

Equivalenty,

$$\overline{\sum_{i=1}^{n} c_i \alpha_i^{k+j-1} g(\alpha_i)^{-2}} = \overline{0}, \qquad j = 1, \ldots, r, \quad k = 0, \ldots, r.$$

This can be written as

$$\overline{\sum_{k=0}^{r} \lambda_k \sum_{i=1}^{n} c_i \alpha_i^{k+j-1} g(\alpha_i)^{-2}} = \overline{0}, \qquad \forall j = 1, \ldots, r, \ \forall \lambda_k \in GR(4^h, 4).$$

Rearranging the terms,

$$\overline{\sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-2} \left(\sum_{k=0}^{r} \lambda_k \alpha_i^k \right)} = \overline{0}, \forall j = 1, \ldots, r, \ \forall \lambda_k \in GR(4^h, 4).$$

If we set $g_2(X) = \sum_{i=0}^{r} \lambda_i X^i$, then

$$\overline{\sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-2} g_2(\alpha_i)} = \overline{0}, \qquad \forall g_2 \in \mathcal{P}.$$

When $\boldsymbol{c} \in \Gamma_4(L, g)$, by (2) this is equivalent to

$$\sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-1} + 2 \sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-2} g_2(\alpha_i) = 0, \qquad j = 1, \ldots, r, \ \forall g_2 \in \mathcal{P}.$$

It can be easily proved that $(g(\alpha_i) + 2g_2(\alpha_i))^{-1} = g(\alpha_i)^{-1}(1 + 2g(\alpha_i)^{-1} g_2(\alpha_i))$. Thus, if $\boldsymbol{c} \in \Gamma_4(L, g)$ then

$$\sum_{i=1}^{n} c_i \alpha_i^{j-1} (g(\alpha_i) + 2g_2(\alpha_i))^{-1} = 0, \qquad j = 1, \ldots, r, \ \forall g_2 \in \mathcal{P},$$

and therefore $\boldsymbol{c} \in \Gamma_4(L, g + 2g_2)$. We have proved that $\Gamma_4(L, g) \subseteq \Gamma_4(L, g + 2g_2)$. But $\deg g + 2g_2 = \deg \overline{g + 2g_2} = r$ and $\overline{g + 2g_2} = \overline{g}$ is square free, so $\Gamma_4(L, g + 2g_2) \subseteq \Gamma_4(L, g)$ for all $g_2 \in \mathcal{P}$. We conclude that $\Gamma_4(L, g + 2g_2) = \Gamma_4(L, g)$. □

Example 2. Let us see some examples showing that the result in Theorem 1 fails when one of the hypothesis is not satisfied. Let $u \in GR(4^4, 4)$ such that $\mathcal{T}_4 \setminus \{0\} = \langle u \rangle$ and

$$L = (u^8, u^{12}, u^{13}, u, u^{11}, u^9, u^6, u^{14}, u^3, u^{10}, u^7, u^2) \in \mathcal{T}_4^{12}.$$

(i) Let $g_1(X) = 2X^3 + X^2 + X$. Then

$$\Gamma_4(L, g_1) = \langle (1,0,0,0,3,3,3,3,0,0,0,1), (0,2,0,0,2,2,0,0,2,2,0,2),$$
$$(0,0,0,2,0,0,2,2,2,0,2,2) \rangle,$$

whereas

$$\Gamma_4(L, g_1 + 2X^3) = \langle (1,0,0,0,3,3,3,3,0,0,0,1), (0,1,0,0,1,3,0,0,1,1,2,3),$$
$$(0,0,1,0,1,2,3,0,0,0,3,3), (0,0,0,1,0,0,3,3,3,2,3,1)\rangle.$$

Note that $3 = \deg g_1 \geq \deg \overline{g_1} = 2$.

(ii) Let $g_2(X) = X^2 + X$.

$$\Gamma_4(L, g_2) = \Gamma_4(L, g_1 + 2X^3) \neq \Gamma_4(L, g_1) = \Gamma_4(L, g_2 + 2X^3).$$

In this particular case, note that $X^3 \notin \mathcal{P}$.

(iii) Finally, let $g_3(X) = X^2$. In this case, $g_3(X)$ is not square free, and $\Gamma_4(L, g_3) \neq \Gamma_4(L, g_3 + 2X + 2X^2)$. In fact,

$$\Gamma_4(L, g_3) = \langle (1,0,0,0,0,0,0,1,0,1,1,0), (0,1,0,0,0,0,0,0,0,0,1,1),$$
$$(0,0,1,0,0,0,0,1,0,2,2,3), (0,0,0,1,0,0,0,1,1,3,2,3),$$
$$(0,0,0,0,1,0,0,1,1,0,3,3), (0,0,0,0,0,1,0,1,0,3,2,1),$$
$$(0,0,0,0,0,0,1,0,1,0,2,1), (0,0,0,0,0,0,0,2,1,1,1,1),$$
$$(0,0,0,0,0,0,0,0,2,2,2,2)\rangle,$$

while

$$\Gamma_4(L, g_3 + 2X + 2X^2) = \langle (1,0,0,0,0,1,1,0,0,3,0,1), (0,1,1,0,0,0,1,3,0,1,0,0),$$
$$(0,0,2,0,0,0,0,2,0,0,0,2), (0,0,0,1,0,0,0,1,1,3,2,3),$$
$$(0,0,0,0,1,1,0,2,1,3,1,0), (0,0,0,0,0,0,2,0,2,0,2,0,2),$$
$$(0,0,0,0,0,0,2,0,0,2,2,0), (0,0,0,0,0,0,0,0,0,2,2,2,2)\rangle.$$

4.2 Changes in L

Every element in the Galois ring $GR(4^h, 4)$ can be uniquely written as $a + 2b$, where $a, b \in \mathcal{T}_h$. In particular, every element in $\mathbb{Z}/4\mathbb{Z}$ can be expressed as $a + 2b$, where a and b are either 0 or 1. The elements a and b are usually denoted by $\gamma_0(c)$ and $\gamma_1(c)$, respectively [10]. For arbitrary elements α_i not necessarily in $\mathcal{T}_h$, we define the generalized quaternary Goppa codes as follows.

Definition 4. Let $n, h \in \mathbb{N}$, $g(X) \in GR(4^h, 4)[X]$ of degree r and $L = (\alpha_1, \ldots, \alpha_n) \in GR(4^h, 4)$ with $\overline{\alpha_i} \neq \overline{\alpha_j}$ for $i \neq j$ and $g(\alpha_i)$ units. We define the generalized quaternary Goppa code of length n and parameters g and L as the $\mathbb{Z}/4\mathbb{Z}$-linear code with parity-check matrix (2) and denote it by $\Gamma_4^{(e)}(L, g)$.

This generalized version of quaternary Goppa codes satisfies every property from Proposition 1 and Theorem 1. Moreover, since the difference between two components of L is still a unit, one can compute the minimum distance of the code based on the Vandermonde-like minors of the parity-check matrix and obtain as a result that the minimum distance remains greater than $r+1$ [1]. Summarizing, from this point of view the restriction $\alpha_i \in \mathcal{T}_h$ is not necessary.

Theorem 2. *Let $\Gamma_4^{(e)}(L+2L_2, g)$ be a generalized quaternary Goppa code, where $L = (\alpha_1, \ldots, \alpha_n)$ and $L_2 = (\beta_1, \ldots, \beta_n)$ and $L, L_2 \in \mathcal{T}_h^n$. If $\overline{\boldsymbol{c}}$ is a codeword of $\Gamma_2(\overline{L}, \overline{g})$, then, for all $\boldsymbol{d} \in (\mathbb{Z}/4\mathbb{Z})^n$, $\boldsymbol{c} + 2\boldsymbol{d} \in \Gamma_4^{(e)}(L + 2L_2, g)$ if and only if*

$$\overline{\sum_{i=1}^{n} c_i \left(\gamma_1(\alpha_i^{j-1} g(\alpha_i)^{-1}) + (j-1)\alpha_i^{j-2}\beta_i g(\alpha_i)^{-1} + \alpha_i^{j-1}\beta_i g(\alpha_i)^{-2} g'(\alpha_i) + \overline{\sum_{k=i+1}^{n} c_k \sqrt{\alpha_i^{j-1} g(\alpha_i)^{-1} \alpha_k^{j-1} g(\alpha_k)^{-1}}} \right)} = \overline{\sum_{i=1}^{n} d_i \alpha_i^{j-1} g(\alpha_i)^{-1}}$$

for all $j = 1, \ldots, r$. Moreover, if $\boldsymbol{c} + 2\boldsymbol{d} \in \Gamma_4^{(e)}(L, g)$, then $\boldsymbol{c} + 2\boldsymbol{d} \in \Gamma_4^{(e)}(L + 2L_2, g)$ iff

$$\overline{\sum_{i=1}^{n} c_i \alpha_i^{j-2} \beta_i g(\alpha_i)^{-1} \left(j - 1 + \alpha_i g(\alpha_i)^{-1} g'(\alpha_i)\right)} = \overline{0}$$

for all $j = 1, \ldots, r$.

Proof. On the one hand, it is easy to prove that $g(\alpha_i + 2\beta_i) = g(\alpha_i) + 2\beta_i g'(\alpha_i)$, so $g(\alpha_i + 2\beta_i)^{-1} = g(\alpha_i)^{-1}(1 + 2\beta_i g(\alpha_i)^{-1} g'(\alpha_i))$. Moreover, it is also straightforward that $(\alpha_i + 2\beta_i)^{j-1} = \alpha_i^{j-1} + 2(j-1)\alpha_i^{j-2}\beta_i$. By definition, $\boldsymbol{c} + 2\boldsymbol{d} \in \Gamma_4^{(e)}(L + 2L_2, g)$ iff

$$\sum_{i=1}^{n} c_i (\alpha_i + 2\beta_i)^{j-1} g(\alpha_i + 2\beta_i)^{-1} = 0, \qquad j = 1, \ldots, r,$$

or equivalently,

$$\sum_{i=1}^{n} (c_i + 2d_i) \alpha_i^{j-1} g(\alpha_i)^{-1} + 2 \sum_{i=1}^{n} c_i \alpha_i^{j-2} \beta_i g(\alpha_i)^{-1} \left(j - 1 + \alpha_i g(\alpha_i)^{-1} g'(\alpha_i)\right) = 0. \tag{3}$$

If $\boldsymbol{c} + 2\boldsymbol{d} \in \Gamma_4(L, g)$, then the first term is zero and we conclude the proof. If $\overline{\boldsymbol{c}} \in \Gamma_2(\overline{L}, \overline{g})$, then we have $\gamma_0(\sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-1}) = 0$, so $\sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-1} = 2\gamma_1(\sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-1})$, which results in (as showed in [10])

$$\sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-1} = 2 \left(\sum_{i=1}^{n} c_i \gamma_1(\alpha_i^{j-1} g(\alpha_i)^{-1}) + \sum_{i=1}^{n} \sum_{k=i+1}^{n} c_i c_k \sqrt{\alpha_i^{j-1} g(\alpha_i)^{-1} \alpha_k^{j-1} g(\alpha_k)^{-1}} \right).$$

Substituting this expression in (3) concludes the proof. □

Example 3. As we can see in this example, generalized quaternary Goppa codes are not invariant under L modulo 2. In fact, let us reconsider Example 2, and let $L_2 = (u, 0, \ldots, 0) \in \mathcal{T}_5^{12}$. Then

$$\Gamma_4^{(e)}(L + 2L_2, g_2) = \langle (1,0,0,0,1,3,3,3,0,0,2,3), (0,1,0,0,1,3,0,0,1,1,2,3), \\ (0,0,1,0,1,2,3,0,0,0,3,3), (0,0,0,1,0,0,3,3,3,2,3,1) \rangle,$$

which differs from $\Gamma_4^{(e)}(L, g_2) = \Gamma_4(L, g_2)$.

We leave the problem of simplifying conditions in Theorem 2 open, in order to determine more precisely the changes in the code implied by varying the elements in L modulo 2.

5 Alternate definition

In section 3 we have defined quaternary Goppa codes by generalizing the definition of binary Goppa codes as alternant codes as introduced in [1]. Definition 3 is used in the proofs of sections 3 and 4.1, but now we want to generalize Definition 1 directly, in terms of polynomial modular arithmetic.

Definition 5. Let $n, h \in \mathbb{N}$, $g(X) \in GR(4^h, 4)[X]$ of degree r and $L = (\alpha_1, \ldots, \alpha_n) \in \mathcal{T}_h^n$ with $\alpha_i \neq \alpha_j$ for $i \neq j$ and $g(\alpha_i)$ units. We define the polynomial quaternary Goppa code as

$$\Gamma_4^{(p)}(L, g) = \left\{ \boldsymbol{c} \in (\mathbb{Z}/4\mathbb{Z})^n \mid \sum_{i=1}^{n} \frac{c_i}{X - \alpha_i} \equiv 0 \pmod{g(X)} \right\}.$$

If the elements of L are taken in the Galois ring $GR(4^h, 4)$ with $\overline{\alpha_i} \neq \overline{\alpha_j}$ for $i \neq j$, we will refer to the resulting code as a generalized polynomial quaternary Goppa code and we denote it by $\Gamma_4^*(L, g)$.

In the case of classic Goppa codes, Definitions 3 and 5 are equivalent [5]. In the quaternary case, they are also equivalent provided the leading coefficient of g is a unit in the Galois ring $GR(4^h, 4)$.

Lemma 3. *Let $\Gamma_4(L, g)$ be a quaternary Goppa code and $\Gamma_4^{(p)}(L, g)$ the corresponding polynomial quaternary Goppa code. Then, $\Gamma_4(L, g) \leq \Gamma_4^{(p)}(L, g)$ and, if the leading coefficient of g is a unit, the equality holds.*

Proof. Let $g(X) = \sum_{i=0}^{r} g_i X^i$ and H as in (2). By definition, $\boldsymbol{c} \in \Gamma_4(L, g)$ iff $\boldsymbol{c}H^\intercal = \boldsymbol{0}$, and

this implies $\boldsymbol{c}H^{\intercal}H_g^{\intercal} = \mathbf{0}$, where

$$H_g = \begin{pmatrix} g_r & 0 & 0 & \dots & 0 \\ g_{r-1} & g_r & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ g_2 & g_3 & \dots & g_r & 0 \\ g_1 & g_2 & \dots & g_{r-1} & g_r \end{pmatrix}.$$

Observe that when the leading coefficient of g is a unit, the condition is equivalent since H_g is invertible. This matrix equality represents the following equalities.

$$\left.\begin{aligned} g_r(c_1 g(\alpha_1)^{-1} + \cdots + c_n g(\alpha_n)^{-1}) &= 0 \\ g_{r-1}(c_1 g(\alpha_1)^{-1} + \cdots + c_n g(\alpha_n)^{-1}) + g_r(c_1\alpha_1 g(\alpha_1)^{-1} + \cdots + c_n\alpha_n g(\alpha_n)^{-1}) &= 0 \\ &\vdots \\ g_1(c_1 g(\alpha_1)^{-1} + \cdots + c_n g(\alpha_n)^{-1}) + g_{r-1}(c_1\alpha_1 g(\alpha_1)^{-1} + \cdots + c_n\alpha_n g(\alpha_n)^{-1}) & \\ + \cdots + g_r(c_1\alpha_1^{r-1} g(\alpha_1)^{-1} + \cdots + c_n\alpha_n^{r-1} g(\alpha_n)^{-1}) &= 0 \end{aligned}\right\},$$

which can be written compiled into one polynomial equality. Namely,

$$\sum_{k=0}^{r-1}\left(\sum_{j=1}^{r-k} g_{k+j}\sum_{i=1}^{n} c_i\alpha_i^{j-1} g(\alpha_i)^{-1}\right) X^k = 0.$$

Rearranging the terms,

$$\sum_{i=1}^{n} c_i g(\alpha_i)^{-1}\sum_{k=0}^{r-1} X^k \sum_{j=1}^{r-k} g_{k+j}\alpha_i^{j-1} = 0. \tag{4}$$

Note that

$$\sum_{k=0}^{r-1} X^k \sum_{j=1}^{r-k} g_{k+j}\alpha_i^{j-1} = \sum_{j=0}^{r-1} g_j \sum_{k=1}^{j} \alpha_i^{j-k} X^k = \sum_{k=0}^{r} g_k \left(\frac{X^k - \alpha_i^k}{X - \alpha_i}\right) = \frac{g(X) - g(\alpha_i)}{X - \alpha_i}.$$

Thus, and since the degree of g is greater than the term on the left-hand side of (4), such equation can be written as

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

Therefore, $\boldsymbol{c} \in \Gamma_4(L, g)$ implies (and is equivalent to, when the leading coefficient of g is a unit)

$$\sum_{i=1}^{n} \frac{c_i}{X - \alpha_i} \equiv 0 \pmod{g(X)}, \qquad \text{i.e. } \boldsymbol{c} \in \Gamma_4^{(p)}(L, g).$$

□

Example 4. In general, if the leading coefficient of g is not a unit, then the equality does not hold. For instance, let us consider Example 2 again, and let $g(X) = 2X^3 + X^2 + X$. Then,

$$\Gamma_4^{(p)}(L, g_1) = \Gamma_4(L, g_2) \gneq \Gamma_4(L, g_1).$$

The following lemma is a key ingredient to relate the two definitions of quaternary Goppa codes.

Lemma 4. *Let $g(X)$ be a regular polynomial in $GR(4^h, 4)[X]$, i.e. $\overline{g(X)} \neq 0$. Then, there exists a monic polynomial $g^*(X) \in GR(4^h, 4)$ such that $\overline{g(X)} = \overline{g^*(X)}$, g and g^* have the same roots and there exists a unit $u(X) \in GR(4^h, 4)[X]$ such that $u(X)g(X) = g^*(X)$.*

Proof. The proof can be found in Chapter XIII of [7]. □

Theorem 3. *There exists a monic polynomial g^* such that $\Gamma_4^{(p)}(L, g) = \Gamma_4^{(p)}(L, g^*)$.*

Proof. We know, by Lemma 4, that $\Gamma_4^{(p)}(L, g) = \Gamma_4^{(p)}(L, ug^*)$, where $u(X)$ is a unit in $GR(4^h, 4)[X]$ and $g^*(X)$ is a monic polynomial such that $\overline{g(X)} = \overline{g^*(X)}$. By Definition 5, $\boldsymbol{c} \in \Gamma_4^{(p)}(L, ug^*)$ if

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

Since the elements in L are not roots of g, then $(u(X), X - \alpha_i) = 1$ for $i = 1, \ldots, n$. Multiplying the term in the left-hand side by $\prod_{i=1}^{n}(X - \alpha_i)$, it follows that $\boldsymbol{c} \in \Gamma_4^{(p)}(L, ug^*)$ if and only if $u(X)g^*(X)$ divides

$$\sum_{i=1}^{n} c_i \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (X - \alpha_i).$$

But, since u is a unit, this condition is verified exactly when $g^*(X)$ divides this term. Since g^* has the same roots as g and therefore $(g^*(X), X - \alpha_i) = 1$ for every $i = 1, \ldots, n$, this is equivalent to $\boldsymbol{c} \in \Gamma_4^{(p)}(L, g^*)$. □

A whole diagram of the relations between the various versions of Goppa codes can be seen in Figure 1. It follows that the polynomial versions of Goppa codes have similar properties to the originals.

Corollary 1. *Let $\Gamma_4^{(p)}(L, g)$ be a polynomial quaternary Goppa code.*

(i) The minimum distance of $\Gamma_4^{(p)}(L, g)$ is $d \geq \deg \overline{g} + 1$.

(ii) $\overline{\Gamma_4^{(p)}(L, g)} \leq \Gamma_2(\overline{L}, \overline{g})$.

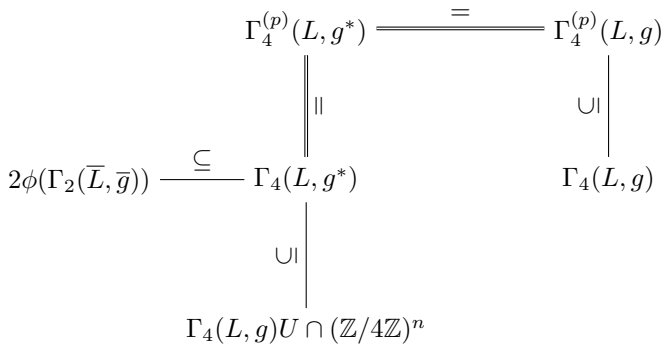

Figure 1: A map showing the relations between the different versions of quaternary Goppa codes presented in this article. Polynomial g^* is the monic polynomial associated with g by Lemma 4 and U is a diagonal matrix formed by the inverses of $u(\alpha_i)$, where u is a unit in $GR(4^h, 4)[X]$ that satisfies $g^*(X) = g(X)u(X)$.

(iii) $\Gamma_4^{(p)}(L, g) \cap 2\,(\mathbb{Z}/4\mathbb{Z})^n \leq 2\phi(\Gamma_2(\overline{L}, \overline{g}))$.

(iv) $|\Gamma_4(L, g)| = |\overline{\Gamma_4(L, g)}| \cdot |\Gamma_2(\overline{L}, \overline{g})|$.

(v) If $\overline{g}$ is square free, then $\Gamma_4^{(p)}(L, g) = \Gamma_4^{(p)}(L, g + 2g_2)$, for all $g_2(X) \in GR(4^h, 4)[X]$.

Proof. Applying Theorem 3, there exists a monic polynomial $g^*(X) \in GR(4^h, 4)$ such that $\Gamma_4^{(p)}(L, g) = \Gamma_4^{(p)}(L, g^*)$. This, along with Lemma 3, the proof of the minimum distance in [1] and Proposition 1, proves parts (i) to (iv).

Let us prove part (v). Let $g_2(X) \in GR(4^h, 4)[X]$. We know by Lemma Theorem 3 that there exists a monic $g_2^*(X) \in GR(4^h, 4)[X]$ such that, by Definition 5,

$$\Gamma_4^{(p)}(L, g + 2g_2) = \Gamma_4^{(p)}(L, g_2^*).$$

On the other hand, g^* and g_2^* are both monic and have the same degree since by Lemma 4 $\overline{g^*} = \overline{g} = \overline{g + 2g_2} = \overline{g_2^*}$, so there exists g_2' such that $g_2^* = g^* + 2g_2'$ and $\deg g_2' \leq \deg g^*$. But, since by Lemma 3 $\Gamma_4^{(p)}(L, g^*) = \Gamma_4(L, g^*)$, $\Gamma_4^{(p)}(L, g_2^*) = \Gamma_4(L, g_2^*)$ and $\overline{g^*} = \overline{g}$ is square free, Theorem 1 implies that necessarily $\Gamma_4^{(p)}(L, g^*) = \Gamma_4^{(p)}(L, g_2^*)$. We conclude that $\Gamma_4^{(p)}(L, g) = \Gamma_4^{(p)}(L, g + 2g_2)$. □

Finally, it should be noted that these results also work with the generalized version of the polynomial quaternary Goppa codes. In fact, the same proofs are valid for any choice of L's.

However, regarding the generalization of polynomial quaternary Goppa codes we present the following result.

Theorem 4. *Let $n, h \in \mathbb{N}$, $g(X) \in GR(4^h, 4)[X]$ of degree r, and let $L = (\alpha_1, \ldots, \alpha_n)$ and $L_2 = (\beta_1, \ldots, \beta_n)$ be with $L, L_2 \in GR(4^h, 4)^n$, $\overline{\alpha_i} \neq \overline{\alpha_j}$ for $i \neq j$ and $g(\alpha + 2\beta_i)$ units for every $i = 1, \ldots, n$. Then,*

$$\Gamma_4^*(L + 2L_2, g) = \left\{ \boldsymbol{c} \in (\mathbb{Z}/4\mathbb{Z})^n \mid \sum_{i=1}^{n} \frac{c_i}{X - \alpha_i} + 2\sum_{i=1}^{n} \beta_i \frac{c_i}{(X - \alpha_i)^2} \equiv 0 \pmod{g(X)} \right\}.$$

Proof. It is easy to check that the inverse of $X - \alpha_i + 2\beta_j$ modulo $g(X)$ is $(X - \alpha_i)^{-1}(1 + 2\beta_i(X - \alpha_i)^{-1})$ and thus

$$\begin{aligned}\Gamma_4^*(L + 2L_2, g) &= \left\{ \boldsymbol{c} \in (\mathbb{Z}/4\mathbb{Z})^n \mid \sum_{i=1}^{n} \frac{c_i}{X - \alpha_i + 2\beta_i} \equiv 0 \pmod{g(X)} \right\} \\ &= \left\{ \boldsymbol{c} \in (\mathbb{Z}/4\mathbb{Z})^n \mid \sum_{i=1}^{n} \frac{c_i}{X - \alpha_i} + 2\sum_{i=1}^{n} \beta_i \frac{c_i}{(X - \alpha_i)^2} \equiv 0 \pmod{g(X)} \right\}.\end{aligned}$$

□

Corollary 2. *Let $\Gamma_4^*(L + 2L_2, g)$ be a generalized polynomial quaternary Goppa code, where $L_2 = (\beta_1, \ldots, \beta_n)$. If $\overline{\beta_1} = \cdots = \overline{\beta_n}$ then*

$$\Gamma_4^*(L + 2L_2, g) = \Gamma_4^*(L, g).$$

Proof. It is a direct consequence of Theorem 4. In fact, let $\boldsymbol{c}, \boldsymbol{d} \in \{0, 1\}^n$. By Corollary 1 both $\boldsymbol{c} + 2\boldsymbol{d} \in \Gamma_4^*(L + 2L_2, g)$ and $\boldsymbol{c} + 2\boldsymbol{d} \in \Gamma_4^*(L, g)$ imply $\overline{\boldsymbol{c} + 2\boldsymbol{d}} \in \Gamma_2(\overline{L}, \overline{g})$ and thus $\overline{\sum_{i=1}^{n} c_i/(X - \alpha_i)} \equiv \overline{0}$ modulo $\overline{g}(X)$. Hence, squaring the term and multiplying it by the constant $\overline{\beta_i}$, it follows that $\overline{\sum_{i=1}^{n} \beta_i c_i/(X - \alpha_i)^2} \equiv \overline{0}$ modulo $\overline{g}(X)$, or equivalently, $2\sum_{i=1}^{n} \beta_i c_i/(X - \alpha_i)^2 \equiv 0$ modulo $g(X)$. We conclude that $\sum_{i=1}^{n} \frac{c_i + 2d_i}{X - \alpha_i} \equiv 0$ if and only if $\sum_{i=1}^{n} \frac{c_i + 2d_i}{X - \alpha_i} + 2\sum_{i=1} \beta_i \frac{c_i}{(X - \alpha_i)^2} \equiv 0$ and therefore $\Gamma_4^*(L + 2L_2, g) = \Gamma_4^*(L, g)$. □

Example 5. Let g_2, L and L_2 be as in Example 3. Then

$$\Gamma_4^*(L + 2L_2, g_2) = \Gamma_4^{(e)}(L + 2L_2, g_2) \neq \Gamma_4^{(e)}(L, g_2) = \Gamma_4^*(L, g_2).$$

This shows that generalized versions of polynomial quaternary Goppa codes are not invariant under L modulo 2.

6 Applications to cryptography

Goppa codes are the core of the original McEliece cryptosystem [8]. In this article we present the following variation of the scheme, orientated to Galois rings. Niederreiter's cryptosystem [11] can be equally generalized to rings.

Definition 6. Let R be a Galois ring, $n \in \mathbb{N}$ and $\mathcal{C} \subseteq R^n$ be a R-linear code with generator matrix G, error-correcting capacity $t \geq \delta$ and an efficient decoding algorithm $\mathcal{D}$. We define the Ring McEliece Cryptosystem as follows. The secret key is formed by G, $\mathcal{D}$, a random permutation matrix P and a random nonsingular matrix S. The pair (G', δ) forms the public key, where $G' = SGP$. We define the encryption function as $E(\boldsymbol{m}) = \boldsymbol{m}G' + \boldsymbol{e}$, where $\boldsymbol{e} \in R^n$ verifies $w(\boldsymbol{e}) \leq \delta$. In order to decrypt a ciphertext, we multiply it by P^{-1}, apply the decoding algorithm $\mathcal{D}$ and we conclude by solving linear equation systems to obtain the original message.

The security of both schemes (the original and the ring-based) is based on two major points. On the one hand, the problem of decoding random linear codes over the ring R. The proof presented by Berlekamp, McEliece and van Tilborg in [2] can be easily generalized to any Galois ring by just working with the zero and identity elements of the ring. On the other hand, one should ask the code $\mathcal{C}$ to be indistinguishable from a random code, i.e., one should not give any hint of G when publishing G'.

One of the most well-known families of linear codes over finite fields are Kerdock codes. These codes are binary and nonlinear, but their preimage under the Gray map is $\mathbb{Z}/4\mathbb{Z}$-linear [4]. However, the linear closure of classic Kerdock codes [6] and relatives [3] are Reed-Muller codes of order 2, which were proved to be distinguishable [9]. This also implies that Preparata, Delsarte-Goethals and other related codes are also distinguishable. Therefore, an indistinguishable code for the ring (or at least $\mathbb{Z}/4\mathbb{Z}$) version of McEliece needs to be found. Given their use in the binary version, Goppa codes seem as a good candidate for this task. In fact, Goppa codes distinguishability has not been proved for 40 years, and given the relations we have presented in this article, it seems likely that the distinguishability of their quaternary version is hard to prove as well. We now present a relation between the distinguishability of both version of codes.

Theorem 5. *Let $\mathcal{C}$ be the family of quaternary Goppa codes with generator polynomial whose leading coefficient is a unit. The Goppa distinguishability problem is as (computationally) hard as the distinguishability of codes from $\mathcal{C}$.*

Proof. Let us assume there exists a distinguisher $\mathcal{D}$ for binary Goppa codes, and let $\Gamma_4(L, g) \in \mathcal{C}$.

Then, computing $\Gamma_4(L,g) \cap 2\,(\mathbb{Z}/4\mathbb{Z})^n$ results in a subcode of $\Gamma_4(L,g)$ equivalent to $\Gamma_2(\overline{L},\overline{g})$, a binary Goppa code. Applying $\mathcal{D}$ to this code we could also distinguish $\Gamma_4(L,g)$. We have therefore reduced the distinguishability of an arbitrary code from $\mathcal{C}$ to the Goppa distinguishability problem. □

This result is valid also for the polynomial and generalized versions of the codes. Moreover, by Lemma 3, in polynomial versions of the code, the leading coefficient needs not be a unit. However, the converse is yet to be proved.

7 Conclusions

In this article we have studied the Goppa codes version over the ring $\mathbb{Z}/4\mathbb{Z}$. We have generalized de Andrade and Palazzo's definition in a particular case, and showed the 'inclusion' of binary Goppa codes in their quaternary versions. Finally, in terms of the coefficients, we have proved that in most of the cases varying g modulo 2 does not modify the code at all. Moreover, if we add a constant modulo 2 to each element in L, the code remains the same. An open question is whether we can manipulate this adding term to obtain stricter results in Proposition 1.

With cryptographic purposes, the results obtained inspire a version of McEliece cryptosystem over $\mathbb{Z}/4\mathbb{Z}$. This cryptosystem is promising to be secure with quaternary Goppa codes, due to the similarities with the binary version. However, the indistinguishability of these codes, and therefore, the security of the scheme, with respect to the binary case is yet to be proved.

References

[1] Andrade, A. A. de and Palazzo Jr., R. 'Goppa and Srivastava Codes over Finite Rings'. Computational & Applied Mathematics 24, no. 2 (August 2005). https://doi.org/10.1590/S0101-82052005000200005.

[2] Berlekamp, E., McEliece, R. and van Tilborg, H. 'On the Inherent Intractability of Certain Coding Problems (Corresp.)'. IEEE Transactions on Information Theory 24, no. 3 (May 1978): 384–86. https://doi.org/10.1109/TIT.1978.1055873.

[3] Borges, J., Phelps, K. T., Rifà, J. and Zinoviev, V. 'On Z4-Linear Preparata-like and Kerdock-like Code'. IEEE Trans. Information Theory 49 (2003): 2834–43. https://doi.org/10.1109/TIT.2003.819329.

[4] Hammons Jr, A. R., Kumar, P. V., Calderbank, A. R., Sloane, N. J. A. and Solé, P. 'The Z_4-Linearity of Kerdock, Preparata, Goethals and Related Codes'. ArXiv:Math/0207208, 23 July 2002. http://arxiv.org/abs/math/0207208.

[5] Goppa, V. D. 'A New Class of Linear Correcting Codes'. Probl. Peredachi Inf. 6, no. 3 (1970): 24–30.

[6] MacWilliams, F. J. and Sloane, N. J. A. 'The Theory of Error-Correcting Codes'. North-Holland Mathematical Library 16. Amsterdam: North-Holland Publ.Co, 1981.

[7] McDonald, B. R. 'Finite Rings with Identity'. M. Dekker, 1974.

[8] McEliece, R. J. 'A Public-Key Cryptosystem Based On Algebraic Coding Theory'. Deep Space Network Progress Report 44 (January 1978): 114–16.

[9] Minder, L. and Shokrollahi, A. 'Cryptanalysis of the Sidelnikov Cryptosystem'. In Advances in Cryptology - EUROCRYPT 2007, edited by Moni Naor, 347–60. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2007.

[10] Nechaev, A. A. 'Kerdock's code in cyclic form'. Discrete Mathematics and Applications, 1991, 1:4, 365–384, 1989.

[11] Niederreiter, H. 'Knapsack Type Cryptosystems and Algebraic Coding Theory'. Problems of Control and Information Theory 15 (1 January 1986): 183–90.

[12] Patterson, N. 'The Algebraic Decoding of Goppa Codes'. IEEE Transactions on Information Theory 21, no. 2 (March 1975): 203–7. https://doi.org/10.1109/TIT.1975.1055350.