A Gröbner Approach to Dual-Containing Cyclic Left Module (θ, δ)-Codes over Finite Commutative Frobenius Rings

Hedongliang Liu (lia.liu@tum.de)[1], Cornelia Ott (cornelia.ott@dlr.de)[2], and Felix Ulmer (felix.ulmer@univ-rennes1.fr)[3]

[1]School of Computation Information and Technology, Technical University of Munich, D-80333 München, Germany
[2]Institute of Communications and Navigation, German Aerospace Center (DLR), D-82234 Oberpfaffenhofen-Wessling, Germany
[3*]Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France

Abstract

For a skew polynomial ring $R = A[X; \theta, \delta]$ where A is a commutative Frobenius ring, θ an endomorphism of A and δ a θ-derivation of A, we consider cyclic left module codes $\mathcal{C} = Rg/Rf \subset R/Rf$ where g is a left and right divisor of f in R. In this paper, we derive a parity check matrix when A is a finite commutative Frobenius ring using only the framework of skew polynomial rings. We consider rings $A = B[a_1, \dots, a_s]$ which are free B-modules where the restriction of δ and θ to B are polynomial maps. If a Gröbner basis can be computed over B, then we show that all Euclidean and Hermitian dual-containing codes $\mathcal{C} = Rg/Rf \subset R/Rf$ can be computed using a Gröbner basis. We also give an algorithm to test if the dual code is again a cyclic left module code. We illustrate our approach for rings of order 4 with non-trivial endomorphism and the Galois ring of characteristic 4.

1 Introduction

For a (non-commutative) skew polynomial ring $R = A[X; \theta, \delta]$ where A is a commutative Frobenius ring, θ an endomorphism of the ring A and δ a θ-derivation of A (Definition 1), we consider codes that are cyclic left modules (i.e., generated by one element in R) of the form $\mathcal{C} = Rg/Rf \subset R/Rf$ with $f = hg$ for $g, f, h \in R$. In order to obtain a parity check matrix for such codes we will make the additional assumption that there exists $\hbar \in R$ such that $f = hg = g\hbar$ (i.e., g is a left and right divisor of f). A parity check matrix of such codes has been derived in a general approach in [10],

*Corresponding author.

The work of H. Liu has been supported by the German Research Foundation (DFG) with a German Israeli Project Cooperation (DIP) under grants no. PE2398/1-1, KR3517/9-1. The work of F. Ulmer has been by French projects ANR-11-LABX-0020-01"Centre Henri Lebesgue".

Keywords: self-dual code, dual-containing code, skew polynomial, module code, Gröbner basis, non-zero derivation, code over rings

in [4, Corollary 4] for $A = \mathbb{F}_q$ and in [8, 9] and for a finite commutative Frobenius ring A. The framework of pseudo-linear transformations is used in [8, 9, 10], while in this paper we only use the framework of skew polynomial rings. The entries of the parity check matrix are expressions in images under compositions of θ and δ of the coefficients of $\hbar$ and g, which are difficult to solve when searching for self-dual/dual-containing codes.

If $A = B[a_1, \dots, a_s]$ is a free B-module and the restriction of δ and θ to B are polynomial maps (Definition 4) then we can transform algebraic expressions of images under θ and δ into polynomial expressions over B. By representing the unknown coefficients of $\hbar$ and g as a linear combination of the algebra basis $B[a_1, \dots, a_s]$, we obtain multivariate polynomial expressions for the entries of a parity check matrix. The smallest unitary subring of a finite commutative ring A (the image of the canonical map $\mathbb{Z} \to A$ given by $1 \mapsto 1$) is either isomorphic to a finite field $\mathbb{F}_p$ of prime order or to an integer modular ring $\mathbb{Z}_m = \mathbb{Z}/(m)$ (note that p or m here is the characteristic of the ring A). Since θ and δ are polynomial maps over the smallest subalgebra $B \subset A$ and since polynomial equations over B can be solved using a Gröbner basis [1, 2], our approach applies to many rings A. Within the computation complexity constraints of the Gröbner basis, we can find all dual-containing codes $\mathcal{C} = Rg/Rf \subset R/Rf$ over A for any given parameters $[n, k]$. Using this approach we can also test various properties of codes $\mathcal{C} = Rg/Rf \subset R/Rf$.

1. In Section 4.2.1, we give an algorithm to compute, within the capability of the Gröbner basis computation, all (Hermitian-) dual-containing codes $\mathcal{C} = Rg/Rf \subset R/Rf$ over A for any given parameters $[n, k]$. Dual-containing codes play an important role in constructing quantum error-correcting codes.

2. In Table 8 and Table 3, we give examples of Hamming weight distribution of (Hermitian-) dual-containing codes $\mathcal{C} = Rg/Rf \subset R/Rf$ that could not be found without considering either non-zero derivations or non-trivial endomorphisms.

3. In Section 5, we give an example of a generating polynomial g of a $[6, 4]$ dual-containing code where all 8 polynomials $f = hg = g\hbar$ of degree 6 are non-central.

4. We give a procedure to decide whether the (Hermitian-) dual code $\mathcal{C}^\perp$ of a cyclic left module $\mathcal{C} = Rg/Rf \subset R/Rf$ is again a cyclic left module code $Rg^\perp/Rf \subset R/Rf$, i.e., generated by a single polynomial $g^\perp$.

5. In Section 4.2.2, we use the previous algorithm to show that many (Hermitian-) dual-containing codes $\mathcal{C} = Rg/Rf \subset R/Rf$ have a dual code which is not a cyclic left module code.

We apply our method to all commutative rings of order 4: $A = \mathbb{F}_2[v]/(v^2 + v)$, $A = \mathbb{F}_2[u]/(u^2)$, and $A = \mathbb{F}_4$, which have a non-trivial endomorphism. We also give some examples in characteristic 4 for the Galois ring

$$A = \mathrm{GR}(2, 2) = \mathbb{Z}_4[X]/(X^2 + X + 1).$$

2 Preliminaries

2.1 Skew Polynomial Rings

Let $A \neq \{0\}$ be a **unitary ring** (i.e., there exists $1 \in A \setminus \{0\}$, such that $1 \cdot a = a \cdot 1 = a, \forall a \in A$). We only consider **unitary endomorphisms** θ with the property that $\theta(1) = 1$. The identity automorphism will be denoted by id.

Definition 1. *Let $A \neq \{0\}$ be a unitary ring and θ an endomorphism of A. A **θ-derivation** is a map $\delta : A \to A$ such that, for all $a, b \in A$*

$$\delta(a+b) = \delta(a) + \delta(b) \quad \textit{and} \quad \delta(a\,b) = \delta(a)\,b + \theta(a)\,\delta(b).$$

*A θ-derivation δ is an **inner θ-derivation** if there exists $\beta \in A$ with the property that $\delta(x) = \beta x - \theta(x)\beta$ for all $x \in A$. For $\beta = 0$ we obtain the zero derivation which we denote 0.*

We also use the exponential notation $\theta(a) = a^\theta$ and $\delta(a) = a^\delta$ throughout the paper. Skew polynomial rings have been introduced and studied by Ore in [14]. A **skew polynomial ring** R is defined as a set of (left) polynomials $R = A[X;\theta,\delta] = \left\{\sum_{i=0}^n a_i X^i \mid a_i \in A, n \in \mathbb{N}\right\}$ with coefficients in the ring A. The addition in R is the usual polynomial addition and the multiplication is defined using the rule $Xa = a^\theta X + a^\delta$ which is extended using associativity and distributivity.

If the leading coefficient of $g \in R$ is invertible, then $\deg(hg) = \deg(h) + \deg(g)$ for all $h \in R$. In the case of a non-division ring A, if θ is an automorphism and the leading coefficient of $g \in R$ is invertible, then for any $f \in R$, we can perform a right (resp. left) division of f by g and we obtain a unique right (resp. left) remainder of degree $< \deg(g)$. To see this, let $g = \sum_{i=0}^m g_i X^i$, $f = \sum_{i=0}^n f_i X^i$ and $m \leq n$. Then for the right (resp. left) division, the degree of $f - (f_n \theta^{n-m}(g_m^{-1}) X^{n-m}) g$ (resp. $f - g \cdot (\theta^{-m}(g_m^{-1} f_n) X^{n-m})$) is less than the degree of f. To show that the right[1] division of $f \in R$ by a fixed $g \in R$ is unique, suppose that $f = hg + r = \tilde{h}g + \tilde{r}$. This implies that $(h - \tilde{h})g = \tilde{r} - r$. If $h - \tilde{h} = c_s X^s + \ldots$ is non-zero, then the leading monomial in $(h-\tilde{h})g$ is $c_s \theta^s(g_m) X^{s+m}$. A unitary automorphism maps 1 to 1 and invertible elements to invertible elements, so that $c_s \theta^s(g_m)$ is non-zero. Since the right side of $(h - \tilde{h})g = \tilde{r} - r$ is of degree $< m$ we obtain $h = \tilde{h}$ and $r = \tilde{r}$. Note that a unique right division of any $f \in R$ by a polynomial g with invertible leading coefficient exists even if θ is just an endomorphism.

2.2 Cyclic Left Module (θ,δ)-Codes $Rg/Rf \subset R/Rf$

Definition 2. *Let A be a finite ring, θ an endomorphism of A, δ a θ-derivation of A and $R = A[X;\theta,\delta]$ the corresponding skew polynomial ring. Let $f \in R$ be a **monic** skew polynomial of degree n and $g \in R$ be a right divisor of f. A **cyclic left module (θ,δ)-code** (in short (θ,δ)-code) is defined as $\mathcal{C} = Rg/Rf \subset R/Rf$ in the polynomial representation, and as*

$$C = \{\boldsymbol{c} = (c_0, c_1, \ldots, c_{n-1}) \mid c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} \in Rg/Rf\}$$

in the vector representation.

Note that (θ,δ)-codes with endomorphism and derivation have been studied in [7, 8, 9, 15]. For $\delta = 0$ and $f = X^n - 1$ we obtain θ-cyclic codes characterized by

$$(a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \in C \;\Rightarrow\; (\theta(a_{n-1}), \theta(a_0), \theta(a_1), \ldots, \theta(a_{n-2})) \in C$$

while the classical cyclic code correspond to $f = X^n - 1$, $\theta = \mathrm{id}$ and $\delta = 0$ (in this case R is a commutative univariate ring).

Proposition 1. *Let $g \in R = A[X;\theta,\delta]$ of degree $n-k$ be a right divisor of a monic skew polynomial $f \in R$ of degree n. A cyclic left module (θ,δ)-code $\mathcal{C} = Rg/Rf \subset R/Rf$ has the following properties:*

[1] The uniqueness of the left division can be shown in the similar manner.

- *The left R-module R/Rf is also a free A-module isomorphic to A^n with A-basis $(1, X, \dots, X^{n-1})$.*
- *Rg/Rf is a left R-submodule of R/Rf.*
- *Rg/Rf is also a free left A-submodule of $R/Rf \cong A^n$ of dimension $k = \deg(f) - \deg(g)$ (i.e. a linear code of length n and dimension k over the alphabet A).*
- *If g is a left and right divisor of $f = hg = g\hbar$, then we can assume that all the three polynomials in $f = hg$ for a cyclic left module (θ,δ)-code $Rg/Rf \subset R/Rf$ are monic (i.e. have leading coefficient 1). The monic generator polynomial g of a cyclic left module (θ,δ)-code $Rg/Rf \subset R/Rf$ is unique.*
- *If g is a left and right divisor of $f = hg = g\hbar$ and θ is an automorphism, then we can assume that all the four polynomials in $f = hg = g\hbar$ for a cyclic left module (θ,δ)-code $Rg/Rf \subset R/Rf$ are monic.*

Proof. Since f is monic we can perform a right division of any element of R by f and produce a unique remainder of degree $< n$. Therefore any element of the R-module R/Rf has a unique representation (the remainder of the division) of degree $< n$ in R/Rf. Viewed as an A-module, R/Rf is a free A-module with basis $1, X, \dots, X^{n-1}$ (i.e. every element in R/Rf is a unique linear combination of those elements).

For $g \in R$ we have $Rf \subset Rg$ if and only if g is a right factor of f and in this case Rg/Rf is a cyclic left R-submodule of R/Rf generated by $g + Rf$. The leading coefficient g_{n-k} of $g = \sum_{i=0}^{n-k} g_i X^i$ is a right divisor of 1 and is therefore invertible. This shows that $\deg(hg) = \deg(h) + \deg(g)$ for all $h \in R$ and implies that the R-module Rg/Rf is a free A-module of rank k of A^n with basis $g, Xg, \dots, X^{k-1}g$.

We now prove the fourth statement for $g = g_{n-k}X^{n-k} + \dots + g_0$ and $h = h_k X^k + \dots + h_0$. If $f = hg = g\hbar$, since f is monic, the leading coefficient of $f = hg$ is $h_k \theta^k(g_{n-k}) = 1$, showing that h_k and $\theta^k(g_{n-k})$ are invertible. We obtain

$$\begin{aligned} f &= \underbrace{(h_k X^k + \dots + h_0)}_{h} \cdot \underbrace{(g_{n-k}X^{n-k} + \dots + g_0)}_{g} \\ &= \underbrace{(h_k X^k + \dots + h_0) \cdot g_{n-k}}_{\tilde{h}} \cdot \underbrace{g_{n-k}^{-1} \cdot (g_{n-k}X^{n-k} + \dots + g_0)}_{\tilde{g}} \end{aligned}$$

In this representation $\tilde{g}$ is a monic polynomial. Since the endomorphism θ maps 1 to 1, the product rule of $A[X;\theta,\delta]$ shows that the leading coefficient of $\tilde{h}\tilde{g}$ is the leading coefficient of $\tilde{h}$. Because $\tilde{h}\tilde{g} = f$ is monic, we obtain that $\tilde{h}$ is also a monic polynomial. The polynomials g and $\tilde{g}$ differ by an invertible element. Using the above equations in both directions we see that any multiple of g by a polynomial of degree $\leq k-1$ is also a multiple of $\tilde{g}$ by a polynomial of degree $\leq k-1$ and vice versa. Therefore $Rg/Rf = R\tilde{g}/Rf$, showing that g and $\tilde{g}$ generate the same codes. Hence, without loss of generality, we can assume that f, h and g are monic. If C is a cyclic left module (θ,δ)-code with parameters $[n,k]$ and monic generator polynomial g, then any codeword is of the form $c = m \cdot g$ with $\deg(g) = n-k$ and $\deg(m) < k$. In particular the only monic polynomial of degree $n-k$ in $\mathcal{C}$ is $g = 1 \cdot g$.

We now show that $\hbar = \hbar_k X^k + \dots + \hbar_0$ is monic if θ is an automorphism. According to the above we can assume that f and g are monic, so that the leading coefficient $\theta^{n-k}(\hbar_k)$ in $g\hbar = f$ must be 1. Since θ^{n-k} is an automorphism, we obtain that $\hbar_k = 1$. ∎

Example 1. *The Frobenius chain ring $A = \mathbb{F}_2[u]/(u^2)$ is a free $\mathbb{F}_2$-module $\mathbb{F}_2[u]$ with $\mathbb{F}_2$ basis $[1, u]$. The only automorphism of A is the identity $\theta_1 : x \mapsto x$. There is a unique endomorphism defined by $\theta_2(u) = 0$ (note that $\theta_2(1) = 1$) which is a polynomial map on $\mathbb{F}_2$ and on A itself $\theta_2 : x \mapsto x^2$. Any θ-derivation δ is determined by $\delta(u)$ (note that $\delta(1) = \delta(0) = 0$). The list of θ-derivation is:*

	Automorphism	*Endomorphism*
	$\theta_1 = \mathrm{id}$	$\theta_2 : u \mapsto 0$
$\delta_1 = 0$	$u \mapsto 0$	$u \mapsto 0$
δ_2	$u \mapsto 1$	
δ_3	$u \mapsto u$	$u \mapsto u$
δ_4	$u \mapsto u + 1$	

We marked the inner θ-derivation by a gray cell.

In Proposition 1 we showed that all the three polynomials in $f = hg$ for a cyclic left module (θ, δ)-code $Rg/Rf \subset R/Rf$ can be chosen to be monic. If θ is a non-trivial endomorphism, i.e., not an automorphism, the $\hbar$ in the decomposition $f = g\hbar$ is not necessarily monic. To see this, consider the ring $R = A[X; \theta_2(u) = 0, \delta_3(u) = u]$ and the code Rg/Rf with $g = X^2 + uX + u + 1$ and $f = X^4 + (u + 1)X^3 + X + u + 1$. It can be found that $f = hg$ with $h = X^2 + (u + 1)X + 1$, and $f = g\hbar$ with $\hbar = (u + 1)X^2 + (u + 1)X + u + 1$ or $\hbar = (u + 1)X^2 + X + u + 1$.

The **encoding** of the information $(b_0, b_1, \ldots, b_{k-1}) \in A^k$ in a cyclic left module (θ, δ)-code $\mathcal{C} = Rg/Rf \subset R/Rf$ is given by the coefficients of $(\sum_{i=0}^{k-1} b_i X^i)g \in R$. A **generator matrix** of the code is of the following form:

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & \\ g_0^{\delta} & g_1^{\delta} + g_0^{\theta} & g_2^{\delta} + g_1^{\theta} & \cdots & g_{n-k}^{\theta} & 0 & \cdots \\ \vdots & \ddots & \ddots & \cdots & \ddots & \ddots & \\ g_0^{\delta^{k-1}} & & \cdots & & \cdots & & g_{n-k}^{\theta^{k-1}} \end{pmatrix}$$

The rows are given by the coefficients of $g, X \cdot g, \ldots, X^{k-1} \cdot g$ and can be computed using the rule $Xa = a^{\theta}X + a^{\delta}$ for $a \in A$. In particular, the code is completely determined by g, θ and δ.

Example 2. *In the notations of the above definition, consider a unitary polynomial $f = hg$ in $R = A[X; \theta, \delta]$ of degree 4 with $g = g_1 X + g_0$, $h = \sum_{i=0}^{3} h_i X^i$ and $h_3 g_1 = 1$. The code $\mathcal{C} = Rg/Rf \subset R/Rf$ is a $[4, 3]_A$ code whose generating matrix is*

$$G = \begin{pmatrix} g_0 & g_1 & 0 & 0 \\ g_0^{\delta} & g_1^{\delta} + g_0^{\theta} & g_1^{\theta} & 0 \\ g_0^{\delta^2} & g_0^{\delta\theta} + g_0^{\theta\delta} + g_1^{\delta^2} & g_0^{\theta^2} + g_1^{\delta\theta} + g_1^{\theta\delta} & g_1^{\theta^2} \end{pmatrix}.$$

If θ is of the form $a \mapsto a^{p^m}$ and δ is an inner θ-derivation $a \mapsto \beta a - \theta(a)\beta$ (those are the only possibilities if A is a finite field $\mathbb{F}_q$), then the entries of the above matrix become polynomials in the coefficients of g and allow sophisticated computations. This is the reason why almost all known examples of self dual (θ, δ)-code consider A to be a finite field.

Definition 3 (Hermitian Inner Product and Hermitian Dual)**.** *Let σ be an automorphism of A whose order divides 2. The **σ-Hermitian inner product** of $\boldsymbol{x}, \boldsymbol{y} \in A^n$ is defined as $\langle \boldsymbol{x}, \boldsymbol{y} \rangle_\sigma = \sum_{i=1}^{n} x_i \sigma(y_i)$. The **($\sigma$-Hermitian) dual code** of a code C is defined as*

$$C^{\perp_\sigma} = \{\boldsymbol{v} \mid \langle \boldsymbol{v}, \boldsymbol{c} \rangle_\sigma = 0, \ \forall \boldsymbol{c} \in C\} .$$

*A code is σ-**dual-containing** if $C^{\perp_\sigma} \subset C$ and σ-*self dual *if $C = C^{\perp_\sigma}$.*

If $\sigma = \mathrm{id}$, the identity automorphism, we obtain the Euclidean inner product over A^k and the Euclidean dual. In this case, we omit the σ in the notation.

Lemma 1. *([16]) Let A be a commutative Frobenius ring and C be a linear code over A. Then for the (Hermitian) dual code $C^{\perp_\sigma}$ we have $|C| \cdot |C^{\perp_\sigma}| = |A|^n$.*

3 Parity Check Matrix and Generating Matrix of the Euclidean and Hermitian Dual Code

A parity check matrix of a cyclic left module (θ, δ)-code $\mathcal{C} = Rg/Rf \subset R/Rf$ over a field $\mathbb{F}_q$ (where all derivations must be inner) is given in [4, Corollary 4] and over a commutative Frobenius ring in [8, 9]. In [15] a parity check matrix for a cyclic left module (θ, δ)-code $\mathcal{C} = Rg/Rf \subset R/Rf$ over the ring $A = (\mathbb{Z}/4\mathbb{Z})[X]/(X^2 - 1)$ is studied when $f = hg$ is a central polynomial. Our approach is similar to [4] and [15]. In this case Rg/Rf is an ideal in R/Rf. In the next theorem we follow the assumption in [4, 6, 8] that g is both a right and a left divisor of f, i.e., $f = hg = g\hbar$, in which case Rg/Rf is usually only a submodule of R/Rf. The assumption that $f = hg = g\hbar$ is much weaker than the assumption that f is central (see the $[6, 4]$ example in Section 5).

Lemma 2. *Let θ be an endomorphism of the finite ring A, δ a θ-derivation on A, $R = A[X; \theta, \delta]$, $f \in R$ a monic polynomial having both a right and a left divisor g (i.e. $f = hg = g\hbar$) and $\mathcal{C} = Rg/Rf \subset R/Rf$ a cyclic left module (θ, δ)-code. A word in A^n corresponding to an element $w \in R$ of degree $< n$ is a codeword of $\mathcal{C}$ if and only if (the coset of) $w \cdot \hbar = 0$ in R/Rf. We obtain an $n \times n$ matrix M such that the vector representation of $\mathcal{C}$ is $C = \{\boldsymbol{w} \in A^n \mid \boldsymbol{w}M = \vec{0}\}$ (i.e. $C = \mathrm{lker}(M)$ is a left kernel of M), where the entries of M are images under compositions of θ and δ of the coefficients of $\hbar$ and g. The i-th row of M corresponds to the coefficients of $X^{i-1}\hbar \mod f$, for $i = 1, \ldots, n$.*

Proof. Since f is monic, an element of $A^n \cong R/Rf$ has a unique representation as a remainder of the right division by f, which corresponds to a polynomial $w \in R$ of degree $< n$. Following [5, Lemma 8] we now show that w corresponds to a codeword if and only if (the coset of) $w \cdot \hbar = 0$ in R/Rf. If $w \in \mathcal{C}$, then $w = \tilde{w}g$ for some $\tilde{w} \in R$. Therefore $w\hbar = \tilde{w}g\hbar = \tilde{w}(h \cdot g)$ showing that $w\hbar = 0$ in $R/Rf = R/R(h \cdot g)$. Conversely, if $w\hbar = 0$ in $R/Rf = R/R(h \cdot g)$, then $w\hbar = \tilde{w}(h \cdot g) = \tilde{w}(g\hbar)$ for some $\tilde{w} \in R$. Since $\hbar$ is not a zero divisor in R we obtain $w = \tilde{w}g$, showing that $w \in \mathcal{C}$.

Since f is monic, a word in A^n corresponds to a coset $w = \sum_{i=0}^{n-1} a_i X^i \in R/Rf$. Such a coset $w = \sum_{i=0}^{n-1} c_i$ belongs to $\mathcal{C}$ if and only if $w\hbar = 0$ in R/Rf. The coefficients of

$$w\hbar \mod f = \left(\sum_{i=0}^{n-1} c_i X^i\right)\left(\sum_{i=0}^{k} \hbar_i X^i\right) \mod f$$

are obtained by bringing the coefficients $\hbar_i$ to the left side and performing the right division of f. The code C corresponds to the left kernel of this linear system and can therefore be represented as the left kernel of a matrix M, i.e., $\sum_{i=0}^{n-1} c_i M_{i,j} X^j = 0,\ \forall j \in [0, n-1]$. The entries $M_{ij} \in A$ are the images under θ and δ of the coefficients of $\hbar$ and f. Since $f = g\hbar$, the entries $M_{ij} \in A$ are images under θ and δ of the coefficients of $\hbar$ and g. The i-the row of M corresponds to the contribution of $c_i X^i \cdot \hbar \mod f$ in the product $w\hbar = 0 \mod f$. ∎

Example 3 (A toy example for $n = 3, k = 1$). *Consider a ring A, a skew polynomial ring $R = A[X;\theta,\delta]$ and $f = X^3 + \sum_{i=0}^{2} f_i X^i \in R$ such that $f = g\hbar$ in $A[X;\theta,\delta]$ for $g = g_2X^2 + g_1X + g_0$ and $\hbar = \hbar_1 X + \hbar_0$. According to Lemma 2, $w = c_0 + c_1X + c_2X^2$ belongs to $\mathcal{C} = Rg/Rf \subset R/Rf$ if and only if $w\hbar = 0$ in R/Rf, i.e. $w\hbar \equiv 0 \mod f$. Since*

$$\begin{aligned} w\hbar \mod f = & \left(c_2(\hbar_1^{\theta\delta} + \hbar_1^{\delta\theta} + \hbar_0^{\theta^2} - \hbar_1^{\theta^2} f_2) + c_1\hbar_1^{\theta}\right) X^2 \\ & + \left(c_2(\hbar_1^{\delta^2} + \hbar_0^{\theta\delta} + \hbar_0^{\delta\theta} - \hbar_1^{\theta^2} f_1) + c_1(\hbar_1^{\delta} + \hbar_0^{\theta}) + c_0\hbar_1\right) X \\ & + c_2(\hbar_0^{\delta^2} - \hbar_1^{\theta^2} f_0) + c_1\hbar_0^{\delta} + c_0\hbar_0 \end{aligned}$$

we obtain the condition $w \in \mathcal{C} \Leftrightarrow \boldsymbol{w} \cdot M = \boldsymbol{0}$ where $\boldsymbol{w} = (c_0, c_1, c_2)$ and

$$M = \begin{pmatrix} \hbar_0 & \hbar_1 & 0 \\ \hbar_0^{\delta} & \hbar_1^{\delta} + \hbar_0^{\theta} & \hbar_1^{\theta} \\ \hbar_0^{\delta^2} - \hbar_1^{\theta^2} f_0 & \hbar_1^{\delta^2} + \hbar_0^{\theta\delta} + \hbar_0^{\delta\theta} - \hbar_1^{\theta^2} f_1 & \hbar_1^{\theta\delta} + \hbar_1^{\delta\theta} + \hbar_0^{\theta^2} - \hbar_1^{\theta^2} f_2 \end{pmatrix}. \tag{1}$$

Note that the entry M_{ij} corresponds to the coefficient of the term c_iX^j in the polynomial $w\hbar \mod f$.

The following result is contained in [8, 9] where the result is proven using pseudo-linear transformation or Matrix-Product Codes, while we give a proof within the setting of skew polynomial rings.

Theorem 1. *(cf. [8, 15]) Let θ be an endomorphism of the finite Frobenius commutative ring A, δ a θ-derivation on A, $R = A[X;\theta,\delta]$ a skew polynomial ring, $f \in R$ a monic polynomial having a right and left divisor g (i.e. $f = hg = g\hbar$) and $\mathcal{C} = Rg/Rf \subset R/Rf$ a cyclic left module (θ,δ)-code. Let C be the vector representation of $\mathcal{C}$. The dual code $C^{\perp}$ is a free A-module code and $|C| \cdot |C^{\perp}| = |A|^n$. There exists a parity check matrix H for the code C such that it is a generator matrix of the dual code $C^{\perp}$. The entries of the matrix H are images under compositions of θ and δ of the coefficients of $\hbar$ and g.*

Proof. We denote by $\tilde{C}$ the code generated by the columns of the $n \times n$ matrix M in Lemma 2 whose left kernel is exactly the code C. Then the columns of M form a generating set of $\tilde{C}$. By construction we have that $\tilde{C} \subset C^{\perp}$. Note that $\boldsymbol{w} \in C$ if and only if $\boldsymbol{w}M = \boldsymbol{0}$, which is equivalent to $\boldsymbol{w}$ is orthogonal to all generators of $\tilde{C}$. Therefore $C = \tilde{C}^{\perp}$. By Lemma 1 we have that $|\tilde{C}^{\perp}| \cdot |\tilde{C}| = |A|^n$. From $C = \tilde{C}^{\perp}$ and $|C| = |A|^k$ we then get $|\tilde{C}| = |A|^{n-k}$. By Lemma 1 we also have that $|C^{\perp}| \cdot |C| = |A|^n$, which implies that $|C^{\perp}| = |A|^{n-k}$. Since $\tilde{C} \subset C^{\perp}$ and both codes have the same number of elements we get $\tilde{C} = C^{\perp}$.

It is shown in Lemma 2 that for $i = 1, \ldots, n-k$, the i-th row of M corresponds to $X^{i-1}\hbar$ (e.g. the gray part in (1)). This shows that the right-upper $(n-k) \times (n-k)$ submatrix of M is lower triangular with invertible diagonal elements $\hbar_k, \theta(\hbar_k), \ldots, \theta^{n-k-1}(\hbar_k)$ and the right-most $n-k$ columns of M are therefore linearly independent. Hence, the A-submodule generated by the right-most $n-k$ columns of M contains $|A|^{n-k}$ elements. This shows that $C^{\perp}$ is a free A-module generated by the right-most $n-k$ columns of M which (after transposing) form a parity check matrix of C (see (2) for an example). ■

Example 4. *According to Theorem 1, the dual of the code in Example 3 is generated by the right-most two columns M in (1) which (after transposing) form a parity check matrix of C,*

$$H = \begin{pmatrix} \hbar_1 & \hbar_1^{\delta} + \hbar_0^{\theta} & \hbar_1^{\delta^2} + \hbar_0^{\theta\delta} + \hbar_0^{\delta\theta} - \hbar_1^{\theta^2} f_1 \\ 0 & \hbar_1^{\theta} & \hbar_1^{\theta\delta} + \hbar_1^{\delta\theta} + \hbar_0^{\theta^2} - \hbar_1^{\theta^2} f_2 \end{pmatrix}. \tag{2}$$

Theorem 2. *Let σ be an automorphism of order 2 of A, θ be an endomorphism of the finite Frobenius commutative ring A, δ be a θ-derivation on A, $R = A[X;\theta,\delta]$ a skew polynomial ring, $f \in R$ a monic polynomial having a right and left divisor g (i.e. $f = hg = g\hbar$) and $\mathcal{C} = Rg/Rf \subset R/Rf$ a cyclic left module (θ,δ)-code. Let C be the vector representation of $\mathcal{C}$ and $C^{\perp}$ the dual code of C. If we apply σ to all entries of the generator matrix $G^{\perp} := H$ of the dual code $C^{\perp}$, then we obtain a generator matrix $G^{\perp_\sigma}$ of the σ-Hermitian dual code $C^{\perp_\sigma}$ of C. The coefficients of the matrix $\sigma(H)$ are expressions in images under compositions of θ, δ and σ of the coefficients of $\hbar$ and g.*

Proof. For each row $g_s, s \in \{1,\ldots,k\}$ of a generating matrix G of C and each row $g_t^{\perp}, t \in \{1,\ldots,n-k\}$ of a generating matrix of $G^{\perp}$ of $C^{\perp}$ we have $\langle g_s, g_t^{\perp}\rangle = \sum_{i=1}^{n} g_{s,i}\, g_{t,i}^{\perp} = 0$. Therefore

$$\langle g_s, \sigma(g_t^{\perp})\rangle_\sigma = \sum_{i=1}^{n} g_{s,i}\,\sigma(\sigma(g_{t,i}^{\perp})) = \sum_{i=1}^{n} g_{s,i}\, g_{t,i}^{\perp} = 0.$$

Since the $n-k$ rows of $G^{\perp}$ generate a free code of dimension $|A|^{n-k}$ and σ is an automorphism, the $n-k$ rows of $\sigma(G^{\perp})$ also generate a free code of dimension $|A|^{n-k}$. Lemma 1 implies that they generate $C^{\perp_\sigma}$. ∎

4 Computing all Dual-Containing (θ,δ)-Codes

For the case $\delta = 0$ and $A = \mathbb{F}_q$, the generators of the dual code have been derived in [3, 5, 6, 8, 9]. For an arbitrary Frobenius ring A or $\delta \neq 0$, the dual code is much less studied. The algorithms in this section will allow us to show that the dual of a cyclic left module (θ,δ)-code is in general not a cyclic left module (θ,δ)-code.

4.1 Polynomial Maps

Our first goal is to transform algebraic expressions in the images under θ and δ of the coefficients of $\hbar$ and g (cf. M in (1) above), into multivariate polynomials over some subalgebra of A.

Definition 4. *A* ***polynomial map*** *on a ring B is a map $f : B \to B; x \mapsto \sum_{i=0}^{s} b_i x^i$, where $s \in \mathbb{N}$ and $b_i \in B$.*

Lemma 3. *Let θ be an endomorphism of the finite ring A, δ a θ-derivation of A and $B \subset A$ a subring. Let $\mathcal{E}$ be a system of finitely many equations over A that are polynomial expressions in the images under θ and δ of a finite set of variables $y_1,\ldots,y_m$. If $A = B[a_1,\ldots,a_s]$ ($s \in \mathbb{N}$) is a free B-module and the restriction of δ and θ to B are polynomial maps, then all solutions in A^m of the system $\mathcal{E}$ correspond to the solutions in B^{ms} of a system of polynomial equations over B in the variables $y_{1,1},\ldots,y_{1,s},\ldots,y_{m,1},\ldots,y_{m,s}$ where $y_i = y_{i,1}a_1 + \cdots + y_{i,s}a_s$.*

Proof. The image of the B-basis $a_1, \dots, a_s$ of A under δ and θ are expressions of the form $\theta(a_i) = \gamma_{i,1}a_1 + \cdots + \gamma_{i,s}a_s$ and $\delta(a_i) = \beta_{i,1}a_1 + \cdots + \beta_{i,s}a_s$ for some given $\gamma_{i,j}$ and $\beta_{i,j}$ in B:

$$\begin{aligned}
y_i^\theta &= (y_{i,1}a_1 + \cdots + y_{i,s}a_s)^\theta \\
&= y_{i,1}^\theta a_1^\theta + \cdots + y_{i,s}^\theta a_s^\theta \\
&= y_{i,1}^\theta (\gamma_{1,1}a_1 + \cdots + \gamma_{1,s}a_s) + \cdots + y_{i,s}^\theta (\gamma_{s,1}a_1 + \cdots + \gamma_{s,s}a_s) \\
y_i^\delta &= (y_{i,1}a_1 + \cdots + y_{i,s}a_s)^\delta \ = \ (y_{i,1}a_1)^\delta + \cdots + (y_{i,s}a_s)^\delta \\
&= y_{i,1}^\delta a_1 + y_{i,1}^\theta a_1^\delta + \cdots + y_{i,s}^\delta a_s + y_{i,s}^\theta a_s^\delta \\
&= y_{i,1}^\delta a_1 + y_{i,1}^\theta (\beta_{1,1}a_1 + \cdots + \beta_{1,s}a_s) + \cdots + y_{i,s}^\delta a_s + y_{i,s}^\theta (\beta_{s,1}a_1 + \cdots + \beta_{s,s}a_s)
\end{aligned}$$

Using

1. the algebra relations $a_ia_j = \mu_{i,j,1}a_1 + \ldots + \mu_{i,j,s}a_s$ (where $\mu_{i,j,s} \in B$ are given),
2. the additive and multiplicative properties of θ and δ,
3. the fact that the restriction of δ and θ to B are polynomial maps on B (so that $y_{i,j}^\theta$ and $y_{i,j}^\delta$ are polynomials in $y_{i,j}$ over B),

we can recursively transform any system of polynomial equations in the variables $y_1, \dots, y_m$, whose solutions are in A^m, into a system of polynomial equations in the variables $y_{1,1}, \dots, y_{1,s}, \dots y_{m,1}, \dots, y_{m,s}$, whose solutions are in B^{ms}. ∎

The following two examples show that there are endomorphism θ and θ-derivation δ of a ring A which are not polynomial maps over A, but only polynomial maps over a subring B.

Example 5. *Consider the Frobenius ring $A = \mathbb{F}_2[v]/(v^2+v)$ of order 4. There are two automorphisms $\theta_1 = \mathrm{id}$ and θ_2 of order two, and two non-trivial endomorphisms θ_3 and θ_4. Any θ-derivation δ is determined by $\delta(v)$ (note that $\delta(1) = \delta(0) = 0$). All the θ-derivations are listed below:*

	Automorphism		*Endomorphism*	
	$\theta_1 = \mathrm{id}$	$\theta_2(v) = v+1$	$\theta_3(v) = 0$	$\theta_4(v) = 1$
$\delta_1 = 0$	$v \mapsto 0$	$v \mapsto 0$	$v \mapsto 0$	$v \mapsto 0$
δ_2		$v \mapsto 1$		
δ_3		$v \mapsto v$	$v \mapsto v$	
δ_4		$v \mapsto v+1$		$v \mapsto v+1$

The inner θ-derivations are marked by a gray cell. Here all θ-derivations are inner.

Suppose that the automorphism θ_2 is a polynomial map on A of the form

$$f : x \mapsto \sum_{i\in\mathbb{N}_0} (\alpha_{i,1}v + \alpha_{i,0})x^i \ = \ \sum_{i\in\mathbb{N}_0} \alpha_{i,1}vx^i + \sum_{i\in\mathbb{N}_0} \alpha_{i,0}x^i \qquad (\alpha_{i,j} \in \mathbb{F}_2).$$

Then $\theta_2(0) = 0 \Rightarrow \alpha_{0,0} = 0$. Since $\alpha_{i,j} \in \{0,1\}$, $f(v)$ is a multiple of positive powers of v. Since $v^2 = v$ we get that $f(v)$ is a sum of v, which is either v or 0 in this ring. Since $\theta_2(v) = v+1$, we obtain that θ_2 is not a polynomial map on A.

Example 6. *We keep the notation of Example 1 for the ring $A = \mathbb{F}_2[u]/(u^2)$. The only automorphism of A is the identity $\theta_1 : x \mapsto x$ which is a polynomial map. Suppose that a derivation δ of A is given by a polynomial map $\delta : x \mapsto \sum_{i=0}^{t} b_i x^i$ over A (where $b_i \in A$). Since $\delta(1) = 0$, we must have $b_0 = 0$ in the polynomial map. From $u^2 = 0$, we obtain $\delta : u \mapsto \sum_{i=1}^{t} b_i u^i = b_1 u$. Write $b_1 = \beta_{1,1}u + \beta_{1,0} \in A$ for some $\beta_{1,1}, \beta_{1,0} \in \mathbb{F}_2$, then $\delta(u) = \beta_{1,1}u^2 + \beta_{1,0}u = \beta_{1,0}u$, which can never be $u + 1$ or 1. Hence, $\delta_2(u) = 1$ and $\delta_4(u) = u + 1$ are not polynomial maps on A. For this ring we will always work over $B = \mathbb{F}_2$ even for δ_1 and δ_3. Codes of small length over A are classified in [11, 12].*

Lemma 4. *Automorphisms and derivations of a finite Frobenius ring A are polynomial maps over the smallest unitary subring B of A.*

Proof. The smallest unitary subring B of A is the image of the canonical map $\mathbb{Z} \to A$ given by $1 \mapsto 1$ and is either isomorphic to a finite field $\mathbb{F}_p$ of prime order or to an integer modular ring $\mathbb{Z}_m = \mathbb{Z}/(m)$ (here p or m is the characteristic of the ring A). Since any automorphism θ is given by $x \mapsto x$ and θ-derivation δ is given by $x \mapsto 0$ on B, they are both polynomial maps on B. ∎

4.2 Computations via Gröbner Basis over $B \subset A$

In this section we assume that θ and δ are polynomial maps over a subalgebra $B \subset A$ (this is always the case for the smallest unitary subring B of A by Lemma 4) and that $A = B[a_1, \ldots, a_s]$ is a free B-module. This will enable us to transform any expression in θ and δ over A into a polynomial expression over B (Lemma 3). The classical algorithm to solve systems of polynomial equations in a multivariate polynomial commutative ring $B[y_{1,1}, \ldots, y_{1,s}, \ldots, y_{m,1}, \ldots, y_{m,s}]$ is via **Gröbner basis**. This algorithm exists in particular if B is a field or an integer quotient ring ([1, 2]), and therefore always over the smallest unitary subring B of the finite unitary ring A (Lemma 4).

4.2.1 An Algorithm to Compute All Dual-Containing (θ, δ)-Codes

We first express the unknown coefficients in A of g and $\hbar$ as linear combinations in a given B-basis of A over B with unknown coefficients x_i in B. The expressions in images under compositions of θ and δ of the coefficients of $\hbar$ and g then become polynomials in the variables x_i in B. We then obtain a parity check matrix whose coefficients are polynomials in the variables x_i. We can impose that g divides $g\hbar$ on the right by imposing that all the coefficients of the remainder, whose entries are polynomials in the unknown x_i, to be zero. We can also impose $C^\perp \subset C$ by imposing all the entries $\boldsymbol{M}^\top \cdot \boldsymbol{M}$, which are also polynomials in the unknown x_i, to be zero. All these conditions lead to a multivariate polynomial system in the unknowns x_i with coefficients in B. If a Gröbner basis algorithm exists for the ring B, then we can compute all dual-containing cyclic left module (θ, δ)-codes $\mathcal{C} = Rg/Rf \subset R/Rf$ for the fixed parameters $[n, k]$. Note that $\mathcal{C}^\perp \subset \mathcal{C}$ is a property of the code $\mathcal{C}$ and is therefore independent of the choice of $h, f, \hbar$. In other words, if $\mathcal{C}^\perp \subset \mathcal{C}$ holds for some valid solution of $h, f, \hbar$, then this will hold for any valid solution of $h, f, \hbar$. We therefore simply have to compute an elimination basis for the possible polynomials g and keep those skew polynomials g that can be extended to a solution of the whole system.

Algorithm 1: Computing all *dual-containing* cyclic module (θ, δ)-codes for given $[n, k]$.

Input: A, θ, δ, a subalgebra $B \subset A$ over which $A = B[a_1, \ldots, a_s]$ is free and over which θ, δ are polynomial maps and the Gröbner basis can be computed, code parameters n, k.

Output: A set of solutions $\mathcal{P} = \{g, \hbar, f \mid \mathcal{C} = Rg/Rf \text{ is dual-containing}\}$

$P_1 \leftarrow B[g_{0,1}, \ldots, g_{0,s}, \ldots, g_{n-k-1,1}, \ldots, g_{n-k-1,s}, \hbar_{0,1}, \ldots, \hbar_{0,s}, \ldots, \hbar_{k-1,1}, \ldots, \hbar_{k-1,s}]$;
`/* multivariate ring over` B `*/`

$\mathcal{P} \leftarrow \{\}$; `/* Initialize a set to collect` $g, \hbar$ `of self-dual codes */`

foreach $\hbar_k = \sum_{j=1}^{s} \hbar_{k,j} a_j \in \{\textit{invertible element of } A\}$ **do**

  LSEs $\leftarrow$ {Constraints such that $g_{i,j}, \hbar_{i,j} \in B$} ; `/*` $g_{i,j}^p = g_{i,j}, \hbar_{i,j}^p = \hbar_{i,j}$ `if` $B = \mathbb{F}_p$ `*/`

  $g \leftarrow \sum_{i=0}^{n-k-1} (\sum_{j=1}^{s} g_{i,j} a_j) X^i + X^{n-k}$; `/*` $g \in P_1[X; \theta, \delta]$ `*/`

  $\hbar \leftarrow \sum_{i=0}^{k-1} (\sum_{j=1}^{s} \hbar_{i,j} a_j) X^i + (\sum_{j=1}^{s} \hbar_{k,j} a_j) X^k$; `/*` $\hbar \in P_1[X; \theta, \delta]$ `*/`

  $f \leftarrow g \cdot \hbar$; `/*` $LC(f)$ `may not be monic but does not contain variable */`

  $h, r \leftarrow$ quotient, remainder of g right dividing f ; `/*` $h, r \in P_1[X; \theta, \delta]$ `*/`

  LSEs $\xleftarrow{\text{Append}}$ {All coefficients of r are 0 } ; `/* implies` $g \mid_r f$ `*/`

  $\boldsymbol{G} \leftarrow$ a generator matrix constructed from g;

  $\boldsymbol{M} \leftarrow$ the matrix constructed from $\hbar$ according to Example 3;

  LSEs $\xleftarrow{\text{Append}}$ {All entries in $\boldsymbol{M}^\top \cdot \boldsymbol{M}$ are 0} ; `/* implies` $C^\perp \subseteq C$ `*/`

  $\mathcal{S} \leftarrow$ {solutions of $g_{0,1}, \ldots, g_{n-k-1,s}, \hbar_{0,1}, \ldots, \hbar_{k-1,s}$ from the Groebner basis of LSEs};

  $\mathcal{P} \xleftarrow{\text{Append}} \{g, \hbar, f \in A[X; \theta, \delta] : \forall \text{ solution in } \mathcal{S}\}$;

  `/*` $g, \hbar \in A[X; \theta, \delta]$ `are reconstructed by evaluating coefficients of` $g, \hbar \in P_1[X; \theta, \delta]$ `for each solution in` $\mathcal{S}$`;` f `is reconstructed by` $f = g \cdot \hbar$ `*/`

end

4.2.2 Is the Dual $C^{\perp_\sigma}$ of a Cyclic Module (θ, δ)-Code Again a Cyclic Module (θ, δ)-Code ?

In the following let σ be the identity or an automorphism of order 2 of A. Note that the rows of the generator matrix $G^{\perp_\sigma} = \sigma(H)$ in Theorem 2 correspond to skew polynomials $p_1, \ldots, p_k$ in R/Rf which form an A-basis of the free code $C^{\perp_\sigma}$. If the (Hermitian-) dual code $C^{\perp_\sigma}$ is a cyclic module code $Rg^{\perp_\sigma}/R\tilde{f} \subset R/R\tilde{f}$ generated by some monic skew polynomial $g^{\perp_\sigma}$ of degree k, then this monic polynomial $g^{\perp_\sigma}$ is a left divisor of all the polynomials $p_1, \ldots, p_k$.

We follow the notations in Algorithm 1. We first set up a monic polynomial

$$g^{\perp_\sigma} = \sum_{i=0}^{k-1} (\sum_{j=1}^{s} g_{i,j}^{\perp_\sigma} a_j) X^i + X^k \in R$$

in the unknowns $g_{0,1}^{\perp_\sigma}, \ldots, g_{0,s}^{\perp_\sigma}, \ldots, g_{k-1,s}^{\perp_\sigma}$ over B. Then we perform a right division of all polynomials $p_1, \ldots, p_{n-k}$ by $g^{\perp_\sigma}$ and set the remainders $r_1, \ldots, r_{n-k}$ to zero. Note that the coefficients of all $r_1, \ldots, r_{n-k}$ are polynomials in $B[g_{0,1}^{\perp_\sigma}, \ldots, g_{k-1,s}^{\perp_\sigma}]$ and must all be zero. This leads to a polynomial system over B that can be solved by an algorithm via Gröbner basis. If the Gröbner basis is $\{1\}$ then $C^{\perp_\sigma}$ is not a cyclic module code in R/Rf for any $f \in R$. Otherwise the Gröbner basis gives the generator polynomial $g^{\perp_\sigma}$ of degree k of the cyclic module code $C^{\perp_\sigma}$.

5 Computational Results for $A = \mathbb{F}_2[v]/(v^2+v)$

We keep the notation used in Example 5 and compute the dual-containing cyclic left module (θ, δ)-code over the ring $A = \mathbb{F}_2[v]/(v^2+v)$ using the algorithm given in Section 4.2.1. Lemma 4 shows that we can use the subalgebra $B = \mathbb{F}_2 \subset A$ for the algorithm. Codes of small length over A are classified in [12]. We follow [11] and define the Lee weight of $0, 1, v, v+1$ respectively as $0, 2, 1, 1$ and the Bachoc weight respectively as $0, 1, 2, 2$. Table 1a and Table 2 give an overview of the best Euclidean and Hermitian dual-containing codes $\mathcal{C} = Rg/Rf \subset R/Rf$ (the algorithm found all such codes). The empty set indicates that the approach shows that no dual-containing code $Rg/Rf \subset R/Rf$ exists for the parameter $[n, k]$. A question mark indicates that such dual-containing codes exist, but we did not compute the minimal distance. The codes that could not have been found without considering non-zero derivations are marked in gray; the codes that only can be found by a non-zero derivation and an endomorphism which is not an automorphism are marked in dark gray. Examples of such codes are the three weight distributions of the $[6, 4]$ codes in Table 3. Table 3 and 4 show more precisely which Hamming weight enumerators could only be found by using specific (θ, δ) combinations.

Besides the complexity of a Gröbner basis, the complexity of our approach is also linked to the fact that many decompositions $f = hg = g\hbar$ can exist for a fixed g, and that all combinations lead to the same code whose generating matrix is constructed only from g and the corresponding $A[X; \theta, \delta]$. To illustrate this we present in more detail the results for the $[6, 4]$ code with Hamming weight enumerator $1 + 13w^2 + 24w^3 + \ldots$. There are four possible generator polynomials g presented in Table 5. Note that given g and $A[X; \theta, \delta]$ one can compute a generating matrix immediately. We consider the first polynomial $g = X^2 + X + v + 1 \in \left(\mathbb{F}_2[v]/[v^2+v]\right)[X; \theta_3, \delta_3]$ of Table 5. There exist 8 *non-central* polynomials f for which there are polynomials $h, \hbar$ such that $f = hg = g\hbar$, i.e., g is a left and right divisor of f:

$$
\begin{aligned}
f_1 &= X^6 + vX^4 + vX^3 + vX + v + 1 = (X^4 + X^3 + vX^2 + X + v + 1) \cdot g \\
f_2 &= X^6 + X^5 + (v+1)X^4 + X^3 + vX + v + 1 \\
&= (X^4 + vX^2 + (v+1)X + 1) \cdot g \\
f_3 &= X^6 + (v+1)X^4 + vX^3 + vX^2 + X + v + 1 \\
&= (X^4 + X^3 + (v+1)X^2 + 1) \cdot g \\
f_4 &= X^6 + X^5 + vX^4 + X^3 + vX^2 + X + v + 1 \\
&= (X^4 + (v+1)X^2 + vX + v + 1) \cdot g \\
f_5 &= X^6 + vX^4 + vX^3 + X^2 + (v+1)X = (X^4 + X^3 + vX^2 + X + v) \cdot g \\
f_6 &= X^6 + X^5 + (v+1)X^4 + X^3 + X^2 + (v+1)X \\
&= (X^4 + vX^2 + (v+1)X) \cdot g \\
f_7 &= X^6 + (v+1)X^4 + vX^3 + (v+1)X^2 = (X^4 + X^3 + (v+1)X^2) \cdot g \\
f_8 &= X^6 + X^5 + vX^4 + X^3 + (v+1)X^2 = (X^4 + (v+1)X^2 + vX + v) \cdot g
\end{aligned}
$$

For each f, there is a unique h corresponding to $f = hg$ and 16 distinct $\hbar$ such that $f = g\hbar$, where

Table 1: Results on dual-containing cyclic module (θ, δ)-code over $\mathbb{F}_2[v]/(v^2+v)$.

(a) Best Hamming, Lee and Bachoc d_H, d_L, d_B distance of dual-containing (θ, δ)-codes over $\mathbb{F}_2[v]/[v^2+v]$.

$n \setminus k$	2	3	4	5	6	7	8	9	10	11	12
3	1, 1, 2										
4	2, 2, 4	2, 2, 2									
5		$\emptyset$	$\emptyset$								
6		2, 2, 2	2, 2, 2	2, 2, 2							
7			3, 3, 5	$\emptyset$	$\emptyset$						
8			4, 4, 7	2, 2, 4	2, 2, 2	2, 2, 2					
9				$\emptyset$	$\emptyset$	$\emptyset$	1, 1, 2				
10				2, 2, 2	2, 2, 2	$\emptyset$	$\emptyset$	2, 2, 2			
11					$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$		
12					4, 4, 6	3, 3, 4	2, 2, ?	2, ?, ?	?, ?, ?	?, ?, ?	
13						$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$

(b) For the dual-containing codes C, is $C^\perp$ a cyclic module code, according to Section 4.2.2?

$n \setminus k$	2	3	4	5	6	7	8	9
3	None							
4	All	Some						
5		/	/					
6		All	Some	Some				
7			All	/	/			
8			All	Some	Some	Some		
9				/	/	/	None	
10				All	Some	/	/	All

(c) The number of dual-containing (θ, δ)-codes and codes whose dual is also a cyclic module $\theta, \delta)$ code. (We only listed for the parameters marked with "Some" in Table 1(b) above.)

small

$[n, k]$	# of dual-containing cyclic module codes Rg/Rf for each (θ, δ) # of above codes for which the dual code is also a cyclic module (θ, δ)-code								
	$(\mathrm{Id}; 0)$	$(\theta_2, 0)$	(θ_2, δ_2)	(θ_2, δ_3)	(θ_2, δ_4)	$(\theta_3, 0)$	(θ_3, δ_3)	$(\theta_4, 0)$	(θ_4, δ_4)
$[4, 3]$	1 1	1 1	3 1	1 1	1 1	1 1	2 1	1 1	2 1
$[6, 4]$	1 1	1 1	1 1	2 1	2 1	1 1	4 2	1 1	4 2
$[6, 5]$	1 1	1 1	1 1	2 1	2 1	1 1	1 1	1 1	1 1
$[8, 5]$	1 1	3 3	5 1	1 1	1 1	1 1	8 1	1 1	8 1
$[8, 6]$	1 1	3 3	5 3	1 1	1 1	1 1	4 2	1 1	4 2
$[8, 7]$	1 1	1 1	3 1	1 1	1 1	1 1	2 1	1 1	2 1
$[10, 6]$	1 1	1 1	1 1	1 1	1 1	1 1	16 2	1 1	16 2

Table 2: Best Hamming, Lee and Bachoc distance of θ_2-Hermitian dual-containing (θ, δ)-codes over $\mathbb{F}_2[v]/[v^2+v]$

$n \setminus k$	2	3	4	5	6	7	8	9
4	$2,2,4$	$2,2,2$						
5		$2,2,2$	$1,1,2$					
6		$3,3,4$	$2,2,4$	$2,2,2$				
7			$3,3,5$	$1,1,2$	$1,1,2$			
8			$3,3,6$	$2,2,4$	$2,2,2$	$2,2,2$		
9				$1,1,2$	$\emptyset$	$\emptyset$	$\emptyset$	
10				$2,2,2$	$2,2,2$	$\emptyset$	$\emptyset$	$2,2,2$

Table 3: Hamming weight enumerator of dual-containing (θ, δ)-codes over $\mathbb{F}_2[v]/[v^2+v]$.

$[n,k]$	Hamming Weight	Constructed with (θ, δ)
[4,2]	$1+6w^2+9w^4$	all combinations (θ, δ) provide such an example
	$1+4w^2+4w^3+7w^4$	$(\theta_2, \delta_2), (\theta_3, \delta_3), (\theta_4, \delta_4)$
[6,3]	$1+9w^2+27w^4+\ldots$	all combinations (θ, δ) provide such an example
[6,4]	$1+9w^2+24w^3+\ldots$	all combinations (θ, δ) provide such an example
	$1+17w^2+24w^3+\ldots$	$(\theta_2, \delta_3), (\theta_2, \delta_3)$
	$1+2w+11w^2+\ldots$	$(\theta_3, \delta_3), (\theta_4, \delta_4)$
	$1+13w^2+24w^3+\ldots$	$(\theta_3, \delta_3), (\theta_4, \delta_4)$
[8,4]	$1+12w^2+54w^4+\ldots$	all combinations (θ, δ) provide such an example
	$1+28w^4+56w^5+\ldots$	$(\theta_2, 0)$
	$1+4w^2+38w^4+\ldots$	$(\theta_2, \delta_2), (\theta_3, \delta_3), (\theta_4, \delta_4)$

Table 4: Hamming weight enumerator of θ_2-Hermitian dual-containing (θ, δ)-codes over $\mathbb{F}_2[v]/[v^2+v]$.

$[n,k]$	Hamming Weight	Constructed with (θ, δ)
[4,2]	$1+6w^2+9w^4$	all combinations (θ, δ) provide such an example
	$1+2w^2+8w^3+5w^4$	$(\theta_2, 0)$
[4,3]	$1+18w^2+\ldots$	all combinations (θ, δ) provide such an example
	$1+2w+16w^2+\ldots$	$(\theta_2, \delta_2), (\theta_3, \delta_3), (\theta_4, \delta_4)$
	$1+2w+12w^2+\ldots$	$(\theta_2, \delta_3), (\theta_2, \delta_4)$
[5,3]	$1+8w^2+14w^3+\ldots$	$(\theta_2, \delta_3), (\theta_2, \delta_4)$
	$1+w+6w^2+\ldots$	$(\theta_3, \delta_3), (\theta_4, \delta_4)$
[5,4]	$1+3w+22w^2+\ldots$	$(\theta_2, \delta_3), (\theta_2, \delta_4)$
[6,3]	$1+9w^2+27w^4+\ldots$	all combinations (θ, δ) provide such an example
	$1+8w^3+21w^4+\ldots$	$(\theta_3, \delta_3), (\theta_4, \delta_4)$

Table 5: $[6,4]$ dual-containing (θ,δ)-codes over $\mathbb{F}_2[v]/[v^2+v]$ with Hamming weight enumerator $1+13w^2+24w^3+\dots$.

Index	g	(θ,δ)	$\mathbf{G}$
1	$g = X^2+X+v+1$	(θ_3,δ_3)	$\begin{pmatrix} v+1 & 1 & 1 & 0 & 0 & 0 \\ v & 1 & 1 & 1 & 0 & 0 \\ v & 0 & 1 & 1 & 1 & 0 \\ v & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$
2	$g = X^2+(v+1)X+1$	(θ_3,δ_3)	$\begin{pmatrix} 1 & v+1 & 1 & 0 & 0 & 0 \\ 0 & v+1 & 1 & 1 & 0 & 0 \\ 0 & v & 1 & 1 & 1 & 0 \\ 0 & v & 0 & 1 & 1 & 1 \end{pmatrix}$
3	$g = X^2+vX+1$	(θ_4,δ_4)	$\begin{pmatrix} 1 & v & 1 & 0 & 0 & 0 \\ 0 & v & 1 & 1 & 0 & 0 \\ 0 & v+1 & 1 & 1 & 1 & 0 \\ 0 & v+1 & 0 & 1 & 1 & 1 \end{pmatrix}$
4	$g = X^2+X+v$	(θ_4,δ_4)	$\begin{pmatrix} v & 1 & 1 & 0 & 0 & 0 \\ v+1 & 1 & 1 & 1 & 0 & 0 \\ v+1 & 0 & 1 & 1 & 1 & 0 \\ v+1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$

one of $\hbar$ is equal to h. The following are the other 15 distinct $\hbar \neq h$ such that $f_1 = g\cdot\hbar$:

$$\begin{aligned}
f_1 &= g\cdot\big(X^4+(v+1)X^3+vX^2+(v+1)X+v+1\big) \\
&= g\cdot\big(X^4+X^3+vX^2+(v+1)X+v+1\big) \\
&= g\cdot\big(X^4+(v+1)X^3+(v+1)X+v+1\big) = g\cdot\big(X^4+X^3+(v+1)X+v+1\big) \\
&= g\cdot\big(X^4+(v+1)X^3+vX^2+X+v+1\big) = g\cdot\big(X^4+(v+1)X^3+X+v+1\big) \\
&= g\cdot\big(X^4+X^3+X+v+1\big) = g\cdot\big(X^4+(v+1)X^3+vX^2+(v+1)X+1\big) \\
&= g\cdot\big(X^4+X^3+vX^2+(v+1)X+1\big) = g\cdot\big(X^4+(v+1)X^3+(v+1)X+1\big) \\
&= g\cdot\big(X^4+X^3+(v+1)X+1\big) = g\cdot\big(X^4+(v+1)X^3+vX^2+X+1\big) \\
&= g\cdot\big(X^4+X^3+vX^2+X+1\big) = g\cdot\big(X^4+(v+1)X^3+X+1\big) \\
&= g\cdot\big(X^4+X^3+X+1\big)
\end{aligned}$$

The $[8,4,d_H=5]$ code in Table 2 that achieves the Singleton bound in Hamming metric are obtained with $g = X^4+(v+1)X^3+X^2+vX+1$ and $g = X^4+vX^3+X^2+(v+1)X+1$ in $\big(\mathbb{F}_2[v]/[v^2+v]\big)[X;\mathrm{id},\theta_2]$.

We apply the algorithm presented in Section 4.2.2 to verify for which dual-containing codes $C = Rg/Rf \subset R/Rf$ the dual code $C^\perp$ is again a cyclic module (θ,δ)-code. See in Table 1b and Table 1c for an overview. We list two examples below which show that the dual of a dual-containing cyclic module (θ,δ)-code is not always a cyclic module (θ,δ)-code:

- For $[n=4,k=3]$, we found three $g\in A[X;\theta_2,\delta_2]$ that generate dual-containing cyclic module codes: $g_1 = X+v+1$, $g_2 = X+1$, $g_3 = X+v$ where only the dual of $g_2 = X+1$ is a cyclic module code, with $g_2^\perp = X^3+X^2+X+1$.

- For $[n=6,k=4]$, we found four $g \in A[X;\theta_3,\delta_3]$ that generate dual-containing cyclic module codes: $g_1 = X^2+(v+1)X+v+1$, $g_2 = X^2+X+1$, $g_3 = X^2+X+v+1$, $g_4 = X^2+(v+1)X+1$. Only the dual of g_2 and g_4 are cyclic module codes, with $g_2^{\perp} = X^4+X^3+X+1$ and $g_4^{\perp} = X^4+(v+1)X^3+X+v+1$, respectively.

6 Computational Results for $A = \mathbb{F}_2[u]/(u^2)$

We keep the notations of Example 1 for the ring $A = \mathbb{F}_2[u]/(u^2)$. Lemma 4 and Algorithm 1 show that we can search dual-containing cyclic left module (θ,δ)-code $\mathcal{C} = Rg/Rf \subset R/Rf$ over the subalgebra $B = \mathbb{F}_2 \subset A$ using a Gröbner basis approach. We follow [11] and define the Lee weight of $0,1,u,u+1$ respectively as $0,1,2,1$ and the Euclidean weight respectively as $0,1,4,1$. Table 6 give an overview of the best dual-containing codes $\mathcal{C} = Rg/Rf \subset R/Rf$ (the algorithm found all such codes). For the cell marked in gray, the dual-containing cyclic module codes are only found from the maps (id,δ_2) and (id,δ_4).

Table 6: Best Hamming, Lee, and Euclidean distances of dual-containing cyclic module (θ,δ)-codes over $\mathbb{F}_2[u]/(u^2)$.

$n \setminus k$	2	3	4	5	6	7	8	9
4	$2,4,4$	$2,2,2$						
5		$\emptyset$	$1,2,2$					
6		$2,4,4$	$2,2,2$	$2,2,2$				
7			$3,3,3$	$\emptyset$	$1,2,2$			
8			$4,4,4$	$2,4,4$	$2,2,2$	$2,2,2$		
9				$\emptyset$	$\emptyset$	$\emptyset$	$1,2,2$	
10				$2,4,6$	$2,4,5$	$\emptyset$	$\emptyset$	$2,2,2$

Table 7 gives an overview whether the dual codes $C^{\perp}$ of the dual-containing codes found by Algorithm 1 are again cyclic module (θ,δ)-codes.

Table 8 shows examples for which Hamming weight enumerators could only be found using specific (θ,δ) combinations. In particular the gray cells indicate those that can only be obtained using a non-zero derivation.

7 Computational Results for $A = \mathbb{F}_4$

Consider the field $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ where $\alpha^2 = \alpha+1$. There are two automorphisms: $\theta_1 = \mathrm{id}$ and the Frobenius automorphism $\theta_2 : x \mapsto x^2$. θ_2 is of order 2 and is a polynomial map on both $\mathbb{F}_4$ and $\mathbb{F}_2$. All the θ-derivations are inner derivations and are marked in gray in the list below:

	Automorphism	
	$\theta_1 = \mathrm{id}$	$\theta_2(\alpha) = \alpha+1$
$\delta_1 = 0$	$\alpha \mapsto 0$	$\alpha \mapsto 0$
δ_2		$\alpha \mapsto 1$
δ_3		$\alpha \mapsto \alpha$
δ_4		$\alpha \mapsto \alpha+1$

Table 7: For which dual-containing cyclic module codes C is the dual $C^{\perp}$ again a cyclic module code, according to Section 4.2.2?

$n \setminus k$	2	3	4	5	6	7	8	9
4	All	All						
5		/	(id, δ_2): None (id, δ_4): All					
6		All	All	All				
7			All	/	All			
8			All	All	All	All		
9				/	/	/	(id, δ_2): None (id, δ_4): Some	
10				All	All	/	/	All

Table 8: Hamming weight enumerator of dual-containing (θ, δ)-codes over $\mathbb{F}_2[u]/[u^2]$.

$[n, k]$	Hamming Weight	Constructed with (θ, δ)
[4,2]	$1 + 2w^2 + 8w^3 + 5w^4$	$(\mathrm{id}, 0), (\mathrm{id}, \delta_2), (\mathrm{id}, \delta_3), (\theta_2, \delta_2)$
	$1 + 6w^2 + 9w^4$	all maps
[8,4]	$1 + 4w^2 + 30w^4 + \ldots$	$(\mathrm{id}, 0), (\theta_2, \delta_2)$
	$1 + 4w^2 + 46w^4 + \ldots$	$(\mathrm{id}, 0)$
	$1 + 4w^2 + 16w^3 + \ldots$	$(\mathrm{id}, 0)$
	$1 + 12w^2 + 54w^4 + \ldots$	all maps
	$1 + 26w^4 + 64w^5 + \ldots$	(id, δ_2)
[8,5]	$1 + 4w^2 + 16w^3 + 94w^4 + \ldots$	$(\mathrm{id}, 0), (\mathrm{id}, \delta_2)$
	$1 + 4w^2 + 16w^3 + 110w^4 + \ldots$	$(\mathrm{id}, 0)$
	$1 + 12w^2 + 102w^4 + \ldots$	all maps
	$1 + 16w^2 + 8w^3 + 114w^4 + \ldots$	(id, δ_2)

Following [11] we define the Lee weight of $0, 1, \alpha, \alpha+1$ respectively as $0, 2, 1, 1$ and following [13] we define the Euclidean weight respectively as $0, 1, 2, 1$.

Table 9 shows the existence and the best Hamming, Lee and Euclidean distance of the θ_2-Hermitian dual-containing cyclic module (θ, δ)-codes $\mathcal{C} = Rg/Rf \subset R/Rf$ over $\mathbb{F}_4$. The gray cells indicate the codes that can only be obtained using a non-zero derivation.

Table 9: The best Hamming, Lee and Euclidean d_H, d_L, d_E distance of θ_2-Hermitian dual-containing codes $Rg/Rf \subset R/Rf$ over $\mathbb{F}_4$.

$n \setminus k$	2	3	4	5	6	7	8	9
4	$2,2,2$	$2,2,2$						
5		$3,3,3$	$1,1,1$					
6		$4,4,4$	$2,2,2$	$2,2,2$				
7			$3,3,3$	$\emptyset$	$1,1,1$			
8			$2,2,2$	$2,2,2$	$2,2,2$	$2,2,2$		
9				$\emptyset$	$\emptyset$	$\emptyset$	$1,1,1$	
10				$4,4,4$	$3,3,3$	$2,2,2$	$2,2,2$	$2,2,2$

Table 10 provides some examples of the Hamming weight distributions. This shows that in Hermitian case, non-zero derivation does produce other code than in the $\delta = 0$ case. In the $\delta = 0$ case we could not exhibit new codes.

Table 10: Weight enumerator of θ_2-Hermitian dual-containing cyclic module (θ, δ) codes over $\mathbb{F}_4$.

$[n, k]$	Hamming Weight Enumerator	Constructed with (θ, δ)
[4,3]	$1 + 18w^2 + 24w^3 + 211w^4$	all maps
	$1 + 6w + 12w^2 + 18w^3 + 27w^4$	(θ_2, δ_2)
[5,4]	$1 + 9w + 30w^2 + 54w^3 + 81w^4 + 81w^5$	(θ_2, δ_2)
[6,5]	$1 + 45w^2 + 120w^3 + 315w^4 + 360w^5 + 183w^6$	all maps
	$1 + 12w + 57w^2 + 144w^3 + 243w^4 + \ldots$	(θ_2, δ_2)
[7,6]	$1 + 15w + 93w^2 + 315w^3 + 675w^4 + \ldots$	(θ_2, δ_2)
[8,7]	$1 + 84w^2 + 336w^3 + 1470w^4 + \ldots$	all maps
	$1 + 18w + 138w^2 + 594w^3 + 1620w^4 + \ldots$	(θ_2, δ_2)
[9,8]	$1 + 21w + 192^2 + 1008w^3 + 3402w^4 + \ldots$	(θ_2, δ_2)
[10,9]	$1 + 135w^2 + 720w^3 + 4410w^4 + 15120w^5 + \ldots$	all maps
	$1 + 24w + 255w^2 + 1584w^3 + 6426w^4 + \ldots$	(θ_2, δ_2)

8 Computation Results for the Galois Ring $A = GR(4, 2)$

The galois ring $A = GR(4, 2) = Z_4[u] = (\mathbb{Z}/4\mathbb{Z})[u]/(u^2+u+1)$ is a Frobenius ring of order 16. This ring has two automorphisms: $\theta_1 = \mathrm{id}$ and $\theta_2(u) = 3u+3$ of order 2. The zero derivation is the only id-derivation. The θ_2-derivations are all inner (i.e. $\delta : a \mapsto \beta a - \theta_2(a)\beta, \forall \beta \in A$): $\delta_1(u) = 0$, $\delta_2(u) =$

u, $\delta_3(u) = 2u$, $\delta_4(u) = 3u$, $\delta_5(u) = 1$, $\delta_6(u) = u + 1$, $\delta_7(u) = 2u + 1$, $\delta_8(u) = 3u + 1$, $\delta_9(u) = 2$, $\delta_{10}(u) = u + 2$, $\delta_{11}(u) = 2u + 2$, $\delta_{12}(u) = 3u + 2$, $\delta_{13}(u) = 3$, $\delta_{14}(u) = u + 3$, $\delta_{16}(u) = 3u + 3$.

We computed all $[4, 2]$ self-dual and $[4, 3]$ dual-containing cyclic left module (θ, δ)-codes over $A = GR(4, 2)$ by Algorithm 1. For the $[4, 2]$ codes, there are 8 g's given by each map in Table 11. They generate $[4, 2, d_H = 3]$ codes with distinct codebooks (i.e. the codewords in the codes are not all equal), however, with the same weight enumerator $1 + 60w^3 + 195w^4$. For each g there are 16 f's which are all central and including one in the form of $X^n - a$ for some $a \in \mathbb{Z}_4$. The $[4, 3]$ codes can be obtained from all maps. From each map, there are four unique g's. For each g there are more than 1000 f's which include at least one central f and an f in the form of $X^n - a$ for some $a \in \mathbb{Z}_4$. All the codes have the same weight enumerator given in Table 11.

Table 11: The best Hamming distance d_H of dual-containing codes $Rg/Rf \subset R/Rf$ over $GR(4, 2)$.

$[n, k]$	existing code for map (θ_i, δ_j)	best d_H	Weight Distribution
[3,2]	$(1, 1), (2, 2), (2, 4), (2, 6), (2, 8),$ $(2, 10), (2, 12), (2, 14), (2, 16)$	2	$1 + 45w^2 + 210w^3$
$[4, 2]$	$(2, 1), (2, 3), (2, 9), (2, 11)$	3	$1 + 60w^3 + 195w^4$
$[4, 3]$	All maps	2	$1 + 90w^2 + 840w^3 + 3165w^4$
$[5, 3]$	$\emptyset$	/	/

References

[1] W. W. Adams and P. Loustaunau, *An Introduction to Grobner Bases.* American Mathematical Society, 1994, no. 3.

[2] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system I: The user language," *Journal of Symbolic Computation*, vol. 24, no. 3-4, pp. 235–265, 1997.

[3] D. Boucher, P. Solé, and F. Ulmer, "Skew constacyclic codes over Galois rings," *Advances in mathematics of communications*, vol. 2, no. 3, pp. 273–292, 2008.

[4] D. Boucher and F. Ulmer, "Codes as modules over skew polynomial rings," in *Cryptography and Coding: 12th IMA International Conference, Cryptography and Coding 2009, Cirencester, UK, December 15-17, 2009. Proceedings 12.* Springer, 2009, pp. 38–55.

[5] ——, "Coding with skew polynomial rings," *Journal of Symbolic Computation*, vol. 44, no. 12, pp. 1644–1656, 2009.

[6] ——, "A note on the dual codes of module skew codes," in *IMA International Conference on Cryptography and Coding.* Springer, 2011, pp. 230–243.

[7] ——, "Linear codes using skew polynomials with automorphisms and derivations," *Designs, codes and cryptography*, vol. 70, pp. 405–431, 2014.

[8] M. Boulagouaz and A. Deajim, "Characterizations and properties of principal (f, σ, δ)-codes over rings," *arXiv preprint arXiv:1809.10409*, 2018.

[9] ——, "Matrix-product codes over commutative rings and constructions arising from (σ,δ)-codes," *Journal of Mathematics*, vol. 2021, pp. 1–10, 2021.

[10] M. Boulagouaz and A. Leroy, "(σ, δ)-codes," *Advances in Mathematics of Communications*, vol. 7, no. 4, pp. 463–474, 2013.

[11] S. T. Dougherty and K. Shiromoto, "Maximum distance codes over rings of order 4," *IEEE Transactions on Information Theory*, vol. 47, no. 1, pp. 400–404, 2001.

[12] W. C. Huffman, "On the classification and enumeration of self-dual codes," *Finite Fields and Their Applications*, vol. 11, no. 3, pp. 451–490, 2005.

[13] S. Ling and P. Solé, "Type II codes over $\mathbb{F}_4 + u\mathbb{F}_4$," *European Journal of Combinatorics*, vol. 22, no. 7, pp. 983–997, 2001. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0195669801905098

[14] O. Ore, "Theory of non-commutative polynomials," *Annals of mathematics*, pp. 480–508, 1933.

[15] A. Sharma and M. Bhaintwal, "A class of skew-cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ with derivation," *Advances in Mathematics of Communications*, vol. 12, no. 4, 2018.

[16] S. Szabo and J. A. Wood, "Properties of dual codes defined by nondegenerate forms," *Journal of Algebra Combinatorics Discrete Structures and Applications*, pp. 105–113, 2017.