Codes over Affine Algebras with a Finite Commutative Chain coefficient Ring

E. Martínez-Moro*[1], A. Piñera-Nicolás†[1], and I.F. Rúa†[2]

[1]Institute of Mathematics (IMUVa), Universidad de Valladolid,
edgar.martinez@uva.es, alejandro.pinera@uva.es
[2]Departamento de Matemáticas, Universidad de Oviedo,
rua@uniovi.es

September 14, 2017

Abstract

We consider codes defined over an affine algebra $\mathcal{A} = R[X_1, \ldots, X_r]/\langle t_1(X_1), \ldots, t_r(X_r)\rangle$, where $t_i(X_i)$ is a monic univariate polynomial over a finite commutative chain ring R. Namely, we study the $\mathcal{A}-$submodules of $\mathcal{A}^l$ ($l \in \mathbb{N}$). These codes generalize both the codes over finite quotients of polynomial rings and the multivariable codes over finite chain rings. Some codes over Frobenius local rings that are not chain rings are also of this type. A canonical generator matrix for these codes is introduced with the help of the Canonical Generating System. Duality of the codes is also considered.

Keywords: Finite Commutative Chain Ring; Affine Algebra; Multivariable Codes; Quasi-cyclic codes; Codes over non-chain local Frobenius rings.

AMS classification: 11T71, 94B99, 81P70, 13M10

1 Introduction

Quasi-cyclic codes over a finite commutative chain ring R can be represented as $(R[x]/\langle x^n - 1\rangle)$-submodules of $(R[x]/\langle x^n - 1\rangle)^l$, generalizing the well known construction for finite fields in, for example, [3]. For finite commutative chain ring, the one-generator codes have been extensively studied (see, for example, the classical paper [21] and the references included in [7]), whereas for finite fields the general situation was studied in [11] and recently generalized in [1] to codes over finite quotients of polynomial rings, i.e., to $\mathbb{F}[x]/\langle f(x)\rangle$-submodules

*Partially funded by MINECO MTM2015-65764-C3-1-P.

†Partially supported by MINECO-13-MTM2013-45588-C3-1-P, and Principado de Asturias Grant GRUPIN14-142.

of $(\mathbb{F}[x]/\langle f(x)\rangle)^l$ where $l \in \mathbb{N}$ and $f(x)$ is a monic polynomial. Furthermore, Jitman and Ling studied quasi-abelian codes over finite fields using techniques based on the Discrete Fourier Transform. They also gave a structural characterization, as well as an enumeration, of one-generator quasi-abelian codes in [8].

In this paper we will consider codes defined over an affine algebra $\mathcal{A} = R[X_1,\ldots,X_r]/\langle t_1(X_1),\ldots,t_r(X_r)\rangle$, where each $t_i(X_i)$ is a monic univariate polynomial over a finite commutative chain ring R, i.e., $\mathcal{A}-$submodules of $\mathcal{A}^l$. Therefore, this class of codes includes the codes defined in [1] and also, when $l = 1$, multivariable codes over finite commutative chain rings [15, 16]. The proposed approach, which uses the concept of Canonical Generating System introduced in [20], allows the study of quasi-cyclic codes over a finite commutative chain ring and their multivariable generalizations in a broader polynomial way, that is, beyond the one-generator case. Notice that for several generators a trace representation can also be derived from the ideas in [12], see for example Section 4 in [7]. The former approach provides a way for defining codes over some Frobenius local rings which are not chain rings. Some of them, as can be seen in Examples 1, 5 and 6, have not been previously explored in the literature.

The outline of the paper is as follows. In Section 2 we state the basic facts on finite commutative chain rings and some examples of known families of codes that are included in our definition. The construction of a canonical generator matrix for our codes is provided in Section 3. In the final section duality of these codes is considered.

2 Basic definitions and examples

An associative, commutative, unital, finite ring R is called *chain ring* if it has a unique maximal ideal M and it is principal (i.e, generated by an element a). This condition is equivalent [5, Proposition 2.1] to the fact that the set of ideals of R is the chain (hence its name) $\langle 0\rangle = \langle a^t\rangle \subsetneq \langle a^{t-1}\rangle \subsetneq \cdots \subsetneq \langle a^1\rangle = M \subsetneq \langle a^0\rangle = R$, where t is the nilpotency index of the generator a. The quotient ring $\overline{R} = R/M$ is a finite field $\mathbb{F}_q$ where $q = p^d$ is a prime number power. Examples of finite commutative chain rings include Galois rings $GR(p^n, d)$ of characteristic p^n and p^{nd} elements (here $a = p$, and $t = n$) and, in particular, finite fields ($\mathbb{F}_q = GR(p, d)$) [19, 2]. Any element $r \in R$, can be written as $r = a^i r'$, where $0 \le i \le t$ and $0 \ne \overline{r'} \in \mathbb{F}_q$. The exponent i is unique, and it is called the *norm* of r, written $\|r\|$.

Affine algebras with a finite commutative chain coefficient ring are quotients $\mathcal{A} = R[X_1,\ldots,X_r]/\langle t_1(X_1),\ldots,t_r(X_r)\rangle$, where $t_j(X_j) \in R[X_j]$ are monic polynomials of degree n_j. (i.e., $|\mathcal{A}| = |R|^n$, where $n := \prod_{j=1}^r n_j$). Let us denote every element f in the affine algebra $\mathcal{A}$ as $f = \sum f_{\mathbf{i}}\mathbf{X}^{\mathbf{i}}$, where $\mathbf{i} = (i_1,\ldots,i_r) \in \mathbb{N}_0^r$, $f_{\mathbf{i}} \in R$ and $\mathbf{X}^{\mathbf{i}} = X_1^{i_1}\ldots X_r^{i_r}$. If we require $0 \le i_j < n_j$ for all $1 \le j \le r$, then the expresion is unique. We implicitely require this condition through the paper and identify the element $f \in \mathcal{A}$ with the polynomial $\sum f_{\mathbf{i}}\mathbf{X}^{\mathbf{i}} \in R[X_1,\ldots,X_r]$.

Definition 1. *Let l be a natural number. A* linear code of index l over the affine algebra $\mathcal{A}$ *(an $\mathcal{A}-$*code*) is an $\mathcal{A}-$submodule C of the direct product $E = \mathcal{A}^l$.*

For all $1 \leq i \leq l$, we shall denote by $\pi_i(f_1, \ldots, f_l) = f_i$ the canonical projection on the $i-$th component $\pi_i : E \to \mathcal{A}$.

Example 1. *We start giving some examples of codes that can be seen, according to our construction, as codes over affine algebras:*

1. *Ideals of $\mathcal{A}$ (i.e., linear codes of index $l = 1$) are the* multivariable codes *introduced in [15, 16]. As particular cases we have the multivariable codes over a finite field $\mathbb{F}_q$ [22], and well-known families of codes over a finite chain ring alphabet, such as* cyclic *$(r = 1, t_1(X_1) = X_1^{n_1} - 1)$,* negacyclic *$(r = 1, t_1(X_1) = X_1^{n_1} + 1)$,* constancyclic *$(r = 1, t_1(X_1) = X_1^{n_1} + \lambda)$,* polycyclic *$(r = 1)$ and* abelian codes *$(t_i(X_i) = X_i^{n_i} - 1, \forall i = 1, \ldots, r)$ [5, 13].*

2. Quasi-cyclic *codes over a finite commutative chain ring are obtained when $r = 1, t_1(X_1) = X_1^{n_1} - 1$ and $l > 1$. See for example [3, 7] and the references therein.*

3. Quasi-abelian *codes over a finite field are obtained when $r > 1$ and $t_i(X_i) = X_1^{n_i} - 1$, $i = 1, \ldots, r$ and $l > 1$ [8].*

4. *The* codes over finite quotients of polynomial rings *studied in [1] are particular cases when the coefficient ring R is the finite field $\mathbb{F}_q$ and the polynomial ring is univariate, i.e., $r = 1$.*

5. *Codes over non-chain rings of order 16, $\mathbb{F}_2[u, v]/\langle u^2, v^2\rangle$ and $\mathbb{Z}_4[x]/\langle x^2\rangle$ of [17] and codes over the family of rings $R_k = \mathbb{F}_2[u_1, \ldots, u_k]/\langle u_1^2, \ldots, u_k^2\rangle$ studied in [6].*

Remark 1. *Notice that some kind of codes over Frobenius local rings can be described using codes over affine algebras. In particular, in some of them the alphabet is not a chain ring and the usual matricial approach over those rings can not be used. This is the case of the* linear codes over the ring $\mathbb{Z}_4[x]/\langle x^2+2x\rangle$ *studied by Martínez-Moro, Szabo and Yildiz in [18], which can be obtained when $R = \mathbb{Z}_4, r = 1, t_1(X_1) = X_1^2 + 2X_1$ and $l > 1$. Some of these codes give Gray images which are extremal Type* II *$\mathbb{Z}_4-$codes, as it can be seen in Example 4.*

Remark 2. *Observe that any $\mathcal{A}-$code C is also an $R-$module. However, C is non necessarily free neither as $\mathcal{A}-$module nor as $R-$module. This makes a difference with codes over the finite quotients of (univariate) polynomial rings (over finite fields), which are always $\mathbb{F}_q-$vector spaces [1, page 166].*

Definition 2. *Let $\preceq$ be an admissible monomial order on $\mathbb{N}_0^r$, i.e., a monomial order such that $\mathbf{0} \preceq \mathbf{i}$ and $\mathbf{i} + \mathbf{k} \preceq \mathbf{j} + \mathbf{k}$, for all $\mathbf{i}, \mathbf{j}, \mathbf{k} \in \mathbb{N}_0^r$ with $\mathbf{i} \preceq \mathbf{j}$ [20]. For any $f \in \mathcal{A}$ we can associate an element $\phi(f) \in R^n$ by listing its coefficients in the order given by $\preceq$. The map $\phi : \mathcal{A} \to R^n$ can be extended to $\Phi : E \to R^{nl}$ coordinatewise, and the $R-$*image *of an $\mathcal{A}-$code C is defined as the $R-$linear code $\Phi(C) \subseteq R^{nl}$.*

From now on, we shall assume that an admissible monomial order $\preceq$ is fixed (e.g., the lexicographic, graded lex or graded reverse lex orders [4]). If w is a weight function in the ring R (for instance, the Hamming weight when $R = \mathbb{F}_q$ or the Lee weight if $R = \mathbb{Z}/4\mathbb{Z}$), then it can be used to induce the weight $w^{nl} : E \to \mathbb{R}$, given by $w^{nl}(f_1, \ldots, f_l) = \sum_{j=1}^{nl} w(\Phi(f_1, \ldots, f_l)_j)$ [9, Section 3].

It is natural to expect that the codes under study are generally not generated by a single codeword (observe that repeated-root multivariable codes are particular examples [16, 14]). So, following [1], generators of an $\mathcal{A}-$code C will be given in terms of a generator matrix.

Definition 3. *Let C be an $\mathcal{A}-$code, we shall say that $G \in \mathcal{A}^{k\times l}$ ($k \in \mathbb{N}$) is a* generator matrix *of C if the rows of G generate C as an $\mathcal{A}-$submodule of E, i.e., $C = \left\langle g^{(1)}, \ldots, g^{(k)} \right\rangle_{\mathcal{A}} = \{\sum_{i=1}^{k} f_i g^{(i)} \mid f_i \in \mathcal{A}\}$ (with $fg = (fg_1, \ldots, fg_l) \in E$). A matrix $G \in \mathcal{A}^{K\times l}$ ($K \in \mathbb{N}$) will be called* generator matrix over R *if the rows of G generate C as an $R-$submodule of E, i.e., $C = \left\langle g^{(1)}, \ldots, g^{(K)} \right\rangle_R = \{\sum_{i=1}^{K} r_i g^{(i)} \mid r_i \in R\}$ (with $rg = (rg_1, \ldots, rg_l) \in E$).*

It is clear that from every generator matrix G of C, a generator matrix over R can be obtained by a substitution of every row $g^{(i)}$ of G by the set of rows $\{X_1^{m_1} \ldots X_r^{m_r} g^{(i)} \mid 0 \leq m_i < n_i\}$.

3 A canonical generator matrix for $\mathcal{A}-$codes

In this section we show that any $\mathcal{A}-$code can be described by a generator matrix G in a canonical form which generalizes that of [1, Section 2] for codes over finite quotients of (univariate) polynomial rings (over finite fields), and that of [16, Section 4] for repeated-root multivariable codes over finite commutative chain rings. As in the latter, the *Canonical Generating Systems (CGS)* introduced in [20] is the main tool in our study. We refer the reader to such a reference for details.

Recall that in this paper we implicitely identify the elements in $\mathcal{A}$ with multivariate polynomials $\sum f_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$ with $0 \leq i_j < n_j$ for all $1 \leq j \leq r$. If $f = \sum f_{\mathbf{i}} \mathbf{X}^{\mathbf{i}} \in \mathcal{A}$ and $\mathbf{i} \in \mathbb{N}_0^r$, then $\mathrm{Cf}(f, \mathbf{X}^{\mathbf{i}})$ denotes the coefficient $f_{\mathbf{i}}$. The set $\mathfrak{S}(f) = \{\mathbf{i} \in \mathbb{N}_0^r \mid f_{\mathbf{i}} \neq 0\}$ is the *support* of f, and the *norm* of f is $\|f\| = \max_{\mathbf{i}}\{\|f_{\mathbf{i}}\|\}$. The *leading degree* of f, $\mathrm{ldg}(f)$, is the maximal $\mathbf{i}$ (w.r.t. $\preceq$) such that $\|f_{\mathbf{i}}\| = \|f\|$. The *leading term* (resp. *coefficient, monomial*) is defined as $\mathrm{Lt}(f) = \mathbf{X}^{\mathrm{ldg}(f)}$ (resp. $\mathrm{Lc}(f) = \mathrm{Cf}(f, \mathrm{Lt}(f)), \mathrm{Lm}(f) = \mathrm{Lc}(f)\mathrm{Lt}(f)$).

If $f, h, g \in \mathcal{A}$, we say that f is *$L-$reduced to h mod g* if there exists $r \in R$ with the condition $0 \neq r\mathrm{Lc}(g) = \mathrm{Cf}(f, \mathbf{X}^{\mathbf{i}}\mathrm{Lt}(g))$, such that $h = f - r\mathbf{X}^{\mathbf{i}} g$. In general, given a subset $\chi \in \mathcal{A}$, we say that f is *$L-$reduced to h mod χ* if there exists a sequence of $L-$reductions of h_i to h_{i+1} mod $g_i \in \chi$ ($i = 1, \ldots, w-1$) with $h_0 = f, h_w = h$.

The polynomial $f \in \mathcal{A}$ is called *normal mod $\chi \subseteq \mathcal{A}$*, if it can not be $L-$reduced mod χ. The set of all polynomials normal mod χ is denoted $N(\chi)$. The polynomial $h \in \mathcal{A}$ is called a *normal form* of f mod χ, if $h \in N(\chi)$ and f

is $L-$reduced to h mod χ. The set of all normal forms of f mod χ is denoted $NF(f, \chi)$.

A finite subset $\mathcal{F} \subset \mathbb{N}_0^r$ is called *Ferrers diagram* if, given $\mathbf{s} \in \mathcal{F}$, we have $\mathbf{u} \in \mathcal{F}$ for all $\mathbf{u} \leq \mathbf{s}$ (i.e., $u_j \leq s_j$, for all $1 \leq j \leq r$). If $\mathcal{KF}$ denotes the set of minimal elements in the partially ordered set $(\mathbb{N}_0^r \setminus \mathcal{F}, \leq)$, then an $\mathcal{F}$-*monic* polynomial is a polynomial of the form $g^{\mathbf{s}} = \mathbf{X}^{\mathbf{s}} - \sum_{\mathbf{u}\in\mathcal{F}} g_{\mathbf{u}}\mathbf{X}^{\mathbf{u}}$, where $\mathbf{s} \in \mathcal{KF}$. A set of $\mathcal{F}$-monic polynomials of the form $\chi = \{g^{\mathbf{s}} \mid \mathbf{s} \in \mathcal{KF}\}$ is called a *characteristic set*. If, besides, $|\chi| = |\overline{\chi}|$ and the set $\overline{\chi}$ is a reduced Gröbner basis of the ideal $\langle\overline{\chi}\rangle \subseteq \mathbb{F}_q[X_1, \ldots, X_r]$, then χ is called a *Krull system*.

As an application of [20, Theorem 4.3] to affine algebras, we have the following result, which generalizes [1, Theorem 1] and also [16, Theorem 2].

Theorem 1. *Let C be a nonzero $\mathcal{A}-$code, and let $\preceq$ be a fixed monomial order on $\mathbb{N}_0^r$. Then, there exist:*

1. *A natural number $1 \leq k \leq l$, and two sequences of k natural numbers ($1 \leq i_1 < \cdots < i_k \leq l$ and $0 \leq x_1, \ldots, x_k \leq t-1$);*
2. *k strictly decreasing chain of Ferrers diagrams $\mathcal{F}_0^j \supset \mathcal{F}_1^j \supset \cdots \supset \mathcal{F}_{x_j}^j$ and k sequences of x_j+1 natural numbers $0 = b_0^j < b_1^j < \cdots < b_{x_j}^j < b_{x_j+1}^j = t$ (for all $1 \leq j \leq k$);*

such that for all $1 \leq j \leq k$:

1. *If $(f_1, \ldots, f_l) \in C$, then for all $0 \leq m \leq x_j$ such that $\mathfrak{S}(f_{i_j}) \subseteq \mathcal{F}_m^j$, we have $\|f_{i_j}\| \geq b_{m+1}^j$;*
2. *There exists, for all $0 \leq m \leq x_j$, a Krull system χ_m^j of $\mathcal{F}_m^j$-monic polynomials such that $a^{b_m^j}\mathcal{F}_m \subseteq \pi_{i_j}(C_{i_j})$, where C_{i_j} is the subcode of C whose codewords have the first i_j components equal to zero;*
3. *The set $\chi^j = \chi_0^j \cup a^{b_1^j}\chi_1^j \cup \cdots \cup a^{b_{x_j}^j}\chi_{x_j}^j$ is a* CGS *of $\pi_{i_j}(C_{i_j})$, i.e.,*
   (a) *The projection $\pi_{i_j}(C_{i_j})$ is the $\mathcal{A}-$submodule (i.e., the ideal of $\mathcal{A}$) generated by χ^j;*
   (b) *$f_{i_j} \in \pi_{i_j}(C_{i_j})$ if and only if the recurring sequence given by $h_0 = f, h_{m+1} = NF(h_m, \chi_m^j)$ satisfies $\|h_m\| \geq b_m^j$, for all $0 \leq m \leq x_j$, and $h_{m+1} = 0$;*
   (c) *If we define $|\mathcal{F}_{-1}^j| = n(= \prod_{j=1}^r n_j)$, then*
   $$|\pi_{i_j}(C_{i_j})| = q^{\sum_{m=0}^{x_j}(t-b_m^j)(|\mathcal{F}_{m-1}^j|-|\mathcal{F}_m^j|)}$$
   (d) *The code C has $q^{\sum_{j=1}^k\sum_{m=0}^{x_j}(t-b_m^j)(|\mathcal{F}_{m-1}^j|-|\mathcal{F}_m^j|)}$ codewords.*
4. *For all $0 \leq m \leq x_j, g \in \chi_m^j$ and $z \in \{i_j, \ldots, l\}$, there exist elements $h_z^{j,m,g} \in \mathcal{A}$ such that for each $s \in \{i_{j+1}, \ldots, i_k\}$ the polynomial $h_s^{j,m,g}$ is a*

normal form mod χ^s and the matrix with rows

$$\overrightarrow{g_h} = \left(0 \ , \ \ldots \ , \ 0 \ , \ a^{\overset{(i_j}{b^j_m}} g \ , \ h^{j,m,g}_{i_j+1} \ , \ \ldots \ , \ h^{j,m,g}_{l} \right)$$

is a generator matrix of C.

Before the proof, let us introduce an example to illustrate the theorem.

Example 2. *Consider the $\mathbb{Z}_8[X_1, X_2]/\left\langle X_1^4, X_2^4 \right\rangle -$code C of index $l = 3$ generated by the following codewords:*

$$\left\{(X_1^2, X_1^2, 4X_2), (X_2^2, X_2^2, 0), (X_1X_2, X_1X_2, 4X_1), (2X_2, 2X_2, 0), (4X_1, 4X_1, 0)\right\}.$$

Let us obtain its canonical generator matrix w.r.t. the lexicographic monomial order. We begin with the computation of the CGS of the (ideal in $\mathbb{Z}_8[X_1, X_2]$ corresponding to the) projection $\pi_1(C)$, i.e., $\left\langle X_1^4, X_2^4, X_1^2, X_2^2, X_1X_2, 2X_2, 4X_1 \right\rangle$. It is $\chi^1 = \chi_0^1 \cup 2\chi_1^1 \cup 4\chi_2^1$, where $\chi_0^1 = \{X_1^2, X_2^2, X_1X_2\}$, $\chi_1^1 = \{X_1^2, X_2\}$, $\chi_2^1 = \{X_1, X_2\}$. And so the corresponding Ferrers diagrams are $\mathcal{F}_2^1 = \{(0,0)\} \subseteq \mathcal{F}_1^1 = \mathcal{F}_2^1 \cup \{(1,0)\} \subseteq \mathcal{F}_0^1 = \mathcal{F}_1^1 \cup \{(0,1)\}$. Therefore,

$$|\pi_1(C)| = 2^{(3-0)(16-3)+(3-1)(3-2)+(3-2)(2-1)} = 2^{42}.$$

Next, as $C_2 = C_3$ (any codeword with a zero as first component begins with $(0,0)$) we proceed with the computation of the CGS of the (ideal in $\mathbb{Z}_8[X_1, X_2]$ corresponding to the) projection $\pi_3(C_3)$, i.e., $\left\langle X_1^4, X_2^4, 4(X_1^2 + X_2^2), 4X_1X_2, 4X_2^3 \right\rangle$. It is $\chi^2 = \chi_0^2 \cup 4\chi_1^2$, where $\chi_0^2 = \{X_1^4, X_2^4\}$, $\chi_1^2 = \{X_1^2 + X_2^2, X_1X_2, X_2^3\}$. And so the corresponding Ferrers diagrams are $\mathcal{F}_2^1 = \{(0,0), (1,0), (0,1), (0,2)\} \subseteq \mathcal{F}_1^0 = \{0,1,2,3\} \times \{0,1,2,3\}$. Therefore,

$$|\pi_2(C)| = 2^{(3-0)(16-16)+(3-2)(16-4)} = 2^{12}.$$

Hence, the code has 2^{54} codewords and its canonical generator matrix is:

$$\left(\begin{array}{cc|c} X_1^2 & X_1^2 & 4X_2 \\ X_2^2 & X_2^2 & 0 \\ X_1X_2 & X_1X_2 & 4X_1 \\ 2X_1^2 & 2X_1^2 & 0 \\ 2X_2 & 2X_2 & 0 \\ 4X_1 & 4X_1 & 0 \\ 4X_2 & 4X_2 & 0 \\ \hline 0 & 0 & 4(X_1^2 + X_2^2) \\ 0 & 0 & 4X_1X_2 \\ 0 & 0 & 4X_2^3 \end{array} \right).$$

Observe that the polynomials X_1^4, X_2^4 in the CGS do not correspond to any row in the matrix, as they are reduced to zero mod the defining ideal of $\mathcal{A}$. Notice also that the elements in the upper right corner are normal forms mod χ^2.

Proof. For all $i = 1, \dots, l+1$, let $C_i = \cap_{j=1}^{i-1} \pi_j^{-1}(0)$ be the subset of C consisting of those codewords of the form $(0, \overset{(i-1}{\dots}, 0, g_i, \dots, g_l)$. It is straightforward to check that $C = C_1 \supseteq C_2 \supseteq \cdots \supseteq C_{l+1} = \{0\}$ is a decreasing chain of $\mathcal{A}-$(sub)codes of C. Let us refine this chain by preserving only those nonzero C_i such that $C_i \neq C_{i+1}$, i.e., there exists a natural number $k \in \{1, \dots, l\}$ and a sequence of k natural numbers $1 \leq i_1 < \cdots < i_k \leq l$ such that $C = C_{i_1} \supsetneq C_{i_2} \supsetneq \cdots \supsetneq C_{i_k} \neq \{0\}$ with the conditions $C_s = C_{i_{j+1}}$ for all $i_j < s \leq i_{j+1}$ and for all $j \in \{1, \dots, k-1\}$ (i.e,. any codeword with its $s-1$ first components equal to zero, must have the following $i_{j+1} - s$ components equal to zero, too), $C_s = 0$, for all $s > i_k$, and $C_s = C$, for all $s \leq i_1$.

For each $1 \leq j \leq k$, consider the projection $\pi_{i_j}(C_{i_j}) \subseteq \mathcal{A}$. It is clear that it is an ideal of $\mathcal{A}$, because C is an $\mathcal{A}-$code. Therefore, we can lift it to a unique ideal $I_{i_j} \lhd R[X_1, \dots, X_r]$ containing $\langle t_1(X_1), \dots, t_r(X_r) \rangle$ and such that $I_{i_j} / \langle t_1(X_1), \dots, t_r(X_r) \rangle \cong \pi_{i_j}(C)$. Therefore, we can apply [20, Theorem 4.3] to find the $k+1$ sequences of natural numbers $0 \leq x_1, \dots, x_k \leq t-1$ and $0 = b_0^j < b_1^j < \cdots < b_{x_j}^j < b_{x_j+1}^j = t$ and the k strictly decreasing chain of Ferrers diagrams $\mathcal{F}_0^j \supset \mathcal{F}_1^j \supset \cdots \supset \mathcal{F}_{x_j}^j$ (where $1 \leq j \leq k$) satisfying items #1,#2 and #3 of the theorem.

Now, for all $1 \leq j \leq k$, $0 \leq m \leq x_j$ and $g \in \chi_m^j$, since $a^{b_m^j} g \in a^{b_m^j} \chi_m^j \subseteq \chi^j \subseteq \pi_{i_j}(C_{i_j})$, there exist elements $w_z^{j,m,g} \in \mathcal{A}$ (for all $z \in \{i_j + 1, \dots, l\}$) such that

$$\overrightarrow{g_w} = \left(0 \ , \ \dots \ , \ 0 \ , \ \overset{(i_j}{a^{b_m^j} g} \ , \ w_{i_j+1}^{j,m,g} \ , \ \dots \ , \ w_l^{j,m,g} \right) \in C.$$

We claim that the matrix W consisting on all the elements of this form is a generator matrix of C. Namely, if c is a nonzero codeword in C, then there exists $j \in \{1, \dots, k\}$ such that $c \in C_{i_j} \setminus C_{i_{j+1}}$ (where $C_{i_{k+1}} := \{0\}$), i.e., the codeword has the form $(0, \overset{(i_j-1}{\dots}, 0, c_{i_j}, \dots, c_l)$. Because $c_{i_j} \in \pi_{i_j}(C_{i_j})$ we can apply the $L-$reduction of c_{i_j} mod χ^j to the element c (simply substitute the elements $a^{b_m^j} g$ in χ^j by the corresponding row $\overrightarrow{g_w}$). The remaining word is in C, but since its i_j-th component is zero, it must be an element in C_s where $s \in \{i_{j+1}, \dots, i_{k+1}\}$. If $s = i_{k+1}$, then such a codeword is zero and we have shown that c is generated by the rows of W. Otherwise, we can apply the same argument inductively to reduce the remaining codeword mod $\chi^{j+1}, \dots,$ mod χ^k, until the zero codeword is obtained.

Finally, the generator form stated in the theorem is obtained when we apply the $L-$reduction of $w_s^{j,m,g}$ mod χ^s to the corresponding rows of the matrix W (where $s \in \{i_{j+1}, \dots, i_k\}, 1 \leq j < k, 0 \leq m \leq x_j$ and $g \in \chi_m^j$).

□

Example 3. *The (punctured) Generalized Kerdock Code [10] has a multivariable presentation over the Galois ring $R = GR(q^2, 2^2)$ ($q = 2^d$) of order q^2 and characteristic 2^2, which can be seen as an $\mathcal{A}-$code in our setting (with* $\mathcal{A} = R[X_1, \dots, X_r] / \left\langle X_1^{q^m-1} - 1, X_2^2 - 1, \dots, X_r^2 - 1 \right\rangle, m \geq 3$ *odd,* $r = d+1$, *and $l = 1$) [16]. We will show that the (extended) Generalized Kerdock Code admits also an $\mathcal{A}-$code presentation with $l > 1$, and we will obtain its generator matrix.*

Any element $b \in R$ can be decomposed as $b = \gamma_0(b) + 2\gamma_1(b)$, where $\gamma_i(b) \in \Gamma(R) = \{b^q = b \mid b \in R\}$ (the Teichmüller Coordinate Set (TCS) *of R). The multiplicative group $1 + 2R$ is a direct product $\langle\eta_1\rangle \times \cdots \times \langle\eta_d\rangle$ of d subgroups of order 2. If $S = GR(q^{2m}, 2^2)$ is the Galois extension of odd degree m over R, then the multiplicative group on nonzero elements in its TCS $\Gamma(S) = \{b^{q^m} = b \mid b \in S\}$ is cyclic. Let $\theta \in \Gamma(S)$ be one of its generators (of order $\tau = q^m - 1$). Consider the trace map* Tr *from S onto R.*

The (punctured) Generalized Kerdock Code is equivalent to the projection of the $A-$code of index $l = 1$

$$C = \left\{ \left(\sum_{i_1=0}^{\tau-1} \sum_{i_2=0}^{1} \cdots \sum_{i_r=0}^{1} \left((\mathrm{Tr}(\xi\theta^{i_1}) + b)\eta_1^{i_2} \dots \eta_l^{i_r} \right) X_1^{i_1} X_2^{i_2} \dots X_r^{i_r} \right) \mid \xi \in S, b \in R \right\}$$

with the map $\gamma_1^{\tau q} = \overbrace{\gamma_1 \times \cdots \times \gamma_1}^{\tau q}$, i.e., $\gamma_1^{\tau q}(\Phi(C)) \subseteq \Gamma(R)^{\tau q}$.

For any codeword

$$(f_{\xi,b}) := \left(\sum_{i_1=0}^{\tau-1} \sum_{i_2=0}^{1} \cdots \sum_{i_r=0}^{1} \left((\mathrm{Tr}(\xi\theta^{i_1}) + b)\eta_1^{i_2} \dots \eta_d^{i_r} \right) X_1^{i_1} X_2^{i_2} \dots X_r^{i_r} \right)$$

with $\xi \in S, b \in R$, observe that the parity-check sum of

$$(\mathrm{Tr}(\xi) + b, \mathrm{Tr}(\xi\theta) + b, \dots, \mathrm{Tr}(\xi\theta^{\tau-1}) + b, b)$$

is zero, and define

$$g_{\xi,b} := \sum_{i_1=0}^{\tau-1} \sum_{i_2=0}^{1} \cdots \sum_{i_r=0}^{1} \left(b\eta_1^{i_2} \dots \eta_d^{i_r} \right) X_1^{i_1} X_2^{i_2} \dots X_r^{i_r}.$$

Consider the $\mathcal{A}-$code $D = \{(f_{\xi,b}, g_{\xi,b}) \mid \xi \in S, b \in R\}$ of index $l = 2$. Its image $\gamma_1^{2\tau q}(\Phi(D))$, when punctured in the first q^{m+1} components, is equivalent to the (extended) Generalized Kerdock Code.

Let us obtain the generator matrix of Theorem 1 for D. From [16] we know that the $\mathcal{A}-$code C is 1-generated by the codeword

$$(H_0 P(X_1) Q(X_2, \dots, X_r))$$

where H_0 is the trailing coefficient of the unique irreducible divisor $H(X_1) \in R[X_1]$ of $X_1^\tau - 1$ such that $H(\theta) = 0$, $P(X_1) = \frac{X_1^\tau - 1}{(X_1-1)H^*(X_1)}$ ($H^*(X_1)$ is the reciprocal polynomial of $H(X_1)$) and

$$Q(X_2, \dots, X_r) = \sum_{i_2=0}^{1} \cdots \sum_{i_r=0}^{1} (\eta_1^{i_2} \dots \eta_d^{i_r}) X_2^{i_2} \dots X_r^{i_r}.$$

Therefore, D is also $1-$generated by construction, and its generator matrix is given by

$$\left(H_0 P(X_1) Q(X_2, \ldots, X_r)\ ,\ \sum_{i_1=0}^{\tau-1} \frac{H_0}{H^*(1)} X_1^{i_1} Q(X_2, \ldots, X_r) \right)$$

because the sum of the coefficients of the polynomial $H_0 P(X_1)$ is $\frac{-H_0}{H^*(1)}$.

4 Canonical generator matrix of the dual code

In this section we present some results about duality of codes. If R is a finite commutative quasi-Frobenius ring, duality for $R-$linear codes can be defined through the inner product of R^{nl}: $(r_1, \ldots, r_{nl}) \cdot (s_1, \ldots, s_{nl}) = \sum_{j=1}^{nl} r_j s_j$. This notion can be translated into $\mathcal{A}-$codes using the map Φ.

Definition 4. *The R-*dual code *of the $\mathcal{A}-$code C is*

$$C^{\perp_R} = \{e \in E \mid \Phi(e) \cdot \Phi(c) = 0 \text{ , for all } c \in C\}.$$

In the special case of $\mathcal{A} = R[X_1, \ldots, X_r]/\left\langle X_1^{n_1} - 1, \ldots, X_r^{n_r} - 1\right\rangle$, it is customary to define an Hermitian inner product on E: $\langle (f_1, \ldots, f_l), (g_1, \ldots, g_l)\rangle = \sum_{j=1}^{l} f_j \overline{g_j}$, where $\bar{\cdot}$ is a conjugation map on $\mathcal{A}$ defined by

$$\begin{array}{ccc} \bar{\cdot} : \mathcal{A} & \longrightarrow & \mathcal{A} \\ \sum f_{\mathbf{i}} \mathbf{X}^{\mathbf{i}} & \longrightarrow & \sum f_{\mathbf{i}} \mathbf{X}^{\mathbf{n}-\mathbf{i}} \end{array},$$

with $\mathbf{n} = (n_1, \ldots, n_r)$. The (usual) Euclidean inner product $\cdot$ on R^{nl} and the Hermitian product $\langle \cdot, \cdot \rangle$ on E can be related using the following result, whose proof can be found in Proposition 3.2 of [12].

Proposition 1. *Let C be a code over $E = \mathcal{A}^l$. Let us denote by $\perp_E$ the dual taken with respect the Euclidean inner product $\cdot$ of R^{nl} and $\perp_H$ the dual in E taken with respect the Hermitian inner product $\langle \cdot, \cdot \rangle$. If $\Phi : E \to R^{nl}$ is the map of Definition 2, then $\Phi(C)^{\perp_E} = \Phi(C^{\perp_H})$.*

However, in some cases, we have to consider $\mathcal{A}$-duality instead of R-duality. For example, this happens with codes over the Frobenius local ring $\mathbb{Z}_4[X]/\langle X^2 \rangle$, since it is not possible to construct a duality preserving map from the ring $\mathcal{A}$ to R^n, as can be seen on [18]. On the other hand, if there exists a map θ from the ring $\mathcal{A}$ to R^n that preserves duality, then $\mathcal{A}$-duality can be analized as R-duality. This is the case of the following example which provides a code over an affine algebra whose Gray image has good properties.

Example 4. *Let $R = \mathbb{Z}_4$ and $t_1(X_1) = X_1^2 + 2X_1$ and let*

$$A = \begin{bmatrix} 2X_1 & 3+3X_1 & 3+3X_1 & 3+3X_1 \\ 3+3X_1 & 2X_1 & 3+3X_1 & 3+3X_1 \\ 3+3X_1 & 3+X_1 & 2X_1 & 1+3X_1 \\ 3+3X_1 & 1+3X_1 & 3+X_1 & 2X_1 \end{bmatrix}.$$

Then, $[I_4|A]$ is the generator matrix of a self-dual code C over R of length 8 such that its Gray image is a Type II extremal self-dual code over $\mathbb{Z}_4$ of length 16 (see [17] and [18] for details).

If $\mathcal{A}$-duality is considered, the dual code is defined as

$$C^{\perp_{\mathcal{A}}} = \left\{ e \in E \; | e \cdot c = \sum_{i=1}^{l} e_i c_i = 0 \text{ , for all } c \in C \right\}.$$

As the code C can be seen as a subgroup of $(E, +)$, it can be proved that there exists a group isomorphism $C^{\perp_{\mathcal{A}}} \cong E/C$ and so, $|C^{\perp_{\mathcal{A}}}||C| = |E|$ (see [9]).

A matrix H whose rows generate the dual code $C^{\perp_{\mathcal{A}}}$ as $\mathcal{A}$-module is known as *parity-check matrix* of the code C. If such a matrix exists, then $C = \{c \in E \,|\, Hc^t = 0\}$, that is, $C = \ker H$. All linear codes over a quasi-Frobenius ring have a parity-check matrix H.

We will use the canonical generator systems (CGS) in order to find a parity-check matrix of a given code C. We will only consider codes over univariate polynomial rings $\mathcal{A} = R[X]/\langle t_1(X) \rangle$, with $t_1(X)$ monic and such that $\mathcal{A}$ is Frobenius. In the following, we will denote $\mathcal{A}$-duality as $\perp$.

Let C be an $\mathcal{A}$-code of index l. As in Theorem 1 let us consider the decreasing chain of $\mathcal{A}-$(sub)codes of C given by $C = C_1 \supseteq C_2 \supseteq \cdots \supseteq C_{l+1} = \{0\}$, with $C_i = \cap_{j=1}^{i-1} \pi_j^{-1}(0)$ for $i = 1, \ldots, l+1$. Let us denote by C' the punctured code of C_2 on the first position.

Lemma 1. *Let c' be an element of $C'^{\perp}$. Then, there exists an element $c \in \mathcal{A}$ such that (c, c') is an element of $C^{\perp}$.*

Proof. Let us suppose that there exists at least one element of C with $c_1 \neq 0$. Otherwise, any element $c' \in C'^{\perp}$ can be extended to an element $(c_1, c') \in C^{\perp}$ by concatenation of any $c_1 \in \mathcal{A}$, and the result follows trivially.

Following Theorem 1, there exist k Canonical Generating Systems (CGS) $\chi^j = \chi_0^j \cup a^{b_1^j} \chi_1^j \cup \ldots \cup a^{b_{x_j}^j} \chi_{x_j}^j$, with $0 = b_0^j < b_1^j < \cdots < b_{x_j}^j < b_{x_{j+1}}^j = t$, such that, for $j = 1, \ldots, k$, the set χ^j generates the projection $\pi_{i_j}(C_{i_j})$ as $\mathcal{A}$-submodule.

Let us define the map $\varphi : C^{\perp} \to C'^{\perp}$ such that for any $c = (c_1, c_2, \ldots, c_l) \in E$, $\varphi(c) = (c_2, \ldots, c_l)$. Since $c \in C^{\perp}$, clearly $c \cdot e = 0$ for all $e \in C_2$, so $0 = \sum_{i=2}^{l} c_i e_i$, i.e., $(c_2, \ldots, c_l) \in C'^{\perp}$ and φ is well defined. Moreover, φ is an $\mathcal{A}$-linear map and $\ker \varphi = \{(c_1, 0, \ldots, 0) \in E \,|\, c_1 \cdot G_i = 0 \text{ for all } G_i \in \chi^1\}$. The ring $\mathcal{A}$ is Frobenius so, from Theorem 1, it follows that $|C'^{\perp}| = q^{(l-1)nt - \sum_{j=2}^{k} \sum_{m=0}^{x_k} (t - b_i^j)(|\mathcal{F}_{m-1}^j| - |\mathcal{F}_m^j|)}$, where n is the degree of the polynomial $t_1(X_1)$ and $\mathcal{F}_m^j$ is the Ferrers diagram associated to χ_m^j. On the other hand, also by Theorem 1, we have that $|\ker \varphi| = q^{nt - \sum_{m=0}^{x_1} (t - b_m^1)(|\mathcal{F}_{m-1}^1| - |\mathcal{F}_m^1|)} = |C^{\perp}|/|C'^{\perp}|$. Then, φ is a surjective map and the result follows.

$\square$

Theorem 2. *Let C be an $\mathcal{A}$-code of index l and let H' be a generator matrix of the code $C'^{\perp}$. Then, there exist polinomials $G'_0, \ldots, G'_s$ and $h_{s+1}, \ldots, h_k$ in*

$\mathcal{A}$ *such that the matrix*

$$\left[\begin{array}{c|ccc} G'_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ G'_s & 0 & \dots & 0 \\ \hline h_{s+1} & & & \\ \vdots & & H' & \\ h_k & & & \end{array}\right]$$

is a parity-check matrix of the code C*.*

Proof. From Theorem 1, we know that there exists a Canonical Generator System χ^1 which generates the projection $\pi_1(C_1)$ as $\mathcal{A}$-submodule. Since $\mathcal{A}$ is a univariate polynomial ring, then $\chi^1 = \{G_0, G_1, \dots, G_{x_1}\}$ where G_i are polynomials such that $||G_i|| = b_i^1$. Now, for each $1 \leq i \leq x_1$, let us denote $A_i = \{g \in \mathcal{A} \,|\, g \cdot G_i = 0\}$, the annihilator of G_i in $\mathcal{A}$. The intersection $A = \cap_{i=1}^{x_1} A_i$ is an ideal of $\mathcal{A}$ so, by [20, Theorem 4.3], there exists $\chi' = \{G'_0, G'_1, \dots, G'_s\}$, a Canonical Generator System of the ideal A. Since each row $(h'_{i2}, \dots, h'_{il})$, $s+1 \leq i \leq k$, of H' is an element of $C'^{\perp}$, by Lemma 1 it is possible to find a polinomial $h_i \in \mathcal{A}$ such that $(h_i, h'_{i2}, \dots, h'_{il}) \in C^{\perp}$.

It is easy to see that any row of the matrix H is in $C^{\perp}$. First of all, notice that the polynomials G'_i, $1 \leq i \leq s$, generate A, so the row $(G'_i, 0, \dots, 0)$ is an element of $C^{\perp}$. The other rows of H are in $C^{\perp}$ by construction. Conversely, let $c = (c_1, c_2, \dots, c_l) \in C^{\perp}$, then $c' = (c_2, \dots, c_l) \in C'^{\perp}$ will be generated by the rows $h'^{(i)}$ of H'. That is, there exist elements $\beta_{s+1}, \dots, \beta_k \in \mathcal{A}$ such that $c' = \sum_{i=s+1}^{k} \beta_i h'^{(i)}$. If we denote by $(G_j, G_{j2}, \cdots, G_{jl})$ the j-th row of the generator matrix G of C, it is clear that $h_i G_j + \sum_{w=2}^{l} h'_{iw} G_{jw} = 0$ for each $1 \leq j \leq x_1$. So, for each j

$$\sum_{i=s+1}^{k} \beta_i h_i G_j = \sum_{i=s+1}^{k} \beta_i \left(- \sum_{w=2}^{l} h'_{iw} G_{jw} \right) = - \sum_{w=2}^{l} c_w G_{jw} = c_1 G_j.$$

Then, we have that $(c_1 - \sum_{i=s+1}^{k} \beta_i h_i) G_j = 0$ for $j = 1, \dots, x_1$. That is, $c_1 - \sum_{i=s+1}^{k} \beta_i h_i \in A$ and so, it can be written as an $\mathcal{A}$-linear combination of polynomials $G'_0, \dots, G'_s$. The proof is complete. □

We finish this section with two examples of parity-check matrices of codes over the rings $\mathbb{Z}_4[X]/\langle X^2 + 2X \rangle$ and $\mathbb{Z}_4[X]/\langle X^2 \rangle$, respectively. Both rings are local and Frobenius but none of them is a chain ring. These rings are studied in [17].

Example 5. *Let us consider the code* C *over* $\mathbb{Z}_4[X]/\langle X^2 + 2X \rangle$ *of index 2 whose generator matrix is given by*

$$\begin{bmatrix} X & 0 \\ 2 & X \\ 0 & 2 \end{bmatrix}.$$

The parity-check matrix of C is calculated as follows. First of all, notice that $H' = [2]$. On the other hand, it is easy to see that $A_1 = Ann(\langle X\rangle) = \langle X+2\rangle$ and $A_2 = Ann(\langle 2\rangle) = \langle 2\rangle$, so $A = \langle 2X\rangle$. The polynomial h_2 should satisfy the conditions

$$\begin{array}{rcl} h_2X + 0 & = & 0, \\ h_2 2 + 2X & = & 0 \end{array}$$

which imply $h_2 = X + 2$. Then, the parity-check matrix of C will be

$$\left[\begin{array}{cc} 2X & 0 \\ X+2 & 2 \end{array}\right] \backsim \left[\begin{array}{cc} X+2 & 2 \end{array}\right].$$

So the dual code $C^\perp$ is generated by the single word $(X+2, 2)$.

Example 6. *Let C be the code of index 2 over $\mathbb{Z}_4[X]/\langle X^2\rangle$ whose generator matrix is the same one that in Example 5. In order to find the parity-check matrix of C, we notice that $H' = [2]$ and that $A_1 = Ann(\langle X\rangle) = \langle X\rangle$, $A_2 = Ann(\langle 2\rangle) = \langle 2\rangle$. Therefore $A = \langle 2X\rangle$. Finally, the polynomial h_2 satisfies the conditions*

$$\begin{array}{rcl} h_2X + 0 & = & 0, \\ h_2 2 + 2X & = & 0 \end{array}$$

which yield to $h_2 = X$. So, the parity-check matrix of C is

$$\left[\begin{array}{cc} 2X & 0 \\ X & 2 \end{array}\right] \backsim \left[\begin{array}{cc} X & 2 \end{array}\right].$$

Notice that the dual code $C^\perp$ is also generated by a single word: $(X, 2)$. As it is referred in [17] there is no duality preserving map from the ring $\mathcal{A} = \mathbb{Z}_4[X]/\langle X^2\rangle$ to $\mathbb{Z}_4^2$. So, $\mathcal{A}$-duality cannot be analized as $\mathbb{Z}_4-$duality.

References

[1] T. P. Berger and N. E. Amrani. Codes over finite quotients of polynomial rings. *Finite Fields and Their Applications*, (25):165–181 (2015), 2014.

[2] G. Bini and F. Flamini. *Finite commutative rings and their applications.* Kluwer Academic Publishers, Boston, MA, 2002.

[3] Y. Cao. 1-generator quasi-cyclic codes over finite chain rings. *Applicable Algebra in Engineering, Communication and Computing*, 24(1):53–72, 2013.

[4] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms.* Springer, New York, 2007.

[5] H. Q. Dinh and S. R. López-Permouth. Cyclic and negacyclic codes over finite chain rings. *IEEE Trans. Inform. Theory*, 50(8):1728–1744, 2004.

[6] S. T. Dougherty, B. Yildiz, and S. Karadeniz. Codes over Rk, Gray maps and their binary images. *Finite Fields and Their Applications*, 17(3):205–219, 2011.

[7] J. Gao, L. Shen, and F.-W. Fu. Bounds on quasi-cyclic codes over finite chain rings. *Journal of Applied Mathematics and Computing*, 50(1):577–587, 2016.

[8] S. Jitman and S. Ling. Quasi-abelian codes. *Designs, Codes and Cryptography*, 74(3):511–531, 2015.

[9] V. L. Kurakin, A. S. Kuzmin, V. T. Markov, A. V. Mikhalev, and A. A. Nechaev. Linear codes and polylinear recurrences over finite rings and modules (a survey). In *Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999)*, volume 1719 of *Lecture Notes in Comput. Sci.*, pages 365–391. Springer, Berlin, 1999.

[10] A. S. Kuz′min and A. A. Nechaev. Linearly representable codes and the Kerdock code over an arbitrary Galois field of characteristic 2. *Uspekhi Mat. Nauk*, 49(5(299)):165–166, 1994.

[11] K. Lally and P. Fitzpatrick. Algebraic structure of quasicyclic codes. *Discrete Applied Mathematics*, 111(12):157–175, 2001.

[12] S. Ling and P. Solé. On the Algebraic Structure of Quasi-cyclic Codes II: Chain Rings. *Designs, Codes and Cryptography*, 30:113–130, 2003.

[13] S. R. López-Permouth, H. Özadam, F. Özbudak, and S. Szabo. Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes. *Finite Fields Appl.*, 19:16–38, 2013.

[14] E. Martínez-Moro, A. P. Nicolás, and I. F. Rúa. Multivariable codes in principal ideal polynomial quotient rings with applications to additive modular bivariate codes over $\mathbb{F}_4$. *Submitted*, 2015.

[15] E. Martínez-Moro and I. F. Rúa. Multivariable codes over finite chain rings: serial codes. *SIAM J. Discrete Math.*, 20(4):947–959, 2006.

[16] E. Martínez-Moro and I. F. Rúa. On repeated-root multivariable codes over a finite chain ring. *Designs, Codes and Crypt.*, 45:219–227, 2007.

[17] E. Martínez-Moro and S. Szabo. On codes over local Frobenius non-chain rings of order 16. volume 634 of *Contemp. Math.*, pages 227–241. Amer. Math. Soc., Providence, RI, 2015.

[18] E. Martínez-Moro, S. Szabo, and B. Yildiz. Linear codes over $\mathbb{Z}_4[x]/\langle x^2 + 2x\rangle$. *Int. J. Inf. Coding Theory*, 3(1):78–96, Apr. 2015.

[19] B. R. McDonald. *Finite rings with identity*. Marcel Dekker, Inc., New York, 1974. Pure and Applied Mathematics, Vol. 28.

[20] A. A. Nechaev and D. A. Mikhailov. A canonical system of generators of a unitary polynomial ideal over a commutative Artinian chain ring. *Diskret. Mat.*, 13(4):3–42, 2001.

[21] G. H. Norton and A. Sălăgean. On the structure of linear and cyclic codes over a finite chain ring. *Appl. Algebra Engrg. Comm. Comput.*, 10(6):489–506, 2000.

[22] A. Poli and L. Huguet. *Error correcting codes.* Prentice Hall International, Hemel Hempstead, 1992.