Proceedings of the 16th International Conference
on Computational and Mathematical Methods
in Science and Engineering, CMMSE 2016
4–8 July, 2016.

Linear and Cyclic Codes over direct product of Finite Chain Rings

Joaquim Borges[1], Cristina Fernández-Córdoba[1] and Roger Ten-Valls[1]

[1] *Department of Information and Communications Engineering,*
Universitat Autònoma de Barcelona

emails: joaquim.borges@uab.cat, cristina.fernandez@uab.cat, roger.ten@uab.cat

Abstract

We introduce a new type of linear and cyclic codes. These codes are defined over a direct product of two finite chain rings. The definition of these codes as certain submodules of the direct product of copies of these rings is given and the cyclic property is defined. Cyclic codes can be seen as submodules of the direct product of polynomial rings. Generator matrices for linear codes and generator polynomials for cyclic codes are determined.

Key words: Codes over rings, linear codes, cyclic codes, finite chain rings
MSC 2000: 94B60, 94B25

1 Introduction

Linear codes are a special family of codes with rich mathematical structure. One of the most studied class of linear codes is the class of linear cyclic codes. The algebraic structure of cyclic codes makes easier their implementation. For this reason many practically important codes are cyclic.

The study of codes over rings has been growing since it was proven in [8] that certain notorious non-linear binary codes can be seen as binary images under the Gray map of linear codes over $\mathbb{Z}_4$. In particular, the family of codes over chain rings has received much attention because it includes some good codes (e.g. [6], [9]).

In recent times, linear codes with sets of coordinates over different rings are studied (e.g. $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ in [3], $\mathbb{Z}_{p^r}^\alpha \times \mathbb{Z}_{p^s}^\beta$ in [2]). Also, linear cyclic codes over these kind of structures are studied, see [1], [4], [5] and [7].

 ISBN: 978-84-608-6082-2

In this paper we present the structure of linear and cyclic codes over direct product of finite chain rings, $\mathcal{R}_1$ and $\mathcal{R}_2$. Linear codes can be seen as certain submodules of $\mathcal{R}_1^{\alpha} \times \mathcal{R}_2^{\beta}$, and cyclic codes as submodules of $\mathcal{R}_{\alpha,\beta} = \frac{\mathcal{R}_1[x]}{\langle x^{\alpha}-1\rangle} \times \frac{\mathcal{R}_2[x]}{\langle x^{\beta}-1\rangle}$. We determine the generator matrix in standard form and the generator polynomials in the cyclic case. Finally, we present examples to illustrate some particular cases.

2 Review of cyclic codes over finite chain rings

Let $\mathcal{R}$ be a finite chain ring with maximal ideal $\langle\gamma\rangle$ and let e be the nilpotency of γ. It is well-know that there exist a prime p and a positive integer m such that $|\mathcal{R}/\langle\gamma\rangle| = q = p^m$ and $|\mathcal{R}| = q^e = p^{me}$.

Let C be a cyclic code of length n over $\mathcal{R}$. It is known that we can identify C as an ideal of $\mathcal{R}[x]/(x^n-1)$. We assume that n is a positive integer such that it is coprime with p. Therefore, the polynomial x^n-1 has a unique decomposition as a product of basic irreducible polynomials that are pairwise coprime over $\mathcal{R}[x]$.

Theorem 2.1 ([6, Theorem 3.5])**.** *Let C be a cyclic code of length n over a finite chain ring $\mathcal{R}$, which has maximal ideal $\langle\gamma\rangle$ and e is the nilpotency of γ. Then, there exist polynomials $g_0, g_1, \ldots, g_{e-1}$ in $\mathcal{R}[x]$ such that $C = \langle g_0, \gamma g_1, \ldots, \gamma^{e-1} g_{e-1}\rangle$ and $g_{e-1} \mid g_{e-2} \mid \cdots \mid g_1 \mid g_0 \mid (x^n-1)$.*

Let $C = \langle g_0, \gamma g_1, \ldots, \gamma^{e-1} g_{e-1}\rangle$ be a cyclic code of length n and let $g = g_0 + \gamma g_1 + \cdots + \gamma^{e-1} g_{e-1}$. Since g_0 is a factor of x^n-1 and for $i = 1 \ldots e-1$ the polynomial g_i is a factor of g_{i-1}, we will denote $\hat{g}_0 = \frac{x^n-1}{g_0}$ and $\hat{g}_i = \frac{g_{i-1}}{g_i}$ for $i = 1 \ldots e-1$. Define $G = \prod_{i=0}^{e-1} \hat{g}_i$, then it is clear that $Gg = \left(\prod_{i=0}^{e-1} \hat{g}_i\right) g = 0$ over $\mathcal{R}[x]/(x^n-1)$.

Lemma 2.2. *Let C be a cyclic code of length n over a finite chain ring $\mathcal{R}$, which has maximal ideal $\langle\gamma\rangle$ and e is the nilpotency of γ. Let $g_0, g_1, \ldots, g_{e-1}$ in $\mathcal{R}[x]$ such that $C = \langle g_0, \gamma g_1, \ldots, \gamma^{e-1} g_{e-1}\rangle$ and $g_{e-1} \mid g_{e-2} \mid \cdots \mid g_1 \mid g_0 \mid (x^n-1)$. Then*

1. $\gamma^{e-1} g = \gamma^{e-1} g_{e-1} \frac{G}{\hat{g}_0}$,
2. $\gamma^{e-1-i} (\prod_{j=0}^{i-1} \hat{g}_j) g = \gamma^{e-1} g_{e-1} \frac{G}{\hat{g}_i}$, *for* $i = 1, \ldots, e-1$.

Proof. Let $g = g_0 + \gamma g_1 + \cdots + \gamma^{e-1} g_{e-1}$. Then

$$\gamma^{e-1} g = \gamma^{e-1} g_0 \tfrac{1}{g_1} \tfrac{g_1}{g_2} \ldots \tfrac{g_{e-3}}{g_{e-2}} \tfrac{g_{e-2}}{g_{e-1}} g_{e-1} = \gamma^{e-1} g_{e-1} \hat{g}_1 \hat{g}_2 \ldots \hat{g}_{e-2} \hat{g}_{e-1} = \gamma^{e-1} g_{e-1} \frac{G}{\hat{g}_0},$$

 ISBN: 978-84-608-6082-2

and 1 holds. For $i = 1, \ldots, e-1$ we have that

$$\begin{aligned}\gamma^{e-1-i}(\prod_{j=0}^{i-1}\hat{g}_j)g =& \gamma^{e-1-i}(\prod_{j=0}^{i-1}\hat{g}_j)\gamma^i g_i \frac{1}{g_{i+1}}\frac{g_{i+1}}{g_{i+2}}\cdots\frac{g_{e-2}}{g_{e-1}}g_{e-1}\\ =& \gamma^{e-1}g_{e-1}\hat{g}_0\hat{g}_1\cdots\hat{g}_{i-1}\hat{g}_{i+1}\cdots\hat{g}_{e-1} = \gamma^{e-1}g_{e-1}\frac{G}{\hat{g}_i},\end{aligned}$$

and statement 2 is proved.

□

Corollary 2.3 (of Th. 2.1)**.** *Let C be a cyclic code of length n over a finite chain ring $\mathcal{R}$ such that $C = \langle g_0, \gamma g_1, \ldots, \gamma^{e-1}g_{e-1}\rangle$ with $g_{e-1} \mid g_{e-2} \mid \cdots \mid g_1 \mid g_0 \mid (x^n-1)$. Then,*

$$|C| = |\mathcal{R}/\langle\gamma\rangle|^{\sum_{i=0}^{e-1}(e-i)\deg(\hat{g}_i)}.$$

Proof. From the previous definition of $\hat{g}_i$, these polynomials are the same polynomials described in [6, Theorem 3.4]. □

Theorem 2.4. *Let C be a cyclic code of length n over a finite chain ring $\mathcal{R}$, which has maximal ideal $\langle\gamma\rangle$ and e is the nilpotency of γ. Let $g_0, g_1, \ldots, g_{e-1}$ polynomials in $\mathcal{R}[x]$ such that $C = \langle g_0, \gamma g_1, \ldots, \gamma^{e-1}g_{e-1}\rangle$ and $g_{e-1} \mid g_{e-2} \mid \cdots \mid g_1 \mid g_0 \mid (x^n-1)$. Then the polynomial $g = g_0 + \gamma g_1 + \cdots + \gamma^{e-1}g_{e-1}$ is a generating polynomial of C, i.e., $C = \langle g\rangle$.*

Proof. Clearly $g = g_0+\gamma g_1+\cdots+\gamma^{e-1}g_{e-1} \in C$. then, we only have to prove that $\gamma^i g_i \in \langle g\rangle$, for all $i = 0, \ldots, e-1$.

Case $e = 2$: We have that $g = g_0 + \gamma g_1$, and $C = \langle g_0, \gamma g_1\rangle$. Then, $\gamma g = \gamma g_0 = \gamma g_1 \frac{g_0}{g_1}$ and $\frac{x^n-1}{g_0}g = \gamma g_1 \frac{x^n-1}{g_0}$, since $\frac{g_0}{g_1}$ and $\frac{x^n-1}{g_0}$ are coprime then γg_1 belongs to $\langle g\rangle$ and hence g_0 also belongs to $\langle g\rangle$.

Case $e = 3$: We have that $g = g_0 + \gamma g_1 + \gamma^2 g_2$, and $C = \langle g_0, \gamma g_1, \gamma^2 g_2\rangle$. Now $\gamma^2 g = \gamma^2 g_2 \frac{g_1}{g_2}\frac{g_0}{g_1}$, $\gamma\frac{x^n-1}{g_0}g = \gamma^2 g_2 \frac{x^n-1}{g_0}\frac{g_1}{g_2}$ and $\frac{x^n-1}{g_0}\frac{g_0}{g_1}g = \gamma^2 g_2 \frac{x^n-1}{g_0}\frac{g_0}{g_1}$, since $\gcd(\frac{g_0}{g_1}, \frac{g_1}{g_2}, \frac{x^n-1}{g_0}) = 1$ then $\gamma^2 g_2$ belongs to $\langle g\rangle$, hence $g_0 + \gamma g_1$. So $\langle g\rangle = \langle g_0 + \gamma g_1, \gamma^2 g_2\rangle$. Arguing as in case $e = 2$ it is straightforward that $\langle g\rangle = \langle g_0, \gamma g_1, \gamma^2 g_2\rangle$.

In the general case, let $g = g_0 + \gamma g_1 + \cdots + \gamma^{e-1}g_{e-1}$ and define, as in Lemma 2.2, the polynomials G and $\hat{g}_i$ for $i \in \{0, \ldots, e-1\}$. Then, $\gamma^{e-1}g = \gamma^{e-1}g_{e-1}\frac{G}{\hat{g}_0} \in \langle g\rangle$ and $\gamma^{e-1-i}(\prod_{j=0}^{i-1}\hat{g}_j)g = \gamma^{e-1}g_{e-1}\frac{G}{\hat{g}_i} \in \langle g\rangle$, for $i \in \{1, \ldots, e-1\}$. Since $\gcd(\frac{G}{\hat{g}_0}, \frac{G}{\hat{g}_1}, \ldots, \frac{G}{\hat{g}_{e-1}}) = 1$, we have that $\gamma^{e-1}g_{e-1} \in \langle g\rangle$ and $\langle g\rangle = \langle g_0 + \gamma g_1 + \cdots + \gamma^{e-2}g_{e-2}, \gamma^{e-1}g_{e-1}\rangle$.

Reasoned similarly, one obtains that $\langle g\rangle = \langle g_0, \gamma g_1, \ldots, \gamma^{e-1}g_{e-1}\rangle$. □

Theorem 2.5. *Let $C = \langle g\rangle = \langle g_0 + \gamma g_1 + \cdots + \gamma^{e-2}g_{e-2} + \gamma^{e-1}g_{e-1}\rangle$ be a cyclic code of length n over a finite chain ring $\mathcal{R}$, which has maximal ideal $\langle\gamma\rangle$ and e is the nilpotency of*

 ISBN: 978-84-608-6082-2

γ with $g_{e-1} \mid g_{e-2} \mid \cdots \mid g_1 \mid g_0 \mid (x^n-1)$. We define the sets

$$S_{\gamma^j} = \left[x^i (\prod_{t=0}^{j-1} \hat{g}_t) g \right]_{i=0}^{\deg(\hat{g}_j)},$$

for $0 \leq j < e$. Then,

$$S = \bigcup_{j=0}^{e-1} S_{\gamma^j}$$

forms a minimal generating set for C as an $\mathcal{R}$-module.

Proof. Let $c \in \mathcal{C}$. Then, $c = dg$ with $d \in \mathcal{R}[x]$. If $\deg(d) < \deg(\hat{g}_0)$ then $dg \in \langle S_{\gamma^0} \rangle_{\mathcal{R}}$ and $c \in \langle S \rangle_{\mathcal{R}}$. Otherwise, compute $d = d_0\hat{g}_0 + r_0$ with $\deg(r_0) < \deg(\hat{g}_0)$, so $dg = d_0\hat{g}_0 g + r_0 g$ and $r_0 g \in \langle S_{\gamma^0} \rangle_{\mathcal{R}}$.

If $\deg(d_0) < \deg(\hat{g}_1)$ then $d_0\hat{g}_0 g \in \langle S_{\gamma^1} \rangle_{\mathcal{R}}$ and $c \in \langle S \rangle_{\mathcal{R}}$. Otherwise, compute $d_0 = d_1\hat{g}_1 + r_1$ with $\deg(r_1) < \deg(\hat{g}_1)$, so $d_0\hat{g}_0 g = d_1\hat{g}_1\hat{g}_0 g + r_1\hat{g}_0 g$ and $r_1\hat{g}_0 g \in \langle S_{\gamma^1} \rangle_{\mathcal{R}}$.

In the worst case and reasoning similarly, one obtains that $c \in \langle S \rangle_{\mathcal{R}}$ if $d_{e-2}(\prod_{t=0}^{e-2} \hat{g}_t) g \in \langle S \rangle_{\mathcal{R}}$. It is obvious that if $\deg(d_{e-2}) < \deg(\hat{g}_{e-1})$ then $d_{e-2}(\prod_{t=0}^{e-2} \hat{g}_t) g \in \langle S_{\gamma^{e-1}} \rangle_{\mathcal{R}}$, if not, $d_{e-2} = d_{e-1}\hat{g}_{e-1} + r_{e-1}$. Therefore,

$$d_{e-2}(\prod_{t=0}^{e-2} \hat{g}_t) g = d_{e-1}(\prod_{t=0}^{e-1} \hat{g}_t) g + r_{e-1}(\prod_{t=0}^{e-2} \hat{g}_t) g = r_{e-1}(\prod_{t=0}^{e-2} \hat{g}_t) g \in \langle S_{\gamma^{e-1}} \rangle.$$

Since $r_{e-1}(\prod_{t=0}^{e-2} \hat{g}_t) g \in \langle S_{\gamma^{e-1}} \rangle$ then $c \in \langle S \rangle_{\mathcal{R}}$, so S is a generating set. By the definition of S clearly

$$|S| = |\mathcal{R}/\langle\gamma\rangle|^{\sum_{i=0}^{e-1}(e-i)\deg(\hat{g}_i)}.$$

By Corollary 2.3, $|C| = |S|$ and S is a minimal generating set. □

3 Linear codes over $\mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$

Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be finite chain rings where γ_1 and γ_2 are generators of the maximal ideals of $\mathcal{R}_1$ and $\mathcal{R}_2$ with nilpotency indices e_1 and e_2, respectively. We will suppose that $\mathcal{R}_1$ and $\mathcal{R}_2$ have the same residue field $K = \mathcal{R}_1/\langle\gamma_1\rangle = \mathcal{R}_2/\langle\gamma_2\rangle$, with $|K| = q = p^m$. By $\bar{}: \mathcal{R}_i \to K$, we will denote the natural projection that maps $r \mapsto \bar{r} = r + \langle\gamma_i\rangle$, for $i = 1$ or 2.

Let $T_1 = \{r_0, \ldots, r_{q-1}\}$ and $T_2 = \{r'_0, \ldots, r'_{q-1}\}$ be the Teichmüller sets of representatives of $\mathcal{R}_1$ and $\mathcal{R}_2$, resp., then we can arrange the subscripts such that $\bar{r}_i = \bar{r'}_i$. Assume that $e_1 \leq e_2$. Then we can consider the surjective ring homomorphism

$$\begin{array}{rccc} \pi: & \mathcal{R}_2 & \to & \mathcal{R}_1 \\ & \gamma_2 & \mapsto & \gamma_1 \\ & r'_j & \mapsto & r_j. \end{array}$$

 ISBN: 978-84-608-6082-2

Note that $\pi({\gamma_2}^i) = 0$ if $i \geq e_1$. For $a \in \mathcal{R}_2$ and $b \in \mathcal{R}_1$, define a multiplication $*$ as follows: $a * b = \pi(a)b$. Then, $\mathcal{R}_1$ is an $\mathcal{R}_2$-module with external multiplication $*$ given by π. Since $\mathcal{R}_1$ is commutative then $*$ has the commutative property. Then, we can generalize this multiplication over the ring $\mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$ as follows. Let a be an element of $\mathcal{R}_2$ and $\mathbf{u} = (u \mid u') = (u_0, u_1, \ldots, u_{\alpha-1} \mid u'_0, u'_1, \ldots, u'_{\beta-1}) \in \mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$. Then,

$$a{*}\mathbf{u} = (\pi(a)u_0, \pi(a)u_1, \ldots, \pi(a)u_{\alpha-1} \mid au'_0, au'_1, \ldots, au'_{\beta-1}).$$

With this external operation the ring $\mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$ is also an $\mathcal{R}_2$-module.

Definition 3.1. *A subset $\mathcal{C} \subseteq \mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$ is a linear code if it is a submodule of $\mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$.*

The next result gives the structure of a generator matrix of a linear code.

Proposition 3.2. *Let $\mathcal{C}$ be a linear code over $\mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$. Then $\mathcal{C}$ is permutation equivalent to a code with generator matrix of the form*

$$G = \left(\begin{array}{c|c} B & T \\ S & A \end{array}\right),$$

where

$$B = \begin{pmatrix} I_{k_0} & B_{0,1} & B_{0,2} & B_{0,3} & \cdots & B_{0,e_1-1} & B_{0,e_1} \\ 0 & \gamma_1 I_{k_1} & \gamma_1 B_{1,2} & \gamma_1 B_{1,3} & \cdots & \gamma_1 B_{1,e_1-1} & \gamma_1 B_{1,e_1} \\ 0 & 0 & \gamma_1^2 I_{k_2} & \gamma_1^2 B_{2,3} & \cdots & \gamma_1^2 B_{2,e_1-1} & \gamma_1^2 B_{2,e_1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \gamma_1^{e_1-1} I_{k_{e_1-1}} & \gamma_1^{e_1-1} B_{e_1-1,e_1} \end{pmatrix},$$

$$T = \begin{pmatrix} 0 \cdots & \gamma_2^{e_2-e_1} T_{0,1} & \gamma_2^{e_2-e_1} T_{0,2} & \cdots & \gamma_2^{e_2-e_1} T_{0,e_1} \\ 0 \cdots & 0 & \gamma_2^{e_2-e_1+1} T_{1,2} & \cdots & \gamma_2^{e_2-e_1+1} T_{1,e_1} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 \cdots & 0 & 0 & \cdots & \gamma_2^{e_2-1} T_{e_1-1,e_1} \end{pmatrix},$$

$$A = \begin{pmatrix} I_{l_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & A_{0,e_1-1} & A_{0,e_2} \\ 0 & \gamma_2 I_{l_1} & \gamma_2 A_{1,2} & \gamma_2 A_{1,3} & \cdots & \gamma_2 A_{1,e_2-1} & \gamma_2 A_{1,e_2} \\ 0 & 0 & \gamma_2^2 I_{l_2} & \gamma_2^2 A_{2,3} & \cdots & \gamma_2^2 A_{2,e_2-1} & \gamma_2^2 A_{2,e_2} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \gamma_2^{e_2-1} I_{l_{e_2-1}} & \gamma_2^{e_2-1} A_{e_2-1,e_2} \end{pmatrix},$$

$$S = \begin{pmatrix} 0 & S_{0,1} & S_{0,2} & \cdots & S_{0,e_1-1} & S_{0,e_1} \\ 0 & S_{1,1} & S_{1,2} & \cdots & S_{1,e_1-1} & S_{1,e_1} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & S_{e_2-e_1-1,1} & S_{e_2-e_1-1,2} & \cdots & S_{e_2-e_1-1,e_1-1} & S_{e_2-e_1-1,e_1} \\ 0 & 0 & \gamma_1 S_{e_2-e_1,2} & \cdots & \gamma_1 S_{e_2-e_1,e_1-1} & \gamma_1 S_{e_2-e_1,e_1} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \gamma_1^{e_1-2} S_{e_2-3,e_1-1} & \gamma_1^{e_1-3} S_{e_2-2,e_1} \\ 0 & 0 & 0 & \cdots & 0 & \gamma_1^{e_1-1} S_{e_2-2,e_1} \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

where the entries in $\gamma_1^i B_{i,j}$ and $\gamma_1^i S_{i,j}$ are in $\langle \gamma_1^i \rangle$ and the ones in $\gamma_2^t A_{t,j}$ and $\gamma_2^t T_{t,j}$ are in $\langle \gamma_2^t \rangle$.

 ISBN: 978-84-608-6082-2

Proof. Similiar to [2, Theorem 4] □

Let $\mathcal{C}_X$ be the canonical projection of $\mathcal{C}$ on the first α coordinates and $\mathcal{C}_Y$ on the last β coordinates. The canonical projection is a linear map. Then, $\mathcal{C}_X$ and $\mathcal{C}_Y$ are $\mathcal{R}_1$ and $\mathcal{R}_2$ linear codes of length α and β, respectively. A code $\mathcal{C}$ is called *separable* if $\mathcal{C}$ is the direct product of $\mathcal{C}_X$ and $\mathcal{C}_Y$, i.e., $\mathcal{C} = \mathcal{C}_X \times \mathcal{C}_Y$. Moreover, if $\mathcal{C}$ is separable then

$$G = \left(\begin{array}{c|c} B & 0 \\ 0 & A \end{array}\right).$$

Example 1. *Let $\mathcal{C}$ be a linear code over $\mathbb{Z}_2^3 \times \left(\frac{\mathbb{Z}_2[u]}{\langle u^3\rangle}\right)^4$ generated by the matrix*

$$\left(\begin{array}{ccc|cccc} 1 & 1 & 0 & u & u+u^2 & 1+u & 1+u^2 \\ 0 & 1 & 0 & 1 & u & u^2 & 0 \\ 0 & 1 & 1 & 0 & u^2 & 0 & u^2 \\ 1 & 1 & 1 & u^2 & u & u+u^2 & 0 \end{array}\right).$$

Hence, as described in Theorem 3.2, $\mathcal{C}$ is permutation equivalent to a code generated by the following matrix:

$$G = \left(\begin{array}{ccc|cccc} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & 0 & 0 & u \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & u & u+u^2 \end{array}\right).$$

Note that $\mathcal{C}$ is not separable.

4 Cyclic codes over $\mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$

Definition 4.1. *Let $\mathcal{C}$ be a linear code over $\mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$. The code $\mathcal{C}$ is called* cyclic *if*

$$(u_0, u_1, \ldots, u_{\alpha-2}, u_{\alpha-1} \mid u'_0, u'_1, \ldots, u'_{\beta-2}, u'_{\beta-1}) \in \mathcal{C}$$

implies

$$(u_{\alpha-1}, u_0, u_1, \ldots, u_{\alpha-2} \mid u'_{\beta-1}, u'_0, u'_1, \ldots, u'_{\beta-2}) \in \mathcal{C}.$$

Let $\mathbf{u} = (u_0, u_1, \ldots, u_{\alpha-1} \mid u'_0, \ldots, u'_{\beta-1})$ be a codeword in $\mathcal{C}$ and let i be an integer. We then denote by $\mathbf{u}^{(i)} = (u_{0+i}, u_{1+i}, \ldots, u_{\alpha-1+i} \mid u'_{0+i}, \ldots, u'_{\beta-1+i})$ the ith shift of $\mathbf{u}$, where the subscripts are read modulo α and β, respectively.

We remark that in this paper the definition of a cyclic code over $\mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$ is clear as long as $\mathcal{R}_1$ and $\mathcal{R}_2$ are different rings, since the elements on the first α coordinates and the ones in the last β coordinates belong from different rings, $\mathcal{R}_1$ and $\mathcal{R}_2$, respectively. In the

 ISBN: 978-84-608-6082-2

particular case that $\mathcal{R}_1 = \mathcal{R}_2$, the cyclic code over $\mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$ is known in the literature as *double cyclic code*, see [4], [7]. The term double cyclic is given in order to distinguish the cyclic code over $\mathcal{R}_1^\alpha \times \mathcal{R}_1^\beta$ from the cyclic code over $\mathcal{R}_1^{\alpha+\beta}$.

Note that $\mathcal{C}_X$ and $\mathcal{C}_Y$ are $\mathcal{R}_1$ and $\mathcal{R}_2$ cyclic codes of length α and β, respectively.

Denote by $\mathcal{R}_{\alpha,\beta}$ the ring $\mathcal{R}_1[x]/(x^\alpha - 1) \times \mathcal{R}_2[x]/(x^\beta - 1)$. There is a bijective map between $\mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$ and $\mathcal{R}_{\alpha,\beta}$ where $\mathbf{u} = (u_0, u_1, \ldots, u_{\alpha-1} \mid u'_0, \ldots, u'_{\beta-1})$ maps to $\mathbf{u}(x) = (u_0 + u_1 x + \cdots + u_{\alpha-1}x^{\alpha-1} \mid u'_0 + \cdots + u'_{\beta-1}x^{\beta-1})$.

Note that we can extend the map π to the polynomial ring $\mathcal{R}_2[x]$ applying this map to each of the coefficients of a given polynomial.

Definition 4.2. *Define the operation* $* : \mathcal{R}_2[x] \times \mathcal{R}_{\alpha,\beta} \to \mathcal{R}_{\alpha,\beta}$ *as*

$$\lambda(x) * (p(x) \mid q(x)) = (\pi(\lambda(x))p(x) \mid \lambda(x)q(x)),$$

where $\lambda(x) \in \mathcal{R}_2[x]$ *and* $(p(x) \mid q(x)) \in \mathcal{R}_{\alpha,\beta}$.

The ring $\mathcal{R}_{\alpha,\beta}$ with the external operation $*$ is a $\mathcal{R}_2[x]$-module. Let $\mathbf{u}(x) = (u(x) \mid u'(x))$ be an element of $\mathcal{R}_{\alpha,\beta}$. Note that if we operate $\mathbf{u}(x)$ by x we get

$$\begin{aligned} x * \mathbf{u}(x) = x * (u(x) \mid u'(x)) &= (u_0 x + \cdots + u_{\alpha-1}x^\alpha \mid u'_0 x + \cdots + u'_{\beta-1}x^\beta) \\ &= (u_{\alpha-1} + \cdots + u_{\alpha-2}x^{\alpha-1} \mid u'_{\beta-1} + \cdots + u'_{\beta-2}x^{\beta-1}). \end{aligned}$$

Hence, $x * \mathbf{u}(x)$ is the image of the vector $\mathbf{u}^{(1)}$. Thus, the operation of $\mathbf{u}(x)$ by x in $R_{\alpha,\beta}$ corresponds to a shift of $\mathbf{u}$. In general, $x^i * \mathbf{u}(x) = \mathbf{u}^{(i)}(x)$ for all i.

4.1 Algebraic structure and generators of cyclic codes

In this subsection, we study submodules of $\mathcal{R}_{\alpha,\beta}$. We describe the generators of such submodules and state some properties. From now on, $\langle S \rangle$ will denote the $\mathcal{R}_2[x]$-submodule generated by a subset S of $\mathcal{R}_{\alpha,\beta}$.

For the rest of the discussion we will consider that α and β are coprime integers with p. From this assumption, we know that $\mathcal{R}_1[x]/\langle x^\alpha - 1\rangle$ and $\mathcal{R}_2[x]/\langle x^\beta - 1\rangle$ are principal ideal rings, see [6].

Theorem 4.3. *Every submodule* $\mathcal{C}$ *of the* $\mathcal{R}_2[x]$*-module* $\mathcal{R}_{\alpha,\beta}$ *can be written as*

$$\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle,$$

where $b(x), a(x)$ *are generator polynomials in* $\mathcal{R}_1[x]/(x^\alpha - 1)$ *and* $\mathcal{R}_2[x]/(x^\beta - 1)$ *resp., and* $\ell(x) \in \mathcal{R}_1[x]/(x^\alpha - 1)$.

 ISBN: 978-84-608-6082-2

Proof. Let $\psi_X : \mathcal{R}_{\alpha,\beta} \to \mathcal{R}_1[x]/(x^\alpha - 1)$ and $\psi_Y : \mathcal{R}_{\alpha,\beta} \to \mathcal{R}_2[x]/(x^\beta - 1)$ be the canonical projections, let $\mathcal{C}$ be a submodule of $\mathcal{R}_{\alpha,\beta}$.
Define $\mathcal{C}' = \{(p(x)|q(x)) \in \mathcal{C} \mid q(x) = 0\}$. It is easy to check that $\mathcal{C}' \cong \psi_X(\mathcal{C}')$ by $(p(x) \mid 0) \mapsto p(x)$. Hence, by Theorem 2.4, $\psi_X(\mathcal{C}')$ is finitely generated by one element and so is $\mathcal{C}'$. Let $b(x)$ be a generator of $\psi_X(\mathcal{C}')$, then $(b(x) \mid 0)$ is a generator of $\mathcal{C}'$.
As $\mathcal{R}_2[x]/(x^\beta - 1)$ is also a principal ideal ring, then $\mathcal{C}_Y = \psi_Y(\mathcal{C})$ is generated by one element. Let $a(x) \in \mathcal{C}_Y$ such that $\mathcal{C}_Y = \langle a(x) \rangle$, then there exists $\ell(x) \in \mathcal{R}_1[x]/(x^\alpha - 1)$ such that $(\ell(x) \mid a(x)) \in \mathcal{C}$.
We claim that

$$\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle.$$

Let $(p(x) \mid q(x)) \in \mathcal{C}$, then $q(x) = \psi_Y(p(x) \mid q(x)) \in \mathcal{C}_Y$. So, there exists $\lambda(x) \in \mathcal{R}_2[x]$ such that $q(x) = \lambda(x)a(x)$. Now,

$$(p(x) \mid q(x)) - \lambda(x) * (\ell(x) \mid a(x)) = (p(x) - \pi(\lambda(x))\ell(x) \mid 0)$$

belongs to $\mathcal{C}'$. Then, there exists $\mu(x) \in \mathcal{R}_2[x]$ such that $(p(x) - \pi(\lambda(x))\ell(x) \mid 0) = \mu(x) * (b(x) \mid 0)$. Thus,

$$(p(x) \mid q(x)) = \mu(x) * (b(x) \mid 0) + \lambda(x) * (\ell(x) \mid a(x)).$$

So, $\mathcal{C}$ is finitely generated by $\langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$. □

From the previous results, it is clear that we can identify double cyclic codes in $\mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$ as submodules of $\mathcal{R}_{\alpha,\beta}$. So, any submodule of $\mathcal{R}_{\alpha,\beta}$ is a cyclic code. From now on, we will denote by $\mathcal{C}$ indistinctly both the code and the corresponding submodule of $\mathcal{R}_{\alpha,\beta}$.

In the following, a polynomial $f(x)$ in $\mathcal{R}_1[x]$ or $\mathcal{R}_2[x]$ will be denoted simply by f.

Proposition 4.4. *Let $\mathcal{C}$ be a cyclic code over $\mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$. Then, there exist polynomials ℓ and $b_{e_1-1}|b_{e_1-2}|\dots|b_1|b_0|(x^\alpha - 1)$ over $\mathcal{R}_1[x]$ and $a_{e_2-1}|a_{e_2-2}|\dots|a_1|a_0|(x^\beta - 1)$ over $\mathcal{R}_2[x]$ such that*

$$\mathcal{C} = \langle (b_0 + \gamma_1 b_1 + \dots + {\gamma_1}^{e_1-1} b_{e_1-1} \mid 0), (\ell \mid a_0 + \gamma_2 a_1 + \dots + {\gamma_2}^{e_2-1} a_{e_2-1}) \rangle.$$

Proof. Let $\mathcal{C}$ be a cyclic code over $\mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$. By Theorem 4.3, there exist polynomials $b, \ell \in \mathcal{R}_1[x]/(x^\alpha - 1)$ and $a \in \mathcal{R}_2[x]/(x^\beta - 1)$ such that $\mathcal{C} = \langle (b \mid 0), (\ell \mid a) \rangle$. By Theorem 2.4, one can consider $b = b_0 + \gamma_1 b_1 + \dots + {\gamma_1}^{e_1-1} b_{e_1-1}$ and $a = a_0 + \gamma_2 a_1 + \dots + {\gamma_2}^{e_2-1} a_{e_2-1}$ such that $b_{e_1-1}|b_{e_1-2}|\dots|b_1|b_0|(x^\alpha - 1)$ and $a_{e_2-1}|a_{e_2-2}|\dots|a_1|a_0|(x^\beta - 1)$. □

For the rest of the discussion, any cyclic code $\mathcal{C}$ over $\mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$ is of the form $\mathcal{C} = \langle (b \mid 0), (\ell \mid a) \rangle$, where $b = b_0 + \gamma_1 b_1 + \dots + {\gamma_1}^{e_1-1} b_{e_1-1}$ and $a(x) = a_0 + \gamma_2 a_1 + \dots + {\gamma_2}^{e_2-1} a_{e_2-1}$, for polynomials b_i and a_j as in Proposition 4.4.

 ISBN: 978-84-608-6082-2

Example 2. *Let* $\mathcal{R}_1 = \frac{\mathbb{F}_9[u]}{\langle u^2\rangle}$ *and* $\mathcal{R}_2 = \frac{\mathbb{F}_9[u]}{\langle u^3\rangle}$, *with* $\gamma_1 = u$, $e_1 = 2$, $\gamma_2 = u$, *and* $e_2 = 3$. *Let* ξ *be a generator of the multiplicative group* $\mathbb{F}_9^*$. *Consider the cyclic code over* $\left(\frac{\mathbb{F}_9[u]}{\langle u^2\rangle}\right)^4 \times \left(\frac{\mathbb{F}_9[u]}{\langle u^3\rangle}\right)^{10}$ *generated by*

$$\mathcal{C} = \langle (u(x^2-1) \mid 0), (u \mid (x^4 + \xi^3 x^2 + 1) + u(x^2 + \xi^5 x + 1) + u^2)\rangle.$$

Then,

$$b_0 = x^4 - 1, \quad b_1 = x^2 - 1, \quad \ell = u, a_0 = x^4 + \xi^3 x^2 + 1, \quad a_1 = x^2 + \xi^5 x + 1, \quad a_2 = 1.$$

4.2 Minimal generating sets

Our goal is to find a set generators for a cyclic code, $\mathcal{C}$, as an $\mathcal{R}_2$-module. Once we found it, we are going to use it to determine the size of $\mathcal{C}$ in terms of the generator polynomials.

Since b_0 is a factor of $x^\alpha - 1$ and for $i = 1 \dots e_1 - 1$ the polynomial b_i is a factor of b_{i-1}, we will denote $\hat{b}_0 = \frac{x^\alpha - 1}{b_0}$, $\hat{b}_i = \frac{b_{i-1}}{b_i}$ for $i = 1 \dots e_1 - 1$, and $\hat{b}_{e_1} = b_{e_1 - 1}$. In the same way, we define $\hat{a}_0 = \frac{x^\beta - 1}{a_0}$, $\hat{a}_j = \frac{a_{j-1}}{a_j}$ for $j = 1 \dots e_2 - 1$, and $\hat{a}_{e_2} = a_{e_2 - 1}$.

Theorem 4.5. *Let* $\mathcal{C}$ *be a cyclic code over* $\mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$ *which has maximals ideals* $\langle \gamma_1 \rangle \subset \mathcal{R}_1$ *and* $\langle \gamma_2 \rangle \subset \mathcal{R}_2$ *with nilpotent indices* e_1 *and* e_2, *respectively. Define*

$$B_j = \left[x^i \Big(\prod_{t=0}^{j-1} \hat{b}_t \Big) * (b \mid 0) \right]_{i=0}^{\deg(\hat{b}_j) - 1},$$

for $0 \le j < e_1$, *and*

$$A_k = \left[x^i \Big(\prod_{t=0}^{k-1} \hat{a}_t \Big) * (\ell \mid a) \right]_{i=0}^{\deg(\hat{a}_k) - 1}.$$

for $0 \le k < e_2$. *Then,*

$$S = \left(\bigcup_{j=0}^{e_1 - 1} B_j \right) \bigcup \left(\bigcup_{k=0}^{e_2 - 1} A_k \right)$$

forms a minimal generating set for $\mathcal{C}$ *as an* $\mathcal{R}_2$*-module. Moreover,*

$$|\mathcal{C}| = q^{\sum_{i=0}^{e_1 - 1} (e_1 - i) \deg(\hat{b}_i) + \sum_{j=0}^{e_2 - 1} (e_2 - j) \deg \hat{a}_j},$$

where q *is the cardinality of the residue field.*

 ISBN: 978-84-608-6082-2

Proof. By Theorem 2.5, it is clear that the elements in S are $\mathcal{R}_2$-lineal independent since $\left(\bigcup_{j=0}^{e_1-1} B_j\right)_X$ and $\left(\bigcup_{k=0}^{e_2-1} A_k\right)_Y$ are minimal generating sets for the codes $\mathcal{C}_X$ and $\mathcal{C}_Y$, respectively. Let c be a codeword of $\mathcal{C}$, then $c = q*(b \mid 0) + d*(\ell \mid a)$. Reasoning similarly as in Theorem 2.5, we have that $q*(b \mid 0) \in \langle \bigcup_{j=0}^{e_1-1} B_j \rangle_{\mathcal{R}_2}$. So, we have to prove that $d*(\ell \mid a) \in \langle S \rangle_{\mathcal{R}_2}$.

If $\deg(d) < \deg(\hat{a}_0)$ then $d*(\ell \mid a) \in \langle A_0 \rangle_{\mathcal{R}_2}$ and $c \in \langle S \rangle_{\mathcal{R}_2}$. Otherwise, compute $d = d_0\hat{a}_0 + r_0$ with $\deg(r_0) < \deg(\hat{a}_0)$, so $d*(\ell \mid a) = d_0\hat{a}_0 * (\ell \mid a) + r_0 * (\ell \mid a)$ and $r_0 * (\ell \mid a) \in \langle A_0 \rangle_{\mathcal{R}_2}$.

In the worst case and reasoning similarly, one obtains that $c \in \langle S \rangle_{\mathcal{R}_2}$ if $d_{e_2-2}(\prod_{t=0}^{e_2-2} \hat{a}_t) * (\ell \mid a) \in \langle S \rangle_{\mathcal{R}_2}$. It is obvious that if $\deg(d_{e_2-2}) < \deg(\hat{a}_{e_2-1})$ then $d_{e_2-2}(\prod_{t=0}^{e_2-2} \hat{a}_t) * (\ell \mid a) \in \langle A_{e_2-1} \rangle_{\mathcal{R}_2}$, if not $d_{e_2-2} = d_{e_2-1}\hat{a}_{e_2-1} + r_{e_2-1}$. Therefore,

$$d_{e_2-2}\left(\prod_{t=0}^{e_2-2} \hat{a}_t\right) * (\ell \mid a) = d_{e_2-1}\left(\prod_{t=0}^{e_2-1} \hat{a}_t\right) * (\ell \mid a) + r_{e_2-1}\left(\prod_{t=0}^{e_2-2} \hat{a}_t\right) * (\ell \mid a).$$

On one hand, $r_{e_2-1}(\prod_{t=0}^{e_2-2} \hat{a}_t) * (\ell \mid a) \in \langle A_{e_2-1} \rangle_{\mathcal{R}_2}$. On the other hand, $d_{e_2-1}(\prod_{t=0}^{e_2-1} \hat{a}_t) * (\ell \mid a) = d_{e_2-1}(\prod_{t=0}^{e_2-1} \hat{a}_t) * (\ell \mid 0)$ and then $d_{e_2-1}(\prod_{t=0}^{e_2-1} \hat{a}_t) * (\ell \mid a) = f * (b \mid 0) \in \langle \bigcup_{j=0}^{e_1-1} B_j \rangle_{\mathcal{R}_2}$. Thus, $c \in \langle S \rangle_{\mathcal{R}_2}$ and S is a minimal generating set for $\mathcal{C}$. □

Example 3. *Consider* $\mathcal{R}_{\alpha,\beta} = \mathbb{Z}_2[x]/(x^2-1) \times \mathbb{Z}_4[x]/(x^3-1)$ *and the cyclic code*

$$\mathcal{C} = \langle (x-1 \mid (x^2+x+1)+2) \rangle,$$

where $b_0(x) = x^2-1$, $\ell(x) = x-1$, $a_0(x) = x^2+x+1$ *and* $a_1(x) = 1$. *Then,* $S = \{(x-1 \mid x^2+x+3), (0 \mid 2x+2), (0 \mid 2x^2+2x)\}$ *and*

$$|\mathcal{C}| = 2^{\sum_{j=0}^{2-1}(2-j)deg(\hat{a}_j)} = 2^4 = 16.$$

Example 4. *From Example 2, consider the cyclic code over* $\left(\frac{\mathbb{F}_9[u]}{\langle u^2 \rangle}\right)^4 \times \left(\frac{\mathbb{F}_9[u]}{\langle u^3 \rangle}\right)^{10}$ *generated by*

$$\mathcal{C} = \langle (u(x^2-1) \mid 0), (u \mid (x^4+\xi^3x^2+1) + u(x^2+\xi^7x+1) + u^2) \rangle.$$

Let $b = u(x^2-1), \ell = u$ *and* $a = (x^4+\xi^3x^2+1) + u(x^2+\xi^7x+1) + u^2$. *Then, a minimal generating set for* $\mathcal{C}$ *is the union of*

$$B_0 = \emptyset,\ B_1 = \left[x^i * (u(x^2-1) \mid 0)\right]_{i=0}^{1},$$

$$A_0 = \left[x^i * (\ell \mid a)\right]_{i=0}^{5},\ A_1 = \left[x^i\mu * (\ell \mid a)\right]_{i=0}^{1},$$

and

$$A_2 = \left[x^i\lambda * (\ell \mid a)\right]_{i=0}^{1},$$

where $\mu = x^6 + \xi^7x^4 + \xi^3x^2 + 2$ *and* $\lambda = x^8 + \xi x^7 + \xi x^6 + x^5 + 2x^3 + \xi^5x^2 + \xi^5x + 2$. *So,*

$$|\mathcal{C}| = 9^{\sum_{i=0}^{2-1}(2-i)deg(\hat{b}_i) + \sum_{j=0}^{3-1}(3-j)deg(\hat{a}_j)} = 9^{2+24} = 9^{26}.$$

 ISBN: 978-84-608-6082-2

Acknowledgements

This work has been partially supported by the Spanish MINECO grants TIN2013-40524-P and MTM2015-69138-REDT, and by the Catalan AGAUR grant 2014SGR-691.

References

[1] T. Abualrub, I. Siap, N. Aydin, $\mathbb{Z}_2\mathbb{Z}_4$-*additive cyclic codes*, IEEE Trans. Info. Theory **60(3)** (2014) 1508–1514.

[2] I. Aydogdu, I. Siap, *On* $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$*-additive codes*, Linear and Multilinear Algebra **63(10)** (2014) 2089–2102.

[3] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà and M. Villanueva, $\mathbb{Z}_2\mathbb{Z}_4$*-linear codes: generator matrices and duality*, Des., Codes and Crypto. **54(2)** (2010) 167–179.

[4] J. Borges, C. Fernández-Córdoba, R. Ten-Valls, $\mathbb{Z}_2$*-double cyclic codes*, arXiv:1410.5604.

[5] J. Borges, C. Fernández-Córdoba, R. Ten-Valls, $\mathbb{Z}_2\mathbb{Z}_4$*-additive cyclic codes, generator polynomials and dual codes*, arXiv:1406.4425.

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

[7] J. Gao, M. Shi, T. Wu and F. Fu, *On double cyclic codes over* $\mathbb{Z}_4$, Finite Fields and Their Applications **39** (2016) 233–250.

[8] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *The* $\mathbb{Z}_4$*-Linearity of Kerdock, Preparata, Goethals, and Related Codes*, IEEE Trans. Info. Theory **40(2)** (1994) 301–319.

[9] G. Norton, A. Salagean, *On the structure of linear and cyclic codes over finite chain rings* Appl. Algebra Eng. Commun. Comput. **10** (2000) 489–506.

 ISBN: 978-84-608-6082-2