This is a pre-copy-editing, author-produced PDF of an article accepted for publication in Advances in mathematics of communications following peer review. The definitive publisher-authenticated version of Borges, J., Fernández-Córdoba, C. and Ten-Valls, *R. "*On Zpr Zps-additive cyclic codes*"* in *Advances in mathematics of communications,* vol. 12, issue 1 (2018), p. 169-179 *is available online at: DOI 10.3934/amc.2018011*

On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes

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

September 12, 2016

Abstract

A $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code, with $r \leq s$, is a $\mathbb{Z}_{p^s}$-submodule of $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$. We introduce $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes. These codes can be seen as $\mathbb{Z}_{p^s}[x]$-submodules of $\mathcal{R}_{r,s}^{\alpha,\beta} = \frac{\mathbb{Z}_{p^r}[x]}{\langle x^{\alpha}-1\rangle} \times \frac{\mathbb{Z}_{p^s}[x]}{\langle x^{\beta}-1\rangle}$. We determine the generator polynomials of a code over $\mathcal{R}_{r,s}^{\alpha,\beta}$ and a minimal spanning set over $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ in terms of the generator polynomials. We also study the duality in the module $\mathcal{R}_{r,s}^{\alpha,\beta}$. Our results generalise those for $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes.

Key Words: Additive codes, codes over rings, cyclic codes, duality.

1 Introduction

$\mathbb{Z}_2\mathbb{Z}_4$-additive codes have been introduced in [4] and intensely studied during last years. The set of coordinates of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code can be partitioned into two subsets, the set of coordinates over $\mathbb{Z}_2$ and the set of coordinates over $\mathbb{Z}_4$. In recent times, $\mathbb{Z}_2\mathbb{Z}_4$-additive codes were generalized to $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes in [2], and later to $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes, in [3]. In [2] and [3], the authors determine, in particular, the standard forms of generator and parity-check matrices and present some bounds on the minimum distance.

One of the most studied class of codes is the class of cyclic codes. For example, the algebraic structure and the generators of cyclic codes over $\mathbb{Z}_{p^m}$ have been studied in [7] and [10]. Newly, the concept of double cyclic codes over rings appeared in the literature. A double cyclic code is a code such that the set of coordinates can be partitioned into two subsets such that any cyclic shift of the coordinates of both subsets leaves invariant the code. Notice that if one of these sets of coordinates is empty then we obtain a cyclic code. We can find examples of double cyclic codes over the rings $\mathbb{Z}_2$ and $\mathbb{Z}_4$ in [5] and [9],

*Manuscript received Month day, year; revised Month day, year.

†J. Borges is with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (e-mail: joaquim.borges@uab.cat).

‡C. Fernández-Córdoba is with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (e-mail: cristina.fernandez@uab.cat).

§R. Ten-Valls is with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (e-mail: roger.ten@uab.cat).

¶This work has been partially supported by the Spanish MINECO grant TIN2013-40524-P and by the Catalan AGAUR grant 2014SGR-691.

respectively. Also, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes have been defined in [1]. These codes have the property that a simultaneous cyclic shift of the coordinates over $\mathbb{Z}_2$ and the coordinates over $\mathbb{Z}_4$ of a codeword is also a codeword. A $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code is identified as a $\mathbb{Z}_4[x]$-module of a certain ring. The duality of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes has been studied in [6].

After all these papers, it becomes natural the study of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes. On the one hand, as the study of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes, presented in [3], with the cyclic property. And, on the other hand, as a generalization of the different types of cyclic codes studied in [1, 5, 6, 9, 7, 10].

The aim of this paper is the study of the algebraic structure of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes. We will assume that $r \leq s$. As $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes can be identified as $\mathbb{Z}_{p^s}[x]$-submodules of $\frac{\mathbb{Z}_{p^r}[x]}{\langle x^\alpha - 1\rangle} \times \frac{\mathbb{Z}_{p^s}[x]}{\langle x^\beta - 1\rangle}$ then, Section 2 reviews cyclic codes over $\mathbb{Z}_{p^m}$ and details a minimal generating set of a cyclic code over $\mathbb{Z}_{p^m}$ as a $\mathbb{Z}_{p^m}$-module. In Section 3, we recall definitions and basic results of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes, defined in [3]. In Section 4, we give the definition of a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code, we discuss the algebraic structure of these codes, we determine the generator polynomials of a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code, and we describe a minimal generating set for the code as a $\mathbb{Z}_{p^s}$-module in terms of the generator polynomials. Finally, in Section 5, we study the duality of these codes over the $\mathbb{Z}_{p^s}[x]$-module $\frac{\mathbb{Z}_{p^r}[x]}{\langle x^\alpha - 1\rangle} \times \frac{\mathbb{Z}_{p^s}[x]}{\langle x^\beta - 1\rangle}$.

2 Cyclic codes over $\mathbb{Z}_{p^m}$

Let p be a prime number and let $\mathbb{Z}_{p^m}$ be the ring of integers modulo p^m. A linear code of length n over $\mathbb{Z}_{p^m}$ is a submodule of $\mathbb{Z}_{p^m}^n$, and a cyclic code of length n over $\mathbb{Z}_{p^m}$ is a linear code with the property that if $(c_0, \cdots, c_{n-2}, c_{n-1})$ is a codeword then $(c_{n-1}, c_0, \cdots, c_{n-2})$ is also a codeword.

Let $g_1, \ldots, g_r$ be polynomials in a $\mathbb{Z}_{p^m}[x]$-module. We denote by $\langle g_1, \ldots, g_r\rangle$ the $\mathbb{Z}_{p^m}[x]$-submodule, resp. $\langle g_1, \ldots, g_r\rangle_{\mathbb{Z}_{p^m}}$ the $\mathbb{Z}_{p^m}$-submodule, generated by $g_1, \ldots, g_r$.

Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{Z}_{p^m}$. We can identify $\mathcal{C}$ as an ideal of $\mathbb{Z}_{p^m}[x]/\langle x^n - 1\rangle$. 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 $\mathbb{Z}_{p^m}[x]$.

Theorem 2.1 ([8, Theorem 3.5])**.** *Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{Z}_{p^m}$. Then, there exist polynomials $g_0, g_1, \ldots, g_{m-1}$ in $\mathbb{Z}_{p^m}[x]$ such that $\mathcal{C} = \langle g_0, pg_1, \ldots, p^{m-1}g_{m-1}\rangle$ and $g_{m-1} \mid g_{m-2} \mid \cdots \mid g_1 \mid g_0 \mid (x^n - 1)$.*

Let $\mathcal{C} = \langle g_0, pg_1, \ldots, p^{m-1}g_{m-1}\rangle$ be a cyclic code of length n and let $g = g_0 + pg_1 + \cdots + p^{m-1}g_{m-1}$. Since g_0 is a factor of $x^n - 1$ and, for $i = 1 \ldots m-1$, the polynomial g_i is a factor of g_{i-1}, we may define the polynomials $\hat{g}_0 = \frac{x^n-1}{g_0}$ and $\hat{g}_i = \frac{g_{i-1}}{g_i}$ for $i = 1 \ldots m-1$. Define $G = \prod_{i=0}^{m-1} \hat{g}_i$. It is clear that $Gg = \left(\prod_{i=0}^{m-1} \hat{g}_i\right) g = 0$ over $\mathbb{Z}_{p^m}[x]/\langle x^n - 1\rangle$.

Lemma 2.2. *Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{Z}_{p^m}$. Let $g_0, g_1, \ldots, g_{m-1}$ in $\mathbb{Z}_{p^m}[x]$ such that $\mathcal{C} = \langle g_0, pg_1, \ldots, p^{m-1}g_{m-1}\rangle$ and $g_{m-1} \mid g_{m-2} \mid \cdots \mid g_1 \mid g_0 \mid (x^n - 1)$, and let $g = g_0 + pg_1 + \cdots + p^{m-1}g_{m-1}$. Then,*

1. $p^{m-1}g = p^{m-1}g_{m-1}\frac{G}{\hat{g}_0}$,

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

Proof. We have that

$$\begin{aligned} p^{m-1}g = & \quad p^{m-1}g_0\tfrac{1}{g_1}\tfrac{g_1}{g_2}\cdots\tfrac{g_{m-3}}{g_{m-2}}\tfrac{g_{m-2}}{g_{m-1}}g_{m-1} \\ = & \quad p^{m-1}g_{m-1}\hat{g}_1\hat{g}_2\cdots\hat{g}_{m-2}\hat{g}_{m-1} \\ = & \quad p^{m-1}g_{m-1}\frac{G}{\hat{g}_0}, \end{aligned}$$

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

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

and statement 2 is proved.

□

From Theorem 2.1, we get the following result.

Corollary 2.3. *Let* $\mathcal{C}$ *be a cyclic code of length* n *over* $\mathbb{Z}_{p^m}$ *such that* $\mathcal{C} = \langle g_0, pg_1, \ldots, p^{m-1}g_{m-1}\rangle$ *with* $g_{m-1} \mid g_{m-2} \mid \cdots \mid g_1 \mid g_0 \mid (x^n - 1)$. *Then,*

$$|\mathcal{C}| = p^{\sum_{i=0}^{m-1}(m-i)\deg(\hat{g}_i)}.$$

Proof. From the previous definition of $\hat{g}_i$, these polynomials are the same polynomials described in [8, Theorem 3.4]. □

In [7], it is proved that $\mathbb{Z}_{p^m}[x]/\langle x^n - 1\rangle$ is a principal ideal ring. Furthermore, they showed how are the generator polynomials of the ideals. Joining these results we obtain the following.

Theorem 2.4 ([7])**.** *Let* $\mathcal{C}$ *be a cyclic code of length* n *over* $\mathbb{Z}_{p^m}$. *Let* $g_0, g_1, \ldots, g_{m-1}$ *polynomials in* $\mathbb{Z}_{p^m}[x]$ *such that* $\mathcal{C} = \langle g_0, pg_1, \ldots, p^{m-1}g_{m-1}\rangle$ *and* $g_{m-1} \mid g_{m-2} \mid \cdots \mid g_1 \mid g_0 \mid (x^n - 1)$. *Then, the polynomial* $g = g_0 + pg_1 + \cdots + p^{m-1}g_{m-1}$ *is a generator polynomial of* $\mathcal{C}$, *i.e.,* $\mathcal{C} = \langle g\rangle$.

Theorem 2.5. *Let* $\mathcal{C} = \langle g\rangle = \langle g_0 + pg_1 + \cdots + p^{m-2}g_{m-2} + p^{m-1}g_{m-1}\rangle$ *be a cyclic code of length* n *over* $\mathbb{Z}_{p^m}$ *with* $g_{m-1} \mid g_{m-2} \mid \cdots \mid g_1 \mid g_0 \mid (x^n - 1)$. *We define the following sets*

$$S_0 = \left\{x^i g\right\}_{i=0}^{\deg(\hat{g}_0)} = \left\{x^i(g_0 + pg_1 + \cdots + p^{m-2}g_{m-2} + p^{m-1}g_{m-1})\right\}_{i=0}^{\deg(\hat{g}_0)},$$

$$S_1 = \left\{x^i\hat{g}_0 g\right\}_{i=0}^{\deg(\hat{g}_1)} = \left\{x^i(pg_1\hat{g}_0 + \cdots + p^{m-2}g_{m-2}\hat{g}_0 + p^{m-1}g_{m-1}\hat{g}_0)\right\}_{i=0}^{\deg(\hat{g}_1)},$$

$$\vdots$$

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

$$\vdots$$

$$S_{m-1} = \left\{ x^i (\prod_{t=0}^{m-2} \hat{g}_t) g \right\}_{i=0}^{\deg(\hat{g}_{m-1})} = \left\{ x^i (\prod_{t=0}^{m-2} \hat{g}_t) p^{m-1} g_{m-1} \right\}_{i=0}^{\deg(\hat{g}_{m-1})}.$$

Then,

$$S = \bigcup_{j=0}^{m-1} S_j$$

forms a minimal generating set for $\mathcal{C}$ as a $\mathbb{Z}_{p^m}$-module.

Proof. Let $c \in \mathcal{C}$. We have that $c = dg$ with $d \in \mathbb{Z}_{p^m}[x]$. If $\deg(d) < \deg(\hat{g}_0)$ then $dg \in \langle S_0 \rangle_{\mathbb{Z}_{p^m}}$ and $c \in \langle S \rangle_{\mathbb{Z}_{p^m}}$. 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 $r_0 g \in \langle S_0 \rangle_{\mathbb{Z}_{p^m}}$.

If $\deg(d_0) < \deg(\hat{g}_1)$, then $d_0 \hat{g}_0 g \in \langle S_1 \rangle_{\mathbb{Z}_{p^m}}$ and $c \in \langle S \rangle_{\mathbb{Z}_{p^m}}$. 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 $r_1 \hat{g}_0 g \in \langle S_1 \rangle_{\mathbb{Z}_{p^m}}$.

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

$$d_{m-2}(\prod_{t=0}^{m-2} \hat{g}_t) g = d_{m-1}(\prod_{t=0}^{m-1} \hat{g}_t) g + r_{m-1}(\prod_{t=0}^{m-2} \hat{g}_t) g = r_{m-1}(\prod_{t=0}^{m-2} \hat{g}_t) g \in \langle S_{m-1} \rangle_{\mathbb{Z}_{p^m}}.$$

Since $r_{m-1}(\prod_{t=0}^{m-2} \hat{g}_t) g \in \langle S_{m-1} \rangle_{\mathbb{Z}_{p^m}}$, we have that $c \in \langle S \rangle_{\mathbb{Z}_{p^m}}$, and hence S is a generating set. If one compute $|S|$ clearly

$$|S| = \sum_{i=0}^{m-1} (m-i) \deg(\hat{g}_i).$$

By Corollary 2.3, $|\mathcal{C}| = |\langle S \rangle|$ and S is a minimal generating set. □

3 $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes

Let $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$ be the rings of integers modulo p^r and p^s, respectively, with p prime and $r \leq s$. Since the residue field of both $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$ is $\mathbb{Z}_p$, an element b of $\mathbb{Z}_{p^r}$ could be written uniquely as $b = b_0 + pb_1 + p^2 b_2 + \cdots + p^{r-1} b_{r-1}$, and any element $a \in \mathbb{Z}_{p^s}$ as $a = a_0 + pa_1 + p^2 a_2 + \cdots + p^{s-1} a_{s-1}$, where $b_i, a_j \in \mathbb{Z}_p$. Then we can consider the surjective ring homomorphism

$$\begin{array}{rccl} \pi: & \mathbb{Z}_{p^s} & \twoheadrightarrow & \mathbb{Z}_{p^r} \\ & a & \mapsto & a \mod p^r. \end{array}$$

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

Definition 3.1. *A $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code $\mathcal{C}$ is a $\mathbb{Z}_{p^s}$-submodule of $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$.*

The structure of the generator matrix in standard form and the type of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes are defined and determined in [3].

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. Then, $\mathcal{C}_X$ and $\mathcal{C}_Y$ are $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$ 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., $\mathcal{C} = \mathcal{C}_X \times \mathcal{C}_Y$.

Since $r \leq s$, we consider the inclusion map

$$\begin{array}{rccc} \iota: & \mathbb{Z}_{p^r} & \hookrightarrow & \mathbb{Z}_{p^s} \\ & b & \mapsto & b \end{array}.$$

Let $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$, then the inner product is defined in [3] as

$$\mathbf{u} \cdot \mathbf{v} = p^{s-r} \sum_{i=0}^{\alpha-1} \iota(u_i v_i) + \sum_{j=0}^{\beta-1} u'_j v'_j \in \mathbb{Z}_{p^s},$$

and the dual code of a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code $\mathcal{C}$ is defined in a natural way as

$$\mathcal{C}^{\perp} = \{\mathbf{v} \in \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta} \mid \mathbf{u} \cdot \mathbf{v} = 0, \ \forall \mathbf{u} \in \mathcal{C}\}.$$

Let $\mathcal{C}$ be a separable code in $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$, then $\mathcal{C}^{\perp}$ is also separable and $\mathcal{C}^{\perp} = \mathcal{C}_X^{\perp} \times \mathcal{C}_Y^{\perp}$.

4 $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes

Definition 4.1. *Let $\mathcal{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code. 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 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. Note that if $\mathcal{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ is cyclic, then $\mathcal{C}_X$ (resp. $\mathcal{C}_Y$) is a cyclic code over $\mathbb{Z}_{p^r}^{\alpha}$ (resp. $\mathbb{Z}_{p^s}^{\beta}$).

We remark that in this paper the definition of a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code is well defined as long as $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$ are different rings, since the elements on the first α coordinates and the ones in the last β coordinates belong to different rings, $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$, respectively. In the particular case that $r = s$, the cyclic code in $\subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^r}^{\beta}$ is known in the literature as *double cyclic code*, see [5], [9]. The term double cyclic is given in order to distinguish the cyclic code in $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^r}^{\beta}$ from the cyclic code in $\mathbb{Z}_{p^r}^{\alpha+\beta}$.

Denote by $\mathcal{R}_{r,s}^{\alpha,\beta}$ the ring $\mathbb{Z}_{p^s}[x]/\langle x^{\alpha}-1\rangle \times \mathbb{Z}_{p^s}[x]/\langle x^{\beta}-1\rangle$. There is a bijective map between $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ and $\mathcal{R}_{r,s}^{\alpha,\beta}$ given by:

$$(u_0, u_1, \ldots, u_{\alpha-1} \mid u'_0, \ldots, u'_{\beta-1}) \mapsto (u_0 + u_1 x + \cdots + u_{\alpha-1} x^{\alpha-1} \mid u'_0 + \cdots + u'_{\beta-1} x^{\beta-1}).$$

We denote the image of the vector $\mathbf{u}$ by $\mathbf{u}(x)$. Note that we can extend the maps ι and π to the polynomial rings $\mathbb{Z}_{p^r}[x]$ and $\mathbb{Z}_{p^s}[x]$ applying these maps to each of the coefficients of a given polynomial.

Definition 4.2. *Define the operation* $* : \mathbb{Z}_{p^s}[x] \times \mathcal{R}_{r,s}^{\alpha,\beta} \to \mathcal{R}_{r,s}^{\alpha,\beta}$ *as*

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

where $\lambda(x) \in \mathbb{Z}_{p^s}[x]$ *and* $(t(x) \mid q(x)) \in \mathcal{R}_{r,s}^{\alpha,\beta}$.

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

$$\begin{aligned} x * \mathbf{u}(x) &= x * (u(x) \mid u'(x)) \\ &= (u_0x + \cdots + u_{\alpha-2}x^{\alpha-1} + u_{\alpha-1}x^{\alpha} \mid u'_0x + \cdots + u'_{\beta-2}x^{\beta-1} + u'_{\beta-1}x^{\beta}) \\ &= (u_{\alpha-1} + u_0x + \cdots + u_{\alpha-2}x^{\alpha-1} \mid u'_{\beta-1} + u'_0x + \cdots + u'_{\beta-2}x^{\beta-1}). \end{aligned}$$

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 section, we study submodules of $\mathcal{R}_{r,s}^{\alpha,\beta}$. We describe the generators of such submodules and state some properties. From now on, $\langle S \rangle$ will denote the $\mathbb{Z}_{p^s}[x]$-submodule generated by a subset S of $\mathcal{R}_{r,s}^{\alpha,\beta}$.

For the rest of the discussion we will consider that α and β are coprime integers with p. From this assumption, we know that $\mathbb{Z}_{p^r}[x]/(x^{\alpha}-1)$ and $\mathbb{Z}_{p^s}[x]/(x^{\beta}-1)$ are principal ideal rings, see [7], [8].

Theorem 4.3. *Every submodule* $\mathcal{C}$ *of the* $\mathbb{Z}_{p^s}[x]$*-module* $\mathcal{R}_{r,s}^{\alpha,\beta}$ *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* $\mathbb{Z}_{p^r}[x]/(x^{\alpha}-1)$ *and* $\mathbb{Z}_{p^s}[x]/(x^{\beta}-1)$ *resp., and* $\ell(x) \in \mathbb{Z}_{p^r}[x]/(x^{\alpha}-1)$.

Proof. Let $\psi_X : \mathcal{R}_{r,s}^{\alpha,\beta} \to \mathbb{Z}_{p^r}[x]/\langle x^{\alpha}-1 \rangle$ and $\psi_Y : \mathcal{R}_{r,s}^{\alpha,\beta} \to \mathbb{Z}_{p^s}[x]/\langle x^{\beta}-1 \rangle$ be the canonical projections, let $\mathcal{C}$ be a submodule of $\mathcal{R}_{r,s}^{\alpha,\beta}$. 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 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 $\mathbb{Z}_{p^s}[x]/\langle x^{\beta}-1 \rangle$ 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 $\ell(x) \in \mathbb{Z}_{p^r}[x]/\langle x^{\alpha}-1 \rangle$ 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 $\lambda(x) \in \mathbb{Z}_{p^s}[x]$ such that $q(x) = \lambda(x)a(x)$. Now,

$$(p(x) \mid q(x)) - \lambda(x) * (\ell(x) \mid a(x)) = (p(x) - \pi(\lambda(x))\ell(x) \mid 0) \in \mathcal{C}'.$$

Then, there exists $\mu(x) \in \mathbb{Z}_{p^s}[x]$ 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 codes in $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ that are cyclic as submodules of $\mathcal{R}_{r,s}^{\alpha,\beta}$. So, any submodule of $\mathcal{R}_{r,s}^{\alpha,\beta}$ is a cyclic code. From now on, we will denote by $\mathcal{C}$ indistinctly both the code and the corresponding submodule.

In the following, a polynomial $f(x) \in \mathbb{Z}_{p^r}[x]$ or $\mathbb{Z}_{p^s}[x]$ will be denoted simply by f.

Proposition 4.4. *Let $\mathcal{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Then, there exist polynomials ℓ and $b_0|b_1|\ldots|b_{r-1}|(x^{\alpha}-1)$ over $\mathbb{Z}_{p^r}[x]$, and polynomials $a_0|a_1|\cdots|a_{s-1}|(x^{\beta}-1)$ over $\mathbb{Z}_{p^s}[x]$ such that*

$$\mathcal{C} = \langle (b_0 + pb_1 + \cdots + p^{r-1}b_{r-1} \mid 0), (\ell \mid a_0 + pa_1 + \cdots + p^{s-1}a_{s-1}) \rangle.$$

Proof. Let $\mathcal{C}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. By Theorem 4.3, there exist polynomials $b, \ell \in \mathbb{Z}_{p^s}[x]/\langle x^{\alpha}-1 \rangle$ and $a \in \mathbb{Z}_{p^s}[x]/\langle x^{\beta}-1 \rangle$ such that $\mathcal{C} = \langle (b \mid 0), (\ell \mid a) \rangle$. By Theorem 2.4, one can consider $b = b_0 + pb_1 + \cdots + p^{r-1}b_{r-1}$ and $a = a_0 + pa_1 + \cdots + p^{s-1}a_{s-1}$ such that $b_{r-1}|b_{r-2}|\ldots|b_1|b_0|(x^{\alpha}-1)$ and $a_{s-1}|a_{s-2}|\ldots|a_1|a_0|(x^{\beta}-1)$. □

For the rest of the discussion any cyclic code $\mathcal{C}$ over $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ is of the form $\mathcal{C} = \langle (b \mid 0), (\ell \mid a) \rangle$, where $b = b_0 + pb_1 + \cdots + p^{r-1}b_{r-1}$ and $a(x) = a_0 + pa_1 + \cdots + p^{s-1}a_{s-1}$, for polynomials b_i and a_j as in Proposition 4.4. Since b_0 is a factor of $x^{\alpha}-1$ and for $i = 1 \ldots r-1$ 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 $i = 1 \ldots r-1$, and $\hat{b}_r = b_{r-1}$. 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 $j = 1 \ldots s-1$, and $\hat{a}_s = a_{s-1}$.

Proposition 4.5. *Let $\mathcal{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Then,*

$$\prod_{t=0}^{s-1} \hat{a}_t * (\ell \mid a) \in \langle (b \mid 0) \rangle.$$

Proof. $\prod_{t=0}^{s-1} \hat{a}_t * (\ell \mid a) = \frac{x^{\beta}-1}{a_{s-1}} * (\ell \mid a) = (\pi(\frac{x^{\beta}-1}{a_{s-1}})\ell \mid \frac{x^{\beta}-1}{a_{s-1}}a) = (\pi(\frac{x^{\beta}-1}{a_{s-1}})\ell \mid 0)$. □

Theorem 4.6. *Let $\mathcal{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Define*

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

for $0 \leq j \leq r-1$, and

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

for $0 \leq k \leq s-1$. *Then,*

$$S = \left(\bigcup_{j=0}^{r-1} B_j\right) \bigcup \left(\bigcup_{t=0}^{s-1} A_t\right)$$

forms a minimal generating set for $\mathcal{C}$ *as a* $\mathbb{Z}_{p^s}$*-module. Moreover,*

$$|\mathcal{C}| = p^{\sum_{i=0}^{r-1}(r-i)\deg(\hat{b}_i)+\sum_{j=0}^{s-1}(s-j)\deg(\hat{a}_j)}.$$

Proof. By Theorem 2.5, it is clear that the elements in S are $\mathbb{Z}_{p^s}$-linear independent since $\left(\bigcup_{j=0}^{r-1} B_j\right)_X$ and $\left(\bigcup_{t=0}^{s-1} A_t\right)_Y$ 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, $q*(b \mid 0) \in \langle \bigcup_{j=0}^{r-1} B_j \rangle_{\mathbb{Z}_{p^s}}$. So we have to prove that $d*(\ell \mid a) \in \langle S \rangle_{\mathbb{Z}_{p^s}}$.

If $\deg(d) < \deg(\hat{a}_0)$ then $d*(\ell \mid a) \in \langle A_0 \rangle_{\mathbb{Z}_{p^s}}$ and $c \in \langle S \rangle_{\mathbb{Z}_{p^s}}$. Otherwise, compute $d = d_0\hat{a}_0 + r_0$ with $\deg(r_0) < \deg(\hat{a}_0)$. Then, $d*(\ell \mid a) = d_0\hat{a}_0 * (\ell \mid a) + r_0 * (\ell \mid a)$ and $r_0 * (\ell \mid a) \in \langle A_0 \rangle_{\mathbb{Z}_{p^s}}$.

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

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

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

The *order* of an element $\mathbf{v}$ of an abelian group, $ord(\mathbf{v})$, is the smallest positive integer m such that $m \cdot \mathbf{v} = 0$. Let $\mathcal{C}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code. Define

$$\mathcal{C}_{p^i} = \{\mathbf{v} = (v \mid v') \in \mathcal{C} \mid ord(\mathbf{v}) = p^i \text{ and } ord(v') = p^i\}.$$

Let k_0 be the dimension of $\mathcal{C}_{p^r}$ restricted in the first α coordinates, i.e., $k_0 = \dim((\mathcal{C}_{p^r})_X)$. Define $k_i = \dim((\mathcal{C}_{p^{r-i}})_X) - \sum_{j=0}^{i-1} k_j$, for $i = 1, \ldots, r-1$. The code $\mathcal{C}$ is of type $(\alpha, \beta; k_0, k_1, \ldots, k_{r-1}; l_0, \ldots, l_{s-1})$ if it is group isomorphic to $\mathbb{Z}_{p^r}^{k_0} \times \mathbb{Z}_{p^{r-1}}^{k_1} \times \cdots \times \mathbb{Z}_p^{k_{r-1}} \times \mathbb{Z}_{p^s}^{l_0} \times \cdots \times \mathbb{Z}_p^{l_{s-1}}$. With this definition, it is clear that $|\mathcal{C}| = p^{\sum_{i=0}^{r-1}(r-i)k_i + \sum_{j=0}^{s-1}(s-j)l_j}$. The type and the generator matrices of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes were given in [3].

Example 1. *In this example, we show the standard form of the generator matrix, according to [3], of a* $\mathbb{Z}_4\mathbb{Z}_8$*-additive code of type* $(\alpha, \beta; k_0, k_1; l_0, l_1, l_2)$.

$$\left(\begin{array}{ccc|ccccc} I_{k_0} & B_{0,1} & B_{0,2} & 0 & 0 & 2T_{0,1} & 2T_{0,2} \\ 0 & 2I_{k_1} & 2B_{1,2} & 0 & 0 & 0 & 4T_{1,2} \\ \hline 0 & S_{0,1} & S_{0,2} & I_{l_0} & A_{0,1} & A_{0,2} & A_{0,3} \\ 0 & 0 & 2S_{1,2} & 0 & 2I_{l_1} & 2A_{1,2} & 2A_{1,3} \\ 0 & 0 & 0 & 0 & 0 & 4I_{l_2} & 4A_{2,3} \end{array}\right).$$

In this example, $\mathcal{C}_{2^2}$ is generated by

$$\left(\begin{array}{ccc|cccc} I_{k_0} & B_{0,1} & B_{0,2} & 0 & 0 & 2T_{0,1} & 2T_{0,2} \\ 0 & 2S_{0,1} & 2S_{0,2} & 2I_{l_0} & 2A_{0,1} & 2A_{0,2} & 2A_{0,3} \\ 0 & 0 & 2S_{1,2} & 0 & 2I_{l_1} & 2A_{1,2} & 2A_{1,3} \end{array}\right),$$

and $\mathcal{C}_2$ is generated by

$$\left(\begin{array}{ccc|cccc} 2I_{k_0} & 2B_{0,1} & 2B_{0,2} & 0 & 0 & 4T_{0,1} & 4T_{0,2} \\ 0 & 2I_{k_1} & 2B_{1,2} & 0 & 0 & 0 & 4T_{1,2} \\ 0 & 0 & 0 & 4I_{l_0} & 4A_{0,1} & 4A_{0,2} & 4A_{0,3} \\ 0 & 0 & 0 & 0 & 4I_{l_1} & 4A_{1,2} & 4A_{1,3} \\ 0 & 0 & 0 & 0 & 0 & 4I_{l_2} & 4A_{2,3} \end{array}\right).$$

The following result relates the type and the generator polynomials of a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code when $r = 1$.

Proposition 4.7. *Let $\mathcal{C} \subseteq \mathbb{Z}_p^\alpha \times \mathbb{Z}_{p^s}^\beta$ be a $\mathbb{Z}_p\mathbb{Z}_{p^s}$-additive cyclic code of type $(\alpha, \beta; k_0; l_0, \ldots, l_{s-1})$. Then*

- $k_0 = \alpha - \deg(\gcd(b, \frac{x^\beta - 1}{a_{s-2}} l))$,
- $l_j = \deg(\hat{a}_j)$ *for* $j \in \{0, \ldots, s-2\}$,
- $l_{s-1} = \deg(\hat{a}_{s-1}) + \deg(\gcd(b, \frac{x^\beta - 1}{a_{s-2}} l)) - \deg(b)$.

Proof. By Theorem 4.6, it follows from the sets $A_0, \ldots, A_{s-2}$ that $l_j = \deg(\hat{a}_j)$ for $j \in \{0, \ldots, s-2\}$. By the definition, k_0 is the dimension of the space generated by the firsts α coordinates of B_0 and A_{s-1} that it is generated by the greatest common divisor of b and $\frac{x^\beta - 1}{a_{s-2}} l$. Therefore, $k_0 = \alpha - \deg(\gcd(b, \frac{x^\beta - 1}{a_{s-2}} l))$. Finally, by Theorem 4.6, since $|\mathcal{C}| = p^{\deg(\hat{b}) + \sum_{j=0}^{s-1}(s-j)\deg(\hat{a}_j)} = p^{k_0 + \sum_{j=0}^{s-1}(s-j)l_j}$ and $\deg(\hat{b}) = \alpha - \deg(b)$, it is straightforward that

$$l_{s-1} = \deg(\hat{a}_{s-1}) + \deg(\gcd(b, \frac{x^\beta - 1}{a_{s-2}} l)) - \deg(b).$$

□

For the general case, it is easy to prove that, for $i \in \{0, \ldots, s-r-1\}$, $l_i = \deg(\hat{a}_i)$. But the computation of the remaining parameters become a really meticulous and tedious work. This is because one has to obtain the generator matrix in standard form, described in [3], as the proper linear combination of the sets B_j and A_k from Theorem 4.6.

5 Duality for cyclic codes

Let $\mathcal{C}$ be a $\mathbb{Z}_p\mathbb{Z}_{p^s}$-additive cyclic code and let $\mathcal{C}^\perp$ be the dual code of $\mathcal{C}$. Taking a vector $\mathbf{v}$ of $\mathcal{C}^\perp$, $\mathbf{u} \cdot \mathbf{v} = 0$ for all $\mathbf{u}$ in $\mathcal{C}$. Since $\mathbf{u}$ belongs to $\mathcal{C}$, we know that $\mathbf{u}^{(-1)}$ is also a codeword. So, $\mathbf{u}^{(-1)} \cdot \mathbf{v} = \mathbf{u} \cdot \mathbf{v}^{(1)} = 0$ for all $\mathbf{u}$ from $\mathcal{C}$, therefore $\mathbf{v}^{(1)}$ is in $\mathcal{C}^\perp$ and $\mathcal{C}^\perp$ is also a cyclic code. Consequently, we obtain the following proposition.

Proposition 5.1. *Let $\mathcal{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Then, the dual code of $\mathcal{C}$ is also a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code.*

Proposition 5.2. *Let $\mathcal{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Then,*

$$|\mathcal{C}^{\perp}| = p^{\sum_{i=1}^{r} i \deg(\hat{b}_i) + \sum_{j=1}^{s} j \deg(\hat{a}_j)},$$

Proof. It is well known that $|\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}| = |\mathcal{C}||\mathcal{C}^{\perp}| = p^{\alpha r + \beta s}$ and that $|\mathcal{C}^{\perp}| = p^l$, for some l. By Theorem 4.6, $|\mathcal{C}| = p^{\sum_{i=0}^{r-1}(r-i)\deg(\hat{b}_i) + \sum_{j=0}^{s-1}(s-j)\deg(\hat{a}_j)}$. Therefore,

$$\begin{aligned} l = & \quad \alpha r + \beta s - \textstyle\sum_{i=0}^{r-1}(r-i)\deg(\hat{b}_i) + \sum_{j=0}^{s-1}(s-j)\deg(\hat{a}_j) \\ = & \quad \textstyle\sum_{i=1}^{r} i \deg(\hat{b}_i) + \sum_{j=1}^{s} j \deg(\hat{a}_j). \end{aligned}$$

□

Finally, we exhibit a polynomial operation equivalent to the inner product of vectors, as in [6].

The *reciprocal polynomial* of a polynomial $p(x)$ is $x^{\deg(p(x))}p(x^{-1})$ and is denoted by $p^*(x)$. We denote the polynomial $\sum_{i=0}^{m-1} x^i$ by $\theta_m(x)$, and the least common multiple of α and β by $\mathfrak{m}$.

Definition 5.3. *Let $\mathbf{u}(x) = (u(x) \mid u'(x))$ and $\mathbf{v}(x) = (v(x) \mid v'(x))$ be elements in $\mathcal{R}_{r,s}^{\alpha,\beta}$. We define the map*

$$\circ : \mathcal{R}_{r,s}^{\alpha,\beta} \times \mathcal{R}_{r,s}^{\alpha,\beta} \longrightarrow \mathbb{Z}_{p^s}[x]/\langle x^{\mathfrak{m}} - 1\rangle,$$

such that

$$\begin{aligned} \circ(\mathbf{u}(x), \mathbf{v}(x)) = & p^{s-r}\iota(u(x)v^*(x))\theta_{\frac{\mathfrak{m}}{r}}(x^r)x^{\mathfrak{m}-1-\deg(v(x))} + \\ & + u'(x)v'^*(x)\theta_{\frac{\mathfrak{m}}{s}}(x^s)x^{\mathfrak{m}-1-\deg(v'(x))} \mod (x^{\mathfrak{m}} - 1). \end{aligned}$$

The map $\circ$ is linear in each of its arguments; i.e., if we fix the first entry of the map invariant, while letting the second entry vary, then the result is a linear map. Similarly, when fixing the second entry invariant. Then, the map $\circ$ is a bilinear map between $\mathbb{Z}_{p^s}[x]$-modules.

From now on, we denote $\circ(\mathbf{u}(x), \mathbf{v}(x))$ by $\mathbf{u}(x) \circ \mathbf{v}(x)$. Note that $\mathbf{u}(x) \circ \mathbf{v}(x)$ belongs to $\mathbb{Z}_{p^s}[x]/\langle x^{\mathfrak{m}} - 1\rangle$.

Theorem 5.4. *Let $\mathbf{u}$ and $\mathbf{v}$ be vectors in $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ with associated polynomials $\mathbf{u}(x) = (u(x) \mid u'(x))$ and $\mathbf{v}(x) = (v(x) \mid v'(x))$, respectively. Then, $\mathbf{v}$ is orthogonal to $\mathbf{u}$ and all its shifts if and only if*

$$\mathbf{u}(x) \circ \mathbf{v}(x) = 0.$$

Proof. Let $\mathbf{u}^{(i)} = (u_{0+i}u_{1+i}\ldots u_{\alpha-1+i} \mid u'_{0+i}\ldots u'_{\beta-1+i})$ be the ith shift of $\mathbf{u}$. Then,

$$\mathbf{u}^{(i)} \cdot \mathbf{v} = 0 \text{ if and only if } p^{s-r}\sum_{j=0}^{\alpha-1}\iota(u_j v_{j+i}) + \sum_{k=0}^{\beta-1} u'_k v'_{k+i} = 0 \mod p^s.$$

Let $S_i = p^{s-r}\sum_{j=0}^{\alpha-1}\iota(u_jv_{j+i}) + \sum_{k=0}^{\beta-1}u'_kv'_{k+i}$. One can check that

$$\begin{aligned}\mathbf{u}(x)\circ\mathbf{v}(x) &= p^{s-r}\sum_{n=0}^{\alpha-1}\left(\theta_{\frac{\mathfrak{m}}{\alpha}}(x^\alpha)\sum_{j=0}^{\alpha-1}\iota(u_jv_{j+n})x^{\mathfrak{m}-1-n}\right)\\ &\quad+\sum_{t=0}^{\beta-1}\left(\theta_{\frac{\mathfrak{m}}{\beta}}(x^\beta)\sum_{k=0}^{\beta-1}u'_kv'_{k+t}x^{\mathfrak{m}-1-t}\right) \mod (x^{\mathfrak{m}}-1)\\ &= \theta_{\frac{\mathfrak{m}}{\alpha}}(x^\alpha)\left(\sum_{n=0}^{\alpha-1}\sum_{j=0}^{\alpha-1}p^{s-r}\iota(u_jv_{j+n})x^{\mathfrak{m}-1-n}\right)\\ &\quad+\theta_{\frac{\mathfrak{m}}{\beta}}(x^\beta)\left(\sum_{t=0}^{\beta-1}\sum_{k=0}^{\beta-1}u'_kv'_{k+t}x^{\mathfrak{m}-1-t}\right) \mod (x^{\mathfrak{m}}-1).\end{aligned}$$

Then, arranging the terms one obtains that

$$\mathbf{u}(x)\circ\mathbf{v}(x) = \sum_{i=0}^{\mathfrak{m}-1}S_ix^{\mathfrak{m}-1-i} \mod (x^{\mathfrak{m}}-1).$$

Thus, $\mathbf{u}(x)\circ\mathbf{v}(x) = 0$ if and only if $S_i = 0$ for $0 \le i \le \mathfrak{m}-1$. □

Theorem 5.4 shows that $\circ$ is the corresponding polynomial operation to the inner product of vectors. Finally, the following example illustrates this correspondence.

Example 2. *Let $\mathcal{R}_{3,9}^{4,5} = \mathbb{Z}_3^4 \times \mathbb{Z}_9^5$, then the inner product is*

$$\mathbf{u}\cdot\mathbf{v} = 3^{2-1}\sum_{i=0}^{4-1}\iota(u_iv_i) + \sum_{j=0}^{5-1}u'_jv'_j \in \mathbb{Z}_9.$$

Let $\mathbf{u} = (1,1,1,1 \mid 1,1,1,1,1)$ and $\mathbf{v} = (1,0,1,0 \mid 2,0,1,0,0)$. Clearly, all the shifts of $\mathbf{v}$ are orthogonal to $\mathbf{u}$. Then,

$$\begin{aligned}\mathbf{u}(x)\circ\mathbf{v}(x) &= (x^3+x^2+x+1 \mid x^4+x^3+x^2+x+1)\circ(x^2+1 \mid x^3+2)\\ &= 3^{2-1}\iota\left((x^3+x^2+x+1)(x^2+1)^*\right)\theta_{\frac{20}{4}}(x^4)x^{20-1-2}\\ &\quad+(x^4+x^3+x^2+x+1)(x^3+2)^*\theta_{\frac{20}{5}}(x^5)x^{20-1-3} \mod (x^{20}-1)\\ &= 3(x^3+x^2+x+1)(x^2+1)\theta_5(x^4)x^{17}\\ &\quad+(x^4+x^3+x^2+x+1)(2x^3+1)\theta_4(x^5)x^{16} \mod (x^{20}-1)\\ &= 5x^{38}+5x^{37}+8x^{36}+4x^{18}+4x^{17}+x^{16} \mod (x^{20}-1)\\ &= 0.\end{aligned}$$

References

[1] T. Abualrub, I. Siap, N. Aydin. $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. *IEEE Trans. Info. Theory*, vol. 60, No. 3, pp. 1508-1514, 2014.

[2] I. Aydogdu, I. Siap. The Structure of $\mathbb{Z}_2\mathbb{Z}_{2^s}$-Additive Codes: Bounds on the Minimum Distance. *Applied Mathematics & Information Sciences*, vol. 7, No. 6, pp. 2271-2278, 2013.

[3] I. Aydogdu, I. Siap. On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes. *Linear and Multilinear Algebra*, vol. 63, No. 10, pp. 2089-2102, 2014.

[4] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà and M. Villanueva. $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality. *Designs, Codes and Cryptography*, vol. 54, No. 2, pp. 167-179, 2010.

[5] J. Borges, C. Fernández-Córdoba, R. Ten-Valls. $\mathbb{Z}_2$-double cyclic codes. arXiv:1410.5604, 2014.

[6] 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, 2014.

[7] A.R. Calderbank, N.J.A. Sloane. Modular and p-adic cyclic codes. *Designs, Codes and Cryptography*, vol. 6, pp. 21-35, 1995.

[8] H.Q. Dinh, S.R. López-Permouth Cyclic and negacyclic codes over finite chain rings. *Lecture Notes in Computer Science*, n. 5228, pp. 46-55, 2008.

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

[10] P. Kanwar, S.R. López-Permouth. Cyclic Codes over the Integers Modulo p^m. *Finite Fields and their Applications*, vol. 3, pp. 334-352, 1997.