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

J. Borges[1], C. Fernández-Córdoba[1], R. Ten-Valls[1]

[1] *Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, Spain, {joaquim.borges, cristina.fernandez, roger.ten}@uab.cat*
This work has been partially supported by the Spanish MEC grant TIN2013-40524-P and by the Catalan AGAUR grant 2014SGR-691.

The $\mathbb{Z}_2\mathbb{Z}_4$-additive codes has been introduced in [**?**] and intensively studied during last years. Recently, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes has been defined in [**?**] and identified as $\mathbb{Z}_4[x]$-modules of a certain ring. The duality of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes has been studied in [**?**].

In recent times, $\mathbb{Z}_2\mathbb{Z}_4$-additive codes were generalized to $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additives codes in [**?**]. They determine, in particular, the standard forms of generator and parity-check matrices and present some bounds on the minimum distance.

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 $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$ is $\mathbb{Z}_p$, then an element b of $\mathbb{Z}_{p^r}$ could be written uniquely as $b = b_0 + pb_1 + p^2b_2 + \cdots + p^{r-1}b_{r-1}$, and any element $a \in \mathbb{Z}_{p^s}$ as $a = a_0 + pa_1 + p^2a_2 + \cdots + p^{s-1}a_{s-1}$, where $b_i, a_j \in \mathbb{Z}_p$.

Then we can consider the surjective ring homomorphism $\pi : \mathbb{Z}_{p^s} \twoheadrightarrow \mathbb{Z}_{p^r}$, where $\pi(a) = a \mod p^r$.

Note that $\pi(p^i) = 0$ if $i \geq r$. Let $a \in \mathbb{Z}_{p^s}$ and $b \in \mathbb{Z}_{p^r}$. We define a multiplication $*$ as follows: $a * b = \pi(a)b$. Then, $\mathbb{Z}_{p^r}$ is a $\mathbb{Z}_{p^s}$-module with external multiplication given by π. Since $\mathbb{Z}_{p^r}$ is commutative, then $*$ 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 1. *A $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code $\mathscr{C}$ is a $\mathbb{Z}_{p^s}$-submodule of $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$.*

The structure of the generator matrices in standard form and the type of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additives codes are defined and determinated in [**?**].

Let $\mathscr{C}_\alpha$ be the canonical projection of $\mathscr{C}$ on the first α coordinates and $\mathscr{C}_\beta$ on the last β coordinates. The canonical projection is a linear map. Then, $\mathscr{C}_\alpha$ and $\mathscr{C}_\beta$ are $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$ linear codes of length α and β, respectively. A code $\mathscr{C}$ is called *separable* if $\mathscr{C}$ is the direct product of $\mathscr{C}_\alpha$ and $\mathscr{C}_\beta$, i.e., $\mathscr{C} = \mathscr{C}_\alpha \times \mathscr{C}_\beta$.

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 [**?**] 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 $\mathscr{C}$ in $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ is defined in a natural way as

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

Let $\mathscr{C}$ be a separable code, then $\mathscr{C}^{\perp}$ is also separable and $\mathscr{C}^{\perp} = \mathscr{C}_{\alpha}^{\perp} \times \mathscr{C}_{\beta}^{\perp}$.

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

Definition 2. *Let $\mathscr{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code. The code $\mathscr{C}$ is called* cyclic *if*

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

implies

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

Let $\mathbf{u} = (u_0, u_1, \ldots, u_{\alpha-1} \mid u'_0, \ldots, u'_{\beta-1})$ be a codeword in $\mathscr{C}$ and let i be an integer. Then we 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 $\mathscr{C}_{\alpha}$ and $\mathscr{C}_{\beta}$ are $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$ cyclic codes of length α and β.

In the particular case that $r = s$, the simultaneous shift of two sets of coordinates that leave invariant the code $\mathscr{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^r}^{\beta}$ is known in the literature as *double cyclic code* over $\mathbb{Z}_{p^r}$, see [**?**], [**?**]. The term *double cyclic* is given in order to distinguish the cyclic code $\mathscr{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^r}^{\beta}$ to the cyclic code $\mathscr{C}' \subseteq \mathbb{Z}_{p^r}^{\alpha+\beta}$.

Denote by $\mathscr{R}_{r,s}^{\alpha,\beta}$ the ring $\mathbb{Z}_{p^r}[x]/(x^{\alpha}-1) \times \mathbb{Z}_{p^s}[x]/(x^{\beta}-1)$. There is a bijective map between $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ and $\mathscr{R}_{r,s}^{\alpha,\beta}$ 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 this map to each of the coefficients of a given polynomial.

Definition 3. *Define the operation* $*: \mathbb{Z}_{p^s}[x] \times \mathscr{R}_{r,s}^{\alpha,\beta} \to \mathscr{R}_{r,s}^{\alpha,\beta}$ *as*

$$\lambda(x) * (u(x) \mid u'(x)) = (\pi(\lambda(x))u(x) \mid \lambda(x)u'(x)),$$

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

The ring $\mathscr{R}_{r,s}^{\alpha,\beta}$ 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 $\mathscr{R}_{r,s}^{\alpha,\beta}$. Note that if we operate $\mathbf{u}(x)$ by x we get

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

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

Now, we study submodules of $\mathscr{R}_{r,s}^{\alpha,\beta}$. 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 $\mathscr{R}_{r,s}^{\alpha,\beta}$.

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 [**?**],[**?**].

Theorem 4. *The* $\mathbb{Z}_{p^s}[x]$*-module* $\mathscr{R}_{r,s}^{\alpha,\beta}$ *is noetherian, and every submodule* $\mathscr{C}$ *of* $\mathscr{R}_{r,s}^{\alpha,\beta}$ *can be written as*

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

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* $\ell(x) \in \mathbb{Z}_{p^r}[x]/(x^{\alpha}-1)$.

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 $\mathscr{R}_{r,s}^{\alpha,\beta}$. So, any submodule of $\mathscr{R}_{r,s}^{\alpha,\beta}$ is a cyclic code. From now on, we will denote by $\mathscr{C}$ indistinctly both the code and the corresponding submodule.

Proposition 5. *Let* $\mathscr{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ *be a* $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$*-additive cyclic code. Then, there exist polynomials* $\ell(x)$ *and* $b_0(x)|b_1(x)|\dots|b_{r-1}(x)|(x^{\alpha}-1)$ *over* $\mathbb{Z}_{p^r}[x]$*, and polynomials* $a_0(x)|a_1(x)|\cdots|a_{s-1}(x)|(x^{\beta}-1)$ *over* $\mathbb{Z}_{p^s}[x]$ *such that*

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

Let $b(x)=b_0(x)+pb_1(x)+\cdots+p^{r-1}b_{r-1}(x)$ and $a(x)=a_0(x)+pa_1(x)+\cdots+p^{s-1}a_{s-1}(x)$, for polynomials $b_i(x)$ and $a_j(x)$ as in Proposition **??**. Then, for the rest of the discussion, we assume that a cyclic code $\mathscr{C}$ over $\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$ is generated by $\langle(b(x)\mid 0),(\ell(x)\mid a(x))\rangle$. Since $b_0(x)$ is a factor of $x^{\alpha}-1$ and for $i=1\ldots r-1$ the polynomial $b_i(x)$ is a factor of $b_{i-1}(x)$, we will denote $\hat{b}_0(x)=\frac{x^{\alpha}-1}{b_0(x)}$ and $\hat{b}_i(x)=\frac{b_{i-1}(x)}{b_i(x)}$ for $i=1\ldots r-1$. In the same way, we define $\hat{a}_0(x)=\frac{x^{\beta}-1}{a_0(x)}$, $\hat{a}_j(x)=\frac{a_{j-1}(x)}{a_j(x)}$ for $j=1\ldots s-1$.

Proposition 6. *Let $\mathscr{C}\subseteq\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Then,*

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

Theorem 7. *Let $\mathscr{C}\subseteq\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Define*

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

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

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

for $0\le k\le s-1$. Then,

$$S=\bigcup_{j=0}^{r-1}B_{p^j}\bigcup_{t=0}^{s-1}A_{p^t}$$

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

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

Let $\mathscr{C}$ be a cyclic code and $\mathscr{C}^{\perp}$ the dual code of $\mathscr{C}$. Taking a vector $\mathbf{v}$ of $\mathscr{C}^{\perp}$, $\mathbf{u}\cdot\mathbf{v}=0$ for all $\mathbf{u}$ in $\mathscr{C}$. Since $\mathbf{u}$ belongs to $\mathscr{C}$, 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 $\mathscr{C}$, therefore $\mathbf{v}^{(1)}$ is in $\mathscr{C}^{\perp}$ and $\mathscr{C}^{\perp}$ is also a cyclic code over $\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$. Consequently, we obtain the following proposition.

Proposition 8. *Let $\mathscr{C}\subseteq\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Then the dual code of $\mathscr{C}$ is also a cyclic code in $\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$.*

Proposition 9. *Let $\mathscr{C} \subseteq \mathbb{Z}_{p^r}^\alpha \times \mathbb{Z}_{p^s}^\beta$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Then,*

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

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 10. *Let $\mathbf{u}(x) = (u(x) \mid u'(x))$ and $\mathbf{v}(x) = (v(x) \mid v'(x))$ be elements in $\mathscr{R}_{r,s}^{\alpha,\beta}$. We define the map $\circ : \mathscr{R}_{r,s}^{\alpha,\beta} \times \mathscr{R}_{r,s}^{\alpha,\beta} \longrightarrow \mathbb{Z}_{p^s}[x]/(x^\mathfrak{m}-1)$, 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 $\mathbb{Z}_{p^s}[x]/(x^\mathfrak{m}-1)$.

Theorem 11. *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*

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

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. On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes. Linear and Multilinear Algebra, DOI: 10.1080/03081087.2014.952728, 2014.

[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. *Designs, Codes and Cryptography*, vol. 54, No. 2, pp. 167-179, 2010.

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

[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, 2014.

[6] A.R. Calderbank, N.J.A. Sloane. Modular and p-adic cyclic codes. *Designs, Codes and Cryptography*, vol. 37, No. 6, pp. 21-35, 1995.

[7] 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.

[8] J. Gao, M. Shi, T. Wu and F. Fu. On double cyclic codes over $\mathbb{Z}_4$. arXiv: 1501.01360, 2015.