

LINEAR AND CYCLIC CODES OVER SOME SPECIAL RINGS

Cristina Flaut and Bianca Liana Bercea-Straton

Received: 28 May 2026; Revised: 10 September 2026; Accepted: 15 September 2026

Communicated by Sait Halicioglu

ABSTRACT. The study of linear and cyclic codes over some types of finite rings has enabled the development of highly efficient codes with optimal parameters. Due to the algebraic properties of these rings, error-correction algorithms can be well adapted to diverse noisy channels, enhancing real-time performance. Furthermore, by using ideals in polynomial rings, cyclic codes ensure that hardware implementation remains remarkably straightforward and fast. For these reasons, in this paper, we describe linear and cyclic codes over the rings of the form $R_{s,p} = \mathbb{Z}_p[u]/(f(u)/(u-s))$, where p is a prime number and $f(u) = u^p - u$, with $s \in \{0, 1, \dots, p-1\}$.

Mathematics Subject Classification (2020): 94B05, 94B15

Keywords: Cyclic code, linear code, Hamming weight

1. Introduction

The study of linear and cyclic codes defined over finite rings represents a fundamental direction in information theory and cryptography, with crucial applications in ensuring the integrity and security of modern data. Unlike traditional codes constructed exclusively over finite fields (such as binary ones), the richer algebraic structures of rings allow for a much higher information density and superior modeling of complex communication channels. Their theoretical importance is driven by the deep connections between algebra and other branches of mathematics (combinatorics, algebraic geometry) providing great tools for designing highly efficient decoding algorithms capable of detecting and correcting multiple errors. Practically, these codes form the foundation of current standards in data storage technologies (such as flash memory or optical discs) and advanced telecommunication systems, where energy efficiency and transmission reliability are essential. Thus, their analysis remains crucial for technological evolution and the security of global digital infrastructures.

In this paper, all rings R are considered commutative and unitary rings.

Definition 1.1. i) ([1], [7]) Let R be a commutative and unitary ring. Over R a linear code $\mathcal{C}$ of length n is an R -submodule of R^n . If R is a field, then a linear code is an $[n, k]$ code if the dimension of this R -subspace is k . For this case, we can associate a $k \times n$ matrix to an $[n, k]$ linear code. The rows of this matrix form a basis in $\mathcal{C}$ and is called the generator matrix of the code $\mathcal{C}$. If this matrix is under the form $(I_k \mid M)$, where I_k is $k \times k$ matrix and M is a $k \times (n - k)$ parity matrix, used to determine the error-checking bits, this form is called systematic.

Remark 1.2. i) [1, Theorem 2.1] We consider the ring $R_n = R[x]/(x^n - 1)$. We associate to the vector $c = (c_1, \dots, c_n)$ the polynomial $c(x) = c_1 + c_2x + \dots + c_nx^n$ in R_n . In the ring R_n a subset $\mathcal{C}$ of R_n is a cyclic code if and only if $\mathcal{C}$ is an ideal of R_n .

ii) If $\mathcal{C}$ is a linear code of length n over the ring R , for a codeword $c = (c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$, the Hamming weight $w_H(c)$ is the number of coordinates i in which c_i is different from zero in the ring R . The minimum Hamming weight of the code $\mathcal{C}$ is $w_{\min}(\mathcal{C}) = \min\{w_H(c), c \in \mathcal{C}\}$. The Hamming distance d between two codewords, $c = (c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$, $c' = (c'_0, c'_1, \dots, c'_{n-1}) \in \mathcal{C}$ is the number of positions in which the corresponding symbols are different:

$$d(c, c') = |i, c_i \neq c'_i|.$$

The minimum Hamming distance of a linear code, d_H , is the minimum Hamming distance between two nonzero different codewords, which is the minimum Hamming weight of all its nonzero codewords.

$$d_H = \min \{d(c, c'), c, c' \in \mathcal{C}, c \neq c'\}.$$

With the above notations, a Maximum Distance Separable code (MDS) is a code such that $d_H = n - k + 1$.

iii) [2, Theorem 2.8] The socle of the R -module M , $Soc(M)$, is the sum of its minimal submodules. A finite ring is called a Frobenius ring if its socle is a principal ideal. The direct product of fields is a Frobenius ring.

iv) [7] On R^n we define the dot product

$$x \cdot y = \sum_{i=1}^n x_i y_i,$$

for $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in R^n$. For a linear code $\mathcal{C}$ over the ring R , we define the dual of the code $\mathcal{C}$, denoted $\mathcal{C}^\perp$,

$$\mathcal{C}^\perp = \{x \in R^n, x \cdot y = 0, \text{ for all } y \in \mathcal{C}\}.$$

v) If R is a field, the generator matrix of the code $\mathcal{C}^\perp$ is an $(n - k) \times n$ matrix, denoted H , and called the parity check matrix for the code $\mathcal{C}$. If the generator matrix of the code $\mathcal{C}$ is in the systematic form $(I_k \mid M)$, then the parity check matrix of the dual code has the form $(-M^t \mid I_{n-k})$.

vi) [3, Theorem 1] On a finite commutative Frobenius ring R , if I is an ideal of R , then $|I| |I^\perp| = |R|$, therefore for a linear code defined on the finite Frobenius rings, we can define the dual of this code.

vii) [5, 235-236] In a ring R , the element $e \in R$ is called idempotent if $e^2 = e$. Two idempotents e_1 and e_2 are called orthogonal if $e_1 e_2 = 0$. If $(e_i)_{i \in I}$ represents a family of idempotents of the ring R , such that $e_i e_j = \delta_{ij} e_i$, where δ_{ij} is the Kronecker symbol and $\sum_{i \in I} e_i = 1$, then the ring R can be written in the form:

$$R = \bigoplus_{i \in I} e_i R,$$

called the Peirce decomposition.

2. Linear and cyclic codes over the ring $R_{s,p}$

There are many papers dedicated to the study of diverse types of linear and cyclic codes. In several papers, codes over different special rings were studied, as for example: over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q, v^3 = v$, where q is an odd prime power, in [4], over the ring $R = \mathbb{F}_2 + v\mathbb{F}_2$, with $v^2 = v$, in [8], over the ring $R = \mathbb{F}_p + v\mathbb{F}_p + \dots + v^{p-1}\mathbb{F}_p$, where p is a prime number and $v^p = v$, in [6], etc. We can remark that the involved polynomials are of the form $f(v) = v^p - v = v(v-1)(v-2)\dots(v-p+1)$, p is a prime number, that means polynomials having all p distinct roots as all elements from $\mathbb{Z}_p$. For this reason, we consider a good idea the study of the linear and cyclic codes over the rings of the form $R_{s,p} = \mathbb{Z}_p[u]/(f(u)/(u-s))$, where:

- p is a prime number
- the involved polynomial has only $p-2$ distinct roots as elements in $\mathbb{Z}_p$.

For this purpose, we consider $f(u)$ of the form $f(u) = u^p - u = u(u-1)\dots(u-p+1)$.

We choose an arbitrary $s \in \{0, 1, \dots, p-1\}$ and define the ring

$$R_{s,p} = \mathbb{Z}_p[u]/(f(u)/(u-s)).$$

We consider the set $I_s = \{0, 1, 2, \dots, p-1\} - \{s\}$. The ring $R_{s,p}$, defined above, has cardinality p^{p-1} . We denote

$$Q_{sr}(u) = \frac{f(u)}{(u-s)(u-r)} = \prod_{i \neq s, i \neq r, s \neq r} (u-i),$$

and $g_s(u) = (u - r)Q_{sr}(u) = \frac{f(u)}{(u-s)}$. Using these notations, the ring $R_{s,p}$ can be written under the form:

$$R_{s,p} = \mathbb{Z}_p[u] / (f(u) / (u - s)) = \mathbb{Z}_p[u] / (g_s(u)).$$

We remark that $R_{s,p} = \prod_{i \in I_s} \mathbb{Z}_p[u] / (u - i) = \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{p-1 \text{ times}}$, since $\mathbb{Z}_p[u] / (u - i) \simeq \mathbb{Z}_p$.

For $r \in I_s$, we consider the element $q_r = Q_{sr}(r)^{-1} \bmod p$.

Proposition 2.1. *By using the above notations, the following statements are true:*

- i) *The element $\alpha_r(u) = q_r Q_{sr}(u)$ is an idempotent in the ring $R_{s,p}$.*
- ii) *$\alpha_i(u)\alpha_j(u) = 0$ for $i \neq j$ and $\sum_{j \in I_s} \alpha_j(u) = 1$.*

Proof. i) Indeed, we will prove that $\alpha_r^2(u) = \alpha_r(u) \bmod g_s(u)$, for all $r \in I_s$.

$$\begin{aligned} \alpha_r^2(u) - \alpha_r(u) &= q_r Q_{sr}(u)^2 - q_r Q_{sr}(u) = \\ &= q_r^2 Q_{sr}^2(u) - q_r Q_{sr}(u) = q_r Q_{sr}(u) (q_r Q_{sr}(u) - 1), \end{aligned}$$

then

$$Q_{sr}(u) \mid (\alpha_r^2(u) - \alpha_r(u)).$$

Now, we compute the element $\alpha_r^2(u) - \alpha_r(u)$.

We obtain

$$\begin{aligned} \alpha_r^2(r) - \alpha_r(r) &= q_r Q_{sr}(r) (q_r Q_{sr}(r) - 1) = \\ &= Q_{sr}(r)^{-1} Q_{sr}(r) (Q_{sr}(r)^{-1} Q_{sr}(r) - 1) = 0. \end{aligned}$$

Then $(u - r) \mid (\alpha_r^2(u) - \alpha_r(u))$ and $g_s(u) \mid (\alpha_r^2(u) - \alpha_r(u))$. We get $\alpha_r^2(u) = \alpha_r(u) \bmod g_s(u)$ and it results that $\alpha_r(u)$ is a nontrivial idempotent in $R_{s,p}$.

ii) It is clear that $\alpha_i(u)\alpha_j(u) = 0$. We must prove that $\sum_{j \in I_s} \alpha_j(u) = 1$. If $l \in I_s$, we have $\sum_{j \in I_s} \alpha_j(l) = 1$, since $\alpha_l(l) = Q_{sl}(l)^{-1} Q_{sl}(l) = 1$, if $j = l$ and $\alpha_j(l) = 0$, for $j \neq l$. Therefore, $\{\alpha_j(u)\}_{j \in I_s}$ represents a set of orthogonal idempotents. $\square$

From the above proposition, it results that we can apply the Peirce decomposition, and the ring $R_{s,p}$ has the following form:

$$R_{s,p} = \bigoplus_{i \in I_s} \alpha_i R_{s,p}. \quad (1)$$

Proposition 2.2. *Let $\mathcal{C}$ be a linear code of length n and dimension k over the ring $R_{s,p}$.*

i) From relation (1), we have

$$\mathcal{C} = \bigoplus_{i \in I_s} \alpha_i \mathcal{C}_i, \quad (2)$$

where $\mathcal{C}_i, i \in I_s$, are linear codes of length n and dimension k over the field $\mathbb{Z}_p$.

ii) $|\mathcal{C}| = \prod_{i \in I_s} |\mathcal{C}_i| = p^{(p-1)k}$.

iii) If $\mathcal{C}_i$ are linear codes of length n and dimension k_i over the field $\mathbb{Z}_p, i \in I_s$, and G_i is its generator matrix, we obtain that the generator matrix of the code $\mathcal{C}$ has the form

$$G = \sum_{i \in I_s} \alpha_i G_i.$$

iv) For the linear code $\mathcal{C}$, the minimum Hamming distance, $d_H(\mathcal{C})$, has the following formula:

$$d_H(\mathcal{C}) = \min_{i \in I_s} \{d_H(\mathcal{C}_i)\}.$$

Proof. i) The element $x \in R_{s,p}$ has the following form $x = \sum_{i=0}^{p-1} x_i u^i, x_i \in \mathbb{Z}_p$. From here, by using the fact that $\{\alpha_i\}_{i \in I_s}$ are orthogonal idempotents, we obtain $\alpha_i x = x_i \alpha_i, x_i \in \mathbb{Z}_p$, for all $i \in I_s$. From here, it results that relation (2) is true.

ii) We have that $|\mathcal{C}_i| = p^k$, therefore $\prod_{i \in I_s} |\mathcal{C}_i| = p^{(p-1)k}$. Since $\mathcal{C}$ is a linear code of length n and dimension k over the ring $R_{s,p}$, we have $|\mathcal{C}| = |R_{s,p}|^k = (p^{(p-1)})^k = p^{(p-1)k}$.

iii) It is obvious from the above results.

iv) It is obvious from the definition of Hamming distance. $\square$

Remark 2.3. It is clear that the linear codes $\mathcal{C}_i$ are of the form:

$$\mathcal{C}_i = \{x_i \in \mathbb{Z}_p^n, \text{ such that there are } x_j \in \mathbb{Z}_p^n, \text{ for all } j \in I_s - \{i\}, \text{ with } \sum_{i=0}^{p-1} x_i u^i \in \mathcal{C}\}, i \in I_s.$$

Proposition 2.4. Let $\mathcal{C} = \bigoplus_{i \in I_s} \alpha_i \mathcal{C}_i$ be a linear code of length n over the ring $R_{s,p}$. Therefore, its dual code has the following form:

$$\mathcal{C}^\perp = \bigoplus_{i \in I_s} \alpha_i \mathcal{C}_i^\perp.$$

Proof. Indeed, let $c \in \mathcal{C}$, $c = \bigoplus_{i \in I_s} \alpha_i c_i$. We denote $\mathcal{D} = \bigoplus_{i \in I_s} \alpha_i \mathcal{C}_i^\perp$. Let $d \in \bigoplus_{i \in I_s} \alpha_i \mathcal{C}_i^\perp, d = \bigoplus_{i \in I_s} \alpha_i d_i$. We compute $c \cdot d = \prod_{i \in I_s} \alpha_i c_i d_i = 0$, therefore $c \cdot d = 0$. From here, it results that $\mathcal{D} \subseteq \mathcal{C}^\perp$. Since the ring $R_{s,p}$ is a Frobenius ring, then

$|\mathcal{C}||\mathcal{C}^\perp| = |R_{s,p}|^n$. From here, we have $|\mathcal{D}| = \prod_{i \in I_s} |\mathcal{C}_i^\perp| = \prod_{i \in I_s} \frac{|\mathbb{Z}_p^n|}{|\mathcal{C}_i|} = \prod_{i \in I_s} \frac{p^n}{p^{k_i}} = \frac{p^{n(p-1)}}{\prod_{i \in I_s} p^{k_i}} = \frac{|R_{s,p}|^n}{|\mathcal{C}|} = |\mathcal{C}^\perp|$. Therefore, $\mathcal{D} = \mathcal{C}^\perp$. $\square$

In the following, we consider the ring $R_{s,p,n} = R_{s,p}[x]/(x^n - 1)$.

Remark 2.5. A linear code $\mathcal{C}$ of length n over the ring $R_{s,p}$ is a cyclic code of length n over the ring $R_{s,p}$ if and only if $\mathcal{C}$ is an ideal in $R_{s,p,n}$, or, equivalently, if $c = (c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$, then $c = (c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in \mathcal{C}$.

Proposition 2.6. Let $\mathcal{C} = \bigoplus_{i \in I_s} \alpha_i \mathcal{C}_i$ be a linear code over the ring $R_{s,p}$. Then $\mathcal{C} = \bigoplus_{i \in I_s} \alpha_i \mathcal{C}_i$ is a cyclic code of length n over the ring $R_{s,p}$ if and only if the codes $\mathcal{C}_i$ are cyclic codes of length n over the ring $\mathbb{Z}_p[x]/(x^n - 1)$, for all $i \in I_s$.

Proof. Indeed, we consider the codewords $c_i = (c_{i,0}, c_{i,1}, \dots, c_{i,n-1}) \in \mathcal{C}_i, i \in I_s$ and $c_j = \sum_{i \in I_s} \alpha_i c_{ij}, j \in \{0, 1, \dots, n-1\}$. From here, we obtain that $c = (c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$. Since $\mathcal{C}$ is a cyclic code, we have that $(c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in \mathcal{C}$. It results $(c_{n-1}, c_0, c_1, \dots, c_{n-2}) = \sum_{i \in I_s} \alpha_i (c_{i,n-1}, c_{i,0}, \dots, c_{i,n-2})$. From relation (2), we obtain the unicity of the linear codes decomposition over the ring $R_{s,p}$, then $(c_{i,n-1}, c_{i,0}, \dots, c_{i,n-2}) \in \mathcal{C}_i$ and $\mathcal{C}_i$ is a cyclic code for all $i \in I_s$.

For the converse statement, we consider that $\mathcal{C}_i$ are cyclic codes over the field $\mathbb{Z}_p$, for all $i \in I_s$, and let $c = (c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$. Since

$$c = \sum_{i \in I_s} \alpha_i (c_{i,0}, \dots, c_{i,n-2}, c_{i,n-1}) \in \bigoplus_{i \in I_s} \alpha_i \mathcal{C}_i,$$

it results that the linear code c is a cyclic code of length n over the ring $R_{s,p}$. $\square$

3. Some examples

In this section, we will provide some examples of the above studied codes: linear codes, the attached dual codes and cyclic codes. These examples are important to well understand the properties of these codes. Linear codes use a simple generator matrix, which makes encoding and decoding fast for computers. Computers only need to store a small generator matrix instead of a massive list of every possible codeword. Also, linear codes have a measurable distance, that tells us how many errors the code can catch or fix. Dual codes are important in syndrome decoding and cyclic codes turn binary data into mathematical polynomials, making calculations neat and predictable.

Linear codes. Let $p = 5$ and $f(u) = u^5 - u = u(u-1)(u-2)(u-3)(u-4)$. We choose $s = 4$ and we define $R_{4,5} = \mathbb{Z}_5[u]/(u(u-1)(u-2)(u+2))$. This ring

has cardinality 5^4 . We denote with $I_4 = \{0, 1, 2, 3\}$. We have

$$Q_{4r}(u) = \frac{u(u-1)(u-2)(u-3)(u-4)}{(u-4)(u-r)} = \prod_{i \neq 4, i \neq r, r \neq 4} (u-i).$$

We consider $g_4(u) = (u-r)Q_{4r}(u) = \frac{f(u)}{(u-4)}$. Then

$$R_{4,5} = \mathbb{Z}_5[u] / (u(u-1)(u-2)(u-3)).$$

We denote with $q_r = Q_{4r}(r)^{-1} \bmod 5$, $r \in I_4$. The element $\alpha_r(u) = q_r Q_{4r}(u)$ is an idempotent in the ring $R_{4,5}$. We have the following idempotents: $\alpha_0(u) = q_0 Q_{40}(u) = 4(u-1)(u-2)(u-3)$; $\alpha_1(u) = q_1 Q_{41}(u) = 3u(u-2)(u-3)$; $\alpha_2(u) = q_2 Q_{42}(u) = 2u(u-1)(u-3)$; $\alpha_3(u) = q_3 Q_{43}(u) = u(u-1)(u-2)$.

i) We consider a linear code of length 5 and dimension 3 given by the following generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & u^3 + 3u^2 + 2u + 1 & u^3 + u^2 + 4u + 1 \\ 0 & 1 & 0 & 3u^3 + 3u^2 + 4u + 2 & 2u^3 + u^2 + u \\ 0 & 0 & 1 & 4u^3 + 4u^2 + 2u & 4u^3 + 2u^2 + u + 3 \end{pmatrix},$$

$$\mathcal{C} = \alpha_0 \mathcal{C}_0 \oplus \alpha_1 \mathcal{C}_1 \oplus \alpha_2 \mathcal{C}_2 \oplus \alpha_3 \mathcal{C}_3.$$

We have that

$$G = \begin{pmatrix} 1 & 0 & 0 & \alpha_0 + 2\alpha_1 + \alpha_3 & \alpha_0 + 2\alpha_1 + \alpha_2 + 4\alpha_3 \\ 0 & 1 & 0 & 2\alpha_0 + 2\alpha_1 + \alpha_2 + 2\alpha_3 & 4\alpha_1 + 2\alpha_2 + \alpha_3 \\ 0 & 0 & 1 & 2\alpha_2 & 3\alpha_0 + 2\alpha_3 \end{pmatrix}.$$

$$\text{Therefore, } G = \alpha_0 \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 3 \end{pmatrix} + \alpha_1 \begin{pmatrix} 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 2 & 4 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} +$$

$$+ \alpha_2 \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 2 & 0 \end{pmatrix} + \alpha_3 \begin{pmatrix} 1 & 0 & 0 & 1 & 4 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & 2 \end{pmatrix}, \text{ where}$$

$$G_0 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 3 \end{pmatrix} \text{ is the generator matrix for the linear code } \mathcal{C}_0,$$

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 2 & 4 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \text{ is the generator matrix for the linear code } \mathcal{C}_1,$$

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 2 & 0 \end{pmatrix} \text{ is the generator matrix for the linear code } \mathcal{C}_2,$$

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 4 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & 2 \end{pmatrix} \text{ is the generator matrix for the linear code } \mathcal{C}_3.$$

We remark that $d_H(\mathcal{C}_0) = 2$, $d_H(\mathcal{C}_1) = 1$, $d_H(\mathcal{C}_2) = d_H(\mathcal{C}_3) = 2$, therefore $d_H(\mathcal{C}) = 1$.

ii) We consider the linear code

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 3u^3 + 4u^2 + 3u + 1 & 4u^3 + u^2 + u + 3 \end{pmatrix},$$

$$\mathcal{C} = \alpha_0 \mathcal{C}_0 \oplus \alpha_1 \mathcal{C}_1 \oplus \alpha_2 \mathcal{C}_2 \oplus \alpha_3 \mathcal{C}_3.$$

We have that

$$G = \begin{pmatrix} 1 & 0 & 0 & \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 & \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 \\ 0 & 1 & 0 & \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 & 2\alpha_0 + 2\alpha_1 + 2\alpha_2 + 2\alpha_3 \\ 0 & 0 & 1 & \alpha_0 + \alpha_1 + 2\alpha_2 + 2\alpha_3 & 3\alpha_0 + 4\alpha_1 + \alpha_2 + 3\alpha_3 \end{pmatrix}.$$

$$\text{Therefore, } G = \alpha_0 \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{pmatrix} + \alpha_1 \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 4 \end{pmatrix} +$$

$$+ \alpha_2 \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 2 & 1 \end{pmatrix} + \alpha_3 \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 2 & 3 \end{pmatrix}, \text{ where}$$

$$G_0 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{pmatrix} \text{ is the generator matrix for the linear code } \mathcal{C}_0,$$

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 4 \end{pmatrix} \text{ is the generator matrix for the linear code } \mathcal{C}_1,$$

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 2 & 1 \end{pmatrix} \text{ is the generator matrix for the linear code } \mathcal{C}_2,$$

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 2 & 3 \end{pmatrix} \text{ is the generator matrix for the linear code } \mathcal{C}_3.$$

We remark that $d_H(\mathcal{C}_0) = d_H(\mathcal{C}_1) = d_H(\mathcal{C}_2) = d_H(\mathcal{C}_3) = 3$, therefore $d_H(\mathcal{C}) = 3$. This code is an MDS code (Maximum Distance Separable code).

Dual codes. i) For the dual code, we know that if the generator matrix G has the form $(I_3 \mid M)$, then the parity check matrix H is of the form $(-M^t \mid I_2)$. Since $G_0 =$

$$(I_3 \mid M_0), \text{ we obtain } H_0 = \begin{pmatrix} 4 & 3 & 0 & 1 & 0 \\ 4 & 0 & 2 & 0 & 1 \end{pmatrix}. \text{ From } G_1 = \begin{pmatrix} 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 2 & 4 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix},$$

$$\text{we get } H_1 = \begin{pmatrix} 3 & 3 & 0 & 1 & 0 \\ 3 & 1 & 0 & 0 & 1 \end{pmatrix}; \text{ to } G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 2 & 0 \end{pmatrix} \text{ it corresponds to}$$

$$H_2 = \begin{pmatrix} 0 & 4 & 3 & 1 & 0 \\ 4 & 3 & 0 & 0 & 1 \end{pmatrix} \text{ and for } G_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 4 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & 2 \end{pmatrix}, \text{ we obtain}$$

$$H_3 = \begin{pmatrix} 4 & 3 & 0 & 1 & 0 \\ 1 & 4 & 3 & 0 & 1 \end{pmatrix}. \text{ Therefore, the matrix of the dual code } \mathcal{C}^\perp \text{ is}$$

$$H = \begin{pmatrix} 4u_0 + 3u_1 + 4u_3 & 3u_0 + 3u_1 + 4u_2 + 3u_3 & 3u_2 & 1 & 0 \\ 4u_0 + 3u_1 + 4u_2 + u_3 & u_1 + 3u_2 + 4u_3 & 2u_0 + 3u_3 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 4u^3 + 2u^2 + 3u + 4 & 2u^3 + 2u^2 + u + 3 & u^3 + u^2 + 3u & 1 & 0 \\ 4u_0 + 3u_1 + 4u_2 + u_3 & 3u^3 + 4u^2 + 4u & u^3 + 3u^2 + 4u + 2 & 0 & 1 \end{pmatrix}.$$

ii) In this case, for the dual code, we obtain: for G_0 , we have $H_0 = \begin{pmatrix} 4 & 4 & 4 & 1 & 0 \\ 4 & 3 & 2 & 0 & 1 \end{pmatrix}$; for G_1 , we obtain $H_1 = \begin{pmatrix} 4 & 4 & 4 & 1 & 0 \\ 4 & 3 & 1 & 0 & 1 \end{pmatrix}$; for G_2 , it results $H_2 = \begin{pmatrix} 4 & 4 & 3 & 1 & 0 \\ 4 & 3 & 4 & 0 & 1 \end{pmatrix}$; for G_3 , we get $H_3 = \begin{pmatrix} 4 & 4 & 3 & 1 & 0 \\ 4 & 3 & 2 & 0 & 1 \end{pmatrix}$.

Therefore, the matrix of the dual code $\mathcal{C}^\perp$ is

$$H = \begin{pmatrix} 4\alpha_0 + 4\alpha_1 + 4\alpha_2 + 4\alpha_3 & 4\alpha_0 + 4\alpha_1 + 4\alpha_2 + 4\alpha_3 & 4\alpha_0 + 4\alpha_1 + 3\alpha_2 + 3\alpha_3 & 1 & 0 \\ 4\alpha_0 + 4\alpha_1 + 4\alpha_2 + 4\alpha_3 & 3\alpha_0 + 3\alpha_1 + 3\alpha_2 + 3\alpha_3 & 2\alpha_0 + \alpha_1 + 4\alpha_2 + 2\alpha_3 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 4 & 4 & 2u^3 + u^2 + 2u + 4 & 1 & 0 \\ 4 & 3 & u^3 + 4u^2 + 4u + 2 & 0 & 1 \end{pmatrix}.$$

A cyclic code of length 4 over the ring $R_{4,5}$. We have that $x^4 - 1 = (x - 1)(x - 2)(x - 3)(x - 4)$. We consider $g_0(x) = x - 2$, $g_1(x) = x - 3$, $g_2(x) = (x - 1)(x - 2) = x^2 - 3x + 2$, $g_3(x) = (x - 4)$. Therefore, the generator polynomial for the code $\mathcal{C}$ is

$$\begin{aligned} g(x) &= \alpha_0 g_0(x) + \alpha_1 g_1(x) + \alpha_2 g_2(x) + \alpha_3 g_3(x) = \\ &= (2u^3 + 2u^2 + u)x^2 + (2u^3 + 2u^2 + u + 1)x + (3u^3 + 4u^2 + 2u + 3). \end{aligned}$$

A cyclic code of length 5 over the ring $R_{4,5}$. We have $x^5 - 1 = (x - 1)^5 \pmod{5}$. We consider $g_0(x) = x - 1 = x + 4$, $g_1(x) = (x - 1)^3 = x^3 + 2x^2 + 3x + 4$, $g_2(x) = (x - 1)^2 = x^2 + 3x + 1$, $g_3(x) = (x - 1)^4 = x^4 + x^3 + x^2 + x + 1$. Therefore, the generator polynomial for the code $\mathcal{C}$ is

$$g(x) = (u^3 + 2u^2 + 2u)x^4 + (4u^3 + 2u^2)x^3 + (4u^3 + 4u^2 + 4u)x^2 + (4u^2 + 3u + 1)x + (u^3 + 3u^2 + u + 4).$$

4. Conclusions and future work

Studying linear and cyclic codes over finite rings has led to efficient codes with optimal parameters. The algebraic properties of finite rings make it easy to adapt algorithms to different noisy channels, improving real-time error correction. By using ideals in polynomial rings, cyclic codes keep hardware implementation very simple and fast. These mathematical structures remain essential for secure data storage.

Looking ahead, the development of codes over finite rings allowed the expansion of several cutting-edge domains (post-quantum cryptography integration, advanced wireless and space communications), which emphasize their continued relevance in the modern digital era.

Acknowledgement. The authors thank anonymous reviewers for their valuable comments and suggestions, which greatly improved the quality of this paper.

Disclosure statement. The authors report that there are no competing interests to declare.

References

- [1] A. A. de Andrade and R. Palazzo, Jr., *Linear codes over finite rings*, TEMA Tend. Mat. Apl. Comput., 6(2) (2005), 207-217.
- [2] M. Greferath, A. Nechaev and R. Wisbauer, *Finite quasi-Frobenius modules and linear codes*, J. Algebra Appl., 3(3) (2004), 247-272.

- [3] T. Honold, *Characterization of finite Frobenius rings*, Arch. Math. (Basel), 76(6) (2001), 406-415.
- [4] F. Ma, J. Gao and F.-W. Fu, *Constacyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ and their applications of constructing new non-binary quantum codes*, Quantum Inf. Process., 17(6) (2018), 122 (19 pp).
- [5] K. McCrimmon, *A Taste of Jordan Algebras*, Universitext, Springer-Verlag, New York, 2004.
- [6] M. Sari and I. Siap, *On quantum codes from cyclic codes over a class of nonchain rings*, Bull. Korean Math. Soc., 53(6) (2016), 1617-1628.
- [7] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math., 121(3) (1999), 555-575.
- [8] S. Zhu, Y. Wang and M. Shi, *Some results on cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$* , IEEE Trans. Inform. Theory, 56(4) (2010), 1680-1684.

Cristina Flaut (Corresponding Author)

Faculty of Mathematics and Computer Science

Ovidius University of Constanța, România

Bd. Mamaia 124, 900527, Constanța

e-mail: cflaut@univ-ovidius.ro; cristina_flaut@yahoo.com

Bianca Liana Bercea-Straton

Doctoral School of Mathematics

Ovidius University of Constanța, România

Bd. Mamaia 124, 900527, Constanța

e-mail: biancaliana99@yahoo.com