



Cyclic Codes over a Non-Local Non-Unital Ring

Adel Alahmadi, Malak Altairy, Patrick Solé

► To cite this version:

Adel Alahmadi, Malak Altairy, Patrick Solé. Cyclic Codes over a Non-Local Non-Unital Ring. Mathematics, 2024, 10.3390/math12060866 . hal-04506243

HAL Id: hal-04506243

<https://hal.science/hal-04506243>

Submitted on 15 Mar 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Article

Cyclic Codes over a Non-Local Non-Unital Ring

Adel Alahmadi ^{1,*} , Malak Altairy ^{1,2} and Patrick Solé ³ ¹ Research Group of Algebraic Structures and Applications, Mathematics Department, Faculty of Science, King Abdulaziz University, Jeddah 21589, Saudi Arabia; m_altairy@su.edu.sa² Math Department, Shaqra University, Shaqra 11961, Saudi Arabia³ I2M Lab (CNRS, Aix Marseille University, Centrale Marseille), 13009 Marseilles, France; sole@enst.fr

* Correspondence: analahmadi@kau.edu.sa

Abstract: We study cyclic codes over the ring H of order 4 and characteristic 2 defined by generators and relations as $H = \langle a, b \mid 2a = 2b = 0, a^2 = 0, b^2 = b, ab = ba = 0 \rangle$. This is the first time that cyclic codes over a non-unital ring are studied. Every cyclic code of length n over H is uniquely determined by the data of an ordered pair of binary cyclic codes of length n . We characterize self-dual, quasi-self-dual, and linear complementary dual cyclic codes H . We classify cyclic codes of length at most 7 up to equivalence. A Gray map between cyclic codes of length n over H and quasi-cyclic codes of length $2n$ over \mathbb{F}_2 is studied.

Keywords: non-unital rings; cyclic codes; self-orthogonal codes

MSC: 94 B15; 16 D10



Citation: Alahmadi, A.; Altairy, M.; Solé, P. Cyclic Codes over a Non-Local Non-Unital Ring. *Mathematics* **2024**, *12*, 866. <https://doi.org/10.3390/math12060866>

Academic Editor: Jonathan Blackledge

Received: 16 September 2023

Revised: 17 October 2023

Accepted: 19 October 2023

Published: 15 March 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Cyclic codes over finite fields [1,2] and finite rings [3–9] constitute the most popular class of algebraic codes for many reasons, both practical and theoretical. Their clean algebraic structure enables the practitioner to use efficient encoding and decoding techniques [10,11]. It also permits the theoretician to derive strong lower bounds on the minimum distance (BCH, Hartmann–Tzeng, van Lint/Wilson, Roos) [1,12–14]. At the heart of this popularity lies the quotient ring $A[x]/(x^n - 1)$, where x is a formal variable and A the code alphabet (a finite ring). Ideals in this ring are in one-to-one correspondence with cyclic codes of length n over A . This ring is principal and every ideal admits a monic generator, say, $g(x)$. The roots of $g(x)$ allow for the computation of various bounds on the minimum distance. The dual of such a code is generated by the quotient of $x^n - 1$ by $g(x)$. In recent years, a theory of codes over non-unital rings emerged [15–17]. The absence of a unit element for the multiplication forbids the researcher investigating cyclic codes over a non-unital ring A to use the auxiliary ring $A[x]/(x^n - 1)$, simply because $x^n - 1$ is not available in $A[x]$. In such a case, alternative strategies have to be derived. In this paper we study the fundamental algebraic properties (generation, duality) of cyclic codes over a special non-unital ring without any polynomial formalism.

In particular, we investigate cyclic codes over the non-unital ring H in the classification of Rhagavendran [18] and the notation of Fine [19]. This ring is semi-local with two maximal ideals. Essentially, every cyclic code over H can be regarded as an ordered pair of binary cyclic codes of the same length. This structure theorem is used to characterize self-dual, quasi-self-dual, and linear complementary dual (LCD) cyclic codes over H . It is also used to classify isomorphism classes of cyclic codes of given length up to length 7. A Gray map between codes of length n over H and codes of length $2n$ over \mathbb{F}_2 is introduced. The Gray image of a cyclic code is proved to be quasi-cyclic of index 2.

The material is organized as follows. The next section collects basic notations and notions needed for the other sections. Section 3 considers the structure of cyclic codes over H . Section 4 studies the Gray map of cyclic code over H , Section 5 investigates the automorphism group of a cyclic code, and Section 6 applies this information to classifying

cyclic codes of a given length up to permutation. Section 7 derives conditions for LCD-ness. Section 8 contains numerical examples. Section 9 concludes this article.

2. Preliminaries

2.1. Binary Codes

The Hamming weight of $x \in \mathbb{F}_2^n$ is denoted by $wt(x)$. The dual of a binary linear code C is signified by C^\perp and defined as :

$$C^\perp = \{y \in \mathbb{F}_2^n \mid \forall x \in C, (x, y) = 0\},$$

where $(x, y) = \sum_{i=1}^n x_i y_i$, denotes the standard inner product. A code C is **self-orthogonal** if it is included in its dual: $C \subseteq C^\perp$. A code is **even** if all its code words have even weight. All binary self-orthogonal codes are even, but not all even binary codes are self-orthogonal. Two binary codes are **equivalent** if there is a permutation of coordinates that maps one to the other.

A linear code C of length n over \mathbb{F}_2 is cyclic provided that, for each vector $c = (c_0 \dots c_{n-2} c_{n-1})$ in C , the vector $c_{n-1} c_0 \dots c_{n-2}$, obtained from c by the cyclic shift of coordinates $i \mapsto i + 1 \pmod{n}$, is also in C .

2.2. Rings and Modules

Following [19], we define a ring on two generators a, b by their relations

$$H = \langle a, b \mid 2a = 2b = 0, a^2 = 0, b^2 = b, ab = ba = 0 \rangle.$$

Thus, H has characteristic 2 and consists of four elements $H = \{0, a, b, c\}$, with $c = a + b$. The addition table is immediate from these definitions

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

The multiplication table is as follows.

×	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	0	b	b
c	0	0	b	b

From this table, we deduce that this ring is commutative and that it does not have an unity element for the multiplication. Two absorbing elements are 0 and a . It is semi-local with two maximal ideals, $J_a = \{0, a\}$ and $J_b = \{0, b\}$. Denote by $\alpha_a : H \mapsto \mathbb{F}_2$ the reduction map with respect to J_a , and by $\alpha_b : H \mapsto \mathbb{F}_2$ is the map of reduction map with respect to J_b . Thus, $\alpha_a(a) = \alpha_b(b) = 0$, and $\alpha_a(b) = \alpha_b(a) = 1$. Note that these two applications are morphisms for addition but for not multiplication. They can be extended in the obvious way into maps from H^n to \mathbb{F}_2^n . This ring decomposition induces a code decomposition in the following way. The code C over H can be written as a direct sum (in the sense of modules)

$$C = aC_a \oplus bC_b,$$

where $C_a = \alpha_b(C)$ and $C_b = \alpha_a(C)$. Sometimes we will use the inner product notation (x, r) for $x \in \mathbb{F}_2^n, r \in H^n$ to mean

$$(x, r) = \sum_{i=1}^n x_i r_i = \sum_{x_i=1} r_i.$$

A linear H -code C of length n is an H -submodule of H^n . It can be regarded as the H -span of the rows of a generator matrix. With that code, we attach two binary codes of length n : $\alpha_a(C)$ and $\alpha_b(C)$. An additive code of length n over \mathbb{F}_4 is an additive subgroup of \mathbb{F}_4^n . It is an \mathbb{F}_2 vector space of size 4^k elements for some $k \leq n$. Using a generator matrix G , such a code can be cast as the \mathbb{F}_2 -span of the rows of G . With every linear H -code C we associate an additive \mathbb{F}_4 -code $\phi_H(C)$ by the alphabet substitution

$$0 \rightarrow 0, a \rightarrow \omega, b \rightarrow 1, c \rightarrow \omega^2,$$

where $\mathbb{F}_4 = \mathbb{F}_2[\omega]$, extended in the obvious way to \mathbb{F}_4^n .

We use the notation of the Magma package [20]

$$[< 0, 1 >, \dots, < i, A_i >, \dots, < n, A_n >]$$

for the weight distribution of a code, where A_i is the number of code words of weight i . Two H -codes are permutation-equivalent if there is a permutation of coordinates that maps one to the other.

Equip H^n with an inner product by the rule $(x, y) = \sum_{i=1}^n x_i y_i$. The dual C^\perp of C is the module defined by

$$C^\perp = \{y \in H^n \mid \forall x \in C, (x, y) = 0\}.$$

Thus, the dual of a module is a module. A code is self-dual if it is equal to its dual.

A code C is self-orthogonal if $\forall x, y \in C, (x, y) = 0$.

3. The Structure of Cyclic Codes over H

Definition 1. A cyclic code C of length n over H is a linear code with property that if $c = (c_0, c_1, \dots, c_{n-1}) \in C$ then $\sigma(c) = (c_{n-1}, c_0, \dots, c_{n-2}) \in C$.

Example 1. The repetition code of length 2, defined by $R_2 = \{00, aa, bb, cc\}$ is a cyclic code over H .

The dual of R_2 is defined by $R_2^\perp = \{00, aa, bb, cc, cb, bc, a0, 0a\}$. It is also a cyclic code over H .

Example 2. Let $C = aC_a \oplus bC_b$, where C_a and C_b are binary codes generated by the matrix

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Then C is a cyclic code of length 3 over H such that $C_a = \{000, 101, 110, 011\} = C_b$.
 $\Rightarrow |C_a| = 4$ and $|C_b| = 4$. Hence, $|C| = |C_a||C_b| = 4^2 = 16$.

Then $C = \{000, a0a, aa0, 0aa, b0b, bb0, 0bb, c0c, cc0, 0cc, cba, abc, cab, acb, bac, bca\}$.

The following result is of crucial importance to our study.

Theorem 1. If $C = aC_a \oplus bC_b$ is an arbitrary linear code over H , then C is a cyclic code if and only if C_a and C_b are both cyclic.

Proof. (\Rightarrow) Let T be the permutation matrix corresponding to the shift.

It can be seen that T commutes with both α_a and α_b . We know $TC \subseteq C$.

Hence, $\alpha_a(TC) = T\alpha_a(C) \subseteq \alpha_a(C)$. This implies that $C_b = \alpha_a(C)$ is cyclic.

Same argument with $C_a = \alpha_b(C)$.

(\Leftarrow) Suppose that C_a and C_b are both cyclic. We want to prove that C is cyclic.

Let $C = ac_1 + bc_2$ be an arbitrary code word in C where $c_1 = (x_0, x_1, \dots, x_{n-1}) \in C_a$ and $c_2 = (y_0, y_1, \dots, y_{n-1}) \in C_b$.

We need to prove that $c' = ac_1' + bc_2' \in C$. Then

$$\begin{aligned} c &= a(x_0, x_1, \dots, x_{n-1}) + b(y_0, y_1, \dots, y_{n-1}) \\ &= (ax_0 + by_0, ax_1 + by_1, \dots, ax_{n-1} + by_{n-1}) \end{aligned} \quad (1)$$

As C_a and C_b are both cyclic, then $c_1' = (x_{n-1}, x_0, \dots, x_{n-2}) \in C_a$ and $c_2' = (y_{n-1}, y_0, \dots, y_{n-2}) \in C_b$.

Hence, (1) will become

$$\begin{aligned} c' &= (ax_{n-1} + by_{n-1}, ax_0 + by_0, \dots, ax_{n-2} + by_{n-2}) \\ &= a(x_{n-1}, x_0, \dots, x_{n-2}) + b(y_{n-1}, y_0, \dots, y_{n-2}) \in C \end{aligned}$$

Hence, we proved C is a cyclic code over H . \square

To derive more corollaries of Theorem 1, we require some definitions pertaining to the duality of H -codes.

Definition 2.

- A code of length n is *quasi-self-dual* if it is self-orthogonal and of size 2^n .
- A quasi-self-dual code over H with all weights even is called a *Type IV* code.
- A QSD H -code is called *quasi-Type IV QT4* if C_a is an even code.
- A linear code C is called an *LCD code* (Linear Complementary Dual Code) if $C \cap C^\perp = 0$.

For LCD codes over finite fields see [21].

Corollary 1. A code C of length n over H is cyclic QSD if and only if:

1. C_b is a cyclic self-orthogonal $[n, k]$ binary code.
2. C_a is a cyclic $[n, n-k]$ binary code.

Proof. By combining Theorem 1 and [15] (Lemma 1) we obtain the proof. \square

Corollary 2. A code C over H is cyclic Type IV if C_b is a cyclic self-orthogonal binary code and $C_a = C_b^\perp$.

Proof. By combining Theorem 1 and [15] (Theorem 5) we obtain the result. \square

Corollary 3. Every cyclic QT4 code of length n over H is of the form $aC_a \oplus bC_b$ where:

1. C_b is a cyclic self-orthogonal $[n, k]$ binary code.
2. C_a is an even cyclic binary $[n, n-k]$ code.

Proof. By combining Theorem 1 and [15] (Lemma 2) we obtain the proof. \square

Corollary 4. Let C be a cyclic code over H , then C is an LCD cyclic code if and only if C_b is LCD cyclic and $C_a = \{0\}$.

Proof. By combining Theorem 1 and [22] (Theorem 5.11) we obtain the result. \square

To prepare for the study of self-dual cyclic codes over H , we need the following theorem. The proof is omitted.

Theorem 2 ([22] (Theorem 22)). Let C^\perp be the dual code of C over H . Then $C^\perp = a\mathbb{F}_2^n \oplus bC_b^\perp$.

The next result follows.

Corollary 5. If C is a cyclic code over H , then the dual code C^\perp of C is also cyclic.

Proof. By Theorem 2, we have $C^\perp = a\mathbb{F}_2^n \oplus bC_b^\perp$. Since the dual code of binary cyclic code is also cyclic, by Theorem 1 and the fact that \mathbb{F}_2^n is a cyclic code, we obtain the result. \square

In the next results, we study the additive code of cyclic codes over H .

Corollary 6. *If C is cyclic code over H , then the additive code $\phi_H(C)$ is also cyclic.*

Proof. The proof is direct from Theorem 1. \square

Corollary 7. *If the binary code $\phi_H(C)$ is cyclic, then $\phi_H(C^\perp)$ is also cyclic.*

Proof. By combining Corollary 5 and Corollary 6, we obtain the proof. \square

If C is a cyclic code of length n over H , then the relation $\phi_H(C^\perp) = \phi_H(C)^\perp$ is not true in general as the following example shows.

Example 3. Let $C = \{00, bb\}$ be a cyclic code of length 2 over H then the dual of C is $C^\perp = \{00, aa, bb, cc, cb, bc, a0, 0a\}$ and $\phi_H(C) = \{00, 11\}$.

$$\phi_H(C^\perp) = \{00, \omega\omega, 11, \omega^2\omega^2, \omega^21, 1\omega^2, \omega0, 0\omega\} \text{ and}$$

$$\phi_H(C)^\perp = \{00, 10, \omega^2\omega, \omega\omega, \omega\omega^2, \omega^2\omega^2, 11, 01\}.$$

4. Gray Map

Any code word of H can be expressed as $c = ax + by$, where a, b are generators for the ring H and x, y are arbitrary elements in \mathbb{F}_2 . The Lee weights of $0, a, b, c \in H$ are 0, 1, 1, 2, respectively. The **Gray map** from H to $\mathbb{F}_2 \times \mathbb{F}_2$ is given by $\Psi(c) = (x, y)$. The Gray map is a bijection. This map can be extended to H^n in a natural way. For any $s = (s_0, s_1, \dots, s_{n-1}) \in H^n$, where $s_i = au_i + bv_i, 0 \leq i \leq n-1$, we define $\Psi(s) = (u(s), v(s))$, where $u(s) = (u_0, u_1, \dots, u_{n-1}), v(s) = (v_0, v_1, \dots, v_{n-1})$.

Then Ψ is a weight-preserving map from $(H^n, \text{Lee weight})$ to $(\mathbb{F}_2^{2n}, \text{Hamming weight})$, that is, $w_L(s) = w_H(\Psi(s))$.

Example 4. Let $C = aC_a \oplus bC_b$, where C_a and C_b are binary codes generated by $G_a = \begin{pmatrix} 1 & 1 \end{pmatrix}$ and $G_b = \begin{pmatrix} 1 & 1 \end{pmatrix}$, then $C_a = \{00, 11\} = C_b$. Therefore, $C = \{00, aa, bb, cc\}$ and we can write the code C as $C = \{a(00) + b(00), a(11) + b(00), a(00) + b(11), a(11) + b(11)\}$. Hence, $\Psi(C) = \{0000, 1100, 0011, 1111\}$.

The following result characterizes the Gray image of an H -code as a function of its two binary components.

Theorem 3. *Let C be a linear code of length n over H . Then $\Psi(C) = C_a \oplus C_b$.*

Proof. For any $(u_0, u_1, \dots, u_{n-1}, v_0, v_1, \dots, v_{n-1}) \in \Psi(C)$, let $c_i = au_i + bv_i, i = 0, 1, \dots, n-1$. Since Ψ is bijection, $c = (c_0, c_1, \dots, c_{n-1}) \in C$. By the definition of C , we obtain that $(u_0, u_1, \dots, u_{n-1}) \in C_a, (v_0, v_1, \dots, v_{n-1}) \in C_b$; therefore, $(u_0, u_1, \dots, u_{n-1}, v_0, v_1, \dots, v_{n-1}) \in C_a \oplus C_b$. This implies that $\Psi(C) \subseteq C_a \oplus C_b$.

On the other hand, for any $(u_0, u_1, \dots, u_{n-1}, v_0, v_1, \dots, v_{n-1}) \in C_a \oplus C_b$ where $(u_0, u_1, \dots, u_{n-1}) \in C_a, (v_0, v_1, \dots, v_{n-1}) \in C_b$. Since C is linear, we have $c = au_i + bv_i \in C$, and it follows that $\Psi(c) = (u_0, u_1, \dots, u_{n-1}, v_0, v_1, \dots, v_{n-1})$, which gives $C_a \oplus C_b \subseteq \Psi(C)$. Therefore, $\Psi(C) = C_a \oplus C_b$. \square

As a consequence, we characterize the Gray image of the dual code.

Corollary 8. *Let C be a linear code of length n over H and $\Psi(C) = C_a \oplus C_b$ then $\Psi(C^\perp) = F_2^n \oplus C_b^\perp$.*

Proof. It follows directly from Theorem 2. \square

Proposition 1. Let d_H and d_L be the minimum Hamming and Lee weights of a linear code C over H , respectively. Then, $d_H = d_L = \min\{d(C_a), d(C_b)\}$, where $d(C_a)$ and $d(C_b)$ denote the minimum weight of a binary code C_a and C_b , respectively.

Proof. Since Ψ is a weight-preserving map, then $d_L(C) = d_H(\Psi(C)) = d_H(C_a \oplus C_b) = \min\{d(C_a), d(C_b)\}$, and $d_H = d_L$ is obvious. \square

To prepare for the study of the relation between Gray map and duality, we need the following Corollary and the following Proposition.

Corollary 9 ([22] (Corollary 24)). Let $C = aC_a \oplus bC_b$ be a linear code of length n over H . Then C is nice if and only if $C_a = \{0\}$.

Proposition 2. Let C^\perp be the dual code of C over H . If C is a nice code over H , then $\Psi(C^\perp) = \Psi(C)^\perp$. Moreover, if C is a self-orthogonal code, so $\Psi(C)$.

Proof. (\subseteq) For any $c_1 = au_1 + bv_1 \in C$, $c_2 = au_2 + bv_2 \in C^\perp$ where $u_1, u_2, v_1, v_2 \in F_2^n$. Since $c_1 \cdot c_2 = 0$ implies $b(v_1 \cdot v_2) = 0$, thus we can obtain that $\Psi(c_1) \cdot \Psi(c_2) = (u_1, v_1) \cdot (u_2, v_2) = u_1u_2 + v_1v_2 = 0$, which means $\Psi(C^\perp) \subseteq \Psi(C)^\perp$.

(\supseteq) Let $\Psi(c_1) = \Psi(au_1 + bv_1) = (u_1, v_1) \in \Psi(C)$ and $\Psi(c_2) = \Psi(au_2 + bv_2) = (u_2, v_2) \in \Psi(C)^\perp$ where $u_1, u_2, v_1, v_2 \in F_2^n$. Since $\Psi(c_1) \cdot \Psi(c_2) = 0$ implies $u_1u_2 + v_1v_2 = 0$, thus we can obtain that $c_1 \cdot c_2 = a^2u_1u_2 + abu_1v_2 + bau_2v_1 + b^2v_1v_2 = 0 + 0 + 0 + b(v_1 \cdot v_2) = 0$, which means $\Psi(C)^\perp \subseteq \Psi(C^\perp)$. Hence, $\Psi(C^\perp) = \Psi(C)^\perp$. \square

Proposition 3. If C is an LCD code over H then $\Psi(C)$ is also an LCD code over F_2 .

Proof. Since C is an LCD code over H then we have $C \cap C^\perp = \{0\}$ and C_a is nice. We want to prove that $\Psi(C) \cap \Psi(C)^\perp = \{0\}$.

Consider,

$$\begin{aligned} \{0\} &= \Psi(0) \\ &= \Psi(C \cap C^\perp) \\ &= \Psi(C) \cap \Psi(C^\perp) \text{ because } \Psi \text{ is a bijection} \\ &= \Psi(C) \cap \Psi(C)^\perp \text{ by Proposition 2} \end{aligned}$$

Hence, $\Psi(C)$ is an LCD code over H . \square

To prepare for the study of the symmetry of Gray images, we need the following Definition.

Definition 3. Let φ_s be the quasi-cyclic shift on $(F_2^n)^s$ given by:

$\varphi_s(x^{(1)}|x^{(2)}|\dots|x^{(s)}) = (\sigma(x^{(1)})|\sigma(x^{(2)})|\dots|\sigma(x^{(s)}))$. A quasi-cyclic code C of index s and length ns over F_2 is a subset of $(F_2^n)^s$ such that $\varphi_s(C) = C$, where σ is the cyclic shift in length n .

Corollary 10. If C is a cyclic code of length n over H , then $\Psi(C)$ is a binary quasi-cyclic code of index 2 and length $2n$.

Proof. It follows directly from the definition of quasi-cyclic codes. \square

5. Automorphism Group

Let C be a linear code of length n over H and σ a permutation of the symmetric group S_n acting on $\{0, 1, \dots, n-1\}$. We associate with this code a linear code $\sigma(C)$ defined by:

$$\sigma(C) = \left\{ (x_{\sigma^{-1}(0)}, \dots, x_{\sigma^{-1}(n-1)}) | (x_0, \dots, x_{n-1}) \in C \right\}$$

We say that the code C and C' are equivalent if there exists a permutation $\sigma \in S_n$ such that $C' = \sigma(C)$.

The automorphism group of C is the subgroup of S_n given by:

$$\text{Aut}(C) = \{\sigma \in S_n \mid \sigma(C) = C\}.$$

Example 5. Let $C = aC_a \oplus bC_b$, where C_a and C_b are binary codes generated by the matrix

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Then C is a linear cyclic code of length 3 over H such that $C_a = \{000, 101, 110, 011\} = C_b$. Consider $\sigma = (1, 3)$ then a generator matrix will become $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ and we obtain $C_a = \{000, 101, 110, 011\} = C_b$. Therefore, $\sigma(C) = C$. So $\sigma \in \text{Aut}(C)$.

Example 6. Let $C = aC_a \oplus bC_b$ where C_a and C_b are binary codes generated by the matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Then C is a cyclic code of length 7 over H , where

$$C_a = \{0000000, 1011100, 0101110, 0010111, 1110010, 0111001, 1001011, 1100101\} = C_b.$$

And let $C' = aC'_a \oplus bC'_b$, where C'_a and C'_b are binary codes generated by the matrix

$$G' = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Then C' is a cyclic code of length 7 over H , where

$$C'_a = \{0000000, 1110100, 0111010, 0011101, 10011100, 0100111, 1101001, 1010011\} = C'_b.$$

Hence, $\sigma(C) = C'$ where $\sigma = (264)(35)$. Therefore, C and C' are equivalent codes.

The following result shows the relationship between the equivalence of two linear codes over H and that of their constituents.

Lemma 1. Let $C = aC_a \oplus bC_b$ and $C' = aC'_a \oplus bC'_b$ be two codes over H . Then C and C' are equivalent if and only if there exists a permutation $\sigma \in S_n$ such that $\sigma(C_a) = C'_a$ and $\sigma(C_b) = C'_b$.

Proof. The first direction: If C and C' are equivalent, then $C' = \sigma(C)$

$$\begin{aligned} aC'_a \oplus bC'_b &= \sigma(aC_a \oplus bC_b), \\ &= \sigma(aC_a) \oplus \sigma(bC_b), \\ &= a\sigma(C_a) \oplus b\sigma(C_b). \end{aligned}$$

By taking α_a and α_b for both sides, we obtain: $\sigma(C_a) = C'_a$ and $\sigma(C_b) = C'_b$.

Conversely, suppose that there exists a permutation $\sigma \in S_n$ such that $\sigma(C_a) = C'_a$ and $\sigma(C_b) = C'_b$. Then, we can write:

$$\begin{aligned} \sigma(C) &= \sigma(aC_a \oplus bC_b), \\ &= \sigma(aC_a) \oplus \sigma(bC_b), \\ &= a\sigma(C_a) \oplus b\sigma(C_b), \\ &= aC'_a \oplus bC'_b, \\ &= C'. \end{aligned}$$

Hence, C and C' are equivalent. \square

As consequences from the previous lemma, we derive the following two results.

Proposition 4. Let $C = aC_a \oplus bC_b$ and $C' = aC'_a \oplus bC'_b$ be two self-dual codes over H . Then C and C' are equivalent if and only if there exists a permutation $\sigma \in S_n$ such that $\sigma(C_b) = C'_b$.

Proof. By combining Theorem 2 and Lemma 1, we obtain the proof. \square

Proposition 5. Let $C = aC_a \oplus bC_b$ and $C' = aC'_a \oplus bC'_b$ be two LCD codes over H . Then C and C' are equivalent if and only if there exists a permutation $\sigma \in S_n$ such that $\sigma(C_b) = C'_b$.

Proof. By combining Corollary 4 and Lemma 1, we obtain the proof. \square

6. Classification

The following characterization result is easy but essential to understand the classification technique.

Lemma 2. A code C of length n over H is cyclic if and only if it is of the form $aC_a \oplus bC_b$ where:

- C_a is a cyclic $[n, k_1]$ binary code.
- C_b is a cyclic $[n, k_2]$ binary code.

Proof. The proof is obtained directly from Theorem 1. \square

To classify cyclic codes, we thus have to find all codes that are permutation-equivalent to $aC_a \oplus bC_b$ for a given pair (C_a, C_b) . This is a similar situation to the classification of self-dual codes over Z_{pq} and we follow the method there. Here, SDR stands for System of Distinct Representatives of cyclic code, that is to say, elements that are representative of subsets (here the double cosets) in a set (here the group S_n) partition. The following result is an immediate generalization of [23] (Theorem 3.5) from Z_{pq} to H . Its proof is omitted.

Theorem 4 ([15] (Theorem 6)). Let (C_a, C_b) be a pair of codes as defined in Lemma 1, with respective permutation groups A and B . Then, the set

$$S_{C_a, C_b} := \{aC_a \oplus b\sigma(C_b) \mid \sigma \text{ runs over a SDR of } A \backslash S_n / B\}.$$

forms a set of non-equivalent codes. In particular, $|S_{C_a, C_b}| = |A \backslash S_n / B|$.

The immediate application is the next result.

Corollary 11. Let L_a be the set of all non-equivalent $[n, k_1]$ cyclic binary codes. Let L_b be the set of all non-equivalent $[n, k_2]$ cyclic binary codes. Then, the set of all cyclic codes over H is, up to permutation, the disjoint union $\bigsqcup_{\substack{C_a \in L_a \\ C_b \in L_b}} S_{C_a, C_b}$.

Proof. By application of the maps α_a and α_b , the following observation is immediate. If the pairs C_a, C_b and C'_a, C'_b are distinct, then none of the codes in S_{C_a, C_b} are equivalent to any of the codes in $S_{C'_a, C'_b}$. \square

7. LCD Cyclic Codes over H

We prepare for the main result of this section by recalling some results on binary cyclic codes.

Definition 4. A linear code C of length n over H is said to be reversible if for any code word $c = (c_0, c_1, \dots, c_{n-1}) \in C$ implies $c^r = (c_{n-1}, c_{n-2}, \dots, c_1, c_0) \in C$.

Lemma 3 ([24]). If C_b is an $[n, k]$ cyclic code over \mathbb{F}_2 with generator polynomial $g(x)$ then it is an LCD code if and only if $g(x) = \tilde{g}(x)$ and all the monic irreducible factors of $g(x)$ have the same multiplicity in $x^n - 1$ and $g(x)$. In particular, for $\gcd(n, 2) = 1$, C_b is an LCD code if and only if it is a reversible code.

Lemma 4 ([25] (Theorem 1)). Let C_b be a cyclic code over a finite field \mathbb{F}_2 having generator polynomial $g(x)$. Then C_b is a reversible code if and only if $g(x) = \tilde{g}(x)$.

Proposition 6 ([22]). Let $C = aC_a \oplus bC_b$ be any linear code of length n over H . Then C is LCD if and only if C_b is LCD and $C_a = \{0\}$.

Corollary 12. Let $C = aC_a \oplus bC_b$ be a cyclic code of arbitrary length n over H . Then C is LCD if and only if $C_a = \{0\}$ and the generator polynomial $g(x)$ of C_b is self-reciprocal and the multiplicity of each monic irreducible factor of $g(x)$ is the same in $g(x)$ and $x^n - 1$.

Proof. It follows from Lemma 3 and Proposition 6. \square

Theorem 5. Let n be an odd positive integer and $C = aC_a \oplus bC_b$ be a cyclic code over H of length n . Then C is LCD if and only if C_b is reversible and $C_a = \{0\}$.

Proof. Let C be an LCD over H . Then C_b is LCD over \mathbb{F}_2 i.e., C_b is a reversible code over \mathbb{F}_2 by Lemma 3. Hence, $C = aC_a \oplus bC_b$ is also a reversible code over H .

Conversely, let C be a reversible code over H . Then $c = a\{0\} + by \in C$ implies that $c^r \in C$ where $y = (y_0, y_1, \dots, y_{n-1}) \in C_b$. We can write

$$\begin{aligned} c^r &= (a \cdot 0 + by_0, a \cdot 0 + by_1, \dots, a \cdot 0 + by_{n-1})^r \\ &= (a \cdot 0 + by_{n-1}, a \cdot 0 + by_{n-2}, \dots, a \cdot 0 + by_1, a \cdot 0 + by_0) \\ &= a\{0\} + by^r. \end{aligned}$$

This implies that C_b is reversible over \mathbb{F}_2 and LCD over \mathbb{F}_2 also. Therefore, C is LCD over H . \square

In the following example we will show an LCD cyclic code over H .

Example 7. The code $C = \{000, bbb\}$ of length 3 over H is an LCD cyclic where $C_a = \{0\}$ and C_b is generated by $G_b = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$.

$$\text{Then the dual code of } C \text{ generated by } G = \begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \\ 0 & b & b \\ b & 0 & b \end{pmatrix}. \text{ We obtain } C \cap C^\perp = \{0\}$$

8. Numerical Results

In the following, we classify, up to equivalence, cyclic codes up to length 7 (Tables 1–18). All the computations needed for this section were performed in Magma [20].

The generator matrices of the classified cyclic codes up to $n = 7$ can be found at: <https://www.kau.edu.sa/GetFile.aspx?id=316077&fn=Gen> (accessed on 10 September 2023).

Length 2 (8 Codes)

Table 1. Weight distribution of cyclic codes of length 2.

Generator Matrix	Weight Distribution
G_1 and G_2	$[< 0, 1 >, < 2, 1 >]$
G_3 and G_4	$[< 0, 1 >, < 1, 2 >, < 2, 1 >]$
G_5	$[< 0, 1 >, < 2, 3 >]$
G_6 and G_7	$[< 0, 1 >, < 1, 2 >, < 2, 5 >]$
G_8	$[< 0, 1 >, < 1, 6 >, < 2, 9 >]$

Table 2. List of all binary cyclic codes of length 2.

Index	Generator Polynomial
0	$x^2 - 1$
1	$x - 1$
2	1

Table 3. Cyclic codes of length 2.

Generator Matrix	d_H	Index C_a	Index C_b	Self-Orthogonal	QSD	Even
G_1	2	0	1	Yes	No	Yes
G_2	2	1	0	Yes	No	Yes
G_3	1	0	2	No	No	No
G_4	1	2	0	Yes	Yes	No
G_5	2	1	1	Yes	Yes	Yes
G_6	1	1	2	No	No	No
G_7	1	2	1	Yes	No	No
G_8	1	2	2	No	No	No

- Codes are not self-dual except G_7 .
- Codes are not LCD except G_3 .
- Codes neither Type IV nor QT4 except G_5 .

Length 3 (15 Codes)

Table 4. Weight distribution of cyclic codes of length 3.

Generator Matrix	Weight Distribution
G_1 and G_2	$[< 0, 1 >, < 3, 1 >]$
G_3 and G_4	$[< 0, 1 >, < 2, 3 >]$
G_5	$[< 0, 1 >, < 3, 3 >]$
G_6 and G_7	$[< 0, 1 >, < 1, 3 >, < 2, 3 >, < 3, 1 >]$
G_8 and G_9	$[< 0, 1 >, < 2, 3 >, < 3, 4 >]$
G_{10}	$[< 0, 1 >, < 2, 9 >, < 3, 6 >]$
G_{11} and G_{12}	$[< 0, 1 >, < 1, 3 >, < 2, 3 >, < 3, 9 >]$
G_{13} and G_{14}	$[< 0, 1 >, < 1, 3 >, < 2, 15 >, < 3, 13 >]$
G_{15}	$[< 0, 1 >, < 1, 9 >, < 2, 27 >, < 3, 27 >]$

Table 5. List of all binary cyclic codes of length 3.

Index	Generator Polynomial
0	$x^3 - 1$
1	$x - 1$
2	$x^2 + x + 1$
3	1

Table 6. Cyclic codes of length 3.

Generator Matrix	d_H	Index C_a	Index C_b	Self-Orthogonal	Even	LCD
G_1	3	0	2	No	No	Yes
G_2	3	2	0	Yes	No	No
G_3	2	0	1	No	Yes	Yes
G_4	2	1	0	Yes	Yes	No
G_5	3	2	2	No	No	No
G_6	2	0	3	No	Yes	Yes
G_7	2	3	0	Yes	Yes	No
G_8	2	1	2	No	No	No
G_9	2	2	1	No	No	No
G_{10}	2	1	1	No	No	No
G_{11}	1	2	3	No	No	No
G_{12}	1	3	2	No	No	No
G_{13}	1	1	3	No	No	No
G_{14}	1	3	1	No	No	No
G_{15}	1	3	3	No	No	No

- Codes are neither self-dual nor Type IV or QT4 .
- Codes are not QSD.

*Length 4 (24 Codes)***Table 7.** Weight distribution of cyclic codes of length 4.

Generator Matrix	Weight Distribution
G_1 and G_2	$[< 0, 1 >, < 4, 1 >]$
G_3 and G_4	$[< 0, 1 >, < 2, 2 >, < 4, 1 >]$
G_5	$[< 0, 1 >, < 4, 3 >]$
G_6 and G_7	$[< 0, 1 >, < 2, 6 >, < 4, 1 >]$
G_8 and G_9	$[< 0, 1 >, < 2, 2 >, < 4, 5 >]$
G_{10}	$[< 0, 1 >, < 2, 6 >, < 4, 9 >]$
G_{11} and G_{12}	$[< 0, 1 >, < 2, 6 >, < 4, 9 >]$
G_{13} and G_{14}	$[< 0, 1 >, < 1, 4 >, < 2, 6 >, < 3, 4 >, < 4, 1 >]$
G_{15} and G_{16}	$[< 0, 1 >, < 1, 4 >, < 2, 6 >, < 3, 4 >, < 4, 17 >]$
G_{17} and G_{18}	$[< 0, 1 >, < 2, 10 >, < 3, 8 >, < 4, 13 >]$
G_{19} and G_{20}	$[< 0, 1 >, < 1, 4 >, < 2, 14 >, < 3, 20 >, < 4, 25 >]$
G_{21}	$[< 0, 1 >, < 2, 18 >, < 3, 24 >, < 4, 21 >]$
G_{22} and G_{23}	$[< 0, 1 >, < 1, 4 >, < 2, 30 >, < 3, 52 >, < 4, 41 >]$
G_{24}	$[< 0, 1 >, < 1, 12 >, < 2, 54 >, < 3, 108 >, < 4, 81 >]$

Table 8. List of all binary cyclic codes of length 4.

Index	Generator Polynomial
0	$x^4 - 1$
1	$x + 1$
2	$x^2 + 1$
3	$x^3 + x^2 + x + 1$
4	1

Table 9. Cyclic codes of length 4.

Generator Matrix	d_H	Index C_a	Index C_b	Self-Orthogonal	Even
G_1	4	0	3	Yes	Yes
G_2	4	3	0	Yes	Yes
G_3	2	0	2	Yes	Yes
G_4	2	2	0	Yes	Yes
G_5	4	3	3	Yes	Yes
G_6	2	0	1	No	Yes
G_7	2	1	0	Yes	Yes
G_8	2	3	2	Yes	Yes
G_9	2	2	3	Yes	Yes
G_{10}	2	2	2	Yes	Yes
G_{11}	2	3	1	No	Yes
G_{12}	2	1	3	Yes	Yes
G_{13}	1	0	4	No	No
G_{14}	1	4	0	Yes	No
G_{15}	1	3	4	No	No
G_{16}	1	4	3	Yes	No
G_{17}	2	2	1	No	No
G_{18}	2	1	2	Yes	No
G_{19}	1	2	4	No	No
G_{20}	1	4	2	Yes	No
G_{21}	2	1	1	No	No
G_{22}	1	1	4	No	No
G_{23}	1	4	1	No	No
G_{24}	1	4	4	No	No

- Codes are not self-dual except G_{20} .
- Codes are not QSD except G_{10}, G_{12} and G_{14} .
- Codes are not Type IV except G_{10} and G_{12} .
- Codes are not QT4 except G_{10} and G_{12} .
- Codes are not LCD except G_{13} .

Length 5 (15 Codes)

Table 10. Weight distribution of cyclic codes of length 5.

Generator Matrix	Weight Distribution
G_1 and G_2	$[< 0, 1 >, < 5, 1 >]$
G_3 and G_4	$[< 0, 1 >, < 2, 10 >, < 4, 5 >]$
G_5	$[< 0, 1 >, < 5, 3 >]$
G_6 and G_7	$[< 0, 1 >, < 1, 5 >, < 2, 10 >, < 3, 10 >, < 4, 5 >, < 5, 1 >]$
G_8 and G_9	$[< 0, 1 >, < 2, 10 >, < 4, 5 >, < 5, 16 >]$
G_{10}	$[< 0, 1 >, < 2, 30 >, < 3, 60 >, < 4, 105 >, < 5, 60 >]$
G_{11} and G_{12}	$[< 0, 1 >, < 1, 5 >, < 2, 10 >, < 3, 10 >, < 4, 5 >, < 5, 33 >]$
G_{13} and G_{14}	$[< 0, 1 >, < 1, 5 >, < 2, 50 >, < 3, 130 >, < 4, 205 >, < 5, 121 >]$
G_{15}	$[< 0, 1 >, < 1, 15 >, < 2, 90 >, < 3, 270 >, < 4, 405 >, < 5, 243 >]$

Table 11. List of all binary cyclic codes of length 5.

Index	Generator Polynomial
0	$x^5 - 1$
1	$x + 1$
2	$x^4 + x^3 + x^2 + x + 1$
3	1

Table 12. Cyclic codes of length 5.

Generator Matrix	d_H	Index C_a	Index C_b	Self-Orthogonal	Even	LCD
G_1	5	0	2	No	No	Yes
G_2	5	2	0	Yes	No	No
G_3	2	0	1	No	Yes	Yes
G_4	2	1	0	Yes	Yes	No
G_5	5	2	2	No	No	No
G_6	1	0	3	No	No	Yes
G_7	1	3	0	Yes	No	No
G_8	2	1	2	No	No	No
G_9	2	2	1	No	No	No
G_{10}	2	1	1	No	No	No
G_{11}	1	2	3	No	No	No
G_{12}	1	3	2	No	No	No
G_{13}	1	1	3	No	No	No
G_{14}	1	3	1	No	No	No
G_{15}	1	3	3	No	No	No

- Codes are neither self-dual nor Type IV or QT4.
- Codes are not QSD except G_7 .

Length 6 (80 Codes)

Table 13. Weight distribution of cyclic codes of length 6.

Generator Matrix	Weight Distribution
G_1 and G_2	$[< 0, 1 >, < 6, 1 >]$
G_3 and G_4	$[< 0, 1 >, < 3, 2 >, < 6, 1 >]$
G_5 and G_6	$[< 0, 1 >, < 4, 3 >]$
G_7 and G_8	$[< 0, 1 >, < 2, 3 >, < 4, 3 >, < 6, 1 >]$
G_9 and G_{10}	$[< 0, 1 >, < 2, 3 >, < 3, 8 >, < 4, 3 >, < 6, 1 >]$
G_{11} and G_{12}	$[< 0, 1 >, < 2, 6 >, < 4, 9 >]$
G_{13} and G_{14}	$[< 0, 1 >, < 2, 15 >, < 4, 15 >, < 6, 1 >]$
G_{15} and G_{16}	$[< 0, 1 >, < 1, 6 >, < 2, 15 >, < 3, 20 >, < 4, 15 >, < 5, 6 >, < 6, 1 >]$
G_{17}	$[< 0, 1 >, < 6, 3 >]$
G_{18} and G_{19}	$[< 0, 1 >, < 3, 2 >, < 6, 5 >]$
G_{20} and G_{21}	$[< 0, 1 >, < 4, 3 >, < 6, 4 >]$
G_{22} and G_{23}	$[< 0, 1 >, < 2, 3 >, < 4, 3 >, < 6, 9 >]$
G_{24} and G_{25}	$[< 0, 1 >, < 2, 3 >, < 3, 8 >, < 4, 3 >, < 6, 17 >]$
G_{26} and G_{27}	$[< 0, 1 >, < 2, 6 >, < 4, 9 >, < 6, 16 >]$
G_{28} and G_{29}	$[< 0, 1 >, < 1, 3 >, < 2, 6 >, < 3, 10 >, < 4, 9 >, < 5, 3 >, < 6, 32 >]$
G_{30} and G_{31}	$[< 0, 1 >, < 1, 6 >, < 2, 15 >, < 3, 20 >, < 4, 15 >, < 5, 6 >, < 6, 65 >]$
G_{32}	$[< 0, 1 >, < 3, 6 >, < 6, 9 >]$
G_{33} and G_{34}	$[< 0, 1 >, < 3, 2 >, < 4, 3 >, < 5, 6 >, < 6, 4 >]$
G_{35} and G_{36}	$[< 0, 1 >, < 2, 3 >, < 3, 2 >, < 4, 9 >, < 5, 6 >, < 6, 11 >]$
G_{37} and G_{38}	$[< 0, 1 >, < 2, 3 >, < 3, 12 >, < 4, 15 >, < 5, 12 >, < 6, 21 >]$
G_{39} and G_{40}	$[< 0, 1 >, < 2, 6 >, < 3, 8 >, < 4, 9 >, < 5, 24 >, < 6, 16 >]$
G_{41} and G_{42}	$[< 0, 1 >, < 2, 15 >, < 3, 8 >, < 4, 39 >, < 5, 24 >, < 6, 41 >]$
G_{43} and G_{44}	$[< 0, 1 >, < 1, 6 >, < 2, 15 >, < 3, 36 >, < 4, 63 >, < 5, 54 >, < 6, 81 >]$
G_{45}	$[< 0, 1 >, < 4, 9 >, < 6, 6 >]$
G_{46} and G_{47}	$[< 0, 1 >, < 2, 3 >, < 4, 15 >, < 6, 13 >]$
G_{48} and G_{49}	$[< 0, 1 >, < 2, 3 >, < 3, 8 >, < 4, 15 >, < 5, 24 >, < 6, 13 >]$
G_{50} and G_{51}	$[< 0, 1 >, < 2, 6 >, < 4, 21 >, < 5, 24 >, < 6, 12 >]$
G_{52} and G_{53}	$[< 0, 1 >, < 2, 15 >, < 4, 39 >, < 5, 48 >, < 6, 25 >]$
G_{54} and G_{55}	$[< 0, 1 >, < 1, 6 >, < 2, 15 >, < 3, 20 >, < 4, 63 >, < 5, 102 >, < 6, 49 >]$
G_{56}	$[< 0, 1 >, < 2, 9 >, < 4, 27 >, < 6, 27 >]$
G_{57} and G_{58}	$[< 0, 1 >, < 2, 9 >, < 3, 8 >, < 4, 51 >, < 5, 24 >, < 6, 35 >]$
G_{59} and G_{60}	$[< 0, 1 >, < 2, 9 >, < 3, 12 >, < 4, 39 >, < 5, 36 >, < 6, 31 >]$

Table 13. Cont.

Generator Matrix	Weight Distribution
G_{61} and G_{62}	$[< 0, 1 >, < 2, 21 >, < 3, 24 >, < 4, 75 >, < 5, 72 >, < 6, 63 >]$
G_{63} and G_{64}	$[< 0, 1 >, < 1, 6 >, < 2, 27 >, < 3, 68 >, < 4, 135 >, < 5, 150 >, < 6, 125 >]$
G_{65}	$[< 0, 1 >, < 2, 9 >, < 3, 24 >, < 4, 99 >, < 5, 72 >, < 6, 51 >]$
G_{66} and G_{67}	$[< 0, 1 >, < 2, 9 >, < 3, 32 >, < 4, 75 >, < 5, 96 >, < 6, 43 >]$
G_{68} and G_{69}	$[< 0, 1 >, < 2, 21 >, < 3, 56 >, < 4, 171 >, < 5, 168 >, < 6, 95 >]$
G_{70} and G_{71}	$[< 0, 1 >, < 1, 6 >, < 2, 27 >, < 3, 132 >, < 4, 327 >, < 5, 342 >, < 6, 189 >]$
G_{72}	$[< 0, 1 >, < 2, 18 >, < 3, 12 >, < 4, 81 >, < 5, 108 >, < 6, 36 >]$
G_{73} and G_{74}	$[< 0, 1 >, < 2, 27 >, < 3, 48 >, < 4, 159 >, < 5, 192 >, < 6, 85 >]$
G_{75} and G_{76}	$[< 0, 1 >, < 1, 6 >, < 2, 39 >, < 3, 116 >, < 4, 303 >, < 5, 390 >, < 6, 169 >]$
G_{77}	$[< 0, 1 >, < 2, 45 >, < 3, 120 >, < 4, 315 >, < 5, 360 >, < 6, 183 >]$
G_{78} and G_{79}	$[< 0, 1 >, < 1, 6 >, < 2, 75 >, < 3, 260 >, < 4, 615 >, < 5, 726 >, < 6, 365 >]$
G_{80}	$[< 0, 1 >, < 1, 18 >, < 2, 135 >, < 3, 540 >, < 4, 1215 >, < 5, 1458 >, < 6, 729 >]$

Table 14. List of all binary cyclic codes of length 6.

Index	Generator Polynomial
0	$x^6 - 1$
1	$x + 1$
2	$x^2 + 1$
3	$x^2 + x + 1$
4	$x^3 + 1$
5	$x^4 + x^2 + x + 1$
6	$x^4 + x^3 + x + 1$
7	$x^5 + x^4 + x^3 + x^2 + x + 1$
8	1

Table 15. Cyclic codes of length 6.

Generator Matrix	d_H	Index C_a	Index C_b	Self-Orthogonal	Even
G_1	6	0	7	Yes	Yes
G_2	6	7	0	Yes	Yes
G_3	3	0	5	No	No
G_4	3	5	0	Yes	No
G_5	4	0	6	Yes	Yes
G_6	4	6	0	Yes	Yes
G_7	2	0	4	Yes	Yes
G_8	2	4	0	Yes	Yes
G_9	2	0	3	No	No
G_{10}	2	3	0	Yes	No
G_{11}	2	0	2	No	Yes
G_{12}	2	2	0	Yes	Yes

Table 15. Cont.

Generator Matrix	d_H	Index C_a	Index C_b	Self-Orthogonal	Even
G_{13}	2	0	1	No	Yes
G_{14}	2	1	0	Yes	Yes
G_{15}	1	0	8	No	No
G_{16}	1	8	0	Yes	No
G_{17}	6	7	7	Yes	Yes
G_{18}	3	7	5	No	No
G_{19}	3	5	7	Yes	No
G_{20}	4	7	6	Yes	Yes
G_{21}	4	6	7	Yes	Yes
G_{22}	2	7	4	Yes	Yes
G_{23}	2	4	7	Yes	Yes
G_{24}	2	7	3	No	No
G_{25}	2	3	7	Yes	No
G_{26}	2	7	2	No	Yes
G_{27}	2	2	7	Yes	Yes
G_{28}	1	7	1	No	No
G_{29}	1	1	7	Yes	No
G_{30}	1	7	8	No	No
G_{31}	1	8	7	Yes	No
G_{32}	3	5	5	No	No
G_{33}	3	5	6	Yes	No
G_{34}	3	6	5	No	No
G_{35}	2	5	4	Yes	No
G_{36}	2	4	5	No	No
G_{37}	2	5	3	No	No
G_{38}	2	3	5	No	No
G_{39}	2	5	2	No	No
G_{40}	2	2	5	No	No
G_{41}	2	5	1	No	No
G_{42}	2	1	5	No	No
G_{43}	1	5	8	No	No
G_{44}	1	8	5	No	No
G_{45}	4	6	6	Yes	Yes
G_{46}	2	6	4	Yes	Yes
G_{47}	2	4	6	Yes	Yes
G_{48}	2	6	3	No	No

Table 15. Cont.

Generator Matrix	d_H	Index C_a	Index C_b	Self-Orthogonal	Even
G_{49}	2	3	6	Yes	No
G_{50}	2	6	2	No	No
G_{51}	2	2	6	Yes	No
G_{52}	2	6	1	No	No
G_{53}	2	1	6	Yes	No
G_{54}	1	6	8	No	No
G_{55}	1	8	6	Yes	No
G_{56}	2	4	4	Yes	Yes
G_{57}	2	4	3	No	No
G_{58}	2	3	4	Yes	No
G_{59}	2	4	2	No	No
G_{60}	2	2	4	Yes	No
G_{61}	2	4	1	No	No
G_{62}	2	1	4	Yes	No
G_{63}	1	4	8	No	No
G_{64}	1	8	4	Yes	No
G_{65}	2	3	3	No	No
G_{66}	2	3	2	No	No
G_{67}	2	2	3	No	No
G_{68}	2	3	1	No	No
G_{69}	2	1	3	No	No
G_{70}	1	3	8	No	No
G_{71}	1	8	3	No	No
G_{72}	2	2	2	No	No
G_{73}	2	2	1	No	No
G_{74}	2	1	2	No	No
G_{75}	1	2	8	No	No
G_{76}	1	8	2	No	No
G_{77}	2	1	1	No	No
G_{78}	1	1	8	No	No
G_{79}	1	8	1	No	No
G_{80}	1	8	8	No	No

- Codes are not self-dual except G_{64} .
- Codes are not QSD except $G_{16}, G_{29}, G_{49}, G_{51}$ and G_{56} .
- Codes are not Type IV except G_{56} .
- Codes are not QT4 except G_{51} and G_{56} .
- Codes are not LCD except G_3, G_{11} and G_{15} .

Length 7 (63 Codes)

Table 16. Weight distribution of cyclic codes of length 7.

Generator Matrix	Weight Distribution
G_1 and G_2	$[< 0, 1 >, < 7, 1 >]$
G_3 and G_4	$[< 0, 1 >, < 4, 7 >]$
G_5 and G_6	$[< 0, 1 >, < 4, 7 >]$
G_7 and G_8	$[< 0, 1 >, < 3, 7 >, < 4, 7 >, < 7, 1 >]$
G_9 and G_{10}	$[< 0, 1 >, < 3, 7 >, < 4, 7 >, < 7, 1 >]$
G_{11} and G_{12}	$[< 0, 1 >, < 2, 21 >, < 4, 35 >, < 6, 7 >]$
G_{13} and G_{14}	$[< 0, 1 >, < 1, 7 >, < 2, 21 >, < 3, 35 >, < 4, 35 >, < 5, 21 >, < 6, 7 >, < 7, 1 >]$
G_{15}	$[< 0, 1 >, < 7, 3 >]$
G_{16} and G_{17}	$[< 0, 1 >, < 4, 7 >, < 7, 8 >]$
G_{18} and G_{19}	$[< 0, 1 >, < 4, 7 >, < 7, 8 >]$
G_{20} and G_{21}	$[< 0, 1 >, < 3, 7 >, < 4, 7 >, < 7, 17 >]$
G_{22} and G_{23}	$[< 0, 1 >, < 3, 7 >, < 4, 7 >, < 7, 17 >]$
G_{24} and G_{25}	$[< 0, 1 >, < 2, 21 >, < 4, 35 >, < 6, 7 >, < 7, 64 >]$
G_{26} and G_{27}	$[< 0, 1 >, < 1, 7 >, < 2, 21 >, < 3, 35 >, < 4, 35 >, < 5, 21 >, < 6, 7 >, < 7, 129 >]$
G_{28}	$[< 0, 1 >, < 4, 21 >, < 6, 42 >]$
G_{29} and G_{30}	$[< 0, 1 >, < 4, 14 >, < 5, 21 >, < 6, 21 >, < 7, 7 >]$
G_{31} and G_{32}	$[< 0, 1 >, < 3, 7 >, < 4, 21 >, < 5, 42 >, < 6, 42 >, < 7, 15 >]$
G_{33} and G_{34}	$[< 0, 1 >, < 3, 7 >, < 4, 21 >, < 5, 42 >, < 6, 42 >, < 7, 15 >]$
G_{35} and G_{36}	$[< 0, 1 >, < 2, 21 >, < 4, 91 >, < 5, 168 >, < 6, 175 >, < 7, 56 >]$
G_{37} and G_{38}	$[< 0, 1 >, < 1, 7 >, < 2, 21 >, < 3, 35 >, < 4, 147 >, < 5, 357 >, < 6, 343 >, < 7, 113 >]$
G_{39}	$[< 0, 1 >, < 4, 21 >, < 6, 42 >]$
G_{40} and G_{41}	$[< 0, 1 >, < 3, 7 >, < 4, 21 >, < 5, 42 >, < 6, 42 >, < 7, 15 >]$
G_{42} and G_{43}	$[< 0, 1 >, < 3, 7 >, < 4, 21 >, < 5, 42 >, < 6, 42 >, < 7, 15 >]$
G_{44} and G_{45}	$[< 0, 1 >, < 2, 21 >, < 4, 91 >, < 5, 168 >, < 6, 175 >, < 7, 56 >]$
G_{46} and G_{47}	$[< 0, 1 >, < 1, 7 >, < 2, 21 >, < 3, 35 >, < 4, 147 >, < 5, 357 >, < 6, 343 >, < 7, 113 >]$
G_{48}	$[< 0, 1 >, < 3, 21 >, < 4, 21 >, < 5, 126 >, < 6, 42 >, < 7, 45 >]$
G_{49} and G_{50}	$[< 0, 1 >, < 3, 14 >, < 4, 49 >, < 5, 84 >, < 6, 70 >, < 7, 38 >]$
G_{51} and G_{52}	$[< 0, 1 >, < 2, 21 >, < 3, 28 >, < 4, 203 >, < 5, 336 >, < 6, 287 >, < 7, 148 >]$
G_{53} and G_{54}	$[< 0, 1 >, < 1, 7 >, < 2, 21 >, < 3, 91 >, < 4, 371 >, < 5, 693 >, < 6, 567 >, < 7, 297 >]$
G_{55}	$[< 0, 1 >, < 3, 21 >, < 4, 21 >, < 5, 126 >, < 6, 42 >, < 7, 45 >]$
G_{56} and G_{57}	$[< 0, 1 >, < 2, 21 >, < 3, 28 >, < 4, 203 >, < 5, 336 >, < 6, 287 >, < 7, 148 >]$
G_{58} and G_{59}	$[< 0, 1 >, < 1, 7 >, < 2, 21 >, < 3, 91 >, < 4, 371 >, < 5, 693 >, < 6, 567 >, < 7, 297 >]$
G_{60}	$[< 0, 1 >, < 2, 63 >, < 3, 210 >, < 4, 735 >, < 5, 1260 >, < 6, 1281 >, < 7, 546 >]$
G_{61} and G_{62}	$[< 0, 1 >, < 1, 7 >, < 2, 105 >, < 3, 455 >, < 4, 1435 >, < 5, 2541 >, < 6, 2555 >, < 7, 1093 >]$
G_{63}	$[< 0, 1 >, < 1, 21 >, < 2, 189 >, < 3, 945 >, < 4, 2835 >, < 5, 5103 >, < 6, 5103 >, < 7, 2187 >]$

Table 17. List of all binary cyclic codes of length 7.

Index	Generator Polynomial
0	$x^7 - 1$
1	$x + 1$
2	$x^3 + x + 1$
3	$x^3 + x^2 + 1$
4	$x^4 + x^3 + x^2 + 1$
5	$x^4 + x^2 + x + 1$
6	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
7	1

Table 18. Cyclic codes of length 7.

Generator Matrix	d_H	Index C_a	Index C_b	Self-Orthogonal	Even
G_1	7	0	6	No	No
G_2	7	6	0	Yes	No
G_3	4	0	4	Yes	Yes
G_4	4	4	0	Yes	Yes
G_5	4	0	5	Yes	Yes
G_6	4	5	0	Yes	Yes
G_7	3	0	2	No	No
G_8	3	2	0	Yes	No
G_9	3	0	3	No	No
G_{10}	3	3	0	Yes	No
G_{11}	2	0	1	No	Yes
G_{12}	2	1	0	Yes	Yes
G_{13}	1	0	7	No	No
G_{14}	1	7	0	Yes	No
G_{15}	7	6	6	No	No
G_{16}	4	6	4	Yes	No
G_{17}	4	4	6	No	No
G_{18}	4	6	5	Yes	No
G_{19}	4	5	6	No	No
G_{20}	3	6	2	No	No
G_{21}	3	2	6	No	No
G_{22}	3	6	3	No	No
G_{23}	3	3	6	No	No
G_{24}	2	6	1	No	No
G_{25}	2	1	6	No	No
G_{26}	1	6	7	No	No
G_{27}	1	7	6	No	No
G_{28}	4	4	4	Yes	Yes

Table 18. Cont.

Generator Matrix	d_H	Index C_a	Index C_b	Self-Orthogonal	Even
G_{29}	4	4	5	Yes	No
G_{31}	3	4	2	No	No
G_{32}	3	2	4	Yes	No
G_{33}	3	4	3	No	No
G_{34}	3	3	4	Yes	No
G_{35}	2	4	1	No	No
G_{36}	2	1	4	Yes	No
G_{37}	1	4	7	No	No
G_{38}	1	7	4	Yes	No
G_{39}	4	5	5	Yes	Yes
G_{42}	3	5	3	No	No
G_{43}	3	3	5	Yes	No
G_{44}	2	5	1	No	No
G_{45}	2	1	5	Yes	No
G_{46}	1	5	7	No	No
G_{47}	1	7	5	Yes	No
G_{48}	3	2	2	No	No
G_{49}	3	2	3	No	No
G_{51}	2	2	1	No	No
G_{52}	2	1	2	No	No
G_{53}	1	2	7	No	No
G_{54}	1	7	2	No	No
G_{55}	3	3	3	No	No
G_{56}	2	3	1	No	No
G_{57}	2	1	3	No	No
G_{58}	1	3	7	No	No
G_{59}	1	7	3	No	No
G_{60}	2	1	1	No	No
G_{61}	1	1	7	No	No
G_{62}	1	7	1	No	No
G_{63}	1	7	7	No	No

- Codes are neither self-dual nor Type IV or QT4.
- Codes are not LCD except G_1 , G_{11} and G_{13} .
- Codes are not QSD except G_{14} , G_{32} , G_{34} , G_{41} and G_{43} .

Remark 1. In the case of length equal to 7, there are four equivalent codes, and they are G_{34} equivalent to G_{41} , G_{29} equivalent to G_{30} , G_{33} equivalent to G_{40} , and G_{49} equivalent to G_{50} .

In Table 19, we summarized the number of codes according to the Hamming weight.

Table 19. Number of cyclic codes over H .

$d \setminus n$	2	3	4	5	6	7
1	5	7	9	7	19	15
2	3	5	12	5	46	13
3		3			7	20
4			3		5	12
5				3		
6					3	
7						3
Total	8	15	24	15	80	63

9. Conclusions and Open Problems

In this article, we have studied cyclic codes over the non-unitary ring H . We have given criteria for a cyclic code over H to be self-dual or quasi-self-dual. We have derived an algorithm to classify cyclic codes of given length, based on the classification of cyclic binary codes of that length and the knowledge of their automorphism group. A Gray map allows us to construct quasi-cyclic codes of index 2 from cyclic codes over H .

In the future, we plan to study the same questions over other non-unitary rings, possibly of characteristic larger than 2.

Author Contributions: Conceptualization, A.A. and P.S.; Methodology, M.A.; Validation, P.S.; Investigation, A.A., M.A. and P.S.; Resources, A.A. and P.S.; Data curation, M.A.; Writing—original draft, M.A.; Writing—review & editing, M.A.; Project administration, A.A.; Funding acquisition, A.A. This article was written in equal co-authorship. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by The Deanship of Scientific Research (DSR) at King Abdulaziz University (KAU), Jeddah, Saudi Arabia, of funder grant number KEP-PhD: 100-130-1443.

Data Availability Statement: All computations performed in this paper are available upon request from the authors.

Acknowledgments: The authors are grateful for support of the The Deanship of Scientific Research (DSR) at King Abdulaziz University (KAU), Jeddah, Saudi Arabia, for funding this project, under grant no. KEP-PhD: 100-130-1443.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bose, R.C.; Ray-Chaudhuri, D.K. On a Class of Error Correcting Binary Group Codes. *Inf. Control* **1960**, *3*, 68–79. [\[CrossRef\]](#)
2. Hocquenghem, A. Codes correcteurs d'erreurs. *Chiffres* **1959**, *2*, 147–156. (In French)
3. Abdualrub, T.; Oehmeke, R. Cyclic codes of length 2^e over Z_4 . *Discret. Appl. Math.* **2003**, *128*, 3–9. [\[CrossRef\]](#)
4. Blackford, T. Cyclic codes of oddly even length over Z_4 . *Discret. Appl. Math.* **2003**, *128*, 27–46. [\[CrossRef\]](#)
5. Dougherty, S.T.; Ling, S. Cyclic Codes over Z_4 of Even Length. *Des. Codes Cryptogr.* **2006**, *39*, 127–153. [\[CrossRef\]](#)
6. Jitman, S.; Sangwisut, E.; Udomkavanich, P. Hulls of cyclic codes over Z_4 . *Discret. Math.* **2020**, *343*, 111621. [\[CrossRef\]](#)
7. Pless, V.; Qian, Z. Cyclic codes and quadratic residue codes over Z_4 . *IEEE Trans. Inf. Theory* **1996**, *42*, 1594–1600. [\[CrossRef\]](#)
8. Prakash, O.; Yadav, S.; Verma, R.K. Constacyclic and Linear Complementary Dual Codes over $F_q + uF_q$. *Def. Sci. J.* **2020**, *70*, 626–632. [\[CrossRef\]](#)
9. Zhu, S.; Wang, Y.; Shi, M. Some Results on Cyclic Codes over $F_2 + vF_2$. *IEEE Trans. Inf. Theory* **2010**, *56*, 1680–1684. [\[CrossRef\]](#)
10. MacWilliams, F.J.; Sloane, N.J.A. *The Theory of Error Correcting Codes*; Elsevier: Berlin/Heidelberg, Germany, 1977; Volume 16.
11. Shi, M.; Alahmadi, A.; Solé, P. *Codes and Rings: Theory and Practice*; Academic Press: Cambridge, MA, USA, 2017.
12. Hartman, C.R.P.; Tzeng, K.K. Generalizations of the BCH bound. *Inf. Control* **1972**, *20*, 489–498. [\[CrossRef\]](#)
13. Roos, C. A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound. *J. Comb. Theory Ser. A* **1982**, *33*, 229–232. [\[CrossRef\]](#)
14. van Lint, J.H.; Wilson, R. On the Minimum Distance of Cyclic Codes. *IEEE Trans. Inf. Theory* **1986**, *32*, 23–40. [\[CrossRef\]](#)
15. Alahmadi, A.; Alkathiry, A.; Altassan, A.; Basaffar, W.; Bonnecaze, A.; Shoaib, H.; Solé, P. Type IV codes over a non-local non-unital ring. *Proyecciones* **2020**, *39*, 963–978. [\[CrossRef\]](#)

16. Alahmadi, A.; Altassan, A.; Basaffar, W.; Bonnecaze, A.; Shoaib, H.; Solé, P. Quasi Type IV codes over a non-unital ring. *Appl. Algebra Eng. Commun. Comput.* **2021**, *32*, 217–228. [[CrossRef](#)]
17. Alahmadi, A.; Altassan, A.; Basaffar, W.; Shoaib, H.; Bonnecaze, A.; Solé, P. Type IV codes over a non-unital ring. *J. Algebra Its Appl.* **2022**, *21*, 2250142. [[CrossRef](#)]
18. Raghavendran, R. Finite associative rings. *Compos. Math.* **1969**, *21*, 195–229.
19. Fine, B. Classification of finite rings of order p^2 . *Math. Mag.* **1993**, *66*, 248–252. [[CrossRef](#)]
20. Bosma, W.; Cannon, J.; Playoust, C. The Magma algebra system I: The user language. *J. Symb. Comput.* **1997**, *24*, 235–265. [[CrossRef](#)]
21. Massey, J.L. Linear codes with complementary duals. *Discret. Math.* **1992**, *106*, 337–342. [[CrossRef](#)]
22. Alahmadi, A.; Melaibari, A.; Solé, P. Duality of codes over non-unital rings of order four. *IEEE Access* **2023**, *11*, 53120–53133. [[CrossRef](#)]
23. Park, Y.H. The classification of self-dual modular codes. *Finite Fields Appl.* **2011**, *17*, 442–460. [[CrossRef](#)]
24. Yang, X.; Massey, J.L. The condition for a cyclic code to have a complementary dual. *Discret. Math.* **1994**, *126*, 391–393. [[CrossRef](#)]
25. Massey, J.L. Reversible codes. *Inf. Control* **1964**, *7*, 369–380. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.