Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 11** : 1–7.
ISSN-0037-8712
doi:10.5269/bspm.78664

Double Cyclic and Quantum Codes

Shashirekha G. and Vadiraja Bhatta G. R.*

ABSTRACT: In this paper, we explore the structure of $\mathbb{Z}_2 + u\mathbb{Z}_2 = \{0, 1, u, u+1\} = \mathbb{Z}_2[u]$-additive codes, where $u^2 = 0$ and their generalization to double cyclic codes. We establish the algebraic framework for these codes over the ring $\mathbb{Z}_2[u]$ and its extensions. Additionally, we provide explicit generators for double cyclic codes and define the Gray map to derive corresponding binary linear codes and quantum codes. Finally, we present an example illustrating the construction of a binary linear code.

Keywords: Linear code, cyclic code, double cyclic code, binary linear code, quantum code.

Contents

1. Introduction

Cyclic codes over finite rings or fields have been extensively studied due to their importance and simplicity compared to other types of linear codes. Since they form a subcategory of linear codes, their coding procedures are typically less complex. Moreover, these codes exhibit rich algebraic structures, making them particularly appealing in coding theory. The study of coding theory over rings and modules generalizes traditional linear codes over fields. Instead of relying solely on field structures, the alphabet in such codes may be a ring or a module. In this context, the codes are represented as submodules of a free module over the ring or module. Recently, the traditional requirement of linearity has been relaxed, with additivity becoming a preferred property. Additionally, the scope has expanded to include codes with mixed alphabets.

Abualrub and Siap [2] investigated reversible cyclic codes of arbitrary length over the ring $\mathbb{Z}_4$, determining their generators and providing a classification based on their generator structures. Shi et al. [12] examined $(1+2u)$-constacyclic codes over $R = \mathbb{Z}_4 + u\mathbb{Z}_4$ and introduced a novel Gray map from R to $\mathbb{Z}_4^2$. They demonstrated that the Gray images of these codes are cyclic codes of length $2n$ over $\mathbb{Z}_4$. The authors also compared the parameters of these codes with existing entries in an online database, identifying codes with improved parameters. Wang and Shi [13] explored $\mathbb{Z}_p\mathbb{Z}_p^k$-additive cyclic codes, describing their generator polynomials and establishing necessary and sufficient conditions for $\mathbb{Z}_p\mathbb{Z}_p^2$-additive cyclic codes whose Gray images are linear over $\mathbb{Z}_p$. Islam and Prakash [8] presented complete sets of minimal generating sets and generator polynomials for cyclic codes of length β over $\mathbb{Z}_p[u,v]$, as well as for $\mathbb{Z}_p\mathbb{Z}_p[u,v]$-additive cyclic codes of length (α, β). Later, Islam et al. [9] introduced a novel Gray map to construct quasi-cyclic and cyclic codes over $\mathbb{Z}_4$ from constacyclic codes over $\mathbb{Z}_4[u]$. They showed that Gray images of certain additive constacyclic codes, including skew codes over $\mathbb{Z}_4\mathbb{Z}_4[u]$, yield generalized quasi-cyclic codes over $\mathbb{Z}_4$. Bag et al. [5] demonstrated that Gray images of quasi-cyclic codes over $\mathbb{Z}_4$

* Corresponding author.
2020 *Mathematics Subject Classification:* 94B15, 94B05.
Submitted August 28, 2025. Published March 13, 2026

are equivalent to quasi-cyclic, cyclic, and permuted forms of λ-constacyclic codes over R. They also derived skew λ-constacyclic codes over R and established their equivalence to cyclic and quasi-cyclic codes over $\mathbb{Z}_4$. Prakash et al. [16] studied mixed-alphabet $\mathbb{Z}_4\mathbb{Z}_4[u^3]$-additive λ-constacyclic and cyclic codes for units $\lambda = 1 + 2u^2, 3 + 2u^2$, identifying minimal generating sets and generator polynomials for these additive cyclic codes. Singh and Kewat [1] investigated cyclic codes over $\mathbb{Z}_p[u]/\langle u^k \rangle$, determining a set of generators for these codes. Özen et al. [15] analyzed constacyclic and cyclic codes with a shift constant of $(2+u)$ over $R = \mathbb{Z}_4 + u\mathbb{Z}_4$ with $u^2 = 1$. They identified generator structures for cyclic codes over this ring and their spanning sets. Additionally, they demonstrated that cyclic codes over $\mathbb{Z}_4$ can be represented via their $\mathbb{Z}_4$-images, providing several examples of codes with superior parameters compared to standard $\mathbb{Z}_4$-linear codes. Yildiz and Aydin [19] explored the algebraic structures of cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, highlighting their generators and discovering new linear codes over $\mathbb{Z}_4$. Aydogdu et al. [4] presented the algebraic structure of constacyclic and cyclic codes and their duals over the R-module $\mathbb{Z}_2^\alpha R^\beta$, where $R = \mathbb{Z}_2[u] = \mathbb{Z}_2 + u\mathbb{Z}_2 = \{0, 1, u, u+1\}$ with $u^2 = 0$. They determined generating sets, code types, sizes, and properties of both the codes and their duals, identifying optimal families of codes. Abualrub et al. [3] investigated $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes as $\mathbb{Z}_4[l]$-submodules of $R_{r,s}$, deriving their generator polynomials and presenting an infinite family of Maximum Distance Separable codes. They also obtained binary linear codes with optimal parameters derived from these additive cyclic codes. Shi and Wang [12] studied $\mathbb{Z}_p\mathbb{Z}_p^k$-additive cyclic codes, analyzing their algebraic structures, generator polynomials, and minimal spanning sets. They provided necessary and sufficient conditions for a class of $\mathbb{Z}_p^2$-additive codes whose Gray images are linear. Borges et al. [6] examined $\mathbb{Z}_2\mathbb{Z}_4$-additive codes and their binary images under the Gray map, determining parameters and forms for their generator and parity-check matrices. Borges et al. [10] further analyzed $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, identifying all codes with odd lengths β whose Gray images are linear binary codes. They demonstrated that these codes are permutation-equivalent to $\mathbb{Z}_2$-double cyclic codes. Wu et al. [17] focused on $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, detailing their generator polynomials, minimal generating sets, and dual structures. They provided a comprehensive description of the duals of separable codes and highlighted specific cases for non-separable codes.

The paper is organized as follows: Section 2 introduces key preliminaries on linear codes, Lee distance, and Hamming distance. Section 3 presents foundational results on additive codes. Section 4 discusses the algebraic structure and generators of double cyclic codes. In Section 5, we define the Gray map to derive binary linear codes and quantum codes. Finally, we provide an example in this section and conclude in the last section.

2. Preliminaries

In our study, we denote the ring $\mathbb{Z}_2[u]$ as $\mathbb{Z}_2[u] = \mathbb{Z}_2 + u\mathbb{Z}_2 = \{0, 1, u, u+1\}$. This structure represents a finite commutative ring of size 4 and characteristic 2, where $u^2 = 0$. The ring contains three distinct ideals they are the trivial ideal $\langle 0 \rangle$, the entire ring $\langle 1 \rangle = \mathbb{Z}_2[u]$, and the unique maximal ideal $\langle u \rangle = \{0, u\}$. Within this structure, 1 and $1 + u$ are units, while 0 and u are non-units. A linear code C of length n is defined as a non-empty subset of $\mathbb{Z}_2[u]^n$ that forms a submodule under the $\mathbb{Z}_2[u]$-module structure. Each element of C is referred to as a codeword. In coding theory, a linear code C of length n over F_q is a subspace of the vector space F_q^n.

A set $S \subseteq F_q^n$ is cyclic if, for every $(c_0, c_1, \ldots, c_{n-1}) \in S$, the shifted vector $(c_{n-1}, c_0, \ldots, c_{n-2})$ is also in S. A linear code that satisfies this property is called a cyclic code. Cyclic codes are a special class of error-correcting codes where each cyclic shift of a codeword yields another codeword [11]. Similarly, constacyclic codes generalize this concept, for some constant λ, if $(d_1, d_2, \ldots, d_n)$ is a codeword, then $(\lambda d_n, d_1, \ldots, d_{n-1})$ must also be a codeword [15]. The Hamming distance between two words $p = (p_1, p_2, \ldots, p_n)$ and $s = (s_1, s_2, \ldots, s_n)$ of the same length n is the number of positions where p and s differ. It is given by $d_H(p, s) = \sum_{i=1}^n d_H(p_i, s_i)$, where $d_H(p_i, s_i) = 1$ if $p_i \neq s_i$ and 0 otherwise. The Hamming weight of a codeword p is the number of non-zero components in p, computed as $\mathrm{wt}_H(p) = \sum_{i=1}^n \mathrm{wt}_H(p_i)$, where $\mathrm{wt}_H(p_i) = 1$ if $p_i \neq 0$. The Lee distance measures the dissimilarity between two codewords p and s over a q-ary alphabet $\{0, 1, \ldots, q-1\}$, defined as $d_L(p, s) = \sum_{i=1}^n \min(|p_i - s_i|, q - |p_i - s_i|)$. When $q = 2$ or 3, the Lee and Hamming distances coincide, as both count the number of differing symbols between two words. The Lee weight of a codeword $p = (p_1, p_2, \ldots, p_n)$ is defined as $\mathrm{wt}_L(p) = \sum_{i=1}^n \min(|p_i|, q - |p_i|)$.

3. $Z_2[u]Z_2[u]$-Additive Codes

The set $Z_2[u]Z_2[u] = \{(f,g) \mid f,g \in Z_2[u]\}$ forms a commutative group under component-wise addition. For a code of length $n=\mu+\nu$, we define $Z_2[u]^\mu \times Z_2[u]^\nu = \{(f,g) \mid f=(f_0,f_1,\ldots,f_{\mu-1}) \in Z_2[u]^\mu, g=(g_0,g_1,\ldots,g_{\nu-1}) \in Z_2[u]^\nu\}$, where μ and ν are positive integers. The group $Z_2[u]^\mu \times Z_2[u]^\nu$ is commutative under component-wise addition. We define a map $\eta : Z_2[u] \to Z_2$ by $\eta(l+um)=l$, and a multiplication

$$* : Z_2[u] \times Z_2[u]Z_2[u] \to Z_2[u]Z_2[u]$$

given by

$$d*(f,g) = (\eta(d)f, \eta(d)g), \quad \text{where } d,f,g \in Z_2[u].$$

This multiplication is extended to the elements of $Z_2[u]^\mu \times Z_2[u]^\nu$ and $Z_2[u]$ as follows:

$$d*(f,g) = (\eta(d)f_0, \eta(d)f_1, \ldots, \eta(d)f_{\mu-1}, \eta(d)g_0, \eta(d)g_1, \ldots, \eta(d)g_{\nu-1}),$$

where $f=(f_0,f_1,\ldots,f_{\mu-1}) \in Z_2[u]^\mu$ and $g=(g_0,g_1,\ldots,g_{\nu-1}) \in Z_2[u]^\nu$.

Theorem 3.1 [14] *The set $Z_2[u]^\mu \times Z_2[u]^\nu$ forms a $Z_2[u]$-module under the multiplication $*$ defined above.*

Definition 3.1 A non-empty subset $C \subseteq Z_2[u]^\mu \times Z_2[u]^\nu$ is called a $Z_2[u]Z_2[u]$-additive code of length (μ,ν) if it is a $Z_2[u]$-submodule of $Z_2[u]^\mu \times Z_2[u]^\nu$.

Definition 3.2 A $Z_2[u]Z_2[u]$-additive code C of length (μ,ν) is said to be a $Z_2[u]Z_2[u]$-additive cyclic code if, for any $z=(f_0,f_1,\ldots,f_{\mu-1},g_0,g_1,\ldots,g_{\nu-1}) \in C$, its cyclic shift $\sigma_{\mu,\nu} = (f_{\mu-1},f_0,\ldots,f_{\mu-2},g_{\nu-1}, g_0,\ldots,g_{\nu-2})$ also belongs to C.

We extend the ring homomorphism $\eta : Z_2[u][x] \to Z_2[x]$ as follows $\eta\left(\sum_{i=0}^n k_i x^i\right) = \sum_{i=0}^n \eta(k_i)x^i$. Let $R_{\mu,\nu} = Z_2[u][x]/\langle x^\mu - 1\rangle \times Z_2[u][x]/\langle x^\nu - 1\rangle$. Then $R_{\mu,\nu}$ becomes a $Z_2[u][x]$-module with multiplication defined as $k(x)*(f(x),g(x)) = (\eta(k(x))f(x), \eta(k(x))g(x))$, where $k(x),f(x),g(x) \in Z_2[u][x]$. For any $Z_2[u]Z_2[u]$-additive code C of length (μ,ν), a codeword $z=(f_0,f_1,\ldots,f_{\mu-1},g_0,g_1,\ldots,g_{\nu-1}) \in C$ corresponds to a polynomial $z(x) = (b(x),c(x)) \in R_{\mu,\nu}$, where $f(x) = f_0 + f_1x + \cdots + f_{\mu-1}x^{\mu-1} \in Z_2[u][x]/\langle x^\mu - 1\rangle$ and $g(x) = g_0 + g_1x + \cdots + g_{\nu-1}x^{\nu-1} \in Z_2[u][x]/\langle x^\nu - 1\rangle$.

Theorem 3.2 [14] *A $Z_2[u]Z_2[u]$-additive code C of length (μ,ν) is a $Z_2[u]Z_2[u]$-additive cyclic code if and only if it is a $Z_2[u][x]$-submodule of $R_{\mu,\nu}$.*

Proof: Assume C is a $Z_2[u]Z_2[u]$-additive cyclic code of length (μ,ν). For $k(x) \in Z_2[u][x]$ and $z(x) = (f(x),g(x)) \in C$. We can show that $x*(f(x),g(x)) = (xf(x), xg(x))$, where $xf(x)$ and $xg(x)$ are cyclic shifts of $f(x)$ in $Z_2[u][x]/ < x^\mu - 1 >$ and $g(x)$ in $Z_2[u][x]/ < x^\nu - 1 >$, respectively. By induction, $x^i * (f(x),g(x)) \in C$ for any positive integer $i \geq 1$, and thus $k(x)*(f(x),g(x)) \in C$. This shows C is a $Z_2[u][x]$-submodule of $R_{\mu,\nu}$.

Conversely, if C is a $Z_2[u][x]$-submodule of $R_{\mu,\nu}$, the closure under multiplication implies $x*(f(x),g(x)) \in C$, ensuring C is a $Z_2[u]Z_2[u]$-additive cyclic code of length (μ,ν). □

4. Generators of double cyclic codes

Definition 4.1 *A binary linear code C of length $n=\mu+\nu$ is called a $\mathbb{Z}_2[u]$-double cyclic code if for any codeword $(c_0,c_1,\ldots,c_{\mu-1} \mid c'_0,c'_1,\ldots,c'_{\nu-1}) \in C$, its cyclic shift $(c'_{\nu-1},c_0,c_1,\ldots,c_{\mu-2} \mid c_{\nu-1},c'_0,c'_1,\ldots, c'_{\nu-2}) \in C$.*

Let $c=(c_0,c_1,\ldots,c_{\mu-1} \mid c_0,\ldots,c_{\nu-1})$ represent a codeword in the binary linear code C, and let $i \in \mathbb{Z}$. The *i-th shift* of c, is $c^{(i)} = (c_{0-i},c_{1-i},\ldots,c_{\mu-1-i},c_{0-i},\ldots,c_{\nu-1-i})$. If $C \subseteq \mathbb{Z}_2^\mu \times \mathbb{Z}_2^\nu$ is a $\mathbb{Z}_2$-double cyclic code, then C_μ and C_ν are the projections of C onto the first μ-coordinates and the last ν-coordinates, respectively. C_μ and C_ν are binary cyclic codes of lengths μ and ν, respectively. The code C is called *separable* if it is the direct product of C_μ and C_ν. There is a natural correspondence between $\mathbb{Z}_2^\mu \times \mathbb{Z}_2^\nu$

and $\mathbb{Z}_2[x]/(x^\mu - 1) \times \mathbb{Z}_2[x]/(x^\nu - 1)$ given by the map $(c_0, c_1, \ldots, c_{\mu-1}, c_0, c_1, \ldots, c_{\nu-1}) \mapsto (c(x) \mid d(x))$, where $c(x) = c_0 + c_1 x + \cdots + c_{\mu-1}x^{\mu-1}$ and $d(x) = d_0 + d_1 x + \cdots + d_{\nu-1}x^{\nu-1}$. Let $C \subseteq Z_2[u]^\mu \times Z_2[u]^\nu$ be a submodule. Define $\Upsilon : C \to Z_2[u]^\mu$ and $\Upsilon' : C \to Z_2[u]^\nu$ be the cannonical projections, and let K and K' be a submodule of $Z_2[u]^\mu \times Z_2[u]^\nu$. Then $K = \{(0, d)$ such that $\Upsilon(K) \in Z_2[u]^\mu\}$ and $K' = \{(c, 0)$ such that $\Upsilon'(K') \in Z_2[u]^\nu\}$.

The above discussion is summarized as follows.

Theorem 4.1 *Let $C \subseteq \mathbb{Z}_2[x]/(x^\mu - 1) \times \mathbb{Z}_2[x]/(x^\nu - 1)$ and projections $\Upsilon(C) \subseteq \mathbb{Z}_2[x]/(x^\mu - 1)$, $\Upsilon'(C) \subseteq \mathbb{Z}_2[x]/(x^\nu - 1)$ Then*

1. *$\Upsilon(C)$ and $\Upsilon'(C)$ are submodules of their respective polynomial rings.*
2. *If C is separable, then $C \cong \Upsilon(C) \times \Upsilon'(C)$.*

Theorem 4.2 *Every submodule $C \subseteq \mathbb{Z}_2[x]/(x^\mu - 1) \times \mathbb{Z}_2[x]/(x^\nu - 1)$ can be expressed as $C = \langle (b(x), 0), (e(x), a(x)) \rangle$, where $b(x), e(x) \in \mathbb{Z}_2[x]/(x^\mu - 1)$, $a(x) \in \mathbb{Z}_2[x]/(x^\nu - 1)$, and $b(x) \mid x^\mu - 1$, $a(x) \mid x^\nu - 1$, with $\deg(e(x)) < \deg(b(x))$.*

Proof: By the structure theorem for modules over principal ideal rings, $Z_2[u]/(x^\mu - 1)$ and $Z_2[u]/(x^\nu - 1)$ are principal ideal rings. This implies that every submodule of $Z_2[u]^\mu$ and $Z_2[u]^\nu$ is finitely generated. Let $\Upsilon : Z_2[u]^\mu \times Z_2[u]^\nu \to Z_2[u]^\mu$ and $\Upsilon' : Z_2[u]^\mu \times Z_2[u]^\nu \to Z_2[u]^\nu$ be the canonical projections. Denote $\Upsilon(C) = C_\mu$ and $\Upsilon'(C) = C_\nu$, which are submodules of $Z_2[u]^\mu$ and $Z_2[u]^\nu$, respectively. Since $Z_2[u]/(x^\mu - 1)$ and $Z_2[u]/(x^\nu - 1)$ are principal ideal rings, there exist generators $b(x) \in C_\mu$ and $a(x) \in C_\nu$ such that $C_\mu = \langle b(x) \rangle, \quad b(x) \mid (x^\mu - 1), C_\nu = \langle a(x) \rangle, \quad a(x) \mid (x^\nu - 1)$. Now consider the submodule C. By definition, $\Upsilon'(C) = C_\nu = \langle a(x) \rangle$, so there exists an $e(x) \in Z_2[u]^\mu$ such that $(e(x), a(x)) \in C$. Additionally, $(b(x), 0) \in C$ since $b(x)$ generates C_μ. We claim that $C = \langle (b(x), 0), (e(x), a(x)) \rangle$. Let $(p(x), q(x)) \in C$. We must show that $(p(x), q(x))$ is a linear combination of $(b(x), 0)$ and $(e(x), a(x))$. First, since $q(x) \in \Upsilon'(C) = C_\nu = \langle a(u) \rangle$, there exists $\lambda(x) \in Z_2[u]$ such that $q(x) = \lambda(x)a(x)$. Now consider $(p(x), q(x)) - \lambda(x)(e(x), a(x)) = (p(x) - \lambda(x)e(x), 0)$. The first component $p(x) - \lambda(x)e(x) \in \pi_\mu(C) = C_\mu = \langle b(x) \rangle$, so there exists $\mu(x) \in Z_2[u]$ such that $p(x) - \lambda(x)e(x) = \mu(x)b(x)$. Thus $(p(x), q(x)) = \mu(x)(b(x), 0) + \lambda(x)(e(x), a(x))$. This shows that C is generated by $(b(x), 0)$ and $(e(x), a(x))$. Finally, the condition $\deg(e(x)) < \deg(b(x))$ ensures uniqueness of the generators, completing the pf. □

Theorem 4.3 *Let $C = \langle (b(x), 0), (e(x), a(x)) \rangle \subseteq Z_2[u]/(x^\mu - 1) \times Z_2[u]/(x^\nu - 1)$, where $b(x) \mid x^\mu - 1$ and $a(x) \mid x^\nu - 1$. Then the dimension of C is viewed as $\dim(C) = \mu + \nu - \deg(b(x)) - \deg(a(x))$.*

Proof: The modules $Z_2[u]^\mu$ and $Z_2[u]^\nu$ consist of vectors over $Z_2[u]$ of lengths μ and ν, respectively. The degrees of $b(x)$ and $a(x)$, which divide $x^\mu - 1$ and $x^\nu - 1$, determine the constraints on C. The projection of C onto the first component is $\langle b(x) \rangle \subseteq Z_2[u]^\mu$, with $\mu - \deg(b(x))$ free binary variables. Similarly, the projection onto the second component is $\langle a(x) \rangle \subseteq Z_2[u]^\nu$, with $\nu - \deg(a(x))$ free binary variables. The generators of C, $(b(x), 0)$ and $(e(x), a(x))$, Hence, the total dimension of C is $\dim(C) = \mu + \nu - \deg(b(x)) - \deg(a(x))$. □

Theorem 4.4 *The projections of C onto $\mathbb{Z}_2[u]^\mu$ and $\mathbb{Z}_2[u]^\nu$ are:*

$$\Upsilon(C) = \langle b(x) \rangle, \quad \Upsilon'(C) = \langle a(x) \rangle.$$

Proof: Consider the submodule $C = \langle (b(x), 0), (e(x), a(x)) \rangle \subseteq \mathbb{Z}_2[u]^\mu \times \mathbb{Z}_2[u]^\nu$. The projection $\Upsilon(C)$ maps C to its first component in $\mathbb{Z}_2[u]^\mu$. The generator $(b(x), 0)$ maps to $b(x)$, while $(e(x), a(x))$ projects to $e(x)$, which is constrained to have $\deg(e(x)) < \deg(b(x))$. Thus, $\Upsilon(C) = \langle b(x) \rangle$.

Similarly, the projection $\Upsilon'(C)$ maps C to its second component in $\mathbb{Z}_2[u]^\nu$. The generator $(b(x), 0)$ maps to 0, while $(e(x), a(x))$ maps to $a(x)$, yielding $\Upsilon'(C) = \langle a(x) \rangle$. Hence, the projections are $\Upsilon(C) = \langle b(x) \rangle, \quad \Upsilon'(C) = \langle a(x) \rangle$. □

Theorem 4.5 *A minimal generating set for C as a $\mathbb{Z}_2[u]$-module is*

$$S_1 = \{x^i(b(x),0) \mid 0 \le i < \mu - \deg(b(x))\},$$
$$S_2 = \{x^j(e(x),a(x)) \mid 0 \le j < \nu - \deg(a(x))\}.$$

The union $S_1 \cup S_2$ forms a basis for C.

Proof: The generator $(b(x),0)$ of C corresponds to the projection $\langle b(x)\rangle \subseteq \mathbb{Z}_2[u]^{\mu}$. Shifting $b(x)$ by powers of x, the set $S_1 = \{x^i(b(x),0) \mid 0 \le i < \mu - \deg(b(x))\}$ spans all elements of $\langle b(x)\rangle$ in $\mathbb{Z}_2[u]^{\mu}$. Similarly, the generator $(e(x),a(x))$ corresponds to the projection $\langle a(x)\rangle \subseteq \mathbb{Z}_2[u]^{\nu}$. The set $S_2 = \{x^j(e(x),a(x)) \mid 0 \le j < \nu - \deg(a(x))\}$ spans all elements involving $a(x)$ in $\mathbb{Z}_2[u]^{\nu}$. Together, $S_1 \cup S_2$ spans the entirety of C as a $\mathbb{Z}_2[u]$-module, providing a minimal and complete generating set for C. □

5. Quantum Codes over $\mathbb{Z}_2[u]^{\mu} \times \mathbb{Z}_2[u]^{\nu}$

We define a Gray map:

$$\Phi : \mathbb{Z}_2[u]^{\mu} \times \mathbb{Z}_2[u]^{\nu} \to \mathbb{Z}_2^n,$$

where $n = 2\mu + 2\nu$, as follows $\Phi\big((q+ur)(x),(s+ut)(x)\big) = \big(r(x),(q\oplus r)(x),t(x),(s\oplus t)(x)\big)$. Here, the elements $(q+ur)(x) \in \mathbb{Z}_2[u]^{\mu}$ and $(s+ut)(x) \in \mathbb{Z}_2[u]^{\nu}$ are expressed in the forms:$(q+ur)(x) = ((q_0+ur_0), x(q_1+ur_1), \ldots, x^{\mu-1}(q_{\mu-1}+ur_{\mu-1})) \in \mathbb{Z}_2[u]^{\mu}$ and $(s+ut)(x) = ((s_0+ut_0), x(s_1+ut_1), \ldots, x^{\mu-1}(s_{\mu-1}+ut_{\nu-1})) \in \mathbb{Z}_2[u]^{\nu}$.

The map Φ transforms the Lee distance on $\mathbb{Z}_2[u]^{\mu} \times \mathbb{Z}_2[u]^{\nu}$ to the Hamming distance on $\mathbb{Z}_2^n$. The Lee weight of a coordinate $r \in \mathbb{Z}_2[u]$ is defined as

$$\mathrm{wt}_L(r) = \begin{cases} 2, & \text{if } r = u,\\ 1, & \text{if } r \in \{1, 1+u\},\\ 0, & \text{otherwise.}\end{cases}$$

For a codeword (b_2, b_3), its Lee weight is the sum of the individual Lee weights of b_2 and b_3 $\mathrm{wt}(b) = \mathrm{wt}_L(b_2) + \mathrm{wt}_L(b_3)$. The Hamming weight of a vector in $\mathbb{Z}_2^n$ corresponds to the count of its non-zero entries, while the Hamming distance is the number of positions where two vectors differ. Thus, Φ preserves the Lee distance by transforming it into the Hamming distance, making it an isometry.

Theorem 5.1 *The Gray map $\Phi : \mathbb{Z}_2[u]^{\mu} \times \mathbb{Z}_2[u]^{\nu} \longrightarrow \mathbb{Z}_2^n$ defined as $\Phi(q_0+ur_0, s_0+ut_0) = (r_0, q_0 \oplus r_0, t_0, s_0 \oplus t_0)$ is an isometry, preserving distances between elements.*

Proof: To prove that Φ is an isometry, we need to show that the Lee distance in $\mathbb{Z}_2[u]^{\mu} \times \mathbb{Z}_2[u]^{\nu}$ is preserved as the Hamming distance in $\mathbb{Z}_2[u]^n$ under the mapping Φ. Let (q_0+ur_0, s_0+ut_0) and $(q_0'+ur_0', s_0'+ut_0')$ be two arbitrary elements in $\mathbb{Z}_2[u]^{\mu} \times \mathbb{Z}_2[u]^{\nu}$. The Lee distance between these two elements is defined $d_L((q_0+ur_0, s_0+ut_0),(q_0'+ur_0', s_0'+ut_0')) = wt((q_0+ur_0)-(q_0'+ur_0'))+wt((s_0+ut_0)-(s_0'+ut_0'))$, where $\mathrm{wt}(\mathbf{x})$ denotes the Hamming weight (number of nonzero elements) of vector $\mathbf{x}$. Applying the Gray map Φ to these elements, we have $\Phi(q_0+ur_0, s_0+ut_0) = X = (r_0, q_0\oplus r_0, t_0, s_0\oplus t_0)$. Similarly, $\zeta(q_0'+ur_0', s_0'+ut_0') = X' = (r_0', q_0'\oplus r_0', t_0', s_0'\oplus t_0')$. The Hamming distance between these two elements in $\mathbb{Z}_2^n$ is given by $d_H(x,x') = wt(x-x')$. We can observe that the Lee distance and the Hamming distance in this context are equivalent due to the specific mapping of Φ, where the operations $\oplus$ correspond to the modulo 2 addition. Therefore, the Gray map Φ preserves the distances between elements, and it is an isometry. □

Example 5.1 *Consider the module structure $\mathbb{Z}_2[u]^{\mu} \times \mathbb{Z}_2[u]^{\nu}$, where $\mu = \nu = 1$. The code C in this case is $\{00, 0u, u0, uu\}$. Applying the Gray map $\Phi : \mathbb{Z}_2[u]^{\mu} \times \mathbb{Z}_2[u]^{\nu} \to \mathbb{Z}_2^n$ to any element in C results in a binary linear code. For instance, consider the element uu $\Phi(uu) = (1, 0\oplus 1, 1, 0\oplus 1)$. Simplifying this $\Phi(uu) = (1,1,1,1)$. The full image of C under the Gray map, denoted as $\Phi(C)$, is $\{0000, 0011, 1100, 1111\}$.*

This demonstrates how the Gray map transforms elements from $\mathbb{Z}_2[u]^{\mu} \times \mathbb{Z}_2[u]^{\nu}$ into binary vectors while preserving their structure and properties.

Theorem 5.2 *Let C be a $\mathbb{Z}_2[u]^\mu \times \mathbb{Z}_2[u]^\nu$-additive code of length (μ, ν), and let $C^\perp$ be its dual code, defined as $C^\perp = \{w \in \mathbb{Z}_2[u]^\mu \times \mathbb{Z}_2[u]^\nu : \langle v, w\rangle = 0, \forall v \in C\}$. If the binary image of $C^\perp$ under the Gray map, $\Phi(C^\perp)$, is contained in $\Phi(C)$ (i.e., $\Phi(C^\perp) \subseteq \Phi(C)$), then a quantum code $Q(C)$ with parameters (n, k, d_Q) can be constructed, where $n = 2\mu + 2\nu$, $k = n - \dim(\Phi(C)) - \dim(\Phi(C^\perp))$, and $d_Q = \min\big(d(\Phi(C)), d(\Phi(C^\perp))\big)$.*

Proof: Using the Calderbank-Shor-Steane (CSS) construction, a quantum code can be derived from two classical binary codes C_1 and C_2, provided $C_2 \subseteq C_1$. In this setting, the Gray map Φ transforms the $\mathbb{Z}_2[u]^\mu \times \mathbb{Z}_2[u]^\nu$-additive codes C and $C^\perp$ into binary linear codes $\Phi(C)$ and $\Phi(C^\perp)$, respectively. The condition $\Phi(C^\perp) \subseteq \Phi(C)$ ensures compatibility with the CSS construction. The length of the quantum code $Q(C)$ is determined by the length of the binary vectors, $n = 2\mu + 2\nu$. The dimension of $Q(C)$ is computed as $k = n - \dim(\Phi(C)) - \dim(\Phi(C^\perp))$. The minimum distance d_Q of the quantum code is the minimum of the distances of the binary codes $d_Q = \min\big(d(\Phi(C)), d(\Phi(C^\perp))\big)$. This construction ensures that $Q(C)$ is a valid quantum code with the specified parameters. $\square$

6. Conclusion

In this study, we have characterized the algebraic structure of $\mathbb{Z}_2[u]$-additive and $\mathbb{Z}_2[u]$-double cyclic codes. We established that these codes can be interpreted as submodules of polynomial rings, and we defined the conditions under which they are cyclic. We also identified the generators of these codes and provided a framework for understanding their dimensional properties. This work extends the theory of cyclic codes into a broader algebraic setting, offering new perspectives on the structure and properties of linear codes over finite rings. The results obtained contribute to the understanding of coding theory and its algebraic foundations.

Acknowledgment

The authors express their gratitude to the Manipal Institute of Technology, MAHE, Manipal, India, for providing research facilities. Additionally, they would like to thank the referees for their careful reading and valuable comments, which greatly contributed to improving the manuscript.

References

1. A. K. Singh and P. K. Kewat, *On cyclic codes over the ring $Z_p[u]/\langle u^k\rangle$*. Designs, Codes and Cryptography 74, 1–13 (2015).
2. T. Abualrub and I. Siap, *Reversible cyclic codes over Z_4*. Australas. J. Combin. 38, 195–205 (2007).
3. T. Abualrub, I. Siap and N. Aydin, *Z_2Z_4-Additive Cyclic Codes*. IEEE Trans. Inform. Theory 63(3), 1508–1514 (2014).
4. I. Aydogdu, T. Abualrub and I. Siap, *$Z_2Z_2[u]$–Cyclic and Constacyclic Codes*. IEEE Trans. Inform. Theory 63(8), 4883–4893 (2016).
5. T. Bag, H. Islam, O. Prakash and A. K. Upadhyay, *A study of constacyclic codes over the ring $Z_4[u]/\langle u^2 - 3\rangle$*. Discrete Math. Algorithms Appl. 10(4), 1850056–10 (2018).
6. J. Borges, C. Fernández, J. Pujol, J. Rifá and M. Villanueva, *Z_2Z_4-linear codes: generator matrices and duality*. Designs, Codes and Cryptography 54(2), 167–179 (2010).
7. M. Greferath, *An introduction to ring-linear coding theory*. In: Gröbner Bases, Coding, and Cryptography, Springer, 219–238 (2009).
8. H. Islam and O. Prakash, *On $Z_pZ_p[u, v]$-additive cyclic and constacyclic codes*. arXiv Preprint, 1–21 (2019).
9. H. Islam, O. Prakash and P. Solé, *$Z_4Z_4[u]$-additive cyclic and constacyclic codes*. Adv. Math. Commun. 15, 737–755 (2021).
10. J. Borges, S. T. Dougherty, C. Fernández-Córdoba and R. Ten-Valls, *Binary Images of Z_2Z_4-Additive Cyclic Codes*. IEEE Trans. Inform. Theory 64(12), 7551–7556 (2018).
11. S. Ling and C. Xing, *Coding Theory: A First Course*. Cambridge Univ. Press, Cambridge, UK (2004).
12. M. Shi, L. Qian, L. Sok, N. Aydin and P. Solé, *On constacyclic codes over $Z_4[u]/\langle u^2 - 1\rangle$ and their Gray images*. Finite Fields Appl. 45, 86–95 (2017).
13. M. Shi and X. Wang, *Gray Images of Cyclic Codes over Z_p^2 and $Z_pZ_p^2$*. Discrete Math. 346(7), 1–14 (2022).

14. G. Shashirekha, G. R. Vadiraja Bhatta and P. Poojary, *$Z_2[u]Z_2[u]$-Additive Codes*. Discrete Math. Algorithms Appl. 16 (2024).

15. M. Özen, F. Z. Uzekmek, N. Aydin and N. T. Özzaim, *Cyclic and some constacyclic codes over the ring $Z_4[u]/\langle u^2-1\rangle$*. Finite Fields Appl. 38, 27–39 (2016).

16. O. Prakash, S. Yadav, H. Islam and P. Solé, *On $Z_4Z_4[u^3]$-additive constacyclic codes*. Adv. Math. Commun. 17(1), 246–261 (2023).

17. T. Wu, J. Gao, Y. Gao and F.-W. Fu, *$Z_2Z_2Z_4$-additive cyclic codes*. Adv. Math. Commun. 12(4), 641–657 (2018).

18. B. Yildiz and Ö. Z. Özger, *Generalization of the Lee weight to Z_{p^k}*. TWMS J. Appl. Eng. Math. 2(2), 145–153 (2012).

19. B. Yildiz and N. Aydin, *On cyclic codes over Z_4+uZ_4 and their Z_4-images*. Int. J. Inform. Coding Theory 2(4), 226–237 (2014).

Shashirekha G.,
Department of Mathematics,
Manipal Institute of Technology, Manipal Academy of Higher Education,
Manipal, 576104, Karnataka, India.
E-mail address: shashirekha842@gmail.com

and

Vadiraja Bhatta G. R.,
Department of Mathematics,
Manipal Institute of Technology, Manipal Academy of Higher Education,
Manipal, 576104, Karnataka, India.
E-mail address: grvbhatta@gmail.com, vadiraja.bhatta@manipal.edu