Bull. Math. Soc. Sci. Math. Roumanie
Tome 66 (114), No. 3, 2023, 337–354

$\mathbb{Z}_p(\mathbb{Z}_p + u\mathbb{Z}_p + u^2\mathbb{Z}_p)$-additive cyclic codes

by

Arazgol Ghajari[(1)], Kazem Khashyarmanesh[(2)]

Abstract

Let $\mathcal{R} = \mathbb{Z}_p + u\mathbb{Z}_p + u^2\mathbb{Z}_p$ be a commutative ring with $u^3 = u$ and p is an odd prime. The $\mathbb{Z}_p\mathcal{R}$-additive cyclic codes can be considered as $\mathcal{R}[x]$-submodules of $\frac{\mathbb{Z}_p[x]}{<x^\alpha-1>} \times \frac{\mathcal{R}[x]}{<x^\beta-1>}$, for some positive integers α and β. In this paper, we study the algebraic structure of $\mathbb{Z}_p\mathcal{R}$-additive cyclic codes of length (α, β). To do this, we determine their generator polynomials and minimal generating sets. Moreover, we discuss the duality of the $\mathbb{Z}_p\mathcal{R}$-additive cyclic codes and obtain their generator polynomials. We also study the structure of additive constacyclic codes and quantum codes over $\mathbb{Z}_p\mathcal{R}$.

Key Words: Additive cyclic codes, additive constacyclic codes, minimal generating set.
2010 Mathematics Subject Classification: Primary 12E20; Secondary 94B05, 94B15, 94B60.

1 Introduction

Codes over finite rings have studied since 1970s. Cyclic codes are the important class of linear codes. In 1973, Delsarte [10] introduced the additive codes in terms of association schemes as the subgroups of a commutative group which provides a generalization of cyclic codes. Over the past twenty years or so, by using different techniques, there have appeared in the literature several results giving generalizations of cyclic codes. Some of them can be found in [1, 5, 7, 8, 9, 17]. Recently, codes over mixed alphabet rings viewed as submodules have studied. In one of the such studied, Aydogdu et al. [3] have introduced and described the algebraic properties of $\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$-additive codes with $u^2 = 0$. Also, they determined the standard forms of generator and parity check matrices for these codes. Later, Aydogdu et al. [4] studied $\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$-additive cyclic codes and constacyclic codes. They obtained some optimal binary linear codes as the Gray images of $\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$-additive cyclic codes. Islam et al. [16] continued to explore codes over mixed alphabets and they introduced the mixed alphabets $\mathbb{Z}_4(\mathbb{Z}_4+u\mathbb{Z}_4)$-additive cyclic codes and constacyclic codes which lead to generalizing the codes over $\mathbb{Z}_4$ as well as $\mathbb{Z}_4 + u\mathbb{Z}_4$, where $u^2 = 0$. Meanwhile, Diao et al. [11] have studied the algebraic structure of additive cyclic codes over $\mathbb{Z}_p(\mathbb{Z}_p + u\mathbb{Z}_p)$ with $u^2 = u$. They constructed some optimal linear codes over finite fields and MDSS codes of these codes and they also obtained some quantum codes from additive cyclic codes over the ring $\mathbb{Z}_p(\mathbb{Z}_p+u\mathbb{Z}_p)$. After, Bag et al. [6] have studied quantum codes from cyclic codes over the ring $\frac{\mathbb{Z}_p[u]}{<u^3-u>}$ (see also [15]). Recently, Hou et al. [14] constructed a class of $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes where $v^2 = v$. They studied the asymptotic properties of this class of codes. The purpose of this paper is to study the $\mathbb{Z}_p\mathcal{R}$-additive cyclic codes, where $\mathcal{R} = \mathbb{Z}_p + u\mathbb{Z}_p + u^2\mathbb{Z}_p$ with $u^3 = u$.

The main motive of this work is to find out the generator polynomial, minimal spanning set of $\mathbb{Z}_p\mathcal{R}$-additive cyclic codes and determine the generator polynomials of a dual code. The paper is organized as follows: In the next section we discuss the structural properties of $\mathbb{Z}_p\mathcal{R}$-additive cyclic codes and find the minimal generating sets of these codes. Moreover, get some properties of separable additive cyclic codes and the Gray image of a additive cyclic code over $\mathbb{Z}_p\mathcal{R}$. In Section 3, we determine the generator polynomials of the dual codes of $\mathbb{Z}_p\mathcal{R}$-additive cyclic codes. In the final section, we describe $\mathbb{Z}_p\mathcal{R}$-additive constacyclic codes and quantum codes.

2 $\mathbb{Z}_p\mathcal{R}$-additive cyclic codes

In this paper, we determine the minimal generating sets of $\mathbb{Z}_p\mathcal{R}$-additive cyclic codes. Assume that $\mathbb{Z}_p$ is the ring of integers modulo p, where p is an odd prime and suppose that

$$\mathcal{R} = \{(1-u^2)a + 2^{-1}(u^2+u)b + 2^{-1}(u^2-u)c \mid \quad a, b, c \in \mathbb{Z}_p\}$$

with $u^3 = u$, where $(1-u^2)$, $2^{-1}(u^2+u)$ and $2^{-1}(u^2-u)$ are orthogonal idempotents of $\mathcal{R}$. We suppose that $a+ub+u^2c = (1-u^2)a + 2^{-1}(u^2+u)(a+b+c) + 2^{-1}(u^2-u)(a-b+c)$ is an element of $\mathcal{R}$. Then $a+bu+cu^2$ is a unit over $\mathcal{R}$ if and only if $a, a+b+c$ and $a-b+c$ are units of $\mathbb{Z}_p^* = \mathbb{Z}_p\backslash\{0\}$. It is clear that $\mathbb{Z}_p$ a subring of the ring $\mathcal{R}$. Being inspired by the structure of $\mathbb{Z}_p\mathcal{R}$-additive codes, we define the following set

$$\mathbb{Z}_p\mathcal{R} = \{(a,b) |\ a \in \mathbb{Z}_p,\ b \in \mathcal{R}\}.$$

Consider the map $\rho : \mathcal{R} \to \mathbb{Z}_p$ given by

$$\rho((1-u^2)a + 2^{-1}(u^2+u)b + 2^{-1}(u^2-u)c) = a,$$

where a, b, c are arbitrary elements of $\mathbb{Z}_p$. Obviously, ρ is a ring homomorphism. So we can define a multiplication

$$\begin{aligned} * : \mathcal{R} \times \mathbb{Z}_p\mathcal{R} &\to \mathbb{Z}_p\mathcal{R} \\ d * (a,b) &= (\rho(d)a, db), \end{aligned}$$

where $d = (1-u^2)\mathfrak{a} + 2^{-1}(u^2+u)\mathfrak{b} + 2^{-1}(u^2-u)\mathfrak{c} \in \mathcal{R}$ with $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \in \mathbb{Z}_p$. Thus the extension of multiplication $*$ to $(a_0, \cdots, a_{\alpha-1}, b_0, \cdots, b_{\beta-1}) \in \mathbb{Z}_p^\alpha \times \mathcal{R}^\beta$ by the elements of $\mathcal{R}$ is defined by

$$d * (a,b) = (\rho(d)a_0, \cdots, \rho(d)a_{\alpha-1}, db_0, \cdots, db_{\beta-1}),$$

where $a = (a_0, a_1, \cdots, a_{\alpha-1}) \in \mathbb{Z}_p^\alpha$ and $b = (b_0, \cdots, b_{\beta-1}) \in \mathcal{R}^\beta$. Now, in view of the above multiplication, it is easy to see that $\mathbb{Z}_p^\alpha \times \mathcal{R}^\beta$ is an $\mathcal{R}$-module.

Definition 1. *Suppose that C is a non-empty subset of $\mathbb{Z}_p^\alpha \times \mathcal{R}^\beta$. Then C is called a $\mathbb{Z}_p\mathcal{R}$-additive code if C is an $\mathcal{R}$-submodule of $\mathbb{Z}_p^\alpha \times \mathcal{R}^\beta$.*

Now, consider a Gray map

$$\begin{aligned} \phi : \mathcal{R} &\to \mathbb{Z}_p^3 \\ \phi((1-u^2)a + 2^{-1}(u^2+u)b &+ 2^{-1}(u^2-u)c) = (a,b,c), \end{aligned}$$

where $a, b, c \in \mathbb{Z}_p$. The map ϕ is linear and its extension is

$$\phi : \mathcal{R}^\beta \to \mathbb{Z}_p^{3\beta}$$
$$\phi(s_0, \cdots, s_{\beta-1}) = (a_0, \cdots, a_{\beta-1}, b_0, \cdots, b_{\beta-1}, c_0, \cdots, c_{\beta-1}),$$

where $s_i = (1-u^2)a_i + 2^{-1}(u^2+u)b_i + 2^{-1}(u^2-u)c_i \in \mathcal{R}$ for $i = 0, \cdots, \beta-1$. Now, with the aid of the map ϕ, we define a Gray map φ as follows:

$$\varphi : \mathbb{Z}_p^\alpha \times \mathcal{R}^\beta \to \mathbb{Z}_p^{\alpha+3\beta}$$
$$\varphi(d_0, \cdots, d_{\alpha-1}, s_0, \cdots, s_{\beta-1}) = (d_0, \cdots, d_{\alpha-1}, \phi(s_0, \cdots, s_{\beta-1})),$$

where $d_i \in \mathbb{Z}_p$ for $i = 0, \cdots, \alpha-1$. The image $C = \varphi(C)$ of a $\mathbb{Z}_p\mathcal{R}$-additive code over $\mathbb{Z}_p$ is said to be a $\mathbb{Z}_p\mathcal{R}$-linear code of length $n = \alpha + 3\beta$.

Definition 2. *For a codeword* $\mathrm{x} \in \mathbb{Z}_p^n = \{(x_1, \cdots, x_n)\ x_i \in \mathbb{Z}_p\}$, *the Hamming weight of* x *is defined as the number of non-zero coordinate positions, which is denoted by* $w_H(\mathrm{x})$.

Let $\mathcal{C}$ be a cyclic code over $\mathbb{Z}_p$. The Hamming distance between two codewords $x, y \in \mathcal{C}$ is defined as $d_H(x, y) = w_H(x - y)$ and defined the minimum Hamming distance of $\mathcal{C}$ over $\mathbb{Z}_p$ as $d_H(\mathcal{C}) = \min\{d_H(x, y) \mid \ x \neq y \ \text{ for all } x, y \in \mathcal{C}\}$.

Definition 3. *Let* $w = (w_0, \cdots, w_{\alpha-1}, \mathrm{w}_0, \cdots, \mathrm{w}_{\beta-1})$ *be an element of* $\mathbb{Z}_p^\alpha \times \mathcal{R}^\beta$. *The Lee weight of* w *is defined as*

$$w_L(w) = w_H(\varphi(w)).$$

For any elements $v, w \in \mathbb{Z}_p^\alpha \times \mathcal{R}^\beta$, the Lee distance is $d_L(v, w) = w_L(v - w)$. An inner product for elements $v = (v_0, \cdots, v_{\alpha-1}, \mathrm{v}_0, \cdots, \mathrm{v}_{\beta-1})$, $w = (w_0, \cdots, w_{\alpha-1}, \mathrm{w}_0,$ $\cdots, \mathrm{w}_{\beta-1})$ of $\mathbb{Z}_p^\alpha \times \mathcal{R}^\beta$ is defined as

$$v \cdot w = (1-u^2)\sum_{i=0}^{\alpha-1} v_i w_i + \sum_{j=0}^{\beta-1} \mathrm{v}_j \mathrm{w}_j.$$

Assume that C is a $\mathbb{Z}_p\mathcal{R}$-additive code. Then the dual code of C, denoted by $C^\perp$, is defined to be

$$C^\perp = \{v \in \mathbb{Z}_p^\alpha \times \mathcal{R}^\beta \quad \mid v \cdot u = 0 \quad \text{for all} \quad u \in C\}.$$

Put $\mathcal{R}_{\alpha,\beta} := \mathbb{Z}_p[x]/\langle x^\alpha - 1\rangle \times \mathcal{R}[x]/\langle x^\beta - 1\rangle$. Identifying each $v = (a, b) \in \mathbb{Z}_p^\alpha \times \mathcal{R}^\beta$ with of polynomials $(a(x), b(x))$, where $a(x) = \sum_{i=0}^{\alpha-1} a_i x^i \in \mathbb{Z}_p[x]/\langle x^\alpha - 1\rangle$ and $b(x) = \sum_{j=0}^{\beta-1} b_j x^j$ $\in \mathcal{R}[x]/\langle x^\beta - 1\rangle$, we get a one-to-one correspondence between $\mathbb{Z}_p^\alpha \times \mathcal{R}^\beta$ and $\mathcal{R}_{\alpha,\beta}$. For any $f(x) = \sum f_i x^i \in \mathcal{R}[x]$ and $(a(x), b(x)) \in \mathcal{R}_{\alpha,\beta}$, we define the product $f(x) * (a(x), b(x)) = (\rho(f(x))a(x), f(x)b(x))$, where $\rho(f(x)) = \sum \rho(f_i)x^i$.

Definition 4. *A* $\mathbb{Z}_p\mathcal{R}$*- additive code* C *of length* (α, β) *is called a* $\mathbb{Z}_p\mathcal{R}$*-additive cyclic code if, for any* $z = (c_0, \cdots, c_{\alpha-1}, r_0, \cdots, r_{\beta-1}) \in C$, *we have*

$$\sigma_{\alpha,\beta}(z) = (c_{\alpha-1}, c_0, \cdots, c_{\alpha-2}, r_{\beta-1}, r_0, \cdots, r_{\beta-2}) \in C,$$

where $\sigma_{\alpha,\beta}$ *is a permutation of* $\mathbb{Z}_p^\alpha\mathcal{R}^\beta$.

Definition 5. *A $\mathbb{Z}_p\mathcal{R}$-additive code C is cyclic in $\mathbb{Z}_p^\alpha \times \mathcal{R}^\beta$ if and only if C is an $\mathcal{R}[x]$-submodule of $\mathcal{R}_{\alpha,\beta}$.*

Definition 6. *A unique monic polynomial of the lowest degree for a non-zero submodule M of $\mathcal{R}_{\alpha,\beta}$ is called a generator polynomial. For a $\mathbb{Z}_p\mathcal{R}$-additive cyclic code C, this generator polynomial is called a generator polynomial C.*

In the following theorem, we determine the generator polynomial of the $\mathbb{Z}_p\mathcal{R}$-additive cyclic code C.

Theorem 1. *Let C be a $\mathbb{Z}_p\mathcal{R}$-additive cyclic code of length (α,β). Then C is an $\mathcal{R}[x]$-submodule of $\mathcal{R}_{\alpha,\beta}$ given by*

$$C = \langle (f(x),0),(l(x),(1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x))\rangle,$$

where $f(x)|(x^\alpha-1)$, $f_i(x)|(x^\beta-1)$ for $i=1,2,3$, and also $f(x),l(x)\in\mathbb{Z}_p[x]/\langle x^\alpha-1\rangle$, $f_i(x)\in\mathcal{R}[x]/\langle x^\beta-1\rangle$ for $i=1,2,3$.

Proof. Assume that the map

$$\eta : \mathbb{Z}_p[x]/\langle x^\alpha-1\rangle \times \mathcal{R}[x]/\langle x^\beta-1\rangle \to \mathcal{R}[x]/\langle x^\beta-1\rangle \quad \text{given by} \quad (a(x),b(x)) \mapsto b(x)$$

is the projection map. Clearly, the map η is an $\mathcal{R}[x]$-module homomorphism with

$$\mathrm{Ker}(\eta) = \{(f'(x),0)\in C| \quad f'(x)\in\mathbb{Z}_p[x]/\langle x^\alpha-1\rangle\}.$$

Put $S := \{f'(x)\in\mathbb{Z}_p/\langle x^\alpha-1\rangle|(f'(x),0)\in\mathrm{Ker}(\eta)\}$. It is clear that S is a principal ideal. Therefore, there exists a monic polynomial $f(x)\in\mathbb{Z}_p[x]/\langle x^\alpha-1\rangle$ such that $S=\langle f(x)\rangle$. Thus, $\mathrm{Ker}(\eta)=\langle (f(x),0)\rangle$. We know that the homomorphic image of C under η is an ideal of $\mathcal{R}[x]/\langle x^\beta-1\rangle$. By [12, Theorem 4], we have

$$\eta(C) = \langle (1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x)\rangle,$$

where f_i are monic polynomials over $\mathbb{Z}_p$ with $f_i(x)|(x^\beta-1)$ for $1\le i\le 3$. Since C is an $\mathcal{R}[x]$-submodule of $\mathcal{R}_{\alpha,\beta}$ and it is generated by

$$(f(x),0),(l(x),(1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x)),$$

for some $l(x)\in\mathbb{Z}_p[x]/\langle x^\alpha-1\rangle$. This means that

$$C = \langle (f(x),0),(l(x),(1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x))\rangle,$$

where $f(x),l(x)\in\mathbb{Z}_p[x]/\langle x^\alpha-1\rangle$ and $f_i(x)\in R[x]/\langle x^\beta-1\rangle$, with $f(x)|(x^\alpha-1)$ and $f_i(x)|(x^\beta-1)$ for $1\le i\le 3$. ∎

Let $C=\langle (f(x),0),(l(x),(1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x))\rangle$ be a $\mathbb{Z}_p\mathcal{R}$-additive cyclic code of length (α,β). Assume that C_α (respectively C_β) is the canonical projection of C on the first α (respectively last β) coordinates. We know that $C_\alpha=\langle \gcd(f(x),l(x))\rangle$ is a cyclic code of length α over $\mathbb{Z}_p$, and $C_\beta=\langle (1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x)\rangle$ is a cyclic code of length β over $\mathcal{R}$.

Lemma 1. *Let the situation and notation be as in 1. Suppose that* $C = \langle (f(x),0),(l(x),(1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x))\rangle$ *is a* $\mathbb{Z}_p\mathcal{R}$*-additive cyclic code. Then* $((1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x))|(x^\beta-1)$*, where* $f_i(x)g_i(x)=(x^\beta-1)$ *for* $1\le i\le 3$.

Proof. We know that $f_i(x)|(x^\beta-1)$ for $1\le i\le 3$. Thus, there are the polynomials $g_i(x)$ such that $f_i(x)g_i(x)=(x^\beta-1)$ for $1\le i\le 3$. So, we get

$$\begin{aligned}((1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x))((1-u^2)g_1(x)\\ +2^{-1}(u^2+u)g_2(x)+2^{-1}(u^2-u)g_3(x))=(x^\beta-1).\end{aligned}$$

This implies that

$$((1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x))|(x^\beta-1).$$

□

Lemma 2. *Let the situation and notation be as in 1. Assume that* C *is a* $\mathbb{Z}_p\mathcal{R}$*-additive cyclic code and given by*

$$C=\langle (f(x),0),(l(x),(1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x))\rangle,$$

where $f_i(x)g_i(x)=(x^\beta-1)$ *for* $1\le i\le 3$*. Thus,* $f(x)|g_1(x)l(x)$.

Proof. We have

$$\begin{aligned}&((1-u^2)g_1(x)+2^{-1}(u^2+u)g_2(x)+2^{-1}(u^2-u)g_3(x))*\\ &(l(x),(1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x))\\ &=(l(x)g_1(x),0).\end{aligned}$$

This implies that $(l(x)g_1(x),0)\in \mathrm{Ker}(\eta)$. Hence $f(x)|l(x)g_1(x)$. □

The following corollary is immediate from the above lemma.

Corollary 1. *Let the situation and notation be as in 1. Let* C *be a* $\mathbb{Z}_p\mathcal{R}$*-additive code given by*

$$C=\langle (f(x),0),(l(x),(1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x))\rangle,$$

where $f_i(x)g_i(x)=(x^\beta-1)$ *for* $1\le i\le 3$*. Then* $f(x)|\gcd(f(x),l(x)g_1(x))$.

Definition 7. *Let* $S=\{\mathsf{v}_1,\cdots,\mathsf{v}_n\}$ *be a set of vectors.The vectors* $\mathsf{v}_1,\cdots,\mathsf{v}_n$ *span a vector space* D *of* $\mathbb{Z}_p$*, if*

(i) $\mathsf{v}_1,\cdots,\mathsf{v}_n\in D$,

(ii) $\mathsf{u}=x_1\mathsf{v}_1+x_2\mathsf{v}_2+\cdots+x_n\mathsf{v}_n$ *for all* $\mathsf{u}\in D, x_i\in\mathbb{Z}_p$ *with* $1\le i\le n$.

The span vector space is denoted by $\mathrm{Span}(S)$.

Let C be a non-empty subset of $\mathbb{Z}_p^\alpha\mathcal{R}^\beta$. If C forms a subspace of $\mathbb{Z}_p^\alpha\mathcal{R}^\beta$, then C is called a linear code. In the next theorem, we obtain a minimal generating set of $\mathbb{Z}_p\mathcal{R}$-additive cyclic code.

Theorem 2. *Suppose that C is a $\mathbb{Z}_p\mathcal{R}$-additive cyclic code of length (α,β) and $f_i(x), g_i(x)$ are monic polynomials such that $f_i(x)g_i(x) = (x^\beta - 1)$ for $1 \leq i \leq 3$. Let*

$$S_1 = \bigcup_{i=0}^{\alpha-deg(f(x))-1} \{x^i * (f(x),0)\},$$
$$S_2 = \bigcup_{i=0}^{deg(g_1(x))-1} \{x^i * (l(x),(1-u^2)f_1(x))\},$$
$$S_3 = \bigcup_{i=0}^{deg(g_2(x))-1} \{x^i * (0,2^{-1}(u^2+u)f_2(x))\},$$
$$S_4 = \bigcup_{i=0}^{deg(g_3(x))-1} \{x^i * (0,2^{-1}(u^2-u)f_3(x))\}.$$

Then $S_1 \cup S_2 \cup S_3 \cup S_4$ is a generating set of C. Furthermore, C has p^k codewords, where

$$k = \alpha - \deg(f(x)) + \deg(g_1(x)) + \deg(g_2(x)) + \deg(g_3(x)).$$

Proof. Assume that $c(x)$ is an arbitrary codeword in C. Then there exist $c_1(x), c_2(x) \in \mathcal{R}[x]$ such that

$$\begin{aligned} c(x) = c_1(x) * (f(x),0) + c_2(x) * ((1-u^2)f_1(x) \\ + 2^{-1}(u^2+u)f_2(x) + 2^{-1}(u^2-u)f_3(x)). \end{aligned}$$

If $\deg(c_1(x)) \leq (\alpha - \deg(f(x)) - 1)$, then $c_1(x) * (f(x),0) \in \mathrm{Span}(S_1)$. Otherwise, by applying the division algorithm, there exist polynomials $q(x)$ and $r(x)$ in $\mathcal{R}[x]$ such that

$$c_1(x) = \frac{(x^\alpha - 1)}{f(x)} q(x) + r(x),$$

where $\deg(r(x)) \leq (\alpha - \deg(f(x)) - 1)$ or $r(x) = 0$. Hence,

$$\begin{aligned} c_1(x) * (f(x),0) &= (\frac{x^\alpha - 1}{f(x)} q(x) + r(x)) * (f(x),0) \\ &= r(x) * (f(x),0). \end{aligned}$$

This implies that $c_1(x) * (f(x),0) \in \mathrm{Span}(S_1)$, and so

$$c_2(x) = (1-u^2)a(x) + 2^{-1}(u^2+u)b(x) + 2^{-1}(u^2-u)d(x).$$

We have

$$\begin{aligned}
c_2(x)*&(l(x),(1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x))\\
&=((1-u^2)a(x)+2^{-1}(u^2+u)b(x)+2^{-1}(u^2-u)d(x))\\
&*(l(x),(1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x))\\
&=a(x)*(l(x),(1-u^2)f_1(x))+b(x)*(0,2^{-1}(u^2+u)f_2(x))\\
&+d(x)*(0,2^{-1}(u^2-u)f_3(x)).
\end{aligned}$$

According to Lemma 2, $f(x)|l(x)g_1(x)$. Therefore, $f(x)h(x)=l(x)g_1(x)$ for some polynomial $h(x)$. If $\deg(a(x))\le\deg(g_1(x))-1$, then $a(x)*(l(x),(1-u^2)f_1(x))\in\mathrm{Span}(S_2)$. Otherwise, by using the division algorithm, there exist $q_1(x),r_1(x)\in\mathcal{R}[x]$ such that

$$a(x)=g_1(x)q_1(x)+r_1(x),$$

where $\deg(r_1(x))\le\deg(g_1(x))-1$ or $r_1(x)=0$. Therefore,

$$\begin{aligned}
a(x)*(l(x),(1-u^2)f_1(x))&=(q_1(x)g_1(x)+r_1(x))*(l(x),(1-u^2)f_1(x))\\
&=q_1(x)(l(x)g_1(x),0)+r_1(x)*(l(x),(1-u^2)f_1(x)).
\end{aligned}$$

Hence $q_1(x)*(l(x)g_1(x),0)\in\mathrm{Span}(S_1)$ and $r_1(x)*(l(x),(1-u^2)f_1(x))\in\mathrm{Span}(S_2)$. If $\deg(b(x))\le\deg(g_2(x))-1$, then $b(x)*(0,2^{-1}(u^2+u)f_2(x))\in\mathrm{Span}(S_3)$. Again, by applying the division algorithm, there exist $q_2(x),r_2(x)\in\mathcal{R}[x]$ such that

$$b(x)=g_2(x)q_2(x)+r_2(x),$$

where $\deg(r_2(x))\le\deg(g_2(x))-1$ or $r_2(x)=0$. Thus

$$\begin{aligned}
b(x)*(0,2^{-1}(u^2+u)f_2(x))&=(g_2(x)q_2(x)+r_2(x))*(0,2^{-1}(u^2+u)f_2(x))\\
&=r_2(x)*(0,2^{-1}(u^2+u)f_2(x)).
\end{aligned}$$

Furthermore, we have $r_2(x)*(0,2^{-1}(u^2+u)f_2(x))\in\mathrm{Span}(S_3)$.
Now, if $\deg(d(x))\le\deg(g_3(x))-1$, then $d(x)*(0,2^{-1}(u^2-u)f_3(x))\in\mathrm{Span}(S_4)$. Finally, by using the division algorithm, there exist $q_3(x),r_3(x)\in\mathcal{R}[x]$ such that

$$d(x)=g_3(x)q_3(x)+r_3(x),$$

where $\deg(r_3(x))\le\deg(g_3(x))-1$ or $r_3(x)=0$. Therefore,

$$\begin{aligned}
d(x)*(0,2^{-1}(u^2-u)f_3(x))&=(g_3(x)q_3(x)+r_3(x))*(0,2^{-1}(u^2-u)f_3(x))\\
&=r_3(x)*(0,2^{-1}(u^2-u)f_3(x)).
\end{aligned}$$

Thus we can assume that $d(x)*(0,2^{-1}(u^2-u)f_3(x))\in\mathrm{Span}(S_4)$. Clearly, the elements in $S_1\cup S_2\cup S_3\cup S_4$ are $\mathcal{R}$-linearly independent, and so $S_1\cup S_2\cup S_3\cup S_4$ is a minimal generating set of C as an $\mathcal{R}$-module. Moreover, $|C|=p^k$, where

$$k=\alpha-\deg(f(x))+\deg(g_1(x))+\deg(g_2(x))+\deg(g_3(x)).$$

□

Definition 8. *Let C be a $\mathbb{Z}_p\mathcal{R}$-additive linear code. Then C is called a self-orthogonal $\mathbb{Z}_p\mathcal{R}$-additive code if $C \subseteq C^{\perp}$.*

Lemma 3. *Suppose that C is a self orthogonal $\mathbb{Z}_p\mathcal{R}$-additive cyclic code. Then $\varphi(C)$ is a self-orthogonal code.*

Proof. Let $\mathrm{x} = (x_0, \cdots, x_{\alpha-1}, \mathrm{x}_0, \cdots, \mathrm{x}_{\beta-1})$ and $\mathrm{y} = (y_0, \cdots, y_{\alpha-1}, \mathrm{y}_0, \cdots, \mathrm{y}_{\beta-1})$ be codewords in C, where $\mathrm{x}_i = (1-u^2)a_i + 2^{-1}(u^2+u)b_i + 2^{-1}(u^2-u)c_i$ and $\mathrm{y}_i = (1-u^2)\mathrm{a}_i + 2^{-1}(u^2+u)\mathrm{b}_i + 2^{-1}(u^2-u)\mathrm{c}_i$ with a_i, a_i, b_i, b_i, $c_i, \mathrm{c}_i \in \mathbb{Z}_p$ for $0 \leq i \leq \beta - 1$. Then

$$\begin{aligned}
\mathrm{x} \cdot \mathrm{y} &= (1-u^2)\sum_{i=0}^{\alpha-1}(x_i y_i) + \sum_{j=0}^{\beta-1}(\mathrm{x}_j \mathrm{y}_j) \\
&= (1-u^2)\sum_{i=0}^{\alpha-1}(x_i y_i) + \sum_{j=0}^{\beta-1}((1-u^2)a_j\mathrm{a}_j + 2^{-1}(u^2+u)b_j\mathrm{b}_j + 2^{-1}(u^2-u)c_j\mathrm{c}_j) \\
&= 0.
\end{aligned}$$

This implies that

$$\begin{aligned}
\sum_{i=0}^{\alpha-1}(x_i y_i) &= 0, \qquad & \sum_{j=0}^{\beta-1}(a_j\mathrm{a}_j) &= 0, \\
\sum_{j=0}^{\beta-1}(b_j\mathrm{b}_j) &= 0, \qquad & \sum_{j=0}^{\beta-1}(c_j\mathrm{c}_j) &= 0,
\end{aligned}$$

over $\mathbb{Z}_p$. Thus $\varphi(\mathrm{x}) \cdot \varphi(\mathrm{y}) = 0$. Hence $\varphi(C)$ is self orthogonal. ∎

Definition 9. *A $\mathbb{Z}_p\mathcal{R}$-additive code C is called separable if C is the direct product of C_α and C_β, that is, $C = C_\alpha \times C_\beta$ and $l = 0$.*

Lemma 4. *Let the situation and notation be as in 1 and let*

$$C = \langle (f(x), 0), (0, (1-u^2)f_1(x) + 2^{-1}(u^2+u)f_2(x) + 2^{-1}(u^2-u)f_3(x)) \rangle$$

be a $\mathbb{Z}_p\mathcal{R}$-additive cyclic code. Then $C = C_\alpha \times C_\beta$ is a separable code, where C_α is a $\mathbb{Z}_p$-cyclic code and C_β is a cyclic code over $\mathcal{R}$.

Proof.

$$\begin{aligned}
(c_\alpha, c_\beta) \in C \Leftrightarrow\ & c_\alpha = w_1 f(x), \quad \text{and} \\
& c_\beta = w_2((1-u^2)f_1(x) + 2^{-1}(u^2+u)f_2(x) + 2^{-1}(u^2-u)f_3(x)) \\
\Leftrightarrow\ & c_\alpha \in C_\alpha = \langle f(x) \rangle \quad \text{and} \\
& c_\beta \in C_\beta = \langle (1-u^2)f_1(x) + 2^{-1}(u^2+u)f_2(x) + 2^{-1}(u^2-u)f_3(x) \rangle \\
\Leftrightarrow\ & C = C_\alpha \times C_\beta, \quad \text{where} \quad C_\alpha = \langle f(x) \rangle \quad \text{and} \\
& C_\beta = \langle (1-u^2)f_1(x) + 2^{-1}(u^2+u)f_2(x) + 2^{-1}(u^2-u)f_3(x) \rangle.
\end{aligned}$$

∎

Proposition 1. *Let C be a $\mathbb{Z}_p\mathcal{R}$-additive cyclic code of length (α, β). Then C is a separable code if and only if C_α is a cyclic code of length α over $\mathbb{Z}_p$ and C_β is a cyclic code of length β over $\mathcal{R}$.*

Proof. Let C be a separable code. Suppose that $(a_0, \cdots, a_{\alpha-1}, b_0, \cdots, b_{\beta-1})$ is a codeword in C, where $(a_0, \cdots, a_{\alpha-1}) \in C_\alpha$ and $(b_0, \cdots, b_{\beta-1}) \in C_\beta$. It is clear that

$$(a_{\alpha-1}, a_0, \cdots, a_{\alpha-2}, b_{\beta-1}, b_0, \cdots, b_{\beta-2}) \in C.$$

So $(a_{\alpha-1}, a_0, \cdots, a_{\alpha-2}) \in C_\alpha$ and $(b_{\beta-1}, b_0, \cdots, b_{\beta-2}) \in C_\beta$.

For the converse implication, assume that C_α (*respectively* C_β) is a cyclic code over $\mathbb{Z}_p$ (*respectively* $\mathcal{R}$). Then $(a_{\alpha-1}, a_0, \cdots, a_{\alpha-2}) \in C_\alpha$ and $(b_{\beta-1}, b_0, \cdots, b_{\beta-2}) \in C_\beta$. These imply that $(a_{\alpha-1}, a_0, \cdots, a_{\alpha-2}, b_{\beta-1}, b_0, \cdots, b_{\beta-2})$ belongs to $C_\alpha \times C_\beta = C$. ∎

Lemma 5. *Let $C = C_\alpha \times C_\beta$ be a separable additive code of length $\alpha + \beta$ over $\mathbb{Z}_p\mathcal{R}$. Then $C^\perp \subseteq C$ if and only if $C_\alpha^\perp \subseteq C_\alpha$ and $C_\beta^\perp \subseteq C_\beta$.*

Proof. Let $C_\alpha^\perp \subseteq C_\alpha$ and $C_\beta^\perp \subseteq C_\beta$. Then we get $C_\alpha^\perp \times C_\beta^\perp \subseteq C$. Conversely, suppose that $C^\perp \subseteq C$. Obviously, $C_\alpha^\perp \subseteq C$ and $C_\beta^\perp \subseteq C$. Thus, the sentence is completed. ∎

Note that the converse implication in Lemma 2.14 is not true in general. Moreover, $C^\perp \neq C_\alpha^\perp \times C_\beta^\perp$ in general.

3 Duality of $\mathbb{Z}_p\mathcal{R}$-additive cyclic codes

In this section, we shall study the properties of the duality of $\mathbb{Z}_p\mathcal{R}$-additive cyclic codes. In [11, Theorem 4.1], it was shown that the dual code of a $\mathbb{Z}_p\mathcal{R}$-additive cyclic code is also a $\mathbb{Z}_p\mathcal{R}$-additive cyclic. Hence, we denote

$$C^\perp = \langle (\overline{f}(x), 0), (\bar{l}(x), (1-u^2)\overline{f}_1(x) + 2^{-1}(u^2+u)\overline{f}_2(x) + 2^{-1}(u^2-u)\overline{f}_3(x)) \rangle,$$

where $\overline{f}_i(x)\overline{g}_i(x) = x^\beta - 1$ in $\mathcal{R}[x]$ for $1 \leq i \leq 3$ and $\overline{f}(x), \bar{l}(x) \in \mathbb{Z}_p[x]/\langle x^\alpha - 1\rangle$ with $\overline{f}(x)|(x^\alpha - 1)$, $\deg(\bar{l}(x)) \leq \deg(\overline{f}(x))$ and $\overline{f}(x)|\bar{l}(x)\overline{g}_1(x)$. Recall that the reciprocal polynomial of a polynomial $p(x)$ is $x^{\deg(p(x))}p(x^{-1})$ and is denoted by $p^*(x)$. As in the theory of dual cyclic codes, the reciprocal polynomials play an important role on our method in this section. We denote the polynomial $\sum_{i=0}^{m-1} x^i$ by $\theta_m(x)$ in which m denotes the least common multiple of α and β.

Proposition 2. *For any positive integers m and n, we have*

$$x^{nm} - 1 = (x^n - 1)\theta_m(x^n).$$

Definition 10. *Let* $\mathrm{v}(x) = (v(x), \mathfrak{v}(x))$ *and* $\mathrm{w}(x) = (w(x), \mathfrak{w}(x))$ *be elements in* $\mathcal{R}_{\alpha,\beta}$. *We define the map*

$$\Omega : \mathcal{R}_{\alpha,\beta} \times \mathcal{R}_{\alpha,\beta} \to \mathcal{R}[x]/\langle x^m - 1\rangle$$

by defining

$$\begin{aligned}\Omega(\mathrm{v}(x),\mathrm{w}(x)) &= (1-u^2)v(x)\theta_{\frac{m}{\alpha}}(x^{\alpha})x^{m-1-deg(w(x))}w^*(x)\\ &+ \mathfrak{v}(x)\theta_{\frac{m}{\beta}}(x^{\beta})x^{m-1-deg(\mathfrak{w}(x))}\mathfrak{w}^*(x) \quad mod\ (x^m-1)\end{aligned}$$

The map Ω is a bilinear map between $\mathcal{R}[x]$-modules.

By using a method similar that used in the proof of Proposition 1 in [11], one can establish the next proposition.

Proposition 3. *Assume that* $\mathrm{v}=(v,\mathfrak{v})$, $\mathrm{w}=(w,\mathfrak{w})\in Z_p^{\alpha}\times\mathcal{R}^{\beta}$. *Then* v *is orthogonal to* w *and all its shifts if and only if*

$$\Omega(\mathrm{v}(x),\mathrm{w}(x))=0.$$

Proposition 4. *Suppose that* $\mathrm{v}=(v(x),\mathfrak{v}(x))$ *and* $\mathrm{w}=(w(x),\mathfrak{w}(x))$ *are elements in* $\mathcal{R}_{\alpha,\beta}$ *such that* $\Omega(\mathrm{v}(x),\mathrm{w}(x))=0$. *If* $\mathfrak{v}(x)$ *or* $\mathfrak{w}(x)$ *equals 0, then* $v(x)w^*(x)\equiv 0 \mod (x^{\alpha}-1)$ *over* $\mathbb{Z}_p$. *If* $v(x)=0$ *or* $w(x)=0$, *then* $\mathfrak{v}(x)\mathfrak{w}^*(x)\equiv 0 \mod (x^{\beta}-1)$ *over* $\mathcal{R}$.

Proof. The proof process is the same as that of Proposition 2 in [11]. □

Lemma 6. *Suppose that* $C=\langle (f(x),0),(l(x),(1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x))\rangle$ *is a* $\mathbb{Z}_p\mathcal{R}$*-additive cyclic code. Then*

$$\begin{aligned}
\mid C_{\alpha}\mid &= p^{\alpha-deg(gcd(f(x),l(x)))}, \quad \mid C_{\beta}\mid = p^{3\beta-deg(f_1(x))-deg(f_2(x))-deg(f_3(x))},\\
\mid (C_{\alpha})^{\perp}\mid &= p^{deg(gcd(f(x),l(x)))}, \quad \mid (C_{\beta})^{\perp}\mid = p^{deg(f_1(x))+deg(f_2(x))+deg(f_3(x))},\\
\mid (C^{\perp})_{\alpha}\mid &= p^{deg(f(x))}, \quad \mid 2^{-1}(u^2-u)(C^{\perp})_{\beta}\mid = p^{deg(f_3(x))},\\
\mid (C^{\perp})_{\beta}\mid &= p^{deg(f_1(x))+deg(f_2(x))+deg(f_3(x))+deg(f(x))-deg(gcd(f(x),l(x)))},\\
\mid (1-u^2)C_{\beta}\mid &= p^{\beta-deg(f_1(x))}, \quad \mid 2^{-1}(u^2+u)C_{\beta}\mid = p^{\beta-deg(f_2(x))},\\
\mid 2^{-1}(u^2-u)C_{\beta}\mid &= p^{\beta-deg(f_3(x))}, \quad \mid (1-u^2)(C_{\beta})^{\perp}\mid = p^{deg(f_1(x))},\\
\mid 2^{-1}(u^2+u)(C_{\beta})^{\perp}\mid &= p^{deg(f_2(x))}, \quad \mid 2^{-1}(u^2-u)(C_{\beta})^{\perp}\mid = p^{deg(f_3(x))},\\
\mid (1-u^2)(C^{\perp})_{\beta}\mid &= p^{deg(f_1(x))+deg(f(x))-deg(gcd(f(x),l(x)))},\\
\mid 2^{-1}(u^2+u)(C^{\perp})_{\beta}\mid &= p^{deg(f_2(x))}.
\end{aligned}$$

Proof. We know that $C_{\alpha}=\langle \gcd(f(x),l(x))\rangle$ and that $C_{\beta}=\langle (1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x)\rangle$, which are cyclic codes of lengths α (over $\mathbb{Z}_p$) and β (over $\mathcal{R}$), respectively. Thus $\mid C_{\alpha}\mid = p^{\alpha-\deg(\gcd(f(x),l(x)))}$ and $\mid C_{\beta}\mid = p^{3\beta-\deg(f_1(x))-\deg(f_2(x))-\deg(f_3(x))}$. Furthermore, one can calculate the size of each codes $(C^{\perp})_{\alpha}$, $(C^{\perp})_{\beta}$.

From Theorem 4 in [12], we have that $(1-u^2)C_{\beta}=\langle (1-u^2)f_1(x)\rangle$, $2^{-1}(u^2+u)C_{\beta}=\langle 2^{-1}(u^2+u)f_2(x)\rangle$ and $2^{-1}(u^2-u)C_{\beta}=\langle 2^{-1}(u^2-u)f_3(x)\rangle$. Hence, $\mid 2^{-1}(u^2+u)C_{\beta}\mid = p^{\beta-\deg(f_2(x))}$, $\mid (1-u^2)C_{\beta}\mid = p^{\beta-\deg(f_1(x))}$, $\mid 2^{-1}(u^2-u)C_{\beta}\mid = p^{\beta-\deg(f_3(x))}$. So, one can easily obtain the size of $\mid (1-u^2)(C_{\beta})^{\perp}\mid$, $\mid (1-u^2)(C^{\perp})_{\beta}\mid$, $\mid 2^{-1}(u^2+u)(C_{\beta})^{\perp}\mid$, $\mid 2^{-1}(u^2+u)(C^{\perp})_{\beta}\mid$, $\mid 2^{-1}(u^2-u)(C_{\beta})^{\perp}\mid$, $\mid 2^{-1}(u^2-u)(C^{\perp})_{\beta}\mid$. □

We determine the degree of the generator polynomials of a dual code. These results can be helpful to determine the generator polynomials of a dual code.

Theorem 3. *Let* $C = \langle (f(x),0),(l(x),(1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x))\rangle$ *be a* $\mathbb{Z}_p\mathcal{R}$*-additive cyclic code and with dual code*

$$C^{\perp} = \langle (\overline{f}(x),0),(\bar{l}(x),(1-u^2)\overline{f}_1(x)+2^{-1}(u^2+u)\overline{f}_2(x)+2^{-1}(u^2-u)\overline{f}_3(x))\rangle.$$

Then

$$\begin{aligned}
deg(\overline{f}(x)) &= \alpha - deg(gcd(f(x),l(x))),\\
deg(\overline{f}_1(x)) &= \beta - deg(f_1(x)) - deg(f(x)) + deg(gcd(f(x),l(x))),\\
deg(\overline{f}_2(x)) &= \beta - deg(f_2(x)),\\
deg(\overline{f}_3(x)) &= \beta - deg(f_3(x)).
\end{aligned}$$

Proof. It is easy to see that $(C_\alpha)^{\perp}$ is a cyclic code and that is generated by $\overline{f}(x)$. Therefore $\mid (C_\alpha)^{\perp} \mid = p^{\alpha-\deg(\overline{f}(x))}$. According to Lemma 6, $\mid (C_\alpha)^{\perp} \mid = p^{\deg(\gcd(f(x),l(x)))}$. Then $\deg(\overline{f}(x)) = \alpha - \deg(\gcd(f(x),l(x)))$. Also, we know that $(1-u^2)(C^{\perp})_\beta$ is a cyclic code and that is generated by $(1-u^2)\overline{f}_1(x)$. Moreover, by Lemma 6, $\mid (1-u^2)(C^{\perp})_\beta \mid = p^{\deg(f_1(x)+\deg(f(x))-\deg(\gcd(f(x),l(x)))}$.

Hence $\deg(\overline{f}_1(x)) = \beta - \deg(f_1(x)) - \deg(f(x)) + \deg(\gcd(f(x),l(x)))$. Now, one can show that $2^{-1}(u^2+u)(C^{\perp})_\beta$ is a cyclic code and that is generated by $2^{-1}(u^2+u)\overline{f}_2(x)$. Hence $\mid 2^{-1}(u^2+u)(C^{\perp})_\beta \mid = p^{\beta-\deg(\overline{f}_2(x))}$, and so $\mid 2^{-1}(u^2+u)(C^{\perp})_\beta \mid = p^{\deg(f_2(x))}$. Thus $\deg(\overline{f}_2(x)) = \beta - \deg(f_2(x))$. Clearly, $(2^{-1}(u^2-u)(C^{\perp})_\beta) = \langle 2^{-1}(u^2-u)\overline{f}_3(x)\rangle$ is a cyclic code. In view of Lemma 6, we have $\mid 2^{-1}(u^2-u)(C^{\perp})_\beta \mid = p^{\deg(f_3(x))}$. Thus $\deg(\overline{f}_3(x)) = \beta - \deg(f_3(x))$. ∎

Proposition 5. *Suppose that* $C = \langle (f(x),0),(l(x),(1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x))\rangle$ *is a* $\mathbb{Z}_p\mathcal{R}$*-additive cyclic code, where* $f_i(x)g_i(x) = x^\beta - 1$ *for* $1 \leq i \leq 3$*. Let*

$$C^{\perp} = \langle (\overline{f}(x),0),(\bar{l}(x),(1-u^2)\overline{f}_1(x)+2^{-1}(u^2+u)\overline{f}_2(x)+2^{-1}(u^2-u)\overline{f}_3(x))\rangle,$$

where $f_i(x)g_i(x) = x^\beta - 1$ *for* $i = 1,2,3$*. Then*

$$\overline{f}(x) = (x^\alpha - 1)/\gcd(f(x),l(x))^*.$$

Proof. Since $(\overline{f}(x),0) \in C^{\perp}$, we have that $\Omega((f(x),0),(\overline{f}(x),0)) = 0$ and that

$$\Omega((l(x),(1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x)),(\overline{f}(x),0)) = 0.$$

According to Proposition 4, $f(x)\overline{f}^*(x) \equiv 0$ and $l(x)\overline{f}^*(x) \equiv 0 \mod (x^\alpha - 1)$ over $\mathbb{Z}_p$. Therefore, $\gcd(l(x),f(x))\overline{f}^*(x) \equiv 0 \mod (x^\alpha - 1)$. Hence, there exists $\nu \in \mathbb{Z}_p$ such that $\gcd(f(x),l(x))\overline{f}^*(x) = \nu(x^\alpha - 1)$. Furthermore, $\gcd(f(x),l(x)) \mid (x^\alpha - 1)$. Then we may assume $\nu = 1$. Hence $\overline{f}(x) = (x^\alpha - 1)/(\gcd(f(x),l(x))^*$. ∎

Proposition 6. *Suppose that* $C = \langle (f(x), 0), (l(x), (1-u^2)f_1(x) + 2^{-1}(u^2+u)f_2(x) + 2^{-1}(u^2-u)f_3(x))\rangle$ *is a* $\mathbb{Z}_p\mathcal{R}$*-additive cyclic code, where* $f_i(x)g_i(x) = (x^\beta - 1)$ *for all* $1 \le i \le 3$*, and let*

$$C^\perp = \langle (\overline{f}(x), 0), (\bar{l}(x), (1-u^2)\overline{f}_1(x) + 2^{-1}(u^2+u)\overline{f}_2(x) + 2^{-1}(u^2-u)\overline{f}_3(x))\rangle,$$

where $\overline{f}_i(x)\overline{g}_i(x) = (x^\beta - 1)$ *for* $1 \le i \le 3$*. Then*

$$\overline{f}_1(x) = (x^\beta - 1)gcd(f(x), l(x))^*/f^*(x)f_1(x)^*.$$

Proof. Clearly

$$\begin{aligned}
&(1-u^2)f(x)/\gcd(f(x), l(x)) * (l(x), (1-u^2)f_1(x) + 2^{-1}(u^2+u)f_2(x)\\
&+ 2^{-1}(u^2-u)f_3(x)) - l(x)/\gcd(f(x), l(x)) * (f(x), 0)\\
&= (0, (1-u^2)f_1(x)f(x)/\gcd(f(x), l(x))) \in C.
\end{aligned}$$

Furthermore,

$$\begin{aligned}
(1-u^2)*(\bar{l}(x), (1-u^2)\overline{f}_1(x) + 2^{-1}(u^2+u)\overline{f}_2(x) + 2^{-1}(u^2-u)\overline{f}_3(x))\\
= (\bar{l}(x), (1-u^2)\overline{f}_1(x)) \in C^\perp.
\end{aligned}$$

Thus

$$\Omega((0, (1-u^2)f(x)f_1(x)/\gcd(f(x), l(x))), (\bar{l}(x), (1-u^2)\overline{f}_1(x))) = 0.$$

In view of Proposition 4, we have

$$(1-u^2)(f(x)/\gcd(f(x), l(x)))\ f_1(x)\overline{f}_1^*(x) \equiv 0 \bmod (x^\beta - 1).$$

Therefore

$$(1-u^2)(f(x)/\gcd(f(x), l(x)))f_1(x)\overline{f}_1^*(x) = \upsilon(x^\beta - 1).$$

Since $\overline{f}_1(x) \mid (x^\beta - 1)$, $(f(x)f_1(x)/\gcd(f(x), l(x)))^* \mid (x^\beta - 1)$, according to Proposition 3, we have

$$\deg(\overline{f}_1(x)) = \beta - \deg(f_1(x)) - \deg(f(x)) + \deg(\gcd(f(x), l(x))).$$

Thus we may assume that $\upsilon = 1$, and so

$$\overline{f}_1(x) = (x^\beta - 1)\gcd(f(x), l(x))^*/f^*(x)f_1^*(x).$$

□

Proposition 7. *Suppose that* $C = \langle (f(x), 0), (l(x), (1-u^2)f_1(x) + 2^{-1}(u^2+u)f_2(x) + 2^{-1}(u^2-u)f_3(x))\rangle$ *is a* $\mathbb{Z}_p\mathcal{R}$*-additive cyclic code, where* $f_i(x)g_i(x) = (x^\beta - 1)$ *for* $1 \le i \le 3$*, and let*

$$C^\perp = \langle (\overline{f}(x), 0), (\bar{l}(x), (1-u^2)\overline{f}_1(x) + 2^{-1}(u^2+u)\overline{f}_2(x) + 2^{-1}(u^2-u)\overline{f}_3(x))\rangle,$$

where $\overline{f}_i(x)\overline{g}_i(x) = (x^\beta - 1)$ *for* $1 \le i \le 3$*. Then*

$$\overline{f}_2(x) = (x^\beta - 1)/f_2^*(x).$$

Proof. Clearly

$$2^{-1}(u^2+u) * (\bar{l}(x), (1-u^2)\overline{f}_1(x) + 2^{-1}(u^2+u)\overline{f}_2(x) \\ + 2^{-1}(u^2-u)\overline{f}_3(x)) = (0, 2^{-1}(u^2+u)\overline{f}_2(x)) \in C^{\perp}.$$

Hence

$$\Omega((0, 2^{-1}(u^2+u)\overline{f}_2(x)), (l(x), (1-u^2)f_1(x) \\ + 2^{-1}(u^2+u)f_2(x) + 2^{-1}(u^2-u)f_3(x))) = 0.$$

Now, by Lemma 3, we obtain $2^{-1}(u^2+u)f_2(x)\overline{f}_2^*(x) \equiv 0 \mod (x^\beta - 1)$. Thus $2^{-1}(u^2+u)f_2(x)\overline{f}_2^*(x) = \zeta(x^\beta - 1)$, for some $\zeta \in \mathcal{R}[x]$. Since $f_2(x)|(x^\beta-1)$, $\overline{f}_2^*(x)|(x^\beta-1)$ for some $\zeta \in \mathcal{R}[x]$, we have $\zeta = 1$. Thus $\overline{f}_2(x) = (x^\beta - 1)/f_2^*(x)$. ∎

By using the method similar that used in the proof of Proposition 7, one can establish the next proposition.

Proposition 8. *Suppose that* $C = \langle (f(x), 0), (l(x), (1-u^2)f_1(x) + 2^{-1}(u^2+u)f_2(x) + 2^{-1}(u^2-u)f_3(x))\rangle$ *is a* $\mathbb{Z}_p\mathcal{R}$*-additive cyclic code, where* $f_i(x)g_i(x) = (x^\beta - 1)$ *for all* $1 \le i \le 3$*, and let*

$$C^{\perp} = \langle (\overline{f}(x), 0), (\bar{l}(x), (1-u^2)\overline{f}_1(x) + 2^{-1}(u^2+u)\overline{f}_2(x) + 2^{-1}(u^2-u)\overline{f}_3(x))\rangle,$$

where $\overline{f}_i(x)\overline{g}_i(x) = (x^\beta - 1)$ *for all* $1 \le i \le 3$*. Then*

$$\overline{f}_3(x) = (x^\beta - 1)/f_3^*(x).$$

Proposition 9. *Assume that* $C = \langle (f(x), 0), (l(x), (1-u^2)f_1(x) + 2^{-1}(u^2+u)f_2(x) + 2^{-1}(u^2-u)f_3(x))\rangle$ *is a* $\mathbb{Z}_p\mathcal{R}$*-additive cyclic code, and let*

$$C^{\perp} = \langle (\overline{f}(x), 0), (\bar{l}(x), (1-u^2)\overline{f}_1(x) + 2^{-1}(u^2+u)\overline{f}_2(x) + 2^{-1}(u^2-u)\overline{f}_3(x))\rangle,$$

where $\overline{f}_i(x)\overline{g}_i(x) = x^\beta - 1$ *for* $i = 1, 2, 3$*. Then*

$$\bar{l}(x) = \vartheta(x^\beta - 1)/f^*(x), \ \textit{where}$$

$\vartheta = -x^{m-\deg(f_1(x))+\deg(l(x))}(l^*(x)/\deg(f(x), l(x))^*)^{-1} \mod f^*(x)/\gcd(f(x), l(x))^*$.

Proof. The proof is similar to that of Proposition 6 in [11]. ∎

4 Quantum constacyclic code from $\mathbb{Z}_p\mathcal{R}$-additive constacyclic codes

Let λ be a unit element in $\mathcal{R}$ with $\lambda^2 = 1$. A linear code $\mathfrak{C}$ of length $\mathfrak{n}$ over $\mathcal{R}$ is called λ-constacyclic if, for every codeword $(c_0, c_1, \cdots, c_{\mathfrak{n}-1})$ in $\mathfrak{C}$, we have $(\lambda c_{\mathfrak{n}-1}, c_0, \cdots, c_{\mathfrak{n}-2}) \in \mathfrak{C}$.

It is well known that a λ-constacyclic code of length $\mathfrak{n}$ over $\mathcal{R}$ can be identified with an ideal in the quotient ring $\mathcal{R}[x]/\langle x^{\mathfrak{n}} - \lambda\rangle$. The $\mathcal{R}$-module isomorphism as follows:

$$\Gamma : \mathcal{R}^{\mathfrak{n}} \to \mathcal{R}[x]/\langle x^{\beta} - \lambda\rangle$$
$$(c_0, c_1, \cdots, c_{\mathfrak{n}-1}) \mapsto (c_0 + c_1 x + \cdots + c_{\mathfrak{n}-1}x^{\mathfrak{n}-1}) \mod(x^{\beta} - \lambda).$$

In the case when $\lambda = 1$, λ-constacyclic codes are just cyclic codes and while $\lambda = -1$, λ-constacyclic codes are known as negacyclic codes. Put

$$\mathcal{R}_{\alpha,\beta,\lambda} = \mathbb{Z}_p[x]/\langle x^{\alpha} - 1\rangle \times \mathcal{R}[x]/\langle x^{\beta} - \lambda\rangle.$$

Let $\mathfrak{C}$ be a code of length $\mathfrak{n}$ over $\mathcal{R}$, and $\Gamma(\mathfrak{C})$ be its polynomial representation, that is,

$$\Gamma(\mathfrak{C}) = \{\sum_{i=0}^{\mathfrak{n}-1} r_i x^i \quad | \quad (r_0, r_1, \cdots, r_{\mathfrak{n}-1}) \in \mathfrak{C}\}.$$

It is easy to see that:

Lemma 7. *Let $\mathfrak{C}$ be a λ-constacyclic code, where $\lambda = \delta + \theta u + \mu u^2$ of length $\mathfrak{n}$ over $\mathcal{R}$. Then $\mathfrak{C} = \langle (1 - u^2)\mathrm{f}_1(x) + 2^{-1}(u^2 + u)\mathrm{f}_2(x) + 2^{-1}(u^2 - u)\mathrm{f}_3(x)\rangle$, where $\mathrm{f}_1(x)$ generates a δ-constacyclic code with $\mathrm{f}_1(x)|(x^{\beta} - \delta)$, $\mathrm{f}_2(x)$ generates a $(\delta + \theta + \mu)$-constacyclic code with $\mathrm{f}_2(x)|(x^{\beta} - (\delta + \theta + \mu))$ and $\mathrm{f}_3(x)$ generates a $(\delta - \theta + \mu)$-constacyclic code with $\mathrm{f}_3(x)|(x^{\beta} - (\delta - \theta + \mu))$. Moreover, $\mathrm{f}_i(x)$ are the monic polynomials for all $1 \leq i \leq 3$.*

Proof. It is similar to the proof of Theorem 3.2 appeared in [2]. □

Theorem 4. *Let C be a $\mathbb{Z}_p\mathcal{R}$-additive constacyclic code of length (α, β) over $\mathcal{R}$. Then C is a $\mathbb{Z}_p\mathcal{R}$-submodule of $\mathcal{R}_{\alpha,\beta,\lambda}$ given by*

$$C = \langle (f(x), 0), (l(x), (1 - u^2)f_1(x) + 2^{-1}(u^2 + u)f_2(x) + 2^{-1}(u^2 - u)f_3(x))\rangle,$$

where $f_1(x)$ generates a δ-constacyclic code with $f_1(x)|(x^{\beta} - \delta)$, $f_2(x)$ generates a $(\delta+\theta+\mu)$-constacyclic code with $f_2(x)|(x^{\beta} - (\delta+\theta+\mu))$, $f_3(x)$ generates a $(\delta-\theta+\mu)$-constacyclic code with $f_3(x)|(x^{\beta} - (\delta - \theta + \mu))$ and $f(x)|(x^{\alpha} - 1)$. Moreover, $f(x)$ and $f_i(x)$ are the monic polynomials for $i = 1, 2, 3$.

Proof. Consider the projection map

$$\psi : \mathbb{Z}_p[x]/\langle x^{\alpha} - 1\rangle \times \mathcal{R}[x]/\langle x^{\beta} - \lambda\rangle \to \mathcal{R}[x]/\langle x^{\beta} - \lambda\rangle$$
$$(a(x), b(x)) \mapsto b(x),$$

where $a(x) \in \mathbb{Z}_p[x]/\langle x^{\alpha} - 1\rangle$, $b(x) \in \mathcal{R}[x]/\langle x^{\beta} - \lambda\rangle$. It is clear that the map ψ is an $\mathcal{R}[x]$-module homomorphism. Suppose that C is a $\mathbb{Z}_p\mathcal{R}$-additive constacyclic code. Then $\psi(C)$ is an $\mathcal{R}[x]$-submodule of $\mathcal{R}[x]/\langle x^{\beta} - \lambda\rangle$. Hence, by Lemma 7,

$$\psi(C) = \langle (1 - u^2)f_1(x) + 2^{-1}(u^2 + u)f_2(x) + 2^{-1}(u^2 - u)f_3(x)\rangle,$$

where $f_1(x)|(x^\beta-\delta)$, $f_2(x)|(x^\beta-(\delta+\theta+\mu))$, $f_3(x)|(x^\beta-(\delta-\theta+\mu))$. Furthermore, we have $\mathrm{Ker}(\psi)=\{(h(x),0)\in C \quad | \quad h(x)\in\mathbb{Z}_p[x]/\langle x^\alpha-1\rangle\}$. Define

$$D=\{h(x)\in\mathbb{Z}_p[x]/\langle x^\alpha-1\rangle \quad | \quad (h(x),0)\in\mathrm{Ker}(\psi)\}.$$

Obviously, D is an ideal of the principal ring $\mathbb{Z}_p[x]/\langle x^\alpha-1\rangle$. Hence, $D=\langle f(x)\rangle$. Thus $\mathrm{Ker}(\psi)=\langle(f(x),0)\rangle$. Moreover, there exists $l(x)\in\mathbb{Z}_p[x]/\langle x^\alpha-1\rangle$ such that

$$C=\langle(f(x),0),(l(x),(1-u^2)f_1(x)+2^{-1}(u^2+u)f_2(x)+2^{-1}(u^2-u)f_3(x))\rangle,$$

where $f(x)|(x^\alpha-1)$, $f_1(x)|(x^\beta-\delta)$, $f_2(x)|(x^\beta-(\delta+\theta+\mu))$, $f_3(x)|(x^\beta-(\delta-\theta+\mu))$. □

Definition 11. *The $\mathbb{Z}_p\mathcal{R}$-additive code C is called constacyclic code if, for any codeword $z=(c_0,c_1,\cdots,c_{\alpha-1},r_0,r_1,\cdots,r_{\beta-1})$ in C, we have*

$$\sigma_{\lambda,\beta}(z)=(c_{\alpha-1},c_0,\cdots,c_{\alpha-2},\lambda r_{\beta-1},r_0,\cdots,r_{\beta-2})\in C.$$

Lemma 8. *Let C be a $\mathbb{Z}_p\mathcal{R}$-additive code of length (α,β). Then C is a $\mathbb{Z}_p\mathcal{R}$-additive constacyclic code if and only if it is a $\mathbb{Z}_p\mathcal{R}[x]$-submodule of $\mathcal{R}_{\alpha,\beta,\lambda}$.*

Definition 12. *[18] Let n be a positive integer and $1\leq l\lneq n$. Let C be a linear code of length n over R. Then C is called a quasi-cyclic code of index l if for any $(c_0,c_1,\cdots,c_{n-1})\in\mathsf{C}$, we have*

$$(c_{n-l},c_{n-l+1},\cdots,c_{n-1},c_0,\cdots,c_{n-l-1})\in\mathsf{C}.$$

Definition 13. *[13, Definition 2] Let $m_1,m_2,\cdots,m_l$ be positive integers and $R_i=\dfrac{R[x]}{\langle x_i^m-1\rangle}$ for $i=1,\cdots,l$. Then an $R[x]$-submodule $\mathfrak{R}=R_1\times R_2\times\cdots\times R_l$ is called a generalized quasi-cyclic code of length $(m_1,\cdots,m_l)$ with index l over R. If $m=m_i$ for $i=1,\cdots,l$, then C is called a quasi-cyclic code with length ml.*

Lemma 9. *Suppose that C is a $\mathbb{Z}_p\mathcal{R}$-additive constacyclic code of length (α,β). Then $\varphi(C)$ is a generalized quasi-cyclic code of length $(\alpha,3\beta)$ over $\mathbb{Z}_p$.*

Proof. The proof can be easily obtained. □

Corollary 2. *Let C be a $\mathbb{Z}_p\mathcal{R}$-additive constacyclic code of length (α,α). Then $\varphi(C)$ is a quasi-cyclic code of length 4α and index 2 over $\mathbb{Z}_p$.*

Proof. The proof follows from Definition 13 and Lemma 9. □

The following lemma is immediate from [6].

Lemma 10. *Let $\mathfrak{C}=\langle(1-u^2)\mathrm{f}_1(x)+2^{-1}(u^2+u)\mathrm{f}_2(x)+2^{-1}(u^2-u)\mathrm{f}_3(x)\rangle$ be a λ-constacyclic code of length β over $\mathcal{R}$, where $\lambda=\delta+\theta u+\mu u^2$, and let $\delta=\pm1$, $\delta+\theta+\mu=\pm1$, $\delta-\theta+\mu=\pm1$. Then $\mathfrak{C}^\perp\subseteq\mathfrak{C}$ if and only if*

$$\begin{aligned} x^\alpha-\delta\equiv 0 \quad &mod \quad \mathrm{f}_1(x)\mathrm{f}_1^*(x),\\ x^\beta-(\delta+\theta+\mu)\equiv 0 \quad &mod \quad \mathrm{f}_2(x)\mathrm{f}_2^*(x) \quad and\\ x^\beta-(\delta-\theta+\mu)\equiv 0 \quad &mod \quad \mathrm{f}_3(x)\mathrm{f}_3^*(x).\end{aligned}$$

Proposition 10. *Let $\mathfrak{C} = \langle (1-u^2)\mathrm{f}_1 + 2^{-1}(u^2+u)\mathrm{f}_2 + 2^{-1}(u^2-u)\mathrm{f}_3 \rangle$ be a λ- constacyclic code of length β over $\mathcal{R}$, where $\lambda = \delta + \theta u + \mu u^2$. If, there exists a dual containing λ-constacyclic code of length β over $\mathcal{R}$, then*

$$\lambda \in \{\pm 1, \pm(1-u-u^2), \pm(1+u-u^2), \pm(1-2u^2)\}.$$

Proof. Suppose that $\mathfrak{C}$ is a dual containing λ-constacyclic code over β, where $\lambda = \delta + \theta u + \mu u^2$. By Lemma 7, $\mathrm{f}_1(x)$ generates a δ-constacyclic code over $\mathbb{Z}_p$, $\mathrm{f}_2(x)$ generates a $(\delta - \theta + \mu)$-constacyclic code, and also $\mathrm{f}_3(x)$ generates a $(\delta + \theta + \mu)$-constacyclic code. By Lemma 10, we get $\delta = \pm 1$, $\delta - \theta + \mu = \pm 1$ and $\delta + \theta + \mu = \pm 1$.
Set $\delta = 1$. Then

1. If $\delta - \theta + \mu = 1$ and $\delta + \theta + \mu = 1$, then $\theta = \mu = 0$ implying $\lambda = 1$.

2. If $\delta - \theta + \mu = 1$ and $\delta + \theta + \mu = -1$, then $\theta = -1$, $\mu = -1$. This means that $\lambda = 1 - u - u^2$.

3. If $\delta - \theta + \mu = -1$ and $\delta + \theta + \mu = -1$, then $\theta = 1$, $\mu = -1$. This implies that $\lambda = 1 + u - u^2$.

4. If $\delta - \theta + \mu = -1$ and $\delta + \theta + \mu = -1$, then $\theta = 0$, $\mu = -2$. This means that $\lambda = 1 - 2u^2$.

Similarly, we set $\delta = -1$ to deduce that $\lambda = -1 + 2u^2, -1 + u + u^2, -1 - u + u^2, -1$, respectively.
□

In the following corollary, we shall establish a generalization of Lemma 10 to $\mathbb{Z}_p\mathcal{R}$-additive codes.

Corollary 3. *Let $C = C_\alpha \times C_\beta$ be a separable $\mathbb{Z}_p\mathcal{R}$-additive constacyclic code of length $\alpha + \beta$ with $\lambda = \delta + \theta u + \mu u^2$, where $C_\alpha = \langle f(x) \rangle$ and $C_\beta = \langle (1-u^2)f_1(x) + 2^{-1}(u^2+u)f_2(x) + 2^{-1}(u^2-u)f_3(x) \rangle$ with conditions $\delta = \pm 1$, $\delta + \theta + \mu = \pm 1$, $\delta - \theta + \mu = \pm 1$. Then $C^\perp \subseteq C$ if and only if the following conditions are satisfied*

$$\begin{aligned} x^\alpha - 1 &\equiv 0 \quad mod \quad (f(x)f^*(x)), \\ x^\beta - \delta &\equiv 0 \quad mod \quad (f_1(x)f_1^*(x)), \\ x^\beta - (\delta + \theta + \mu) &\equiv 0 \quad mod \quad (f_2(x)f_2^*(x)), \\ x^\beta - (\delta - \theta + \mu) &\equiv 0 \quad mod \quad (f_3(x)f_3^*(x)). \end{aligned}$$

Lemma 11. *[6]. Let $\mathfrak{C}$ be a $(\delta + \theta u + \mu u^2)$-constacyclic code of length s over $\mathcal{R}$. If $\mathfrak{C}^\perp \subseteq \mathfrak{C}$, then there exists a quantum error-correcting code with parameters $[[3\mathrm{s}, 2\mathrm{k} - 3\mathrm{s}, \geq d_G]]_q$ where d_G is the minimum Gray weight of $\mathfrak{C}$ and k is the dimension of the code $\phi_1(\mathfrak{C})$.*

From Corollary 3 and Lemma 11, we can construct non-binary quantum codes as follows.

Theorem 5. *Let $C = \langle (f(x), 0), (0, (1-u^2)f_1(x) + 2^{-1}(u^2+u)f_2(x) + 2^{-1}(u^2-u)f_3(x)) \rangle$ be a $[\alpha + \beta, p^k, d_L]$ separable $\mathbb{Z}_p\mathcal{R}$-additive constacyclic code, where d_L is the minimum Lee distance of C. Then there exists a quantum code with parameters $[[n, 2k - n, \geqslant d_L]]_p$, where $n = \alpha + 3\beta$.*

Example 1. *It is clear that, in* $\mathbb{Z}_3[x]$*, we have the following equalities:*

$$x^6 - 1 = (1+x)^3(2+x)^3 \quad \text{and}$$
$$x^{12} - 1 = (1+x)^3(2+x)^3(1+x^2)^3.$$

Let $\alpha = 6$ *and* $\beta = 12$*. Suppose that* $f(x) = f_1(x) = f_2(x) = (1+x)$*,* $f_3(x) = (1+x^2)$ *and* $C = \langle (f(x), 0), (0, (1-u^2)f_1(x) + 2^{-1}(u^2+u)f_2(x) + 2^{-1}f_3(x))\rangle$*. Therefore, C is a separable additive constacyclic code with parameters* $[18, 3^{37}, 2]$*, where* $\lambda = 1 + u - u^2$*. As all* $f_i(x)f_i^*(x)$ *divide* $x^{12} - 1$ *for* $1 \leq i \leq 3$*,* $f(x)f^*(x)$ *divide* $x^6 - 1$ *and* $C^\perp \subseteq C$*. Thus, there exists a quantum code with parameters* $[[42, 32, 2]]_3$*.*

Example 2. *Suppose that* $\alpha = \beta = 15$*. It is clear that* $x^{15} - 1 = (4+x)^5(1+x+x^2)^5$ *in* $\mathbb{Z}_5[x]$*. Let* $f(x) = f_1(x) = f_2(x) = f_3(x) = (1+x+x^2)$ *and* $C = \langle (f(x), 0), (0, (1-u^2)f_1(x) + 2^{-1}(u^2+u)f_2(x) + 2^{-1}(u^2-u)f_3(x))\rangle$*. So, C is a separable additive constacyclic code with parameters* $[30, 5^{52}, 3]$*, where* $\lambda = 1 - u + u^2$*. Clearly, it satisfies the conditions in Corollary 3. We get a quantum code with parameters* $[[60, 44, 3]]_5$*.*

Conclusion: In this paper, we studied the algebraic structure of additive cyclic codes and orthogonal codes over $\mathbb{Z}_p\mathcal{R}$. We obtained the generator polynomials of this family of codes and their dual codes. We also determined the minimal generating sets of additive cyclic codes. We described some properties of the Gray image of a additive cyclic code over $\mathbb{Z}_p\mathcal{R}$ be a linear code over $\mathbb{Z}_p$. We also argumented the structure of additive constacyclic codes and quantum codes and showed that our results can be generalized to $\mathbb{Z}_p\mathcal{R}$-additive constacyclic codes and quantum codes.

Acknowledgement *The authors are deeply grateful to the referees for careful reading of the manuscript and making valuable suggestions which improved this paper.*

References

[1] T. Abualrub, I. Siap, N. Aydin, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, *IEEE Trans. Inform. Theory*, **60**, 1508–1514 (2014).

[2] M. Al-Ashker, M. I. Satariah, Constacyclic codes over the ring $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$, *Palest. J. Math.*, **5**, 167–174 (2016).

[3] I. Aydogdu, T. Abualrub, I. Siap, On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes, *Int. J. Comput. Math*, **92**, 1806–1814 (2015).

[4] I. Aydogdu, T. Abualrub, I. Siap, $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic and constacyclic codes, *IEEE Trans. Inform. Theory*, **63**, 4883–4893 (2017).

[5] Ch. Bachoc, Ph. Gaborit, On extremal additive $\mathbb{F}_4$ codes of length 10 to 18, *International Workshop on Coding and Cryptography* (Paris, 2001), Electron. Notes Discrete Math., **6**, Elsevier Sci. B. V., Amsterdam (2001).

[6] T. Bag, A. K. Upadhyay, M. Ashraf, G. Mohammad, Quantum codes from cyclic codes over the ring $\dfrac{\mathbb{F}_p[u]}{\langle u^3 - u\rangle}$, *Asian-European Jornal of Mathematics*, **13**, 205008 (2020).

[7] A. Blokhuis, A. E. Brouwer, Small additive quaternary codes, *European J. Combin*, **25**, 161–167(2004).

[8] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, M. Villanueva, $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality, *Des. Codes Cryptogr.*, **54**, 167–179 (2010).

[9] J. Borges, C. Fernández-Córdoba, R. Ten-Valls, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, generator polynomials, and dual codes, *IEEE Trans. Inform. Theory*, **62**, 6348–6354 (2016).

[10] P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Rep. Suppl.*, VI (1973).

[11] L. Diao, J. Gao, J. Lu, Some results on $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes, *Adv. Math. Commun*, **14**, 555–572 (2020).

[12] J. Gao, Some results on linear codes over $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$, *J. Appl. Comput*, **47**, 473-485 (2015).

[13] Y. Gao, J. Gao, T. Wu, F.-W. Fu, 1-generator quasi-cyclic and generalized quasi-cyclic codes over the ring $\frac{\mathbb{Z}_4[u]}{\langle u^2-1\rangle}$, *Appl. Algebra Engrg. Comm. Comput.*, **28**, 457–467(2017).

[14] X. Hou, J. Gao, $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes are asymptotically good, *J. Appl. Math. Comput.*, **66**, 871–884 (2021).

[15] H. Islam, O. Prakash, New quantum codes from constacyclic and additive constacyclic codes, *Quantum Inf. Process*, **19**, no. 319 (2020).

[16] H. Islam, O. Prakash, P. Sole, $\mathbb{Z}_4\mathbb{Z}_4[u]$-additive cyclic and constacyclic codes, *Adv. Math. Commun.*, **15**, 737–755 (2021).

[17] B. Lindström, Group partitions and mixed perfect codes, *Canad. Math. Bull.*, **18**, 57–60 (1975).

[18] S. Ling, Ch. Xing, *Coding Theory: a first course*, National University of Singapore, New York (2004).

Received: 25.11.2021
Revised: 18.06.2022
Accepted: 21.06.2022

(1) Department of Pure Mathematics, Ferdowsi University of Mashhad,
P. O. Box 1159-91775, Mashhad, Iran
E-mail: `Ghajari3051@gmail.com`

(2) Department of Pure Mathematics, Ferdowsi University of Mashhad,
P. O. Box 1159-91775, Mashhad, Iran
E-mail: `khashyar@ipm.ir`