DOI: 10.2478/auom-2024-0002
An. Şt. Univ. Ovidius Constanţa
sciendo
Vol. 32(1),2024, 19–43

The study of $\mathbb{Z}_p\mathbb{Z}_p[u,v]$-additive cyclic codes and their application in obtaining Optimal and MDSS codes

Mohammad Ashraf, Mohd Asim, Ghulam Mohammad and Washiqur Rehman

Abstract

Let $\mathbf{S} = \mathbb{Z}_p[u,v]/\langle u^2, v^2, uv - uv\rangle$ be a semi-local ring, where p is a prime number. In the present article, we determine the generating sets of $\mathbf{S}$ and use them to construct the structures of $\mathbb{Z}_p\mathbf{S}$-additive cyclic and constacyclic codes. The minimal polynomials and spanning sets of $\mathbb{Z}_p\mathbf{S}$-additive cyclic and constacyclic codes are also determined. These codes are identified as $\mathbf{S}[y]$-submodules of the ring $\mathbf{S}_{\beta_1,\beta_2} = \mathbb{Z}_p[y]/\langle y^{\beta_1} - 1\rangle \times \mathbf{S}[y]/\langle y^{\beta_2} - 1\rangle$. Some results that represent the relationship between the minimal polynomials of $\mathbb{Z}_p\mathbf{S}$-additive cyclic codes and their duals have been obtained. Furthermore, optimal $\mathbb{Z}_p\mathbf{S}$-additive codes and maximum distance separable codes have been evaluated (see Table 1). Finally, we use MAGMA software to find the parameters of Optimal and MDSS codes.

1 Introduction

Error-correcting codes were initially investigated over finite fields, but later more general structures have been considered and implemented. Numerous authors are interested in the study of codes over rings.

The study over mixed alphabet has introduced new options and paths to be explored. In one such study, additive codes were defined by Delsarte in

Key Words: polynomial ring; additive cyclic codes; Gray map.
2010 Mathematics Subject Classification: 94B05, 94B15, 94B60
Received: 11.01.2023
Accepted: 18.04.2023

1973 in terms of association schemes (see for reference [15, 16]). In general, an additive code is defined as a subgroup of the underlying abelian group. In the special case of a binary Hamming scheme, when the underlying abelian group is of order 2^n, the only structure for the abelian group are those of the form $\mathbb{Z}_2^{\beta_1} \times \mathbb{Z}_4^{\beta_2}$ with $\beta_1 + 2\beta_2 = n$. Therefore, the subgroup C of $\mathbb{Z}_2^{\beta_1} \times \mathbb{Z}_4^{\beta_2}$ is the only additive code in a binary Hamming scheme.

In 2013, Aydogdu et al. [9] extended the study of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes to $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes. Further, they studied $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes and defined mixed codes consisting of the binary part and non-binary part from the ring $\mathbb{Z}_2 + u\mathbb{Z}_2$, $u^2 = 0$ which is another generalization of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. Aydogdu and Siap generalized $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes to $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes in [10]. In 2019, Minjia Shi et al.[21] described $\mathbb{Z}_2\mathbb{Z}_2[u,v]$-additive cyclic code, where $u^2 = v^2 = 0$, $uv = vu$ which were the generalization of previously introduced $\mathbb{Z}_2\mathbb{Z}_4$- additive cyclic codes. Later, Borges et al. [12] obtained some interesting results on $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes. Note that in $\mathbb{Z}_2\mathbb{Z}_4$-additive codes and $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes, $\mathbb{Z}_2$ is considered as $\mathbb{Z}_4$-algebra and $\mathbb{Z}_{2^s}$-algebra respectively. Also in $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive code, $\mathbb{Z}_2$ is known as a $\mathbb{Z}_2[u]$-algebra and $\mathbb{Z}_{p^r}$ is a $\mathbb{Z}_{p^s}$-algebra in $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes.

In 2018, J. Gao et al. [17] gave the structural properties of additive cyclic codes over $\mathbb{Z}_p\mathbb{Z}_p[u]$. They also found the minimal generating sets of additive cyclic codes over $\mathbb{Z}_2\mathbb{Z}_2[u,v]$ and determined the relationship between the generators of the additive codes and their dual code. In 2019, Islam et al. [18] studied the structural properties of the ring $\mathbb{Z}_p\mathbb{Z}_p[u,v]$, where $u^2 = v^2 = uv = vu = 0$ and found $\mathbb{Z}_p\mathbb{Z}_p[u,v]$-additive cyclic codes and constacyclic codes. Furthermore, they determined the generator polynomials, minimal spanning sets of additive cyclic and constacyclic codes over $\mathbb{Z}_p\mathbb{Z}_p[u,v]$.

In this article, we consider semi-local ring $\mathbf{S} = \mathbb{Z}_p + u\mathbb{Z}_p + v\mathbb{Z}_p + uv\mathbb{Z}_p$, where $u^2 = v^2 = 0$, $uv = vu$ with prime characteristic p and evaluate $\mathbb{Z}_p\mathbf{S}$-additive cyclic codes and constacyclic codes. We also find the optimal $\mathbb{Z}_p\mathbf{S}$-additive codes and maximum distance separable with respect to singleton bound(MDSS) codes. It is to noted that the additive code of length (β_1, β_2) is the subgroup of the commutative group $\mathbb{Z}_p^{\beta_1} \times \mathbf{S}^{\beta_2}$. The $\mathbb{Z}_p\mathbf{S}$-additive code is a linear code over $\mathbb{Z}_p$ if $\beta_2 = 0$ and over $\mathbf{S}$ if $\beta_1 = 0$. Clearly, we observe that it is the generalization of linear code over $\mathbb{Z}_p$ and $\mathbf{S}$. Furthermore, we obtain the generator polynomials and minimal spanning sets for $\mathbb{Z}_p\mathbf{S}$-additive cyclic codes and constacyclic codes. These codes are classified as $\mathbf{S}[y]$-submodules of the ring $S_{\beta_1,\beta_2} = \mathbb{Z}_p[y]/\langle y^{\beta_1} - 1\rangle \times \mathbf{S}[y]/\langle y^{\beta_2} - 1\rangle$.

This paper is organized as follows: In Section 2, we present some basic definitions and properties of the ring $\mathbf{S} = \mathbb{Z}_p + u\mathbb{Z}_p + v\mathbb{Z}_p + uv\mathbb{Z}_p$, where $u^2 = 0$, $v^2 = 0$, $uv = vu$. We also define the Gray maps and include some results. The generator polynomials and spanning sets for $\mathbb{Z}_p\mathbf{S}$-additive cyclic codes are discussed in Section 3. A result which guarantees that a code to be maximum distance separable with respect to singleton bound(MDSS) has also been provided. Section 4 contains the results based on the relationship between additive cyclic codes and their duals. Section 5 is devoted to the study of $\mathbb{Z}_p\mathbf{S}$-additive constacyclic codes and related results. In Section 6, some examples of $\mathbb{Z}_p\mathbf{S}$-additive cyclic codes, constacyclic codes and optimal codes have been included. Section 7 brings the article to a conclusion.

Some of the concepts on $\mathbb{Z}_p\mathbb{Z}_p[u,v]$-additive codes described in this paper have been implemented by MAGMA which is a software package designed to solve computationally hard problems in algebra, number theory, geometry and combinatorics.

2 PRELIMINARIES

Let $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ be finite field and $\mathbf{S} = \mathbb{Z}_p + u\mathbb{Z}_p + v\mathbb{Z}_p + uv\mathbb{Z}_p$, where $u^2 = 0$, $v^2 = 0$ and $uv = vu$ be a non chain ring with characteristic p. Any element $z \in \mathbf{S}$ can be written as $z = a + ub + uc + uvd$ for all $a, b, c, d \in \mathbb{Z}_p$. An element $z = a + ub + uc + uvd \in \mathbf{S}$ is a unit if a is a unit. The total number of ideals in $\mathbf{S}$ are listed as $I_1 = \{0\}$, $I_2 = \langle u \rangle$, $I_3 = \langle v \rangle$, $I_4 = \langle uv \rangle$, $I_5 = \langle u + av \rangle$ and $I_6 = \langle u, v \rangle$, where a is nonzero element of $\mathbb{Z}_p$. Since $I_6 = \langle u, v \rangle$ is the unique maximal ideal in $\mathbf{S}$, the finite commutative ring $\mathbf{S}$ is a local ring. Let

$$\mathbb{Z}_p\mathbf{S} = \{(c, c^{'}) \mid c \in \mathbb{Z}_p, \ c^{'} \in \mathbf{S}\}.$$

Define a map

$$\theta : \mathbf{S} \longrightarrow \mathbb{Z}_p$$

such that $\theta(a + ub + uc + uvd) = a$. Clearly, θ is a well-defined onto ring homomorphism. Let $\mathbb{Z}_p^{\beta_1}$ be β_1-tuples over $\mathbb{Z}_p$ and $\mathbf{S}^{\beta_2}$ be β_2-tuples over $\mathbf{S}$, where β_1 and β_2 are positive integers. Let $\mathbf{y} = (y^{'} \mid y^{"}) \in \mathbb{Z}_p^{\beta_1} \times \mathbf{S}^{\beta_2}$ be a vector, where $y^{'} = (y_0^{'}, y_1^{'}, \ldots, y_{\beta_1-1}^{'})$ and $y^{"} = (y_0^{"}, y_1^{"}, \ldots, y_{\beta_2-1}^{"})$. For any $z = a + ub + uc + uvd \in \mathbf{S}$, the $\mathbf{S}$-scalar multiplication on $\mathbb{Z}_p^{\beta_1} \times \mathbf{S}^{\beta_2}$ is defined as follows:

$$z\mathbf{y} = (\theta(z)y_0^{'}, \theta(z)y_1^{'}, \ldots, \theta(z)y_{\beta_1-1}^{'} \mid zy_0^{"}, zy_1^{"}, \ldots, zy_{\beta_2-1}^{"}) \in \mathbb{Z}_p^{\beta_1} \times \mathbf{S}^{\beta_2}, \quad (2.1)$$

where $\theta(z)y_i^{'}$ and $zy_j^{"}$ are performed mod$p$ for all $i = 0, 1, \ldots, \beta_1 - 1$ and $j = 0, 1, \ldots, \beta_2 - 1$. The $\mathbb{Z}_p^{\beta_1} \times \mathbf{S}^{\beta_2}$ forms a $\mathbf{S}$-module under usual addition and multiplication defined in (2.1). Let $\mathbf{S}_{\beta_1,\beta_2} = \mathbb{Z}_p[y]/\langle y^{\beta_1} - 1 \rangle \times \mathbf{S}[y]/\langle y^{\beta_2} - 1 \rangle$. Define a map

$$\Phi : \mathbb{Z}_p^{\beta_1} \times \mathbf{S}^{\beta_2} \longrightarrow \mathbf{S}_{\beta_1,\beta_2}$$

$$d = (f \mid g) \longmapsto d(y) = (f(y) \mid g(y)),$$

where $(f \mid g) = (f_0, f_1, \ldots, f_{\beta_1-1} \mid g_0, g_1, \ldots, g_{\beta_2-1})$, $f(y) = f_0 + f_1 y + \cdots + f_{\beta_1-1} y^{\beta_1-1}$ and $g(y) = g_0 + g_1 y + \cdots + g_{\beta_2-1} y^{\beta_2-1}$. For any $h(y) = h_0 + h_1 y + \cdots + h_l y^l \in \mathbf{S}[y]$ and

$d(y) = (f(y) \mid g(y)) \in \mathbf{S}_{\beta_1,\beta_2}$, define the $\mathbf{S}[y]$-scalar multiplication

$$h(y) \cdot d(y) = (\theta(h(y)f(y) \mid h(y)g(y)), \tag{2.2}$$

where $\theta(h(y)) = \theta(h_0) + \theta(h_1)y + \cdots + \theta(h_l)y^l$. Then $\mathbf{S}_{\beta_1,\beta_2}$ forms a $\mathbf{S}[y]$-module under usual addition and scalar multiplication of polynomials defined in (2.2).

Definition 2.1. *A non-empty subset C of $\mathbb{Z}_p^{\beta_1} \times \boldsymbol{S}^{\beta_2}$ is called a $\mathbb{Z}_p\boldsymbol{S}$-additive code if C is a subgroup of $\mathbb{Z}_p^{\beta_1} \times \boldsymbol{S}^{\beta_2}$, that is, C is isomorphic to $\mathbb{Z}_p^{n_1} \times \mathbb{Z}_p^{4n_2} \times \mathbb{Z}_p^{3n_3} \times \mathbb{Z}_p^{2n_4} \times \mathbb{Z}_p^{n_5}$, for some positive integers n_1, n_2, n_3, n_4 and n_5.*

If C is a $\mathbb{Z}_p\mathbf{S}$-additive code isomorphic to $\mathbb{Z}_p^{n_1} \times \mathbb{Z}_p^{4n_2} \times \mathbb{Z}_p^{3n_3} \times \mathbb{Z}_p^{2n_4} \times \mathbb{Z}_p^{n_5}$, then C is of type $(\beta_1, \beta_2, n_1, n_2, n_3, n_4, n_5)$. It is called $\mathbb{Z}_p\mathbf{S}$-additive linear code. For any $z_1 = (a_0, a_1, \ldots, a_{\beta_1-1} \mid b_0, b_1, \ldots, b_{\beta_2-1})$ and $z_2 = (c_0, c_1, \ldots, c_{\beta_1-1} \mid d_0, d_1, \ldots, d_{\beta_2-1})$, the inner product is defined as

$$\begin{aligned} \mathbf{z}_1 \cdot \mathbf{z}_2 &= (uva_0c_0 + uva_1c_1 + \cdots + uva_{\beta_1-1}c_{\beta_1-1} + b_0d_0 \\ &\quad + b_1d_1 + \cdots + b_{\beta_2-1}d_{\beta_2-1})(\mathrm{mod} p) \\ &= (uv \sum_{i=0}^{\beta_1-1} a_i c_i + \sum_{k=0}^{\beta_2-1} b_k c_k)(\mathrm{mod} p). \end{aligned}$$

Definition 2.2. *A non-empty subset C of $\mathbb{Z}_p^{\beta_1} \times \boldsymbol{S}^{\beta_2}$ is called a $\mathbb{Z}_p\boldsymbol{S}$-additive cyclic code if*

(*i*) *C is additive code;*

(*ii*) *For any codeword $\boldsymbol{z} = (a_0, a_1, \ldots, a_{\beta_1-1} \mid b_0, b_1, \ldots, b_{\beta_2-1}) \in C$ its cyclic shift $T(\boldsymbol{z}) = (a_{\beta_1-1}, a_0, \ldots, a_{\beta_1-2} \mid b_{\beta_2-1}, b_0, \ldots, b_{\beta_2-2}) \in C$.*

Definition 2.3. *Let C be any $\mathbb{Z}_p\boldsymbol{S}$-additive cyclic code. Then the dual code of C with respect to the inner product defined as*

$$C^{\perp} = \{z_2 \in \mathbb{Z}_p^{\beta_1} \times \boldsymbol{S}^{\beta_2} \mid \ z_1 \cdot z_2 = 0 \ \mathit{for} \ \ \mathit{all} \ z_1 \in C\}.$$

Let C be a linear code of length n and dimension k over $\mathbf{S}$. The singleton bound is given by $d_G(C) \leq n - k + 1$, and MDS (maximum distance separable code) code if equality holds.

Lemma 2.1. *Let C be a $\mathbb{Z}_p\boldsymbol{S}$-additive code of type $(\beta_1, \beta_2, n_1, n_2, n_3, n_4, n_5)$. Then*

$$d_G(C) \leq (\beta_1 + 4\beta_2) - n_1 - 4n_2 - 3n_3 - 2n_4 - n_5 + 1.$$

Proof. Let C be a $\mathbb{Z}_p\mathbf{S}$-additive code of type $(\beta_1, \beta_2, n_1, n_2, n_3, n_4, n_5)$ and $\mathcal{C} = \Phi(C)$. Then $d_G(C) = d_G(\mathcal{C})$. Suppose that $\mathcal{C}$ is a code of length $\beta_1 + 4\beta_2$ and dimension $n_1 + 4n_2 + 3n_3 + 2n_4 + n_5$. Then applying the singleton bound on $\mathcal{C}$, we get

$$d_G(C) \leq (\beta_1 + 4\beta_2) - n_1 - 4n_2 - 3n_3 - 2n_4 - n_5 + 1.$$

□

Lemma 2.2. *Let C be a $\mathbb{Z}_p\boldsymbol{S}$-additive code of type $(\beta_1, \beta_2, n_1, n_2, n_3, n_4, n_5)$. Then*

$$\frac{d_G(C) - 1}{4} \leq \frac{\beta_1}{4} + \beta_2 - \frac{n_1}{4} - n_2 - \frac{3n_3}{4} - \frac{n_4}{2} - \frac{n_5}{4}.$$

Proof. Proof is directly followed by Lemma 2.1. □

Definition 2.4. *Let C be a $\mathbb{Z}_p\boldsymbol{S}$-additive code. Then C is said to be a maximum distance separable with respect to singleton bound (MDSS) code if it satisfies the equality*

$$\frac{d_G(C) - 1}{4} = \frac{\beta_1}{4} + \beta_2 - \frac{n_1}{4} - n_2 - \frac{3n_3}{4} - \frac{n_4}{2} - \frac{n_5}{4}.$$

Theorem 2.1. *Let C be any $\mathbb{Z}_p\boldsymbol{S}$-additive cyclic code. Then $C^\perp$ is also cyclic.*

Proof. Let C be any $\mathbb{Z}_p\mathbf{S}$-additive cyclic code and $z_2 = (c_0, c_1, \ldots, c_{\beta_1-1} \mid d_0, d_1, \ldots, d_{\beta_2-1}) \in C^\perp$. In order to show $T(z_2) \in C^\perp$, we have to prove that $z_1 \cdot T(z_2) = 0$. Since C is cyclic, we have $T^l(z_1)$ also in C, where $l = \text{lcm}(\beta_1, \beta_2)$. Now, we can write

$$\begin{aligned}
0 &= T^{l-1}(z_1) \cdot z_2 \\
&= (a_1, a_2, \ldots, a_{\beta_1-1}, a_0 \mid b_1, b_2, \ldots, b_{\beta_2-1}, b_0) \cdot (c_0, c_1, \ldots, c_{\beta_1-1} \mid d_0, \\
&\quad d_1, \ldots, d_{\beta_2-1}) \\
&= (uva_1c_0 + uva_2c_1 + \cdots + uva_{\beta_1-1}c_{\beta_1-2} + uva_0c_{\beta_1-1} + b_1d_0 \\
&\quad + b_2d_1 + \cdots + b_{\beta_2-1}d_{\beta_2-1} + b_0d_{\beta_2-1}) \\
&= (uva_0c_{\beta_1-1} + uva_1c_0 + \cdots + uva_{\beta_1-1}c_{\beta_2-2} + uva_0c_{\beta_2-1} + b_0d_{\beta_2-1} \\
&\quad + b_1d_0 + \cdots + b_{\beta_2-1}d_{\beta_2-2}) + b_0d_{\beta_2-1} \\
0 &= z_1 \cdot T(z_2).
\end{aligned}$$

This implies that $T(z_2) \in C^\perp$. Hence $C^\perp$ is $\mathbb{Z}_p\mathbf{S}$-additive cyclic code. □

Definition 2.5. *A subset $C \subseteq \boldsymbol{S}_{\beta_1,\beta_2}$ is called a $\mathbb{Z}_p\boldsymbol{S}$-additive cyclic code if and only if C is a subgroup of $\boldsymbol{S}_{\beta_1,\beta_2}$ and for all $d(y) = (f(y) \mid g(y)) = (f_0 + f_1 y + \cdots + f_{\beta_1-1}y^{\beta_1-1} \mid g_0 + g_1 y + \cdots + g_{\beta_2-1}y^{\beta_2-1})$ in C, we have $y \cdot d(y) = (f_{\beta_1-1} + f_0 y + \cdots + f_{\beta_1-2}y^{\beta_1-1} \mid g_{\beta_2-1} + g_0 y + \cdots + g_{\beta_2-2}y^{\beta_2-1}) \in C$.*

Theorem 2.2. *A code C is a $\mathbb{Z}_p\boldsymbol{S}$-additive cyclic code if and only if C is a $\boldsymbol{S}[y]$-submodule of $\boldsymbol{S}_{\beta_1,\beta_2}$.*

Proof. Let C be a $\mathbb{Z}_p\mathbf{S}$-additive cyclic code. Then we show that for any $d(y) \in C$ and $h(y) \in \mathbf{S}[y]$, $h(y)d(y) \in C$. Assume that $d(y) = (f(y) \mid g(y)) \in C$, where $f(y) = (f_0 + f_1 y + \cdots + f_{\beta_1-1}y^{\beta_1-1})$ and $g(y) = (g_0 + g_1 y + \cdots + g_{\beta_2-1}y^{\beta_2-1})$. Now,

$$yd(y) = (f_{\beta_1-1} + f_0 y + \cdots + f_{\beta_1-2}y^{\beta_1-1} \mid g_{\beta_2-1} + g_0 y + \cdots + g_{\beta_2-2}y^{\beta_1-1}),$$

represents the cyclic shift $T(d(y))$ of $d(y)$. Also, C is $\mathbb{Z}_p\mathbf{S}$- additive cyclic code, so $y^i d(y) \in C$ for all $i \in N$. It follows that $h(y) \cdot d(y) \in C$. This implies that C is $\mathbf{S}[y]$- submodule of $\mathbf{S}_{\beta_1,\beta_2}$. The Converse of this lemma is directly followed by Definition 2.5. □

Let us define the Gray map

$$\phi_1 : \mathbf{S} \longrightarrow \mathbb{Z}_p^4 \tag{2.3}$$

such that $\phi_1(a+ub+vc+uvd) = (a+b+c+d, c+d, b+d, d)$ for all $a, b, c, d \in \mathbf{S}$. Again, define another Gray map

$$\Psi : \mathbb{Z}_p \times \mathbf{S} :\longrightarrow \mathbb{Z}_p \times \mathbb{Z}_p^4 \tag{2.4}$$

such that $\Psi(c \mid c') = (c, \phi_1(c'))$. An extension of the map Ψ in (2.4) is defined as

$$\Psi_1 : \mathbb{Z}_p^{\beta_1} \times \mathbf{S}^{\beta_2} :\longrightarrow \mathbb{Z}_p^n \tag{2.5}$$

such that $\Psi_1(\mathbf{y} = (y' \mid y")) = ((y' \mid \phi_1(y"))$, where $\mathbf{y} = (y'_0, y'_1, \ldots, y'_{\beta_1-1} \mid y"_0, y"_1, \ldots, y"_{\beta_2-1}) \in \mathbb{Z}_p^{\beta_1} \times \mathbf{S}^{\beta_2}$.

Definition 2.6. *Let $\boldsymbol{y} = (y' \mid y") \in \mathbb{Z}_p^{\beta_1} \times \boldsymbol{S}^{\beta_2}$, where $y' \in \mathbb{Z}_p^{\beta_1}$ and $y" \in \boldsymbol{S}^{\beta_2}$. Then the Gray weight of $\boldsymbol{y}$ is defined as*

$$w_G(\boldsymbol{y}) = w_H(y') + w_H(\phi_1(y")),$$

where w_H denotes the Hamming weight.

Definition 2.7. *Let* $\boldsymbol{y}, \boldsymbol{z} \in \mathbb{Z}_p^{\beta_1} \times \boldsymbol{S}^{\beta_2}$. *Then the Gray distance between* $\boldsymbol{y}$ *and* $\boldsymbol{z}$ *is defined as*

$$d_G(\boldsymbol{y}, \boldsymbol{z}) = w_G(\boldsymbol{y} - \boldsymbol{z}) = d_H((y^{'} \mid \phi_1(y^{"}), (z^{'} \mid \phi_1(z^{"}))).$$

Definition 2.8. *Let* $\boldsymbol{y}, \boldsymbol{z} \in \mathbb{Z}_p^{\beta_1} \times \boldsymbol{S}^{\beta_2}$. *Then the Lee distance between* $\boldsymbol{y}$ *and* $\boldsymbol{z}$ *is defined as*

$$d_L(\boldsymbol{y}, \boldsymbol{z}) = w_L(\boldsymbol{y} - \boldsymbol{z}).$$

3 $\mathbb{Z}_p$S-additive cyclic codes

In this section, we obtain the set of generators for $\mathbb{Z}_p\mathbf{S}$-additive cyclic codes as $\mathbf{S}[y]$-submodules of $\mathbf{S}_{\beta_1,\beta_2}$. Here, C will always denote a $\mathbb{Z}_p\mathbf{S}$-additive cyclic code. Since C and $\mathbf{S}[y]/\langle y^{\beta_2} - 1\rangle$ are $\mathbf{S}[y]$-submodules of $\mathbf{S}_{\beta_1,\beta_2}$, we define a mapping

$$\eta : C \longrightarrow \mathbf{S}[y]/\langle y^{\beta_2} - 1\rangle$$

such that $\eta(f(y) \mid g(y)) = g(y)$. Clearly, η is a module homomorphism whose image is $\mathbf{S}[y]$-submodule in $\mathbf{S}[y]/\langle y^{\beta_2} - 1\rangle$ and $ker(\eta)$ is a submodule of C. Further, $\eta(C)$ can easily be identified as an ideal in the ring $\mathbf{S}[y]/\langle y^{\beta_2} - 1\rangle$ (see for reference [14]). Since n is odd and $\eta(C)$ is an ideal in $\mathbf{S}[y]/\langle y^{\beta_2} - 1\rangle$, $\eta(C) = \langle g(y) + up_1(y) + vq_1(y) + uvr_1(y), ua_1(y) + vq_2(y) + uvr_2(y), va_2(y) + uvr_3(y), uva_3(y)\rangle$ with $a_i \mid g_i \mid (y^{\beta_2} - 1)(\mathrm{mod} p)$, for $i = 1, 2, 3$.

$$ker(\eta) = \{(f(y), 0) \in C \mid f(y) \in \mathbb{Z}_p[y]/\langle y^{\beta_1} - 1\rangle\}.$$

Now, let J

$$J = \{f(y) \in \mathbb{Z}_p[y]/\langle y^{\beta_1} - 1\rangle \mid (f(y), 0) \in ker(\eta)\}.$$

It is clear that J is an ideal in the ring $\mathbb{Z}_p[y]/(y^{\beta_1} - 1)$ and hence a cyclic code. Therefore, by the well-known result on generators of binary cyclic codes, we have $J = \langle f(y)\rangle$. Now, for any element $(h(y), 0) \in ker(\eta)$, we have $h(y) \in J = \langle f(y)\rangle$ and it can be written as $h(y) = m_1(y)f(y)$ for some polynomial $m_1(y) \in \mathbb{Z}_p[y]/(y^{\beta_1} - 1)$. Thus, $(h(y), 0) = (m_1(y)f(y), 0)$. This implies that $ker(\eta)$ is a submodule of C generated by an element of the form $(f(y), 0)$, where $f(y) \mid (y^{\beta_1} - 1)(\mathrm{mod} p)$. By the first isomorphism theorem for rings, we have

$$\begin{aligned}\frac{C}{ker(\eta)} \cong\; & \langle g(y) + up_1(y) + vq_1(y) + uvr_1(y), ua_1(y) + vq_2(y) + uvr_2(y), \\ & va_2(y) + uvr_3(y), uva_3(y)\rangle.\end{aligned}$$

This implies that any $\mathbb{Z}_p\mathbf{S}$-additive cyclic code can be generated as a $\mathbf{S}[y]$-submodule of $\mathbf{S}_{\beta_1,\beta_2}$ by $(f_1(y),0)$ and $(f_2(y), g(y)+up_1(y)+vq_1(y)+uvr_1(y))$ $(f_3(y), ua_1(y)+vq_2(y)+uvr_2(y))$, $(f_4(y), va_2(y)+uvr_3(y))$ and $(f_5, uva_3(y))$. Hence, any element in C can be expressed as $d_1(y) \times (f_1(y),0) + d_2(y) \times (f_2(y), g(y)+up_1(y)+vq_1(y)+uvr_1(y)) + d_3(y) \times (f_3(y), ua_1(y)+vq_2(y)+uvr_2(y)) + d_4(y) \times (f_4(y), va_2(y)+uvr_3(y)) + d_5(y) \times (f_5, uva_3(y))$, where $d_1(y)$, $d_2(y)$, $d_3(y)$, $d_4(y)$ and $d_5(y)$ are polynomials in the ring $\mathbf{S}[y]$.

Theorem 3.1. *If* $C = \langle (f_1(y),0),(f_2(y), g(y)+up_1(y)+vq_1(y)+uvr_1(y))(f_3(y), ua_1(y)+vq_2(y)+uvr_2(y)),(f_4(y), va_2(y)+uvr_3(y)),(f_5(y), uva_3(y))\rangle$ *is a* $\mathbb{Z}_p\boldsymbol{S}$-*additive cyclic code, then* $deg(f_i(y)) < deg(f_1(y))$, *where* $i = 2,3,4,5$.

Proof. Suppose that $deg(f_i(y)) \geq deg(f_1(y))$. Then we can assume that

$$deg(f_i(y)) - deg(f_1(y)) = t$$

and the code with generators is of the form

$$\begin{aligned} C^{'} &= \langle (f_1(y),0),((f_2(y), g(y)+up_1(y)+vq_1(y)+uvr_1(y)), \\ &\quad (f_3(y), ua_1(y)+vq_2(y)+uvr_2(y)),(f_4(y), va_2(y)+uvr_3(y)), \\ &\quad (f_5, uva_3(y)) - y^t \cdot (f_1(y), o)\rangle \\ &= \langle (f_1(y),0),(f_2(y)-y^t f_1(y), g(y)+up_1(y)+vq_1(y)+uvr_1(y)), \\ &\quad (f_3(y)-y^t f_1(y), ua_1(y)+vq_2(y)+uvr_2(y)),(f_4(y)-y^t f_1(y), va_2(y) \\ &\quad +uvr_3(y)),(f_5(y)-y^t f_1(y), uva_3(y))\rangle. \end{aligned}$$

This implies that $C^{'} \subseteq C$. Now, for any

$$\begin{aligned} &((l_1(y), g_1(y)+2a_1(y)+up(y)),(l_2(y), ug_2(y)+2a_2(y))) \\ &\quad = ((l_1(y)+y^t f(y),(g_1(y)+2a_1(y)+up(y)),(l_2(y)+y^t f(y), \\ &\quad\quad ug_2(y)+2a_2(y))) - (y^t f(y),0). \end{aligned}$$

This shows that $C \subseteq C^{'}$. Finally, we get $C = C^{'}$. $\square$

Theorem 3.2. *Let* $C = \langle (f_1(y),0),(f_2(y), g(y)+up_1(y)+vq_1(y)+uvr_1(y))\rangle$ *be a* $\mathbb{Z}_p\boldsymbol{S}$-*additive cyclic code of length* (β_1,β_2) *and* $g(y)+up_1(y)+vq_1(y)+uvr_1(y) \mid (y^{\beta_2}-1)$. *If* $l(y) = \frac{(y^{\beta_2}-1)}{g(y)+up_1(y)+vq_1(y)+uvr_1(y)}$, *then* $f_1 \mid lf_2$.

Proof. Let $\eta(l(y)(f_2(y), g(y)+up_1(y)+vq_1(y)+uvr_1(y)) = \eta(l(y)f_2(y),0)$. This implies that $l(y)f_2(y),0) \in ker(\eta)$. Hence, $f_1(y) \mid l(y)f_2(y)$. $\square$

Theorem 3.3. *Let*

$$C = \left\langle \begin{array}{c} (f_1(y),0),(f_2(y), g(y)+up_1(y)+vq_1(y)+uvr_1(y)), \\ (f_3(y), ua_1(y)+vq_2(y)+uvr_2(y)),(f_4(y), va_2(y)+uvr_3(y)), \\ (f_5(y), uva_3(y)) \end{array} \right\rangle$$

be a $\mathbb{Z}_p\boldsymbol{S}$-additive cyclic code of length (β_1, β_2) and $a_i \mid g \mid (y^{\beta_2} - 1)$ for $i = 1, 2, 3$. If $h_g = \frac{(y^{\beta_2}-1)}{g}$, $H_1 = \gcd(h_g p_1, h_g q_1,$ $h_g r_1, (y^{\beta_2}-1))$, $H_2 = \frac{(y^{\beta_2}-1)}{H_1}$, $h_{a_1} = \frac{(y^{\beta_2}-1)}{a_1}$, $I_1 = \gcd(h_{a_1} q_2, h_{a_1} r_2, (y^{\beta_2}-1))$, $I_2 = \frac{(y^{\beta_2}-1)}{I_1}$, $h_{a_2} =$ $\frac{(y^{\beta_2}-1)}{a_2}$, $J_1 = \gcd(h_{a_2} r_3, (y^{\beta_2} - 1))$, $J_2 = \frac{(y^{\beta_2}-1)}{J_1}$, $h_{a_3} = \frac{(y^{\beta_2}-1))}{a_3}$, then

(*i*) $f_1 \mid H_2 h_g f_2$,

(*ii*) $f_1 \mid I_2 h_{a_1} f_3$,

(*iii*) $f_1 \mid J_2 h_{a_2} f_4$,

(*iv*) $f_1 \mid h_{a_3} f_5$.

Proof. (*i*) Since $H_1 \mid h_g p_1$, $H_1 \mid h_g q_1$ and $H_1 \mid h_g r_1$, $h_g p_1 = b_1 H_1$, $h_g q_1 = b_2 H_1$ and $h_g r_1 = b_3 H_1$ for some polynomials $b_1, b_2, b_3 \in \mathbf{S}[y]$. Now,

$$\begin{aligned}
&\eta(H_2 h_g(f_2(y), g(y) + up_1(y) + vq_1(y) + uvr_1(y))) \\
&= \eta(H_2 h_g f_2(y), H_2 h_g g(y) + uH_2 h_g p_1(y) + vH_2 h_g q_1(y) + uvH_2 h_g r_1(y)) \\
&= \eta(H_2 h_g f_2(y), uH_2 H_1 b_1(y) + vH_2 H_1 b_2(y) + uvH_2 H_1 b_3(y)) \\
&= \eta(H_2 h_g f_2(y), 0) \\
&= 0.
\end{aligned}$$

This implies that

$$(H_2 h_g(f_2(y), g(y) + up_1(y) + vq_1(y) + uvr_1(y))) = (H_2 h_g f_2(y), 0) \in C.$$

Therefore, $(H_2 h_g f_2(y), 0) \in ker(\eta) = \langle (f_1, 0) \rangle$. Hence $f_1 \mid H_2 h_g f_2$.

(*ii*) Since $I_1 \mid h_{a_1} q_2$ and $I_1 \mid h_{a_1} r_2$, $h_{a_1} q_2 = c_1 I_1$ and $h_{a_1} r_2 = c_2 I_1$ for some polynomials $c_1, c_2 \in \mathbf{S}[y]$. Now,

$$\begin{aligned}
&\eta(I_2 h_{a_1}(f_3(y), ua_1(y) + vq_2(y) + uvr_2(y))) \\
&= \eta(I_2 h_{a_1} f_3(y), I_2 h_{a_1}(ua_1(y) + vq_2(y) + uvr_2(y))) \\
&= \eta(I_2 h_{a_1} f_3(y), I_2 h_{a_1} ua_1(y) + vI_2 h_{a_1} q_2(y) + uvI_2 h_{a_1} r_2(y))) \\
&= \eta(I_2 h_{a_1} f_3(y), uI_2 I_1 a_1(y) + vI_2 I_2 c_1(y) + uvI_1 I_2 c_2(y))) \\
&= \eta(I_2 h_{a_1} f_3(y), 0) \\
&= 0.
\end{aligned}$$

This implies that $(I_2 h_{a_1}(f_3(y), ua_1(y)+vq_2(y)+uvr_2(y))) = ((I_2 h_{a_1}(f_3(y), 0) \in C$. Therefore, $(I_2 h_{a_1} f_3(y), 0) \in ker(\eta) = \langle (f_1, 0) \rangle$. Hence $f_1 \mid I_2 h_{a_1} f_3$.

(*iii*) Since $J_1 \mid h_{a_2}r_3$, so $h_{a_2}r_3 = d_1J_1$ for some polynomials $d_1 \in \mathbf{S}[y]$. Now,

$$\begin{aligned}
&\eta(J_2h_{a_2}(f_4(y), va_2(y) + uvr_3(y)))\\
&= \eta(J_2h_{a_2}f_4(y), I_2h_{a_1}va_2(y) + uvr_3(y)))\\
&= \eta(J_2h_{a_2}f_4(y), J_2h_{a_2}va_2(y) + uvI_2h_{a_2}r_3(y)))\\
&= \eta(J_2h_{a_2}f_4(y), vJ_2J_1a_2(y) + uvJ_1J_2d_1(y)))\\
&= \eta(J_2h_{a_2}f_4(y), 0)\\
&= 0.
\end{aligned}$$

This implies that $(J_2h_{a_2}(f_4(y), va_2(y) + uvr_3(y))) = ((J_2h_{a_2}(f_4(y), 0) \in C$. Therefore,
$(J_2h_{a_2}f_4(y), 0) \in ker(\eta) = \langle (f_1, 0)\rangle$. Hence $f_1 \mid J_2h_{a_2}f_4$.

(*iv*) Let $\eta(h_{a_3}(f_5(y), uva_3)) = \eta(h_{a_3}f_5(y), 0)$. This implies that $(h_{a_3}f_5(y), 0) \in ker(\eta)$. Hence, $f_1 \mid h_{a_3}f_5$. □

Theorem 3.4. *Let*

$$C = \left\langle \begin{array}{c} (f_1(y), 0), (f_2(y), g(y) + up_1(y) + vq_1(y) + uvr_1(y)), \\ (f_3(y), ua_1(y) + vq_2(y) + uvr_2(y)), (f_4(y), va_2(y) + uvr_3(y)), \\ (f_5(y), uva_3(y)) \end{array} \right\rangle$$

be a $\mathbb{Z}_p\boldsymbol{S}$*-additive cyclic code of length* (β_1, β_2) *and* $a_i \mid g \mid (y^{\beta_2} - 1)$ *for* $i = 1, 2, 3$. *Suppose that* $h_g = \frac{(y^{\beta_2}-1)}{g}$, $h_1 = \gcd(h_gp_1, h_gq_1, h_gr_1, (y^{\beta_2} - 1))$, $h_2 = \frac{(y^{\beta_2}-1)}{h_1}$, $h_{a_1} = \frac{(y^{\beta_2}-1)}{a_1}$, $m_1 = \gcd(h_{a_1}q_2, h_{a_1}r_2, (y^{\beta_2} - 1))$, $m_2 = \frac{(y^{\beta_2}-1)}{m_1}$, $h_{a_2} = \frac{(y^{\beta_2}-1)}{a_2}$, $s_1 = \gcd(h_{a_2}r_3, (y^{\beta_2} - 1))$, $s_2 = \frac{(y^{\beta_2}-1)}{s_1}$, $h_{a_3} = \frac{(y^{\beta_2}-1))}{a_3}$. *Further, assume that*

$$\begin{aligned}
S_1 &= \bigcup_{i=0}^{\beta_1-deg(f_1)-1} \{y^i \cdot (f_1(y), 0)\};\\
S_2 &= \bigcup_{i=0}^{\beta_2-deg(g)-1} \{y^i \cdot (f_2(y), g(y) + up_1(y) + vq_1(y) + uvr_1(y))\};\\
S_3 &= \bigcup_{i=0}^{\beta_2-deg(h_1)-1} \{y^i \cdot (h_gf_2, uh_gp_1(y) + vh_gq_1(y) + uvh_gr_1(y))\};
\end{aligned}$$

$$
\begin{aligned}
S_4 &= \bigcup_{i=0}^{deg(g)-deg(a_1)-1} \{y^i \cdot (f_3(y), ua_1(y) + vq_2(y) + uvr_2(y)\};\\
S_5 &= \bigcup_{i=0}^{\beta_2-deg(m_1)-1} \{y^i \cdot (h_{a_1}f_3(y), vh_{a_1}q_2(y) + uvh_{a_1}r_2(y)\};\\
S_6 &= \bigcup_{i=0}^{deg(a_1)-deg(a_2)-1} \{y^i \cdot (f_4(y), va_2(y) + uvr_3(y)\};\\
S_7 &= \bigcup_{i=0}^{\beta_2-deg(s_1)-1} \{y^i \cdot (h_{a_2}f_4(y), uvh_{a_2}r_3(y)\};\\
S_8 &= \bigcup_{i=0}^{deg(a_2)-deg(a_3)-1} \{y^i \cdot (f_5(y), uva_3(y)\}.
\end{aligned}
$$

Then $S = S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5 \cup S_6 \cup S_7 \cup S_8$ *is a minimal generating set for the code* C *and*

$\mid C \mid = p^{\beta_1-deg(f_1)}p^{10\beta_2-deg(g)-3deg(h_1)-deg(a_1)-2deg(m_1)-deg(a_2)-deg(s_1)-deg(a_3)}$.

Proof. Let $c \in C$ be a codeword and $c_i \in \mathbf{S}[y]$, $i = 1,\ 2,\ 3,\ 4,\ 5$. Then

$$
\begin{aligned}
c &= c_1 \cdot (f_1(y), 0) + c_2 \cdot (f_2(y), g(y) + up_1(y) + vq_1(y) + uvr_1(y))\\
&\quad +c_3 \cdot (f_3(y), ua_1(y) + vq_2(y) + uvr_2(y)) + c_4 \cdot (f_4(y), va_2(y) + uvr_3(y))\\
&\quad +c_5 \cdot (f_5(y), uva_3(y)).\\
c &= (\theta(c_1)f_1(y), 0) + c_2 \cdot (f_2(y), g(y) + up_1(y) + vq_1(y) + uvr_1(y))\\
&\quad +c_3 \cdot (f_3(y), ua_1(y) + vq_2(y) + uvr_2(y)) + c_4 \cdot (f_4(y), va_2(y) + uvr_3(y))\\
&\quad +c_5 \cdot (f_5(y), uva_3(y)).
\end{aligned}
$$

If $deg(\theta(c_1)) \leq \beta_1 - deg(f_1) - 1$, then $\beta_1 - deg(f_1) \in span(S_1)$. Otherwise, by division algorithm, $deg(\theta(c_1) = \frac{(y^{\beta_1}-1)}{f_1(y)}b + d$, where $deg(d) \leq \beta_1 - deg(f_1) - 1$. Therefore,

$$
(\theta(c_1)f_1, 0) = ((\frac{(y^{\beta_1}-1)}{f_1(y)}b + d)f_1, 0) = (df_1, 0) = d(f_1, 0).
$$

This shows that $(\theta(c_1)f_1, 0) \in span(S_1)$. Now, we have to prove

$$
c_2 \cdot (f_2, g(y) + up_1(y) + vq_1(y) + uvr_1(y)) \in span(S_1 \cup S_2 \cup S_3) \subset span(S).
$$

Let us divide c_2 by h_g and write $c_2 = b_1 h_g + d_1$, where $d_1 = 0$ or $deg(d_1) \leq \beta_2 - deg(g) - 1$. Therefore,

$$\begin{aligned} & c_2 \cdot (f_2, g(y) + up_1(y) + vq_1(y) + uvr_1(y)) \\ &= (b_1 h_g + d_1) \cdot ((f_2, g(y) + up_1(y) + vq_1(y) + uvr_1(y)) \\ &= b_1(h_g f_2, uh_g p_1(y) + vh_g q_1(y) + uvh_g r_1(y)) + d_1(f_2, g(y) + up_1(y) + vq_1(y) \\ &\quad + uvr_1(y)). \end{aligned}$$

Cleraly, $d_1(f_2, g(y) + up_1(y) + vq_1(y) + uvr_1(y)) \in span(S_2)$. It remains to show that $b_1(h_g f_2, uh_g p_1(y) + vh_g q_1(y) + uvh_g r_1(y)) \in span(S_1 \cup S_2 \cup S_3)$. Since $h_1 \mid h_g p_1$, $h_1 \mid h_g q_1$, $h_1 \mid h_g r_1$, $h_g p_1 = l_1 h_1$, $h_g q_1 = l_2 h_1$ and $h_g r_1 = l_3 h_1$. Hence, $h_g p_1 h_2 = h_g q_1 h_2 = h_g r_1 h_2 = 0$. Again, by division algorithm, we have $b_1 = b_2 h_2 + d_2$, where $d_2 = 0$ or $deg(d_2) \leq \beta_2 - deg(h_1) - 1$. Now,

$$\begin{aligned} & b_1(h_g f_2, uh_g p_1(y) + vh_g q_1(y) + uvh_g r_1(y)) \\ &= (b_2 h_2 + d_2)(h_g f_2, uh_g p_1(y) + vh_g q_1(y) + uvh_g r_1(y)) \\ &= b_2(h_2 h_g f_2, uh_2 h_g p_1(y) + vh_2 h_g q_1(y) + uvh_2 h_g r_1(y)) \\ &\quad + d_2(h_g f_2, uh_g p_1(y) + vh_g q_1(y) + uvh_g r_1(y)). \\ &= b_2(h_2 h_g f_2, 0) + d_2(h_g f_2, uh_g p_1(y) + vh_g q_1(y) + uvh_g r_1). \end{aligned}$$

By Theorem 3.3, $f_1 | h_2 h_g f_2$, then $b_2(h_2 h_g f_2, 0) \in span(S_1)$. Also, $(h_g f_2, uh_g p_1(y) + vh_g q_1(y) + uvh_g r_1) \in span(S_3)$. Then,

$$c_2 \cdot (f_2, g(y) + up_1(y) + vq_1(y) + uvr_1(y)) \in span(S_1 \cup S_2 \cup S_3).$$

Again, we have to show

$$c_3 \cdot (f_3, ua_1(y) + vq_2(y) + uvr_2(y)) \in span(S_1 \cup S_4 \cup S_5) \subset span(S).$$

Let us divide c_3 by h_{a_1} and write $c_3 = b_3 h_{a_1} + d_3$, where $d_3 = 0$ or $deg(d_3) \leq deg(g) - deg(a_1) - 1$. Therefore,

$$\begin{aligned} & c_3 \cdot (f_3, ua_1(y) + vq_2(y) + uvr_2(y)) \\ &= (b_3 h_{a_1} + d_3) \cdot ((f_3, ua_1(y) + vq_2(y) + uvr_2(y)) \\ &= b_3(h_{a_1} f_3, uh_{a_1} a_1(y) + vh_{a_1} q_2(y) + uvh_{a_1} r_2(y)) \\ &\quad + d_3(f_3, ua_1(y) + vq_2(y) + uvr_2(y)). \end{aligned}$$

Obviuosly, $d_3(f_3, ua_1(y) + vq_2(y) + uvr_2(y)) \in span(S_4)$. It remains to show that
$b_3(h_{a_1} f_3, uh_{a_1} a_1(y) + vh_{a_1} q_2(y) + uvh_{a_1} r_2(y)) \in span(S_1 \cup S_2 \cup S_3)$. Since $m_1 \mid h_{a_1} q_2$ and $m_1 \mid h_{a_1} r_2$, so $h_{a_1} q_2 = l_4 m_1$ and $h_{a_1} r_2 = l_5 m_1$. Hence,

$h_{a_1}q_2m_2 = h_{a_1}r_2m_2 = 0$. Again, by division algorithm, we have $b_3 = b_4m_2 + d_4$, where $d_4 = 0$ or $deg(d_4) \leq \beta_2 - deg(m_1) - 1$. Now,

$$\begin{aligned} & b_3(h_{a_1}f_3, vh_{a_1}q_2(y) + uvh_{a_1}r_2(y)) \\ &= (b_4m_2 + d_4)(h_{a_1}f_3, vh_{a_1}q_2(y) + uvh_{a_1}r_2(y)) \\ &= b_3(m_2h_{a_1}f_3, vm_2h_{a_1}q_2(y) + uvm_2h_{a_1}r_2(y)) \\ &\quad + d_4(h_{a_1}f_3, vh_{a_1}q_2(y) + uvh_{a_1}r_2(y)) \\ &= b_3(m_2h_{a_1}f_3, 0) + d_4(h_{a_1}f_3, vh_{a_1}q_2(y) + uvh_{a_1}r_2). \end{aligned}$$

By Theorem 3.3, $f_1|m_2h_{a_1}f_3$, then $b_3(m_2h_{a_1}f_3, 0) \in span(S_1)$. Also, $(h_{a_1}f_3, vh_{a_1}q_2(y) + uvh_{a_1}r_2) \in span(S_3)$. Hence

$$c_3 \cdot (f_3, ua_1(y) + vq_2(y) + uvr_2(y)) \in span(S_1 \cup S_4 \cup S_5).$$

Again, we have to show

$$c_4 \cdot (f_4, vqa_2(y) + uvr_3(y)) \in span(S_1 \cup S_6 \cup S_7) \subset span(S).$$

Let us divide c_4 by h_{a_2} and write $c_4 = b_5h_{a_2} + d_5$, where $d_5 = 0$ or $deg(d_5) \leq deg(a_1) - deg(a_2) - 1$. Therefore,

$$\begin{aligned} c_4 \cdot (f_4, va_2(y) + uvr_3(y)) &= (b_5h_{a_2} + d_5) \cdot ((f_4, va_2(y) + uvr_3(y)) \\ &= b_4(h_{a_2}f_4, vh_{a_2}a_2(y) + uvh_{a_2}r_3(y)) \\ &\quad + d_5(f_4, va_2(y) + uvr_3(y)). \end{aligned}$$

It is clear that $d_5(f_4, va_2(y) + uvr_3(y)) \in span(S_4)$. It remains to show that

$$b_4(h_{a_2}f_4, vh_{a_2}a_2(y) + uvh_{a_2}r_3(y)) \in span(S_1 \cup S_2 \cup S_3).$$

Since $s_1 \mid h_{a_2}r_3$, we get $h_{a_2}r_3 = l_6s_1$ and hence $h_{a_2}r_3s_2 = 0$. Again, by division algorithm, we have $b_5 = b_6s_2 + d_6$, where $d_6 = 0$ or $deg(d_6) \leq \beta_2 - deg(s_1) - 1$. Now,

$$\begin{aligned} b_5(h_{a_2}f_4, uvh_{a_2}r_3(y)) &= (b_6s_2 + d_6)(h_{a_2}f_4, uvh_{a_2}r_3(y)) \\ &= b_6(s_2h_{a_2}f_4, uvm_2h_{a_3}r_3(y)) + d_6(h_{a_2}f_4, uvh_{a_2}r_3(y)) \\ &= b_6(s_2h_{a_2}f_4, 0) + d_6(h_{a_2}f_4, uvh_{a_2}r_3). \end{aligned}$$

By Theorem 3.3, $f_1|s_2h_{a_2}f_4$ which implies $b_6(s_2h_{a_2}f_4, 0) \in span(S_1)$. Also, $(h_{a_2}f_4, uvh_{a_2}r_3) \in span(S_7)$. Hence

$$c_4 \cdot (f_4, va_2(y) + uvr_3(y)) \in span(S_1 \cup S_6 \cup S_7).$$

Finally, we have to show that $c_4 \cdot (f_5, uva_3(y)) \in span(S_8)$. By division algorithm, we have $c_5 = h_{a_3}b_7 + d_7$, where $d_7 = 0$ or $deg(d_7) \leq deg(a_2) - deg(a_3) - 1$. Now,

$$\begin{aligned} c_5(f_5, uva_3) &= (b_7h_{a_3} + d_7)(f_5, uva_3) \\ &= b_7(h_{a_3}f_5, 0) + d_7(f_5, uva_3). \end{aligned}$$

By Theorem 3.3, $f_1|h_{a_3}f_5$ which implies $(h_{a_3}f_5, 0) \in span(S_1)$ and $d_7(f_5, uva_3) \in span(S_8)$. We conclude that $c \in span(S)$, that is, S generates the code C. Thus, S is the minimal spanning set for C because none of the element of S is a linear combination of the other and

$$| C |= p^{\beta_1 - deg(f_1)} p^{10\beta_2 - deg(g) - 3deg(h_1) - deg(a_1) - 2deg(m_1) - deg(a_2) - deg(s_1) - deg(a_3)}.$$

□

The following are immediate consequence of Theorem 3.4.

Corollary 3.1. *Let $C = \langle (f_1(y), 0) \rangle$ be a $\mathbb{Z}_p\boldsymbol{S}$-additive cyclic code of length (β_1, β_2) and $f_1(y) \mid y^{\beta_1} - 1$. If*

$$S_1 = \bigcup_{i=0}^{\beta_1 - deg(f_1) - 1} \{y^i \cdot (f_1(y), 0)\},$$

then S_1 forms a basis for C with $| C |= p^{\beta_1 - deg(f_1)}$.

Corollary 3.2. *Let $C = \langle (f_1(y), 0), (f_2, g(y) + up_1(y) + vq_1(y) + uvr_1(y)) \rangle$ be a $\mathbb{Z}_p\boldsymbol{S}$-additive cyclic code of length (β_1, β_2) and $g(y) + up_1(y) + vq_1(y) + uvr_1(y)) \mid y^{\beta_2} - 1$. If*

$$\begin{aligned} S_1 &= \bigcup_{i=0}^{\beta_1 - deg(f_1) - 1} \{y^i \cdot (f_1(y), 0)\}; \\ S_2 &= \bigcup_{i=0}^{\beta_2 - deg(g_1) - 1} \{y^i \cdot (f_2, g(y) + up_1(y) + vq_1(y) + uvr_1(y))\}, \end{aligned}$$

then $S_1 \cup S_2$ forms a basis for C with $| C |= p^{\beta_1 - deg(f_1)} p^{4(\beta_2 - deg(g_1))}$.

Proof. Let $c \in C$ be a codeword and $c_i \in \mathbf{S}[y]$, $i = 1,\ 2,\ 3,\ 4,\ 5$. Then

$$\begin{aligned} c &= c_1 \cdot (f_1(y), 0) + c_2 \cdot (f_2(y), g(y) + up_1(y) + vq_1(y) + uvr_1(y)) \\ c &= (\theta(c_1)f_1(y), 0) + c_2 \cdot (f_2(y), g(y) + up_1(y) + vq_1(y) + uvr_1(y)). \end{aligned}$$

If $deg(\theta(c_1)) \leq \beta_1 - deg(f_1) - 1$, then $\beta_1 - deg(f_1) \in span(S_1)$. Otherwise, by division algorithm, $deg(\theta(c_1) = \frac{(y^{\beta_1}-1)}{f_1(y)} b + d$, where $deg(d) \leq \beta_1 - deg(f_1) - 1$. Therefore,

$$(\theta(c_1)f_1, 0) \quad = \quad ((\frac{(y^{\beta_1}-1)}{f_1(y)} b + d)f_1, 0) = (df_1, 0) = d(f_1, 0).$$

This shows that $(\theta(c_1)f_1, 0) \in span(S_1)$. Now, we have to prove

$$c_2 \cdot (f_2, g(y) + up_1(y) + vq_1(y) + uvr_1(y)) \in span(S_1 \cup S_2).$$

Since $g(y) + up_1(y) + vq_1(y) + uvr_1(y)) \mid y^{\beta_2} - 1$, there exists h such that $y^{\beta_2} - 1 = h(y)(g(y) + up_1(y) + vq_1(y) + uvr_1(y)))$. Using division algorithm, we have two polynomials $b_1(y)$ and $d_1(y)$ such that

$$c_2 = hb_1 + d_1,$$

where $deg(d_1) = 0$ or $deg(d_1) \leq \beta_2 - deg(g) - 1$. Therefore,

$$\begin{aligned} & c_2 \cdot (f_2, g(y) + up_1(y) + vq_1(y) + uvr_1(y)) \\ = \quad & (hb_1 + d_1) \cdot ((f_2, g(y) + up_1(y) + vq_1(y) + uvr_1(y)) \\ = \quad & b_1(hf_2, 0) + d_1(f_2, g(y) + up_1(y) + vq_1(y) + uvr_1(y)). \end{aligned}$$

Cleraly, $d_1(f_2, g(y) + up_1(y) + vq_1(y) + uvr_1(y)) \in span(S_2)$. Hence, $S_1 \cup S_2$ forms a basis for C with $\mid C \mid = p^{\beta_1 - deg(f_1)} p^{4(\beta_2 - deg(g_1))}$. □

Corollary 3.3. *Let*

$$C \quad = \quad \left\langle \begin{array}{c} (f_1(y), 0), (f_2(y), g(y) + up_1(y) + vq_1(y) + uvr_1(y)), \\ (f_3(y), uva(y) \end{array} \right\rangle$$

be a $\mathbb{Z}_p\boldsymbol{S}$*-additive cyclic code of length* (β_1, β_2)*, where* $a(y) \mid g(y) \mid (y^{\beta_2} - 1)$ *and* $h_g = \frac{(y^{\beta_2}-1)}{g}$, $h_1 = \gcd(h_g p_1, h_g q_1, h_g r_1, (y^{\beta_2} - 1))$, $h_2 = \frac{(y^{\beta_2}-1)}{h_1}$. *If*

$$\begin{aligned} S_1 \quad &= \quad \bigcup_{i=0}^{\beta_1 - deg(f_1) - 1} \{y^i \cdot (f_1(y), 0)\}; \\ S_2 \quad &= \quad \bigcup_{i=0}^{\beta_2 - deg(g_1) - 1} \{y^i \cdot (f_2, g(y) + up_1(y) + vq_1(y) + uvr_1(y))\}; \\ S_3 \quad &= \quad \bigcup_{i=0}^{\beta_2 - deg(h_1) - 1} \{y^i \cdot (h_g f_2, uh_g p_1(y) + vh_g q_1(y) + uvh_g r_1(y))\}; \\ S_4 \quad &= \quad \bigcup_{i=0}^{deg(g) - deg(a) - 1} \{y^i \cdot (f_3(y), uva(y)\}, \end{aligned}$$

then $S = S_1 \cup S_2 \cup S_3 \cup S_4$ *is a minimal generating set for the code* C *and*

$$\mid C \mid = p^{\beta_1 - deg(f_1)} p^{7\beta_2 - 3deg(g) - 3deg(h_1) - deg(a)}.$$

Corollary 3.4. *Let*

$$C = \left\langle \begin{array}{c} (f_1(y),0),(f_2(y),ua_1(y)+vq_2(y)+uvr_2(y)), \\ (f_3(y),uva(y)) \end{array} \right\rangle$$

be a $\mathbb{Z}_p\boldsymbol{S}$*-additive cyclic code of length* (β_1,β_2) *and*
$h_{a_1} = \frac{(y^{\beta_2}-1)}{a_1}$, $m_1 = \gcd(h_{a_1}q_2, h_{a_1}r_2, (y^{\beta_2}-1))$, $m_2 = \frac{(y^{\beta_2}-1)}{m_1}$. *If*

$$\begin{aligned}
S_1 &= \bigcup_{i=0}^{\beta_1 - deg(f_1)-1} \{y^i \cdot (f_1(y),0)\}; \\
S_2 &= \bigcup_{i=0}^{\beta_2 - deg(a_1)-1} \{y^i \cdot (f_2, ua_1(y)+vq_2(y)+uvr_2(y))\}; \\
S_3 &= \bigcup_{i=0}^{\beta_2 - deg(m_1)-1} \{y^i \cdot (h_{a_1}f_2, vh_{a_1}q_2(y)+uvh_{a_1}r_2(y))\}; \\
S_4 &= \bigcup_{i=0}^{deg(a_1) - deg(a)-1} \{y^i \cdot (f_3(y), uva(y)\},
\end{aligned}$$

then $S = S_1 \cup S_2 \cup S_3 \cup S_4$ *is a minimal generating set for the code* C *and*

$$\mid C \mid = p^{\beta_1 - deg(f_1)} p^{5\beta_2 - 2deg(a_1) - 2deg(m_1) - deg(a)}.$$

Corollary 3.5. *Let* $C = \langle (f_1(y),0),(f_2(y),va_2(y)+uvr_2(y)),(f_3(y),uva(y)\rangle$ *be a* $\mathbb{Z}_p\boldsymbol{S}$*-additive cyclic code of length* (β_1,β_2) *and* $h_{a_2} = \frac{(y^{\beta_2}-1)}{a_2}$, $s_1 =$ $\gcd(h_{a_2}r_3,$
$(y^{\beta_2}-1))$, $s_2 = \frac{(y^{\beta_2}-1)}{s_1}$. *If*

$$\begin{aligned}
S_1 &= \bigcup_{i=0}^{\beta_1 - deg(f_1)-1} \{y^i \cdot (f_1(y),0)\}; \\
S_2 &= \bigcup_{i=0}^{\beta_2 - deg(a_2)-1} \{y^i \cdot (f_2, va_2(y)+uvr_3(y))\}; \\
S_3 &= \bigcup_{i=0}^{\beta_2 - deg(s_1)-1} \{y^i \cdot (h_{a_2}f_2, uvh_{a_2}r_3(y))\}; \\
S_4 &= \bigcup_{i=0}^{deg(a_2) - deg(a)-1} \{y^i \cdot (f_3(y), uva(y)\},
\end{aligned}$$

then $S = S_1 \cup S_2 \cup S_3 \cup S_4$ *is a minimal generating set for the code* C *and*

$$|\ C\ | = p^{\beta_1 - deg(f_1)} p^{3\beta_2 - deg(a_2) - deg(s_1) - deg(a)}.$$

Theorem 3.5. *Let* $C = \langle (f_1(y), 0), (f_2(y), g(y) + up_1(y) + vq_1(y) + uvr_1(y)), (f_3(y), uva(y)\rangle$ *be a* $\mathbb{Z}_p\boldsymbol{S}$*-additive cyclic code of length* (β_1, β_2)*, where* $f_1(y) = y + 1$ *and* $f_2(y) = f_3(y) = g(y) = a(y) = 1$*. Then* $\Psi_1(C)$ *is maximum distance separable with respect to singleton bound (MDSS) of parameters* $[\beta_1 + 4\beta_2, p^K, d_G]$*, where*

$$K = \beta_1 + 4\beta_2 - deg(f_1) - deg(a) - deg(g) - 2deg(h_1).$$

Proof. Obviously, $d_G(C) = 2$. Therefore, we have

$$d_G(C) - 1 = deg(f_1(y) + deg(f_2(y)) + deg(f_3(y)) + deg(g(y)) + deg(a(y)).$$

Hence, C is MDSS code. □

4 Duality of $\mathbb{Z}_p\mathbb{Z}_p[u, v]$-additive cyclic codes

In this section, we give the relationship between the generator polynomial of C and dual code. Let $f(y) \in \mathbf{S}[y]$ and $deg(f(y)) = t$. Then its reciprocal polynomial can be defined as $f^*(y) = y^{deg(f(y))} f(\frac{1}{y})$. Assume that $\omega_m(y) = \sum_{i=0}^{m-1} y^i$ be a polynomial. Now, let $m = \text{lcm}\{\beta_1, \beta_2\}$ and $\mathbf{f}(y) = (f(y), f^{'}(y)), \mathbf{g}(y) = (g(y), g^{'}(y)) \in \mathcal{S}_{\beta_1,\beta_2}$. Define a map

$$\zeta : \mathcal{S}_{\beta_1,\beta_2} \times \mathcal{S}_{\beta_1,\beta_2} \longrightarrow \frac{\mathbf{S}[y]}{\langle y^m - 1\rangle}$$

such that

$$\begin{aligned} \zeta(\mathbf{f}(y), \mathbf{g}(y)) \quad &= \quad uvf(y)\omega_{\frac{m}{\beta_1}}(y^{\beta_1})y^{m-1-deg(g(y))}g^*(y) \\ &\quad + f^{'}(y)\omega_{\frac{m}{\beta_2}}(y^{\beta_2})y^{m-1-deg(g^{'}(y))}g^{'*}(y)\text{mod}(\mathrm{y^m} - 1). \end{aligned}$$

Lemma 4.1. *Let* $n_1, n_2 \in \mathbb{N}$*. Then*

$$y^{n_1 n_2} - 1 = (y^{n_1} - 1)\omega_{n_2}(y^{n_1})$$

Proof. Let $x^{n_2} - 1 = (x-1)(x^{n_2-1} + x^{n_2-2} + \cdots + x + 1) = (x-1)\omega_{n_2}(x)$. Putting $x = y^{n_1}$, we get the desired result. □

Lemma 4.2. *Let* $\boldsymbol{f}, \boldsymbol{g} \in \mathbb{Z}_p^{\beta_1} \times \boldsymbol{S}^{\beta_2}$ *with associated polynomial* $\boldsymbol{f}(y) = (f(y), f^{'}(y))$, $\boldsymbol{g}(y) = (g(y), g^{'}(y)) \in \mathcal{S}_{\beta_1,\beta_2}$. *Then* $\boldsymbol{f}$ *is orthogonal to* $\boldsymbol{g}$ *and all its shifts if and only if*

$$\zeta(\boldsymbol{f}(y), \boldsymbol{g}(y)) = 0.$$

Proof. The proof of the following results can be seen in [17]. □

Theorem 4.1. *Let* $\boldsymbol{f}(y) = (f(y), f^{'}(y)), \boldsymbol{g}(y) = (g(y), g^{'}(y)) \in \mathcal{S}_{\beta_1,\beta_2}$ *such that* $\zeta(\boldsymbol{f}(y), \boldsymbol{g}(y)) = 0$. *If* $f^{'}(y) = 0$ *or* $g^{'}(y) = 0$, *then* $f(y)g^*(y) = 0 \bmod(y^{\beta_1} - 1)$ *over* $\mathbb{Z}_p$. *If* $f(y) = 0$ *or* $g(y) = 0$, *then* $f^{'}(y)g^{'*}(y) = 0 \bmod(y^{\beta_2} - 1)$ *over* $\boldsymbol{S}$.

Proof. Suppose that either $\mathbf{f}(y) = (f(y), f^{'}(y)) = 0$ or $\mathbf{g}(y) = (g(y), g^{'}(y)) = 0$. Then we need to show that $f^{'}(y)g^{'*}(y) = 0 \bmod(y^{\beta_2} - 1)$. Since

$$\begin{aligned} 0 &= \zeta(\mathbf{f}(y), \mathbf{g}(y)) \\ &= f^{'}(y)\omega_{\frac{m}{\beta_2}}(y^{\beta_2})y^{m-1-deg(g^{'}(y))}g^{'*}(y)\mathrm{mod}(\mathrm{y^m} - 1), \end{aligned}$$

there exists a polynomial $h(y)$ over $\mathbb{Z}_p$ such that

$$\begin{aligned} f^{'}(y)\omega_{\frac{m}{\beta_2}}(y^{\beta_2})y^{m-1-deg(g^{'}(y))}g^{'*}(y) &= h(y)\mathrm{mod}(\mathrm{y^m} - 1) \\ &= h(y)(y^m - 1). \end{aligned}$$

By proposition 4.1, $y^{m\beta_2} - 1 = (y^{\beta_2} - 1)\omega_m(y^{\beta_2})$, we get

$$\begin{aligned} f^{'}(y)y^m g^{'*}(y) &= h^{'}(y)(y^{\beta_2} - 1) \\ f^{'}(y)g^{'*}(y) &= 0 \bmod(y^{\beta_2} - 1). \end{aligned}$$

Similarly, we can prove other case. □

Theorem 4.2. *Let* $C = \langle (f_1(y), 0), (f_2(y), g(y) + up_1(y) + vq_1(y) + uvr_1(y)) \rangle$ *be a* $\mathbb{Z}_p\boldsymbol{S}$*-additive cyclic code of length* (β_1, β_2). *If* $C^\perp = \langle (\bar{f}_1(y), 0), (\bar{f}_2, \bar{g}(y) + u\bar{p}_1(y) + v\bar{q}_1(y) + uv\bar{r}_1(y)) \rangle$ *is the dual of* C, *then*

(*i*) $\bar{f_1}^*(y)\gcd(f_1(y), f_2(y)) = h_1(y)(y^{\beta_1} - 1)$,

(*ii*) $\bar{g}^*(y)g(y)f_1(y) = h_2(y)(y^{\beta_2} - 1)$.

Proof. (*i*) Since $(f_1(y), 0)$, $(f_2(y), g(y) + up_1(y) + vq_1(y) + uvr_1(y)) \in C$ and $(\bar{f}_1(y), 0) \in C^\perp$, by Proposition 4.2, we get

$$\zeta((f_1(y), 0), (\bar{f}_1(y), 0)) = 0,$$

$$\zeta((f_2(y), g(y) + up_1(y) + vq_1(y) + uvr_1(y)), (\bar{f}_1(y), 0)) = 0.$$

Using Theorem 4.1, we obtain $f_1(y)\bar{f_1}^*(y)=0,\ f_2(y)\bar{f_1}^*(y)=0$. It is obvious that $\bar{f_1}^*(y)\gcd(f_1(y),f_2(y))=0 \bmod (y^{\beta_1}-1)$. This implies that there exits a polynomial $h_1(y)\in\mathbb{Z}_p[y]$ such that

$$\bar{f_1}^*(y)\gcd(f_1(y),f_2(y))=h_1(y)(y^{\beta_1}-1).$$

(ii) We know that $(f_1(y),0),\ (f_2(y),g(y)+up_1(y)+vq_1(y)+uvr_1(y))\in C$. Then any element $c(y)\in C$ can be expressed as

$$\begin{aligned} c(y) &= uv\frac{f_2(y)}{\gcd(f_1(y),f_2(y))}\times(f_1(y),0)+uv\frac{f_1(y)}{\gcd(f_1(y),f_2(y))}\times(f_2(y),\\ &\quad g(y)+up_1(y)+vq_1(y)+uvr_1(y))\\ &= \big(0,uv\frac{f_1(y)}{\gcd(f_1(y),f_2(y))}g(y)\big). \end{aligned}$$

This implies that

$$\zeta((0,uv\frac{f_1(y)}{\gcd(f_1(y),f_2(y))}g(y)),(\bar{f_2},\bar{g}(y)+u\bar{p}_1(y)+v\bar{q}_1(y)+uv\bar{r}_1(y))=0.$$

By Theorem 4.1, we get

$$\begin{aligned} 0 &= uv\frac{f_1(y)}{\gcd(f_1(y),f_2(y))}g(y)\cdot(\bar{g}(y)+u\bar{p}_1(y)+v\bar{q}_1(y)+uv\bar{r}_1(y))^*\\ &= \frac{f_1(y)}{\gcd(f_1(y),f_2(y))}g(y)\bar{g}^*(y). \end{aligned}$$

This means that there exists a polynomial $h_2(y)\in\mathbf{S}[y]$ such that

$$f_1(y)g(y)\bar{g}^*(y)=h_2(y)(y^{\beta_2}-1).$$

□

5 $\mathbb{Z}_p$S-additive constacyclic codes

Definition 5.1. *Let λ be a unit in $\boldsymbol{S}$. A non-empty subset C of $\mathbb{Z}_p^{\beta_1}\times\boldsymbol{S}^{\beta_2}$ is called a $\mathbb{Z}_p\boldsymbol{S}$-additive λ-constacyclic code of length (β_1,β_2) if*

- (i) *C is additive code;*
- (ii) *For any codeword $\boldsymbol{z}=(a_0,a_1,\ldots,a_{\beta_1-1}\mid b_0,b_1,\ldots,b_{\beta_2-1})\in C$ its cyclic shift*

$$T_\lambda(\boldsymbol{z})=(a_{\beta_1-1},a_0,\ldots,a_{\beta_1-2}\mid \lambda b_{\beta_2-1},b_0,\ldots,b_{\beta_2-2})\in C.$$

Let $\mathbf{S}_{\beta_1,\beta_2,\lambda} = \mathbb{Z}_p[y]/\langle y^{\beta_1}-1\rangle \times \mathbf{S}[y]/\langle y^{\beta_2}-\lambda\rangle$. Then $\mathbf{S}_{\beta_1,\beta_2,\lambda}$ forms a $\mathbf{S}[y]$-module under usual addition and scalar multiplication defined in (2.1).

Theorem 5.1. *A code C is a $\mathbb{Z}_p\boldsymbol{S}$-additive constacyclic code of length (β_1,β_2) if and only if C is a $\boldsymbol{S}[y]$-submodule of $\boldsymbol{S}_{\beta_1,\beta_2,\lambda}$.*

Proof. The proof is same as that of Theorem 2.2 □

Let $\beta_2 > 2$ be any prime number. Since C and $\mathbf{S}[y]/\langle y^{\beta_2-1}-\lambda\rangle$ are $\mathbf{S}[y]$-submodules of $\mathbf{S}_{\beta_1,\beta_2,\lambda}$, we define a mapping

$$\eta_1 : C \longrightarrow \mathbf{S}[y]/\langle y^{\beta_2-1}-\lambda\rangle,$$

where $\eta_1(f(y) \mid g(y)) = g(y)$. Clearly, η_1 is a module homomorphism whose image is $\mathbf{S}[y]$-submodule of $\mathbf{S}[y]/\langle y^{\beta_2-1}-\lambda\rangle$ and $ker(\eta_1)$ is a submodule of C. Further, $\eta(C)$ can easily be identified an ideal in the ring $\mathbf{S}[y]/\langle y^{\beta_2-1}-\lambda\rangle$ (see for reference [14]). Since n is odd and $\eta_1(C)$ is an ideal in $\mathbf{S}[y]/\langle y^{\beta_2-1}-\lambda\rangle$, $\eta_1(C)$ is an additive λ-constacyclic code over $\mathbf{S}$ of length $\beta_2 - 1$.

Theorem 5.2. *Let*

$$C = \left\langle \begin{array}{c} (f_1(y),0),(f_2(y),g(y)+up_1(y)+vq_1(y)+uvr_1(y)), \\ (f_3(y),uva(y) \end{array} \right\rangle$$

be a $\mathbb{Z}_p\boldsymbol{S}$-additive constacyclic code of length (β_1,β_2-1) and $h_g = \frac{(y^{\beta_2-1}-\lambda)}{g}$, $h_1 = \gcd(h_gp_1, h_gq_1, h_gr_1, (y^{\beta_2-1}-\lambda))$, $h_2 = \frac{(y^{\beta_2-1}-\lambda)}{h_1}$. If

$$\begin{aligned}
S_1 &= \bigcup_{i=0}^{\beta_1-deg(f_1)-1} \{y^i \cdot (f_1(y),0)\};\\
S_2 &= \bigcup_{i=0}^{\beta_2-deg(g)-2} \{y^i \cdot (f_2, g(y)+up_1(y)+vq_1(y)+uvr_1(y))\};\\
S_3 &= \bigcup_{i=0}^{\beta_2-deg(h_1)-2} \{y^i \cdot (h_gf_2, uh_gp_1(y)+vh_gq_1(y)+uvh_gr_1(y))\};\\
S_4 &= \bigcup_{i=0}^{deg(g)-deg(a)-1} \{y^i \cdot (f_3(y),uva(y)\},
\end{aligned}$$

then $S = S_1 \cup S_2 \cup S_3 \cup S_4$ is a minimal generating set for the code C and

$$\mid C \mid = p^{\beta_1-deg(f_1)}p^{7(\beta_2-1)-3deg(g)-3deg(h_1)-deg(a))}.$$

Proof. Proof is directly followed by Theorem 3.4. □

6 Examples

Example 6.1. *Let C be a $\mathbb{Z}_3\mathbb{Z}_3[u,v]$-additive cyclic code of length $(6,6)$. Then C is $\mathbb{Z}_3[u,v]$-submodule of $\boldsymbol{S}_{6,6} = \mathbb{Z}_3[y]/\langle y^6-1\rangle \times \boldsymbol{S}[y]/\langle y^6-1\rangle$ generated by $\langle (f_1(y),0),(f_2(y),g(y)+up_1(y)+vq_1(y)+uvr_1(y)),(f_3(y),ua_1(y)+vq_2(y)+uvr_2(y)),(f_4(y),va_2(y)+uvr_3(y)),(f_5(y),uva_3(y))\rangle$ as in Theorem 3.4. Let us consider $f_1(y)=y^4+2y^3+y+2$, $f_2(y)=y^2+2y+1$, $f_3(y)=y+1$, $f_4(y)=y+2$, $f_5(y)=y+2$, $g(y)=y^4+y^3+2y+2$, $a_1(y)=(y+2)^2$, $a_2(y)=(y+2)$, $a_3(y)=1$. Then $h_g=(y+1)^2$, $h_1=(y+1)^2$, $h_2=(y+2)^3(y+1)$, $h_{a_1}=(y+1)^3(y+2)$, $m_1=(y+1)^3(y+2)$, $m_2=(y+2)^2$, $h_{a_2}=(y+2)^2(y+1)^3$, $s_1=(y+2)^2(y+1)^3$, $s_2=(y+2)$, If*

$$\begin{aligned}
S_1 &= \bigcup_{i=0}^{1}\{y^i\cdot(f_1(y),0)\}; \quad S_2=\bigcup_{i=0}^{1}\{y^i\cdot(f_2(y),g(y)+uv)\};\\
S_3 &= \bigcup_{i=0}^{3}\{y^i\cdot(h_gf_2,uvh_g)\}; \quad S_4=\bigcup_{i=0}^{1}\{y^i\cdot(f_3(y),ua_1(y)+v)\};\\
S_5 &= \bigcup_{i=0}^{1}\{y^i\cdot(h_{a_1}f_3(y),vh_{a_1}\}; \quad S_6=\{(f_4(y),va_2(y)+2uv)\};\\
S_7 &= \{(h_{a_2}f_4(y),2uvh_{a_2})\}; \quad S_8=\{(f_5(y),uva_3(y))\},
\end{aligned}$$

then $S=S_1\cup S_2\cup S_3\cup S_4\cup S_5\cup S_6\cup S_7\cup S_8$ is a minimal generating set for the code C and $\mid C\mid = 3^{15}$

Example 6.2. *Let C be a $\mathbb{Z}_5\mathbb{Z}_5[u,v]$-additive cyclic code of length $(8,8)$. Then C is $\mathbb{Z}_5[u,v]$-submodule of $\boldsymbol{S}_{8,8} = \mathbb{Z}_5[y]/\langle y^8-1\rangle \times \boldsymbol{S}[y]/\langle y^8-1\rangle$ generated by $\langle (f_1(y),0),(f_2(y),g(y)+up_1(y)+vq_1(y)+uvr_1(y)),(f_3(y),uva(y))\rangle$ as in Corollary 3.3. Let us consider $f_1(y)=y^5+y^4+3y^3+2y+2$, $f_2(y)=y^3+y^2+2y+1$, $f_3(y)=y^2+1$, $g(y)=y^5+3y^4+y+3$, $a(y)=y^2+2$. Then $h_g=y^3+3y^2+4y+3$, $h_1=h_g$, $h_2=g(y)$. If*

$$\begin{aligned}
S_1 &= \bigcup_{i=0}^{2}\{y^i\cdot(f_1(y),0)\}; \quad S_2=\bigcup_{i=0}^{2}\{y^i\cdot(f_2,g(y)+u(1+v)\};\\
S_3 &= \bigcup_{i=0}^{4}\{y^i\cdot(h_gf_2,uh_g+uvh_g))\}; \quad S_4=\bigcup_{i=0}^{2}\{y^i\cdot(f_3(y),uva(y)\},
\end{aligned}$$

then $S=S_1\cup S_2\cup S_3\cup S_4$ is a minimal generating set for the code C and $\mid C\mid = 5^{14}$.

TABLE-1

Optimal and near-optimal codes from $\mathbb{Z}_p\mathbf{S}$-additive cyclic codes.

p	(β_1, β_2)	Generators	$[n,k,d]$
3	(4,4)	$f_1(y) = y^4 - 1,\ f_2(y) = y^3 + 2y^2 + y + 1 = f_3(y),$ $g(y) = y^2 + 1,\ a(y) = 1,\ p_1 = q_1 = r_1 = 1$	$[20, 10, 8]$
3	(5,4)	$f_1(y) = y^5 - 1,\ f_2(y) = y^4 + y^3 + y^2 + y + 1 = f_3(y),$ $g_1(y) = y^2 + 1,\ a(y) = 1,\ p_1 = q_1 = r_1 = 1$	$[21, 10, 9]$
5	(4,4)	$f_1(y) = y^4 - 1,\ f_2(y) = y^3 + y^2 + y + 1,$ $g(y) = y^2 + 3y + 2,\ p_1 = 2 = q_1,\ r_1 = 1$	$[20, 8, 10]$
5	(5,2)	$f_1(y) = y^5 - 1,\ f_2(y) = y^4 + y^3 + y^2 + y + 1,$ $g(y) = y + 1,\ p_1 = r_1 = 1,\ q_1 = 0$	$[13, 4, 9]$
5	(5,4)	$f_1(y) = y^5 - 1,\ f_2(y) = y^4 + y^3 + y^2 + y + 1$ $g(y) = y^2 + 3y + 2,\ p_1 = 2 = q_1,\ r_1 = 1$	$[21, 8, 11]$
5	(7,4)	$f_1(y) = y^7 - 1,\ g(y) = y^2 + 3y + 2,$ $f_2(y) = y^6 + y^5 + y^4 + y^3 + y^2 + y + 1$ $p_1 = 2 = q_1,\ r_1 = 1$	$[23, 8, 13]$
5	(4,6)	$f_1(y) = y^4 - 1,\ f_2(y) = f_3(y) = f_4(y) = 0,$ $f_5(y) = y^3 + y^2 + y + 1,$ $g(y) = y^6 - 1 = a_1(y) = a_2(y)$ $a_3(y) = y^3 + 3y^2 + 2y + 4$	$[28, 4, 20]$
5	(5,6)	$f_1(y) = y^5 - 1,\ f_2(y) = f_3(y) = f_4(y) = 0,$ $f_5(y) = y^4 + y^3 + y^2 + y + 1,$ $g(y) = y^6 - 1 = a_1(y) = a_2(y)$ $a_3(y) = y^3 + 3y^2 + 2y + 4$	$[29, 4, 21]$
7	(6,6)	$f_1(y) = y^6 - 1,\ f_2(y) = f_3(y) = f_4(y) = 0,$ $f_5(y) = y^5 + y^4 + y^3 + y^2 + y + 1,$ $g(y) = y^6 - 1 = a_1(y) = a_2(y)$ $a_3(y) = y^4 + 4y^3 + 6y^2 + 5y + 2$	$[30, 2, 26]$
7	(5,6)	$f_1(y) = y^5 - 1,\ f_2(y) = f_3(y) = f_4(y) = 0,$ $f_5(y) = y^4 + y^3 + y^2 + y + 1,$ $g(y) = y^6 - 1 = a_1(y) = a_2(y)$ $a_3(y) = y^4 + 4y^3 + 6y^2 + 5y + 2$	$[29, 2, 25]$
7	(5,8)	$f_1(y) = y^5 - 1,\ f_2(y) = f_3(y) = f_4(y) = 0,$ $f_5(y) = y^4 + y^3 + y^2 + y + 1,$ $g(y) = y^8 - 1 = a_1(y) = a_2(y)$ $a_3(y) = y^5 + 2y^4 + 6y^3 + y^2 + 5y + 6$	$[37, 3, 29]$
7	(6,8)	$f_1(y) = y^6 - 1,\ f_2(y) = f_3(y) = f_4(y) = 0,$ $f_5(y) = y^5 + y^4 + y^3 + y^2 + y + 1,$ $g(y) = y^8 - 1 = a_1(y) = a_2(y)$ $a_3(y) = y^5 + 2y^4 + 6y^3 + y^2 + 5y + 6$	$[38, 3, 30]$

TABLE-2

The list of MDSS codes.

p	(β_1, β_2)	Generators	[n, k, d]
3	(3,3)	$f_1(y) = y-1,\ f_2(y) = f_3(y) = g(y) = 1 = a(y)$	[15, 8, 2]
3	(4,4)	$f_1(y) = y-1,\ f_2(y) = f_3(y) = g(y) = 1 = a(y)$	[20, 11, 2]
3	(3,4)	$f_1(y) = y-1,\ f_2(y) = f_3(y) = g(y) = 1 = a(y)$	[19, 10, 2]
5	(4,3)	$f_1(y) = y-1,\ f_2(y) = f_3(y) = g(y) = 1 = a(y)$	[16, 9, 2]
5	(4,5)	$f_1(y) = y-1,\ f_2(y) = f_3(y) = g(y) = 1 = a(y)$	[24, 13, 2]
5	(4,7)	$f_1(y) = y-1,\ f_2(y) = f_3(y) = g(y) = 1 = a(y)$	[32, 17, 2]

7 CONCLUSION

In the present article, we describe the structure of semi local ring $\mathbf{S} = \mathbb{Z}_p + u\mathbb{Z}_p + v\mathbb{Z}_p + uv\mathbb{Z}_p$, where $u^2 = v^2 = 0,\ uv = vu$ with prime characteristic p and characterization of $\mathbb{Z}_p\mathbb{Z}_p[u,v]$-additive cyclic codes and constacyclic codes have been given. The algebraic structure of $\mathbb{Z}_p\mathbf{S}$ have also been studied. We also obtain optimal $\mathbb{Z}_p\mathbf{S}$-additive cyclic codes that have a number of advantages over linear codes, including the fact that they are more efficient. Finally, we obtain the maximum distance separable with respect to singleton bound(MDSS) codes. In future work, it will be an interesting problem to generalize this over $\mathbb{Z}_p\mathbb{Z}_p[u_1, \ldots, u_k]$, where $u_i^2 = 0,\ u_iu_j = u_ju_i$ for all $i, j \in \{1, 2, \ldots, k\}$.

Conflict of interest: The authors have no conflict of interest to declare that are relevant to the content of this article.

Data Availability Statement: This manuscript has no associated data set.

Acknowledgment The authors are thankful to the anonymous referees for his/her fruitful comments and suggestions.

Author Contributions: Supervision, M. Ashraf; Conceptualization, M. Ashraf, M. Asim and G. Mohammad; Methodology, M. Ashraf, M. Asim, G. Mohammad and R. Washiq ; Software, M. Asim; Writing-original draft, M. Asim and R. Washiq ; Writing-review & editing, M. Ashraf, G. Mohammad and Validation, M. Ashraf; Formal analysis, M. Ashraf, M. Asim and G. Mohammad; All authors have read and agreed to the published version of the manuscript.

References

[1] Abualrub T and Siap I, Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$, *Des. Codes Cryptogr.* **42**(2007) 273-287

[2] Abualrub T and Siap I, Reversible cyclic codes over $\mathbb{Z}_4$, *Australas. J. Comb.* **38**(2007) 195-205.

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

[4] Asamov T and Aydin N, Table of $\mathbb{Z}_4$ codes, Online available at http://www.asamov.com/$\mathbb{Z}_4$ Codes Accessed on 2019-12-12

[5] Ashraf M and Mohammad G, Skew cyclic codes over $F_q + uF_q + vF_q$, *Asian-Eur. J. Math.* **11**(5)(2018)

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

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

[8] I. Aydogdu, T. Abualrub and I. Siap, On the structure of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear and cyclic codes, *Finite Fields Appl.*, **48**(2017), 241-260.

[9] Aydogdu I and Siap I, The structure of $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes: Bounds on the minimum distance, *Appl. Math. Inf. Sci.* **7**(2013) 2271-2278

[10] Aydogdu I and Siap I, On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes, *Linear Multilinear Algebra* **63**(2015) 2089-2102

[11] Bierbrauer J, The theory of cyclic codes and a generalization to additive codes, *Des. Codes Cryptogr* **25**(2002) 189-206

[12] Borges J, Fernandez-Cordoba C, Pujol J and Rifa J, $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes, *Adv. Math. Commun.* **12**(2018) 169-179

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

[14] Calderbank A R and Sloane N J A, Modular and p-adic cyclic codes, *Des. Codes Cryptogrph.* **6**(1995) 21-35

[15] Delsarte P, An Algebraic Approach to Association Schemes of Coding Theory, *Philips Res. Rep., Supplement* 1973

[16] Delsarte P and Levenshtein V I, Association schemes and coding theory, *IEEE Trans. Inform. Theory* **44**(1998) 2477-2504

[17] Diao L and Gao J, $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes, *Int. J. Comput. Math.* **5**(1)(2018) 1-17

[18] Islam H and Prakash O, On $\mathbb{Z}_p\mathbb{Z}_p[u,v]$-additive cyclic and constacyclic codes, preprint (2019), arXiv:1905.06686v1.

[19] McDonald B R, Finite Rings with Identity (1974) *Marcel Dekker Inc., New York*

[20] MacWilliams F J and Sloane N J A, The Theory of Error-Correcting Codes(1977) *North-Holland, Amsterdam*

[21] Shi M, Wang C, Wu R, Hu Y and Chang Y, One-weight and two-weight $\mathbb{Z}_2\mathbb{Z}_2[u,v]$-additive codes, *Cryptogr. Commun.* **12**(2020) 443-454

[22] Yao T and Zhu S, $\mathbb{Z}_p\mathbb{Z}_{p^s}$ -additive cyclic codes are asymptotically good, *Cryptogr. Commun.* **12**(2020) 253-264

Mohammad Ashraf,
Department of Mathematics,
Aligarh Muslim University,
Aligarh-202002 India
Email: mashraf80@hotmail.com

Mohd Asim,
Department of Mathematics,
Aligarh Muslim University,
Aligarh-202002 India
Email:mohdasim849@gmail.com

Ghulam Mohammad,
Department of Mathematics,
Aligarh Muslim University,
Aligarh-202002 India
Email: mohdghulam202@gmail.com

Washiqur Rehman,
Department of Mathematics,
Aligarh Muslim University,
Aligarh-202002 India
Email: rehmanwasiq@gmail.com