J. Korean Math. Soc. **58** (2021), No. 3, pp. 571–595
https://doi.org/10.4134/JKMS.j190536
pISSN: 0304-9914 / eISSN: 2234-3008

ON $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-CYCLIC CODES AND THEIR WEIGHT ENUMERATORS

Maheshanand Bhaintwal and Soumak Biswas

Abstract. In this paper we study the algebraic structure of $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-cyclic codes, where $u^k = 0$ and p is a prime. A $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-linear code of length $(r+s)$ is an R_k-submodule of $\mathbb{Z}_p^r \times R_k^s$ with respect to a suitable scalar multiplication, where $R_k = \mathbb{Z}_p[u]/\langle u^k\rangle$. Such a code can also be viewed as an R_k-submodule of $\mathbb{Z}_p[x]/\langle x^r-1\rangle \times R_k[x]/\langle x^s-1\rangle$. A new Gray map has been defined on $\mathbb{Z}_p[u]/\langle u^k\rangle$. We have considered two cases for studying the algebraic structure of $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-cyclic codes, and determined the generator polynomials and minimal spanning sets of these codes in both the cases. In the first case, we have considered $(r,p) = 1$ and $(s,p) \neq 1$, and in the second case we consider $(r,p) = 1$ and $(s,p) = 1$. We have established the MacWilliams identity for complete weight enumerators of $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-linear codes. Examples have been given to construct $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-cyclic codes, through which we get codes over $\mathbb{Z}_p$ using the Gray map. Some optimal p-ary codes have been obtained in this way. An example has also been given to illustrate the use of MacWilliams identity.

1. Introduction

Codes over finite rings have attracted the attention of many researchers working in the field of coding theory since 1994 after the remarkable paper by Hammons et al. [8]. Since then there has been extensive work on codes over rings. Most of this work is over commutative rings with identity where the underlying set is a simple alphabet such as $\mathbb{Z}_m$. Recently researchers have taken interest on codes over mixed alphabets such as $\mathbb{Z}_2\mathbb{Z}_4$, $\mathbb{Z}_2\mathbb{Z}_{2^s}$ etc. Some good results on codes over such rings have been obtained and many good codes have been constructed. Borges et al. [5] presented $\mathbb{Z}_2\mathbb{Z}_4$-additive codes as $\mathbb{Z}_4$-submodules (additive groups) of $\mathbb{Z}_2^\alpha\mathbb{Z}_4^\beta$, where α and β are positive integers. Rifà et al. [10] showed that $\mathbb{Z}_2\mathbb{Z}_4$-additive codes can be applied in steganography. Later $\mathbb{Z}_2\mathbb{Z}_4$-additive codes were generalized to $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes in [2]. Generalizing these codes further, Aydogdu and Siap [3] introduced codes over

Received July 30, 2019; Revised August 3, 2020; Accepted February 9, 2021.
2010 *Mathematics Subject Classification.* Primary 94B05, 94B15, 94B60.
Key words and phrases. $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-linear codes, $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-cyclic codes, Gray map, weight enumerators.

$\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$, where p is a prime number. Recently Aydogdu et al. [1] introduced $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes. Working on a slightly more generalized alphabet of this type, Aydogdu et al. [4] studied $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear and cyclic codes. Recently Qian and Cao [9] have studied the algebraic structure of $\mathbb{Z}_p\mathbb{Z}_p[u]$-cyclic codes and their duals. A very important area of coding theory is weight enumerators. Aydogdu et al. [1] have studied Lee weight enumerators of additive codes over $\mathbb{Z}_2\mathbb{Z}_2[u]$ and established the MacWilliams identities for them. Recently Shi et al. [11] have studied the weight enumerators of $\mathbb{Z}_p\mathbb{Z}_{p^k}$-additive codes. But apart from these works, nothing significant has been reported in the literature on weight enumerators and related results on codes over mixed alphabets.

Inspired by the above works and developments, in this paper we consider a more general ring $R_k = \mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle, u^k = 0$, of which the rings like $\mathbb{Z}_2\mathbb{Z}_2[u]$, $\mathbb{Z}_2\mathbb{Z}_2[u^3]$ and $\mathbb{Z}_p\mathbb{Z}_p[u]$, where p is a prime number, are special cases, and study the linear and cyclic codes over this mixed alphabet. We define a scalar multiplication on $\mathbb{Z}_p^r \times R_k^s$, using which a $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-linear code is defined. A new Gray map is introduced. We then study the structure of $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-cyclic codes. A $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-cyclic code can be viewed as an R_k-submodule of $\mathbb{Z}_p[x]/\langle x^r - 1\rangle \times R_k[x]/\langle x^s - 1\rangle$. We consider two cases for studying the structure of $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-cyclic codes. In the first case we consider $(r, p) = 1$ and $(s, p) \neq 1$, and in the second case we consider $(r, p) = 1$ and $(s, p) = 1$. The weight enumerators of $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-linear codes have also been studied. It is well known that the complete weight enumerator of a code gives more information about the code than that is given by the Lee weight enumerator. We have defined the complete weight enumerator for $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-linear codes and obtained the MacWilliams identity for them. An example has been given to illustrate the use of MacWilliams identity. Examples have also been given for the construction of $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-cyclic codes, through which we have obtained some optimal linear codes over $\mathbb{Z}_p$ via the Gray map.

The rest of the paper is organized in the following way. In Section 2 some preliminaries of $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-linear codes are given, and a new Gray map is introduced. In Section 3, the generator polynomials and the minimal spanning sets for $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-cyclic codes of length $(r + s)$ are obtained for both the cases $(r, p) = 1, (s, p) \neq 1$ and $(r, p) = 1, (s, p) = 1$. In Section 4 the complete weight enumerator for $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-linear codes is defined and the MacWilliams identity for these codes is established with respect to the complete weight enumerator.

2. Preliminaries

In this section we introduce $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-linear codes and a Gray map on $\mathbb{Z}_p[u]/\langle u^k\rangle$. Let $R_k = \mathbb{Z}_p[u]/\langle u^k\rangle = \mathbb{Z}_p[u^k] = \mathbb{Z}_p + u\mathbb{Z}_p + u^2\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p$, where $u^k = 0$. The ring R_k is a commutative chain ring with p^k elements and with the unique maximal ideal $\langle u\rangle = uR_k$. The nilpotency index of u is k and the ideals of R_k satisfy the chain condition

$$R_k \supset uR_k \supset u^2R_k \supset \cdots \supset u^kR_k = 0.$$

From now onward, for the ease of notation, we write a $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-code simply a $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-code and a $\mathbb{Z}_p[u]/\langle u^k\rangle$-code simply a $\mathbb{Z}_p[u^k]$-code. A $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-code C of length $(r+s)$ is a non-empty subset of $\mathbb{Z}_p^r \times R_k^s$. The set $\mathbb{Z}_p^r \times R_k^s$ is an additive abelian group but not an R_k-module with respect to the usual multiplication. To make it an R_k-module, we define an auxiliary map $\eta : R_k \to \mathbb{Z}_p$ such that

$$\eta(a_0 + ua_1 + u^2a_2 + \cdots + u^{k-1}a_{k-1}) = a_0. \tag{1}$$

Then for any $d \in R_k$ and $v = (v_0, v_1, \ldots, v_{r-1}, v'_0, v'_1 \ldots, v'_{s-1}) \in \mathbb{Z}_p^r \times R_k^s$, we define

$$d \cdot v = (\eta(d)v_0, \eta(d)v_1, \ldots, \eta(d)v_{r-1}, dv'_0, dv'_1, \ldots, dv'_{s-1}).$$

The set $\mathbb{Z}_p^r \times R_k^s$ is an R_k-module with respect to this multiplication. A $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-linear code of length $(r+s)$ is then defined as an R_k-submodule of $\mathbb{Z}_p^r \times R_k^s$.

Now we define a new Gray map $\phi : R_k \to \mathbb{Z}_p^{p^{k-1}}$ as follows:

$$\begin{array}{rcl} 0 & \mapsto & (000\cdots 00), \\ 1 & \mapsto & (100\cdots 00), \\ u & \mapsto & (110\cdots 00), \\ & & \vdots \\ u^{k-1} & \mapsto & (\underbrace{111\cdots 1}_{k}0\cdots 00), \end{array}$$

and for any $a_0 + a_1u + a_2u^2 + \cdots + a_{k-1}u^{k-1} \in R_k$,

$$\phi(a_0 + a_1u + a_2u^2 + \cdots + a_{k-1}u^{k-1}) \mapsto a_0\phi(1) + a_1\phi(u) + a_2\phi(u^2) + \cdots + a_{k-1}\phi(u^{k-1}).$$

This Gray map is then generalized to $\Phi : \mathbb{Z}_p^r \times R_k^s \to \mathbb{Z}_p^n$, where $n = r + p^{k-1}s$, such that for any $v = (v_0, v_1, \ldots, v_{r-1}) \in \mathbb{Z}_p^r$ and $v' = (v'_0, v'_1, \ldots, v'_{s-1}) \in R_k^s$,

$$\Phi(v, v') = (v_0, v_1, \ldots, v_{r-1}, \phi(v'_0), \phi(v'_1), \ldots, \phi(v'_{s-1})).$$

Thus the Gray image $\Phi(C)$ of a $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-linear code C of length $(r+s)$ is also a linear code of length $n = r + p^{k-1}s$ over $\mathbb{Z}_p$.

3. $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic codes

Cyclic codes over mixed alphabets have attracted the attention of many researchers recently, and several results on them have been obtained [1, 4–7]. The generators of both cyclic codes and their duals over $\mathbb{Z}_2\mathbb{Z}_2[u^3]$ have been studied in [4]. In this section we study the structure of cyclic codes over $\mathbb{Z}_p\mathbb{Z}_p[u^k], u^k = 0$, which is a more generalized alphabet. The authors in [4] have studied cyclic codes of length $(r+s)$ over $\mathbb{Z}_2\mathbb{Z}_2[u^3]$, where r and s both are odd. We consider two cases for studying $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic codes of length $(r+s)$, first the case when $(r,p)=1$ and $(s,p)\neq 1$, and then the case when $(r,p)=1$ and $(s,p)=1$. We follow this pattern throughout the paper.

Definition. A $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-linear code C of length $(r+s)$ is called a cyclic code if

$$(u_0,u_1,\ldots,u_{r-2},u_{r-1}|u'_0,u'_1,\ldots,u'_{s-2},u'_{s-1}) \in C$$

implies that

$$(u_{r-1},u_0,\ldots,u_{r-3},u_{r-2}|u'_{s-1},u'_0,\ldots,u'_{s-3},u'_{s-2}) \in C.$$

Let $\mathbf{u}=(u_0,u_1,\ldots,u_{r-2},u_{r-1}|u'_0,u'_1,\ldots,u'_{s-2},u'_{s-1})$ be a codeword in C and j be an integer. Then the j^{th} shift of $\mathbf{u}$ is denoted by

$$\mathbf{u}^{(j)}=(u_{0-j},u_{1-j},\ldots,u_{r-1-j}|u'_{0-j},u'_{1-j},\ldots,u'_{s-1-j}),$$

where the subscripts in the first r elements are taken modulo r, and the subscripts in the last s elements are taken modulo s. Let C be a $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic code and C_r be the canonical projection of C on its first r coordinates and C_s be the canonical projection of C on its last s coordinates. Since a canonical projection is a linear map, C_r is a $\mathbb{Z}_p$-cyclic code of length r and C_s is an R_k-cyclic code of length s.

Let the image of any vector $\mathbf{u}\in\mathbb{Z}_p^r\times R_k^s$ be denoted by $\mathbf{u}(x)$. Clearly there is a bijective map between $\mathbb{Z}_p^r\times R_k^s$ and $\mathbb{Z}_p[x]/\langle x^r-1\rangle\times R_k[x]/\langle x^s-1\rangle$, given by $\mathbf{u}=(u_0,u_1,\ldots,u_{r-1}|u'_0,u'_1,\ldots,u'_{s-1})\mapsto\mathbf{u}(x)=(u_0+u_1x+\cdots+u_{r-1}x^{r-1}|u'_0+u'_1x+\cdots+u'_{s-1}x^{s-1})$.

Definition. Let $(w(x)|v(x))\in R_{r,s}=\mathbb{Z}_p[x]/\langle x^r-1\rangle\times R_k[x]/\langle x^s-1\rangle$. We define a scalar multiplication

$$\circ: R_k[x]\times R_{r,s}\to R_{r,s}$$

by

$$\beta(x)\circ(w(x)|v(x))=(\eta(\beta(x))w(x)|\beta(x)v(x)),$$

where η is the map defined in (1), and $\eta(\beta(x))=\eta(\beta_0)+\eta(\beta_1)x+\cdots+\eta(\beta_t)x^t$.

Clearly, $R_{r,s}$ is an $R_k[x]$-module with respect to the scalar multiplication $\circ$. Let $\mathbf{u}(x)=(u(x)|u'(x))$ be an element of $R_{r,s}$. Then

$$\begin{aligned}x\circ\mathbf{u}(x)&=x\circ(u(x)|u'(x))\\&=(u_0x+\cdots+u_{r-2}x^{r-1}+u_{r-1}x^r|u'_0x+\cdots+u'_{s-2}x^{s-1}+u'_{s-1}x^s)\\&=(u_{r-1}+u_0x+\cdots+u_{r-2}x^{r-1}|u'_{s-1}+u'_0x+\cdots+u'_{s-2}x^{s-1}).\end{aligned}$$

Hence $x\circ\mathbf{u}(x)$ represents the image of the vector $\mathbf{u}^{(1)}$. Thus, the multiplication of $\mathbf{u}(x)$ by x in $R_{r,s}$ corresponds to a cyclic shift of $\mathbf{u}(x)$. In general $x^i\circ\mathbf{u}(x)$ represents the i^{th} shift $\mathbf{u}^{(i)}$ of $\mathbf{u}$. Then it follows that a $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic code of length $(r+s)$ is an $R_k[x]$-submodule of $R_{r,s}$.

3.1. Generator polynomials of $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic codes

The structure of cyclic codes is mainly determined by their generator polynomials. In this subsection, we study submodules of $R_{r,s}$ and determine their generators.

In the next theorem, we present the structure of $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic codes of length $(r+s)$ when $(r,p)=1$ and $(s,p)\neq 1$. For any subset S of $R_{r,s}$, we use the notation $\langle S\rangle$ for the submodule of $R_{r,s}$ generated by S.

Theorem 3.1. *Let C be a cyclic code of length $(r+s)$ over $\mathbb{Z}_p\mathbb{Z}_p[u^k]$, where $(r,p)=1$, $(s,p)\neq 1$. Then*

(1) $C=\langle (f(x)|0),(l(x)|g(x)+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x))\rangle$, *where* $f(x),l(x),p_i(x)\in\mathbb{Z}_p[x]$ *with* $f(x)|(x^r-1)$, $g(x)|(x^s-1) \pmod p$, $(g(x)+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x))|(x^s-1)$, *and* $\deg p_i(x)<\deg p_{i-1}(x)$, $1\leq i\leq k-1$. *Or*

(2) $C=\langle (f(x)|0),(l_0(x)|g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x)),(l_1(x)|ua_1(x)+u^2q_1(x)+\cdots+u^{k-1}q_{k-2}(x)),\ldots,(l_{k-2}(x)|u^{k-2}a_{k-2}(x)+u^{k-1}t_1(x)),(l_{k-1}(x)|u^{k-1}a_{k-1}(x))\rangle$, *where* $l_0(x),l_1(x),\ldots,l_{k-1}(x)\in\mathbb{Z}_p[x]$ *and* $a_{k-1}(x)|\cdots|a_1(x)|g(x)|(x^s-1)$, $a_1(x)|p_1(x)\left(\frac{x^s-1}{g(x)}\right)$, $a_2(x)|q_1(x)\left(\frac{x^s-1}{a_1(x)}\right)$, $a_2(x)\,|\,p_2(x)\left(\frac{x^s-1}{g(x)}\right)\left(\frac{x^s-1}{a_1(x)}\right)$, $\ldots$, $a_{k-1}(x)\,|\,t_1(x)\left(\frac{x^s-1}{a_{k-2}(x)}\right)$, $\ldots$, $a_{k-1}(x)\,|\, p_{k-1}(x)\left(\frac{x^s-1}{g(x)}\right)\cdots\left(\frac{x^s-1}{a_{k-2}(x)}\right)$ *with* $\deg p_{k-1}(x)<\deg a_{k-1}(x),\ldots,\deg t_1(x)<\deg a_{k-1}(x)$, $\ldots$, $\deg p_1(x)<\deg a_1(x)$.

Proof. Let $\pi_r: C\to\frac{\mathbb{Z}_p[x]}{\langle x^r-1\rangle}$ and $\pi_s: C\to\frac{R_k[x]}{\langle x^s-1\rangle}$ be the projections $(c_1|c_2)\mapsto c_1$ and $(c_1|c_2)\mapsto c_2$ of C on its first r coordinates and the last s coordinates, respectively. Then $C_r=\pi_r(C)$ is a cyclic code of length r over $\mathbb{Z}_p$ and $C_s=\pi_s(C)$ is a cyclic code of length s over R_k. C_r is therefore generated by a monic polynomial $f(x)\in\mathbb{Z}_p[x]$ such that $f(x)\mid(x^r-1)$. Also, from [12, Theorem 3.3],

$$C_s=\langle g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x)\rangle, \tag{2}$$

such that $g(x)\mid(x^s-1)\bmod p$ and $(g(x)+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x))\mid(x^s-1)$ in $\mathbb{Z}_p[u^k]$, or

$$\begin{aligned} C_s=\langle g(x)&+up_1(x)+\cdots+u^{k-1}p_{k-1}(x),ua_1(x)+u^2q_1(x)+\cdots\\ &+u^{k-1}q_{k-2}(x),\ldots,u^{k-2}a_{k-2}(x)+u^{k-1}t_1(x),u^{k-1}a_{k-1}(x)\rangle, \end{aligned}\tag{3}$$

such that $a_{k-1}(x)|\cdots|a_1(x)|g(x)|(x^s-1)$, $a_1(x)|p_1(x)\left(\frac{x^s-1}{g(x)}\right)$, $a_2(x)|q_1(x)\left(\frac{x^s-1}{a_1(x)}\right)$, $a_2(x)\,|\,p_2(x)\left(\frac{x^s-1}{g(x)}\right)\left(\frac{x^s-1}{a_1(x)}\right),\ldots,a_{k-1}(x)\,|\,t_1(x)\left(\frac{x^s-1}{a_{k-2}(x)}\right),\ldots,a_{k-1}(x)|p_{k-1}(x)$ $\left(\frac{x^s-1}{g(x)}\right)\cdots\left(\frac{x^s-1}{a_{k-2}(x)}\right)$ with $\deg p_{k-1}(x)<\deg a_{k-1}(x),\ldots,\deg t_1(x)<\deg a_{k-1}(x)$, $\ldots,\deg p_1(x)<\deg a_1(x)$. (Here we have written the conditions for divisions by $a_i(x)$ in a slightly different manner.)

Now π_s is a homomorphism with

$$\ker \pi_s = \{(c_1 \mid c_2) \in C \mid c_2 = 0\} = \{(c_1 \mid 0) \mid c_1 \in C_r\} = \langle (f(x)|0)\rangle.$$

Also, $C/\ker(\pi_s) \cong C_s$. Now suppose $C_s = \langle g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)\rangle$, as given in (2). Then

$$C/\ker(\pi_s) \cong C_s = \langle g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)\rangle.$$

Then there exists $l(x) \in \mathbb{Z}_p[x]/\langle x^r - 1\rangle$ such that

$$(l(x)|g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)) \in C,$$

and any element of C is generated by

$$\{(f(x) \mid 0), (l(x) \mid g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x))\}.$$

Therefore,

$$C = \langle (f(x) \mid 0), (l(x) \mid g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x))\rangle.$$

Now suppose C_s is given by the equation (3). Then using similar arguments as above, it follows that there exist polynomials $l_0(x), l_1(x), \ldots, l_{k-1}(x) \in \mathbb{Z}_p[x]$ such that

$$\begin{aligned} C = \langle &(f(x)|0), (l_0(x)|g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)), (l_1(x)|ua_1(x) \\ &+ u^2q_1(x) + \cdots + u^{k-1}q_{k-2}(x)), \ldots, (l_{k-2}(x)|u^{k-2}a_{k-2}(x) + u^{k-1}t_1(x)), \\ &(l_{k-1}(x)|u^{k-1}a_{k-1}(x))\rangle. \end{aligned}$$

□

Theorem 3.2. *Let C be a $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic code of length $(r+s)$ where $(r,p) = 1$, $(s,p) = 1$. Then*

(1) $C = \langle (f(x)|0), (l(x)|g(x) + ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x))\rangle$, *where $f(x)$, $l(x)$, $g(x)$, $a_1(x), \ldots, a_{k-1}(x) \in \mathbb{Z}_p[x]$ with $f(x)|(x^r - 1)$ and $a_{k-1}(x)|a_{k-2}(x)|\cdots|a_2(x)|a_1(x)|g(x)|(x^s - 1)$. Or*

(2) $C = \langle (f(x)|0), (l_0(x)|g(x)), (l_1(x)|ua_1(x)), (l_2(x)|u^2a_2(x)), \ldots, (l_{k-1}(x)| u^{k-1}a_{k-1}(x))\rangle$, *where $f(x)$, $l_0(x)$, $l_1(x), \ldots, l_{k-1}(x)$, $g(x)$, $a_1(x), \ldots, a_{k-1}(x) \in \mathbb{Z}_p[x]$ and $f(x)|(x^r-1)$, $a_{k-1}(x)|a_{k-2}(x)|\cdots|a_1(x)|g(x)|(x^s-1)$.*

Proof. (1) Let $\pi_r : C \to \frac{\mathbb{Z}_p[x]}{\langle x^r-1\rangle}$ and $\pi_s : C \to \frac{R_k[x]}{\langle x^s-1\rangle}$ be the projections $(c_1|c_2) \mapsto c_1$ and $(c_1|c_2) \mapsto c_2$, of C on its first r coordinates and the last s coordinates, respectively. Then $C_r = \pi_r(C)$ is a cyclic code of length r over $\mathbb{Z}_p$ and $C_s = \pi_s(C)$ is a cyclic code of length s over R_k. Then there exists a monic polynomial $f(x) \in \mathbb{Z}_p[x]$ such that $f(x) \mid (x^r - 1)$ and C_r is generated by $f(x)$. Also since $(s,p) = 1$, it follows from the theory of cyclic codes over $\mathbb{Z}_p[u]/\langle u^k\rangle$ [12, Theorem 3.4], that $\pi_s(C) = \langle g(x) + ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x)\rangle$ with $g(x), a_1(x), \ldots, a_{k-1}(x) \in R_k[x]$ and $a_{k-1}(x)|a_{k-2}(x)|\cdots|a_1(x)|g(x)|(x^s-1)$. Now as shown in Theorem 3.1, π_s is a homomorphism with $\ker \pi_s = \langle (f(x) \mid 0)\rangle$, and

$$\pi_s(C) = C_s = \langle g(x) + ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x)\rangle.$$

Then there exists a polynomial $l(x) \in \mathbb{Z}_p[x]$ such that

$$C = \langle (f(x)|0), (l(x)|g(x) + ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x))\rangle.$$

(2) Since $(s,p) = 1$, from [12, Theorem 3.4],

$$\begin{aligned}\pi_s(C) = C_s &= \langle g(x) + ua_1(x) + \cdots + u^{k-1}a_{k-1}(x)\rangle \\ &= \langle g(x), ua_1(x), \ldots, u^{k-1}a_{k-1}(x)\rangle.\end{aligned}$$

This implies that there exist polynomials $l_0(x), l_1(x), \ldots, l_{k-1}(x) \in \mathbb{Z}_p[x]$ such that

$$\begin{aligned}C = \langle &(f(x)|0), (l_0(x)|g(x)), (l_1(x)|ua_1(x)), (l_2(x)|u^2a_2(x)), \ldots, \\ &(l_{k-1}(x)|u^{k-1}a_{k-1}(x))\rangle.\end{aligned}$$

□

Proposition 3.3. *Let* $C = \langle (f(x)|0), (l(x)|g(x) + ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x))\rangle$ *be a* $\mathbb{Z}_p\mathbb{Z}_p[u^k]$*-cyclic code of length* $(r+s)$*. Then we can assume that* $\deg l(x) < \deg f(x)$*.*

Proof. By the division algorithm, there exist $q(x), r(x) \in \mathbb{Z}_p[x]$ such that $l(x) = q(x)f(x) + r(x)$, where $\deg r(x) < \deg f(x)$ or $r(x) = 0$. Let

$$C' = \langle (f(x)|0), (r(x)|g(x) + ua_1(x) + \cdots + u^{k-1}a_{k-1}(x))\rangle.$$

We claim that $C' = C$. Since $q(x)(f(x)|0) + (r(x)|g(x) + ua_1(x) + \cdots + u^{k-1}a_{k-1}(x)) = (l(x)|g(x)+ua_1(x)+\cdots+u^{k-1}a_{k-1}(x))$, we have $C \subseteq C'$. Similarly, $-q(x)(f(x)|0) + (l(x)|g(x) + ua_1(x) + \cdots + u^{k-1}a_{k-1}(x)) = (r(x)|g(x) + ua_1(x) + \cdots + u^{k-1}a_{k-1}(x))$ implies that $C' \subseteq C$. Hence $C' = C$. Since $\deg r(x) < \deg f(x)$, the result follows. □

Remark 3.4. The above result holds in both the cases, $(r,p) = 1, (s,p) \neq 1$ and $(r,p) = 1, (s,p) = 1$.

Now we present the generator polynomials of a $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-cyclic code C of length $(r+s)$ in terms of pairwise coprime monic polynomials when $(r,p) = 1, (s,p) = 1$. We use the notation $\hat{a}(x) = \frac{x^s-1}{a(x)}$ for any divisor $a(x)$ of $x^s - 1$. Similarly, we write $\hat{b}(x) = \frac{x^r-1}{b(x)}$ for any divisor of $x^r - 1$.

Theorem 3.5. *Let C be a* $\mathbb{Z}_p\mathbb{Z}_p[u^k]$*-cyclic code of length* $(r+s)$ *with* $(r,p) = 1, (s,p) = 1$*. Then there exists a unique family of pairwise coprime monic polynomials* $F_0, F_1, \ldots, F_k$ *in* $\mathbb{Z}_p[x]$ *such that* $F_0F_1\cdots F_k = x^s - 1$*, and*

$$C = \langle (f(x)|0), (l(x)|\hat{F}_1 + u\hat{F}_2 + \cdots + u^{k-1}\hat{F}_k)\rangle,$$

where $f(x), l(x) \in \mathbb{Z}_p[x]$*,* $f(x)|(x^r - 1)$*, and* $\hat{F}_i = (x^s - 1)/F_i$*,* $0 \le i \le k$*.*

Proof. Let π_s be the projection $(c_1|c_2) \mapsto c_2$ of C on its last s coordinates. Then from Theorem 3.2(2), we have

$$C_s = \langle g(x), ua_1(x), \ldots, u^{k-1}a_{k-1}(x)\rangle,$$

where $g(x), a_1(x), \ldots, a_{k-1}(x) \in \mathbb{Z}_p[x]$ are monic polynomials such that $a_{k-1}(x) | a_{k-2}(x) | \cdots | a_1(x) | g(x) | (x^s - 1)$. We use the substitutions $F_0 = a_{k-1}(x)$, $F_1 = (x^s - 1)/g(x)$, $a_0(x) = g(x)$ and $F_i = a_{i-2}(x)/a_{i-1}(x)$ for $2 \le i \le k$. Then clearly $F_0, F_1, \ldots, F_k$ are monic polynomials in $\mathbb{Z}_p[x]$. We show that they are pairwise coprime. Since $(s,p) = 1$, $x^s - 1$ factorizes into distinct monic irreducible polynomials over $\mathbb{Z}_p$, and as $a_0(x), a_1(x), \ldots, a_{k-1}$ are divisors of $x^s - 1$, none of them has any repeated factor. Then clearly $F_0 = a_{k-1}(x)$ and $F_1 = \frac{x^s-1}{g(x)}$ are coprime as $a_{k-1}(x)|g(x)$. Similarly, F_0 and $F_i = \frac{a_{i-2}(x)}{a_{i-1}(x)}$, for any $2 \le i \le k$, are coprime as $a_{k-1}(x)|a_{i-1}(x)$ for all such i. Now F_1 and F_i, for any $2 \le i \le k$, are coprime as $a_{i-2}(x)|g(x)$ for all $2 \le i \le k$, and hence $\frac{a_{i-2}(x)}{a_{i-1}(x)}|g(x)$, i.e., $F_i \mid g(x)$. Now consider any $F_i = \frac{a_{i-2}(x)}{a_{i-1}(x)}$ and $F_j = \frac{a_{j-2}(x)}{a_{j-1}(x)}$, $2 \le i < j \le k-1$. Since $i < j$, $a_{j-2}(x)|a_{i-1}(x)$, and hence $\frac{a_{j-2}(x)}{a_{j-1}(x)}|a_{i-1}(x)$. Therefore $F_i = \frac{a_{i-2}(x)}{a_{i-1}(x)}$ and $F_j = \frac{a_{j-2}(x)}{a_{j-1}(x)}$ are coprime. Thus F_i's are pairwise coprime.

Now writing $a_i(x)$ in terms of F_i, we get

$$\begin{aligned}
C_s &= \langle g(x), ua_1(x), u^2a_2(x), \ldots, u^{k-1}a_{k-1}(x)\rangle \\
&= \left\langle \frac{(x^s-1)}{F_1}, \frac{u(x^s-1)}{F_1F_2}, \frac{u^2(x^s-1)}{F_1F_2F_3}, \ldots, \frac{u^{k-1}(x^s-1)}{F_1F_2\cdots F_k} \right\rangle \\
&= \langle F_0F_2\cdots F_k, uF_0F_3\cdots F_k, u^2F_0F_4\cdots F_k, \ldots, u^{k-1}F_0\rangle.
\end{aligned}$$

We express these generators of C_s now in terms of $\hat{F}_i$. We have $g(x) = \hat{F}_1 = F_0F_2\cdots F_k \in C$. Since F_1, F_2 are coprime polynomials in $\mathbb{Z}_p[x]$, there exist polynomials $p_0, q_0 \in \mathbb{Z}_p[x]$ such that $p_0F_1 + q_0F_2 = 1$. Then we have

$$\begin{aligned}
a_1(x) &= F_0F_3\cdots F_k \\
&= (p_0F_1 + q_0F_2)F_0F_3\cdots F_k \\
&= p_0F_0F_1F_3\cdots F_k + q_0F_0F_2F_3\cdots F_k \\
&= p_0\hat{F}_2 + q_0\hat{F}_1.
\end{aligned}$$

This implies that $ua_1(x) = u(p_0\hat{F}_2 + q_0\hat{F}_1)$. Now since F_1, F_2; F_2, F_3 and F_3, F_1 are pairs of coprime polynomials, there exist polynomials p_1, q_1; p_2, q_2 and p_3, q_3 in $\mathbb{Z}_p[x]$ such that $p_1F_1 + q_1F_2 = 1$, $p_2F_2 + q_2F_3 = 1$ and $p_3F_3 + q_3F_1 = 1$. Noting that $F_0F_1\cdots F_k = x^s - 1 = 0$ in $\frac{R_k[x]}{\langle x^s-1\rangle}$, we have

$$\begin{aligned}
a_2(x) &= F_0F_4\cdots F_k \\
&= (p_1F_1 + q_1F_2)(p_2F_2 + q_2F_3)(p_3F_3 + q_3F_1)F_0F_4\cdots F_k \\
&= p_1p_2q_3F_1(F_0F_1F_2\cdots F_k) + p_1q_2q_3F_1(F_0F_1F_3\cdots F_k) \\
&\quad + p_1q_2p_3F_3(F_0F_1F_3\cdots F_k) + q_1p_2p_3F_2(F_0F_2F_3\cdots F_k) \\
&\quad + q_1q_2p_3F_3(F_0F_2F_3\cdots F_k) + q_1p_2q_3F_2(F_0F_1F_2F_4\cdots F_k) \\
&= p_1p_2q_3F_1\hat{F}_3 + q_1p_2q_3F_2\hat{F}_3 + p_1q_2p_3F_3\hat{F}_2 + p_1q_2q_3F_1\hat{F}_2
\end{aligned}$$

$$+ q_1p_2p_3F_2\hat{F}_1 + q_1q_2p_3F_3\hat{F}_1$$
$$= \hat{F}_3(p_1'F_1 + q_1'F_2) + \hat{F}_2(p_2'F_3 + q_2'F_1) + \hat{F}_1(p_3'F_2 + q_3'F_3),$$

where $p_1' = p_1p_2q_3$, $q_1' = q_1p_2q_3$, $p_2' = p_1q_2p_3$, $q_2' = p_1q_2q_3$, $p_3' = q_1p_2p_3$, and $q_3' = q_1q_2p_3$. Then

$$u^2a_2(x) = u^2(\hat{F}_3(p_1'F_1 + q_1'F_2) + \hat{F}_2(p_2'F_3 + q_2'F_1) + \hat{F}_1(p_3'F_2 + q_3'F_3)).$$

Proceeding in the similar way, we can find the remaining elements $a_3(x), a_4(x), \dots, a_{k-1}(x)$. The last term $u^{k-1}a_{k-1}(x)$ can be written as

$$u^{k-1}a_{k-1}(x)$$
$$= u^{k-1}((p_1''F_1\hat{F}_k + q_1''F_k\hat{F}_1) + \hat{F}_{k-1}(p_{k-1}''F_1 + q_{k-1}''F_k) + \cdots + \hat{F}_2(p_2''F_1 + q_2''F_k)),$$

where $p_1'', \dots, p_{k-1}''$, $q_1'', \dots, q_{k-1}''$ are defined similarly as above. Therefore,

$$\begin{aligned} C_s = \langle \hat{F}_1, &u(p\hat{F}_2 + q\hat{F}_1),\\ &u^2(\hat{F}_3(p_1'F_1 + q_1'F_2) + \hat{F}_2(p_2'F_3 + q_2'F_1) + \hat{F}_1(p_3'F_2 + q_3'F_3)), \dots,\\ &u^{k-1}((p_1''F_1\hat{F}_k + q_1''F_k\hat{F}_1) + \hat{F}_{k-1}(p_{k-1}''F_1 + q_{k-1}''F_k) + \cdots\\ &\quad + \hat{F}_2(p_2''F_1 + q_2''F_k))\rangle. \end{aligned}$$

Now let

$$I = \langle \hat{F}_1, u\hat{F}_2, u^2\hat{F}_3, \dots, u^{k-1}\hat{F}_k\rangle.$$

We show that $C_s = I$. Clearly $C_s \subseteq I$, as every element in C_s is a linear combination of the elements of I.

To prove that $I \subseteq C_s$, we show that the elements $\hat{F}_1, u\hat{F}_2, u^2\hat{F}_3, \dots, u^{k-1}\hat{F}_k$ are all in C_s. Clearly $\hat{F}_1 \in C_s$. Now consider $u\hat{F}_2$. We have $-q_0u\hat{F}_1 + u(p_0\hat{F}_2 + q_0\hat{F}_1) = up_0\hat{F}_2 \in C_s$. Since $p_0F_1 + q_0F_2 = 1$ and $F_2\hat{F}_2 = 0$ in $R_k[x]/\langle x^s - 1\rangle$, we get $p_0F_1\hat{F}_2 = \hat{F}_2$. Hence $up_0\hat{F}_2 \in C_s$ implies that $up_0F_1\hat{F}_2 = u\hat{F}_2 \in C_s$.

Now we show that $u^2\hat{F}_3 \in C_s$. We have

$$u^2[\hat{F}_3(p_1'F_1 + q_1'F_2) + \hat{F}_2(p_2'F_3 + q_2'F_1) + \hat{F}_1(p_3'F_2 + q_3'F_3)] \in C_s,$$

which implies that

$$\begin{aligned} &u^2[\hat{F}_3(p_1p_2q_3F_1 + q_1p_2q_3F_2) + \hat{F}_2(p_1q_2p_3F_3 + p_1q_2q_3F_1)\\ &\quad + \hat{F}_1(q_1p_2p_3F_2 + q_1q_2p_3F_3)]\\ &= u^2[\hat{F}_3p_2q_3(p_1F_1 + q_1F_2) + \hat{F}_2p_1q_2(p_3F_3 + q_3F_1) + \hat{F}_1q_1p_3(p_2F_2 + q_2F_3)]\\ &= u^2[p_2q_3\hat{F}_3 + p_1q_2\hat{F}_2 + q_1p_3\hat{F}_1] \in C_s. \end{aligned}$$

From this we get

$$u^2[p_2q_3\hat{F}_3 + p_1q_2\hat{F}_2 + q_1p_3\hat{F}_1] - up_1q_2(u\hat{F}_2) - u^2q_1p_3\hat{F}_1 = u^2p_2q_3\hat{F}_3 \in C_s. \tag{4}$$

Now using the relations $p_2F_2 + q_2F_3 = 1, p_3F_3 + q_3F_1 = 1$, we get

$$p_2F_2\hat{F}_3 = \hat{F}_3, \tag{5}$$

$$q_3F_1\hat{F}_3 = \hat{F}_3. \tag{6}$$

From (4), (5), we get $u^2p_2q_3\hat{F}_3F_2 = u^2q_3\hat{F}_3 \in C_s$, and hence from (6), $u^2q_3F_1\hat{F}_3 = u^2\hat{F}_3 \in C_s$. We can similarly show that all the terms $u^3\hat{F}_4, u^4\hat{F}_5, \ldots, u^{k-1}\hat{F}_k$ are also in C_s. Hence $C_s = I$, i.e.,

$$C_s = \langle \hat{F}_1, u\hat{F}_2, u^2\hat{F}_3, \ldots, u^{k-1}\hat{F}_k\rangle.$$

Now we show that F_i, $0 \le i \le k$, are unique. Suppose there exist monic pairwise coprime polynomials $G_i \in \mathbb{Z}_p[x]$, $0 \le i \le k$, such that $G_0G_1\cdots G_k = x^s - 1$ and $C_s = \langle \hat{G}_1, u\hat{G}_2, u^2\hat{G}_3, \ldots, u^{k-1}\hat{G}_k\rangle$. Now since $\hat{G}_1 \in \langle \hat{F}_1, u\hat{F}_2, u^2\hat{F}_3, \ldots, u^{k-1}\hat{F}_k\rangle$, and $\hat{G}_1 \in \mathbb{Z}_p[x]$, we have $\hat{G}_1 = a(x)\hat{F}_1$ for some $a(x) \in \mathbb{Z}_p[x]$. Thus $\hat{F}_1 \mid \hat{G}_1$. Using the same argument for $\hat{F}_1$, we see that $\hat{G}_1 \mid \hat{F}_1$. Since $\hat{F}_1$ and $\hat{G}_1$ are monic polynomials, we get $\hat{G}_1 = \hat{F}_1$.

Now $u\hat{G}_2 \in \langle \hat{F}_1, u\hat{F}_2, u^2\hat{F}_3, \ldots, u^{k-1}\hat{F}_k\rangle$ implies that $u\hat{G}_2 = ua_1(x)\hat{F}_1 + b_1(x)(u\hat{F}_2) = u(a_1(x)\hat{F}_1 + b_1(x)\hat{F}_2)$ for some $a_1(x), b_1(x) \in \mathbb{Z}_p[x]$. Then we get

$$\hat{G}_2 = a_1(x)\hat{F}_1 + b_1(x)\hat{F}_2 = a_1(x)\hat{G}_1 + b_1(x)\hat{F}_2. \tag{7}$$

Now since G_1, G_2 are coprime, there exist $a_1'(x), b_1'(x) \in \mathbb{Z}_p[x]$ such that $a_1'(x)G_1 + b_1'(x)G_2 = 1$. From this we get, $a_1'(x)G_1\hat{G}_2 = \hat{G}_2$. Then from (7), we get

$$\hat{G}_2 = a_1'(x)G_1\hat{G}_2 = a_1'(x)b_1(x)G_1\hat{F}_2.$$

This implies that $\hat{F}_2|\hat{G}_2$. Similarly, $\hat{G}_2|\hat{F}_2$, and hence $\hat{G}_2 = \hat{F}_2$.

To show that $\hat{G}_3 = \hat{F}_3$, again we have from $u^2\hat{G}_3 \in \langle \hat{F}_1, u\hat{F}_2, u^2\hat{F}_3, \ldots, u^{k-1}\hat{F}_k\rangle$ that $u^2\hat{G}_3 = u^2a_2(x)\hat{F}_1 + ub_2(x)(u\hat{F}_2) + c_2(x)(u^2\hat{F}_3) = u^2(a_2(x)\hat{F}_1 + b_2(x)\hat{F}_2 + c_2(x)\hat{F}_3)$ for some $a_2(x), b_2(x), c_2(x) \in \mathbb{Z}_p[x]$. Then

$$\hat{G}_3 = a_2(x)\hat{F}_1 + b_2(x)\hat{F}_2 + c_2(x)\hat{F}_3 = a_2(x)\hat{G}_1 + b_2(x)\hat{G}_2 + c_2(x)\hat{F}_3. \tag{8}$$

Now since G_1G_2 and G_3 are coprime, there exist $a_2'(x), b_2'(x) \in \mathbb{Z}_p[x]$ such that $a_2'(x)G_1G_2 + b_2'(x)G_3 = 1$. From this we get, $a_2'(x)G_1G_2\hat{G}_3 = \hat{G}_3$. Then from (8), we get

$$\hat{G}_3 = a_2'(x)G_1G_2\hat{G}_3 = a_2'(x)c_2(x)G_1G_2\hat{F}_3.$$

This implies that $\hat{F}_3|\hat{G}_3$. Similarly, $\hat{G}_3|\hat{F}_3$, and hence $\hat{G}_3 = \hat{F}_3$. Continuing in this way, we can show that $\hat{G}_i = \hat{F}_i$ for all i, $1 \le i \le k$. Consequently, $G_i = F_i$ for all i, $1 \le i \le k$. Now since $F_0F_1\cdots F_k = G_0G_1\cdots G_k$ and F_i, G_i are monic polynomials in $\mathbb{Z}_p[x]$, we also get $G_0 = F_0$. Thus F_i, $0 \le i \le k$, are unique.

Next we show that $C_s = \langle \hat{F}_1 + u\hat{F}_2 + \cdots + u^{k-1}\hat{F}_k\rangle$. Let

$$I_1 = \langle \hat{F}_1 + u\hat{F}_2 + \cdots + u^{k-1}\hat{F}_k\rangle.$$

Clearly $I_1 \subseteq C_s = \langle \hat{F}_1, u\hat{F}_2, \ldots, u^{k-1}\hat{F}_{k-1}\rangle$. Let $F = \hat{F}_1 + u\hat{F}_2 + \cdots + u^{k-1}\hat{F}_k$. Then $FF_2F_3\cdots F_k = \hat{F}_1F_2F_3\cdots F_k \in I_1$. Since F_1 and $F_2F_3\cdots F_k$ are coprime, there exist polynomials $\ell_1, \ell_2 \in \mathbb{Z}_p[x]$ such that $\ell_1F_1 + \ell_2F_2F_3\cdots F_k = 1$. Then

$$\hat{F}_1 = \hat{F}_1(\ell_1F_1 + \ell_2F_2F_3\cdots F_k) = \ell_2\hat{F}_1F_2F_3\cdots F_k \in I_1$$

as $\hat{F}_1F_2F_3\cdots F_k \in I_1$. Next we have

$$FF_3F_4\cdots F_k = \hat{F}_1F_3F_4\cdots F_k + u\hat{F}_2F_3F_4\cdots F_k \in I_1,$$

which implies that $u\hat{F}_2F_3F_4\cdots F_k \in I_1$, as $\hat{F}_1 \in I_1$ and hence $\hat{F}_1F_3F_4\cdots F_k \in I_1$. Since F_2 and $F_3F_4\cdots F_k$ are coprime, there exist $\ell_1', \ell_2' \in \mathbb{Z}_p[x]$ such that $\ell_1'F_2 + \ell_2'F_3F_4\cdots F_k = 1$. Then

$$u\hat{F}_2 = u\hat{F}_2(\ell_1'F_2 + \ell_2'F_3F_4\cdots F_k) = \ell_2'\left(u\hat{F}_2F_3F_4\cdots F_k\right) \in I_1.$$

Proceeding in this way, we can show that $u^2\hat{F}_3, \ldots, u^{k-1}\hat{F}_k$ all are also in I_1. Therefore, $C_s \subseteq I_1$ and hence

$$C_s = I_1 = \langle \hat{F}_1 + u\hat{F}_2 + \cdots + u^{k-1}\hat{F}_k\rangle.$$

Now from Theorem 3.1, $\ker \pi_s = \langle (f(x)|0)\rangle$, where $f(x)$ is a monic divisor of $x^r - 1$. Also, as $\pi_s(C) = C_s = \langle \hat{F}_1 + u\hat{F}_2 + u^2\hat{F}_3 + \cdots + u^{k-1}\hat{F}_k\rangle$, we get

$$C = \langle (f(x)|0), (l(x)|\hat{F}_1 + u\hat{F}_2 + u^2\hat{F}_3 + \cdots + u^{k-1}\hat{F}_k)\rangle,$$

for some polynomial $l(x) \in \mathbb{Z}_p[x]$. □

In the next result we write $f(x)$ and $l(x)$ also, in the generator polynomial of C obtained in Theorem 3.5, in terms of a monic divisor of $x^r - 1$.

Theorem 3.6. *Let $C = \langle (f(x)|0), (l(x)|\hat{F}_1+u\hat{F}_2+\cdots+u^{k-1}\hat{F}_k)\rangle$ be a $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle$-cyclic code of length $(r+s)$ with $(r,p) = 1, (s,p) = 1$ and $f(x)|(x^r-1)$, where $f(x), l(x)$ and F_i, $0 \le i \le k$, are as defined in Theorem 3.5. Then there exist coprime monic polynomials $G_0, G_1 \in \mathbb{Z}_p[x]$ with $G_0G_1 = x^r - 1$ such that*

$$C = \langle (a(x)\hat{G}_1|0), (b(x)\hat{G}_1|\hat{F}_1 + u\hat{F}_2 + \cdots + u^{k-1}\hat{F}_k)\rangle,$$

where $a(x), b(x) \in \mathbb{Z}_p[x]$.

Proof. Let $G_0 = \gcd(f(x), l(x))$. Then we know that $C_r = \langle G_0\rangle$. Let G_1 be the monic polynomial in $\mathbb{Z}_p[x]$ such that $G_0G_1 = x^r - 1$. Now as $G_0|l(x)$ and $G_0|f(x)$, there exist $a(x), b(x) \in \mathbb{Z}_p[x]$ such that $f(x) = a(x)G_0 = a(x)\hat{G}_1$ and $l(x) = b(x)G_0 = b(x)\hat{G}_1$. Therefore,

$$\begin{aligned} C &= \langle (f(x)|0), (l(x)|\hat{F}_1 + u\hat{F}_2 + \cdots + u^{k-1}\hat{F}_k)\rangle \\ &= \langle (a(x)\hat{G}_1|0), (b(x)\hat{G}_1|\hat{F}_1 + u\hat{F}_2 + \cdots + u^{k-1}\hat{F}_k)\rangle. \end{aligned}$$

□

Proposition 3.7. *Let $C = \langle (f(x)|0), (l(x)|g(x) + ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x))\rangle$ be a $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic code of length $(r+s)$ with $(r,p) = 1$ and $(s,p) = 1$. Then $f(x) \mid \left(\frac{x^s-1}{a_{k-1}(x)}\right) l(x)$.*

Proof. We have

$$\left(\frac{x^s-1}{a_{k-1}(x)}\right)\circ(l(x)|g(x)+ua_1(x)+u^2a_2(x)+\cdots+u^{k-1}a_{k-1}(x))=\left(\frac{x^s-1}{a_{k-1}(x)}l(x)|0\right),$$

which is clearly in $\ker \pi_s = \langle (f(x)|0) \rangle$. This implies that $f(x) \mid \left(\frac{x^s-1}{a_{k-1}(x)}\right) l(x)$. $\square$

Corollary 3.8. *Let*

$$C = \langle (f(x)|0), (l(x)|g(x) + ua_1(x) + u^2 a_2(x) + \cdots + u^{k-1} a_{k-1}(x)) \rangle$$

be a $\mathbb{Z}_p\mathbb{Z}_p[u^k]$*-cyclic code of length of length* $(r+s)$ *with* $(r,p) = 1$ *and* $(s,p) = 1$. *Then* $f(x) \mid \left(\frac{x^s-1}{a_{k-1}(x)}\right) \gcd\,(l(x), f(x))$.

Proof. From Proposition 3.7, $f(x) \mid \left(\frac{x^s-1}{a_{k-1}(x)}\right) l(x)$. Also, clearly

$$f(x) \mid \left(\frac{x^s-1}{a_{k-1}(x)}\right) f(x).$$

Therefore, $f(x) \mid \left(\frac{x^s-1}{a_{k-1}(x)}\right) \gcd(l(x), f(x))$. $\square$

3.2. Minimal spanning sets

In this subsection we find the minimal spanning sets for a $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic code, considered as an R_k-module.

Theorem 3.9. *Let* $(r,p) = 1$ *and* $(s,p) \neq 1$. *Let*

$$C = \langle (f|0), (l_0|g + up_1 + \cdots + u^{k-1}p_{k-1}), (l_1|ua_1 + u^2 q_1 + \cdots + u^{k-1} q_{k-2}), \ldots, (l_{k-2}|u^{k-2}a_{k-2} + u^{k-1}t_1), (l_{k-1}|u^{k-1}a_{k-1}) \rangle$$

be a $\mathbb{Z}_2\mathbb{Z}_2[u^k]$*-cyclic code of length* $(r+s)$ *as given in Theorem 3.1*(2). *Let* $h, h_0, h_1, \ldots, h_{k-1}$ *be monic polynomials in* $\mathbb{Z}_p[x]$ *such that* $fh = x^r - 1$ *and* $a_i h_i = x^s - 1$, $0 \leq i \leq k-1$, *where* $a_0 = g$. *Let*

$$S_1 = \bigcup_{i=0}^{\deg h - 1} \{x^i \circ (f|0)\},$$

$$S_2 = \bigcup_{i=0}^{\deg h_0 - 1} \{x^i \circ (l_0|g + up_1 + u^2 p_2 + \cdots + u^{k-1} p_{k-1})\},$$

$$S_3 = \bigcup_{i=0}^{\deg h_1 - 1} \{x^i \circ (l_1|ua_1 + u^2 q_1 + \cdots + u^{k-1} q_{k-2})\},$$

$$\vdots$$

$$S_k = \bigcup_{i=0}^{\deg h_{k-2} - 1} \{x^i \circ (l_{k-2}|u^{k-2}a_{k-2} + u^{k-1}t_1)\},$$

$$S_{k+1} = \bigcup_{i=0}^{\deg h_{k-1} - 1} \{x^i \circ (l_{k-1}|u^{k-1}a_{k-1})\}.$$

Then $S = S_1 \cup S_2 \cup S_3 \cup \cdots \cup S_{k+1}$ *is a minimal spanning set for* C.

Proof. Let c be a codeword in C. Then

$$c = d \circ (f|0) + d_0 \circ (l_0|g + up_1 + \cdots + u^{k-1}p_{k-1}) + \cdots + d_{k-2} \circ (l_{k-2}|u^{k-2}a_{k-2} + u^{k-1}t_1) + d_{k-1} \circ (l_{k-1}|u^{k-1}a_{k-1})$$

for some $d \in \mathbb{Z}_p[x]$ and $d_0, d_1, \ldots, d_{k-1} \in R_k[x]$. If $\deg d < \deg h - 1$, then $d \circ (f|0) \in \mathrm{Span}(S_1)$, otherwise by division algorithm, we have $d = \alpha h + \beta$ for some $\alpha, \beta \in \mathbb{Z}_p[x]$ such that $\deg \beta < \deg h$. Then

$$\begin{aligned} d \circ (f|0) &= (\alpha h + \beta) \circ (f|0) \\ &= \alpha \circ (hf|0) + \beta \circ (f|0) \\ &= \beta \circ (f|0). \end{aligned}$$

Since $\deg \beta < \deg h$, $\beta \circ (f|0) \in \mathrm{Span}(S_1)$, and hence $d \circ (f|0) \in \mathrm{Span}(S_1)$.

Next we show that the remaining terms in c are in $\mathrm{Span}(S)$, for which we follow the reverse order. Thus we first show that

$$d_{k-1} \circ (l_{k-1}|u^{k-1}a_{k-1}) \in \mathrm{Span}(S).$$

If $\deg d_{k-1} < \deg h_{k-1} - 1$, then $d_{k-1} \circ (l_{k-1}|u^{k-1}a_{k-1}) \in \mathrm{Span}(S_{k+1})$. Otherwise, by division algorithm we have $d_{k-1} = \alpha_{k-1}h_{k-1} + \beta_{k-1}$ for some $\alpha_{k-1}, \beta_{k-1} \in R_k[x]$ such that $\deg \beta_{k-1} < \deg h_{k-1}$. Then

$$\begin{aligned} &d_{k-1} \circ (l_{k-1}|u^{k-1}a_{k-1}) \\ &= (\alpha_{k-1}h_{k-1} + \beta_{k-1}) \circ (l_{k-1}|u^{k-1}a_{k-1}) \\ &= \alpha_{k-1} \circ (h_{k-1}l_{k-1}|u^{k-1}h_{k-1}a_{k-1}) + \beta_{k-1} \circ (l_{k-1}|u^{k-1}a_{k-1}) \\ &= \alpha_{k-1} \circ (h_{k-1}l_{k-1}|0) + \beta_{k-1} \circ (l_{k-1}|u^{k-1}a_{k-1}). \end{aligned}$$

Since $\deg \beta_{k-1} < d_{k-1}$, $\beta_{k-1} \circ (l_{k-1}|u^{k-1}a_{k-1}) \in \mathrm{Span}(S_{k+1})$. So we need only to show that $\alpha_{k-1} \circ (h_{k-1}l_{k-1}|0) \in \mathrm{Span}(S)$. Now $h_{k-1}(l_{k-1} \mid u^{k-1}a_{k-1}) = (h_{k-1}l_{k-1} \mid 0) \in C$. Therefore, $f \mid h_{k-1}l_{k-1}$. Let $h_{k-1}l_{k-1} = \delta_{k-1}f$, $\delta_{k-1} \in \mathbb{Z}_p[x]$. Then we have $\alpha_{k-1} \circ (h_{k-1}l_{k-1}|0) = \alpha_{k-1} \circ (\delta_{k-1}f|0) = \alpha_k\delta_{k-1} \circ (f|0) \in \mathrm{Span}(S_1)$. Thus $d_{k-1} \circ (l_{k-1}|u^{k-1}a_{k-1}) \in \mathrm{Span}(S)$.

Next we show that

$$d_{k-2} \circ (l_{k-2}|u^{k-2}a_{k-2} + u^{k-1}t_1) \in \mathrm{Span}(S).$$

If $\deg d_{k-2} < \deg h_{k-2}$, then $d_{k-2} \circ (l_{k-2}|u^{k-2}a_{k-2} + u^{k-1}t_1) \in \mathrm{Span}(S_k)$. Otherwise, by division algorithm, there exist $\alpha_{k-2}, \beta_{k-2} \in R_k[x]$ such that $d_{k-2} = \alpha_{k-2}h_{k-2} + \beta_{k-2}$ and $\deg \beta_{k-2} < \deg h_{k-2}$. Then

$$\begin{aligned} &d_{k-2} \circ (l_{k-2}|u^{k-2}a_{k-2} + u^{k-1}t_1) \\ &= (\alpha_{k-2}h_{k-2} + \beta_{k-2}) \circ (l_{k-2}|u^{k-2}a_{k-2} + u^{k-1}t_1) \\ &= \alpha_{k-2} \circ (h_{k-2}l_{k-2}|h_{k-2}u^{k-1}t_1) + \beta_{k-2} \circ (l_{k-2}|u^{k-2}a_{k-2} + u^{k-1}t_1). \end{aligned}$$

Since $\deg \beta_{k-2} < \deg h_{k-2}$, $\beta_{k-2} \circ (l_{k-2}|u^{k-2}a_{k-2} + u^{k-1}t_1) \in \mathrm{Span}(S_k)$. So we only need to consider $\alpha_{k-2} \circ (h_{k-2}l_{k-2}|h_{k-2}u^{k-1}t_1)$. We know that $a_{k-1}|(\frac{x^s-1}{a_{k-2}})t_1$, i.e., $a_{k-1} \mid h_{k-2}t_1$. Let $h_{k-2}t_1 = n_{k-1}a_{k-1}$. Now

$$\begin{aligned} &h_{k-2}(l_{k-2}|u^{k-2}a_{k-2} + u^{k-1}t_1) - n_{k-1}(l_{k-1}|u^{k-1}a_{k-1}) \\ &= (h_{k-2}l_{k-2} - n_{k-1}l_{k-1}|0) \in C. \end{aligned}$$

Hence $f(x) \mid (h_{k-2}l_{k-2} - n_{k-1}l_{k-1})$. So there exists $\delta_{k-2} \in \mathbb{Z}_p[x]$ such that $h_{k-2}l_{k-2} - n_{k-1}l_{k-1} = \delta_{k-2}f$. Then $h_{k-2}l_{k-2} = \delta_{k-2}f + n_{k-1}l_{k-1}$. Hence

$$\begin{aligned} &\alpha_{k-2} \circ (h_{k-2}l_{k-2}|u^{k-1}h_{k-2}t_1) \\ &= \alpha_{k-2} \circ (\delta_{k-2}f + n_{k-1}l_{k-1}|u^{k-1}n_{k-1}a_{k-1}) \\ &= \alpha_{k-2} \circ (\delta_{k-2}(f|0) + n_{k-1}(l_{k-1}|u^{k-1}a_{k-1})) \\ &= \alpha_{k-2}\delta_{k-2} \circ (f|0) + \alpha_{k-2}n_{k-1} \circ (l_{k-1}|u^{k-1}a_{k-1}). \end{aligned}$$

Now $\alpha_{k-2}\delta_{k-2} \circ (f|0) \in \mathrm{Span}(S_1)$ and $\alpha_{k-2}n_{k-1} \circ (l_{k-1}|u^{k-1}a_{k-1}) \in \mathrm{Span}(S_{k+1})$. Hence $d_{k-2} \circ (l_{k-2}|u^{k-2}a_{k-2} + u^{k-1}t_1) \in \mathrm{Span}(S)$.

Now let the third last term in c be $d_{k-3} \circ (l_{k-3}|u^{k-3}a_{k-3} + u^{k-2}r_1 + u^{k-1}r_2)$. If $\deg d_{k-3} < \deg h_{k-3}$, then $d_{k-3} \circ (l_{k-3}|u^{k-3}a_{k-3} + u^{k-2}r_1 + u^{k-1}r_2) \in \mathrm{Span}(S_{k-1})$. Otherwise, there exist $\alpha_{k-3}, \beta_{k-3} \in R_k[x]$ such that $d_{k-3} = \alpha_{k-3}h_{k-3} + \beta_{k-3}$ and $\deg \beta_{k-3} < \deg h_{k-3}$. Then

$$\begin{aligned} &d_{k-3} \circ (l_{k-3}|u^{k-3}a_{k-3} + u^{k-2}r_1 + u^{k-1}r_2) \\ &= \alpha_{k-3} \circ (h_{k-3}l_{k-3}|h_{k-3}(u^{k-2}r_1 + u^{k-1}r_2)) \\ &\quad + \beta_{k-3} \circ (l_{k-3}|u^{k-3}a_{k-3} + u^{k-2}r_1 + u^{k-1}r_2). \end{aligned}$$

Since $\deg \beta_{k-3} < \deg h_{k-3}$, $\beta_{k-3} \circ (l_{k-3}|u^{k-3}a_{k-3} + u^{k-2}r_1 + u^{k-1}r_2) \in \mathrm{Span}(S_{k-1})$. We therefore consider $\alpha_{k-3} \circ (h_{k-3}l_{k-3}|h_{k-3}(u^{k-2}r_1 + u^{k-1}r_2))$. We know that $a_{k-2} \mid h_{k-3}r_1$. Let $h_{k-3}r_1 = n_{k-2}a_{k-2}$. Then we have

$$\begin{aligned} &h_{k-3}(l_{k-3}|u^{k-3}a_{k-3} + u^{k-2}r_1 + u^{k-1}r_2) - n_{k-2}(l_{k-1}|u^{k-1}a_{k-1}) \\ &= (h_{k-3}l_{k-3} - n_{k-2}l_{k-1}|u^{k-1}(h_{k-3}r_2 - n_{k-2}t_1)) \in C. \end{aligned}$$

This implies that $a_{k-1} \mid (h_{k-3}r_2 - n_{k-2}t_1)$. Let $h_{k-3}r_2 - n_{k-2}t_1 = n'_{k-2}a_{k-1}$. Then

$$\begin{aligned} &(h_{k-3}l_{k-3} - n_{k-2}l_{k-1}|u^{k-1}(h_{k-3}r_2 - n_{k-2}t_1)) - n'_{k-2}(l_{k-1}|u^{k-1}a_{k-1}) \\ &= (h_{k-3}l_{k-3} - n_{k-2}l_{k-1} - n'_{k-2}l_{k-2} \mid 0) \in C. \end{aligned}$$

Hence $f \mid (h_{k-3}l_{k-3} - n_{k-2}l_{k-1} - n'_{k-2}l_{k-2})$. Let $h_{k-3}l_{k-3} - n_{k-2}l_{k-1} - n'_{k-2}l_{k-2} = \delta_{k-3}f$. Then $h_{k-3}l_{k-3} = \delta_{k-3}f + n_{k-2}l_{k-1} + n'_{k-2}l_{k-2}$. Hence

$$\begin{aligned} &\alpha_{k-3} \circ (h_{k-3}l_{k-3}|h_{k-3}(u^{k-2}r_1 + u^{k-1}r_2)) \\ &= \alpha_{k-3} \circ (\delta_{k-3}f + n_{k-2}l_{k-2} + n'_{k-2}l_{k-1}|u^{k-2}h_{k-3}r_1 + u^{k-1}h_{k-3}r_2) \\ &= \alpha_{k-3} \circ (\delta_{k-3}f + n_{k-2}l_{k-2} + n'_{k-2}l_{k-1}|u^{k-2}n_{k-2}a_{k-2} \end{aligned}$$

$$+ u^{k-1}(n_{k-2}t_1 + n'_{k-2}a_{k-1}))$$
$$= \alpha_{k-3} \circ (\delta_{k-3}(f|0) + n_{k-2}(l_{k-2}|u^{k-2}a_{k-2} + u^{k-1}t_1) + n'_{k-2}(l_{k-1}|u^{k-1}a_{k-1})).$$

Now $\alpha_{k-3}\delta_{k-3} \circ (f|0) \in \mathrm{Span}(S_1)$, $\alpha_{k-3}n_{k-2} \circ (l_{k-2}|u^{k-2}a_{k-2} + u^{k-1}t_1) \in \mathrm{Span}(S_k)$ and $\alpha_{k-3}n_{k-2} \circ (l_{k-2}|u^{k-2}a_{k-2}) \in \mathrm{Span}(S_{k+1})$. Hence

$$d_{k-3} \circ (l_{k-3}|u^{k-3}a_{k-3} + u^{k-2}r_1 + u^{k-1}r_2) \in \mathrm{Span}(S).$$

Proceeding in the same way as above, we can show that all other terms in c are also in $\mathrm{Span}(S)$. Hence S is a spanning set for C. Further, from the forms of the sets $S_1, S_2, \ldots, S_{k+1}$, it is clear that S is a minimal spanning set for C. □

Corollary 3.10. *Let C be a $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic code such that $C = \langle (f(x)|0) \rangle$ where $f(x)|(x^r - 1)$ and $f(x)h(x) = x^r - 1$. Let*

$$S = \bigcup_{i=0}^{\deg h(x)-1} \{x^i \circ (f(x)|0)\}.$$

Then S forms a minimal spanning set for C.

Proof. Since $C = \langle (f(x)|0) \rangle$, it is clear that S forms a minimal spanning set for C. □

In the next theorem, we determine the minimal spanning set of $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic codes of length $(r + s)$ when $(r, p) = 1$ and $(s, p) = 1$.

Theorem 3.11. *Let $C = \langle (f(x)|0), (l(x)|g(x) + ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x)) \rangle$ be a $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic code of length $(r + s)$, with $(r, p) = 1$ and $(s, p) = 1$ and $f(x)$, $l(x)$, $g(x)$, $a_1(x), \ldots, a_{k-1}(x) \in \mathbb{Z}_p[x]$ such that $a_{k-1}(x)|a_{k-2}(x)| \cdots a_1(x)|g|(x^s - 1)$. Let $\deg f(x) = t_1$, $\deg g(x) = t_2$, and $\deg a_i(x) = t_{i+2}$, $i = 1, 2, \ldots, k - 1$. Let $h_0(x) = \frac{x^s-1}{g(x)}$, $m_1(x) = \frac{g(x)}{a_1(x)}$, and $m_i(x) = \frac{a_{i-1}(x)}{a_i(x)}$, $i = 2, 3 \ldots, k - 1$. Define the sets*

$$S_1 = \bigcup_{i=0}^{r-t_1-1} \{x^i \circ (f(x)|0)\},$$
$$S_2 = \bigcup_{i=0}^{s-t_2-1} \{x^i \circ (l(x)|g(x) + ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x))\},$$
$$S_3 = \bigcup_{i=0}^{t_2-t_3-1} \{x^i \circ (l(x)h_0(x)|h_0(x)(ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x)))\},$$
$$S_4 = \bigcup_{i=0}^{t_3-t_4-1} \{x^i \circ (l(x)h_0(x)m_1(x)|h_0(x)m_1(x)(u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x)))\},$$
$$\vdots$$

$$S_{k+1} = \bigcup_{i=0}^{t_k - t_{k+1}-1} \{x^i \circ (l(x)h_0(x)m_1(x)\cdots m_{k-2}(x)|u^{k-1}a_{k-1}(x)h_0(x)m_1(x)\cdots m_{k-2}(x))\}.$$

Then $S = S_1 \cup S_2 \cup S_3 \cup \cdots \cup S_{k+1}$ is a minimal spanning set for C.

Proof. We have $\deg h_0(x) = s - t_2$ and $\deg m_{k-1}(x) = t_k - t_{k+1}$. Let $c(x)$ be a codeword in C. Then there are polynomials $d_1(x) \in \mathbb{Z}_p[x]$ and $d_2(x) \in R_k[x]$ such that

$$c(x) = d_1(x) \circ \left(f(x)|0\right) + d_2(x) \circ (l(x)|g(x) + ua_1(x) + \cdots + u^{k-1}a_{k-1}(x)\right).$$

Then, just as shown in Theorem 3.9, we get $d_1(x) \circ (f(x)|0) \in \mathrm{Span}(S_1)$. Now we show that

$$d_2(x) \circ (l(x)|g(x) + ua_1(x) + \cdots + u^{k-1}a_{k-1}(x)) \in \mathrm{Span}(S).$$

If $\deg d_2(x) \leq s - t_2 - 1$, then $d_2(x) \circ (l(x)|g(x) + ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x)) \in \mathrm{Span}(S_2)$. Otherwise, by division algorithm, there are polynomials $q_2(x), r_2(x)$ such that $d_2(x) = h_0(x)q_2(x) + r_2(x)$, where $r_2(x) = 0$ or $\deg r_2(x) \leq s - t_2 - 1$. This implies that $d_2(x) \circ (l(x)|g(x) + ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x)) = q_2(x) \circ (h_0(x)l(x)|h_0(x)(ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x))) + r_2(x) \circ (l(x)|g(x) + ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x))$. Since $r_2(x) = 0$ or $\deg r_2(x) \leq s - t_2 - 1$,

$$r_2(x) \circ (l(x)|g(x) + ua_1(x) + \cdots + u^{k-1}a_{k-1}(x)) \in \mathrm{Span}(S_2).$$

Now we need to show that

$$q_2(x) \circ (h_0(x)l(x)|h_0(x)(ua_1(x) + \cdots + u^{k-1}a_{k-1}(x))) \in \mathrm{Span}(S).$$

If $\deg q_2(x) \leq t_2 - t_3 - 1$, then

$$q_2(x) \circ (h_0(x)l(x)|h_0(x)(ua_1(x) + \cdots + u^{k-1}a_{k-1}(x))) \in \mathrm{Span}(S_3),$$

and hence $d_2(x) \circ (l(x)|g(x) + ua_1(x) + \cdots + u^{k-1}a_{k-1}(x)) \in \mathrm{Span}(S_2 \cup S_3)$. Otherwise, we use division algorithm to divide $q_2(x)$ by $m_2(x)$. Continuing in this way, dividing successive quotients $q_i(x)$ by $m_i(x)$, $i = 3, \ldots, k-2$, we finally get $d_2(x) \circ (l(x)|g(x) + ua_1(x) + \cdots + u^{k-1}a_{k-1}(x)) \in \mathrm{Span}(S_1 \cup S_2 \cup \cdots \cup S_{k+1})$. Hence $c(x) \in \mathrm{Span}(S_1 \cup S_2 \cup \cdots \cup S_{k+1}) = \mathrm{Span}(S)$. Hence S forms spanning set for C. Moreover, from the forms of the sets $S_1, S_2, \ldots, S_{k+1}$, it is clear that S is a minimal spanning set for C. □

Corollary 3.12. *Let C be a $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic code such that $C = \langle l(x)|g(x) + ua_1(x) + \cdots + u^{k-1}a_{k-1}(x)\rangle$. Let*

$$S_2 = \bigcup_{i=0}^{s-t_2-1} \{x^i \circ (l(x)|g(x) + ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x))\},$$

$$S_3 = \bigcup_{i=0}^{t_2-t_3-1} \{x^i \circ (l(x)h_0(x)|h_0(x)(ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x)))\},$$

$$S_4 = \bigcup_{i=0}^{t_3-t_4-1} \{x^i \circ (l(x)h_0(x)m_1(x)|h_0(x)m_1(x)(u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x)))\},$$

$$\vdots$$

$$S_{k+1} = \bigcup_{i=0}^{t_k-t_{k+1}-1} \{x^i \circ (l(x)h_0(x)m_1(x)\cdots m_{k-2}(x)|u^{k-1}a_{k-1}(x)h_0(x)m_1(x)\cdots m_{k-2}(x))\}.$$

Then $S' = S_2 \cup S_3 \cup \cdots \cup S_{k+1}$ is a minimal spanning set for C.

Proof. Since $C = \langle l(x)|g(x) + ua_1(x) + \cdots + u^{k-1}a_{k-1}(x)\rangle$, clearly S' is a minimal spanning set for C. □

Now we present some examples for constructing codes of the types considered above. In the first two examples, we consider the case $(r,p) = 1, (s,p) \neq 1$, and in the next two examples the case $(r,p) = 1, (s,p) = 1$ is considered. In all the examples, we present the Gray images of generator matrices and the parameters of the corresponding codes over $\mathbb{Z}_p$.

Example 3.13. Let $r = 3$ and $s = 8$, and let $C = \langle (f(x)|0), (l(x)|g(x) + up_1(x) + u^2p_2(x))\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code of length $(r+s)$, where $f(x) = x^3 - 1$, $l(x) = x^2 + x$ and $g(x) = x + 1$, $p_1(x) = 0$, $p_2(x) = 0$. Over $\mathbb{Z}_2$ we get $x^8 - 1 = (x-1)^8 = (g(x))^8$. Then the Gray image of the generator matrix of C is obtained as $G = [A|B]$, where

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

and

$$B = \begin{pmatrix} 00000110000000000000000000000000 \\ 00000101000000000000000000000000 \\ 10000010000000000000000000000000 \\ 01000001000000000000000000000000 \\ 00100101000000000000000000000000 \\ 00010010000000000000000000000000 \\ 00001001000000000000000000000000 \end{pmatrix}.$$

The parameters of the Gray image of C are $[35, 7, 2]_2$.

Example 3.14. Let $r = 3$ and $s = 5$, and let $C = \langle (f(x)|0), (l(x)|g(x)+up_1(x)\rangle$ be a $\mathbb{Z}_5\mathbb{Z}_5[u^2]$-cyclic code of length $(r+s)$, where $f(x) = x^3-1$, $l(x) = x^2+x+1$ and $g(x) = x + 4$, $p_1(x) = 1$. Over $\mathbb{Z}_5$ we get $x^5 - 1 = (x+4)^5 = (g(x))^5$.

Then the Gray image of the generator matrix of C is obtained as

$$G=\begin{pmatrix}1110001111122222111110000000\\0001000010000400004000000000\\0000100001000040000400000000\\0000010000100004000040000000\end{pmatrix}.$$

The parameters of the Gray image of C are $[28,4,4]_5$.

Example 3.15. Let $r=3$ and $s=9$. Let $C=\langle (f(x)|0),(l(x)|g(x)+ua_1(x)+u^2a_2(x))\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code of length $(r+s)$, where $f(x)=x^3-1, l(x)=x^2+x, g(x)=x^9-1, a_1(x)=x^9-1$, and $a_2(x)=x^7+x^6+x^4+x^3+x+1$. Then the generator matrix of the Gray image of C is $G=[A|B]$, where

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

and

$$B=\begin{pmatrix}011110111000000111011100000111011100000\\111000001111100001110000001110111000011 0\end{pmatrix}.$$

The parameters of the Gray image of C are $[39,2,20]_2$.

Example 3.16. Let $r=5$ and $s=7$. Let $C=\langle (f(x)|0),(l(x)|g(x)+ua_1(x))\rangle$ be a $\mathbb{Z}_3\mathbb{Z}_3[u^2]$-cyclic code of length $(r+s)$, where $f(x)=x^5-1, l(x)=x^4+x^3+x^2+x+1, g(x)=x^6+x^5+x^4+x^3+x^2+x+1, a_1(x)=x+2$. Then the generator matrix of the Gray image of C is

$$G=\begin{pmatrix}10000000121112202110022202\\01000000101102011120222002\\00100000222111222000000000\\00010000022211122200000000\\00001000002221112220000000\\00000100011002021120111001\\00000010000001000000100000 00\\00000001210020121120222002\end{pmatrix}.$$

The parameters of the Gray image of C are $[26,8,3]_3$.

In Table 1, we present some optimal codes, which have been obtained from $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic codes via the Gray map.

4. The MacWilliams identity

In this section we establish the MacWilliams identity for $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-linear codes. We first define the complete weight enumerator for linear codes over $\mathbb{Z}_p[u]/\langle u^k\rangle$ and $\mathbb{Z}_p$, and then establish the MacWilliams identity for $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-linear codes with respect to the complete weight enumerator. Since the Mac

TABLE 1. Some optimal p-ary codes obtained from $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic codes.

p	r	s	k	Generators	p-ary Images
2	3	1	2	$f = x^2 + x + 1,\ l = x^2 + 1,\ g = 1$	$[5, 2, 3]_2$
3	11	1	2	$f = (x^5 + 2x^3 + x^2 + 2x + 2)(x^5 + x^4 + 2x^3 + x^2 + 2)$, $l = 2x^9 + x^7 + 2x^6 + x^4 + x^3 + x + 2$, $g = x + 2,\ h = 1,\ a_1 = 1$	$[14, 2, 10]_3$
3	7	1	2	$f = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, $l = 2x^5 + x^4 + x + 1, g = x + 2,\ h = 1,\ a_1 = 1$	$[10, 2, 7]_3$
3	5	3	1	$f = x^5 - 1, l = x^4 + x^3 + x^2 + 2, g = 1$	$[8, 3, 5]_3$
3	7	1	1	$f = x^7 - 1, l = x^6 + x^5 + x + 1, g = 1$	$[8, 1, 8]_3$
3	5	1	1	$f = x^5 - 1, l = x^4 + x^3 + x^2 + x + 1, g = 1$	$[6, 1, 6]_3$
5	7	1	1	$f = x^7 - 1, l = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, g = 1$	$[8, 1, 8]_5$

Williams identity establishes a relation between weight enumerator of a linear code and its dual, we first define a new inner product on $\mathbb{Z}_p^r \times R_k^s$ as follows:

$$v \cdot w = u^{k-1}\left(\sum_{i=1}^{r} v_i w_i\right) + \sum_{j=r+1}^{r+s} v_j w_j,$$

where $v, w \in \mathbb{Z}_p^r \times R_k^s$. The dual $C^\perp$ of a linear code C can then be defined as

$$C^\perp = \{w \in \mathbb{Z}_p^r \times R_k^s \mid v \cdot w = 0 \text{ for all } v \in C\}.$$

In this section, we use the notation $\langle , \rangle$ for the standard Euclidean inner product, i.e., for any $\beta = (\beta_0, \beta_1, \dots, \beta_{\ell-1})$ and $\gamma = (\gamma_0, \gamma_1, \dots, \gamma_{\ell-1})$ in $\mathbb{Z}_p^\ell$ (or R_k^ℓ),

$$\langle \beta, \gamma \rangle = \beta_0\gamma_0 + \beta_1\gamma_1 + \cdots + \beta_{\ell-1}\gamma_{\ell-1}.$$

Then clearly, for any $v = (v'|v'')$ and $w = (w'|w'')$ in $\mathbb{Z}_p^r \times R_k^s$, we have

$$v \cdot w = u^{k-1}\langle v', w' \rangle + \langle v'', w'' \rangle.$$

Let g_i, $1 \le i \le p$, be all the elements of $\mathbb{Z}_p$ and h_j, $1 \le j \le p^k$, be all the elements of $\mathbb{Z}_p[u^k]$ in some order. The *complete weight enumerator* of a $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-linear code C is defined by

$$W_C(X_1, \dots, X_p, Y_1, \dots, Y_{p^k}) = \sum_{(\bar{c}_1|\bar{c}_2) \in C} X_1^{n_{g_1}(\bar{c}_1)} \cdots X_p^{n_{g_p}(\bar{c}_1)} Y_1^{n_{h_1}(\bar{c}_2)} \cdots Y_{p^k}^{n_{h_{p^k}}(\bar{c}_2)},$$

where, for any $(\bar{c}_1|\bar{c}_2) \in C$, $n_{g_i}(\bar{c}_1)$ and $n_{h_j}(\bar{c}_2)$ denote the numbers of appearances of g_i and h_j in $\bar{c}_1$ and $\bar{c}_2$, respectively.

Let t_1 and t_2 be two complex variables such that the exponents of t_1 are the elements of $\mathbb{Z}_p$ and the exponents of t_2 are the elements of $R_k = \mathbb{Z}_p[u^k]$. Moreover, $t_1 = e^{2\pi i/p}$, $t_2 = e^{2\pi i/p^k}$, $t_2^{u^i} = t_2^{p^i} = e^{2\pi i/p^{k-i}}$ for $0 \le i \le k-1$, and ${t_2}^{a+b} = {t_2}^a {t_2}^b$ for any $a, b \in R_k$. Then clearly $t_2^{u^{k-1}} = t_1$. Let f be a complex valued function defined on $\mathbb{Z}_p^r \times R_k^s$. For $x = (x'|x'') \in \mathbb{Z}_p^r \times R_k^s$, denote

$$\hat{f}(x) = \hat{f}(x'|x'') = \sum_{u \in \mathbb{Z}_p^r \times R_k^s} t_2^{u \cdot x} f(u).$$

The function $\hat{f}$ is called the Fourier transform of f.

The following lemma is important for establishing MacWilliams identity for $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-linear codes.

Lemma 4.1. *Let C be a $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-linear code of length $(r+s)$ and $C^\perp$ be its dual. Then for every complex valued function f on $\mathbb{Z}_p^r \times R_k^s$*

$$\sum_{x \in C^\perp} f(x) = \frac{1}{|C|} \sum_{u \in C} \hat{f}(u).$$

Proof. We have

$$\begin{aligned} \sum_{u \in C} \hat{f}(u) &= \sum_{u \in C} \sum_{x \in \mathbb{Z}_p^r \times R_k^s} t_2^{u \cdot x} f(x) \\ &= \sum_{x \in \mathbb{Z}_p^r \times R_k^s} f(x) \sum_{u \in C} t_2^{u \cdot x}. \end{aligned}$$

If $x \in C^\perp$, then $u \cdot x = 0$ for all $u \in C$. Hence the inner sum $\sum_{u \in C} t_2^{u \cdot x}$ is equal to $|C|$. On the other hand, if $x \notin C^\perp$, then there exists $u_0 \in C$ such that $u_0 \cdot x \neq 0$. Since C is a $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-linear code, for the inner sum $\sum_{u \in C} t_2^{u \cdot x}$, we have

$$\begin{aligned} \sum_{u \in C} t_2^{u \cdot x} &= \sum_{u \in C} t_2^{(u+u_0) \cdot x} \\ &= t_2^{u_0 \cdot x} \sum_{u \in C} t_2^{u \cdot x}. \end{aligned}$$

Since $u_0 \cdot x \neq 0$, we have $t_2^{u_0 \cdot x} \neq 1$, and hence the inner sum is 0. Therefore

$$\sum_{x \in C^\perp} f(x) = \frac{1}{|C|} \sum_{u \in C} \hat{f}(u).$$

□

Theorem 4.2. *Let C be a $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-linear code of length $(r+s)$ and let $C^\perp$ be its dual, and t_1 and t_2 be as defined above, g_i, $1 \le i \le p$, be all the elements of $\mathbb{Z}_p$ in some order and h_j, $1 \le j \le p^k$, be all the elements of R_k in some order. Then*

$$W_{C^\perp}(X_1, \ldots, X_p, Y_1, \ldots, Y_{p^k})$$

$$= \frac{1}{|C|} W_C \left(\sum_{i=1}^{p} t_1^{g_1 g_i} X_i, \ldots, \sum_{i=1}^{p} t_1^{g_p g_i} X_i,\ \sum_{j=1}^{p^k} t_2^{h_1 h_j} Y_j, \ldots, \sum_{j=1}^{p^k} t_2^{h_{p^k} h_j} Y_j \right).$$

Proof. We introduce a function $F(x|x')$ over $\mathbb{Z}_p^r \times R_k^s$ such that

$$F(c|c') = \sum_{x \in\ \mathbb{Z}_p^r} {t_1}^{\langle c,x \rangle} \prod_{i=1}^{p} X_i^{n_{g_i}(x)} \sum_{x' \in R_k^s} {t_2}^{\langle c',x' \rangle} \prod_{j=1}^{p^k} Y_j^{n_{h_j}(x')}.$$

Summing $F(c|c')$ over all the codewords in C, we obtain

$$\begin{aligned} \sum_{(c|c') \in C} F(c|c') &= \sum_{(c|c') \in C} \left(\sum_{x \in \mathbb{Z}_p^r} {t_1}^{\langle c,x \rangle} \prod_{i=1}^{p} X_i^{n_{g_i}(x)} \right) \left(\sum_{x' \in R_k^s} {t_2}^{\langle c',x' \rangle} \prod_{j=1}^{p^k} Y_j^{n_{h_j}(x')} \right) \\ &= \sum_{x \in \mathbb{Z}_p^r} \prod_{i=1}^{p} X_i^{n_{g_i}(x)} \sum_{x' \in R_k^s} \prod_{j=1}^{p^k} Y_j^{n_{h_j}(x')} \sum_{(c|c') \in C} {t_1}^{\langle c,x \rangle} {t_2}^{\langle c',x' \rangle} \\ &= \sum_{x \in \mathbb{Z}_p^r} \prod_{i=1}^{p} X_i^{n_{g_i}(x)} \sum_{x' \in R_k^s} \prod_{j=1}^{p^k} Y_j^{n_{h_j}(x')} \sum_{(c|c') \in C} {t_2}^{u^{k-1} \langle c,x \rangle} {t_2}^{\langle c',x' \rangle} \\ &= \sum_{x \in \mathbb{Z}_p^r} \prod_{i=1}^{p} X_i^{n_{g_i}(x)} \sum_{x' \in R_k^s} \prod_{j=1}^{p^k} Y_j^{n_{h_j}(x')} \sum_{(c|c') \in C} {t_2}^{(c|c') \cdot (x|x')}. \end{aligned} \tag{9}$$

From Lemma 4.1, if $(x|x') \in C^{\perp}$, the inner sum in the RHS of (9) is $|C|$, and if $(x|x') \notin C^{\perp}$, then this sum is 0. Hence we have

$$\begin{aligned} &\sum_{(x|x') \in C^{\perp}} \prod_{i=1}^{p} X_i^{n_{g_i}(x)} \prod_{j=1}^{p^k} Y_j^{n_{h_j}(x')} \sum_{(c|c') \in C} {t_2}^{(c|c') \cdot (x|x')} \\ &= |C| \sum_{(x|x') \in C^{\perp}} \prod_{i=1}^{p} X_i^{n_{g_i}(x)} \prod_{j=1}^{p^k} Y_j^{n_{h_j}(x')}. \end{aligned}$$

Therefore from (9) we get

$$\begin{aligned} \sum_{(c|c') \in C} F(c|c') &= |C| \sum_{(x|x') \in C^{\perp}} \prod_{i=1}^{p} X_i^{n_{g_i}(x)} \prod_{j=1}^{p^k} Y_j^{n_{h_j}(x')} \\ &= |C| W_{C^{\perp}}(X_1, \ldots, X_p, Y_1, \ldots, Y_{p^k}). \end{aligned}$$

This implies that

$$W_{C^{\perp}}(X_1, \ldots, X_p, Y_1, \ldots, Y_{p^k}) = \frac{1}{|C|} \sum_{(c|c') \in C} F(c|c'). \tag{10}$$

Now we need to find $F(c|c')$. Let $\delta(x,y)$ be the Kronecker delta function. Then

$$\begin{aligned}
F(c|c') &= \sum_{x\in\ \mathbb{Z}_p^r} {t_1}^{\langle c,x\rangle} \prod_{i=1}^{p} X_i^{n_{g_i}(x)} \sum_{x'\in R_k^s} {t_2}^{\langle c',x'\rangle} \prod_{j=1}^{p^k} Y_j^{n_{h_j}(x')} \\
&= \sum_{(x_1,\ldots,x_r)\in\mathbb{Z}_p^r} \prod_{\ell=1}^{r} \left({t_1}^{c_\ell x_\ell} \prod_{i=1}^{p} X_i^{\delta(x_\ell,g_i)} \right) \\
&\quad \sum_{(x'_1,\ldots,x'_s)\in R_k^s} \prod_{\ell=r+1}^{r+s} \left({t_2}^{c_\ell x_\ell} \prod_{j=1}^{p^k} Y_j^{\delta(x_\ell,h_j)} \right) \\
&= \prod_{\ell=1}^{r} \left(\sum_{i=1}^{p} {t_1}^{c_\ell g_i} X_i \right) \prod_{\ell=r+1}^{s} \left(\sum_{j=1}^{p^k} {t_2}^{c_\ell h_j} Y_j \right) \\
&= \left(\sum_{i=1}^{p} {t_1}^{g_1 g_i} X_i \right)^{n_{g_1}(c)} \cdots \left(\sum_{i=1}^{p} {t_1}^{g_p g_i} X_i \right)^{n_{g_p}(c)} \\
&\quad \cdot \left(\sum_{j=1}^{p^k} {t_2}^{h_1 h_j} Y_j \right)^{n_{h_1}(c')} \cdots \left(\sum_{j=1}^{p^k} {t_2}^{h_{p^k} h_j} Y_j \right)^{n_{h_{p^k}}(c')} .
\end{aligned}$$

Summing the above equation over all codewords of C, we get

$$\begin{aligned}
\sum_{(c|c')\in C} F(c|c') = W_C \Bigg(&\left(\sum_{i=1}^{p} {t_1}^{g_1 g_i} X_i \right)^{n_{g_1}(c)}, \ldots, \left(\sum_{i=1}^{p} {t_1}^{g_p g_i} X_i \right)^{n_{g_p}(c)}, \\
&\left(\sum_{j=1}^{p^k} {t_2}^{h_1 h_j} Y_j \right)^{n_{h_1}(c')}, \ldots, \left(\sum_{j=1}^{p^k} {t_2}^{h_{p^k} h_j} Y_j \right)^{n_{h_{p^k}}(c')} \Bigg). \qquad (11)
\end{aligned}$$

By using the definition of complete weight enumerator, and combining (10) and (11), we get

$$\begin{aligned}
W_{C^\perp}(X_1,\ldots,X_p,Y_1,\ldots,Y_{p^k}) = \frac{1}{|C|} W_C \Bigg(&\sum_{i=1}^{p} {t_1}^{g_1 g_i} X_i, \ldots, \sum_{i=1}^{p} {t_1}^{g_p g_i} X_i, \\
&\sum_{j=1}^{p^k} {t_2}^{h_1 h_j} Y_j, \ldots, \sum_{j=1}^{p^k} {t_2}^{h_{p^k} h_j} Y_j \Bigg).
\end{aligned}$$

□

Now we give an example to illustrate the use of the above identity.

Example 4.3. Let C be a $\mathbb{Z}_2\mathbb{Z}_2[u^2]$-linear code with $r = 2, s = 3$, and with the generator matrix

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

Since C is a $\mathbb{Z}_2[u^2]$-module, we get

$$C = \{(00|000), (11|u00), (10|010), (01|u10), (00|0u0), (10|0\overline{u}0), (11|uu0), (01|u\overline{u}0)\},$$

where $\overline{u} = 1+u$. Let $g_1 = 0, g_2 = 1$ and $h_1 = 0, h_2 = 1, h_3 = u, h_4 = \overline{u} = 1+u$. Then the complete weight enumerator of C is

$$\begin{aligned} W_C(X_1, X_2, Y_1, \ldots, Y_4) &= X_1^2Y_1^3 + X_2^2Y_1^2Y_3 + X_1X_2Y_1^2Y_2 + X_1X_2Y_1Y_2Y_3 \\ &\quad + X_1^2Y_1^2Y_3 + X_1X_2Y_1^2Y_4 + X_2^2Y_1Y_3^2 + X_1X_2Y_1Y_3Y_4. \end{aligned} \tag{12}$$

Now using the MacWilliams identity, the weight enumerator for $C^\perp$ is

$$\begin{aligned} W_{C^\perp}(X_1, X_2, Y_1, \ldots, Y_4) = \frac{1}{|C|} W_C \Bigg(&\sum_{i=1}^{2} t_1^{g_1g_i} X_i,\ \sum_{i=1}^{2} t_1^{g_2g_i} X_i,\ \sum_{j=1}^{4} t_2^{h_1h_j} Y_j, \\ &\sum_{j=1}^{4} t_2^{h_2h_j} Y_j,\ \sum_{j=1}^{4} t_2^{h_3h_j} Y_j,\ \sum_{j=1}^{4} t_2^{h_4h_j} Y_j \Bigg). \end{aligned}$$

After computation and noting that $t_1 = e^{2\pi i/2} = -1, t_2 = e^{2\pi i/2^2} = i$, and $t^u = t^2 = -1$, we get

$$\begin{aligned} &W_{C^\perp}(X_1, X_2, Y_1, \ldots, Y_4) \\ &= \frac{1}{|C|} W_C \big[(X_1 + X_2), (X_1 - X_2), (Y_1 + Y_2 + Y_3 + Y_4), \\ &\quad (Y_1 + iY_2 - Y_3 - iY_4), (Y_1 - Y_2 + Y_3 - Y_4), (Y_1 - iY_2 - Y_3 + iY_4)\big]. \end{aligned}$$

Then from (12) and after doing computation, we get

$$\begin{aligned} &W_{C^\perp}(X_1, X_2, Y_1, \ldots, Y_4) \\ &= X_1^2Y_1^3 + X_1^2Y_1^2Y_2 + 2X_1^2Y_1^2Y_3 + X_1^2Y_1^2Y_4 + X_1^2Y_1Y_2Y_3 + X_1^2Y_1Y_3^2 \\ &\quad + X_1^2Y_1Y_3Y_4 + X_1X_2Y_1^2Y_2 + X_1X_2Y_1^2Y_4 + X_1X_2Y_1Y_2^2 \\ &\quad + 2X_1X_2Y_1Y_2Y_3 + 2X_1X_2Y_1Y_2Y_4 + 2X_1X_2Y_1Y_3Y_4 \\ &\quad + X_1X_2Y_1Y_4^2 + X_1X_2Y_2^2Y_3 + X_1X_2Y_2Y_3^2 + 2X_1X_2Y_2Y_3Y_4 \\ &\quad + X_1X_2Y_3^2Y_4 + X_1X_2Y_3Y_4^2 + X_2^2Y_1^2Y_3 + X_2^2Y_1Y_2Y_3 + 2X_2^2Y_1Y_3^2 \\ &\quad + X_2^2Y_1Y_3Y_4 + X_2^2Y_2Y_3^2 + X_2^2Y_3^3 + X_2^2Y_3^2Y_4. \end{aligned}$$

5. Conclusion

In this paper we have studied linear and cyclic codes over the alphabet $\mathbb{Z}_p\mathbb{Z}_p[u]/\langle u^k\rangle, u^k = 0$. A $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-linear code of length $(r + s)$ is a submodule of $\mathbb{Z}_p^r \times R_k^s$. A new Gray map has been introduced. For $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic codes, we have considered two cases: $(r, p) = 1, (s, p) \neq 1$ and $(r, p) = 1, (s, p) = 1$. MacWilliams identities are established for $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-linear codes. The results of the paper can further be generalized to $\mathbb{Z}_q\mathbb{Z}_q[u^k]$-linear and cyclic codes, where q is a prime power. Also, it may be interesting to study $\mathbb{Z}_p\mathbb{Z}_p[u^k]$-cyclic codes without putting the above restrictions on r and s.

Acknowledgement. The authors are thankful to the anonymous referee for his/her careful reading of the manuscript and helpful suggestions that greatly improved the final presentation of the manuscript. The second author would like to thank Ministry of Human Resource Development (MHRD), India, for providing financial support.

References

[1] I. Aydogdu, T. Abualrub, and I. Siap, *On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes*, Int. J. Comput. Math. **92** (2015), no. 9, 1806–1814. https://doi.org/10.1080/00207160.2013.859854

[2] I. Aydogdu and I. Siap, *The structure of $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes: bounds on the minimum distance*, Appl. Math. Inf. Sci. **7** (2013), no. 6, 2271–2278. https://doi.org/10.12785/amis/070617

[3] ———, *On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes*, Linear Multilinear Algebra **63** (2015), no. 10, 2089–2102. https://doi.org/10.1080/03081087.2014.952728

[4] I. Aydogdu, I. Siap, and R. Ten-Valls, *On the structure of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear and cyclic codes*, Finite Fields Appl. **48** (2017), 241–260. https://doi.org/10.1016/j.ffa.2017.03.001

[5] J. Borges, C. Fernández-Córdoba, and R. Ten-Valls, *$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, generator polynomials, and dual codes*, IEEE Trans. Inform. Theory **62** (2016), no. 11, 6348–6354. https://doi.org/10.1109/TIT.2016.2611528

[6] ———, *$\mathbb{Z}_2$-double cyclic codes*, Des. Codes Cryptogr. **86** (2018), no. 3, 463–479. https://doi.org/10.1007/s10623-017-0334-8

[7] L. Diao and J. Gao, *$\mathbb{Z}_p\mathbb{Z}_p[u]$-additive cyclic codes*, Int. J. Inf. Coding Theory **5** (2018), no. 1, 1–17. https://doi.org/10.1504/IJICOT.2018.091815

[8] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The $\mathbf{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319. https://doi.org/10.1109/18.312154

[9] L. Qian and X. Cao, *Bounds and optimal q-ary codes derived from the $\mathbb{Z}_qR$-cyclic codes*, IEEE Trans. Inform. Theory **66** (2020), no. 2, 923–935. https://doi.org/10.1109/TIT.2019.2927034

[10] J. Rifà and L. Ronquillo, *Product perfect $\mathbb{Z}_2\mathbb{Z}_4$-linear codes in stegonography*, International Symposium on Information Theory and Its Applications (2010), 696–701.

[11] M. Shi, R. Wu, and D. S. Krotov, *On $Z_pZ_{p^k}$-additive codes and their duality*, IEEE Trans. Inform. Theory **65** (2019), no. 6, 3841–3847. https://doi.org/10.1109/TIT.2018.2883759

[12] A. K. Singh and P. K. Kewat, *On cyclic codes over the ring $\mathbb{Z}_p[u]/\langle u^k\rangle$*, Des. Codes Cryptogr. **74** (2015), no. 1, 1–13. https://doi.org/10.1007/s10623-013-9843-2

Maheshanand Bhaintwal
Department of Mathematics
Indian Institute of Technology Roorkee
Roorkee-247667, India
Email address: mahesfma@iitr.ac.in

Soumak Biswas
Department of Mathematics
Indian Institute of Technology Roorkee
Roorkee-247667, India
Email address: soumak.math@gmail.com