Filomat 34:12 (2020), 4199–4214
https://doi.org/10.2298/FIL2012199K

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

Ideal Structure of $\mathbb{Z}_q + u\mathbb{Z}_q$ and $\mathbb{Z}_q + u\mathbb{Z}_q$-Cyclic Codes

Raj Kumar[a], Maheshanand Bhaintwal[a], Ramakrishna Bandi[b]

[a]*Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee, India*
[b]*Department of Mathematics, International Institute of Information Technology, Naya Raipur, India*

Abstract. In this paper, we study cyclic codes of length n over $R = \mathbb{Z}_q + u\mathbb{Z}_q$, $u^2 = 0$, where q is a power of a prime p and $(n, p) = 1$. We have determined the complete ideal structure of R. Using this, we have obtained the structure of cyclic codes and that of their duals through the factorization of $x^n - 1$ over R. We have also computed total number of cyclic codes of length n over R. A necessary and sufficient condition for a cyclic code over R to be self-dual is presented. We have presented a formula for the total number of self-dual cyclic codes of length n over R. A new Gray map from R to $\mathbb{Z}_p^{2r}$ is defined. Using Magma, some good cyclic codes of length 4 over $\mathbb{Z}_9 + u\mathbb{Z}_9$ are obtained.

1. Introduction

The idea of finding good binary codes via the Gray map has inspired many researchers to study codes over finite rings. This idea originated with the breakthrough paper of Hammons et al. [13], wherein it was shown that some well known binary non-linear codes are actually images of some linear codes over $\mathbb{Z}_4$ under the Gray map. Cyclic codes are among the most studied families of codes because of their rich algebraic structure and their relatively efficient encoding and decoding methods. Cyclic codes have been also studied extensively over various finite rings. Their structure over finite chain rings is now well known [8, 16].

Bonnecaze and Udaya [6] have studied cyclic codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, $u^2 = 0$, and provided their basic framework. They have also shown that there exist codes over $\mathbb{F}_2 + u\mathbb{F}_2$ which have better parameters than the corresponding best known codes over $\mathbb{Z}_4$. This initiated the study of cyclic codes over other similar rings such as $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, $u^2 = v^2 = 0, uv = vu$, [25]; $\mathbb{F}_2 + v\mathbb{F}_2$, $v^2 = v$, [26]; $\mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{k-1}\mathbb{F}_q$, $u^k = 0$, [1, 17] etc. Shi et al. [19] have constructed an infinite family of two Lee-weight codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, $u^2 = 0$. In [20], Shi et al. have constructed two new infinite families of trace codes of dimension $2m$ over the ring $\mathbb{F}_p + u\mathbb{F}_p$, $u^2 = u$, where p is an odd prime. Recently, the rings such as $\mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$ [24] and $\mathbb{Z}_4 + v\mathbb{Z}_4$, $v^2 = v$ [4, 5] have been introduced to construct good codes. Yildiz and Karadeniz [24] have studied linear codes and self-dual codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$. Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ have been studied in [2, 3, 23]. Luo and Parampalli [14] have studied the structure of self-dual cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and obtained some good self-dual cyclic codes over $\mathbb{Z}_4$ via the Gray map. Shi et al. [18] have studied

2010 *Mathematics Subject Classification*. 94B05, 94B15
Keywords. cyclic codes, codes over rings, self-dual codes
Received: 30 December 2019; Revised: 14 April 2020; Accepted: 16 June 2020
Communicated by Paola Bonacini
Research supported by the Ministry of Human Resource Development (MHRD), Govt. of India
Email addresses: raj.k1993@yahoo.com (Raj Kumar), mahesfma@iitr.ac.in (Maheshanand Bhaintwal), ramakrishna@iiitnr.edu.in (Ramakrishna Bandi)

constacyclic codes over $\mathbb{Z}_4[u]/\left\langle u^2-1\right\rangle$ with their Gray images. Cao and Li [7] have studied cyclic codes of odd length over $\mathbb{Z}_4[u]/\left\langle u^k\right\rangle$.

In this paper, we study cyclic codes of length n over $R = \mathbb{Z}_q + u\mathbb{Z}_q$, $u^2 = 0$, where q is a power of a prime p with $(n, p) = 1$. For this, we have first determined the complete ideal structure of R, and then using it, we have obtained the structure of cyclic codes of length n over R, i.e., the ideal structure of $R[x]/\langle x^n - 1\rangle$, through the factorization of $x^n - 1$ over R. We also find the duals of cyclic codes over R and determine a necessary and sufficient condition for a cyclic code to be self-dual. Formulas for counting total number of cyclic codes and total number of self-dual cyclic codes of length n over R are presented. We have defined a new Gray map from R to $\mathbb{Z}_p^{2r}$. Some good cyclic codes of length 4 over $\mathbb{Z}_9 + u\mathbb{Z}_9$ are obtained using the computer algebra system Magma.

Gao et al. [11] have also studied cyclic codes of length n over R. Dinh et al. [9, 10] have studied cyclic codes over the ring $\mathbb{Z}_{2^s}[u]/\langle u^k\rangle$ as well as over the ring $GR(p^e, m)[u]/\langle u^k\rangle$. However, our approach for obtaining cyclic codes over R is different from the ones given in [11], [9] or [10]. We first establish the complete ideal structure of R and then obtain the structure of cyclic codes over R using this ideal structure. Moreover, we have also studied self-dual cyclic codes over R and have enumerated the ideals of R, and the cyclic codes and self-dual cyclic codes of length n over R. An ideal structure of R has been presented in [12] also, but this ideal structure is incomplete.

The paper is organized as follows: In Section 2, we determine the complete ideal structure of R. Section 3 describes the algebraic structure of cyclic codes and gives a formula for total number of cyclic codes over R. In Section 4, we study duals of cyclic codes over R, and determine a necessary and sufficient condition for a cyclic code over R to be a self-dual. We also count the total number of self-dual cyclic codes of length n over R. A new Gray map from R to $\mathbb{Z}_p^{2r}$ is defined and some examples of good cyclic codes of length 4 over $\mathbb{Z}_9 + u\mathbb{Z}_9$ are presented.

2. The ring $\mathbb{Z}_q + u\mathbb{Z}_q$ and its ideal structure

Throughout the paper, R denotes the ring $\mathbb{Z}_q + u\mathbb{Z}_q = \{a + ub \mid a, b \in \mathbb{Z}_q\}$ with $u^2 = 0$, $q = p^r$, p a prime and r a positive integer. R can be viewed as the quotient ring $\mathbb{Z}_q[u]/\left\langle u^2\right\rangle$.

In this section, we discuss properties of the ring R and obtain its complete ideal structure. We also determine the cardinalities of the ideals of R and their annihilators.

Lemma 2.1. *An element $a + ub \in R$ is a unit in R if and only if a is a unit in $\mathbb{Z}_q$.*

Proof. Let $a_1 + ub_1$ be a unit in R. Then there exists an element $a_2 + ub_2$ such that $(a_1 + ub_1)(a_2 + ub_2) = 1$, which implies that $a_1a_2 + u(a_1b_2 + a_2b_1) = 1$, from which we get $a_1a_2 = 1$. Therefore a_1 is a unit in $\mathbb{Z}_q$.

Conversely let $a \in \mathbb{Z}_q$ be a unit in $\mathbb{Z}_q$. Suppose that $a + ub \in R$ is a non-unit for some $b \in \mathbb{Z}_q$. Then there exists a non-zero element $c + ud \in R$ such that $(a + ub)(c + ud) = 0$. This implies that $ac = 0$ and $ad + bc = 0$. Now if $c \neq 0$, then $ac = 0$ contradicts the fact that a is a unit in $\mathbb{Z}_q$. If $c = 0$, then $d \neq 0$ and $ad = 0$, which again contradicts the fact that a is a unit. Therefore $a + ub$ must be a unit. Hence the result. □

Thus the set of units of R is $R^* = \{a + ub : a \text{ is a unit in } \mathbb{Z}_q\}$. The set of non-units of R forms an ideal of R, generated by p and u, i.e., the ideal $\langle p, u\rangle$. For if $a + ub$ is any non-unit in R, with $a, b \in \mathbb{Z}_q$, then a is a non-unit in $\mathbb{Z}_q$, and so $a = pc$ for some $c \in \mathbb{Z}_q$. Hence $a + ub \in \langle p, u\rangle$. As $\langle p, u\rangle$ does not contain any unit, it contains precisely the non-units of R. Thus R is a local ring with its unique maximal ideal $\langle p, u\rangle$. Further, R is a non-chain ring as $\langle p, u\rangle$ is not a principal ideal.

Now we determine the structure of ideals of $R = \mathbb{Z}_q + u\mathbb{Z}_q$.

Let I be any ideal of R. Define $\Phi : I \to \mathbb{Z}_q$ such that $\Phi(a + ub) = a$. Clearly Φ is a ring homomorphism with the kernel

$$\text{Ker } \Phi = \{ub \in I \mid b \in \mathbb{Z}_q\}\,.$$

Define $J = \{b \in \mathbb{Z}_q \mid ub \in I\}$. Then J is an ideal of $\mathbb{Z}_q$. So, $J = \langle p^j \rangle$ for some j, $0 \le j \le r$, and hence Ker $\Phi = \langle up^j \rangle$. It is easy to verify that $\Phi(I)$ is also an ideal of $\mathbb{Z}_q$. So, $\Phi(I) = \langle p^i \rangle$, $0 \le i \le r$. Therefore, $I = \langle p^i + u\alpha, up^j \rangle$, where $\alpha \in \mathbb{Z}_q$, $0 \le i, j \le r$. Now since $up^i = u(p^i + u\alpha) \in I$, we have $up^i \in$ Ker Φ, which implies that $p^j \mid p^i$ and hence $j \le i$. Thus

$$I = \langle p^i + u\alpha, up^j \rangle, \ \ \alpha \in \mathbb{Z}_q, \ \ 0 \le i \le r, \ 0 \le j \le i \ .$$

Now an element $\alpha \in \mathbb{Z}_q$ can be written in p-adic representation as $\alpha = \sum_{k=0}^{r-1} a_k p^k$, where $a_k \in \mathbb{Z}_p$. If $a_0 \neq 0$, then α is a unit. Otherwise α is a non-unit. If $\alpha \neq 0$ and t is the smallest non-negative integer such that $a_t \neq 0$, then α can be written as $\alpha = p^t a$, where $a = \sum_{k=t}^{r-1} a_k p^{k-t}$, $0 \le t \le r-1$. Clearly a is a unit. Thus any $\alpha \in \mathbb{Z}_q$ is either zero or can be written as $\alpha = p^t a$, where a is a unit and $0 \le t \le r-1$. Therefore an ideal I of R can be written either as

$$I = \langle p^i, up^j \rangle, \qquad 0 \le j \le i \le r \ ,$$

or as

$$I = \langle p^i + up^t a, up^j \rangle, \qquad 0 \le j \le i \le r, \quad 0 \le t \le r-1 \ ,$$

where a is a unit. Further, if $j = i$, then I is a principal ideal — in the first case $I = \langle p^i \rangle$ and in the second case $I = \langle p^i + up^t a \rangle$. Also, when $i = r$, I is again a principal ideal. Therefore, for I to be a non-principal ideal, we must have $j < i \le r-1$.

Lemma 2.2. *Let $I = \langle p^i + up^t a \rangle$, where a is a unit in $\mathbb{Z}_q$. Then the smallest non-negative integer T such that $up^T \in I$ is $T = \min\{i, \ r - i + t\}$.*

Proof. We have $u(p^i + up^t a) = up^i \in I$ and $p^{r-i}a^{-1}(p^i + up^t a) = up^{r-i+t} \in I$. Since T is the smallest non-negative integer such that $up^T \in I$, it follows that $T \le \min\{i, r-i+t\}$. Again since $up^T \in I$, $up^T = (p^i + up^t a)(q_1 + uq_2)$ for some $q_1 + uq_2 \in \mathbb{Z}_q + u\mathbb{Z}_q$. This implies that $p^i q_1 = 0$, and from this follows that $q_1 = p^{r-i} q_3$ for some $q_3 \in \mathbb{Z}_q$. Now $up^T = up^i q_2 + up^{r-i+t} a q_3 = up^{\min\{i,r-i+t\}}(p^{i-\min\{i,r-i+t\}} q_2 + a q_3 p^{r-i+t-\min\{i,r-i+t\}})$. Therefore $p^T \in \langle p^{\min\{i,r-i+t\}} \rangle$, which implies that $p^{\min\{i,r-i+t\}} \mid p^T$, and so $T \ge \min\{i, r-i+t\}$. Hence $T = \min\{i, r-i+t\}$. □

In Theorem 2.3 and Theorem 2.4 below, we present distinct principal ideals and distinct non-principal ideals, respectively, of R.

Theorem 2.3. *The distinct principal ideals of R are:*

1. $\langle p^i \rangle$, $0 \le i \le r$.
2. $\langle up^j \rangle$, $0 \le j \le r-1$.
3. $\langle p^i + up^t a \rangle$, $1 \le i \le r-1$, $0 \le t \le i-1$, *where* $a = \sum_{k=t}^{T-1} a_k p^{k-t}$, *a unit in* $\mathbb{Z}_q$, *and* $T = \min\{i, \ r-i+t\}$.

Proof. The first two parts are straightforward. We prove (3). Let I be an ideal of R of the form $\langle p^i + up^t \alpha \rangle$, $1 \le i \le r-1$, where $\alpha \in \mathbb{Z}_q$ is a unit and $\alpha = \sum_{k=t}^{r-1} a_k p^{k-t}$. We first show that $t < i$. Suppose $i \le t$. Then $p^i + up^t \alpha = p^i(1 + p^{t-i} u\alpha)$. Since $1 + p^{t-i} u\alpha$ is a unit in R, $\langle p^i + up^t \alpha \rangle = \langle p^i \rangle$. As the ideals $\langle p^i \rangle$ are covered in part (1), for the ideals to be distinct, we must have $t < i$. Also, $t < r-i+t$, as $r > i$. Therefore, $t < T = \min\{i, \ r-i+t\}$.

Now

$$\begin{aligned}
p^i + up^t \alpha &= p^i + up^t \sum_{k=t}^{r-1} a_k p^{k-t} \\
&= p^i + u\left(a_t p^t + a_{t+1} p^{t+1} + \cdots + a_T p^T + \cdots + a_{r-1} p^{r-1}\right) \\
&= p^i + u\left(a_t p^t + a_{t+1} p^{t+1} + \cdots + a_{T-1} p^{T-1}\right) + up^T \left(a_T + \cdots + a_{r-1} p^{r-T-1}\right) \\
&= p^i + up^t \sum_{k=t}^{T-1} a_j p^{j-t} + \delta(p^i + up^t \alpha)(a') \ ,
\end{aligned}$$

where $a' = a_T + \cdots + a_{r-1}p^{r-T-1}$, T is as defined in Lemma 2.2, and

$$\delta = \begin{cases} u & \text{if } T = i\,, \\ p^{r-i}\alpha^{-1} & \text{if } T = r-i+t\,. \end{cases}$$

Then we get

$$(p^i + up^t\alpha)(1-\delta a') = p^i + up^t \sum_{k=t}^{T-1} a_k p^{k-t}\,.$$

Since $1-\delta a'$ is a unit in R for each of the possible values of δ, we get $\langle p^i + up^t\alpha\rangle = \langle p^i + up^t \sum_{k=t}^{T-1} a_k p^{k-t}\rangle = \langle p^i + up^t a\rangle$, where $a = \sum_{k=t}^{T-1} a_k p^{k-t}$. Clearly a is a unit. Thus I can be written in the required form.

Now we shall show that the ideals $\langle p^i + up^t a\rangle$ are distinct for distinct values of i, t and a.

Case 1. Suppose $\langle p^i + up^t a\rangle = \langle p^j + up^s b\rangle$ for some $i \neq j$, $1 \leq i, j \leq r-1$, with a, b units in $\mathbb{Z}_q$. Then $\Phi\left(\langle p^i + up^t a\rangle\right) = \Phi\left(\langle p^j + up^s b\rangle\right)$, where Φ is the map as defined above. This implies that $\langle p^i\rangle = \langle p^j\rangle$, which is a contradiction, as $\langle p^i\rangle$ and $\langle p^j\rangle$ are distinct ideals of $\mathbb{Z}_q$ for $i \neq j$.

Case 2. Suppose for any fixed i and $t \neq s$, $\langle p^i + up^t a\rangle = \langle p^i + up^s b\rangle$, where a, b units in $\mathbb{Z}_q$. We may assume that $t < s$. Then $(p^i + up^t a) = (c + ud)(p^i + up^s b)$ for some $c + ud \in R$. This implies that $c = 1 + p^{r-i}q'$ for some $q' \in \mathbb{Z}_q$, and $p^t a = p^s b(1 + p^{r-i}q') + p^i d$. Then

$$p^t a - p^s b = p^{r-i+s} bq' + p^i d\,,$$

which implies that

$$p^t(a - bp^{s-t}) = p^{r-i+s} bq' + p^i d\,.$$

Since $t < s$ and a is a unit, $a - bp^{s-t}$ is a unit in $\mathbb{Z}_q$. As $r - i + s > t$ and $i > t$, the above relation leads to a contradiction. Therefore, we must have $\langle p^i + p^t au\rangle \neq \langle p^i + p^s bu\rangle$.

Case 3. Suppose for some fixed i and t, we have

$$\langle p^i + p^t au\rangle = \langle p^i + p^t bu\rangle\,,$$

where $a = \sum_{k=t}^{T-1} a_k p^{k-t}$, $b = \sum_{k=t}^{T-1} b_k p^{k-t}$ are units in $\mathbb{Z}_q$. Clearly $0 \leq a,\ b \leq p^{T-t} - 1$. We have $(p^i + p^t au) = (c + du)(p^i + p^t bu)$ for some $c + du \in R$. This implies that $c = 1 + p^{r-i}q'$ for some $q' \in \mathbb{Z}_q$, and $p^t a = p^t b(1 + p^{r-i}q') + p^i d$. It follows that $p^{\min\{i,\ r-i+t\}} \mid p^t(a-b)$, i.e., $p^{T-t} \mid (a-b)$. Since $0 \leq a,\ b < p^{T-t}$, we must have $a = b$.

Now we show that none of the ideals in part (1) and part (2) are covered by the ideals in part (3). Let $I = \langle p^i + up^t a\rangle$, with above conditions on i, t and a. First we observe that I is not the zero ideal $\langle p^r\rangle$, as $i \geq 1$. Now suppose $I = \langle p^j\rangle$ for some $0 \leq j \leq r-1$. Then $(p^i + up^t a) \mid p^j$ and $p^j \mid (p^i + up^t a)$, from which we get $i \leq j$ and $j \leq t$, respectively. Thus we get $i \leq j \leq t$, a contradiction, as $t < i$. Thus ideals in part (1) are not covered by the ideals in part (3). Next it is easy to see that I cannot be equal to an ideal of the form $\langle up^j\rangle$, $0 \leq j \leq r-1$, as $i \geq 1$. Therefore, the ideals in part (2) are also not covered by the ideals in part (3). Hence the result. □

Now we consider the non-principal ideals of R.

Theorem 2.4. *The distinct non-principal ideals of R are*

1. $\langle p^i,\ up^j\rangle$, *where* $0 \leq j < i \leq r-1$.

2. $\langle p^i + up^t a,\ up^j\rangle$, $2 \le i \le r-2$, $0 \le t \le i-2$, $t < j < T$, *where* $T = \min\{i,\ r-i+t\}$, *and* $a = \sum_{k=t}^{j-1} a_k p^{k-t}$, *a unit in* $\mathbb{Z}_q$.

Proof. From Section 2, a non-principal ideal of R is either of the form $\langle p^i,\ up^j\rangle$ or of the form $\langle p^i + up^t a, up^j\rangle$, where $0 \le j < i \le r-1$ and a is a unit. Since $\langle p^i,\ up^j\rangle$ is always non-principal for $j < i$, case (1) is therefore clear. For case (2), let I be an ideal of R of the form $I = \langle p^i + up^t a, up^j\rangle$, where $0 \le j < i \le r-1$ and a is a unit. Then from Lemma 2.2, $up^T \in \langle p^i + up^t a\rangle$. Therefore, if $j \ge T$, then $up^j \in \langle p^i + up^t a\rangle$ and hence $\langle p^i + up^t a, up^j\rangle = \langle p^i + up^t a\rangle$ is a principal ideal. Hence for I to be a non-principal ideal, we must have $j < T$. Now suppose $j \le t$. Then $\langle p^i + up^t a,\ up^j\rangle = \langle p^i,\ up^j\rangle$, as $up^t a \in \langle up^j\rangle$. Since the ideals $\langle p^i,\ up^j\rangle$ have already been considered, for I to be distinct from such ideals, we must have $j > t$. Thus $t < j < T$. Now we show that for any j with $t < j < T$, I cannot be a principal ideal. First we observe that any principal ideal of R can be expressed as $I_1 = \langle p^\ell + up^s b\rangle$, $0 \le \ell \le r$, $0 \le s < \ell$, where b is a unit or zero. Now suppose $I = I_1$. Then $p^\ell + up^s b \in I$ implies that $i \le \ell$, and $p^i + up^t a \in I_1$ implies that $\ell \le i$. Thus we get $\ell = i$, and so $I_1 = \langle p^i + up^s b\rangle$. Now if $b = 0$, then $I_1 = \langle p^i\rangle$ and then $up^j \in I_1$ implies that $j \ge \ell = i$, a contradiction, as $i \ge T$ and $T > j$. Now let b be a unit. Then $I = I_1$ implies that $p^i + up^t a = (\alpha + u\beta)(p^i + up^s b)$ for some $\alpha + u\beta \in R$. From this follows that $\alpha = 1 + p^{r-i}\gamma$ for some $\gamma \in \mathbb{Z}_q$ and $p^t a = \beta p^i + \alpha p^s b$. This implies that $p^t a = p^s(\beta p^{i-s} + \alpha b)$. Since α and b are units and $s < i$, $\beta p^{i-s} + \alpha b$ is a unit. As a is a unit, it follows that $s = t$, so that $I_1 = \langle p^i + up^t b\rangle$. From Lemma 2.2, T is the smallest non-negative integer such that $up^T \in I_1$. Then $up^j \in I_1$ implies that $j \ge T$, a contradiction. Hence $I \ne I_1$.

Now if $i = r-1$, then $T = \min\{r-1, r-(r-1)+t\} = t+1$, and so there is no integer j in this case satisfying $t < j < T$. Therefore, we must have $i \le r-2$. Also, as $i \ge T$, it follows from $t < j < T$ that $t \le i-2$ and $i \ge 2$. □

Summarizing the above results, we present the complete ideal structure of R in the following theorem.

Theorem 2.5. *The distinct ideals of R are:*

1. *Principal ideals:*
   (i) $\langle p^i\rangle$, $0 \le i \le r$.
   (ii) $\langle up^j\rangle$, $0 \le j \le r-1$.
   (iii) $\langle p^i + up^t a\rangle$, $1 \le i \le r-1$, $0 \le t \le i-1$, *where* $a = \sum_{k=t}^{T-1} a_k p^{k-t}$ *is a unit in* $\mathbb{Z}_q$, *and* $T = \min\{i,\ r-i+t\}$.
2. *Non-principal ideals:*
   (i) $\langle p^i,\ up^j\rangle$, $0 \le j < i \le r-1$.
   (ii) $\langle p^i + up^t a,\ up^j\rangle$, $2 \le i \le r-2$, $0 \le t \le i-2$, $t < j < T$, *where* $T = \min\{i,\ r-i+t\}$, *and* $a = \sum_{k=t}^{j-1} a_k p^{k-t}$, *a unit in* $\mathbb{Z}_q$.

Now we determine the cardinalities of the ideals of R.

Theorem 2.6. *The cardinalities of the ideals of R are given as follows:*

1. *Principal ideals:*
   (i) $|\langle p^i\rangle| = p^{2r-2i}$, $0 \le i \le r$.
   (ii) $|\langle up^j\rangle| = p^{r-j}$, $0 \le j \le r-1$.
   (iii)
$$|\langle p^i + up^t a\rangle| = p^{2r-i-T} = \begin{cases} p^{2r-2i}, & \text{for } i \le \left\lfloor \frac{r+t}{2} \right\rfloor, \\ p^{r-t}, & \text{for } i > \left\lfloor \frac{r+t}{2} \right\rfloor, \end{cases}$$
   where a is a unit.
2. *Non-principal ideals:*
   (i) $|\langle p^i, up^j\rangle| = p^{2r-i-j}$.
   (ii) $|\langle p^i + up^t a, up^j\rangle| = p^{2r-i-j}$, a is a unit.

Proof. Let I be any ideal of R. Recall the map $\Phi : I \to \mathbb{Z}_q$ such that $\Phi(a + ub) = a$. Since Φ is a ring homomorphism, $I/\text{Ker } \Phi \cong \Phi(I)$. This implies that $|I| = |\Phi(I)||\text{Ker } \Phi| = |\Phi(I)||J|$, where J is as defined in Section 2, namely $J = \{b \in \mathbb{Z}_q \mid ub \in I\}$. Since both $\Phi(I)$ and J are ideals of $\mathbb{Z}_q$, $\Phi(I) = \langle p^{l_1} \rangle$ and $J = \langle p^{l_2} \rangle$ for some l_1 and l_2, $0 \le l_1, l_2 \le r$, and so $|\Phi(I)| = p^{r-l_1}$ and $|J| = p^{r-l_2}$. Now we compute the cardinalities of ideals as follows.

1. If $I = \langle p^i \rangle$, then $\Phi(I) = \langle p^i \rangle$, and Ker $\Phi = \langle up^i \rangle$. So $J = \langle p^i \rangle$. Therefore $|I| = p^{2r-2i}$.
2. If $I = \langle up^j \rangle$, then $\Phi(I) = \langle 0 \rangle$, and Ker $\Phi = \langle up^j \rangle$, and so $J = \langle p^j \rangle$. Therefore $|I| = p^{r-j}$.
3. If $I = \langle p^i + uap^t \rangle$, where a is a unit, then $\Phi(I) = \langle p^i \rangle$, and from Lemma 2.2, Ker $\Phi = \langle up^T \rangle$. So $J = \langle p^T \rangle$, where $T = \min\{i,\ r - i + t\}$. Therefore $|I| = p^{r-i}p^{r-T} = p^{2r-i-T}$.
4. If $I = \langle p^i + uap^t,\ up^j \rangle$, where a is a unit or zero, then $\Phi(I) = \langle p^i \rangle$ and Ker $\Phi = \langle up^j \rangle$, and so $J = \langle p^j \rangle$. Therefore $|I| = p^{2r-i-j}$.

□

In the following theorem we count the ideals of R.

Theorem 2.7. *The number of distinct ideals of R is*

$$N = \frac{p^{\lfloor \frac{r}{2} \rfloor + 2} + 3p^{r - \lfloor \frac{r}{2} \rfloor + 1} - 4p^2}{(p-1)^2} + \frac{\left(2\left\lfloor \frac{r}{2} \right\rfloor - r\right)p^{r - \lfloor \frac{r}{2} \rfloor} + (3-2r)p}{(p-1)} + 2r + 1.$$

Proof. We count the total number of ideals of R in the following cases. For convenience, we denote $\left\lfloor \frac{r}{2} \right\rfloor$ by ν.

Case (i): The number of ideals of the form $\langle p^i \rangle$, $0 \le i \le r$, is $r + 1$.

Case (ii): The number of ideals of the form $\langle up^i \rangle$, $0 \le i \le r - 1$, is r.

Case (iii): The number of ideals of the form $\langle p^i + up^t a \rangle$, with $a = \sum_{k=t}^{T-1} a_k p^{k-t}$, a unit in $\mathbb{Z}_q$, $1 \le i \le r-1$, $0 \le t \le i-1$ and $T = \min\{i,\ r - i + t\}$, is

$$\begin{aligned}
N_1 &= \sum_{i=1}^{\nu}\sum_{t=0}^{i-1}(p-1)p^{i-t-1} + \sum_{i=\nu+1}^{r-1}\left[\sum_{t=0}^{2i-r-1}(p-1)p^{r-i-1} + \sum_{t=2i-r}^{i-1}(p-1)p^{i-t-1}\right] \\
&= \sum_{i=1}^{\nu}(p^i - 1) + \sum_{i=\nu+1}^{r-1}\left[(p-1)p^{r-i-1}(2i-r) + (p^{r-i} - 1)\right] \\
&= \frac{p^{\nu+1} - p}{p-1} - \nu + 2\left[p\left(\frac{p^{r-\nu-2} - 1}{p-1}\right) - (r-1) + (\nu+1)\,p^{r-\nu-1}\right] - r\left(p^{r-\nu-1} - 1\right) \\
&\quad + \left(\frac{p^{r-\nu} - p}{p-1} - (r - \nu - 1)\right) \\
&= \frac{p^{\nu+1} - p}{p-1} + 2\left[p\left(\frac{p^{r-\nu-2} - 1}{p-1}\right) - (r-1) + (\nu+1)\,p^{r-\nu-1}\right] - rp^{r-\nu-1} + \frac{p^{r-\nu} - p}{p-1} + 1.
\end{aligned}$$

Case (iv): Any non-principal ideal of R can be expressed as $\langle p^i + up^t a,\ up^j \rangle$, $2 \le i \le r-2$, $0 \le t \le i-2$, $T = \min\{i,\ r - i + t\}$, $t < j < T$ and $a = \sum_{k=t}^{T-1} a_k p^{k-t}$ is a unit or zero. When $a = 0$ there are $\sum_{i=1}^{r-1} i = \frac{r(r-1)}{2}$ ideals

of this type. When a is a unit, the number of such ideals is given by

$$\begin{aligned}
N_2' &= \sum_{i=2}^{v}\sum_{t=0}^{i-2}\sum_{j=1+t}^{i-1}(p-1)p^{j-t-1} + \sum_{i=v+1}^{r-2}\left[\sum_{t=0}^{2i-r-1}\sum_{j=1+t}^{r-i+t-1}(p-1)p^{j-t-1} + \sum_{t=2i-r}^{i-2}\sum_{j=1+t}^{i-1}(p-1)p^{j-t-1}\right]\\
&= \sum_{i=2}^{v}\sum_{t=0}^{i-2}(p^{i-t-1}-1) + \sum_{i=v+1}^{r-2}\left[\sum_{t=0}^{2i-r-1}(p^{r-i-1}-1) + \sum_{t=2i-r}^{i-2}(p^{i-t-1}-1)\right]\\
&= \sum_{i=2}^{v}\left[\frac{p^i-p}{p-1}-(i-1)\right] + \sum_{i=v+1}^{r-2}\left[(p^{r-i-1}-1)(2i-r)\right] + \sum_{i=v+1}^{r-2}\left[\frac{p^{r-i}-p}{p-1}-(r-i-1)\right]\\
&= \sum_{i=2}^{v}\left[\frac{p^i-p}{p-1}-(i-1)\right] + \frac{1}{p-1}\left[2\left\{\left(\frac{p^{r-v-1}-p^2}{p-1}\right)-(r-2)p+(v+1)p^{r-v-1}\right\}-r\left(p^{r-v-1}-p\right)\right]\\
&\quad + \left[-2\left(\frac{(r-2)(r-1)}{2}-\frac{(v)(v+1)}{2}\right)+r(r-v-2)\right] + \sum_{i=v+1}^{r-2}\left[\frac{p^{r-i}-p}{p-1}-(r-i-1)\right]\\
&= \left(\frac{p^{v+1}-p^2}{(p-1)^2}\right)-\left[\frac{p}{p-1}(v-1)\right]-\left(\frac{(v)(v+1)}{2}-1\right)+(v-1)\\
&\quad + \frac{1}{p-1}\left[2\left\{\left(\frac{p^{r-v-1}-p^2}{p-1}\right)-(r-2)p+(v+1)p^{r-v-1}\right\}-r\left(p^{r-v-1}-p\right)\right]\\
&\quad + \left[-2\left(\frac{(r-2)(r-1)}{2}-\frac{(v)(v+1)}{2}\right)+r(r-v-2)\right]\\
&\quad + \left[\left(\frac{p^{r-v}-p^2}{(p-1)^2}\right)+\left(-\frac{p}{p-1}-r+1\right)(r-v-2)+\left(\frac{(r-2)(r-1)}{2}\right)-\left(\frac{(v)(v+1)}{2}\right)\right]\\
&= \frac{1}{p-1}\left[2\left\{\left(\frac{p^{r-v-1}-p^2}{p-1}\right)-(r-2)p+(v+1)p^{r-v-1}\right\}-r\left(p^{r-v-1}-p\right)\right]+\left(\frac{p^{r-v}-p^2}{(p-1)^2}\right)\\
&\quad + \left(-\frac{p}{p-1}+1\right)(r-v-2)-\left(\frac{(r-2)(r-1)}{2}\right)+\frac{p^{v+1}-p^2}{(p-1)^2}-\frac{p}{(p-1)}(v-1)+v.
\end{aligned}$$

Therefore total number of non-principal ideals of R is

$$N_2 = N_2' + \frac{r(r-1)}{2}.$$

Adding the number of ideals in Case (i), Case (ii), Case (iii) and Case (iv), and substituting $\left\lfloor \frac{r}{2} \right\rfloor$ for v, we get the total number of ideals N of R. □

Example 2.8. *If $p = 2, r = 2$, then $R = \mathbb{Z}_4 + u\mathbb{Z}_4$. Then from Theorem 2.7, we have $N = 7$. It can be easily verified from [24] that R has 7 distinct ideals which are: $\langle 0\rangle, \langle 1\rangle, \langle 2\rangle, \langle u\rangle, \langle 2u\rangle, \langle 2+u\rangle$, and $\langle 2, u\rangle$.*

Example 2.9. *If $p = 3, r = 2$, then from Theorem 2.7, there are total 8 ideals of $R = \mathbb{Z}_9 + u\mathbb{Z}_9$, which are: $\langle 0\rangle, \langle 1\rangle, \langle 3\rangle, \langle u\rangle, \langle 3u\rangle, \langle 3+u\rangle, \langle 3+2u\rangle$, and $\langle 3, u\rangle$.*

Example 2.10. *Consider R with $p = 3, r = 5$, i.e., the ring $\mathbb{Z}_{3^5} + u\mathbb{Z}_{3^5}$. Then the ideals of R are as given below: Principal ideals:*

(i) $\langle p^i\rangle$, $0 \le i \le r$: $\langle 3^i\rangle$, $0 \le i \le 5$.

(ii) $\langle up^j\rangle$, $0 \le j \le r-1$: $\langle 3^j u\rangle$, $0 \le j \le 4$.

(iii) $\langle p^i + up^t a\rangle$, $1 \le i \le r-1$, $0 \le t \le T-1$, *where* $T = \min\{i,\ r-i+t\}$ *and* $a = \sum_{j=t}^{T-1} a_j p^{j-t}$ *is a unit in $\mathbb{Z}_q$. These ideals are given in Table 1.*

i	$r-i$	t	T	Ideal	a
1	4	0	1	$\langle 3+au\rangle$	1, 2
2	3	0	2	$\langle 3^2+au\rangle$	$1 \le a \le 8,\ a \ne 3,6$
		1		$\langle 3^2+3au\rangle$	1, 2
3	2	0	2	$\langle 3^3+au\rangle$	$1 \le a \le 8,\ \ a \ne 3,6$
		1	3	$\langle 3^3+3au\rangle$	
		2		$\langle 3^3+3^2au\rangle$	1, 2
4	1	0	1	$\langle 3^4+au\rangle$	1, 2
		1	2	$\langle 3^4+3au\rangle$	
		2	3	$\langle 3^4+3^2au\rangle$	
		3	4	$\langle 3^4+3^3au\rangle$	

Table 1: Principal ideals of $\mathbb{Z}_{3^5}+u\mathbb{Z}_{3^5}$

Non-principal ideals:

(i) *The non-principal ideals* $\langle p^i+up^ta,\ p^ju\rangle$ *when* $a=0$, *i.e.,* $\langle p^i,\ p^ju\rangle$ *are :*

$$\langle 3,u\rangle, \langle 3^2,u\rangle, \langle 3^3,u\rangle, \langle 3^4,u\rangle, \langle 3^2,3u\rangle, \langle 3^3,3u\rangle, \langle 3^3,3^2u\rangle, \langle 3^4,3u\rangle, \langle 3^4,3^2u\rangle, \langle 3^4,3^3u\rangle\ .$$

(ii) $\langle p^i+up^ta,\ p^ju\rangle$, $2\le i\le r-2$, $0\le t\le i-2$, $t<j<T$, *where* $T=\min\{i,\ r-i+t\}$, *and* $a=\sum_{k=t}^{j-1}a_kp^{k-t}$ *is a unit in* $\mathbb{Z}_q$. *These ideals are given in Table 2.*

i	$r-i$	t	T	j	Ideal	a
2	4	0	2	1	$\langle 3^2+au, 3u\rangle$	1, 2
3	2	0	2	1	$\langle 3^3+au, 3u\rangle$	
		1		2	$\langle 3^3+3au, 3^2u\rangle$	

Table 2: Non-principal ideals of $\mathbb{Z}_{3^5}+u\mathbb{Z}_{3^5}$.

3. Cyclic codes over R

In this section we study the structure of cyclic codes of length n over R, where $(n,p)=1$. This structure is established by using the ideal structure of R and the factorization of x^n-1 into monic pairwise coprime basic irreducible polynomials over R.

A cyclic shift on R^n is a permutation σ of R^n such that

$$\sigma(c_0,c_1,\ldots,c_{n-1})=(c_{n-1},c_0,\ldots,c_{n-2})\ .$$

A linear code C over R is called a cyclic code, or an R-cyclic code, if it is invariant under the cyclic shift σ, i.e., $\sigma(C)=C$. If the elements of R^n are represented as polynomials of degree at most $n-1$ over R, then it is well known that a subset C of R^n is a cyclic code over R if and only if C is an ideal of the quotient ring $\frac{R[x]}{\langle x^n-1\rangle}$.

Recall that R is a local ring with the unique maximal ideal $\langle p,u\rangle$. We denote the residue field $\frac{R}{\langle p,u\rangle}$ of R by $\overline{R}$. Further, we have $\overline{R}=\frac{R}{\langle p,u\rangle}=\mathbb{F}_p$. The image of any element $a\in R$ under the projection map $\mu: R\to\overline{R}$ is denoted by $\overline{a}$. The map μ is extended to $R[x]\to\overline{R}[x]$ in the usual way. The image of an element $f(x)\in R[x]$ in $\overline{R}[x]$ under this projection is denoted by $\overline{f}(x)$. A polynomial $f(x)\in R[x]$ is called *basic irreducible* if $\overline{f}(x)$ is an irreducible polynomial in $\overline{R}[x]$.

Lemma 3.1. *[11, Lemma 3] Two polynomials $f(x)$ and $g(x)$ of $R[x]$ are coprime if and only if $f(x)$ and $g(x)$ are coprime over $\overline{R}$.*

Now we present the ideal structure of the Galois extension ring $\frac{R[x]}{\langle f\rangle} \simeq \frac{\mathbb{Z}_q[x]}{\langle f\rangle} + u\frac{\mathbb{Z}_q[x]}{\langle f\rangle}$ of R, where f is a basic irreducible polynomial of degree d over $\mathbb{Z}_q$, and enumerate the total number of ideals of $\frac{R[x]}{\langle f\rangle}$. We use the ideal structure of R to obtain the ideal structure of $\frac{R[x]}{\langle f\rangle}$. Now, as in the case of ideals of R (described in Section 2), for an ideal I of $\frac{\mathbb{Z}_q[x]}{\langle f\rangle} + u\frac{\mathbb{Z}_q[x]}{\langle f\rangle}$, define a surjective ring homomorphism $\Psi : I \to \frac{\mathbb{Z}_q[x]}{\langle f\rangle}$ such that $\Psi(a(x) + ub(x)) = a(x)$. It is well known that the ideals of the ring $\frac{\mathbb{Z}_q[x]}{\langle f\rangle}$ are given by $\langle p^i\rangle$, $0 \le i \le r-1$. Therefore, as in the case of ideals of R, the ideal I takes the form

$$I = \langle p^i + uh(x), up^j\rangle, \text{ where } h(x) \in \frac{\mathbb{Z}_q[x]}{\langle f\rangle}.$$

Using p-adic expansion, every element $h(x)$ of $\frac{\mathbb{Z}_q[x]}{\langle f\rangle}$ can be written uniquely as $h(x) = \sum_{k=0}^{r-1} h_k(x)p^k$, where $h_k(x) \in \mathbb{F}_{p^d} = \frac{\mathbb{Z}_p[x]}{\langle \bar{f}\rangle}$. Therefore,

$$I = \langle p^i + up^t \sum_{k=0}^{r-t-1} h_k(x)p^k, up^j\rangle, \text{ where } h_k(x) \in \mathbb{F}_{p^d},\ 0 \le i \le r-1,\ 0 \le j \le i\,.$$

Using similar argument as in Theorem 2.5, we have the following theorem.

Theorem 3.2. *If f is a basic irreducible polynomial of degree d over $\mathbb{Z}_q$, then any ideal of the ring $\frac{R[x]}{\langle f\rangle}$ is of the following form:*

1. *Principal ideals:*
   (i) $\langle p^i\rangle$, $\quad 0 \le i \le r$.
   (ii) $\langle up^j\rangle$, $\quad 0 \le j \le r-1$.
   (iii) $\langle p^i + up^t h(x)\rangle$, $1 \le i \le r-1$, $0 \le t \le i-1$, $h(x) = \sum_{k=t}^{T-1} h_k(x)p^{k-t}$, *where* $h_k(x) \in \mathbb{F}_{p^d}$ $\forall k$ *with* $h_0(x) \ne 0$, *and* $T = \min\{i,\ r-i+t\}$.
2. *Non-principal ideals:*
   (i) $\langle p^i,\ up^j\rangle$, $\quad 0 \le j < i \le r-1$.
   (ii) $\langle p^i + up^t h(x),\ up^j\rangle$, $2 \le i \le r-2$, $0 \le t \le i-2$, $t < j < T$, *where* $T = \min\{i,\ r-i+t\}$, *and* $h(x) = \sum_{k=t}^{j-1} h_k(x)p^{k-t}$, *where* $h_k(x) \in \mathbb{F}_{p^d}$ $\forall$ k *with* $h_0(x) \ne 0$.

It can easily be observed that total number of ideals in $\frac{R[x]}{\langle f\rangle}$ can be obtained by simply replacing p in Theorem 2.7 by p^d, where $d = \deg f$. Therefore we have the following theorem.

Theorem 3.3. *The number of distinct ideals in $\frac{R[x]}{\langle f\rangle}$, where $d = \deg f$, is*

$$\mathcal{N}_d = \frac{p^{d\left(\lfloor \frac{r}{2}\rfloor+2\right)} + 3p^{d\left(r-\lfloor \frac{r}{2}\rfloor+1\right)} - 4p^{2d}}{(p^d-1)^2} + \frac{\left(2\left\lfloor \frac{r}{2}\right\rfloor - r\right)p^{d\left(r-\lfloor \frac{r}{2}\rfloor\right)} + (3-2r)p^d}{(p^d-1)} + 2r + 1.$$

Now we consider the ideal structure of $\frac{R[x]}{\langle x^n-1\rangle}$. As $(n,p) = 1$, it follows from [15, Theorem XIII.11] that $x^n - 1$ factorizes uniquely into monic pairwise coprime basic irreducible polynomials over R. For any factor f of $x^n - 1$, define $\hat{f} = \frac{x^n-1}{f}$. The following result gives the structure of ideals of $\frac{R[x]}{\langle x^n-1\rangle}$.

Lemma 3.4. *[21] Let $x^n - 1 = f_1 f_2 \cdots f_m$, where $f_i, 1 \le i \le m$, be the factorization of $x^n - 1$ into monic pairwise-coprime basic irreducible polynomials over R. As $f_i(x)$ and $\hat{f}_i(x)$ are coprime, let $u_i, v_i \in \mathbb{Z}_q[x]$ such that $u_i\hat{f}_i + v_i f_i = 1$, and let $e_i = u_i\hat{f}_i + \langle x^n - 1\rangle \in R[x]/\langle x^n - 1\rangle$. Then*

1. $e_1, e_2, \cdots, e_m$ *are mutually orthogonal non-zero idempotents of* $R[x]/\langle x^n - 1\rangle$.
2. $e_1 + e_2 + \cdots + e_m = 1$.
3. $R[x]/\langle x^n - 1\rangle = R_1 \oplus R_2 \oplus \cdots \oplus R_m$, *where* $R_i = Re_i$, $1 \le i \le m$.

Theorem 3.5. *Let* $(n, p) = 1$, *and* $x^n - 1 = f_1 f_2 \cdots f_m$ *be the factorization of* $x^n - 1$ *into monic pairwise-coprime basic irreducible polynomials in* $R[x]$. *Then any cyclic code* C *over* R *is of the form*

$$C = \bigoplus_{i=1}^{m} C_i e_i(x) ,$$

where $C_i, 1 \le i \le m$, *is an ideal of the ring* $\frac{R[x]}{\langle f_i\rangle}$.

Proof. Since $x^n - 1 = f_1 f_2 \cdots f_m$ is the factorization of $x^n - 1$ into monic basic irreducible pairwise-coprime polynomials over R, by the Chinese Remainder Theorem we get

$$\frac{R[x]}{\langle x^n - 1\rangle} = \frac{R[x]}{\bigcap_{i=1}^{m}\langle f_i\rangle} = \bigoplus_{i=1}^{m} \frac{R[x]}{\langle f_i\rangle} .$$

It follows that any ideal of the ring $\frac{R[x]}{\langle x^n-1\rangle}$ is a direct sum of the ideals of the $\frac{R[x]}{\langle f_i\rangle}$. Define a map $\Phi_0 : \frac{R[x]}{\langle f_i\rangle} \to R_i$ such that $g + \langle f_i\rangle \mapsto (g + \langle x^n - 1\rangle)e_i = u_i \hat{f}_i g$. It is clear that Φ_0 is an isomorphism. The result then follows from the properties of direct product of rings. □

3.1. Number of cyclic codes

In this subsection, we enumerate the cyclic codes of length n over R.

Theorem 3.6. *Let* $(n, p) = 1$, *and* $x^n - 1 = f_1 f_2 \cdots f_m$ *be the factorization of* $x^n - 1$ *into monic basic irreducible pairwise-coprime polynomials in* $R[x]$. *Then the number of distinct cyclic codes of length* n *over* R *is* $\mathcal{N}_{d_1} \times \mathcal{N}_{d_2} \times \cdots \times \mathcal{N}_{d_m}$, *where* $\mathcal{N}_{d_i}$ *is the total number of ideals in* $\frac{R[x]}{\langle f_i\rangle}$ *as defined in Theorem 3.3,* $1 \le i \le m$.

Proof. Every ideal of $\frac{R[x]}{\langle x^n-1\rangle}$ is of the form $I_1 \oplus \cdots \oplus I_m$, where I_i is an ideal of $\frac{R[x]}{\langle f_i\rangle}$. The number of ideals of $\frac{R[x]}{\langle f_i\rangle}$ is equal to $\mathcal{N}_{d_i}$ as defined in Theorem 3.3. Hence the result. □

Example 3.7. *Let* $n = 7$, $p = 2$, *and* $r = 2$, *i.e.,* $R = \mathbb{Z}_4 + u\mathbb{Z}_4$. *Then* $x^7 - 1$ *factorizes into monic pairwise coprime basic irreducible polynomials over* R *as* $x^7 - 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1) = f_1 f_2 f_3$. *So,* $d_1 = 1$ *and* $d_2 = d_3 = 3$. *From Theorem 3.3, we get* $\mathcal{N}_{d_i} = 2^{d_i} + 5$ *for all* i, $i = 1, 2, 3$. *From Theorem 3.6, the total number of cyclic codes of length 7 over* R *is* $\mathcal{N}_{d_1} \times \mathcal{N}_{d_2} \times \mathcal{N}_{d_3} = (2^1 + 5) \times (2^3 + 5) \times (2^3 + 5) = 1183$, *which can also be verified from [7].*

Example 3.8. *Let* $p = 3, r = 2$, *so that* $R = \mathbb{Z}_9 + u\mathbb{Z}_9$. *Then from Theorem 3.2, there are total 8 ideals of* R. *These are:* $\langle 0\rangle, \langle 1\rangle, \langle 3\rangle, \langle u\rangle, \langle 3u\rangle, \langle 3 + u\rangle, \langle 3 + 2u\rangle, \langle 3, u\rangle$. *Further, for any basic irreducible polynomial* f *of degree* d *over* R, *there are total* $3^d + 5$ *ideals of* $\frac{R[x]}{\langle f\rangle}$, *which are presented in Table 3.*

Ideal (C)	Number of ideals
$\langle 3^i\rangle, i = 0, 1, 2$	3
$\langle 3^i u\rangle, i = 0, 1$	2
$\langle 3 + uh(x)\rangle, h(x) \in \mathbb{F}_{3^d}^{\times}$	$3^d - 1$
$\langle 3, u\rangle$	1

Table 3: Ideals of $(\mathbb{Z}_9 + u\mathbb{Z}_9)[x]/\langle f\rangle$.

4. Duals of cyclic codes over R

For a linear code C of length n over R, the dual of C is defined as

$$C^{\perp} = \{x \in R^n | \, x \cdot c = 0, \forall c \in C\} .$$

In this section, we study duals of cyclic codes of length n over R, where $(n, p) = 1$. We first note the following result.

Proposition 4.1. *The number of codewords in any linear code C of length n over R is p^k, for some integer $k \in \{0, 1, \ldots, 2rn\}$. Moreover, the dual code $C^{\perp}$ of C has p^l codewords, where $k + l = 2rn$.*

Proof. It can be easily verified that R is a Frobenius ring. Therefore, we have $|C||C^{\perp}| = |R|^n = p^{2rn}$ [22]. The result follows. □

In [7], Cao and Li have given the structure of duals of cyclic codes of length n over $\mathbb{Z}_4[u]/\langle u^k \rangle$. In this section, we obtain the structure of the duals of cyclic codes of length n over R using their approach.

For any polynomial $a(x) = \sum_{i=0}^{n-1} a_i x^i \in \frac{R[x]}{\langle x^n-1 \rangle}$, we have $a^*(x) = a(x^{-1}) = a_0 + \sum_{i=1}^{n-1} a_i x^{n-i}$.

Proposition 4.2. *Let a, b be any two elements in R^n and $a(x)$, $b(x)$ be their respective polynomial representations. Then $a \cdot b = 0$ if $a(x)b^*(x) = 0$ in the ring $\frac{R[x]}{\langle x^n-1 \rangle}$.*

Since $x^n - 1$ also factorizes uniquely into monic pariwise coprime basic irreducible polynomials over $\mathbb{Z}_q$, and $\mathbb{Z}_q$ is a subring of R, we may consider such a factorization of $x^n - 1$ over R as a factorization over $\mathbb{Z}_q$. Let $x^n - 1 = f_1 f_2 \cdots f_m$ be the factorization of $x^n - 1$ into monic pairwise-coprime basic irreducible polynomials in $\mathbb{Z}_q[x]$. Then $x^n - 1$ can also be written as $x^n - 1 = (q-1)\tilde{f_1}\tilde{f_2} \cdots \tilde{f_m}$, where $\tilde{f_i}$ is the reciprocal polynomial of f_i, which is defined as $\tilde{f_i}(x) = x^{\deg(f)} f(x^{-1})$. $\tilde{f_1}, \tilde{f_2}, \cdots, \tilde{f_m}$ are pairwise-coprime basic irreducible polynomials in $\mathbb{Z}_q[x]$. Therefore, for every positive integer i, $1 \leq i \leq m$, we have $\langle \tilde{f_i}(x) \rangle = \langle f_{i'}(x) \rangle$, for some unique positive integer i', i.e., $\tilde{f_i}(x) = \omega_i f_{i'}(x)$ for some $\omega_i \in \mathbb{Z}_q^{\times}$, where $1 \leq i' \leq m$.

We define an automorphism α on $\frac{R[x]}{\langle x^n-1 \rangle}$ by

$$\alpha(a(x)) = a^*(x) ,$$

for any $a(x) \in \frac{R[x]}{\langle x^n-1 \rangle}$. This isomorphism induces a permutation of the set $\{1, \cdots, m\}$ such that $\alpha(i) = i'$. So, the component ring $\frac{R[x]}{\langle f_i \rangle}$ of $\frac{R[x]}{\langle x^n-1 \rangle}$ is permuted to the component $\frac{R[x]}{\langle f_{i'} \rangle}$ by α. It is clear that $\alpha^2 = 1$.

Now let $e_i = u_i \hat{f_i} = 1 - v_i f_i$, $1 \leq i \leq m$, be the mutually orthogonal idempotents of $\frac{R[x]}{\langle x^n-1 \rangle}$, as defined in Lemma 3.4. Then $e_i^* = u_i(x^{-1})\hat{f_i}(x^{-1}) = x^n u_i(x^{-1})\hat{f_i}(x^{-1}) = x^{(n-\deg(u_i)-\deg(\tilde{f_i}))}\tilde{u}_i(x)\tilde{\hat{f}}_i(x) = \gamma_i \hat{f}_{i'}$, where $\gamma_i = x^{(n-\deg(u_i)-\deg(\tilde{f_i}))}\tilde{u}_i(x)\hat{\omega}_i$, and $\hat{\omega}_i = \prod_{k=1, k\neq i}^{m} \omega_k$. It can also be observed that $e_i^* = u_i(x^{-1})\hat{f_i}(x^{-1}) = 1 - x^n v_i(x^{-1}) f_i(x^{-1}) = 1 - x^{(n-\deg(v_i)-\deg(f_i))}\tilde{v}_i(x)\tilde{f_i}(x) = 1 - \delta_i f_{i'}$, where $\delta_i = x^{(n-\deg(v_i)-\deg(f_i))}\tilde{v}_i(x)\omega_i$. This implies that $\gamma_i \hat{f}_{i'} = e_i^* = 1 - \delta_i f_{i'}$, i.e., $\gamma_i \hat{f}_{i'} + \delta_i f_{i'} = 1$. From the definition of $e_{i'}$ as given in Lemma 3.4, we get $e_{i'} = \gamma_i \hat{f}_{i'} = e_i^*$.

Theorem 4.3. *Let C be a cyclic code of length n over R such that $C = \bigoplus_{i=1}^{m} C_i e_i(x)$, where C_i are ideals of the ring $\frac{R[x]}{\langle f_i \rangle}$, $1 \leq i \leq m$. Then the dual code $C^{\perp}$ of C is given by $C^{\perp} = \bigoplus_{i=1}^{m} D_{\alpha(i)} e_{\alpha(i)}(x)$, where D_i is an ideal of $\frac{R[x]}{\langle f_i \rangle}$ as presented in the Table 4.*

It can be observed that in Table 4 ideals C_i such that $C_i = D_i$ appear only in the cases (i), (ii), (iv), (v) and (ix), when r is even; and in the cases (vii), (ix), when r is odd. Now we have the following theorem.

Case	C_i		$\lvert C_i\rvert$	D_i	$\lvert D_i\rvert$
(i)	$\langle p^i\rangle$	$0 \le i \le r$	$p^{d(2r-2i)}$	$\langle p^{r-i}\rangle$	p^{d2i}
(ii)	$\langle u\rangle$		p^{dr}	$\langle u\rangle$	p^{dr}
(iii)	$\langle up^i\rangle$	$1 \le i \le r-1$	$p^{d(r-i)}$	$\langle p^{r-i}, u\rangle$	$p^{d(r+i)}$
(iv)	$\langle (p^i + p^t h(x)u)\rangle$	$i \le \left\lfloor \frac{(r+t)}{2} \right\rfloor, h(x) = \sum_{k=0}^{i-t-1} h_k(x)p^k$	$p^{d(2r-2i)}$	$\langle (p^{r-i} + up^{r-2i+t}(p^{i-t} - h^*(x)))\rangle$	p^{2di}
(v)	$\langle (p^i + p^t h(x)u)\rangle$	$i > \left\lfloor \frac{(r+t)}{2} \right\rfloor, h(x) = \sum_{k=0}^{r-i-1} h_k(x)p^k$	$p^{d(r-t)}$	$\langle p^{i-t} + u(-h^*(x)),\ up^{r-i}\rangle$	$p^{d(r+t)}$
(vi)	$\langle p^i + uh(x), up^j\rangle$ (i, j as in Theorem 3.2)	$h(x) = \sum_{k=0}^{j-1} h_k(x)p^k$	$p^{d(2r-i-j)}$	$\langle p^{r-j} + up^{r-i-j}(p^j - h^*(x))\rangle$	$p^{d(i+j)}$
(vii)	$\langle p^i + up^t h(x), up^j\rangle$($i, j$ as in Theorem 3.2)	$h(x) = \sum_{k=0}^{j-t-1} h_k(x)p^k$	$p^{d(2r-i-j)}$	$\langle p^{r-j} + up^{r-i-j+t}\ (p^{j-t} - h^*(x)), up^{r-i}\rangle$	$p^{d(i+j)}$
$(viii)$	$\langle p^i, u\rangle$	$1 \le i \le r-1$	$p^{d(2r-i)}$	$\langle up^{r-i}\rangle$	p^{di}
(ix)	$\langle p^i, up^j\rangle$	$j < i$	$p^{d(2r-i-j)}$	$\langle p^{r-j}, up^{r-i}\rangle$	$p^{d(i+j)}$

Table 4:

Theorem 4.4. *The total number of ideals C_i in $\frac{R[x]}{\langle f_i\rangle}$ such that $C_i = D_i$ is given by*

$$N_{(f,d)} = \begin{cases} \mathscr{N}' + (r-\nu), & \text{if } r \text{ is odd ,} \\ \mathscr{N}' + d'^{\frac{r}{2}} + \frac{r}{2}, & \text{if } r \text{ is even, where} \end{cases}$$

$\mathscr{N}' = \frac{1}{d'-1}\left[\left(\frac{d'^{(\nu+1)}+3d'^{(r-\nu-1)}-3d'^2-d'}{d'-1}\right) + (-2r+7)d' + (2(\nu+1)-r)d'^{(r-\nu-1)}\right] + (2r-\nu-4) - \frac{(r-2)(r-1)}{2}$ *if $d' \neq 1$, and $\mathscr{N}' = 0$ if $d' = 1$, where d' is the total number of polynomial $p(x) \in \mathbb{F}_{p^d}$ such that $p(x) + p^*(x) = 0$ in $\mathbb{F}_{p^d}$ and $\nu = \lfloor \frac{r}{2} \rfloor$.*

Proof. Suppose d' is the total number of polynomials $p(x) \in \mathbb{F}_{p^d}$ such that $p(x) + p^*(x) = 0$ in $\mathbb{F}_{p^d}$. We note that $d' \geq 1$, as the zero polynomial satisfies the given condition.

(a) If r is even, then $C_i = D_i$, if C_i is one of the following cases of Table 4.
  (1) Case (i), $C_i = \langle p^{\frac{r}{2}}\rangle$. Number of ideals in this case is 1.
  (2) Case (iv), $C_i = \langle p^{\frac{r}{2}} + up^t h(x)\rangle$, $0 \le t \le \frac{r}{2} - 1$ with

$$h_j(x) + h_j^*(x) = 0, \ \ 0 \le j \le \frac{r}{2} - t - 1.$$

  Total number of ideals in this case is $\sum_{t=0}^{\frac{r}{2}-1}(d'-1)(d'^{(\frac{r}{2}-t-1)}) = d'^{\frac{r}{2}} - 1$.

(b) If r is either even or odd, then following three cases are common:
  (3) Case (ii), $C_i = \langle u\rangle$,
  (4) Case (vii), $C_i = \langle p^i + up^t h(x), up^{r-i}\rangle$, $t \neq 0$, and

$$h_{j'}(x) + h_{j'}^*(x) = 0, \ \ t < j' \le r - i + t - 1, \ 1 \le t \le i - 2.$$

  Total number of ideals in this case is

$$\begin{aligned}
\mathscr{N}' &= \sum_{i=\nu+1}^{r-2}\sum_{t=1}^{i-2}\sum_{j=t+1}^{T}(d'-1)d'^{(j-t-i)} \\
&= \sum_{i=\nu+1}^{r-2}\left[\sum_{t=1}^{2i-r-1}\sum_{j=1+t}^{r-i+t-1}(d'-1)d'^{(j-t-1)} + \sum_{t=2i-r}^{i-2}\sum_{j=1+t}^{i-1}(d'-1)d'^{(j-t-1)}\right] \\
&= \sum_{i=\nu+1}^{r-2}\left[\sum_{t=1}^{2i-r-1}(d'^{(r-i-1)}-1) + \sum_{t=2i-r}^{i-2}(d'^{(i-t-1)}-1)\right] \\
&= \sum_{i=\nu+1}^{r-2}\left[(d'^{(r-i-1)}-1)(2i-r-1)\right] + \sum_{i=\nu+1}^{r-2}\left[\frac{d'^{(r-i)}-d'}{d'-1} - (r-i-1)\right] \\
&= \frac{1}{d'-1}\left[2\left\{\left(\frac{d'^{(r-\nu-1)}-d'^2}{d'-1}\right) - (r-2)d' + (\nu+1)\,d'^{(r-\nu-1)}\right\} - r\left(d'^{(r-\nu-1)}\right)\right] \\
&\quad + \frac{d'}{d'-1}\left[\left(\frac{d'^{\nu}+d'^{(r-\nu-2)}-d'-1}{(d'-1)}\right) - r + 3\right] + (2r-\nu-4) - \frac{(r-2)(r-1)}{2} \\
&= \frac{1}{d'-1}\left[\left(\frac{d'^{(\nu+1)}+3d'^{(r-\nu-1)}-3d'^2-d'}{d'-1}\right) + (-2r+7)p^{d'} + (2(\nu+1)-r)d'^{(r-\nu-1)}\right] \\
&\quad + (2r-\nu-4) - \frac{(r-2)(r-1)}{2}
\end{aligned}$$

(5) Case (ix), $C = \langle p^i, up^{r-i}\rangle$, $1 \le i \le r-1, r < 2i$. Total number of ideals in this case is $\sum_{i=\nu+1}^{r-1} 1 = r-\nu-1$.

By adding corresponding cases, we have the result. □

We can rearrange $e_1(x), e_2(x), \cdots, e_m(x)$ in this manner such that $\alpha(i) = i'$, $1 \le i \le \gamma$, and $\alpha(i) = \frac{m-\gamma}{2} + i, i = \gamma+1, \cdots, \frac{m-\gamma}{2}$. Now we have the following theorem.

Theorem 4.5. *The total number of self-dual cyclic codes of length n over R is given by*

$$N_{(f_1,d_1)} \times \cdots \times N_{(f_\gamma,d_\gamma)} \times \mathscr{N}_{d_{\gamma+1}} \times \cdots \times \mathscr{N}_{d_{\frac{m-\gamma}{2}}},$$

where $N_{(f_i,d_i)}$ and $\mathscr{N}_{d_i}$ are as given in Theorem 4.4 and Theorem 3.3, respectively.

Proof. Let $x^n - 1 = f_1 f_2 \cdots f_m$ be the factorization of $x^n - 1$ into monic pairwise-coprime basic irreducible polynomials in $\mathbb{Z}_q[x]$. Since $\alpha(i) = i'$, $1 \le i \le \gamma$, total number of ideals C_i in $\frac{\mathbb{Z}_q[x]}{\langle f_i\rangle}$ such that $C_i = D_i$ is given by $N_{(f_i,d_i)}$. For remaining $m - \gamma$ values of i, ideals of $\frac{\mathbb{Z}_q[x]}{\langle f_i\rangle}$ and $\frac{\mathbb{Z}_q[x]}{\langle f_{\alpha(i)}\rangle}$ occur in pairs. Total number of these pairs is $\frac{m-\gamma}{2}$. Hence the result. □

Example 4.6. *Let $n = 8, p = 3, r = 2$, i.e., $R = \mathbb{Z}_9 + u\mathbb{Z}_9$. The factorization of $x^8 - 1$ into coprime basic irreducible polynomials is $x^8 - 1 = (x+1)(x+8)(x^2+1)(x^2+4x+8)(x^2+5x+8) = f_1 f_2 f_3 f_4 f_5$. Then $\langle \tilde{f_1}\rangle = \langle f_1\rangle, \langle \tilde{f_2}\rangle = \langle f_2\rangle, \langle \tilde{f_3}\rangle = \langle f_3\rangle, \langle \tilde{f_4}\rangle = \langle f_5\rangle$, and $\langle \tilde{f_5}\rangle = \langle f_4\rangle$, which implies that $m = 5, d_1 = 1, d_2 = 1, d_3 = 2$, and $\gamma = 3$. As defined in Theorem 4.5, we get $d'_1 = d'_2 = 0$, and $d'_3 = 3$. From Theorem 4.5 total number of self-dual codes of length 8 over R are $2 \times 2 \times 4 \times 14 = 224$. These self dual cyclic codes will take the form*

$$C = \bigoplus_{i=1}^{5} C_i e_i(x),$$

where each of C_1 and C_2 is one of the ideals $\langle 3\rangle$ and $\langle u\rangle$ of R; C_3 is one of the ideals $\langle 3\rangle, \langle u\rangle$ and $\langle 3 + uh(x)\rangle$ of $\frac{R[x]}{\langle f_3\rangle}$, where $h(x)$ is a polynomial of degree 1, i.e. $h(x) = ax$, $a \in \mathbb{F}_3^\times$ which satisfies $h(x) + h^*(x) = 0$; ideals C_4 and C_5 of $\frac{R[x]}{\langle f_4\rangle}$ and $\frac{R[x]}{\langle f_5\rangle}$, respectively, occur in pairs as given in Table 5.

C_4	C_5	Number of ideals
$\langle 3^i\rangle, i = 0, 1, 2$	$\langle 3^{2-i}\rangle$	3
$\langle u\rangle$	$\langle u\rangle$	1
$\langle 3u\rangle$	$\langle 3, u\rangle$	1
$\langle 3 + uh(x)\rangle, h(x) \in \mathbb{F}_{3^2}^{\times}$	$\langle 3 - uh^*(x)\rangle$	8
$\langle 3, u\rangle$	$\langle 3u\rangle$	1

Table 5:

Now we present some examples of cyclic codes of length n over $R = \mathbb{Z}_q + u\mathbb{Z}_q$. For this we first define the Lee weight on R^n.

For any element $a = \sum_{i=0}^{r-1}(a_i + ub_i)p^i \in R$, we define the Gray map φ from R to $\mathbb{Z}_p^{2r}$ as

$$\varphi(a) = \left(\sum_{i=0}^{r-1}(b_i + a_i),\ \sum_{i=0}^{r-1} b_i, \sum_{i=1}^{r-1}(b_i + a_i),\ \sum_{i=1}^{r-1} b_i, \cdots, b_{r-1} + a_{r-1}, b_{r-1}\right).$$

φ can be extended to a map from R^n to $\mathbb{Z}_p^{2rn}$ componentwise. φ is a non-linear isometry from R^n to $\mathbb{Z}_p^{2rn}$. For any element $a \in R$, we define the Lee weight of a as

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

The Lee weight of any element v of R^n is then defined as the rational sum of the Lee weights of its coordinates. The Lee distance $d_L(C)$ of a linear code C over R is defined as the minimum Lee weight of any non-zero codeword in C.

All the computations to determine minimum distance of codes were performed in Magma [27].

Example 4.7. *Let $n = 4, p = 3, r = 2$, so that $R = \mathbb{Z}_9 + u\mathbb{Z}_9$. The factorization of $x^8 - 1$ into coprime basic irreducible polynomials is $x^4 - 1 = (x + 1)(x + 8)(x^2 + 1) = f_1 f_2 f_3$. Then $\langle \tilde{f_1}\rangle = \langle f_1\rangle, \langle \tilde{f_2}\rangle = \langle f_2\rangle, \langle \tilde{f_3}\rangle = \langle f_3\rangle$. Some cyclic codes of length 4 over R are shown in Table 6. We have*

$$\begin{aligned} e_1(x) &= 7x^3 + 7x^2 + 7x + 7 , \\ e_2(x) &= 2x^3 + 7x^2 + 2x + 7 , \\ e_3(x) &= 4x^2 + 5 . \end{aligned}$$

Any cyclic code C of length 4 over R is given by

$$C = C_1 e_1(x) \oplus C_2 e_2(x) \oplus C_3 e_3(x) ,$$

where C_1, C_2 are ideals of $\mathbb{Z}_9$, and C_3 is an ideal of $\frac{\mathbb{Z}_9[x]}{\langle x^2+1\rangle}$. Ideals of $\frac{\mathbb{Z}_9[x]}{\langle x^2+1\rangle}$ are listed in Table 5. The Gray image of C under φ is a non-linear code of length $4n$ over $\mathbb{Z}_3$.

C_1	C_2	C_3	Parameters
$\langle 0\rangle$	$\langle 0\rangle$	$\langle 1\rangle$	$(16, 3^8, 2)$
$\langle 3\rangle$	$\langle u\rangle$	$\langle 3u\rangle$	$(16, 3^{16}, 8)$
$\langle 3\rangle$	$\langle u\rangle$	$\langle 3 + ux\rangle$	$(16, 3^{12}, 8)$
$\langle 3\rangle$	$\langle u\rangle$	$\langle 3 + u(1 + x)\rangle$	$(16, 3^{12}, 8)$
$\langle 3\rangle$	$\langle u\rangle$	$\langle 3 + u\rangle$	$(16, 3^{16}, 4)$
$\langle 3\rangle$	$\langle 3 + u\rangle$	$\langle 3 + u(1 + x)\rangle$	$(16, 3^{12}, 8)$
$\langle u\rangle$	$\langle 3 + u\rangle$	$\langle 3 + u(1 + x)\rangle$	$(16, 3^{12}, 8)$
$\langle 3u\rangle$	$\langle 3 + u\rangle$	$\langle 3 + u(1 + x)\rangle$	$(16, 3^{12}, 8)$
$\langle 3\rangle$	$\langle 3 + u\rangle$	$\langle 3 + ux\rangle$	$(16, 3^{12}, 8)$
$\langle u\rangle$	$\langle 3 + u\rangle$	$\langle 3 + u\rangle$	$(16, 3^{16}, 4)$
$\langle 1\rangle$	$\langle 3 + u\rangle$	$\langle 3 + u\rangle$	$(16, 3^{12}, 4)$
$\langle 3u\rangle$	$\langle 3 + u\rangle$	$\langle 3 + ux\rangle$	$(16, 3^{12}, 8)$
$\langle 3\rangle$	$\langle 3u\rangle$	$\langle 3 + u(1 + x)\rangle$	$(16, 3^{12}, 8)$
$\langle u\rangle$	$\langle 3u\rangle$	$\langle 3 + u(1 + x)\rangle$	$(16, 3^{12}, 8)$
$\langle 1\rangle$	$\langle 3u\rangle$	$\langle 3 + u(1 + x)\rangle$	$(16, 3^{12}, 4)$
$\langle 3u\rangle$	$\langle 3u\rangle$	$\langle 3 + u(1 + x)\rangle$	$(16, 3^{12}, 4)$
$\langle 3\rangle$	$\langle 3u\rangle$	$\langle 3 + ux\rangle$	$(16, 3^{12}, 4)$
$\langle u\rangle$	$\langle 3u\rangle$	$\langle 3 + ux\rangle$	$(16, 3^{12}, 4)$
$\langle 3u\rangle$	$\langle 3u\rangle$	$\langle 3 + ux\rangle$	$(16, 3^{12}, 4)$
$\langle 3\rangle$	$\langle 1\rangle$	$\langle 3 + u(1 + x)\rangle$	$(16, 3^{12}, 4)$
$\langle u\rangle$	$\langle u\rangle$	$\langle 3 + u(1 + x)\rangle$	$(16, 3^{12}, 4)$
$\langle 3u\rangle$	$\langle u\rangle$	$\langle 3 + u(1 + x)\rangle$	$(16, 3^{12}, 4)$
$\langle 3\rangle$	$\langle u\rangle$	$\langle 3 + ux\rangle$	$(16, 3^{12}, 4)$
$\langle u\rangle$	$\langle u\rangle$	$\langle 3 + ux\rangle$	$(16, 3^{12}, 4)$
$\langle 3u\rangle$	$\langle u\rangle$	$\langle 3 + ux\rangle$	$(16, 3^{12}, 4)$
$\langle u\rangle$	$\langle 1\rangle$	$\langle 3 + u(1 + x)\rangle$	$(16, 3^{12}, 4)$
$\langle 3u\rangle$	$\langle 1\rangle$	$\langle 3 + u(1 + x)\rangle$	$(16, 3^{12}, 4)$
$\langle 3\rangle$	$\langle 1\rangle$	$\langle 3 + ux\rangle$	$(16, 3^{12}, 4)$
$\langle u\rangle$	$\langle 1\rangle$	$\langle 3 + ux\rangle$	$(16, 3^{12}, 4)$
$\langle 3u\rangle$	$\langle 1\rangle$	$\langle 3 + ux\rangle$	$(16, 3^{12}, 4)$

Table 6: Cyclic codes of length 4 over $\mathbb{Z}_9 + u\mathbb{Z}_9$.

Acknowledgements. This work was partially supported by Science and Engineering Research Board, DST, Govt. of India, under Grant No. SB/S4/MS: 893/14. Also, the first author would like to thank the Ministry of Human Resource Development (MHRD), India for providing financial support. The authors would also like to thank the anonymous referees for their valuable comments and suggestions.

References

[1] T. Abualrub, I. Siap, 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(3) (2007) 273-287.
[2] R.K. Bandi, M. Bhaintwal, A note on cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, Discrete Mathematics, Algorithms and Applications 08(01) (2016) 1650017 .
[3] R.K. Bandi, M. Bhaintwal, Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, In the proceedings of IWSDA'15 (2015) 47 - 52.
[4] R. K. Bandi, M. Bhaintwal, Codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ with respect to Rosenbloom-Tsfasman metric, In the proceeding of ICACCI'13 (2013) 37 - 41.
[5] R. K. Bandi, M. Bhaintwal, Codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$. In the proceeding of ICACCI'14 (2014) 422 - 427.
[6] P. Bonnecaze, P. Udaya, Cyclic codes and self-dual codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory 45(4) (1999) 1250 - 1255.
[7] Y. Cao, Q. Li, Cyclic codes of odd length over $\frac{\mathbb{Z}_4[u]}{\langle u^k\rangle}$, Cryptogr. Comm. 9(5) (2017) 599–624.

[8] H.Q. Dinh, S.R.L. Permouth, Cyclic codes and negacyclic codes over finite chain ring, IEEE Trans. Inform. Theory 50(8) (2004) 1728-1744.
[9] H.Q. Dinh, A.K. Singh, P. Kumar, S. Sriboonchitta, On the structure of cyclic codes over the ring $\frac{Z_{2^s}[u]}{\langle u^k\rangle}$, Discrete Math. 341(8) (2018) 2243–2275, .
[10] H.Q. Dinh, A.K. Singh, P. Kumar, S. Sriboonchitta, Cyclic codes over the ring $\frac{GR(p^e,m)[u]}{\langle u^k\rangle}$, To Appear in Discrete Math. 343(1) 111543 (to appear in).
[11] J. Gao, F.W. Fu, L. Xiao, R.K. Bandi, Some results on cyclic codes over $\mathbb{Z}_q + u\mathbb{Z}_q$, Discrete Mathematics, Algorithms and Applications 7(4) (2015) 1550058.
[12] J. Gao, F.W. Fu, , L. Xiao, R.K. Bandi, On cyclic codes and quasi-cyclic codes over $\mathbb{Z}_q + u\mathbb{Z}_q$, arxiv:1501.03924v4.pdf (2015).
[13] A. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inform. Theory 40(4) (1994) 301 - 319.
[14] R. Luo, U. Parampalli, Self-dual cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, In the proceedings of IWSDA'15 (2015) 57-61.
[15] B.R. McDonald, Finite Rings with Identity, Marcel Dekker (1974).
[16] G. Norton, A. Sălăgean, On the structure of linear and cyclic codes over a finite chain ring. Appl. Algebra Engrg. Comm. Comput. 10(6) (2000) 489-506.
[17] J.F. Qian, L.N. Zhang, S.X. Zhu, Cyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + \cdots + u^{k-1}\mathbb{F}_p$, IEICE Trans. Fundam. E88-A (2005) 795-797.
[18] M. Shi, Q. Liqin, L. Sok, N. Aydin, P. Solé, On constacyclic codes over $\frac{\mathbb{Z}_4[u]}{\langle u^2-1\rangle}$ and their Gray images, Finite Fields Appl. 45 (2017) 86-95.
[19] M. Shi, Y. Liu, P. Sole, Optimal two-weight codes from trace codes over $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Comm. Letters 20(12) (2016) 2346-2349.
[20] M. Shi, Y. Guan, P. Solé, Two new families of two-weight codes, IEEE Trans. Inform. Theory 63(10) (2017) 6240 - 6246.
[21] Z.X. Wan, Cyclic codes over Galois rings, Algebra Colloq. 6(3) (1999) 291–304.
[22] J. A. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math. 121(199) 555-575.
[23] B. Yildiz, N. Aydin, On cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and their $\mathbb{Z}_4$-images, Int. J. Inf. Coding Theory 2(4) (2014) 226-237.
[24] B. Yildiz, S. Karadeniz, Linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, MacWilliams identities, projections, and formally self-dual codes, Finite Fields Appl. 27 (2014) 24-40.
[25] B. Yildiz, S. Karadeniz, Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes Cryptogr. 58(3) (2011) 221-234.
[26] S. Zhu, Y. Wang, M. Shi, Some results on cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$, IEEE Trans. Inform. Theory 56(4) (2010) 1680-1684.
[27] http://magma.maths.usyd.edu.au/magma/.