TÜBİTAK

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2017) 41: 1235 – 1247

doi:10.3906/mat-1602-35

Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$

Mehmet ÖZEN[1,*], **Nazmiye Tuğba ÖZZAİM**[1], **Nuh AYDIN**[2]
[1]Department of Mathematics, Faculty of Science and Arts, Sakarya University, Sakarya, Turkey
[2]Department of Mathematics and Statistics, Kenyon College, Gambier, Ohio, USA

Received: 10.02.2016 • **Accepted/Published Online:** 01.12.2016 • **Final Version:** 28.09.2017

Abstract: In this paper, we study cyclic codes over the ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$, where $u^3 = 0$. We investigate Galois extensions of this ring and the ideal structure of these extensions. The results are then used to obtain facts about cyclic codes over R. We also determine the general form of the generator of a cyclic code and find its minimal spanning sets. Finally, we obtain many new linear codes over $\mathbb{Z}_4$ by considering Gray images of cyclic codes over R.

Key words: Cyclic codes, Galois extensions, codes over rings, codes over $\mathbb{Z}_4$

1. Introduction

Cyclic codes are one of the most important and most intensively studied classes of linear codes with rich algebraic structure due to their representation as the ideals of a polynomial ring. Another class of codes that has become the subject of much research in recent years is codes over rings. The structure of cyclic codes over various rings is investigated by many authors (e.g., [2, 3, 5, 10]). In [13], Yıldız studied cyclic codes of odd length over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. In [12], the algebraic structure of cyclic codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, where $u^2 = 0$, is determined. Making use of the structure of cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, Yıldız and Aydın conducted a computer search and obtained some new linear codes over $\mathbb{Z}_4$. In [8], cyclic codes over $\mathbb{Z}_q + u\mathbb{Z}_q$, where $u^2 = 0$ and q is the power of a prime, were investigated. In this work, we study cyclic codes over the ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$ where $u^3 = 0$. We determine the structure of cyclic codes over R and obtain many new linear codes over $\mathbb{Z}_4$ from the cyclic codes over R.

This work is organized as follows: In Section 2, we investigate the structure of the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$, where $u^3 = 0$, and we give some basic definitions and theorems. In Section 3, Galois extensions of this ring and the ideal structure of this extension are studied. In the next section, cyclic codes over R are discussed and the general form of the generator of a cyclic code and minimal spanning sets of such codes are obtained, where some of the results from Section 3 are used. In Section 5 we define a Gray-like map to obtain codes over $\mathbb{Z}_4$ from codes over R and show that the $\mathbb{Z}_4$-image of a cyclic code over R is a quasi-cyclic code. Finally, we present some of the results of a computer search in Section 6 that produced many new linear codes over $\mathbb{Z}_4$ from cyclic codes over R.

*Correspondence: ozen@sakarya.edu.tr
2010 *AMS Mathematics Subject Classification:* 94B05, 94B65.
This work was supported by the Research Fund of Sakarya University under project number 2016-02-00-004.

2. Preliminaries

Let R denote the ring $\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4=\{a+ub+u^2c|a,b,c\in\mathbb{Z}_4\}$ where $u^3=0$. It is clear that $R\cong\mathbb{Z}_4[u]/\langle u^3\rangle$. R is a commutative ring with identity, and it has characteristic 4 and order 64. Any element x of R can be written as $x=a+ub+u^2c$, where $a,b,c\in\mathbb{Z}_4$ and x is a unit in R if and only if a is a unit in $\mathbb{Z}_4$. R has 11 nontrivial ideals given by

$$\begin{aligned}
\langle 2u^2\rangle &= \{0,2u^2\}\\
\langle u^2\rangle &= \{0,u^2,2u^2,3u^2\}\\
\langle 2u\rangle &= \{0,2u,2u^2,2u+2u^2\}\\
\langle 2u+u^2\rangle &= \{0,2u^2,2u+u^2,2u+3u^2\}\\
\langle 2u,u^2\rangle &= \{0,u^2,2u^2,3u^2,2u,2u+u^2,2u+2u^2,2u+3u^2\}\\
\langle 2\rangle &= \{0,2,2u,2u^2,2+2u,2+2u^2,2u+2u^2,2+2u+2u^2\}\\
\langle 2+u^2\rangle &= \{0,2u,2u^2,2u+2u^2,2+u^2,2+3u^2,2+2u+u^2,2+2u+3u^2\}\\
\langle 2,u^2\rangle &= \{0,2,2u,u^2,2u^2,3u^2,2+2u,2+u^2,2+2u^2,2+3u^2,\\
&\quad 2u+u^2,2u+2u^2,\ 2u+3u^2,2+2u+u^2,2+2u+2u^2,2+2u+3u^2\}\\
\langle u\rangle &= \{0,u,2u,3u,u^2,2u^2,3u^2,u+u^2,u+2u^2,u+3u^2,2u+u^2,2u+2u^2,\\
&\quad 2u+3u^2,3u+u^2,3u+2u^2,3u+3u^2\}\\
\langle 2+u\rangle &= \{0,2u,u^2,2u^2,3u^2,2+u,2+3u,2u+u^2,2u+2u^2,2u+3u^2,2+u+u^2\\
&\quad 2+u+2u^2,2+u+3u^2,2+3u+u^2,2+3u+2u^2,2+3u+3u^2\}\\
\langle 2,u\rangle &= \{0,2,u,2u,3u,u^2,2u^2,3u^2,2+u,2+2u,2+3u,2+u^2,2+2u^2,2+3u^2,\\
&\quad u+u^{\,2},u+2u^2,u+3u^2,2u+u^2,2u+2u^2,2u+3u^2,3u+u^2,3u+2u^2,\\
&\quad 3u+3u^2,2+u+u^2,2+u+2u^2,2+u+3u,2+2u+u^2,2+2u+2u^2,\\
&\quad 2+2u+3u^2,2+3u+u^2,2+3u+2u^2,2+3u+3u^2\}.
\end{aligned}$$

It is easy to see that R is a local Frobenius ring with $\langle 2,u\rangle$ as its unique maximal ideal. Since the ideals $\langle u^2\rangle$ and $\langle 2u\rangle$ are not comparable, R is not a chain ring. Since the ideal $\langle 2,u\rangle$ cannot be generated by any single element of R, R is not a principal ideal ring either.

Let $\widetilde{R}$ denote the residue field of R. Then we have

$$\widetilde{R}=R/\langle 2,u\rangle=\{0+\langle 2,u\rangle,1+\langle 2,u\rangle\}\cong\mathbb{Z}_2.$$

Now we define the projection map $\sim: R\to\widetilde{R}$ as follows:

$$\sim(x)=\begin{cases}1, & \text{if } x \text{ is a unit}\\ 0, & \text{otherwise.}\end{cases}$$

The image of $x\in R$ under this projection map is denoted by $\widetilde{x}$. Let $R[x]$ denote the polynomial ring over R. The map $\sim$ is extended to $R[x]\to\widetilde{R}[x]$ in the usual way. The image of $f(x)\in R$ under this extended map is denoted by $\widetilde{f}(x)$.

Definition 2.1 *A polynomial $f(x)$ is called basic irreducible in $R[x]$ if $\widetilde{f}(x)$ is an irreducible polynomial in $\widetilde{R}[x]$.*

Irreducible polynomials over finite fields and basic irreducible polynomials over finite local rings play similar roles in algebra.

Definition 2.2 ([9]) *If a polynomial $f(x)\in R[x]$ is not a zero divisor, then it is called a regular polynomial.*

Definition 2.3 *Two polynomials* $f(x), g(x) \in R[x]$ *are said to be coprime if there are polynomials* $a_0(x)$ *and* $a_1(x)$ *in* $R[x]$ *such that*

$$f(x)a_0(x) + g(x)a_1(x) = 1.$$

Theorem 2.4 (Hensel's Lemma [11]) *Let* $f(x)$ *be a monic polynomial in* $\mathbb{Z}_4[x]$ *and assume that* $\tilde{f}(x) = \tilde{f}_1(x)\ \tilde{f}_2(x)...\ \tilde{f}_r(x)$ *where* $\tilde{f}_1(x)\ , \tilde{f}_2(x), ...,\ \tilde{f}_r(x)$ *are pairwise coprime polynomials in* $\mathbb{Z}_2[x]$ *and* $\tilde{f}_i(x) \equiv f_i(x) (\mathrm{mod}\, 2)$. *Then there exist monic polynomials* $h_1(x), h_2(x), \ldots, h_r(x) \in \mathbb{Z}_4[x]$ *with the following properties:*

i) $f(x) = h_1(x)h_2(x)...h_r(x)$.
ii) $\tilde{h}_i(x) = \tilde{f}_i(x)$.
iii) $h_1(x), h_2(x), \ldots, h_r(x)$ *are pairwise coprime polynomials in* $\mathbb{Z}_4[x]$.

3. Galois extensions of $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$, $u^3 = 0$

In this section we study some aspects of Galois extensions of the ring R that will be useful in determining the ideals of $R[x]/\langle x^n - 1\rangle$. Throughout this section, n is assumed to be an odd integer. We first investigate the factorization of $x^n - 1$ over R because of its importance in the study of cyclic codes.

Theorem 3.1 *Let* $h(x)$ *be an irreducible polynomial in* $\mathbb{Z}_2[x]$ *and divide* $x^{2^r-1} - 1$ *for some positive integer* r. *Then there exists a unique basic irreducible polynomial* $f(x)$ *in* $R[x]$ *such that* $f(x)|x^{2^r-1} - 1$ *and* $\tilde{f}(x) = h(x)$.

Proof Since $h(x)|x^{2^r-1} - 1$, there exists $h^{'}(x) \in \mathbb{Z}_2[x]$ such that $h(x) \cdot h^{'}(x) = x^{2^r-1} - 1$. By Theorem 2.4, there exist $f(x), f^{'}(x) \in \mathbb{Z}_4[x]$ such that $f(x) \cdot f^{'}(x) = x^{2^r-1} - 1$ and $f(x) \mod 2 = h(x)$, $f^{'}(x) \mod 2 = h^{'}(x)$. Since $\mathbb{Z}_4$ is a subring of R, the factorization of $x^{2^r-1} - 1$ is valid over R, i.e. $f(x)|(x^{2^r-1} - 1)$ in $R[x]$. Also, $\widetilde{f}(x) \equiv f(x) \mod \langle 2, u\rangle = h(x)$. Since $2^r - 1$ is odd, by Theorem XIII.11 in [9], $x^{2^r-1} - 1$ can be factorized uniquely into pairwise coprime basic irreducible polynomials over R. It follows that $f(x)$ is unique. □

The polynomial $f(x)$ in Theorem 3.1 is called the Hensel lift of $h(x)$ to R. We will need some results about the Galois extension of $\mathbb{Z}_4$ in our study of Galois extensions over the ring R. Therefore, we recall some basic facts about the Galois extension of $\mathbb{Z}_4$. Let $r(x)$ be a monic basic irreducible polynomial of degree k in $\mathbb{Z}_4[x]$. Then the Galois ring over $\mathbb{Z}_4$ is defined as the residue class ring $\mathbb{Z}_4[x]/\langle r(x)\rangle$ and it is denoted by $GR(4, k)$.

Let ε be a root of $r(x)$ and $T = \{0, 1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{2^k-2}\}$ be the Teichmüller set of $GR(4, k)$. Then all elements of $GR(4, k)$ can be expressed uniquely in the form $x_0 + 2x_1$, where $x_0, x_1 \in T$. This representation is called the 2-adic representation.

Now we investigate the Galois extension of R in a similar way. Let $r(x)$ be a monic basic irreducible polynomial of degree k in $R[x]$. Then the Galois ring over R is defined as the residue class ring $R[x]/\langle r(x)\rangle$ and denoted by $GR(R, k)$. If α is a root of $r(x)$, then all elements of $GR(R, k)$ can be expressed uniquely in the form

$$r_0 + r_1\alpha + \cdots + r_{k-1}\alpha^{k-1}, \text{ where } r_i \in R, i = 0, 1, \ldots, k-1,$$

which is called the additive representation of the element of the Galois ring $GR(R,k)$. $GR(R,k)$ is a free R-*module* of rank k with basis $\{1,\alpha,\alpha^2,\ldots,\alpha^{k-1}\}$ and $|GR(R,k)|=64^k$. It is a local ring with unique maximal ideal $\langle 2,u\rangle+\langle r(x)\rangle$. The field F_{2^k} is the residue field of $GR(R,k)$. Moreover,

$$GR(R,k)\cong GR(4,k)[u]/\langle u^3\rangle\cong GR(4,k)+uGR(4,k)+u^2GR(4,k).$$

Therefore, any element x of $GR(R,k)$ can be written as $x=a+ub+u^2c$, where $a,b,c\in GR(4,k)$. Making use of 2-adic representation in $GR(4,k)$, we can write $a=a_1+2a_2, b=b_1+2b_2, c=c_1+2c_2$, for $i=1,2$; $a_i,b_i,c_i\in T$. Thus, the element $x\in GR(R,k)$ can be written in the form $x=a_1+2a_2+u(b_1+2b_2)+u^2(c_1+2c_2)$.

Lemma 3.2 *A nonzero element $x=a_1+2a_2+u(b_1+2b_2)+u^2(c_1+2c_2)\in GR(R,k)$ is unit if and only if $a_1\neq 0$ in T.*

Proof Since $x^4=a_1^4$ for any nonzero element x in $GR(R,k)$, the result is obtained as follows:

$$\begin{aligned} x \text{ is unit} &\iff x^4=a_1^4\in T \text{ is unit}\\ &\iff a_1^4\neq 0\\ &\iff a_1\neq 0. \end{aligned}$$

□

By Lemma 3.2, the group of units $GR^*(R,k)$ of $GR(R,k)$ is given by

$$GR^*(R,k)=\{a_1+2a_2+u(b_1+2b_2)+u^2(c_1+2c_2)|a_i,b_i,c_i\in T,(i=1,2);a_1\neq 0\}.$$

Lemma 3.3 *Let $f(x)$ and $g(x)$ be in $R[x]$. Then $f(x)$ and $g(x)$ are coprime in $R[x]$ if and only if $\tilde{f}(x)$ and $\tilde{g}(x)$ are coprime in $\tilde{R}[x]$.*

Proof Since $f(x)$ and $g(x)$ are coprime in $R[x]$, there are polynomials $a_0(x)$ and $a_1(x)$ in $R[x]$ such that

$$f(x)a_0(x)+g(x)a_1(x)=1,$$

which implies that

$$\tilde{f}(x)\tilde{a_0}(x)+\tilde{g}(x)\tilde{a_1}(x)=1$$

with $\tilde{f}(x),\tilde{a_0}(x),\tilde{g}(x),\tilde{a_1}(x)\in\widetilde{R}[x]$. Thus, $\tilde{f}(x)$ and $\tilde{g}(x)$ are coprime in $\widetilde{R}[x]$.

On the other hand, if $\tilde{f}(x)$ and $\tilde{g}(x)$ are coprime in $\widetilde{R}[x]$, then there are polynomials $\tilde{a_0}(x)$ and $\tilde{a_1}(x)$ in $R[x]$ such that $\tilde{f}(x)\tilde{a_0}(x)+\tilde{g}(x)\tilde{a_1}(x)=1$. Then there exist $s(x),t(x)\in R[x]$ such that

$$f(x)a_0(x)+g(x)a_1(x)=1+2s(x)+ut(x).$$

Let

$$\begin{aligned} \alpha(x)&=1-2s(x)\\ \beta(x)&=1-ut(x)\alpha(x)\\ \delta(x)&=\beta^2(x)+2ut(x)\alpha(x)\\ \Gamma(x)&=\alpha(x)\beta(x)\delta(x). \end{aligned}$$

Then,

$$\Gamma(x)f(x)a_0(x)+\Gamma(x)g(x)a_1(x)=1.$$

Therefore, $f(x)$ and $g(x)$ are coprime in $R[x]$. □

Theorem 3.4 *Let $f(x)$ be a basic irreducible polynomial over R. Then the ideals of the Galois ring $R[x]/\langle f(x)\rangle$ are $\{0\}, \langle 1+\langle f(x)\rangle\rangle, \langle 2+\langle f(x)\rangle\rangle$, $\langle u+\langle f(x)\rangle\rangle, \langle 2u+\langle f(x)\rangle\rangle, \langle u^2+\langle f(x)\rangle\rangle$, $\langle 2u^2+\langle f(x)\rangle\rangle, \langle 2+u+\langle f(x)\rangle\rangle$, $\langle 2+u^2+\langle f(x)\rangle\rangle, \langle 2u+u^2+\langle f(x)\rangle\rangle$ $, \langle (2u,u^2)+\langle f(x)\rangle\rangle, \langle (2,u^2)+\langle f(x)\rangle\rangle$, and $\langle (2,u)+\langle f(x)\rangle\rangle$.*

Proof Let I be a nonzero ideal of $R[x]/\langle f(x)\rangle$ and $g(x)+\langle f(x)\rangle \in I$ for some $g(x) \notin \langle f(x)\rangle$. Since $f(x)$ is a basic irreducible polynomial over R, $\widetilde{f}(x)$ is an irreducible polynomial over $\widetilde{R}$. Therefore, $\gcd(\widetilde{g}, \widetilde{f}) = 1$ or $\widetilde{f}$. Suppose that $\gcd(\widetilde{g}, \widetilde{f}) = 1$. From Lemma 3.4, we have $\gcd(g, f) = 1$ and hence there exist $a_0(x), a_1(x) \in R[x]$ such that

$$f(x)a_0(x) + g(x)a_1(x) = 1,$$

which implies that $g(x)a_1(x) = 1 \mod f(x)$. Therefore, $g(x)$ is an invertible element in I and so $I = \langle 1 + (f(x))\rangle$. Now suppose that $\gcd(\widetilde{g}, \widetilde{f}) = \widetilde{f}$. It follows that there exists $\widetilde{h}(x) \in \widetilde{R}[x]$ such that $\widetilde{g}(x) = \widetilde{f}(x)\widetilde{h}(x)$, or equivalently

$$g(x) = f(x)h(x) + 2h_1(x) + uh_2(x)$$

where $h(x), h_1(x), h_2(x) \in R[x]$ and $\gcd(\widetilde{f}, \widetilde{h_1}) = 1$ or $\gcd(\widetilde{f}, \widetilde{h_2}) = 1$. This shows that $g(x) + \langle f(x)\rangle \in \langle (2,u) + \langle f(x)\rangle\rangle$. Since $I \neq \langle 1 + \langle f(x)\rangle\rangle$, $I \subset \langle (2,u) + \langle f(x)\rangle\rangle$. The nonzero ideals contained in $\langle (2,u) + \langle f(x)\rangle\rangle$ are $\langle 2 + \langle f(x)\rangle\rangle, \langle u + \langle f(x)\rangle\rangle, \langle 2u + \langle f(x)\rangle\rangle, \langle u^2 + \langle f(x)\rangle\rangle$, $\langle 2u^2 + \langle f(x)\rangle\rangle, \langle 2 + u + \langle f(x)\rangle\rangle, \langle 2 + u^2 + \langle f(x)\rangle\rangle, \langle 2u + u^2 + \langle f(x)\rangle\rangle, \langle (2u, u^2) + \langle f(x)\rangle\rangle, \langle (2, u^2) + \langle f(x)\rangle\rangle$, and $\langle (2,u) + \langle f(x)\rangle\rangle$ itself. □

The results about the ideals of a Galois extension of R will be useful in determining the number of cyclic codes of length n over R in the next section.

4. Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$

In this section, we assume again that n is an odd integer. A linear code of length n over R is an R-submodule of R^n. A linear code C over R is called cyclic if $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$ whenever $(c_0, c_1, \ldots, c_{n-1}) \in C$. Let R_n denote the quotient ring $R[x]/\langle x^n - 1\rangle$. Then we consider the usual correspondence between vectors and polynomials

$$\begin{array}{rcl} \phi : R^n & \longrightarrow & R_n \\ c = (c_0, c_1, \ldots, c_{n-1}) & \longrightarrow & c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}. \end{array}$$

It is easily verified that C is a cyclic code if and only if $\phi(C)$ is an ideal of R_n. Therefore, in order to understand cyclic codes over R, we need to understand the structure of the ring R_n.

We know that if S is a finite chain ring and n and the characteristic of S are coprime, then S_n is principal ideal ring [6]. However, since the ring R is not a finite chain ring, this is not necessarily true. Now we show that R_n is, in fact, not a principal ideal ring.

Theorem 4.1 *The ring R_n is not a principal ideal ring.*

Proof In this proof, we use the group rings as defined in [1]. Let $G = \langle g : g^n = 1\rangle$ be a cyclic group order of n. For any group ring RG, the augmentation homomorphism is defined as

$$\xi : RG \longrightarrow R$$

$$\xi(r_0 + r_1 g + \cdots + r_{n-1} g^{n-1}) = r_0 + r_1 + \cdots + r_{n-1}.$$

This map is a surjective ring homomorphism and it can also be defined as

$$\begin{array}{rcl} \xi : R_n & \longrightarrow & \mathrm{R} \\ \xi(r_0 + r_1 x + \cdots + r_{n-1} x^{n-1}) & = & r_0 + r_1 + \cdots + r_{n-1}. \end{array}$$

Now we consider the ideal $I = \langle 2, u \rangle$ of R. Let $J = \xi^{-1}(I)$. Since the inverse image under a ring homomorphism of an ideal is an ideal, J is an ideal of R_n. Suppose that J is a principal ideal. Since I is a homomorphic image of J, it must be a principal ideal. This is a contradiction. Hence, J is not a principal ideal of R_n and therefore the ring R_n is not a principal ideal ring. □

Now, making use of Chinese remainder theorem (CRT), we investigate the ideals of R_n. Since n is odd, $x^n - 1$ can be written as the product of pairwise coprime basic irreducible polynomials over R [11]. Let the polynomials $f_1(x), f_2(x), ..., f_s(x)$ be pairwise coprime basic irreducible polynomials and assume that $x^n - 1 = f_1(x) f_2(x) \cdots f_s(x)$. Let $\widehat{f_i}(x)$ denote the product of all $f_j(x)$ except $f_i(x)$. Then for $i = 1, 2, \ldots, s$, $\widehat{f_i}(x)$ and $f_i(x)$ are coprime and there exist $a_i(x), b_i(x) \in R[x]$ such that

$$f_i(x) a_i(x) + \widehat{f_i}(x) b_i(x) = 1.$$

Let $e_i(x) = \widehat{f_i}(x) b_i(x) + \langle x^n - 1 \rangle$ and $R_i = e_i(x) R_n$. Then R_n has the direct sum decomposition

$$R[x]/\langle x^n - 1 \rangle = R_1 + R_2 + \cdots + R_s.$$

For all $i = 1, 2, ..., s$, the map

$$\begin{array}{rcl} \theta_i : R[x]/\langle f_i(x) \rangle & \longrightarrow & R_i \\ r(x) + \langle f_i(x) \rangle & \longrightarrow & (r(x) + \langle x^n - 1 \rangle) e_i(x) \end{array}$$

is a ring homomorphism. Therefore, we obtain

$$R[x]/\langle x^n - 1 \rangle \cong R[x]/\langle f_1(x) \rangle + R[x]/\langle f_2(x) \rangle + \cdots + R[x]/\langle f_s(x) \rangle.$$

Theorem 4.2 *Let $x^n - 1 = f_1(x) f_2(x) \cdots f_s(x)$ be the unique factorization of $x^n - 1$ where for all $i = 1, 2, \ldots, s$, the polynomials $f_i(x)$ are basic irreducible pairwise coprime over R. Then any ideal in $R[x]/\langle x^n - 1 \rangle$ is sum of the ideals of $R[x]/\langle f_i(x) \rangle, i = 1, 2, \ldots, s$.*

Proof The proof is obtained from the CRT. □

Corollary 4.3 *The number of cyclic codes over R is 13^s, where s is the number of basic irreducible factors of $x^n - 1$.*

Proof From Theorem 4.2, each ideal of $R[x]/\langle x^n - 1 \rangle$ is a sum of the ideals of $R[x]/\langle f_i(x) \rangle, i = 1, 2, \ldots, s$. By Theorem 3.4, $R[x]/\langle f_i(x) \rangle$ has 13 ideals for each i. The result follows from these two facts. □

Now we determine the general form of the generators of cyclic codes over R. First, we consider a homomorphism from $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$ to $\mathbb{Z}_4 + u\mathbb{Z}_4$. Making use of this homomorphism and some results on

cyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$, we determine the general form of the generators of cyclic codes over R. Define a ring homomorphism as follows:

$$\Psi : \mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4 \longrightarrow \mathbb{Z}_4+u\mathbb{Z}_4$$

$$a+ub+u^2c \longrightarrow a+ub \mod u^2.$$

Let C be a cyclic code in R_n. We extend Ψ to a homomorphism $\Phi : R[x]/\langle x^n-1\rangle \longrightarrow (\mathbb{Z}_4+u\mathbb{Z}_4)[x]/\langle x^n-1\rangle$ by

$$\Phi(a_0+a_1x+\cdots+a_{n-1}x^{n-1}) = \Psi(a_0)+\Psi(a_1)x+\cdots+\Psi(a_{n-1})x^{n-1}$$

where $a_i \in R$. We remember that the image of Φ is an ideal in $(\mathbb{Z}_4+u\mathbb{Z}_4)[x]/\langle x^n-1\rangle$, which means that $\Phi(C)$ is a cyclic code over $\mathbb{Z}_4+u\mathbb{Z}_4$. Since the generators of cyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$ are characterized in [12], we can use these results. For some $g(x) \in \mathbb{Z}_4[x]$, we have

$$\Phi(C) = \langle g_1(x)+2a_1(x)+ug(x), u(g_2(x)+2a_2(x))\rangle$$

where for $i=1,2$; $g_i(x), a_i(x)$ are binary polynomials with $a_i(x)|\ g_i(x)|x^n-1 \mod 2$ and $g_i(x)+2a_i(x)$ is a generator of a cyclic code over $\mathbb{Z}_4$. Furthermore, $Ker(\Phi)$ is a cyclic code over $u^2\mathbb{Z}_4[x]$, and therefore

$$Ker\Phi = u^2\langle g_3(x)+2a_3(x)\rangle$$

where $g_3(x)$ and $a_3(x)$ are binary polynomials. Hence, we obtain the following theorem:

Theorem 4.4 *Let C be a cyclic code of length n over R. Then $C = \langle g_1(x)+2a_1(x)+ug(x)+u^2h(x), u(g_2(x)+2a_2(x))+u^2b(x), u^2(g_3(x)+2a_3(x))\rangle$ where $a_i(x)|\ g_i(x)|x^n-1 \mod 2$, and $g_i(x)+2a_i(x)$ is a generator of a cyclic code over $\mathbb{Z}_4$ for $i=1,2,3$.*

Let us define $f_i(x) \in \mathbb{Z}_4[x]$ as $f_i(x) = g_i(x)+2a_i(x)$ for $i=1,2,3$. A generator of C can be written as

$$C = \langle f_1(x)+ug(x)+u^2h(x), uf_2(x)+u^2b(x), u^2f_3(x)\rangle.$$

Also, since $u^2(f_1(x)+ug(x)+u^2h(x)) = u^2f_1(x) \in C$ and $\Phi(u^2f_1(x)) = 0$, we have $u^2f_1(x) \in Ker(\Phi)$, i.e. $f_3(x)|f_1(x)$. Similarly we have $u^2f_2(x) \in Ker(\Phi)$. Also making use of homomorphism in [12], we can obtain $f_2(x)|f_1(x)$ by the above method. This implies that $f_3(x)|f_2(x)|f_1(x)$.

Lemma 4.5 *Let $\alpha(x)$ and $\beta(x)$ be polynomials over R. If $\beta(x)$ is regular, then there exist polynomials $s(x)$ and $t(x)$ such that*

$$\alpha(x) = \beta(x)s(x)+t(x) \text{ where } \deg t(x) < \deg \beta(x).$$

Proof By [9], since $\beta(x)$ is regular, there exist monic $f^*(x)$ and unit $q(x)$ in $R[x]$ such that $\beta(x) = f^*(x)q(x)$. Since $f^*(x)$ is monic, using the division algorithm we have $\alpha(x) = f^*(x)\acute{s}(x)+t(x)$ where $\deg t(x) < \deg f^*(x)$. Multiplying both sides by $q(x)$, we get $q(x)\alpha(x) = q(x)f^*(x)\acute{s}(x)+q(x)t(x)$, which implies $\alpha(x) = \beta(x)s(x)+t(x)$ where $s(x) = (q(x))^{-1}\acute{s}(x)$.

Since $f^*(x)$ is monic, we have $\deg(\beta(x)) = \deg(q(x)) + \deg(f^*(x)) \geq \deg(f^*(x))$. We already know $\deg(t(x)) < \deg(f^*(x))$. Hence, $\deg(t(x)) < \deg(\beta(x))$. □

Theorem 4.6 *Let C be a cyclic code of length n over R. If $C = \langle f_1(x) + ug(x) + u^2h(x), uf_2(x) + u^2b(x), u^2f_3(x)\rangle$, and $f_3(x) = f_1(x)$, then $C = \langle f_1(x) + ug(x) + u^2h(x)\rangle$. Furthermore, if $f_3(x)$ is regular, then $f_1(x) + ug(x) + u^2h(x) | (x^n - 1)$.*

Proof Suppose $f_3(x) = f_1(x)$; then the equality $f_3(x) = f_2(x) = f_1(x)$ follows from $f_3(x)|f_2(x)|f_1(x)$. Since $\Phi(C) = \langle f_1(x) + ug(x), uf_2(x)\rangle$ is a cyclic code over $\mathbb{Z}_4 + u\mathbb{Z}_4$, and $u(f_1(x) + ug(x)) = uf_1(x) = uf_2(x)$, we have $\Phi(C) = \langle f_1(x) + ug(x)\rangle$. Making use of $f_3(x) = f_1(x)$, we have

$$u^2(f_1(x) + ug(x) + u^2h(x)) = u^2f_1(x) = u^2f_3(x) \in \langle f_1(x) + ug(x) + u^2h(x)\rangle.$$

Thus, $C = \langle f_1(x) + ug(x) + u^2h(x)\rangle$.

Now, assuming that $f_3(x) = f_1(x)$ is regular, then so is $f_1(x) + ug(x) + u^2h(x)$. By Lemma 4.5, we have

$$x^n - 1 = (f_1(x) + ug(x) + u^2h(x))s(x) + t(x)$$

where $t(x) = 0$ or $\deg t(x) < \deg(f_1(x) + ug(x) + u^2h(x))$. It follows that $t(x) = (x^n - 1) - (f_1(x) + ug(x) + u^2h(x))s(x) = -s(x)(f_1(x) + ug(x) + u^2h(x)) \in C$. This contradicts that $f_1(x) + ug(x) + u^2h(x)$ has minimum degree in C, unless $t(x) = 0$. Thus, $t(x) = 0$ and $f_1(x) + ug(x) + u^2h(x) | (x^n - 1)$. □

Next, we determine a minimal spanning set and the size of a cyclic code over R. First we need the following definition.

Definition 4.7 *[7] Let R be a local Frobenius ring with unique maximal ideal M and let $r_1, \ldots, r_k$ be elements in R^n. Then $r_1, \ldots, r_k$ are modular independent if and only if $\sum c_ir_i = 0$ implies that $c_i \in M$ for all $i = 1, \ldots, k$.*

Theorem 4.8 *Let n be an odd integer and C be a cyclic code of length n over R.*

1. *If $C = \langle f(x)\rangle$ is a cyclic code of length n over R where $f(x) = f_1(x) + ug(x) + u^2h(x)$ with $\deg f(x) = s$ and $f_1(x)$ is a regular polynomial over $R[x]$, then C is free with rank $= n - s$ and has basis*

$$B = \{f(x), xf(x), \ldots, x^{n-s-1}f(x)\}.$$

2. *If $C = \langle f_1(x) + ug(x) + u^2h(x), uf_2(x) + u^2b(x), u^2f_3(x)\rangle$ is a cyclic code over R where $f_1(x)$, $f_2(x)$, and $f_3(x)$ are monic polynomials with $\deg f_1(x) = s_1, \deg f_2(x) = s_2$ and $\deg f_3(x) = s_3$, then C has rank $n - s_3$ and a minimal spanning set*

$$T = \left\{ \begin{array}{c} f_1(x) + ug(x) + u^2h(x), x(f_1(x) + ug(x) + u^2h(x)), \ldots, x^{n-s_1-1}(f_1(x) + ug(x) + u^2h(x)), \\ uf_2(x) + u^2b(x), x(uf_2(x) + u^2b(x)), \ldots, x^{s_1-s_2-1}(uf_2(x) + u^2b(x)), \\ u^2f_3(x), x(u^2f_3(x)), \ldots, x^{s_2-s_3-1}(u^2f_3(x)) \end{array} \right\}.$$

Proof *(1)* Let $C = \langle f(x)\rangle$ be a cyclic code of length n over R where $f(x) = f_1(x) + ug(x) + u^2h(x)$ and $f_1(x)$ be a regular polynomial over $R[x]$. From Theorem 4.6, we can say that $f(x)|x^n - 1$. Thus, there exists a polynomial $h(x) \in R[x]$ with $\deg h(x) = n - s$ such that $x^n - 1 = f(x)h(x)$. Let $c(x)$ be an element of C

and then $c(x)$ can be expressed as $c(x) = f(x)k(x)$ for some polynomial $k(x)$. If $k(x)$ has degree $n-s-1$ then the proof is done. Otherwise, since $f_1(x)$ is regular, $f_1(x)+ug(x)+u^2h(x)$ is so. Hence, by Lemma 4.5 there exist polynomials $s(x)$ and $t(x)$ such that

$$k(x) = h(x)s(x) + t(x) \text{ where } \deg t(x) \leq n-s-1.$$

Thus, $c(x) = f(x)k(x) = f(x)t(x)$, so B spans C. Now we show that B is linearly independent. Let $a(x) = a_0 + a_1x + \cdots + a_{n-s-1}x^{n-s-1} \in R[x]$ be a polynomial such that $a(x)f(x) = 0$. Since $f(x)$ is regular then there exist polynomial unit $q(x)$ and monic $f^*(x) = f_0^* + f_1^*x + \cdots + f_{n-s-1}^*x^{n-s-1}$ in $R[x]$ where f_{n-s-1}^* is unit such that $f(x) = f^*(x)q(x)$. Thus, we have $a(x)f^*(x)q(x) = 0$. By comparing coefficients we have $a_if^*(x)q(x) = 0$ for all $i = 1, 2, \ldots, n-s-1$. Since $q(x)$ is a unit we get $a_if^*(x) = 0$. Again by comparing coefficients we can say that the coefficient of highest degree of x is $a_if_{n-s-1}^* = 0$ and since f_{n-s-1}^* is unit we have $a_i = 0$ for all $i = 1, 2, \ldots, n-s-1$. Thus, B is basis for C.

(2) Let $C = \langle f_1(x)+ug(x)+u^2h(x), uf_2(x)+u^2b(x), u^2f_3(x)\rangle$ be a cyclic code over R with $\deg f_1(x) = s_1, \deg f_2(x) = s_2$, and $\deg f_3(x) = s_3$. Since $f_3(x)|f_2(x)|f_1(x)$ and $f_i(x)$s are monic, we have $s_1 > s_2 > s_3$. Next we show that T is a minimal spanning set of C. For this, we need to show that T spans $X = \{f_1(x) + ug(x) + u^2h(x), x(f_1(x) + ug(x) + u^2h(x)), \ldots, x^{n-s_1-1}(f_1(x) + ug(x) + u^2h(x)), uf_2(x) + u^2b(x), x(uf_2(x) + u^2b(x)), \ldots, x^{n-s_2-1}(uf_2(x)) + u^2b(x)), u^2f_3(x), x(u^2f_3(x)), \ldots, x^{n-s_3-1}(u^2f_3(x))\}$ and T is modular independent. We first show that $x^{s_2-s_3}(u^2f_3(x)) \in \text{span}(T)$. Assume that the leading coefficient of $x^{s_2-s_3}f_3(x)$ is a_0 and that of $f_2(x)+ub(x)$ is b_0. Then there exist $c_0 \in \mathbb{Z}_4$ such that $a_0 = c_0b_0$. Since $f_2(x)$ is a monic polynomial, $f_2(x)+ub(x)$ is a regular polynomial too. By division algorithm it can be written as

$$u^2x^{s_2-s_3}f_3(x) = u^2c_0(f_2(x)+ub(x)) + u^2t(x)$$

where $u^2t(x) = u^2f_3(x)\alpha(x)$ is a polynomial in C of degree less than s_2. Since any polynomial in C must have degree greater than or equal to $\deg f_3(x) = s_3$, we have $s_3 \leq \deg t(x) < s_2$. Then

$$u^2t(x) = \alpha_0(u^2f_3(x)) + \alpha_1x(u^2f_3(x)) + \cdots + \alpha_{s_2-s_3-1}x^{s_2-s_3-1}(u^2f_3(x)).$$

Hence, $x^{s_2-s_3}(u^2f_3(x)) \in \text{span}(T)$. Similarly, it can be shown that $x^{s_2-s_3+1}(u^2f_3(x))$, $x^{s_2-s_3+2}(u^2f_3(x)), \ldots,$ $x^{n-s_3-1}(u^2f_3(x)) \in \text{span}(T)$. Now we need to show that $x^{s_1-s_2}(uf_2(x)+u^2b(x)) \in \text{span}(T)$. Assume that the leading coefficient of $x^{s_1-s_2}(f_2(x)+ub(x))$ is a_1 and that of $f_1(x)+ug(x)+u^2h(x)$ is b_1. Then there exists a $c_1 \in \mathbb{Z}_4$ such that $a_1 = b_1c_1$. Since $f_1(x)+ug(x)+u^2h(x)$ is a regular polynomial by Lemma 4.5, we have

$$x^{s_1-s_2}(uf_2(x)+u^2b(x) = c_1u(f_1(x)+ug(x)+u^2h(x)) + ur(x)$$

where $\deg ur(x) < s_1$. Since $ur(x) \in C$ it can be expressed as

$$ur(x) = A(x)(uf_2(x)+u^2b(x)) + B(x)(u^2f_3(x))$$

where $\deg B(x) = s_2 - s_3 - 1$ and $\deg A(x) = k$. Since $\deg ur(x) < s_1$, k must be less than $s_1 - s_2$. It follows that $x^{s_1-s_2}(uf_2(x)+u^2b(x)) \in \text{span}(T)$. In the same way, it can be shown that $x^{s_1-s_2+1}(uf_2(x)+u^2b(x)), \ldots, x^{n-s_2-1}(uf_2(x)+u^2b(x)) \in \text{span}(T)$.

Now we show that T is modular independent. Let $f_1(x)+ug(x)+u^2h(x)=g_0+g_1x+\cdots+g_{s_1}x^{s_1}$, $f_2(x)+ub(x)=b_0+b_1x+\cdots+b_{s_2}x^{s_2}$, and $f_3(x)=f_0+f_1x+\cdots+f_{s_3}x^{s_3}$ be monic polynomials, i.e. g_{s_1}, b_{s_2}, and f_{s_3} are unit. Suppose that there exist three polynomials $k(x)=\sum_{i=0}^{n-s_1-1}k_ix^i\in R[x]$, $l(x)=\sum_{i=0}^{s_1-s_2-1}l_ix^i\in R[x]$, and $m(x)=\sum_{i=0}^{s_2-s_3-1}m_ix^i\in\mathbb{Z}_4[x]$ such that

$$k(x)(f_1(x)+ug(x)+u^2h(x))+l(x)(uf_2(x)+u^2b(x))+m(x)(u^2f_3(x))=0. \tag{4.1}$$

If we compare the coefficients of x^{n-1} on both sides of 4.1 as in *(1)*, then we get $k_{n-s_1-1}g_{s_1}=0$. Since g_{s_1} is unit, we have $k_{n-s_1-1}=0$. If we compare the coefficients of x^{n-2} on both sides of 4.1, then we get $k_{n-s_1-2}g_{s_1}+k_{n-s_1-1}g_{s_1-1}=0$. Since g_{s_1} is unit and $k_{n-s_1-1}=0$, we have $k_{n-s_1-2}=0$. Continuing in the same way as above, we get $k_i=0$ for $i=0,1,...,n-s_1-1$. Also, since u is a zero divisor, the coefficients of x containing any l_i for $i=0,1,\ldots,s_1-s_2-1$ are zero only if $l_i\in<2,u>$. By the same reason, for $j=0,1,\ldots,s_2-s_3-1$, $m_j\in<2,u>$. Therefore, T is modular independent. □

We end this section with an observation about the minimum Hamming weight for a cyclic code of length n over R.

Theorem 4.9 *Let $C=\langle f_1(x)+ug(x)+u^2h(x),uf_2(x)+u^2b(x),u^2f_3(x)\rangle$ be a cyclic code of length n over R. Then $w_H(C)=w_H(Ker\Phi)$, where w_H denotes the Hamming weight.*

Proof Suppose that $r(x)=r_0(x)+u\ r_1(x)+u^2\ r_2(x)\in C$ where $r_0(x),r_1(x),r_2(x)\in\mathbb{Z}_4[x]$. Since $u^2r(x)=u^2r_0(x)\in C$, $w_H(u^2r(x))\leq w_H(r(x))$, i.e. $w_H(u^2C)\leq w_H(C)$. On the other hand, since u^2C is a subcode of C, we have $w_H(C)\leq w_H(u^2C)$. Hence, $w_H(C)=w_H(u^2C)$. □

5. $\mathbb{Z}_4$-images of codes over R

We will be interested in $\mathbb{Z}_4$-images of codes over R. To this end, we define the following Gray-like map from R to $\mathbb{Z}_4^3$:

$$\varphi:\mathbb{Z}_4+u\mathbb{Z}_4+u^2\mathbb{Z}_4\longrightarrow\mathbb{Z}_4^3$$
$$\varphi(a+ub+u^2c)=(a,a+b+c,b).$$

This map is then extended to a map from R^n to $\mathbb{Z}_4^{3n}$. We observe that the $\mathbb{Z}_4$-image of a cyclic code over R under φ is a quasi-cyclic (QC) code.

Theorem 5.1 *Let C be a cyclic code of length n over R. Then $\varphi(C)$ is a 3-QC code of length $3n$ over $\mathbb{Z}_4$.*

Proof Let C be a cyclic code of length n over R and let σ denote the cyclic shift operator. Let $\vec{v}=(v_1,v_2,\ldots,v_n)\in C$, where $v_i=a_i+ub_i+u^2c_i$. Then $\sigma(\vec{v})=(v_n,v_1,\ldots,v_{n-1})\in C$, and $\varphi(\sigma(\vec{v}))=(a_n,a_n+b_n+c_n,b_n,a_1,a_1+b_1+c_1,b_1,\ldots,a_{n-1},a_{n-1}+b_{n-1}+c_{n-1},b_{n-1})$.

On the other hand, we have $\varphi(\vec{v})=(a_1,a_1+b_1+c_1,b_1,\ldots,a_n,a_n+b_n+c_n,b_n)$ and $\sigma^3(\varphi(\vec{v}))=(a_n,a_n+b_n+c_n,b_n,a_1,a_1+b_n+c_1,b_1,\ldots,a_{n-1},a_{n-1}+b_{n-1}+c_{n-1},b_{n-1})$

Therefore, $\sigma^3(\varphi(\vec{v}))=\varphi(\sigma(\vec{v}))\in\varphi(C)$. This means that $\varphi(C)$ is a 3-QC code. □

6. Computational results

We conducted a computer search for cyclic codes of odd length n over R in the special case given in Theorem 4.6. This means that our generators are of the form $\langle f(x)+ug(x)+u^2h(x)\rangle$ where f,g,h are polynomials over $\mathbb{Z}_4$ and f is a generator of a cyclic code of length n over $\mathbb{Z}_4$. We also considered $\mathbb{Z}_4$ images of these cyclic codes over R under the map described in the previous section. Our search yielded a number of new linear codes over $\mathbb{Z}_4$. The tables below contain a subset of those codes for $n=7$. The length of the $\mathbb{Z}_4$-images are therefore 21. Each generator is determined by three polynomials over $\mathbb{Z}_4$. We list the coefficients of the polynomials in descending order, so, for example, the polynomial $2x^4+3x+1$ is represented by 20031. When there is a long string of repetition of a digit d, we abbreviate it in the form d^n. For example, 3^4 represents the polynomial $3x^3+3x^2+3x+3$. We considered both the Lee weight and the Euclidean weight for the $\mathbb{Z}_4$-images of these codes, which are the two most important weights for codes over $\mathbb{Z}_4$. The Lee weight $w_L(x)$ of $x\in\mathbb{Z}_4$ is $\min\{|x|,|4-x|\}$. Hence, the Lee weights of 0,1,2,3 are respectively 0,1,2,1. The Euclidean weight $w_E(x)$ of $x\in\mathbb{Z}_4$ is $\min\{x^2,(4-x)^2\}$. Hence, the Euclidean weights of 0,1,2,3 are respectively 0,1,4,1. The Lee (or Euclidean) weight of a vector in $\mathbb{Z}_4^n$ is then defined as the rational sum of the Lee (Euclidean) weight of its coordinates. Table 1 has codes with Euclidean weights and Table 2 has Lee weights.

There is a database of $\mathbb{Z}_4$ linear codes introduced in [4] and available online (Z4Codes.info). The new codes obtained in this work have been added to this database.

Table 1. Some cyclic codes of length 7 with $\mathbb{Z}_4$-images and Euclidean weights.

f(x)	**g(x)**	**h(x)**	**Parameters of $\mathbb{Z}_4$ image**
1113313	2000222	110300	$[21,4^2 2^{15},8]$
2	3313313	313312	$[21,4^1 2^{20},4]$
20222	2002	233202	$[21,4^3 2^9,8]$
$1^6 3$	3113111	3113132	$[21,4^3 2^{18},4]$
2	23213	2303332	$[21,4^4 2^{17},3]$
$1^6 3$	1123003	2101301	$[21,4^5 2^{16},4]$
11323	2200202	2223112	$[21,4^6 2^{12},7]$
11323	220	2031110	$[21,4^6 2^{14},6]$
11323	$1^6 3$	1122132	$[21,4^7 2^{14},4]$
12333	1313113	1123320	$[21,4^8 2^{12},4]$
3^7	120213	3011120	$[21,4^9 2^6,3]$
12313	233301	202121	$[21,4^9 2^8,6]$
1211	3311113	3232310	$[21,4^9 2^{12},4]$
11303	101332	2001210	$[21,4^{10} 2^9,4]$
11323	2312102	3212330	$[21,4^{10} 2^{11},3]$
3231	22020	3313312	$[21,4^{11} 2^1,6]$
1211	1303201	3020223	$[21,4^{11} 2^{10},4]$
11	200	23002	$[21,4^{12} 2^9,4]$
10113	110023	1033223	$[21,4^{13} 2^2,4]$
10113	2210110	2031121	$[21,4^{13} 2^5,3]$
3231	102133	3133202	$[21,4^{14} 2^1,4]$
1211	3322310	3332300	$[21,4^{14} 2^7,2]$
31	3103003	203120	$[21,4^{15} 2^5,4]$
11	3100121	1103323	$[21,4^{15} 2^6,3]$
31	3312122	321201	$[21,4^{16} 2^3,3]$

Table 2. Some cyclic codes of length 7 with $\mathbb{Z}_4$-images and Lee weights.

$\mathbf{f(x)}$	$\mathbf{g(x)}$	$\mathbf{h(x)}$	**Parameters of $\mathbb{Z}_4$ image**
1113313	2000222	110300	$[21, 4^2 2^{15}, 4]$
22	3131333	221212	$[21, 4^2 2^{18}, 2]$
22202	1130120	2120111	$[21, 4^3 2^{12}, 4]$
2	1302030	3220121	$[21, 4^4 2^{14}, 4]$
$1^6 3$	3223011	2202002	$[21, 4^5 2^{15}, 4]$
11323	202	2031110	$[21, 4^6 2^{14}, 4]$
$1^6 3$	230110	3212323	$[21, 4^6 2^{15}, 2]$
1113133	3210231	101213	$[21, 4^8 2^6, 4]$
$1^6 3$	3011032	21322	$[21, 4^8 2^{13}, 2]$
11303	3132322	3122031	$[21, 4^9 2^9, 4]$
3231	22020	3313312	$[21, 4^{11} 2^1, 6]$
1211	1021310	1223110	$[21, 4^{11} 2^9, 4]$
1321	2133	301302	$[21, 4^{12} 2^6, 4]$
10113	110023	1033223	$[21, 4^{13} 2^2, 4]$
3121	3122301	1101123	$[21, 4^{14} 2^0, 4]$
31	1320101	3212112	$[21, 4^{15} 2^3, 4]$
11	2120113	3200330	$[21, 4^{15} 2^6, 2]$
31	3211101	1330033	$[21, 4^{16} 2^0, 4]$

7. Conclusion

In this paper, Galois extensions of the ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$ and the ideal structure of these extensions are investigated. These results are used in the study of cyclic codes over R. The general form of the generators of a cyclic code is determined and minimal spanning sets of such codes are found. Finally, we employed these results to conduct a computer search and obtained many cyclic codes over R whose $\mathbb{Z}_4$ images yielded new linear codes over $\mathbb{Z}_4$.

Acknowledgment

We thank the referees for useful suggestions to improve the presentation of this paper.

References

[1] Abualrub T. Cyclic codes over the ring of integers mod m. PhD, University of Iowa, Iowa City, IA, USA, 1988.

[2] Abualrub T, Siap I. Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$. Design Code Cryptogr 2007; 42: 271-287.

[3] Al-Ashker M, Chen J. Cyclic codes of arbitrary length over $\mathbb{F}_q + u\mathbb{F}_q + ... + u^{k-1}\mathbb{F}_q$. Palestine J Math 2013; 2: 72-80.

[4] Aydin N, Asamov T. A database of $\mathbb{Z}_4$-codes. J Comb Inf Syst Sci 2009; 34: 1-12.

[5] Bonnecaze A, Udaya P. Cyclic codes and self dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE T Inform Theory 1999; 45: 1250-1255.

[6] Dingh HQ, Permóuth SL. Cyclic and negacyclic codes over finite chain rings. IEEE T Inform Theory 2004; 50: 1728-1744.

[7] Dougherty ST, Liu H. Independence of vectors in codes over rings. Design Code Cryptogr 2009; 51: 5568.

[8] Gao J, Fu FW, Xiao L, Bandi RK. Some results on cyclic codes over $\mathbb{Z}_q + u\mathbb{Z}_q$. Discrete Math Algorithms Appl 2015; 7: 1550058.

[9] MacDonald BR. Finite Rings with Identity. New York, NY, USA: Marcel Dekker, 1974.

[10] Singh AK, Kewat PK. On cyclic codes over the ring $\mathbb{Z}_p[u]/ < u^k >$. Design Code Cryptogr 2015; 74: 1-13.

[11] Wan ZX. Finite Fields and Galois Rings. Singapore: World Scientific, 2003.

[12] Yildiz B, Aydin N. On cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and $\mathbb{Z}_4$ images. Int J Inf Coding Theory 2014; 2: 226-237.

[13] Yildiz B, Karadeniz S. Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. Design Code Cryptogr 2011; 58: 221-234.