



Complete classification for simple root cyclic codes over the local ring $\mathbb{Z}_4[v]/\langle v^2 + 2v \rangle$

Yuan Cao^{1,2,3} · Yonglin Cao¹

Received: 18 October 2017 / Accepted: 3 September 2019 / Published online: 7 October 2019
© Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract

Let $R = \mathbb{Z}_4[v]/\langle v^2 + 2v \rangle$. Then R is a local non-principal ideal ring of 16 elements. First, we give the structure of every cyclic code of odd length n over R and obtain a complete classification for these codes. Then we determine the cardinality, the type and its dual code for each of these cyclic codes. Moreover, we determine all self-dual cyclic codes of odd length n over R and provide a clear formula to count the number of these self-dual cyclic codes. Finally, we list some optimal 2-quasi-cyclic self-dual linear codes of length 30 over \mathbb{Z}_4 and obtain 4-quasi-cyclic and formally self-dual binary linear $[60, 30, 12]$ codes derived from cyclic codes of length 15 over $\mathbb{Z}_4[v]/\langle v^2 + 2v \rangle$.

Keywords Cyclic code · Dual code · Self-dual code · Galois ring · Local ring

Mathematics Subject Classification (2010) 94B15 · 94B05 · 11T71

1 Introduction

The catalyst for the study of codes over rings was the discovery of the connection between linear codes over \mathbb{Z}_4 and the Kerdock and Preparata codes, which are non-linear binary codes [2, 3]. Soon after this discovery, codes over many different rings were studied. This led to many new discoveries and concreted the study of codes over rings as an important part of the coding theory discipline. Since \mathbb{Z}_4 is a chain ring, it was natural to expand the

✉ Yonglin Cao
ylcao@sdut.edu.cn

Yuan Cao
yuanco@sdut.edu.cn

¹ School of Mathematics and Statistics, Shandong University of Technology, Zibo, Shandong 255091, China

² Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China

³ Hunan Provincial Key Laboratory of Mathematical Modeling and Analysis in Engineering, Changsha University of Science and Technology, Changsha, Hunan 410114, China

theory to focus on alphabets that are finite commutative chain rings (see [1, 4–6, 11, 12, 16, 17, 19] and [20], for examples) and other type of rings [7, 18].

In 1999, Wood in [23] showed that for certain reasons finite Frobenius rings are the most general class of rings that should be used for alphabets of codes. Then self-dual codes over commutative Frobenius rings were investigated in Dougherty et al. [13]. Especially, codes over an extension rings of \mathbb{Z}_4 were studied in Yildiz et al. [25] and [26] where many good \mathbb{Z}_4 -codes were obtained as images. The ring in the mentioned works was described as $\mathbb{Z}_4[u]/\langle u^2 \rangle = \mathbb{Z}_4 + u\mathbb{Z}_4$ ($u^2 = 0$) which is a local non-principal ring. Shi et al. in [18] studied $(1+2u)$ -constacyclic codes of odd length n over the ring $\mathbb{Z}_4[u]/\langle u^2-1 \rangle = \mathbb{Z}_4+u\mathbb{Z}_4$ ($u^2 = 1$) which is another extension ring of \mathbb{Z}_4 . Properties of these codes and their \mathbb{Z}_4 images were investigated.

Let A be an arbitrary finite commutative ring with identity $1 \neq 0$, and A^\times be the multiplicative group of invertible elements (units) in A . For any $a \in A$, we denote by $\langle a \rangle_A$, or $\langle a \rangle$ for simplicity, the ideal of A generated by a , i.e. $\langle a \rangle_A = aA$. For any ideal I of A , we will identify the element $a + I$ of the residue class ring A/I with $a \pmod I$ in this paper.

For any positive integer N , let $A^N = \{(a_0, a_1, \dots, a_{N-1}) \mid a_i \in A, i = 0, 1, \dots, N-1\}$ which is an A -module with componentwise addition and scalar multiplication by elements of A . Then an A -submodule \mathcal{C} of A^N is called a *linear code* of length N over A . For any vectors $a = (a_0, a_1, \dots, a_{N-1}), b = (b_0, b_1, \dots, b_{N-1}) \in A^N$. The usual *Euclidian inner product* of a and b is defined by $[a, b] = \sum_{j=0}^{N-1} a_j b_j \in A$. Then $[-, -]$ is a symmetric and non-degenerate bilinear form on the A -module A^N . Let \mathcal{C} be a linear code of length N over A . The *dual code* of \mathcal{C} is defined by $\mathcal{C}^\perp = \{a \in A^N \mid [a, b] = 0, \forall b \in \mathcal{C}\}$, and \mathcal{C} is said to be *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$. A linear code \mathcal{C} of length N over A is said to be *cyclic* if $(a_{N-1}, a_0, a_1, \dots, a_{N-2}) \in \mathcal{C}$ for all $(a_0, a_1, \dots, a_{N-1}) \in \mathcal{C}$. Let A be a local ring with residue class field F . Then cyclic codes of length N over R are called *simple root cyclic codes* if $\gcd(N, \text{char}(F)) = 1$.

In this paper, every vector $c = (c_0, c_1, \dots, c_{N-1}) \in A^N$ is viewed as the polynomial $c(x) = \sum_{j=0}^{N-1} c_j x^j$. Then every cyclic code \mathcal{C} is viewed as an ideal in the polynomial residue ring $A[x]/\langle x^N - 1 \rangle$.

In this paper, we adopt the following notation:

- ◊ $\mathbb{Z}_2 = \{0, 1\}$ in which the arithmetic is done modulo 2. Then \mathbb{Z}_2 is a binary finite field.
- ◊ $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ in which the arithmetic is done modulo 4. Then \mathbb{Z}_4 is a finite chain ring with the maximal ideal $2\mathbb{Z}_4 = \{0, 2\}$.
- ◊ $R = \mathbb{Z}_4[v]/\langle v^2 + 2v \rangle = \{a + bv \mid a, b \in \mathbb{Z}_4\} = \mathbb{Z}_4 + v\mathbb{Z}_4$ ($v^2 = 2v$) in which the operations are defined by:

$$\alpha + \beta = (a + c) + v(b + d) \text{ and } \alpha\beta = ac + (ad + bc + 2bd)v,$$

for any $\alpha = a + bv, \beta = c + dv \in \mathbb{Z}_4 + v\mathbb{Z}_4$ with $a, b, c, d \in \mathbb{Z}_4$. Then R is a local Frobenius non-chain ring of 16 elements.

In 2015, linear codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ ($v^2 = 2v$) were studied in [15]. In the paper, a duality preserving Gray map was given and used to present MacWilliams identities and self-dual codes. Some extremal Type II \mathbb{Z}_4 -codes were provided as images of codes over this ring. Recently, we gave a complete classification for negacyclic codes of length $2n$ over $\mathbb{Z}_4 + v\mathbb{Z}_4$, where n is odd, and obtained some good and new self-dual \mathbb{Z}_4 -codes which are Gray images of self-dual negacyclic codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ ([8]).

Now, we follow this line to continue studying cyclic codes of length n over $R = \mathbb{Z}_4 + v\mathbb{Z}_4$, where n is a positive odd integer and $n \geq 3$.

The rest of the paper is organized as follows. In Section 2, we give an explicit representation for every cyclic code of length n over R by determining their generator sets as ideals in the ring $R[x]/\langle x^n - 1 \rangle$. In Section 3, we determine the dual code for each code, present explicitly all distinct self-dual cyclic codes of length n over R and give a clear formula to count the number of all these self-dual cyclic codes. In Section 4, we present all 583443 cyclic codes of length 15 over R and list all 315 self-dual codes among them. As applications, we obtain 162 good self-dual quasi-cyclic codes of index 2 and length 30 with minimum Lee weight 10 and 12 over \mathbb{Z}_4 . From these \mathbb{Z}_4 -codes, we derive 70 quasi-cyclic type II binary formal self-dual $[60, 30, 12]$ codes of index 4.

2 Cyclic codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ of odd length

In this section, we consider cyclic codes of odd length n over the ring $R = \mathbb{Z}_4[v]/\langle v^2 + 2v \rangle = \mathbb{Z}_4 + v\mathbb{Z}_4$ ($v^2 = 2v$), i.e., ideals of the ring

$$R[x]/\langle x^n - 1 \rangle = \left\{ \sum_{i=0}^{n-1} r_i x^i \mid r_i \in R, i = 0, 1, \dots, n - 1 \right\}$$

in which the arithmetic is done modulo $x^n - 1$. From now on, we denote

- $\mathcal{A} = \mathbb{Z}_4[x]/\langle x^n - 1 \rangle = \left\{ \sum_{i=0}^{n-1} a_i x^i \mid a_i \in \mathbb{Z}_4, i = 0, 1, \dots, n - 1 \right\}$

in which the arithmetic is done modulo $x^n - 1$.

Then \mathcal{A} is a finite commutative ring containing \mathbb{Z}_4 as its subring.

- $\mathcal{A} + v\mathcal{A} = \mathcal{A}[v]/\langle v^2 + 2v \rangle = \{ \alpha + \beta v \mid \alpha, \beta \in \mathcal{A} \}$ ($v^2 = 2v$) and the operations are defined by: for any $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathcal{A}$, we have

$$\begin{aligned} (\alpha_1 + \beta_1 v) + (\alpha_2 + \beta_2 v) &= (\alpha_1 + \alpha_2) + v(\beta_1 + \beta_2); \\ (\alpha_1 + \beta_1 v)(\alpha_2 + \beta_2 v) &= \alpha_1 \alpha_2 + v(\alpha_1 \beta_2 + \beta_1 \alpha_2 + 2\beta_1 \beta_2). \end{aligned}$$

Then $\mathcal{A} + v\mathcal{A}$ is a finite commutative local ring containing \mathcal{A} as its subring.

Let $\alpha, \beta \in \mathcal{A}$. Then α and β can be uniquely expressed as $\alpha = \sum_{i=0}^{n-1} a_i x^i$ and $\beta = \sum_{i=0}^{n-1} b_i x^i$ respectively, where $a_i, b_i \in \mathbb{Z}_4$ for all $i = 0, 1, \dots, n - 1$. Now, define a map $\Theta : \mathcal{A} + v\mathcal{A} \rightarrow R[x]/\langle x^n - 1 \rangle$ by

$$\Theta(\alpha + \beta v) = \sum_{i=0}^{n-1} \xi_i x^i, \text{ where } \xi_i = a_i + b_i v \in R, i = 0, 1, \dots, n - 1.$$

Then one can easily verify the following conclusion.

Lemma 1 *The map Θ defined above is an isomorphism of rings from $\mathcal{A} + v\mathcal{A}$ onto $R[x]/\langle x^n - 1 \rangle$.*

In the following, we will identify $\mathcal{A} + v\mathcal{A}$ with $R[x]/\langle x^n - 1 \rangle$ under the ring isomorphism Θ . Therefore, in order to determine all cyclic codes of length n over R , we only need to determine all ideals of the ring $\mathcal{A} + v\mathcal{A}$. To do this, we investigate the structure of the ring \mathcal{A} first.

In this paper, we will regard \mathbb{Z}_2 as a subset of the ring \mathbb{Z}_4 although \mathbb{Z}_2 is not a subring of \mathbb{Z}_4 . Then every element a of \mathbb{Z}_4 has a unique 2-adic expansion: $a = a_0 + 2a_1$, $a_0, a_1 \in \mathbb{Z}_2$. Define $\bar{a} = a_0 = a \pmod{2}$ for all $a \in \mathbb{Z}_4$. This map $\bar{}$ is a surjective homomorphism

of rings from \mathbb{Z}_4 onto \mathbb{Z}_2 , which can be extended into a surjective homomorphism of rings from $\mathbb{Z}_4[x]$ onto $\mathbb{Z}_2[x]$ in the natural way:

$$\overline{f}(x) = \overline{f(x)} = \sum_k \overline{f_k}x^k, \forall f(x) = \sum_k f_kx^k \in \mathbb{Z}_4[x] \text{ where } a_k \in \mathbb{Z}_4.$$

Let $g(x)$ be a monic polynomial in $\mathbb{Z}_4[x]$ of positive integer. Then $g(x)$ is said to be *basic irreducible* if $\overline{g}(x)$ is an irreducible polynomial in $\mathbb{Z}_2[x]$.

As n is odd, by [22, Theorem 13.8] there are pairwise coprime monic basic irreducible polynomials $f_0(x) = x - 1, f_1(x), \dots, f_r(x) \in \mathbb{Z}_4[x]$ such that

$$x^n - 1 = f_0(x)f_1(x) \dots f_r(x), \tag{1}$$

where $\overline{f_j}(x)$ is irreducible in $\mathbb{Z}_2[x]$ and $\deg(f_j(x)) = m_j$ for all $j = 0, 1, \dots, r$. Especially, $f_0(x) = x - 1$ with degree $m_0 = 1$.

For each integer $j, 0 \leq j \leq r$, denote $F_j(x) = \frac{x^n-1}{f_j(x)} \in \mathbb{Z}_4[x]$. Since $\gcd(\overline{F_j}(x), \overline{f_j}(x)) = 1$, we see that $F_j(x)$ and $f_j(x)$ are coprime in $\mathbb{Z}_4[x]$ (cf. [22, Lemma 13.5]). Hence there are polynomials $c_j(x), d_j(x) \in \mathbb{Z}_4[x]$ such that

$$c_j(x)F_j(x) + d_j(x)f_j(x) = 1. \tag{2}$$

In this paper, we adopt the following notation:

- Let $e_j(x) \in \mathcal{A}$ satisfying

$$e_j(x) \equiv c_j(x)F_j(x) = 1 - d_j(x)f_j(x) \pmod{x^n - 1}. \tag{3}$$

- Denote $\mathcal{K}_j = \mathbb{Z}_4[x]/\langle f_j(x) \rangle = \left\{ \sum_{i=0}^{m_j-1} a_i x^i \mid a_i \in \mathbb{Z}_4, i = 0, 1, \dots, m_j - 1 \right\}$ in which the arithmetic is done modulo $f_j(x)$. Then \mathcal{K}_j is a Galois ring of characteristic 4 and cardinality 4^{m_j} (cf. [22, Theorem 14.1]).
- Let $\mathcal{K}_j + v\mathcal{K}_j = \mathcal{K}_j[v]/(v^2 + 2v) = \{\alpha + \beta v \mid \alpha, \beta \in \mathcal{K}_j\}$ ($v^2 = 2v$) and the operations are defined by: for any $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathcal{K}_j$, we have

$$\begin{aligned} (\alpha_1 + \beta_1 v) + (\alpha_2 + \beta_2 v) &= (\alpha_1 + \alpha_2) + v(\beta_1 + \beta_2); \\ (\alpha_1 + \beta_1 v)(\alpha_2 + \beta_2 v) &= \alpha_1\alpha_2 + v(\alpha_1\beta_2 + \beta_1\alpha_2 + 2\beta_1\beta_2). \end{aligned}$$

Then $\mathcal{K}_j + v\mathcal{K}_j$ is a finite commutative local ring containing \mathcal{K}_j as its subring.

By [21, Theorem 2.7] and [7, Lemma 3.2], one can easily deduce the following conclusions.

Lemma 2 *Using the notation above, we have the following conclusions:*

- (i) $e_0(x) + e_1(x) + \dots + e_r(x) = 1, e_j(x)^2 = e_j(x)$ and $e_j(x)e_l(x) = 0$ in the ring \mathcal{A} for all $0 \leq j \neq l \leq r$.
- (ii) For each integer $j, 0 \leq j \leq r, Ae_j(x)$ is a subring of \mathcal{A} with $e_j(x)$ as its multiplicative identity. Define

$$\varphi_j(a(x)) = a(x)e_j(x) \pmod{x^n - 1}, \forall a(x) \in \mathcal{K}_j.$$

Then φ_j is a ring isomorphism from \mathcal{K}_j onto $Ae_j(x)$ with inverse φ_j^{-1} :

$$\varphi_j^{-1}(c(x)) = c(x) \pmod{f_j(x)}, \forall c(x) \in Ae_j(x).$$

(iii) For any $a_j(x) \in \mathcal{K}_j$ and $j = 0, 1, \dots, r$, define

$$\varphi(a_0(x), a_1(x), \dots, a_r(x)) = \sum_{j=0}^r \varphi_j(a_j(x)) = \sum_{j=0}^r e_j(x)a_j(x) \pmod{x^n - 1}.$$

Then φ is a ring isomorphism from $\mathcal{K}_0 \times \mathcal{K}_1 \times \dots \times \mathcal{K}_r$ onto \mathcal{A} .

Now, we give structural properties for cyclic codes of length n over R .

Lemma 3 *Let $\mathcal{C} \subseteq \mathcal{A} + v\mathcal{A}$. Then \mathcal{C} is a cyclic code of length n over R if and only if for each integer $j, 0 \leq j \leq r$, there is a unique ideal C_j of the ring $\mathcal{K}_j + v\mathcal{K}_j$ ($v^2 = 2v$) such that*

$$\mathcal{C} = e_0(x)C_0 \oplus e_1(x)C_1 \oplus \dots \oplus e_r(x)C_r \pmod{x^n - 1}$$

where

$$e_j(x)C_j = \{e_j(x)\alpha + ve_j(x)\beta \mid \alpha + \beta v \in C_j, \alpha, \beta \in \mathcal{K}_j\} \subseteq \mathcal{A} + v\mathcal{A}$$

for all $j = 0, 1, \dots, r$. Then the number of codewords in \mathcal{C} equals $\prod_{j=0}^r |C_j|$.

Proof For any $\xi_j = \alpha_j + \beta_j v \in \mathcal{K}_j + v\mathcal{K}_j$ with $\alpha_j, \beta_j \in \mathcal{K}_j$ for all $j = 0, 1, \dots, r$, we define

$$\begin{aligned} \Phi(\xi) &= \sum_{j=0}^r e_j(x)\xi_j = \sum_{j=0}^r e_j(x)(\alpha_j + v\beta_j) = \sum_{j=0}^r e_j(x)\alpha_j + v \sum_{j=0}^r e_j(x)\beta_j \\ &= \varphi(\alpha_0, \alpha_1, \dots, \alpha_r) + v\varphi(\beta_0, \beta_1, \dots, \beta_r). \end{aligned}$$

Then Φ is an isomorphism of rings from the direct product ring $(\mathcal{K}_0 + v\mathcal{K}_0) \times (\mathcal{K}_1 + v\mathcal{K}_1) \times \dots \times (\mathcal{K}_r + v\mathcal{K}_r)$ onto $\mathcal{A} + v\mathcal{A}$. This conclusion can be proved by Lemma 2 similarly as that for [8, Theorem 4.2(i)]. Here, we omit it.

From the properties of ring isomorphisms and direct product rings, we conclude that \mathcal{C} is a cyclic code of length n over R , i.e. \mathcal{C} is an ideal of $\mathcal{A} + v\mathcal{A}$, if and only if for each integer $j, 0 \leq j \leq r$, there is a unique ideal C_j of the ring $\mathcal{K}_j + v\mathcal{K}_j$ such that

$$\begin{aligned} \mathcal{C} &= \Phi(C_0 \times C_1 \times \dots \times C_r) = \{\Phi(\xi_0, \xi_1, \dots, \xi_r) \mid \xi_j \in C_j, j = 0, 1, \dots, r\} \\ &= \left\{ \sum_{j=0}^r e_j(x)\xi_j \mid \xi_j \in C_j, j = 0, 1, \dots, r \right\} = \sum_{j=0}^r e_j(x)\{\xi_j \mid \xi_j \in C_j\}. \end{aligned}$$

Hence $\mathcal{C} = \bigoplus_{j=0}^r e_j(x)C_j \pmod{x^n - 1}$ and $|\mathcal{C}| = |C_0 \times C_1 \times \dots \times C_r| = \prod_{j=0}^r |C_j|$. \square

By Lemma 3, it is sufficient to determine the ideals of the ring $\mathcal{K}_j + v\mathcal{K}_j$ for all j , in order to determine cyclic codes of length n over R .

As \mathcal{K}_j is a subring of $\mathcal{K}_j + v\mathcal{K}_j$, we can regard $\mathcal{K}_j + v\mathcal{K}_j$ as a \mathcal{K}_j -module. Precisely, $\mathcal{K}_j + v\mathcal{K}_j$ is a free \mathcal{K}_j -module with basis $\{1, v\}$. Let $\mathcal{K}_j^2 = \{(\alpha, \beta) \mid \alpha, \beta \in \mathcal{K}_j\}$. Then \mathcal{K}_j^2 is a free \mathcal{K}_j -module of rank 2 with the componentwise addition and scalar multiplication. Now, define

$$\sigma : \mathcal{K}_j^2 \rightarrow \mathcal{K}_j + v\mathcal{K}_j \text{ via } (\alpha, \beta) \mapsto \alpha + \beta v \ (\forall \alpha, \beta \in \mathcal{K}_j).$$

Then it is obvious that σ is an isomorphism of \mathcal{K}_j -modules from \mathcal{K}_j^2 onto $\mathcal{K}_j + v\mathcal{K}_j$. Moreover, we have the following key conclusion.

Lemma 4 (cf. [10, Lemma 3.4]) *Let $0 \leq j \leq r$. Then C_j is an ideal of the ring $\mathcal{K}_j + v\mathcal{K}_j$ if and only if there is a unique \mathcal{K}_j -submodule S_j of \mathcal{K}_j^2 satisfying the following condition*

$$(0, \alpha + 2\beta) \in S_j, \forall(\alpha, \beta) \in S_j \tag{4}$$

such that $\sigma(S_j) = C_j$.

Therefore, in order to determine all ideals of $\mathcal{K}_j + v\mathcal{K}_j$ ($0 \leq j \leq r$), it is sufficient to determine all \mathcal{K}_j -submodule of \mathcal{K}_j^2 satisfying Condition (4). To do this, we sketch some basic theory of linear codes over Galois rings.

In the rest of the paper, for each integer j , $0 \leq j \leq r$, we denote

- $T_j = \{\sum_{j=0}^{m-1} a_j x^j \mid a_j \in \mathbb{Z}_2\} \subseteq \mathcal{K}_j$;
- $F_j = \mathbb{Z}_2[x]/\langle \bar{f}_j(x) \rangle = \{\sum_{j=0}^{m-1} a_j x^j \mid a_j \in \mathbb{Z}_2\}$ in which the arithmetic is done modulo $\bar{f}_j(x)$ in the polynomial ring $\mathbb{Z}_2[x]$.

Then F_j is an extension field of the binary field \mathbb{Z}_2 of 2^{m_j} elements, and T_j is a subset of \mathcal{K}_j since we regard \mathbb{Z}_2 as a subset of \mathbb{Z}_4 .

To reduce the number of symbols, in this paper we will identify T_j with F_j . Whether T_j is a subset of the Galois ring \mathcal{K}_j or a finite field itself, the reader can easily determine what it means according to the context. In this sense, each element α of \mathcal{K}_j has a unique 2-adic expansion:

$$\alpha = t_0(x) + 2t_1(x), \text{ where } t_0(x), t_1(x) \in T_j.$$

Then $\alpha \in \mathcal{K}_j^\times$ if and only if $t_0(x) \neq 0$. Hence $|\mathcal{K}_j^\times| = (2^{m_j} - 1)2^{m_j}$.

Let $0 \leq j \leq r$ and $L \geq 2$ be a positive integer. Assume S is a linear code of length L over the Galois ring \mathcal{K}_j . By [16, Definition 3.1], a matrix G is called a *generator matrix* for S if the rows of G span S and none of them can be written as an \mathcal{K}_j -linear combination of the other rows of G . Moreover, a generator matrix G is said to be *in standard form* if there is a suitable permutation matrix U of size $L \times L$ such that

$$G = \begin{pmatrix} I_{k_0} & M_{0,1} & M_{0,2} \\ 0 & 2I_{k_1} & 2M_{1,2} \end{pmatrix} U$$

where the columns are grouped into blocks of column sizes k_0, k_1, k with $k_i \geq 0, k = L - (k_0 + k_1)$, $M_{0,2}$ is a matrix over \mathcal{K}_j , $M_{0,1}$ and $M_{1,2}$ are matrices over T_j . Of course, if $k_i = 0$, the matrices $2^i I_{k_i}$ and $2^i M_{i,t}$ ($i = 0, 1$) are suppressed in G . In this case, the following map

$$(\xi, \eta) \mapsto (\xi, \eta)G = (\xi(I_{k_0}, M_{0,1}, M_{0,2}) + \eta(0, 2I_{k_1}, 2M_{1,2}))U$$

(for any $\xi = (\alpha_1, \dots, \alpha_{k_0}) \in \mathcal{K}_j^{k_0}$ and $\eta = (b_1, \dots, b_{k_1}) \in F_j^{k_1}$) is an isomorphism of groups from $(\mathcal{K}_j^{k_0} \times F_j^{k_1}, +)$ onto $(S, +)$. Hence S is an abelian group of type $4^{k_0 m_j} 2^{k_1 m_j}$ and contain $2^{(2k_0+k_1)m_j}$ codewords.

All distinct nontrivial linear codes of length 2 over finite chain rings had been determined (by [9, Example 2.5], for example). Moreover, we have

Lemma 5 *All distinct linear code S_j of length 2 over the Galois ring $\mathcal{K}_j = \mathbb{Z}_4[x]/\langle f_j(x) \rangle$ satisfying Condition (4) in Lemma 4 are given by the following table, where G is a generator matrix of S_j :*

Case	G	type of S_j	$ S_j $
(i)	I_2	$4^{2m_j} 2^0$	2^{4m_j}
	$2I_2$	$4^0 2^{2m_j}$	2^{2m_j}
	0	$4^0 2^0$	1
(ii)	$(2w_j(x), 1)$, where $w_j(x) \in T_j$ arbitrary	$4^{m_j} 2^0$	2^{2m_j}
(iii)	$(0, 2)$	$4^0 2^{m_j}$	2^{m_j}
(iv)	$\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$	$4^{m_j} 2^{m_j}$	2^{3m_j}

Then the number of all codes listed above is equal to $2^{m_j} + 5$.

Proof By $2^2 = 0$ and [9, Example 2.5] we know that the number of linear codes over the Galois ring \mathcal{K}_j of length 2 is equal to $\sum_{i=0}^2 (2i + 1) |T_j|^{2-i} = \sum_{i=0}^2 (2i + 1) 2^{(2-i)m_j} = 4^{m_j} + 3 \cdot 2^{m_j} + 5$. Precisely, every nontrivial linear code S over \mathcal{K}_j of length 2 has one and only one of the following matrices G as its generator matrix:

1. $G = (1, a(x))$, $\forall a(x) \in \mathcal{K}_j$.
2. $G = (2, 2b(x))$, $\forall b(x) \in T_j$.
3. $G = (2w(x), 1)$, $\forall w(x) \in T_j$.
4. $G = (0, 2)$.
5. $G = 2I_2$.
6. $G = \begin{pmatrix} 1 & c(x) \\ 0 & 2 \end{pmatrix}$, $\forall c(x) \in T_j$.
7. $G = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$.

Then by ordinary careful calculations (cf. [10, Appendix]), we obtain the conclusions. \square

As the end of this section, for any integer j , $0 \leq j \leq r$, we determine the ideals of $\mathcal{K}_j + v\mathcal{K}_j$ and their annihilating ideals. For any ideal C of $\mathcal{K}_j + v\mathcal{K}_j$, its annihilating ideal is defined by $\text{Ann}(C) = \{\beta \in \mathcal{K}_j + v\mathcal{K}_j \mid \alpha\beta = 0, \forall \alpha \in C\}$.

Theorem 1 *Let $0 \leq j \leq r$. Then all distinct ideals C_j and their annihilating ideals of the ring $\mathcal{K}_j + v\mathcal{K}_j$ ($v^2 = 2v$) are given by the following table.*

N	C_j	Type of C_j	$ C_j $	$\text{Ann}(C_j)$
I	$\langle 1 \rangle$	$4^{2m_j} 2^0$	2^{4m_j}	$\langle 0 \rangle$
I	$\langle 2 \rangle$	$4^0 2^{2m_j}$	2^{2m_j}	$\langle 2 \rangle$
I	$\langle 0 \rangle$	$4^0 2^0$	1	$\langle 1 \rangle$
2^{m_j}	$\langle 2w_j(x) + v \rangle$	$4^{m_j} 2^0$	2^{2m_j}	$\langle 2(1 + w_j(x)) + v \rangle$
I	$\langle 2v \rangle$	$4^0 2^{m_j}$	2^{m_j}	$\langle 2, v \rangle$
I	$\langle 2, v \rangle$	$4^{m_j} 2^{m_j}$	2^{3m_j}	$\langle 2v \rangle$

where $w_j(x) \in T_j$ arbitrary and N is the number of ideals in the same row.

Therefore, the number of ideals in $\mathcal{K}_j + v\mathcal{K}_j$ is $2^{m_j} + 5$.

Proof It follows from Lemma 4, Lemma 5 and the definition for the \mathcal{K}_j -module isomorphism σ from \mathcal{K}_j^2 onto $\mathcal{K}_j + v\mathcal{K}_j$, immediately. Here, we omit these details. \square

As stated above, by Lemma 3 and Theorem 1 we conclude that the number of cyclic codes over R of odd length n is equal to $\prod_{j=0}^r (2^{m_j} + 5)$. Precisely, all these cyclic codes can be listed easily by Lemma 3 and Theorem 1.

Using the notation of Lemma 3, $\mathcal{C} = \bigoplus_{j=0}^r e_j(x)C_j$ is called the canonical form decomposition of the cyclic code \mathcal{C} with length n over R .

3 Self-dual cyclic codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ of odd length

In this section, we consider how to determine all distinct self-dual cyclic codes over $R = \mathbb{Z}_4 + v\mathbb{Z}_4$ of odd length n precisely. To do this, we need to give the dual code for each cyclic code over R of length n first.

As $x^n = 1$ in the ring $\mathcal{A} = \mathbb{Z}_4[x]/\langle x^n - 1 \rangle$, we have $x^{-1} = x^{n-1}$. For any $\alpha(x) = \sum_{i=0}^{n-1} \alpha_i x^i \in R[x]/\langle x^n - 1 \rangle$, where $\alpha_i = a_i + vb_i \in R$ with $a_i, b_i \in \mathbb{Z}_4$ for all $0 \leq i \leq n-1$, we have that $\alpha(x) = a(x) + vb(x)$ where $a(x), b(x) \in \mathcal{A}$ given by $a(x) = \sum_{i=0}^{n-1} a_i x^i$ and $b(x) = \sum_{i=0}^{n-1} b_i x^i$. Now, we define

$$\tau(\alpha(x)) = \alpha(x^{-1}) = \alpha_0 + \sum_{i=1}^{n-1} \alpha_i x^{n-i} = a(x^{-1}) + vb(x^{-1}),$$

where $a(x^{-1}) = a_0 + \sum_{i=1}^{n-1} a_i x^{n-i}$, $b(x^{-1}) = b_0 + \sum_{i=1}^{n-1} b_i x^{n-i} \in \mathcal{A}$. It can be verified easily that the map τ is a ring automorphism of $R[x]/\langle x^n - 1 \rangle$. Moreover, the following conclusion is well known.

Lemma 6 For any cyclic code \mathcal{C} of length n over R , its dual code is given by $\mathcal{C}^\perp = \tau(\text{Ann}(\mathcal{C})) = \{a(x^{-1}) \mid a(x) \in \text{Ann}(\mathcal{C})\}$, where

$$\text{Ann}(\mathcal{C}) = \{\eta \in R[x]/\langle x^n - 1 \rangle \mid \xi\eta = 0, \forall \xi \in \mathcal{C}\}$$

is the annihilating ideal of \mathcal{C} in $R[x]/\langle x^n - 1 \rangle$.

Since $R[x]/\langle x^n - 1 \rangle = \mathcal{A} + v\mathcal{A}$ ($v^2 = 2v$) by Lemma 1, we see that the restriction of τ on its subring \mathcal{A} is a ring automorphism of \mathcal{A} . We still denote this ring automorphism by τ . Then $\tau(a(x)) = a(x^{-1})$ for all $a(x) \in \mathcal{A}$.

For any polynomial $f(x) = \sum_{i=0}^m a_i x^i \in \mathbb{Z}_4[x]$ of degree $m \geq 0$. The reciprocal polynomial of $f(x)$ is defined by $\tilde{f}(x) = x^m f(\frac{1}{x})$, and $f(x)$ is said to be self-reciprocal if $\tilde{f}(x) = \delta f(x)$ for some $\delta \in \mathbb{Z}_4^\times = \{1, -1\}$. By (1) in Section 2, we have $x^n - 1 = f_0(x)f_1(x) \dots f_r(x)$. This implies

$$x^n - 1 = (-1)\tilde{f}_0(x)\tilde{f}_1(x) \dots \tilde{f}_r(x).$$

Since $f_0(x) = x - 1, f_1(x), \dots, f_r(x)$ are pairwise coprime monic basic irreducible polynomials in $\mathbb{Z}_4[x]$, $\tilde{f}_0(x), \tilde{f}_1(x), \dots, \tilde{f}_r(x)$ are pairwise coprime basic irreducible polynomials in $\mathbb{Z}_4[x]$ as well. Hence for any integer $j, 0 \leq j \leq r$, there is a unique integer $j', 0 \leq j' \leq r$, such that

$$\tilde{f}_j(x) = \delta_j f_{j'}(x) \text{ for some } \delta_j \in \mathbb{Z}_4^\times.$$

Especially, we have $0' = 0$ since $\tilde{f}_0(x) = 1 - x = (-1)f_0(x)$. Then by

$$x^n = 1 \text{ and } x^{mj} f_j(x^{-1}) = \tilde{f}_j(x) \text{ in } \mathcal{A},$$

from the definition for $e_j(x)$ (see (2) and (3)), we deduce that $e_j(x^{-1}) = e_{j'}(x)$.

We still use τ to denote the map $j \mapsto j'$. Then we have

$$\tilde{f}_j(x) = \delta_j f_{\tau(j)}(x) \text{ and } \tau(e_j(x)) = e_j(x^{-1}) = e_{\tau(j)}(x). \tag{5}$$

Whether τ denotes the ring automorphism of \mathcal{A} or this map is determined by the context. The next lemma shows the compatibility of the two uses of τ .

Lemma 7 Using the notation above, we have the following conclusions.

- (i) τ is a permutation on the set $\{0, 1, \dots, r\}$ satisfying $\tau^{-1} = \tau$.

(ii) After a rearrangement of $f_1(x), \dots, f_r(x)$, there exists a unique pair (λ, ρ) of nonnegative integers such that

- $\lambda + 2\rho = r$;
- $\tau(j) = j$, for all $0 \leq j \leq \lambda$;
- $\tau(\lambda + l) = \lambda + l + \rho$ and $\tau(\lambda + l + \rho) = \lambda + l$, for all $1 \leq l \leq \rho$.

(iii) For any integer j , $0 \leq j \leq r$, the map τ_j defined by

$$\tau_j(a(x) + vb(x)) = a(x^{-1}) + vb(x^{-1}) \pmod{f_{\tau(j)}(x)}, \forall a(x), b(x) \in \mathcal{K}_j$$

is an isomorphism of rings from $\mathcal{K}_j + v\mathcal{K}_j$ onto $\mathcal{K}_{\tau(j)} + v\mathcal{K}_{\tau(j)}$, where $x^{-1} = x^{n-1} \pmod{f_{\tau(j)}(x)}$.

Proof (i) It follows from the definition of the map τ and that $f_{\tau(\tau(j))}(x) = \delta_{\tau(j)}^{-1} \tilde{f}_{\tau(j)}(x) = \delta_{\tau(j)}^{-1} \delta_j^{-1} \tilde{f}_j(x) = \delta_{\tau(j)}^{-1} \delta_j^{-1} f_j(x) = f_j(x)$ by (5).

(ii) It follows from (i) and the properties of permutations on a finite set.

(iii) The map τ_j is well-defined and makes the following diagram commutative:

$$\begin{array}{ccc} \mathcal{K}_j + v\mathcal{K}_j & \xrightarrow{\tau_j} & \mathcal{K}_{\tau(j)} + v\mathcal{K}_{\tau(j)} \\ \varphi_j \downarrow & & \downarrow \varphi_j \\ (\mathcal{A} + v\mathcal{A})e_j(x) & \xrightarrow{\tau|_{(\mathcal{A}+v\mathcal{A})e_j(x)}} & (\mathcal{A} + v\mathcal{A})e_{\tau(j)}(x) \end{array},$$

where $\tau|_{(\mathcal{A}+v\mathcal{A})e_j(x)}$ is the restriction of the ring automorphism τ to the subring $(\mathcal{A} + v\mathcal{A})e_j(x)$ of $\mathcal{A} + v\mathcal{A}$. From this and by Lemma 2(ii), we deduce that τ_j is an isomorphism of rings from $\mathcal{K}_j + v\mathcal{K}_j$ onto $\mathcal{K}_{\tau(j)} + v\mathcal{K}_{\tau(j)}$. □

Now, using the notation of Lemma 3 and Theorem 1, we give the dual code for any cyclic code of length n over R .

Theorem 2 Let \mathcal{C} be a cyclic code of length n over R with the canonical form decomposition

$$\mathcal{C} = \bigoplus_{0 \leq j \leq r} e_j(x)C_j,$$

where C_j is an ideal of $\mathcal{K}_j + v\mathcal{K}_j$ listed by Theorem 1 for all j . Then

$$\mathcal{C}^\perp = \bigoplus_{0 \leq j \leq r} e_{\tau(j)}(x)D_{\tau(j)} \pmod{x^n - 1},$$

where $D_{\tau(j)} = \tau_j(\text{Ann}(C_j))$, $0 \leq j \leq r$, is an ideal of $\mathcal{K}_{\tau(j)} + v\mathcal{K}_{\tau(j)}$ determined by the following table:

N	$C_j \pmod{f_j(x)}$	$D_{\tau(j)} \pmod{f_{\tau(j)}(x)}$
3	$\langle 2^k \rangle$ ($k = 0, 1, 2$)	$\langle 2^{2-k} \rangle$
2^{m_j}	$\langle 2w_j(x) + v \rangle$ ($w_j(x) \in T_j$)	$\langle 2(1 + w_j(x^{-1})) + v \rangle$
1	$\langle 2v \rangle$	$\langle 2, v \rangle$
1	$\langle 2, v \rangle$	$\langle 2v \rangle$

where N is the number of the pair $(C_j, D_{\tau(j)})$ of ideals in the same row.

Proof Let $\alpha, \beta \in R[x]/\langle x^n - 1 \rangle = \mathcal{A} + v\mathcal{A}$. By Lemma 3 and its proof, we have that

$$\alpha = \sum_{j=0}^r e_j(x)\xi_j, \quad \beta = \sum_{j=0}^r e_j(x)\eta_j, \quad \text{where } \xi_j, \eta_j \in \mathcal{K}_j + v\mathcal{K}_j.$$

Since $e_j(x)^2 = e_j(x)$ and $e_j(x)e_l(x) = 0$ for all $0 \leq j \neq l \leq r$ by Lemma 2(i), it follows that $\alpha\beta = \sum_{j=0}^r e_j(x)(\xi_j\eta_j)$. This implies that

$$\alpha\beta = 0 \text{ in } R[x]/\langle x^n - 1 \rangle \iff \xi_j\eta_j = 0 \text{ in } \mathcal{K}_j + v\mathcal{K}_j, \quad \forall j = 0, 1, \dots, r.$$

From this we deduce $\text{Ann}(\mathcal{C}) = \bigoplus_{j=0}^r e_j(x)\text{Ann}(C_j) \pmod{x^n - 1}$, where $\text{Ann}(C_j)$ is the annihilating ideal of C_j in $\mathcal{K}_j + v\mathcal{K}_j$ for any $0 \leq j \leq r$. As τ is a ring isomorphism, we have

$$\mathcal{C}^\perp = \tau(\text{Ann}(\mathcal{C})) = \sum_{j=0}^r \tau(e_j(x)\text{Ann}(C_j)).$$

For any integer $j, 0 \leq j \leq r$, by (5) and the definition of τ we have $\tau(e_j(x)) = e_j(x^{-1}) = e_{\tau(j)}(x)$ and

$$\tau(e_j(x)c_j(x)) = e_j(x^{-1})c_j(x^{-1}) = e_{\tau(j)}(x)\tau_j(c_j(x)),$$

where $\tau_j(c_j(x)) = c_j(x^{-1}) = c(x^{n-1}) \pmod{f_{\tau(j)}(x)}$ by Lemma 7(iii), for any $c_j(x) \in \text{Ann}(C_j)$. From these, we deduce that

$$\mathcal{C}^\perp = \bigoplus_{j=0}^r e_{\tau(j)}(x)\tau_j(\text{Ann}(C_j)).$$

Denote $D_{\tau(j)} = \tau_j(\text{Ann}(C_j))$ where $0 \leq j \leq r$. Since τ_j is a ring isomorphism from $\mathcal{K}_j + v\mathcal{K}_j$ onto $\mathcal{K}_{\tau(j)} + v\mathcal{K}_{\tau(j)}$ by Lemma 7(iii), we see that $D_{\tau(j)}$ is an ideal of the ring $\mathcal{K}_{\tau(j)} + v\mathcal{K}_{\tau(j)}$.

Let $C_j = \langle\langle 2w_j(x) + v \rangle\rangle$ where $w_j(x) \in T_j$. By Theorem 1 we have $\text{Ann}(C_j) = \langle 2(1 + w_j(x)) + v \rangle$. Then by the definition of τ_j , it follows that

$$D_{\tau(j)} = \tau_j(\text{Ann}(C_j)) = \langle \tau_j(2(1 + w_j(x)) + v) \rangle = \langle 2(1 + w_j(x^{-1})) + v \rangle$$

$\pmod{f_{\tau(j)}(x)}$. The expressions for $D_{\tau(j)}$ in other cases can be calculated easily. We omit these here. □

For any integer $j, 1 \leq j \leq \lambda$, as $f_j(x)$ is self-reciprocal in $\mathbb{Z}_4[x]$ by Lemma 7(ii) and (5), we see that $\overline{f_j}(x)$ is self-reciprocal in $\mathbb{Z}_2[x]$ and hence its degree m_j must be even. Then it is well known that

$$x^{-1} = x^{2\frac{m_j}{2}} \text{ in the field } F_j = \mathbb{Z}_2[x]/\langle \overline{f_j}(x) \rangle. \tag{6}$$

In the rest of this paper, we adopt the following notation:

- $\mathcal{H}_j = \left\{ \xi \in F_j \mid \xi^{2\frac{m_j}{2}} = \xi \right\}$. Then \mathcal{H}_j is a subfield of F_j with $2\frac{m_j}{2}$ elements.
- Let Tr_j be the trace function from F_j onto its subfield \mathcal{H}_j defined by:

$$\text{Tr}_j(\xi) = \xi + \xi^{2\frac{m_j}{2}}, \quad \forall \xi \in F_j.$$

Then by [22, Corollary 7.17], we have that $|\text{Tr}_j^{-1}(1)| = 2\frac{m_j}{2}$ where

$$\text{Tr}_j^{-1}(1) = \{ \xi \in F_j \mid \text{Tr}_j(\xi) = 1 \} = \{ \xi \in F_j \mid \xi + \xi^{2\frac{m_j}{2}} = 1 \}. \tag{7}$$

Now is the time to list all self-dual cyclic codes over R of length n .

Theorem 3 *Using the notation above, all distinct self-dual cyclic codes of length n over $R = \mathbb{Z}_4 + v\mathbb{Z}_4$ ($v^2 = 2v$) are given by:*

$$\mathcal{C} = \bigoplus_{0 \leq j \leq \lambda + 2\rho} e_j(x)C_j(\text{mod } x^n - 1),$$

where C_j is an ideal of $\mathcal{K}_j + v\mathcal{K}_j$ listed as follows.

- (i) When $j = 0$, there is 1 ideal: $C_0 = \langle 2 \rangle$.
- (ii) When $1 \leq j \leq \lambda$, there are $1 + 2^{\frac{m_j}{2}}$ ideals:

$$C_j = \langle 2 \rangle, \text{ and } C_j = \langle 2w_j(x) + v \rangle \text{ where } w_j(x) \in \text{Tr}_j^{-1}(1) \text{ arbitrary.}$$

- (iii) When $\lambda + 1 \leq j \leq \lambda + \rho$, there are $2^{m_j} + 5$ pairs $(C_j, C_{j+\rho})$ of ideals listed by the following table:

N	$C_j \pmod{f_j(x)}$	$ C_j $	$C_{j+\rho} \pmod{f_{j+\rho}(x)}$
3	$\langle 2^k \rangle, 0 \leq k \leq 2$	$2^{(4-2k)m_j}$	$\langle 2^{2-k} \rangle$
2^{m_j}	$\langle 2w_j(x) + v \rangle, w_j(x) \in T_j$	2^{2m_j}	$\langle 2(1 + w_j(x^{-1})) + v \rangle$
1	$\langle 2v \rangle$	2^{m_j}	$\langle 2, v \rangle$
1	$\langle 2, v \rangle$	2^{3m_j}	$\langle 2v \rangle$

where N is the number of pairs in the same row.

Therefore, the number of self-dual cyclic codes of length n over R is

$$L_n = \prod_{1 \leq j \leq \lambda} (1 + 2^{\frac{m_j}{2}}) \prod_{\lambda + 1 \leq j \leq \lambda + \rho} (2^{m_j} + 5).$$

Proof By Lemma 7(ii) and Theorem 2, we have

$$\mathcal{C}^\perp = \left(\bigoplus_{j=0}^{\lambda} e_j(x)D_j \right) \oplus \left(\bigoplus_{j=\lambda+1}^{\lambda+\rho} e_{j+\rho}D_{j+\rho} \right) \oplus \left(\bigoplus_{j=\lambda+\rho+1}^{\lambda+2\rho} e_{j-\rho}D_{j-\rho} \right),$$

where $D_{j+\rho} = \tau_j(C_j)$ for all $j = \lambda + 1, \dots, \lambda + \rho$. Hence the cyclic code \mathcal{C} is self-dual, i.e., $\mathcal{C} = \mathcal{C}^\perp$, if and only if the following two conditions are satisfied:

- (†) $C_j = D_j = \tau_j(\text{Ann}(C_j))$, for all $0 \leq j \leq \lambda$;
- (‡) C_j is an arbitrary ideal of $\mathcal{K}_j + v\mathcal{K}_j$ and $C_{j+\rho} = D_{j+\rho} = \tau_{j+\rho}(\text{Ann}(C_j))$, for all $j = \lambda + 1, \dots, \lambda + \rho$.

Therefore, the class of self-dual cyclic codes over R of length n is the same as the class of cyclic codes over R of length n : $\mathcal{C} = \bigoplus_{j=0}^{\lambda+2\rho} e_j(x)C_j$, where C_j is an ideal of $\mathcal{K}_j + v\mathcal{K}_j$ satisfying Conditions (†) and (‡) for all j .

Every pair $(C_j, C_{j+\rho})$ of ideals can be determined by the table in Theorem 2, for all $j = \lambda + 1, \dots, \lambda + \rho$. Then in order to determine codes in the latter class, we only need to consider ideals of $\mathcal{K}_j + v\mathcal{K}_j$ satisfying Conditions (†) for all $j = 0, 1, \dots, \lambda$.

Now, let $0 \leq j \leq \lambda$ and C_j is an ideal of $\mathcal{K}_j + v\mathcal{K}_j$ listed by Theorem 2. Then C_j satisfies condition (\dagger) if and only if C_j is given by one of the following two cases:

- $(\dagger-1)$ $C_j = \langle 2 \rangle$.
- $(\dagger-2)$ $C_j = \langle 2w_j(x) + v \rangle$,
 where $w_j(x) \in T_j$ satisfying $w_j(x) \equiv 1 + w_j(x^{-1}) \pmod{f_j(x), \text{ mod } 2}$.

Since $w_j(x)$ is a polynomial in $\mathbb{Z}_2[x]$, the condition is equivalent to $w_j(x) + w_j(x^{-1}) \equiv 1 \pmod{\overline{f_j}(x)}$, i.e.,

$$w_j(x) + w_j(x^{-1}) = 1 \text{ in } F_j = \mathbb{Z}_2[x]/\langle \overline{f_j}(x) \rangle. \tag{8}$$

Now, we have the following two subcases:

- $(\ddagger-2-i)$ When $j = 0$, we have $\overline{f_0}(x) = x - 1$ and $F_0 = \mathbb{Z}_2$. In this case, there is no element $w_j \in \mathbb{Z}_2$ satisfying Condition (8).
- $(\ddagger-2-ii)$ Let $1 \leq j \leq \lambda$. By (6) and $a^2 = a$ for all $a \in \mathbb{Z}_2$, we obtain

$$w_j(x^{-1}) = w_j(x^{2^{\frac{m_j}{2}}}) = (w_j(x))^{2^{\frac{m_j}{2}}}, \forall w_j(x) \in F_j.$$

Hence Condition (8) is equivalent to $w_j(x) \in \text{Tr}_j^{-1}(1)$ by (7).

By Lemma 7(ii) and Theorem 2, we conclude that the class of cyclic codes over R of length n : $\mathcal{C} = \bigoplus_{j=0}^{\lambda+2\rho} e_j(x)C_j$, where C_j is an ideal of $\mathcal{K}_j + v\mathcal{K}_j$ satisfying Conditions (\dagger) and (\ddagger) for all j , is exactly the same as the class of cyclic codes over R of length n listed by the three cases (i)–(iii) of this theorem.

As stated above, we proved the theorem. □

As the end of this section, we list the number L_n of self-dual cyclic codes of length n over $\mathbb{Z}_4 + v\mathbb{Z}_4$ ($v^2 = 2v$), where n is odd and $3 \leq n \leq 49$, by the following table.

n	L_n	\mathcal{M}_n	n	L_n	\mathcal{M}_n
3	3	(2; \emptyset)	27	13851	(2, 6, 18; \emptyset)
5	5	(4; \emptyset)	29	16385	(28; \emptyset)
7	13	(\emptyset ; 3)	31	50653	(\emptyset ; 5, 5, 5)
9	27	(2, 6; \emptyset)	33	107811	(2, 10, 10, 10; \emptyset)
11	33	(10; \emptyset)	35	266565	(4; 3, 12)
13	65	(12; \emptyset)	37	262145	(36; \emptyset)
15	315	(2, 4; 4)	39	799695	(2, 12; 12)
17	289	(8, 8; \emptyset)	41	1050625	(20, 20; \emptyset)
19	513	(18; \emptyset)	43	2146689	(14, 14, 14; \emptyset)
21	2691	(2; 3, 6)	45	11626335	(2, 4, 6; 4, 12)
23	2053	(\emptyset ; 11)	47	8388613	(\emptyset ; 23)
25	5125	(4, 20; \emptyset)	49	27263041	(\emptyset ; 3, 21)

where $\mathcal{M}_n = (m_1, \dots, m_\lambda; m_{\lambda+1}, \dots, m_{\lambda+\rho})$ corresponding to the degrees of monic basic irreducible divisors $f_1(x), \dots, f_\lambda(x); f_{\lambda+1}(x), \dots, f_{\lambda+\rho}(x)$ of $x^n - 1$ in $\mathbb{Z}_4[x]$ (see (1) in Section 1). It is obvious that

$$1 + m_1 + \dots + m_\lambda + 2(m_{\lambda+1} + \dots + m_{\lambda+\rho}) = n.$$

4 Quasi-cyclic code over \mathbb{Z}_4 derived from cyclic codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$

In this section, we consider self-dual 2-quasi-cyclic codes of length $2n$ over \mathbb{Z}_4 derived from self-dual cyclic codes of length n over the ring $R = \mathbb{Z}_4 + v\mathbb{Z}_4$. As in [15, Section 3], we define $\varrho : R \rightarrow \mathbb{Z}_4^2$ by

$$\varrho(\alpha) = (a + b, b), \forall \alpha = a + bv \in R \text{ where } a, b \in \mathbb{Z}_4$$

and let $\theta : R^n \rightarrow \mathbb{Z}_4^{2n}$ be such that $\theta(\alpha_1, \dots, \alpha_n) = (\varrho(\alpha_1), \dots, \varrho(\alpha_n))$, for all $\alpha_1, \dots, \alpha_n \in R$. Let w_L denote the Lee weight on \mathbb{Z}_4 defined by:

$$w_L(0) = 0, w_L(1) = w_L(3) = 1 \text{ and } w_L(2) = 2.$$

We extend w_L in a natural way: for $a + bv \in R$ with $a, b \in \mathbb{Z}_4$, define

$$w_L(a + bv) = w_L(a + b) + w_L(b).$$

With this distance and Gray map definition, the following conclusions have been verified by Martínez-Moro et al. [15].

Proposition 1 ([15, Theorem 3.1]) *Let \mathcal{C} be a linear code of length n and minimum Lee distance d over R . Then $\theta(\mathcal{C})$ is a linear code of length $2n$ over \mathbb{Z}_4 , $|\theta(\mathcal{C})| = |\mathcal{C}|$ and is of minimum Lee distance d .*

Proposition 2 ([15, Proposition 3.3]) *Let \mathcal{C} be a linear code of length n over R . Then $\theta(\mathcal{C}^\perp) = \theta(\mathcal{C})^\perp$. In particular, if \mathcal{C} is self-dual, then $\theta(\mathcal{C})$ is a self-dual code of length $2n$ over \mathbb{Z}_4 and has the same Lee weight distribution.*

Moreover, we have the following properties for cyclic codes over R .

Proposition 3 *Let \mathcal{C} be a cyclic codes of length n over R . Then $\theta(\mathcal{C})$ is a 2-quasi-cyclic code of length $2n$ over \mathbb{Z}_4 .*

Proof Let $\alpha = (\alpha_0, \alpha_1, \dots, \alpha_{n-1}) \in \mathcal{C}$, where $\alpha_i = a_i + b_i v$ with $a_i, b_i \in \mathbb{Z}_4$ for all $i = 0, 1, \dots, n-1$. Then $\theta(\alpha) = (a_0 + b_0, b_0, a_1 + b_1, b_1, \dots, a_{n-1} + b_{n-1}, b_{n-1}) \in \theta(\mathcal{C})$. Since \mathcal{C} is cyclic, we have $(\alpha_{n-1}, \alpha_0, \alpha_1, \dots, \alpha_{n-2}) \in \mathcal{C}$. This implies $(a_{n-1} + b_{n-1}, b_{n-1}, a_0 + b_0, b_0, a_1 + b_1, b_1, \dots, a_{n-2} + b_{n-2}, b_{n-2}) \in \theta(\mathcal{C})$. Hence $\theta(\mathcal{C})$ is a 2-quasi-cyclic code of length $2n$ over \mathbb{Z}_4 . □

As an application, we consider cyclic codes of length 15 over R . In this case, $x^{15} - 1 = f_0(x)f_1(x)f_2(x)f_3(x)f_4(x)$ where $f_0(x) = x - 1, f_1(x) = x^2 + x + 1, f_2(x) = x^4 + x^3 + x^2 + x + 1, f_3(x) = x^4 + 2x^2 + 3x + 1$ and $f_4(x) = \tilde{f}_3(x)$ are monic basic irreducible polynomials in $\mathbb{Z}_4[x]$. Hence $m_1 = 2$ and $m_2 = m_3 = m_4 = 4$. Hence the number of cyclic codes of length 15 over $\mathbb{Z}_4 + v\mathbb{Z}_4$ is

$$(2^1 + 5) \cdot (2^2 + 5) \cdot (2^4 + 5)^3 = 583443.$$

First, for each integer $j, 0 \leq j \leq 4$, we denote $F_j(x) = \frac{x^{15}-1}{f_j(x)}$,

$$\begin{aligned} \diamond \mathcal{K}_j &= \mathbb{Z}_4[x]/\langle f_j(x) \rangle = \left\{ \sum_{i=0}^{m_j-1} a_i x^i \mid a_0, a_1, \dots, a_{m_j-1} \in \mathbb{Z}_4 \right\}. \\ \diamond T_j &= \left\{ \sum_{i=0}^{m_j-1} b_i x^i \mid b_0, b_1, \dots, b_{m_j-1} \in \mathbb{Z}_2 \right\} \subset \mathcal{K}_j. \end{aligned}$$

Then we find polynomials $c_j(x), d_j(x) \in \mathbb{Z}_4[x]$ satisfying $c_j(x)F_j(x) + d_j(x)f_j(x) = 1$ and set $e_j(x) \in \mathbb{Z}_4[x]/\langle x^{15} - 1 \rangle$ such that $e_j(x) \equiv c_j(x)F_j(x) \pmod{x^{15} - 1}$. Precisely, we have

$$\begin{aligned} e_0(x) &= 3x^{14} + 3x^{13} + 3x^{12} + 3x^{11} + 3x^{10} + 3x^9 + 3x^8 + 3x^7 + 3x^6 + 3x^5 + 3x^4 \\ &\quad + 3x^3 + 3x^2 + 3x + 3, \\ e_1(x) &= x^{14} + x^{13} + 2x^{12} + x^{11} + x^{10} + 2x^9 + x^8 + x^7 + 2x^6 + x^5 + x^4 + 2x^3 + x^2 + x + 2, \\ e_2(x) &= x^{14} + x^{13} + x^{12} + x^{11} + x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x, \\ e_3(x) &= x^{12} + 2x^{10} + x^9 + 3x^8 + x^6 + 2x^5 + 3x^4 + x^3 + 3x^2 + 3x, \\ e_4(x) &= 3x^{14} + 3x^{13} + x^{12} + 3x^{11} + 2x^{10} + x^9 + 3x^7 + x^6 + 2x^5 + x^3. \end{aligned}$$

(I) By Lemma 3 and Theorem 1, all distinct 583443 cyclic codes of length 15 over R are given by: $\mathcal{C} = \bigoplus_{j=0}^4 e_j(x)C_j \pmod{x^{15} - 1}$, where

- C_0 is one of the following 7 ideals of $\mathbb{Z}_4 + v\mathbb{Z}_4$:
 - $C_0 = \langle 2^k \rangle$ with $|C_0| = 2^{4-2k}$, where $0 \leq k \leq 2$;
 - $C_0 = \langle 2a + v \rangle$ with $|C_0| = 4$, where $a \in \mathbb{Z}_2 = \{0, 1\}$ arbitrary;
 - $C_0 = \langle 2v \rangle$ with $|C_0| = 2$;
 - $C_0 = \langle 2, v \rangle$ with $|C_0| = 8$.
- C_1 is one of the following 9 ideals of $\mathcal{K}_1 + v\mathcal{K}_1$:
 - $C_1 = \langle 2^k \rangle$ with $|C_1| = 4^{4-2k}$, where $0 \leq k \leq 2$;
 - $C_1 = \langle 2(a_0 + a_1x) + v \rangle$ with $|C_1| = 16$, where $a_0, a_1 \in \mathbb{Z}_2$ arbitrary;
 - $C_1 = \langle 2v \rangle$ with $|C_1| = 4$;
 - $C_1 = \langle 2, v \rangle$ with $|C_1| = 64$.
- C_j is one of the following 21 ideals of $\mathcal{K}_j + v\mathcal{K}_j$ for all $j = 2, 3, 4$:
 - $C_j = \langle 2^k \rangle$ with $|C_j| = 16^{4-2k}$, where $0 \leq k \leq 2$;
 - $C_j = \langle 2(a_0 + a_1x + a_2x^2 + a_3x^3) + v \rangle$ with $|C_j| = 16^2$, where $a_0, a_1, a_2, a_3 \in \mathbb{Z}_2$ arbitrary;
 - $C_j = \langle 2v \rangle$ with $|C_j| = 16$;
 - $C_j = \langle 2, v \rangle$ with $|C_j| = 16^3$.

(II) We have $r = 4, \lambda = 2$ and $\rho = 1$. For $j = 1, 2$, set

$$\begin{aligned} \diamond F_j &= \mathbb{Z}_2[x]/\langle \bar{f}_j(x) \rangle = \{ \sum_{i=0}^{m_j-1} a_i x^i \mid a_0, a_1, \dots, a_{m_j-1} \in \mathbb{Z}_2 \} \\ &\quad \text{in which the arithmetic is done modulo } \bar{f}_j(x); \\ \diamond \text{Tr}_j^{-1}(1) &= \{ a(x) \in F_j \mid a(x) + a(x^{-1}) \equiv 1 \pmod{\bar{f}_j(x)} \}. \end{aligned}$$

Then by $x^{-1} \equiv x^{14} \pmod{\bar{f}_j(x)}$ for $j = 1, 2$, we have the following

$$\begin{aligned} \text{Tr}_1^{-1}(1) &= \{ a + bx \in \mathbb{Z}_2[x]/\langle \bar{f}_1(x) \rangle \mid (a + bx) + (a + bx^{14}) \equiv 1 \pmod{\bar{f}_1(x)} \} = \\ &= \{ a + bx \mid a + bx + a + b(1 + x) + 1 = 0, a, b \in \mathbb{Z}_2 \} = \{ x, 1 + x \}. \\ \text{Tr}_2^{-1}(1) &= \{ a + bx + cx^2 + dx^3 \in \mathbb{Z}_2[x]/\langle \bar{f}_2(x) \rangle \mid (a + bx + cx^2 + dx^3) + (a + bx^{14} + \\ &+ cx^{13} + dx^{12}) \equiv 1 \pmod{\bar{f}_2(x)} \} = \{ a + bx + cx^2 + dx^3 \mid bx + cx^2 + dx^3 + b(1 + x + \\ &+ x^2 + x^3) + cx^3 + dx^2 + 1 = 0, a, b, c, d \in \mathbb{Z}_2 \} = \{ a + x + cx^2 + (1 + c)x^3 \mid a, c \in \mathbb{Z}_2 \}. \end{aligned}$$

By Theorem 3, all 315 self-dual cyclic codes of length 15 over R are given by: $\mathcal{C} = \bigoplus_{j=0}^4 e_j(x)C_j \pmod{x^{15} - 1}$, where

- $C_0 = \langle 2 \rangle = 2(\mathbb{Z}_4 + v\mathbb{Z}_4)$.

- $C_1 = \langle 2 \rangle, C_1 = \langle 2w_1(x) + v \rangle$ where $w_1(x) \in \text{Tr}_1^{-1}(1)$.
- $C_2 = \langle 2 \rangle, C_2 = \langle 2w_2(x) + v \rangle$ where $w_2(x) \in \text{Tr}_2^{-1}(1)$.
- (C_3, C_4) is given by the following table:

N	$C_3 \pmod{f_3(x)}$	$ C_3 $	$C_4 \pmod{f_4(x)}$
3	$\langle 2^k \rangle, 0 \leq k \leq 2$	$2^{4(4-2k)}$	$\langle 2^{2-k} \rangle$
16	$\langle 2w_3(x) + v \rangle$	2^8	$\langle 2(1 + w_3(x^{-1})) + v \rangle$
1	$\langle 2v \rangle$	2^4	$\langle 2, v \rangle$
1	$\langle 2, v \rangle$	2^{12}	$\langle 2v \rangle$

in which N is the number of pairs (C_3, C_4) in the same row, and

$$w_3(x) = a + bx + cx^2 + dx^3;$$

$$w_3(x^{-1}) = a + d + (d + c)x + (c + b)x^2 + bx^3 \equiv w_3(x^{14}) \pmod{f_4(x), 2},$$

for $a, b, c, d \in \mathbb{Z}_2$ arbitrary.

By Proposition 3, we obtain 315 2-quasi-cyclic self-dual codes $\theta(\mathcal{C})$ of length 30 over \mathbb{Z}_4 . Among these codes, there are 70 codes with minimum Lee weight 12. These 70 2-quasi-cyclic self-dual codes over \mathbb{Z}_4 are given by the following table, with C_1, C_2, C_3, C_4 and the type of each \mathbb{Z}_4 -code $\theta(\mathcal{C})$.

C_1	C_2	$C_3 \pmod{f_3(x)}$	$C_4 \pmod{f_4(x)}$	Type
$\langle v + 2x \rangle$	$\langle 2x^3 + 2x + v \rangle$	$\langle 2 \rangle$	$\langle 2 \rangle$	$2^{18}4^6$
$\langle v + 2x + 2 \rangle$	$\langle 2x^3 + 2x + v \rangle$	$\langle 2 \rangle$	$\langle 2 \rangle$	$2^{18}4^6$
$\langle v + 2x \rangle$	$\langle 2x^2 + 2x + v \rangle$	$\langle 2 \rangle$	$\langle 2 \rangle$	$2^{18}4^6$
$\langle v + 2x + 2 \rangle$	$\langle 2x^2 + 2x + v \rangle$	$\langle 2 \rangle$	$\langle 2 \rangle$	$2^{18}4^6$
$\langle v + 2x \rangle$	$\langle 2x^3 + 2x + v + 2 \rangle$	$\langle 2 \rangle$	$\langle 2 \rangle$	$2^{18}4^6$
$\langle v + 2x + 2 \rangle$	$\langle 2x^3 + 2x + v + 2 \rangle$	$\langle 2 \rangle$	$\langle 2 \rangle$	$2^{18}4^6$
$\langle v + 2x \rangle$	$\langle 2x^2 + 2x + v + 2 \rangle$	$\langle 2 \rangle$	$\langle 2 \rangle$	$2^{18}4^6$
$\langle v + 2x + 2 \rangle$	$\langle 2x^2 + 2x + v + 2 \rangle$	$\langle 2 \rangle$	$\langle 2 \rangle$	$2^{18}4^6$
$\langle v + 2x \rangle$	$\langle 2 \rangle$	$\langle 2v \rangle$	$\langle 2, v \rangle$	$2^{18}4^6$
$\langle v + 2x + 2 \rangle$	$\langle 2 \rangle$	$\langle 2v \rangle$	$\langle 2, v \rangle$	$2^{18}4^6$
$\langle v + 2x \rangle$	$\langle 2 \rangle$	$\langle 2, v \rangle$	$\langle 2v \rangle$	$2^{18}4^6$
$\langle v + 2x + 2 \rangle$	$\langle 2 \rangle$	$\langle 2, v \rangle$	$\langle 2v \rangle$	$2^{18}4^6$
$\langle v + 2x \rangle$	$\langle 2x^3 + 2x + v \rangle$	$\langle 2, v \rangle$	$\langle 2v \rangle$	$2^{10}4^{10}$
$\langle v + 2x \rangle$	$\langle 2x^2 + 2x + v \rangle$	$\langle 2v \rangle$	$\langle 2, v \rangle$	$2^{10}4^{10}$
$\langle v + 2x \rangle$	$\langle 2x^3 + 2x + v + 2 \rangle$	$\langle 2, v \rangle$	$\langle 2v \rangle$	$2^{10}4^{10}$
$\langle v + 2x \rangle$	$\langle 2x^2 + 2x + v + 2 \rangle$	$\langle 2v \rangle$	$\langle 2, v \rangle$	$2^{10}4^{10}$
$\langle v + 2x \rangle$	$\langle 2 \rangle$	$\langle 2x^3 + 2x^2 + v \rangle$	$\langle 2x^2 + v \rangle$	$2^{10}4^{10}$
$\langle v + 2x \rangle$	$\langle 2 \rangle$	$\langle 2x^3 + 2x + v \rangle$	$\langle 2x^3 + 2x^2 + 2x + v \rangle$	$2^{10}4^{10}$
$\langle v + 2x \rangle$	$\langle 2 \rangle$	$\langle 2x^3 + 2x^2 + 2x + v \rangle$	$\langle 2x^3 + v \rangle$	$2^{10}4^{10}$
$\langle v + 2x \rangle$	$\langle 2 \rangle$	$\langle 2x^3 + v + 2 \rangle$	$\langle v + 2x + 2 \rangle$	$2^{10}4^{10}$
$\langle v + 2x \rangle$	$\langle 2 \rangle$	$\langle 1 \rangle$	$\langle 0 \rangle$	$2^{10}4^{10}$
$\langle v + 2x + 2 \rangle$	$\langle 2 \rangle$	$\langle 1 \rangle$	$\langle 0 \rangle$	$2^{10}4^{10}$
$\langle v + 2x \rangle$	$\langle 2 \rangle$	$\langle 0 \rangle$	$\langle 1 \rangle$	$2^{10}4^{10}$
$\langle v + 2x + 2 \rangle$	$\langle 2 \rangle$	$\langle 0 \rangle$	$\langle 1 \rangle$	$2^{10}4^{10}$
$\langle 2 \rangle$	$\langle 2x^3 + 2x + v \rangle$	$\langle 2x^3 + v + 2 \rangle$	$\langle v + 2x + 2 \rangle$	2^64^{12}
$\langle 2 \rangle$	$\langle 2x^3 + 2x + v \rangle$	$\langle 2x^3 + 2x^2 + 2x + v + 2 \rangle$	$\langle 2x^3 + v + 2 \rangle$	2^64^{12}
$\langle 2 \rangle$	$\langle 2x^3 + 2x + v \rangle$	$\langle 1 \rangle$	$\langle 0 \rangle$	2^64^{12}
$\langle 2 \rangle$	$\langle 2x^2 + 2x + v \rangle$	$\langle 2x^3 + 2x + v \rangle$	$\langle 2x^3 + 2x^2 + 2x + v \rangle$	2^64^{12}
$\langle 2 \rangle$	$\langle 2x^2 + 2x + v \rangle$	$\langle 2x^3 + 2x^2 + v + 2 \rangle$	$\langle 2x^2 + v + 2 \rangle$	2^64^{12}
$\langle 2 \rangle$	$\langle 2x^2 + 2x + v \rangle$	$\langle 1 \rangle$	$\langle 0 \rangle$	2^64^{12}

(2)	$(2x^2 + 2x + v)$	(0)	(1)	$2^6 4^{12}$
(2)	$(2x^3 + 2x + v + 2)$	$(2x^3 + v)$	$(v + 2x)$	$2^6 4^{12}$
(2)	$(2x^3 + 2x + v + 2)$	$(2x^3 + 2x^2 + 2x + v)$	$(2x^3 + v)$	$2^6 4^{12}$
(2)	$(2x^3 + 2x + v + 2)$	(1)	(0)	$2^6 4^{12}$
(2)	$(2x^2 + 2x + v + 2)$	$(2x^3 + 2x^2 + v)$	$(2x^2 + v)$	$2^6 4^{12}$
(2)	$(2x^2 + 2x + v + 2)$	$(2x^3 + 2x + v + 2)$	$(2x^3 + 2x^2 + 2x + v + 2)$	$2^6 4^{12}$
(2)	$(2x^2 + 2x + v + 2)$	(1)	(0)	$2^6 4^{12}$
(2)	$(2x^2 + 2x + v + 2)$	(0)	(1)	$2^6 4^{12}$
$(v + 2x + 2)$	$(2x^3 + 2x + v)$	(v)	$(v + 2)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^3 + 2x + v)$	$(2x^3 + 2x^2 + v)$	$(2x^2 + v)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^3 + 2x + v)$	$(2x^3 + 2x^2 + v)$	$(2x^2 + v)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^3 + 2x + v)$	$(v + 2)$	(v)	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^3 + 2x + v)$	$(2x^2 + v + 2)$	$(2x^2 + 2x + v)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^3 + 2x + v)$	$(2x^3 + 2x^2 + 2x + v + 2)$	$(2x^3 + v + 2)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^3 + 2x + v)$	(1)	(0)	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^3 + 2x + v)$	(1)	(0)	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v)$	(v)	$(v + 2)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v)$	$(v + 2x)$	$(2x^3 + 2x^2 + v + 2)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^2 + 2x + v)$	$(v + 2x)$	$(2x^3 + 2x^2 + v + 2)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v)$	$(2x^3 + 2x + v)$	$(2x^3 + 2x^2 + 2x + v)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^2 + 2x + v)$	$(v + 2)$	(v)	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v)$	$(2x^3 + v + 2)$	$(v + 2x + 2)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^2 + 2x + v)$	$(2x^3 + v + 2)$	$(v + 2x + 2)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^2 + 2x + v)$	(1)	(0)	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^3 + 2x + v + 2)$	(v)	$(v + 2)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^3 + 2x + v + 2)$	$(2x^3 + v)$	$(v + 2x)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^3 + 2x + v + 2)$	$(2x^2 + v)$	$(2x^2 + 2x + v + 2)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^3 + 2x + v + 2)$	$(2x^3 + 2x + v)$	$(2x^3 + 2x^2 + 2x + v)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^3 + 2x + v + 2)$	$(2x^3 + 2x + v)$	$(2x^3 + 2x^2 + 2x + v)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^3 + 2x + v + 2)$	$(v + 2)$	(v)	$2^2 4^{14}$
$(v + 2x)$	$(2x^3 + 2x + v + 2)$	(1)	(0)	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^3 + 2x + v + 2)$	(1)	(0)	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v + 2)$	(v)	$(v + 2)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v + 2)$	$(2x^3 + 2x^2 + v)$	$(2x^2 + v)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v + 2)$	$(2x^3 + 2x^2 + 2x + v)$	$(2x^3 + v)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^2 + 2x + v + 2)$	$(2x^3 + 2x^2 + 2x + v)$	$(2x^3 + v)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^2 + 2x + v + 2)$	$(v + 2)$	(v)	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v + 2)$	$(v + 2x + 2)$	$(2x^3 + 2x^2 + v)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^2 + 2x + v + 2)$	$(v + 2x + 2)$	$(2x^3 + 2x^2 + v)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v + 2)$	(1)	(0)	$2^2 4^{14}$

There are 92 2-quasi-cyclic self-dual codes $\theta(C)$ of length 30 with minimum Lee weight 10 over \mathbb{Z}_4 derived from the 315 self-dual codes C of length 15 over $\mathbb{Z}_4 + v\mathbb{Z}_4$. These 92 codes are given by the following table, with C_1, C_2, C_3, C_4 and the type of each \mathbb{Z}_4 -code $\theta(C)$.

C_1	C_2	$C_3 \pmod{f_3(x)}$	$C_4 \pmod{f_4(x)}$	Type
(2)	$(2x^3 + 2x + v)$	$(2v)$	$(2, v)$	$2^{14} 4^8$
(2)	$(2x^3 + 2x + v)$	$(2, v)$	$(2v)$	$2^{14} 4^8$
(2)	$(2x^2 + 2x + v)$	$(2v)$	$(2, v)$	$2^{14} 4^8$
(2)	$(2x^2 + 2x + v)$	$(2, v)$	$(2v)$	$2^{14} 4^8$

(2)	$(2x^3 + 2x + v + 2)$	$(2v)$	$(2, v)$	$2^{14}4^8$
(2)	$(2x^3 + 2x + v + 2)$	$(2, v)$	$(2v)$	$2^{14}4^8$
(2)	$(2x^2 + 2x + v + 2)$	$(2v)$	$(2, v)$	$2^{14}4^8$
(2)	$(2x^2 + 2x + v + 2)$	$(2, v)$	$(2v)$	$2^{14}4^8$
$(v + 2x)$	$(2x^3 + 2x + v)$	$(2v)$	$(2, v)$	$2^{10}4^{10}$
$(v + 2x + 2)$	$(2x^3 + 2x + v)$	$(2v)$	$(2, v)$	$2^{10}4^{10}$
$(v + 2x + 2)$	$(2x^3 + 2x + v)$	$(2, v)$	$(2v)$	$2^{10}4^{10}$
$(v + 2x + 2)$	$(2x^2 + 2x + v)$	$(2v)$	$(2, v)$	$2^{10}4^{10}$
$(v + 2x)$	$(2x^2 + 2x + v)$	$(2, v)$	$(2v)$	$2^{10}4^{10}$
$(v + 2x + 2)$	$(2x^2 + 2x + v)$	$(2, v)$	$(2v)$	$2^{10}4^{10}$
$(v + 2x)$	$(2x^3 + 2x + v + 2)$	$(2v)$	$(2, v)$	$2^{10}4^{10}$
$(v + 2x + 2)$	$(2x^3 + 2x + v + 2)$	$(2v)$	$(2, v)$	$2^{10}4^{10}$
$(v + 2x + 2)$	$(2x^3 + 2x + v + 2)$	$(2, v)$	$(2v)$	$2^{10}4^{10}$
$(v + 2x + 2)$	$(2x^2 + 2x + v + 2)$	$(2v)$	$(2, v)$	$2^{10}4^{10}$
$(v + 2x)$	$(2x^2 + 2x + v + 2)$	$(2, v)$	$(2v)$	$2^{10}4^{10}$
$(v + 2x + 2)$	$(2x^2 + 2x + v + 2)$	$(2, v)$	$(2v)$	$2^{10}4^{10}$
$(v + 2x)$	(2)	$(2x^2 + v)$	$(2x^2 + 2x + v + 2)$	$2^{10}4^{10}$
$(v + 2x + 2)$	(2)	$(2x^2 + v)$	$(2x^2 + 2x + v + 2)$	$2^{10}4^{10}$
$(v + 2x)$	(2)	$(v + 2x)$	$(2x^3 + 2x^2 + v + 2)$	$2^{10}4^{10}$
$(v + 2x + 2)$	(2)	$(v + 2x)$	$(2x^3 + 2x^2 + v + 2)$	$2^{10}4^{10}$
$(v + 2x)$	(2)	$(2x^2 + v + 2)$	$(2x^2 + 2x + v)$	$2^{10}4^{10}$
$(v + 2x + 2)$	(2)	$(2x^2 + v + 2)$	$(2x^2 + 2x + v)$	$2^{10}4^{10}$
$(v + 2x)$	(2)	$(v + 2x + 2)$	$(2x^3 + 2x^2 + v)$	$2^{10}4^{10}$
$(v + 2x + 2)$	(2)	$(v + 2x + 2)$	$(2x^3 + 2x^2 + v)$	$2^{10}4^{10}$
(2)	$(2x^3 + 2x + v)$	(v)	$(v + 2)$	2^64^{12}
(2)	$(2x^3 + 2x + v)$	$(2x^3 + 2x^2 + v)$	$(2x^2 + v)$	2^64^{12}
(2)	$(2x^3 + 2x + v)$	$(2x^3 + 2x + v)$	$(2x^3 + 2x^2 + 2x + v)$	2^64^{12}
(2)	$(2x^3 + 2x + v)$	$(v + 2)$	(v)	2^64^{12}
(2)	$(2x^3 + 2x + v)$	$(2x^3 + 2x^2 + v + 2)$	$(2x^2 + v + 2)$	2^64^{12}
(2)	$(2x^3 + 2x + v)$	$(2x^3 + 2x + v + 2)$	$(2x^3 + 2x^2 + 2x + v + 2)$	2^64^{12}
(2)	$(2x^3 + 2x + v)$	(0)	(1)	2^64^{12}
(2)	$(2x^2 + 2x + v)$	(v)	$(v + 2)$	2^64^{12}
(2)	$(2x^2 + 2x + v)$	$(2x^3 + v)$	$(v + 2x)$	2^64^{12}
(2)	$(2x^2 + 2x + v)$	$(2x^3 + 2x^2 + 2x + v)$	$(2x^3 + v)$	2^64^{12}
(2)	$(2x^2 + 2x + v)$	$(v + 2)$	(v)	2^64^{12}
(2)	$(2x^2 + 2x + v)$	$(2x^3 + v + 2)$	$(v + 2x + 2)$	2^64^{12}
(2)	$(2x^2 + 2x + v)$	$(2x^3 + 2x^2 + 2x + v + 2)$	$(2x^3 + v + 2)$	2^64^{12}
(2)	$(2x^3 + 2x + v + 2)$	(v)	$(v + 2)$	2^64^{12}
(2)	$(2x^3 + 2x + v + 2)$	$(2x^3 + 2x^2 + v)$	$(2x^2 + v)$	2^64^{12}
(2)	$(2x^3 + 2x + v + 2)$	$(2x^3 + 2x + v)$	$(2x^3 + 2x^2 + 2x + v)$	2^64^{12}
(2)	$(2x^3 + 2x + v + 2)$	$(v + 2)$	(v)	2^64^{12}
(2)	$(2x^3 + 2x + v + 2)$	$(2x^3 + 2x^2 + v + 2)$	$(2x^2 + v + 2)$	2^64^{12}
(2)	$(2x^3 + 2x + v + 2)$	$(2x^3 + 2x + v + 2)$	$(2x^3 + 2x^2 + 2x + v + 2)$	2^64^{12}
(2)	$(2x^3 + 2x + v + 2)$	(0)	(1)	2^64^{12}
(2)	$(2x^2 + 2x + v + 2)$	(v)	$(v + 2)$	2^64^{12}
(2)	$(2x^2 + 2x + v + 2)$	$(2x^3 + v)$	$(v + 2x)$	2^64^{12}
(2)	$(2x^2 + 2x + v + 2)$	$(2x^3 + 2x^2 + 2x + v)$	$(2x^3 + v)$	2^64^{12}
(2)	$(2x^2 + 2x + v + 2)$	$(v + 2)$	(v)	2^64^{12}
(2)	$(2x^2 + 2x + v + 2)$	$(2x^3 + v + 2)$	$(v + 2x + 2)$	2^64^{12}
(2)	$(2x^2 + 2x + v + 2)$	$(2x^3 + 2x^2 + 2x + v + 2)$	$(2x^3 + v + 2)$	2^64^{12}
$(v + 2x)$	$(2x^3 + 2x + v)$	(v)	$(v + 2)$	2^24^{14}

$(v + 2x)$	$(2x^3 + 2x + v)$	$(2x^3 + 2x + v)$	$(2x^3 + 2x^2 + 2x + v)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^3 + 2x + v)$	$(2x^3 + 2x + v)$	$(2x^3 + 2x^2 + 2x + v)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^3 + 2x + v)$	$(v + 2)$	(v)	$2^2 4^{14}$
$(v + 2x)$	$(2x^3 + 2x + v)$	$(2x^2 + v + 2)$	$(2x^2 + 2x + v)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^3 + 2x + v)$	$(v + 2x + 2)$	$(2x^3 + 2x^2 + v)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^3 + 2x + v)$	$(v + 2x + 2)$	$(2x^3 + 2x^2 + v)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^3 + 2x + v)$	(0)	(1)	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^3 + 2x + v)$	(0)	(1)	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^2 + 2x + v)$	(v)	$(v + 2)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v)$	$(2x^3 + 2x^2 + 2x + v)$	$(2x^3 + v)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^2 + 2x + v)$	$(2x^3 + 2x^2 + 2x + v)$	$(2x^3 + v)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v)$	$(v + 2)$	(v)	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v)$	$(2x^2 + v + 2)$	$(2x^2 + 2x + v)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^2 + 2x + v)$	$(2x^2 + v + 2)$	$(2x^2 + 2x + v)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v)$	$(2x^3 + 2x^2 + 2x + v + 2)$	$(2x^3 + v + 2)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v)$	(1)	(0)	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v)$	(0)	(1)	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^2 + 2x + v)$	(0)	(1)	$2^2 4^{14}$
$(v + 2x)$	$(2x^3 + 2x + v + 2)$	(v)	$(v + 2)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^3 + 2x + v + 2)$	$(2x^2 + v)$	$(2x^2 + 2x + v + 2)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^3 + 2x + v + 2)$	$(2x^3 + 2x^2 + v)$	$(2x^2 + v)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^3 + 2x + v + 2)$	$(2x^3 + 2x^2 + v)$	$(2x^2 + v)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^3 + 2x + v + 2)$	$(v + 2x)$	$(2x^3 + 2x^2 + v + 2)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^3 + 2x + v + 2)$	$(v + 2x)$	$(2x^3 + 2x^2 + v + 2)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^3 + 2x + v + 2)$	$(v + 2)$	(v)	$2^2 4^{14}$
$(v + 2x)$	$(2x^3 + 2x + v + 2)$	(0)	(1)	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^3 + 2x + v + 2)$	(0)	(1)	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^2 + 2x + v + 2)$	(v)	$(v + 2)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v + 2)$	$(2x^3 + v)$	$(v + 2x)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v + 2)$	$(2x^2 + v)$	$(2x^2 + 2x + v + 2)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^2 + 2x + v + 2)$	$(2x^2 + v)$	$(2x^2 + 2x + v + 2)$	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v + 2)$	$(v + 2)$	(v)	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v + 2)$	$(2x^3 + v + 2)$	$(v + 2x + 2)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^2 + 2x + v + 2)$	$(2x^3 + v + 2)$	$(v + 2x + 2)$	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^2 + 2x + v + 2)$	(1)	(0)	$2^2 4^{14}$
$(v + 2x)$	$(2x^2 + 2x + v + 2)$	(0)	(1)	$2^2 4^{14}$
$(v + 2x + 2)$	$(2x^2 + 2x + v + 2)$	(0)	(1)	$2^2 4^{14}$

Let ϕ be the Gray map from \mathbb{Z}_4^{30} onto \mathbb{F}_2^{60} extended by $0 \rightarrow 00, 1 \rightarrow 01, 2 \rightarrow 11, 3 \rightarrow 10$ in the natural way. Then ϕ is a distance and orthogonality preserving bijection from $(\mathbb{Z}_4^{30}, \text{Lee distance})$ onto $(\mathbb{F}_2^{60}, \text{Hamming distance})$. From the 70 2-quasi-cyclic self-dual codes with minimal Lee weight 12 and 92 2-quasi-cyclic self-dual codes with minimum Lee weight 10 over \mathbb{Z}_4 above and by the Gray map ϕ , we derive 70 4-quasi-cyclic type II binary formally self-dual $[60, 30, 12]$ codes and 92 4-quasi-cyclic type II binary formally self-dual $[60, 30, 10]$ codes. It is well known that binary self-dual $[60, 30, 12]$ codes are extremal (cf. [14] and [24]).

Acknowledgements Part of this work was done when Yonglin Cao was visiting the Chern Institute of Mathematics, Nankai University, Tianjin, China. Yonglin Cao would like to thank the institution for the kind hospitality. This research is supported in part by the National Natural Science Foundation of China (Grant Nos. 11671235, 11801324), the Shandong Provincial Natural Science Foundation, China (Grant No.

ZR2018BA007), the Scientific Research Fund of Hubei Provincial Key Laboratory of Applied Mathematics (Hubei University)(Grant No. AM201804) and the Scientific Research Fund of Hunan Provincial Key Laboratory of Mathematical Modeling and Analysis in Engineering (No. 2018MMAEZD09). Yuan Cao and Yonglin Cao contribute equally to this article.

References

1. Abualrub, T., Siap, I.: Cyclic codes over the ring $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$. *Des. Codes Cryptogr.* **42**, 273–287 (2007)
2. Calderbank, A.R., Hammons, A.R. Jr., Kumar, P.V., Sloane, N.J.A., Solé, P.: A linear construction for certain Kerdock and Preparata codes. *Bull. Am. Math. Soc.* **29**(2), 218–222 (1993)
3. Calderbank, A.R., Hammons, A.R. Jr., Kumar, P.V., Sloane, N.J.A., Solé, P.: The \mathbb{Z}_4 -linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inform. Theory* **40**, 301–319 (1994)
4. Cao, Y.: On constacyclic codes over finite chain rings. *Finite Fields Appl.* **24**, 124–135 (2013)
5. Cao, Y., Cao, Y., Li, Q.: The concatenated structure of cyclic codes over \mathbb{Z}_{p^2} . *J. Appl. Math. Comput.* **52**, 363–385 (2016)
6. Cao, Y., Cao, Y., Li, Q.: Concatenated structure of cyclic codes over \mathbb{Z}_4 of length $4n$. *Appl. Algebra in Engrg. Comm. Comput.* **10**, 279–302 (2016)
7. Cao, Y., Li, Q.: Cyclic codes of odd length over $\mathbb{Z}_4[u]/\langle u^k \rangle$. *Cryptogr. Commun.* **9**, 599–624 (2017)
8. Cao, Y., Cao, Y.: Negacyclic codes over the local ring $\mathbb{Z}_4[v]/\langle v^2 + 2v \rangle$ of oddly even length and their Gray images. *Finite Fields Appl.* **52**, 67–93 (2018)
9. Cao, Y., Gao, Y.: Repeated root cyclic \mathbb{F}_q -linear codes over \mathbb{F}_{q^t} . *Finite Fields Appl.* **31**, 202–227 (2015)
10. Cao, Y., Cao, Y.: Complete classification for simple root cyclic codes over local rings $\mathbb{Z}_{p^s}[v]/\langle v^2 - pv \rangle$, <https://www.researchgate.net/publication/320620031>
11. Dinh, H.Q.: Complete distance of all negacyclic codes of length 2^s over \mathbb{Z}_{2^a} . *IEEE Trans. Inf. Theory* **53**, 147–161 (2007)
12. Dinh, H.Q., Dhompongsa, S., Sriboonchitta, S.: On constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. *Discrete Math.* **340**, 832–849 (2017)
13. Dougherty, S.T., Kim, J.-L., Kulosman, H., Liu, H.: Self-dual codes over commutative Frobenius rings. *Finite Fields Appl.* **16**, 14–26 (2010)
14. Harada, M.: Binary extremal self-dual codes of length 60 and related codes. *Des. Codes Cryptogr.* **86**, 1085–1094 (2018)
15. Martínez-Moro, E., Szabo, S., Yildiz, B.: Linear codes over $\frac{\mathbb{Z}_4[x]}{\langle x^2 + 2x \rangle}$. *Int. J. Information and Coding Theory* **3**(1), 78–96 (2015)
16. Norton, G., Sălăgean-Mandache, A.: On the structure of linear and cyclic codes over finite chain rings. *Appl. Algebra in Engrg. Comm. Comput.* **10**, 489–506 (2000)
17. Shi, M., Zhu, S., Yang, S.: A class of optimal p -ary codes from one-weight codes over $F_p[u]/\langle u^m \rangle$. *J. Franklin Inst.* **350**(5), 729–737 (2013)
18. Shi, M., Qian, L., Sok, L., Aydin, N., Solé, P.: On constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2 - 1 \rangle$ and their Gray images. *Finite Fields Appl.* **45**(3), 86–95 (2017)
19. Shi, M., Zhang, Y.: Quasi-twisted codes with constacyclic constituent codes. *Finite Fields Appl.* **39**, 159–178 (2016)
20. Shi, M., Solé, P., Wu, B.: Cyclic codes and the weight enumerators over $\mathbb{F}_2 + v\mathbb{F}_2 + v^2\mathbb{F}_2$. *Applied and Computational Mathematics* **12**(2), 247–255 (2013)
21. Wan, Z.-X.: Cyclic codes over Galois rings. *Algebra Colloq.* **6**(3), 291–304 (1999)
22. Wan, Z.-X.: Lectures on finite fields and Galois rings. World Scientific Pub Co Inc (2003)
23. Wood, J.A.: Duality for modules over finite rings and applications to coding theory. *Am. J. Math.* **121**(3), 555–575 (1999)
24. Yankov, N., Lee, M.H.: New binary self-dual codes of lengths 50–60. *Des. Codes Cryptogr.* **73**, 983–996 (2014)
25. Yildiz, B., Karadeniz, S.: Linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$: Macwilliams identities, projections, and formally self-dual codes. *Finite Fields Appl.* **27**, 24–40 (2014)
26. Yildiz, B., Aydin, N.: Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and \mathbb{Z}_4 images. *International Journal of Information and Coding Theory* **2**(4), 226–237 (2014)