Applicable Algebra in Engineering, Communication and Computing (2022) 33:21–51
https://doi.org/10.1007/s00200-020-00424-0

ORIGINAL PAPER

Self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$

Yuan Cao[1,2,3] · Yonglin Cao[1] · Fang-Wei Fu[4] · Guidong Wang[1]

Received: 26 December 2019 / Accepted: 16 March 2020 / Published online: 27 April 2020

Abstract
For any odd positive integer n, we express cyclic codes over $\mathbb{Z}_4$ of length $4n$ in a new way. Based on the expression of each cyclic code $\mathcal{C}$, we provide an efficient encoder and determine the type of $\mathcal{C}$. In particular, we give an explicit representation and enumeration for all distinct self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$ and correct a mistake in the paper "Concatenated structure of cyclic codes over $\mathbb{Z}_4$ of length $4n$" (Cao et al. in Appl Algebra Eng Commun Comput 10:279–302, 2016). In addition, we obtain 50 new self-dual cyclic codes over $\mathbb{Z}_4$ of length 28.

Keywords Self-dual code · Cyclic code · Encoder · Galois ring

Mathematics Subject Classification 94B15 · 94B05 · 11T71

✉ Yonglin Cao
ylcao@sdut.edu.cn

Yuan Cao
yuancao@sdut.edu.cn

Fang-Wei Fu
fwfu@nankai.edu.cn

Guidong Wang
hbuwgd@163.com

[1] School of Mathematics and Statistics, Shandong University of Technology, Zibo 255091 Shandong, 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 410114, Hunan, China

[4] Chern Institute of Mathematics and LPMC, Nankai University, Tianjin 300071, China

1 Introduction

In [13], it was shown that many interesting binary linear and nonlinear codes are in fact the images under a Gray map of special linear codes over the ring $\mathbb{Z}_4$. This important discovery caused an enormous amount of activity led to the study of codes in this ambient space and linear codes over $\mathbb{Z}_4$ has become one of the most widely studied areas of algebraic coding theory.

The class of self-dual codes is an interesting topic in coding theory due to their connections with other fields of mathematics such as lattices, cryptography, invariant theory, block designs, etc. In particular, self-dual codes over $\mathbb{Z}_4$ relate to combinatorial designs and unimodular lattices (cf. [4, 12, 14–17]). A common theme for the construction of self-dual codes is the use of computational tools and computer search. To make this search feasible, adding an algebraic structure to the codes considered is an effective way.

We begin with the necessary definitions for codes over rings. Let A be a commutative finite ring with identity $1 \neq 0$, and $A^\times$ be the multiplicative group of invertible elements of A. For any $f, g \in A$, the ideal of A generated by f and g is denoted by $\langle f, g\rangle$, i.e., $\langle f, g\rangle = Af + Ag = \{af + bg \mid a, b \in A\}$.

A *code* over A of length N is a nonempty subset $\mathcal{C}$ of A^N. The code $\mathcal{C}$ is said to be *linear* if $\mathcal{C}$ is an A-submodule of A^N. Especially, $\mathcal{C}$ is called a $\mathbb{Z}_4$-linear code when $A = \mathbb{Z}_4$. All codes in this paper are assumed to be linear. The ambient space A^N is equipped with the usual Euclidean inner product, i.e. $[a, b] = \sum_{j=0}^{N-1} a_j b_j$, where $a = (a_0, a_1, \ldots, a_{N-1}), b = (b_0, b_1, \ldots, b_{N-1}) \in A^N$, and the (Euclidean) *dual code* is defined by $\mathcal{C}^\perp = \{a \in A^N \mid [a, b] = 0, \forall b \in \mathcal{C}\}$. If $\mathcal{C}^\perp = \mathcal{C}$, $\mathcal{C}$ is called a (Euclidean) *self-dual code* over A.

The linear code $\mathcal{C}$ is said to be *cyclic* if $(c_{N-1}, c_0, c_1, \ldots, c_{N-2}) \in \mathcal{C}$ for all $(c_0, c_1, \ldots, c_{N-1}) \in \mathcal{C}$. We use the natural connection of cyclic codes to polynomial rings, where $(c_0, c_1, \ldots, c_{N-1})$ is viewed as $c(x) = \sum_{j=0}^{N-1} c_j x^j$ and the cyclic code $\mathcal{C}$ is an ideal in the polynomial residue ring $A[x]/\langle x^N - 1\rangle$.

Let $\mathcal{C}$ be a nonzero $\mathbb{Z}_4$-linear code of length N. Then $\mathcal{C}$ has a generator matrix of the form: $G_\mathcal{C} = \begin{pmatrix} I_{k_0} & A & B \\ 0 & 2I_{k_1} & 2C \end{pmatrix} U$, where U is a suitable $N \times N$ permutation matrix, I_{k_0} and I_{k_1} denotes the $k_0 \times k_0$ and $k_1 \times k_1$ identity matrices, respectively, A and C are $\mathbb{Z}_2$-matrices, and B is a $\mathbb{Z}_4$-matrix. Then $\mathcal{C}$ is an abelian group of type $4^{k_0} 2^{k_1}$ and contains $2^{2k_0+k_2}$ codewords (cf. Wan [23, Proposition 1.1]).

Cyclic codes over $\mathbb{Z}_4$ of odd length n followed from results in [3] and also appeared in more detail in [20] and [21]. Abualrub and Oehmk in [1] determined the generators for cyclic codes over $\mathbb{Z}_4$ for lengths of the form 2^k, and Blackford in [2] presented the generators for cyclic codes over $\mathbb{Z}_4$ of length $2n$.

Let k and n be any integers such that $k \geq 1$ and n is odd. In 2006, Dougherty and Ling [11] gave a representation for cyclic codes over $\mathbb{Z}_4$ of length $2^k n$, described the number and dual codes of all these cyclic codes and obtained a rough description of cyclic codes that are self-dual. In 2012, Kiah et al. [18] determined the number of Euclidean self-dual codes over the Galois ring $\mathrm{GR}(4, s)$ of length 2^k, for any positive integers s and k. In 2016, Jitman et al. [19] pointed out that the determination of the Euclidean dual of a cyclic code in [2, Lemma 9]

and [11, Proposition 5.8] is not correct. Further, Jitman et al. found an incorrect statement about the number of Euclidean self-dual cyclic codes ([11, Corollaries 5.7, 5.9 and Proposition 5.8]), and gave the correct statement by [19, Corollary 4.8].

In 2016, Cao et al. [5] gave a concatenated structure for every cyclic code over $\mathbb{Z}_4$ of length $4n$ from a way different that was used in [2, 11, 18, 19]. However, there was a mistake in [5, Corollary 4.6]. In fact, it gives only a part of self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$, not all these self-dual codes.

There are two problems that need to be improved or addressed in [11, 19]:

1. For arbitrary positive integer k, by [11, Theorem 5.3], Dougherty and Ling divided 29 cases to express cyclic codes over $\mathrm{GR}(4, s)$ of length 2^k and their annihilators. This would lead to a lengthy description for the results of self-dual codes with length $2^k n$, if use [19, Proposition 4.5].
2. It is not convenient to express the result for (self-dual) cyclic codes over $\mathbb{Z}_4$ of length $2^k n$, if use Discrete Fourier Transform. In fact, it is not easy to apply [19, Proposition 4.5] for constructing and designing self-dual cyclic codes over $\mathbb{Z}_4$ of length $2^k n$, for any given concrete integers k and n.

There are similar problems in [5], it is some inconvenient to construct cyclic codes over $\mathbb{Z}_4$ of length $4n$ as well. First, all these cyclic codes were divided into 20 cases to express by [5, Theorem 4.5], which is still a bit lengthy. Second, the expressions for these cyclic codes need to be computed to get them (see [5, Example 3.4 and Theorem 4.5]).

Therefore, it is necessary and meaningful to find a more direct and simple method to express cyclic codes over $\mathbb{Z}_4$ of length $2^k n$ and to determine the self-dual cyclic codes accurately.

Recently, Cao et al. [6] gave an explicit representation for cyclic codes over $\mathbb{Z}_4$ of length $2n$ from a new way different from that was used in [2, 5, 11, 18, 19]. Using this representation, we provided an efficient encoder and the type for every code, and determined the (Euclidean) self-dual codes in this class of cyclic codes precisely. However, the methods used in [6] can not be directly used to the case of length $4n$, there are many key computational problems that require to develop new methods.

The present paper is organized as follows. In Sect. 2, we introduce necessary notations and provide necessary conclusions. In Sect. 3, we give the main results of this paper by four theorems: give an explicit representation for all distinct cyclic codes over $\mathbb{Z}_4$ of length $4n$ (Theorem 3.1); provide an efficient encoder for each of these cyclic code (Theorem 3.2); determine the dual code for every cyclic code (Theorem 3.3); give an explicit representation and enumeration for all distinct self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$ (Theorem 3.4). In addition, we correct a mistake in [5, Corollary 4.6]. In Sect. 4, we describe how to construct self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$ by two examples: when $n = 3$ and when $n = 7$. In particular, we obtain 50 new good self-dual cyclic $\mathbb{Z}_4$-codes $\mathcal{C}$ with basic parameters $(28, |\mathcal{C}| = 2^{28}, d_H = 4, d_L = 8, d_E = 8)$, where d_H, d_L and

d_E are the minimum Hamming distance, Lee distance and Euclidean distance of the codes respectively. In Sect. 5, we give detail proofs for Theorems 3.1–3.4 in Sect. 3. Section 6 concludes the paper.

2 Preliminaries

In this section, we introduce necessary notations and provide necessary conclusions for the following sections.

Let $\mathbb{F}_2 = \{0, 1\}$ in which the arithmetic is done modulo 2, and let $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ in which the arithmetic is done modulo 4. Denote $\mathbb{Z}_4^\times = \{1, 3\} = \{1, -1\}$. Let x, y be indeterminate over $\mathbb{Z}_4$ and $\mathbb{F}_2$. In this paper, we regard $\mathbb{F}_2$ as a subset of the ring $\mathbb{Z}_4$, though $\mathbb{F}_2$ is not a subfield of $\mathbb{Z}_4$. By this view, every element $a \in \mathbb{Z}_4$ has a unique 2-adic expansion: $a = a_0 + 2a_1$, $a_0, a_1 \in \mathbb{F}_2$. Denote $\overline{a} = a_0 = a \pmod 2$. Then $^- : a \mapsto \overline{a}$ $(\forall a \in \mathbb{Z}_4)$ is a surjective ring homomorphism from $\mathbb{Z}_4$ onto $\mathbb{F}_2$, and $^-$ can be extended to a surjective ring homomorphism from $\mathbb{Z}_4[y]$ onto $\mathbb{F}_2[y]$ by: $\overline{f}(y) = \overline{f(y)} = \sum_{i=0}^{d} \overline{b}_i y^i$, for any $f(y) = \sum_{i=0}^{d} b_i y^i \in \mathbb{Z}_4[y]$.

Let $f(y) = \sum_{j=0}^{d} c_j y^j \in \mathbb{Z}_4[y]$ of degree $d \geq 1$. Then $f(y)$ is said to be a *monic basic irreducible polynomial* if $\overline{f}(y)$ is an irreducible polynomial in $\mathbb{F}_2[y]$ and $c_d \in \mathbb{Z}_4^\times$ (cf. [24, Sect. 13.4]). The *reciprocal polynomial* of $f(y)$ is defined as $\widetilde{f}(y) = \widetilde{f(y)} = y^d f(\frac{1}{y}) = \sum_{j=0}^{d} c_j y^{d-j}$. Then $f(y)$ is said to be *self-reciprocal* if $\widetilde{f}(y) = \delta f(y)$ for some $\delta \in \mathbb{Z}_4^\times$. It is known that $\widetilde{\widetilde{f}(y)} = f(y)$ if $f(0) \neq 0$, and $\widetilde{f(y)g(y)} = \widetilde{f}(y)\widetilde{g}(y)$ for any monic polynomials $f(y), g(y) \in \mathbb{Z}_4[y]$ with positive degrees satisfying $f(0), g(0) \in \mathbb{Z}_4^\times$.

Throughout this paper, we assume the following factorization of $y^n - 1$:

$$y^n - 1 = f_1(y) f_2(y) \ldots f_r(y), \tag{1}$$

where $f_1(y) = y - 1, f_2(y), \ldots, f_r(y)$ are pairwise coprime monic basic irreducible polynomials in $\mathbb{Z}_4[y]$ with degree $\deg(f_i(y)) = m_i$ for all $i = 1, \ldots, r$. Then we have $y^n \equiv 1 \pmod{f_i(y)}$.

This implies that $x^{-1} \equiv x^{n-1} \pmod{\overline{f}_i(x)}$ and $x^{-1} \equiv x^{ln-1} \pmod{(\overline{f}_i(x))^l}$ in $\mathbb{F}_2[x]$ for any integer $l \geq 2$.

Additionally, we will adopt the following notation.

1. The ring $\mathcal{B} = \frac{\mathbb{Z}_4[x]}{\langle x^{4n}-1 \rangle} = \{\sum_{j=0}^{4n-1} b_j x^j \mid b_j \in \mathbb{Z}_4,\ j = 0, 1, \ldots, 4n-1\}$ where the arithmetic is done modulo $x^{4n} - 1$.

   Then cyclic codes over $\mathbb{Z}_4$ of length $4n$ are viewed as ideals of the ring $\mathcal{B}$.
2. The ring $\mathcal{R}_i = \frac{\mathbb{Z}_4[x]}{\langle f_i(x^4) \rangle} = \{\sum_{j=0}^{4m_i-1} b_j x^j \mid b_j \in \mathbb{Z}_4,\ j = 0, 1, \ldots, 4m_i - 1\}$ where the arithmetic is done modulo $f_i(x^4)$.

   We regard $\mathcal{R}_i$ as a subset of the ring $\mathcal{B}$ in this paper.

3. The set $\mathcal{T}_i = \{\sum_{j=0}^{m_i-1} t_j x^j \mid t_j \in \mathbb{F}_2 = \{0,1\},\ j = 0,\ldots,m_i-1\}$. Then $|\mathcal{T}_i| = 2^{m_i}$. We regard $\mathcal{T}_i$ as a subset of the ring $\mathcal{R}_i$.

Hereafter, the set $\mathcal{T}_i$ will appear frequently in the succeeding contents.

4. Denote by $F_i(y) = \frac{y^n-1}{f_i(y)} \in \mathbb{Z}_4[y]$. Then there are polynomials $u_i(y), v_i(y) \in \mathbb{Z}_4[y]$ such that (cf. [6, Sect. 2])

$$u_i(y)F_i(y) + v_i(y)f_i(y) = 1. \tag{2}$$

Then we define $\varepsilon_i(x) \in \mathcal{B}$ by the following equation:

$$\varepsilon_i(x) \equiv u_i(x^4)F_i(x^4) = 1 - v_i(x^4)f_i(x^4) \pmod{x^{4n}-1}. \tag{3}$$

5. Let $w_i(x) \in \mathcal{T}_i$ satisfying $f_i(x)^4 \equiv 2\bar{f}_i(x)^2 w_i(x)^2 \pmod{f_i(x^4)}$ in $\mathbb{Z}_4[x]$. Further, let $(w_{i,0}(x), w_{i,1}(x))$ be the unique ordered pair of elements in $\mathcal{T}_i$ satisfying

$$w_i(x)^2 = w_{i,0}(x) + w_{i,1}(x)\bar{f}_i(x) \ (\bmod\ (\bar{f}_i(x))^2) \ \text{ and } \ w_{i,0}(x) \neq 0 \ \text{ in } \ \mathbb{F}_2[x].$$

✓ The elements $w_i(x), w_{i,0}(x), w_{i,1}(x)$ of $\mathcal{T}_i$ play key roles in this paper, and they will be determined later by Theorem 2.5.

6. After a rearrangement of $f_2(y), \ldots, f_r(y)$, there are integers λ, ϵ such that

- ◇ $\lambda \geq 1$, $\epsilon \geq 0$ and $\lambda + 2\epsilon = r$.
- ◇ $f_i(y)$ is self-reciprocal, $i = 1, \ldots, \lambda$.

  Then $m_i = \deg(f_i(y))$ is even, when $2 \leq i \leq \lambda$ (cf. [8, Lemma 3.2]).
- ◇ $\widetilde{f}_{\lambda+j}(y) = c_{\lambda+j} f_{\lambda+\epsilon+j}(y)$ for some $c_{\lambda+j} \in \mathbb{Z}_4^\times$, $j = 1, \ldots, \epsilon$.

7. For any integer i, $2 \leq i \leq \lambda$, we define the following subsets of $\mathcal{T}_i$:

- $\mathcal{V}_i = \left\{ h(x) \in \mathcal{T}_i \mid h(x) + x^{3m_i} h(x^{-1}) \equiv 0 \ (\bmod \bar{f}_i(x)) \ \text{ in } \ \mathbb{F}_2[x] \right\}$.
- $\mathcal{W}_i^{(0)} = \{h_0(x) \in \mathcal{T}_i \mid h_0(x) + x^{2m_i}(w_i(x^{-1})^2 + h_0(x^{-1})) \equiv 0 \ (\bmod \bar{f}_i(x)) \text{ in } \mathbb{F}_2[x]\}$.
- For any $h_0(x) \in \mathcal{W}_i^{(0)}$, define

$$\mathcal{W}_{i,h_0(x)}^{(1)} = \{h_1(x) \in \mathcal{T}_i \mid h_0(x) + h_1(x)\bar{f}_i(x) \equiv \widehat{\delta}_{i,0}(x) + \widehat{\delta}_{i,1}(x)\bar{f}_i(x) \ (\bmod\ (\bar{f}_i(x))^2) \ \text{ in } \ \mathbb{F}_2[x]\},$$

where $\widehat{\delta}_{i,0}(x) = x^{2m_i}(w_i(x^{-1})^2 + h_0(x^{-1}))$ and $\widehat{\delta}_{i,1}(x) = x^{m_i} h_1(x^{-1})$.

✓ The subsets $\mathcal{V}_i, \mathcal{W}_i^{(0)}, \mathcal{W}_{i,h_0(x)}^{(1)}$ of $\mathcal{T}_i$ play key roles in this paper, and they will be determined later by Theorem 2.7.

Then we provide necessary conclusions for the following sections.

First, by substituting x^4 for y in Eqs. (1) and (2), we obtain

$$x^{4n}-1=f_1(x^4)f_2(x^4)\ldots f_r(x^4) \quad \text{and} \quad u_i(x^4)F_i(x^4)+v_i(x^4)f_i(x^4)=1$$

in $\mathbb{Z}_4[x]$ respectively, where $F_i(x^4)=\frac{x^{4n}-1}{f_i(x^4)} \in \mathbb{Z}_4[x]$. From this, by Eq. (3) and Chinese remainder theorem for commutative rings with identity, one can easily verify the following conclusions. Here we omit the proofs.

Lemma 2.1

(i) $\varepsilon_1(x)+\cdots+\varepsilon_r(x)=1, \varepsilon_i(x)^2=\varepsilon_i(x)$ *and* $\varepsilon_i(x)\varepsilon_j(x)=0$ for all $1 \le i \ne j \le r$ *in the ring* $\mathcal{B}$.

(ii) $\mathcal{B}=\mathcal{B}_1 \oplus \ldots \oplus \mathcal{B}_r$, *where* $\mathcal{B}_i=\langle \varepsilon_i(x)\rangle=\mathcal{B}\varepsilon_i(x)$ *is the ideal of* $\mathcal{B}$ *generated by* $\varepsilon_i(x)$, and $\mathcal{B}_i$ *is a commutative ring with* $\varepsilon_i(x)$ *as its multiplicative identity for all* $i=1,\ldots,r$. *Moreover,* $\mathcal{B}$ *is a direct sum of rings* $\mathcal{B}_1,\ldots,\mathcal{B}_r$ *in that* $\mathcal{B}_i\mathcal{B}_j=\{0\}$ for all $i \ne j$.

(iii) *Define the map* $\psi_i : a(x) \mapsto \varepsilon_i(x)a(x) \pmod{x^{4n}-1} (\forall a(x) \in \mathcal{R}_i)$. *Then* ψ_i *is a ring isomorphism from* $\mathcal{R}_i$ *onto* $\mathcal{B}_i$, for $i=1,\ldots,r$.

(iv) *Define a map* ψ *by: for any* $a_i(x) \in \mathcal{R}_i, 1 \le i \le r$, *let*

$$\psi(a_1(x),\ldots,a_r(x))=\sum_{i=1}^{r}\psi_i(a_i(x))=\sum_{i=1}^{r}\varepsilon_i(x)a_i(x) \pmod{x^{4n}-1}.$$

Then ψ *is a ring isomorphism from* $\mathcal{R}_1 \times \cdots \times \mathcal{R}_r$ onto $\mathcal{B}$.

To determine all cyclic codes over $\mathbb{Z}_4$ of length $4n$ (as ideals of the ring $\mathcal{B}$), by Lemma 2.1, we need to give all ideals of the ring $\mathcal{R}_i$ for all i.

Now, let i be an integer, $1 \le i \le r$. Since $f_i(x)$ is a minic basic irreducible polynomial in $\mathbb{Z}_4[x]$ of degree m_i, $\overline{f}_i(x)$ is an irreducible polynomial in $\mathbb{F}_2[x]$ of degree m_i. By $\overline{\mathbb{Z}}_4=\mathbb{F}_2$, we have $f_i(x^4)=\overline{f}_i(x)^4$ as polynomials in $\mathbb{F}_2[x]$. Then, we investigate the structure and properties of the ring $\mathcal{R}_i$. To do this, we introduce the following notation:

- $\overline{\mathcal{R}}_i=\frac{\mathbb{F}_2[x]}{\langle \overline{f}_i(x)^4\rangle}=\mathbb{F}_2[x]/\langle \overline{f}_i(x)^4\rangle=\{\sum_{j=0}^{4m_i-1}a_jx^j \mid a_j \in \mathbb{F}_2,\ j=0,1,\ldots,\ 4m_i-1\}$ in which the arithmetic is done modulo $\overline{f}_i(x)^4$ in $\mathbb{F}_2[x]$.
- $\mathcal{F}_i=\frac{\mathbb{F}_2[x]}{\langle \overline{f}_i(x)\rangle}=\mathbb{F}_2[x]/\langle \overline{f}_i(x)\rangle=\{\sum_{j=0}^{m_i-1}a_jx^j \mid a_j \in \mathbb{F}_2,\ j=0,\ldots,m_i-1\}$ in which the arithmetic is done modulo $\overline{f}_i(x)$ in $\mathbb{F}_2[x]$. Then $\mathcal{F}_i$ is a finite field of 2^{m_i} elements. As a set, we see $\mathcal{T}_i$ and $\mathcal{F}_i$ as the same in this paper.

Lemma 2.2 (cf. [7, Lemma 3.7])

(i) $\overline{\mathcal{R}}_i$ *is a finite chain ring with the maximal ideal* $\langle \overline{f}_i(x)\rangle=\overline{f}_i(x)\overline{\mathcal{R}}_i$, *the nilpotency index of* $\overline{f}_i(x)$ in $\overline{\mathcal{R}}_i$ is equal to 4 *and that* $\overline{\mathcal{R}}_i/\langle \overline{f}_i(x)\rangle \cong \mathcal{F}_i$. *Then all distinct ideals*

of $\overline{\mathcal{R}}_i$ *are given by*: $\{0\} = \langle \bar{f}_i(x)^4 \rangle \subset \langle \bar{f}_i(x)^3 \rangle \subset \langle \bar{f}_i(x)^2 \rangle \subset \langle \bar{f}_i(x) \rangle \subset \langle \bar{f}_i(x)^0 \rangle = \overline{\mathcal{R}}_i$.

(ii) *Every element* β *of* $\overline{\mathcal{R}}_i$ *has a unique* $\bar{f}_i(x)$*-adic expansion:*

$$\beta = t_0(x) + t_1(x)\bar{f}_i(x) + t_2(x)\bar{f}_i(x)^2 + t_3(x)\bar{f}_i(x)^3,\ t_j(x) \in \mathcal{F}_i,\ j = 0, 1, 2, 3.$$

Then β *is an invertible element of* $\overline{\mathcal{R}}_i$*, i.e.* $\beta \in \overline{\mathcal{R}}_i^{\times}$*, if and only if* $t_0(x) \neq 0$.

(iii) $|\bar{f}_i(x)^l \overline{\mathcal{R}}_i| = |\mathcal{F}_i|^{4-l} = 2^{m_i(4-l)}$, *for* $l = 0, 1, 2, 3, 4$.

As we regard $\mathbb{F}_2$ as a subset of $\mathbb{Z}_4$, we will regard $\overline{\mathcal{R}}_i$ as a subset of $\mathcal{R}_i$ hereafter, though $\overline{\mathcal{R}}_i$ is not a subring of $\mathcal{R}_i$. If needed, the reader is referred back to this identification of $\overline{\mathcal{R}}_i$ with a subset of $\mathcal{R}_i$. Then we have $2\mathcal{R}_i = \overline{\mathcal{R}}_i$.

Paralleling to the proof of [6, Lemma 4], one can easily verify the following conclusion. Here, we omit the proof.

Lemma 2.3 *Every element* $a(x)$ *of* $\mathcal{R}_i$ *has a unique* 2*-adic expansion*:

$$a(x) = a_0(x) + 2a_1(x), \quad a_0(x), a_1(x) \in \overline{\mathcal{R}}_i.$$

Then $a(x) \in \mathcal{R}_i^{\times}$ *if and only if* $a_0(x) \in \overline{\mathcal{R}}_i^{\times}$.

Let τ be the surjective ring homomorphism from $\mathcal{R}_i$ onto $\overline{\mathcal{R}}_i$ induced by $^- : \mathbb{Z}_4 \to \mathbb{F}_2$ in the natural way:

$$\tau : a(x) = a_0(x) + 2a_1(x) \mapsto \tau(a(x)) = \overline{a(x)} = a_0(x),$$

for all $a_0(x), a_1(x) \in \overline{\mathcal{R}}_i$. Let C be an ideal of $\mathcal{R}_i$. We define

$$\overline{C} = \tau(C) = \{\overline{a(x)} \mid a(x) \in C\} \quad \text{and} \quad (C : 2) = \{b(x) \in \mathcal{R}_i \mid 2b(x) \in C\}.$$

Then $\overline{C}$ is an ideal of $\overline{\mathcal{R}}_i$ and $(C : 2)$ is an ideal of $\mathcal{R}_i$ satisfying $C \subseteq (C : 2)$.

Lemma 2.4 *Let* l, s *be integers satisfying* $0 \leq s \leq l \leq 4$ *and* $v(x) \in \overline{\mathcal{R}}_i$*. Denote the ideal of* $\mathcal{R}_i$ *generated by* $f_i(x)^l + 2v(x)$ *and* $2\bar{f}_i(x)^s$ *as follows*

$$\begin{aligned} C_{(l,s;v(x))} :=& \langle f_i(x)^l + 2v(x), 2\bar{f}_i(x)^s \rangle \\ =& \{a(x) \cdot (f_i(x)^l + 2v(x)) + b(x) \cdot 2\bar{f}_i(x)^s \mid a(x), b(x) \in \mathcal{R}_i\}. \end{aligned}$$

Then we have the following conclusions:

(i) *We have* $\overline{C}_{(l,s;v(x))} = \langle \bar{f}_i(x)^l \rangle$ and $\overline{(C_{(l,s;v(x))} : 2)} = \langle \bar{f}_i(x)^s \rangle$ in $\overline{\mathcal{R}}_i$.

(ii) *The number of elements in* $C_{(l,s;v(x))}$ *is* $|C_{(l,s;v(x))}| = 2^{m_i(8-(l+s))}$.

(iii) *If* $s = l$*, we have* $C_{(l,s;v(x))} = \langle f_i(x)^l + 2v(x) \rangle$.

(iv) *For any* $u(x), v(x) \in \mathcal{R}_i$*, we have that*

$$C_{(l,s;u(x))} = C_{(l,s;v(x))} \Longleftrightarrow u(x) \equiv v(x) \ (\mathrm{mod}\, \overline{f}_i(x)^s) \text{ in } \mathbb{F}_2[x]. \tag{4}$$

Proof (i) Denote $C = C_{(l,s;v(x))}$ in the following. Then by the definition of $\overline{C}$ and $f_i(x)^l + 2v(x) = \overline{f}_i(x)^l$, it follows that $\overline{C} = \langle \overline{f}_i(x)^l \rangle$ immediately.

By $2\overline{f}_i(x)^s \in C$, we have that $\overline{f}_i(x)^s \in \overline{(C : 2)}$. This implies $\overline{f}_i(x)^s = \tau(\overline{f}_i(x)^s) \in \tau(C : 2) = \overline{(C : 2)}$. Hence $\langle \overline{f}_i(x)^s \rangle \subseteq \overline{(C : 2)}$.

Conversely, let $e(x) \in \overline{(C : 2)}$. Then $e(x) \in \overline{\mathcal{R}}_i$ and $e(x) + 2c(x) \in (C : 2)$ for some $c(x) \in \mathcal{R}_i$. This implies $2e(x) = 2(e(x) + 2c(x)) \in C$. Hence there exist $a(x), b(x) \in \mathcal{R}_i$ such that $2e(x) = a(x) \cdot (f_i(x)^l + 2v(x)) + b(x) \cdot 2\overline{f}_i(x)^s$. Since $f_i(x)^l$ is a monic polynomial in $\mathbb{Z}_4[x]$, by comparing the coefficients on both sides of the equation, we know that $a(x) = 2a_1(x)$ for some $a_1(x) \in \overline{\mathcal{R}}_i$. Therefore, by $2f_i(x)^l = 2\overline{f}_i(x)^l$, $2b(x) = 2\overline{b}(x)$, $4 = 0$ and $s \le l$, it follows that

$$\begin{aligned} 2e(x) =& 2a_1(x) \cdot (f_i(x)^l + 2v(x)) + 2\overline{b}(x)\overline{f}_i(x)^s = 2a_1(x)\overline{f}_i(x)^l + 2\overline{b}(x)\overline{f}_i(x)^s \\ =& 2(a_1(x)\overline{f}_i(x)^{l-s} + \overline{b}(x)) \cdot \overline{f}_i(x)^s. \end{aligned}$$

This implies $e(x) \in \langle \overline{f}_i(x)^s \rangle$. Hence $\overline{(C : 2)} = \langle \overline{f}_i(x)^s \rangle$.

(ii) Let $\tau|_C$ be the restriction of τ on the ideal $C = C_{(l,s;v(x))}$. Then $\tau|_C$ is a surjective ring homomorphism from C onto $\tau(C) = \overline{C} = \{\tau(c(x)) \mid c(x) \in C\}$. This implies $\tau(C) \cong C/\ker(\tau|_C)$, where $\ker(\tau|_C) = \{c(x) \in C \mid \tau(c(x)) = \overline{c}(x) = 0\}$ is the kernel of $\tau|_C$. Therefore, $|C| = |\tau(C)||\ker(\tau|_C)|$. By the definition of τ and $2 \cdot 2 = 0$, we have

$$\begin{aligned} \ker(\tau|_C) =& \{2c_1(x) \in C \mid c_1(x) \in \overline{\mathcal{R}}_i\} \\ =& \{2(c_1(x) + 2b(x)) \in C \mid c_1(x) + 2b(x) \in \mathcal{R}_i,\ c_1(x), b(x) \in \overline{\mathcal{R}}_i\} \\ =& 2(C : 2) = 2\tau(C : 2). \end{aligned}$$

This implies $|\ker(\tau|_C)| = |\tau(C : 2)|$. Then by (i) and Lemma 2.2 (iii), we obtain $|C| = |\tau(C)||\tau(C : 2)| = |\overline{C}||(C : 2)| = 2^{m_i(4-l)} \cdot 2^{m_i(4-s)} = 2^{m_i(8-(l+s))}$.

(iii) Let $s = l$. Then $2\overline{f}_i(x)^s = 2f_i(x)^l = 2(f_i(x)^l + 2v(x)) \subseteq \langle f_i(x)^l + 2v(x) \rangle$. Therefore, $C_{(l,s;v(x))} = \langle f_i(x)^l + 2v(x), 2\overline{f}_i(x)^s \rangle = \langle f_i(x)^l + 2v(x) \rangle$.

(iv) The part "$\Longleftarrow$" can be easily verified. Here, we only prove the part "$\Longrightarrow$". Now, let $C_{(l,s;u(x))} = C_{(l,s;v(x))} = C$. Then we see that $2(u(x) - v(x)) = (f_i(x)^l + 2u(x)) - (f_i(x)^l + 2v(x)) \in C$. This implies $u(x) - v(x) \in (C : 2)$. As $u(x), v(x) \in \overline{\mathcal{R}}_i$, by (i) it follows that $u(x) - v(x) \in \overline{(C : 2)} = \langle \overline{f}_i(x)^s \rangle$. Hence $u(x) \equiv v(x) \ (\mathrm{mod}\, \overline{f}_i(x)^s)$ in $\mathbb{F}_2[x]$. □

Now, we illustrate how to determine elements $w_i(x), w_{i,0}(x), w_{i,0}(x) \in \mathcal{T}_i$.

Theorem 2.5 *Let $1 \le i \le r$. Then $2f_i(x)$ is a divisor of $f_i(x)^2 - f_i(x^2)$ in $\mathbb{Z}_4[x]$* (cf. [6, Lemma 5 (i)]). *Denote $g_i(x) = \frac{f_i(x)^2 - f_i(x^2)}{2f_i(x)} \in \mathbb{Z}_4[x]$ and set $w_i(x) = g_i(x) \ (\mathrm{mod}\ 2)$. Then*

(i) *(cf.* [6, Lemma 5 (i)]) *We have* $f_i(x)^2 = f_i(x^2) + 2f_i(x)w_i(x)$ *in* $\mathbb{Z}_4[x]$ *and* $0 \neq w_i(x) \in \mathcal{T}_i$.

(ii) *We have* $f_i(x)^4 = 2\bar{f}_i(x)^2 w_i(x)^2$. *Moreover, let*

$$w_{i,0}(x) = w_i(x)^2 \pmod{\bar{f}_i(x)} \text{ and } w_{i,1}(x) = \frac{w_i(x)^2 - w_{i,0}(x)}{\bar{f}_i(x)} \pmod{\bar{f}_i(x)}$$

in $\mathbb{F}_2[x]$. *Then* $w_{i,0}(x), w_{i,1}(x) \in \mathcal{T}_i$ *satisfying*

$$w_i(x)^2 = w_{i,0}(x) + w_{i,1}(x)\bar{f}_i(x) \ (\bmod\ (\bar{f}_i(x))^2) \text{ and } w_{i,0}(x) \neq 0 \text{ in } \mathbb{F}_2[x].$$

Proof (ii) By $4 = 0$ and $f_i(x)^2 = f_i(x^2) + 2f_i(x)g_i(x)$ in $\mathbb{Z}_4[x]$, it follows that

$$\begin{aligned} f_i(x)^4 =& \big(f_i(x^2) + 2f_i(x)g_i(x)\big)^2 = f_i(x^2)^2 = f_i((x^2)^2) + 2f_i(x^2)g_i(x^2) \\ =& f_i(x^4) + 2\big(f_i(x)^2 - 2f_i(x)g_i(x)\big)g_i(x^2) \\ =& f_i(x^4) + 2f_i(x)^2 g_i(x^2). \end{aligned}$$

From this and by $w_i(x) = g_i(x) \pmod 2$, we deduce that

$$\begin{aligned} f_i(x)^4 \equiv& 2f_i(x)^2 g_i(x^2) \equiv 2\bar{f}_i(x)^2 \bar{g}_i(x^2) \equiv 2\bar{f}_i(x)^2 w_i(x^2) \\ \equiv& 2\bar{f}_i(x)^2 w_i(x)^2 \pmod{\langle f_i(x^4), 4\rangle}, \end{aligned}$$

i.e. $f_i(x)^4 = 2\bar{f}_i(x)^2 w_i(x)^2$ in the ring $\mathcal{R}_i$. By $0 \neq w_i(x) \in \mathcal{F}_i$, we see that $w_i(x)$ is an invertible element of $\overline{\mathcal{R}}_i$, i.e. $w_i(x) \in \overline{\mathcal{R}}_i^{\times}$, by Lemma 2.2 (ii). This implies $w_i(x)^2 \in \overline{\mathcal{R}}_i^{\times}$. Since $\deg(w_i(x)^2) = 2\deg(w_i(x)) \leq 2m_i - 2$, by Lemma 2.2 (ii), there exists a unique ordered pair $(w_{i,0}(x), w_{i,1}(x))$ of elements in $\mathcal{F}_i$ such that $w_{i,0}(x) \neq 0$ and $w_i(x)^2 = w_{i,0}(x) + w_{i,1}(x)\bar{f}_i(x)$ in $\overline{\mathcal{R}}_i$. The latter implies $w_i(x)^2 \equiv w_{i,0}(x) + w_{i,1}(x)\bar{f}_i(x) \pmod{f_i(x)^4}$, and hence $w_i(x)^2 \equiv w_{i,0}(x) + w_{i,1}(x)\bar{f}_i(x) \pmod{\bar{f}_i(x)^2}$ in $\mathbb{F}_2[x]$. □

In order to determine the subsets $\mathcal{V}_i$, $\mathcal{W}_i^{(0)}$ and $\mathcal{W}_{i,h_0(x)}^{(1)}$ of $\mathcal{F}_i$, for any $h_0(x) \in \mathcal{W}_i^{(0)}$ and $2 \leq i \leq \lambda$, we need the following lemma.

Lemma 2.6 (cf. [6, Lemma 5.1 (i)–(iv)]) *Let* $2 \leq i \leq \lambda$ *and set*

$$\mathcal{H}_i = \{a(x) \in \mathcal{F}_i = \mathbb{F}_2[x]/\langle \bar{f}_i(x)\rangle \mid a(x)^{2^{\frac{m_i}{2}}} \equiv a(x) \pmod{\bar{f}_i(x)}\}.$$

Then we have the following conclusions:

(i) *In the finite field* $\mathcal{F}_i$, *we have* $x^{-1} = x^{2^{\frac{m_i}{2}}}$.

(ii) $\mathcal{H}_i$ *is a subfield of* $\mathcal{F}_i$ *with* $2^{\frac{m_i}{2}}$ *elements*.

(iii) *Let* $\mathrm{Tr}_{\mathcal{F}_i/\mathcal{H}_i}$ *be the trace function from* $\mathcal{F}_i$ *onto* $\mathcal{H}_i$ *defined by*:

$$\mathrm{Tr}_{\mathcal{F}_i/\mathcal{H}_i}(\xi) = \xi + \xi^{2^{\frac{m_i}{2}}}, \quad \forall \xi \in \mathcal{F}_i.$$

Then for any $\alpha \in \mathcal{H}_i$, the number of elements $\xi \in \mathcal{F}_i$ such that $\mathrm{Tr}_{\mathcal{F}_i/\mathcal{H}_i}(\xi) = \alpha$ is $2^{\frac{m_i}{2}}$, i.e. $|\mathrm{Tr}^{-1}_{\mathcal{F}_i/\mathcal{H}_i}(\alpha)| = 2^{\frac{m_i}{2}}$ (cf. [24, Corollary 7.17]).

(iv) *Let $w_i(x)$ be determined by Lemma 2.5. Then $x^{m_i} w_i(x^{-1}) \equiv w_i(x) \,(mod\ \bar{f}_i(x))$ in $\mathbb{F}_2[x]$ and $x^{\frac{m_i}{2}} w_i(x^{-1}) \in \mathcal{H}_i$.*

Finally, the subsets $\mathcal{V}_i$, $\mathcal{W}_i^{(0)}$ and $\mathcal{W}_{i,h_0(x)}^{(1)}$ of $\mathcal{F}_i$ can be calculated by the following theorem.

Theorem 2.7 *Using the notations in Lemma 2.6, we have the following*:

(i) $\mathcal{V}_i = \left\{ x^{\frac{3m_i}{2}} \xi(x) \left(\mathrm{mod}\, \bar{f}_i(x) \right) \mid \xi(x) \in \mathrm{Tr}^{-1}_{\mathcal{F}_i/\mathcal{H}_i}(0) \right\}$. *Therefore, we have* $|\mathcal{V}_i| = |\mathrm{Tr}^{-1}_{\mathcal{F}_i/\mathcal{H}_i}(0)| = 2^{\frac{m_i}{2}}$.

(ii) *We have that $x^{m_i} w_i(x^{-1})^2 \in \mathcal{H}_i$ and*

$$\mathcal{W}_i^{(0)} = \left\{ x^{m_i} \xi(x) \left(\mathrm{mod}\, \bar{f}_i(x) \right) \mid \xi(x) \in \mathrm{Tr}^{-1}_{\mathcal{F}_i/\mathcal{H}_i}\left(x^{m_i} w_i(x^{-1})^2 \right) \right\}.$$

Hence $|\mathcal{W}_i^{(0)}| = |\mathrm{Tr}^{-1}_{\mathcal{F}_i/\mathcal{H}_i}\left(x^{m_i} w_i(x^{-1})^2 \right)| = 2^{\frac{m_i}{2}}$.

(iii) *Let $h_0(x) \in \mathcal{W}_i^{(0)}$. Then $h_0(x) + x^{2m_i}(w_i(x^{-1})^2 + h_0(x^{-1})) \equiv 0 \,(mod\ \bar{f}_i(x))$ in $\mathbb{F}_2[x]$. Let $\varsigma_i(x) \in \mathcal{F}_i$ be defined by*

$$\varsigma_i(x) := \frac{h_0(x) + x^{2m_i}(w_i(x^{-1})^2 + h_0(x^{-1}))}{\bar{f}_i(x)} \left(\mathrm{mod}\, \bar{f}_i(x) \right) \text{ in } \mathbb{F}_2[x].$$

Then we have that $x^{-\frac{m_i}{2}} \varsigma_i(x) \in \mathcal{H}_i$ and

$$\mathcal{W}_{i,h_0(x)}^{(1)} = \left\{ x^{\frac{m_i}{2}} \xi(x) \left(\mathrm{mod}\, \bar{f}_i(x) \right) \mid \xi(x) \in \mathrm{Tr}^{-1}_{\mathcal{F}_i/\mathcal{H}_i}\left(x^{-\frac{m_i}{2}} \varsigma_i(x) \right) \right\}.$$

Hence $|\mathcal{W}_{i,h_0}^{(1)}| = |\mathrm{Tr}^{-1}_{\mathcal{F}_i/\mathcal{H}_i}(x^{-\frac{m_i}{2}} \varsigma_i(x))| = 2^{\frac{m_i}{2}}$.

Proof (i) Let $h(x) \in \mathcal{T}_i = \mathcal{F}_i$. Then $h(x) \in \mathcal{V}_i$ if and only if $h(x)$ satisfies the following congruence relation:

$$h(x) + x^{3m_i} h(x^{-1}) \equiv 0 \,(\mathrm{mod}\, \bar{f}_i(x)) \text{ in } \mathbb{F}_2[x]. \tag{5}$$

By Lemma 2.6 (i), we have $x^{2^{\frac{m_i}{2}}} = x^{-1}$ in $\mathcal{F}_i$. This implies that $(h(x))^{2^{\frac{m_i}{2}}} = h(x^{-1})$. Hence Eq. (5) is equivalent to

$$\begin{aligned}\mathrm{Tr}_{\mathcal{F}_i/\mathcal{H}_i}(x^{-\frac{3m_i}{2}}h(x)) =& x^{-\frac{3m_i}{2}}h(x) + (x^{-\frac{3m_i}{2}}h(x))^{2^{\frac{m_i}{2}}}\\ =& x^{-\frac{3m_i}{2}}h(x) + x^{\frac{3m_i}{2}}h(x^{-1})\\ =& x^{-\frac{3m_i}{2}}\left(h(x) + x^{3m_i}h(x^{-1})\right)\\ =& 0 \text{ in } \mathcal{F}_i.\end{aligned}$$

Now, denote $\xi(x) = x^{-\frac{3m_i}{2}}h(x)$. Then $\xi(x) \in \mathrm{Tr}^{-1}_{\mathcal{F}_i/\mathcal{H}_i}(0)$ and $h(x) = x^{\frac{3m_i}{2}}\xi(x)$. Hence $\mathcal{V}_i = x^{\frac{3m_i}{2}} \cdot \mathrm{Tr}^{-1}_{\mathcal{F}_i/\mathcal{H}_i}(0) = \left\{x^{\frac{3m_i}{2}}\xi(x) \in \mathcal{F}_i \mid \xi(x) \in \mathrm{Tr}^{-1}_{\mathcal{F}_i/\mathcal{H}_i}(0)\right\}$.

(ii) By Lemma 2.6 (iv), we have $x^{\frac{m_i}{2}}w_i(x^{-1}) \in \mathcal{H}_i$. Since $\mathcal{H}_i$ is a subfield of $\mathcal{F}_i$, we obtain $x^{m_i}w_i(x^{-1})^2 = (x^{\frac{m_i}{2}}w_i(x^{-1}))^2 \in \mathcal{H}_i$.

Let $h_0(x) \in \mathcal{F}_i$. Then $h_0(x) \in \mathcal{W}_i^{(0)}$ if and only if $h_0(x)$ satisfies the following congruence relation:

$$h_0(x) + x^{2m_i}(w_i(x^{-1})^2 + h_0(x^{-1})) \equiv 0 \pmod{\bar{f}_i(x)} \text{ in } \mathbb{F}_2[x]. \tag{6}$$

By $x^{2^{\frac{m_i}{2}}} = x^{-1}$ and $(h_0(x))^{2^{\frac{m_i}{2}}} = h_0(x^{-1})$, Eq. (6) is equivalent to that $\mathrm{Tr}_{\mathcal{F}_i/\mathcal{H}_i}(x^{-m_i}h_0(x)) = x^{-m_i}h_0(x) + x^{m_i}h_0(x^{-1}) = x^{m_i}w_i(x^{-1})^2$. Now, we set $\xi(x) = x^{-m_i}h_0(x)$. Then $\xi(x) \in \mathrm{Tr}^{-1}_{\mathcal{F}_i/\mathcal{H}_i}\left(x^{m_i}w_i(x^{-1})^2\right)$ and $h_0(x) = x^{m_i}\xi(x)$. So $\mathcal{W}_i^{(0)} = \{x^{m_i}\xi(x) \in \mathcal{F}_i \mid \xi(x) \in \mathrm{Tr}^{-1}_{\mathcal{F}_i/\mathcal{H}_i}(x^{m_i}w_i(x^{-1})^2)\}$.

(iii) Let $h_0(x) \in \mathcal{W}_i^{(0)}$. Then $h_0(x)$ satisfies Eq. (6). This implies that $h_0(x) + x^{2m_i}(w_i(x^{-1})^2 + h_0(x^{-1}))$ is a multiple of the polynomial $\bar{f}_i(x)$ in $\mathbb{F}_2[x]$. Hence the polynomial $\varsigma_i(x) \in \mathcal{F}_i$ is well-defined.

As $2 \le i \le \lambda$, $f_i(x)$ is self-reciprocal in $\mathbb{Z}_4[x]$. This implies that $\bar{f}_i(x)$ is a self-reciprocal polynomial in $\mathbb{F}_2[x]$, i.e., $\bar{f}_i(x) = f_i(x)$. From this and by $\deg(\bar{f}_i(x)) = m_i$, we deduce $x^{m_i}\bar{f}_i(x^{-1}) = \bar{f}_i(x) = \bar{f}_i(x)$. Further, by Lemma 2.6 (iv), it follows that $w_i(x)^2 = (x^{m_i}w_i(x^{-1})) = x^{2m_i}w_i(x^{-2})$. Hence

$$\begin{aligned}\left(x^{-\frac{m_i}{2}}\varsigma_i(x)\right)^{2^{\frac{m_i}{2}}} =& x^{\frac{m_i}{2}}\left(\frac{h_0(x) + x^{2m_i}(w_i(x^{-1})^2 + h_0(x^{-1}))}{\bar{f}_i(x)}\right)^{2^{\frac{m_i}{2}}}\\ =& x^{\frac{m_i}{2}} \cdot \frac{h_0(x^{-1}) + x^{-2m_i}(w_i(x)^2 + h_0(x))}{\bar{f}_i(x^{-1})}\\ =& x^{\frac{m_i}{2}} \cdot \frac{h_0(x^{-1}) + x^{-2m_i}(w_i(x)^2 + h_0(x))}{x^{-m_i}\bar{f}_i(x)}\\ =& x^{-\frac{m_i}{2}} \cdot \frac{x^{2m_i}h_0(x^{-1}) + w_i(x)^2 + h_0(x)}{\bar{f}_i(x)}\\ =& x^{-\frac{m_i}{2}}\varsigma_i(x).\end{aligned}$$

This implies $x^{-\frac{m_i}{2}}\varsigma_i(x) \in \mathcal{H}_i$.

Now, let $h_1(x) \in \mathcal{F}_i$. Then $h_1(x) \in \mathcal{W}^{(1)}_{i,h_0(x)}$ if and only if $h_1(x)$ satisfies the following congruence relation:

$$h_0(x) + h_1(x)\bar{f}_i(x) \equiv \widehat{\delta}_{i,0}(x) + \widehat{\delta}_{i,1}(x)\bar{f}_i(x) \pmod{\bar{f}_i(x)^2} \text{ in } \mathbb{F}_2[x], \tag{7}$$

where $\widehat{\delta}_{i,0}(x) = x^{2m_i}(w_i(x^{-1})^2 + h_0(x^{-1}))$ and $\widehat{\delta}_{i,1}(x) = x^{m_i}h_1(x^{-1})$. Since

$$\begin{aligned} &h_0(x) + \widehat{\delta}_{i,0}(x) + \widehat{\delta}_{i,1}(x)\bar{f}_i(x) \\ &\quad = h_0(x) + x^{2m_i}(w_i(x^{-1})^2 + h_0(x^{-1})) + x^{m_i}h_1(x^{-1})\bar{f}_i(x) \\ &\quad = \varsigma_i(x)\bar{f}_i(x) + x^{m_i}h_1(x^{-1})\bar{f}_i(x) \pmod{\bar{f}_i(x)^2}, \end{aligned}$$

Equation (7) is equivalent to $\varsigma_i(x) + h_1(x) + x^{m_i}h_1(x^{-1}) \equiv 0 \pmod{\bar{f}_i(x)}$ in $\mathbb{F}_2[x]$, i.e., $\mathrm{Tr}_{\mathcal{F}_i/\mathcal{H}_i}(x^{-\frac{m_i}{2}}h_1(x)) = x^{-\frac{m_i}{2}}h_1(x) + x^{\frac{m_i}{2}}h_1(x^{-1}) = x^{-\frac{m_i}{2}}\varsigma_i(x)$. Therefore, $h_1(x) = x^{\frac{m_i}{2}}\xi(x) \in \mathcal{F}_i$, where $\xi(x) \in \mathrm{Tr}^{-1}_{\mathcal{F}_i/\mathcal{H}_i}(x^{-\frac{m_i}{2}}\varsigma_i(x))$. Hence $\mathcal{W}^{(1)}_{i,h_0(x)} = \left\{ x^{\frac{m_i}{2}}\xi(x) \in \mathcal{F}_i \mid \xi(x) \in \mathrm{Tr}^{-1}_{\mathcal{F}_i/\mathcal{H}_i}\left(x^{-\frac{m_i}{2}}\varsigma_i(x)\right) \right\}$.

Finally, the conclusions $|\mathcal{V}_i| = |\mathcal{W}^{(0)}_i| = |\mathcal{W}^{(1)}_{i,h_0(x)}| = 2^{\frac{m_i}{2}}$ follow from Lemma 2.6 (iii) immediately. □

3 Main results

In this section, we list the main results of this paper by four theorems. Every result here is a significant simplification of the original in that it requires only 10 cases, compared to the 20 cases that the paper [5] requires. In particular, the expression here is much more direct and explicit. Moreover, they are interesting development and a non-trivial extension of the theory in [6].

First, we list all distinct ideals of $\mathcal{B}$ by the following theorem.

Theorem 3.1 *All distinct cyclic codes over $\mathbb{Z}_4$ of length $4n$ are given by:*

$$\mathcal{C} = \bigoplus_{i=1}^{r} \mathcal{C}_i = \sum_{i=1}^{r} \mathcal{C}_i = \{\xi_1(x) + \cdots + \xi_r(x) \mid \xi_i(x) \in \mathcal{C}_i,\ i = 1, \ldots, r\},$$

where

$$\mathcal{C}_i = \varepsilon_i(x)C_i = \{\varepsilon_i(x)b(x) \mid b(x) \in C_i\} \pmod{x^{4n} - 1},$$

which is a subcode of $\mathcal{C}$ for all $i, 1 \le i \le r$, and C_i is an ideal of the ring $\mathcal{R}_i$ listed by the following table:

Case	C_i	Type of $\mathcal{C}_i$	$\lvert\mathcal{C}_i\rvert$	L
1.	$\langle 0\rangle$	$4^0 2^0$	1	1
2.	$\langle 1\rangle$	$4^{4m_i} 2^0$	2^{8m_i}	1

Case	C_i	Type of C_i	$\lvert C_i\rvert$	L
3.	$\langle 2\bar{f}_i(x)^s\rangle\,(s=0,1,2,3)$	$4^0 2^{(4-s)m_i}$	$2^{(4-s)m_i}$	4
4.	$\langle f_i(x)^l, 2\rangle\,(l=1,2,3)$	$4^{(4-l)m_i}2^{lm_i}$	$2^{(8-l)m_i}$	3
5.	$\langle f_i(x)+2h(x)\rangle$	$4^{3m_i}2^0$	2^{6m_i}	2^{m_i}
6.	$\langle f_i(x)^2+2h(x), 2\bar{f}_i(x)\rangle$	$4^{2m_i}2^{m_i}$	2^{5m_i}	2^{m_i}
7.	$\langle f_i(x)^2+2(h_0(x)+h_1(x)\bar{f}_i(x))\rangle$	$4^{2m_i}2^0$	2^{4m_i}	$(2^{m_i})^2$
8.	$\langle f_i(x)^3+2h(x), 2\bar{f}_i(x)\rangle$	$4^{m_i}2^{2m_i}$	2^{4m_i}	2^{m_i}
9.	$\langle f_i(x)^3+2\bar{f}_i(x)h(x), 2\bar{f}_i(x)^2\rangle$	$4^{m_i}2^{m_i}$	2^{3m_i}	2^{m_i}
10.	$\langle f_i(x)^3+2\bar{f}_i(x)\cdot(w_{i,0}(x)+h(x)\bar{f}_i(x))\rangle$	$4^{m_i}2^0$	2^{2m_i}	2^{m_i}

where $h(x), h_0(x), h_1(x) \in \mathcal{T}_i$ arbitrary, and L is the number of ideals C_i in the same row.

Further, let $4^{k_{0,i}}2^{k_{1,i}}$ be the type of the subcode $\mathcal{C}_i$ listed in the table above for all integers i: $1 \le i \le r$. Then the cyclic code $\mathcal{C}$ is of type

$$4^{\sum_{i=1}^r k_{0,i}} 2^{\sum_{i=1}^r k_{1,i}}.$$

Hence the number of codewords in $\mathcal{C}$ is $\prod_{i=1}^r |\mathcal{C}_i| = 2^{2\sum_{i=1}^r k_{0,i}+\sum_{i=1}^r k_{1,i}}$. Moreover, the minimum Hamming distance (Lee distance and Euclidean distance) of $\mathcal{C}$ satisfies $d_{\min}(\mathcal{C}) \le \min\{d_{\min}(\varepsilon_i(x)C_i) \mid i=1,\dots,r\}$.

Therefore, the number of all cyclic codes $\mathcal{C}$ over $\mathbb{Z}_4$ of length $4n$ is equal to $\prod_{i=1}^r (9+5\cdot 2^{m_i}+4^{m_i})$.

Using the notation of Theorem 3.1, $\mathcal{C} = \bigoplus_{j=1}^r \varepsilon_j(x)C_j$ is called the *canonical form decomposition* of the cyclic code $\mathcal{C}$ over $\mathbb{Z}_4$.

Similar to [8, Eq. (9)], in the rest of this paper we identify each polynomial $a(x) = a_0 + a_1 x + \cdots + a_{4n-1}x^{4n-1} \in \mathcal{B} = \frac{\mathbb{Z}_4[x]}{\langle x^{4n}-1\rangle}$ with $(a_0, a_1, \dots, a_{4n-1}) \in \mathbb{Z}_4^{4n}$. Further, for any integer $1 \le \rho \le 4(n-1)$, define:

$$[a(x)]_{\rho,4n} = \begin{pmatrix} a(x) \\ xa(x) \\ \cdots \\ x^{\rho-1}a(x) \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{4n-2} & a_{4n-1} \\ a_{4n-1} & a_0 & \cdots & a_{4n-3} & a_{4n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{4n-\rho+1} & a_{4n-\rho+2} & \cdots & a_{4n-\rho-1} & a_{4n-\rho} \end{pmatrix}, \quad (8)$$

which is a matrix over $\mathbb{Z}_4$ of size $\rho \times 4n$. Then we provide an efficient encoder for each cyclic code $\mathcal{C}$ over $\mathbb{Z}_4$ of length $4n$ by the following theorem.

Theorem 3.2 *Let $\mathcal{C}$ be a cyclic code over $\mathbb{Z}_4$ of length $4n$ with canonical form decomposition $\mathcal{C} = \bigoplus_{i=1}^r \mathcal{C}_i$, where $\mathcal{C}_i = \varepsilon_i(x)C_i$ and C_i is an ideal of $\mathcal{R}_i$ given by the table in Theorem 3.1. Then a generator matrix G_i for each subcode $\mathcal{C}_i$, $1 \le i \le r$, is given by the following table:*

Case	Generator matrix G_i	Subcode $\mathcal{C}_i$
1.	0	$\{0\}$
2.	$[\varepsilon_i(x)]_{4m_i,4n}$	$\{\underline{u}G_i \mid \underline{u} \in \mathbb{Z}_4^{4m_i}\}$
3.	$[2\overline{f}_i(x)^s\varepsilon_i(x)]_{(4-s)m_i,4n}$	$\{\underline{v}G_i \mid \underline{v} \in \mathbb{F}_2^{(4-s)m_i}\}$
4.	$\begin{pmatrix} [f_i(x)^l\varepsilon_i(x)]_{(4-l)m_i,4n} \\ [2\varepsilon_i(x)]_{lm_i,4n} \end{pmatrix}$	$\{(\underline{u},\underline{v})G_i \mid \underline{u} \in \mathbb{Z}_4^{(4-l)m_i}, \underline{v} \in \mathbb{F}_2^{lm_i}\}$
5.	$[(f_i(x)+2h(x))\varepsilon_i(x)]_{3m_i,4n}$	$\{\underline{u}G_i \mid \underline{u} \in \mathbb{Z}_4^{3m_i}\}$
6.	$\begin{pmatrix} [(f_i(x)^2+2h(x))\varepsilon_i(x)]_{2m_i,4n} \\ [2\overline{f}_i(x)\varepsilon_i(x)]_{m_i,4n} \end{pmatrix}$	$\{(\underline{u},\underline{v})G_i \mid \underline{u} \in \mathbb{Z}_4^{2m_i}, \underline{v} \in \mathbb{F}_2^{m_i}\}$
7.	$[(f_i(x)^2+2(h_0(x)+h_1(x)\overline{f}_i(x)))\varepsilon_i(x)]_{2m_i,4n}$	$\{\underline{u}G_i \mid \underline{u} \in \mathbb{Z}_4^{2m_i}\}$
8.	$\begin{pmatrix} [(f_i(x)^3+2h(x))\varepsilon_i(x)]_{m_i,4n} \\ [2\overline{f}_i(x)\varepsilon_i(x)]_{2m_i,4n} \end{pmatrix}$	$\{(\underline{u},\underline{v})G_i \mid \underline{u} \in \mathbb{Z}_4^{m_i}, \underline{v} \in \mathbb{F}_2^{2m_i}\}$
9.	$\begin{pmatrix} [(f_i(x)^3+2\overline{f}_i(x)h(x))\varepsilon_i(x)]_{m_i,4n} \\ [2\overline{f}_i(x)^2\varepsilon_i(x)]_{m_i,4n} \end{pmatrix}$	$\{(\underline{u},\underline{v})G_i \mid \underline{u} \in \mathbb{Z}_4^{m_i}, \underline{v} \in \mathbb{F}_2^{m_i}\}$
10.	$[(f_i(x)^3+2\overline{f}_i(x)(w_{i,0}(x)+h(x)\overline{f}_i(x)))\varepsilon_i(x)]_{m_i,4n}$	$\{\underline{u}G_i \mid \underline{u} \in \mathbb{Z}_4^{m_i}\}$

where $h(x), h_0(x), h_1(x) \in \mathcal{T}_i$ *arbitrary*.

Now, we determine the dual code of each cyclic code.

Theorem 3.3 *Let* $\mathcal{C}$ *be a cyclic code over* $\mathbb{Z}_4$ *of length* $4n$ *with canonical form decomposition* $\mathcal{C} = \bigoplus_{i=1}^{r} \varepsilon_i(x)C_i$, *where* C_i *is an ideal of the ring* $\mathcal{R}_i$. *Then the dual code of* $\mathcal{C}$ *is given by* $\mathcal{C}^{\perp} = \bigoplus_{i=1}^{r} \varepsilon_{\mu(i)}(x)D_{\mu(i)} = \bigoplus_{j=1}^{r} \varepsilon_j(x)D_j$, *where* $D_{\mu(i)}$ *is an ideal of* $\mathcal{R}_{\mu(i)}$ *determined by the following table*:

$C_i \pmod{f_i(x^4)}$	$D_{\mu(i)} \pmod{f_{\mu(i)}(x^4)}$
$\diamond\ \langle 0\rangle$	$\bullet\ \langle 1\rangle$
$\diamond\ \langle 1\rangle$	$\bullet\ \langle 0\rangle$
$\diamond\ \langle 2\overline{f}_i(x)^s\rangle\ (s=0,1,2,3)$	$\bullet\ \langle f_{\mu(i)}(x)^{4-s}, 2\rangle$
$\diamond\ \langle f_i(x)^l, 2\rangle\ (l=1,2,3)$	$\bullet\ \langle 2\overline{f}_{\mu(i)}(x)^{4-l}\rangle$
$\diamond\ \langle f_i(x)+2h(x)\rangle$	$\bullet\ \langle f_{\mu(i)}(x)^3 + 2\overline{f}_{\mu(i)}(x)\cdot(x^{2m_i}w_{i,0}(x^{-1}) + \widehat{\vartheta}_i(x)\overline{f}_{\mu(i)}(x))\rangle$ where $\widehat{\vartheta}_i(x) = x^{m_i}\left(w_{i,1}(x^{-1}) + h(x^{-1})\right)$
$\diamond\ \langle f_i(x)^2+2h(x), 2\overline{f}_i(x)\rangle$	$\bullet\ \langle f_{\mu(i)}(x)^3 + 2\overline{f}_{\mu(i)}(x)\widehat{t}_i(x), 2\overline{f}_{\mu(i)}(x)^2\rangle$ where $\widehat{t}_i(x) = x^{2m_i}\left(w_{i,0}(x^{-1}) + h(x^{-1})\right)$
$\diamond\ \langle f_i(x)^2+2(h_0(x)+h_1(x)\overline{f}_i(x))\rangle$	$\bullet\ \langle f_{\mu(i)}(x)^2 + 2(\widehat{\delta}_{i,0}(x) + \widehat{\delta}_{i,1}(x)\overline{f}_{\mu(i)}(x))\rangle$ where $\widehat{\delta}_{i,0}(x) = x^{2m_i}(w_i(x^{-1})^2 + h_0(x^{-1}))$ and $\widehat{\delta}_{i,1}(x) = x^{m_i}h_1(x^{-1})$
$\diamond\ \langle f_i(x)^3+2h(x), 2\overline{f}_i(x)\rangle$	$\bullet\ \langle f_{\mu(i)}(x)^3 + 2x^{3m_i}h(x^{-1}), 2\overline{f}_{\mu(i)}(x)\rangle$
$\diamond\ \langle f_i(x)^3+2\overline{f}_i(x)h(x), 2\overline{f}_i(x)^2\rangle$	$\bullet\ \langle f_{\mu(i)}(x)^2 + 2\widehat{t}_i(x), 2\overline{f}_{\mu(i)}(x)\rangle$ where $\widehat{t}_i(x) = x^{2m_i}\left(w_{i,0}(x^{-1}) + h(x^{-1})\right)$

$C_i \pmod{f_i(x^4)}$	$D_{\mu(i)} \pmod{f_{\mu(i)}(x^4)}$
$\diamond \langle f_i(x)^3 + 2\overline{f}_i(x)(w_{i,0}(x) + h(x)\overline{f}_i(x))\rangle$	$\bullet \langle f_{\mu(i)}(x) + 2\widehat{\vartheta}_i(x)\rangle$ where $\widehat{\vartheta}_i(x) = x^{m_i}(w_{i,1}(x^{-1}) + h(x^{-1}))$

in which μ is a permutation on the set $\{1, \ldots, r\}$ defined by

$$\mu(i) = i, \text{ if } 1 \le i \le \lambda;\ \mu(\lambda + j) = \lambda + j + \epsilon \text{ and } \mu(\lambda + j + \epsilon) = \lambda + j,\ \forall j = 1, \ldots, \epsilon,$$

and $h(x), h_0(x), h_1(x) \in \mathcal{T}_i$ arbitrary.

Finally, we list all distinct self-dual cyclic codes by the following theorem.

Theorem 3.4 *Using the notation of Sect. 2, all distinct self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$ are given by:*

$$\mathcal{C} = \bigoplus_{1 \le i \le r} \varepsilon_i(x) C_i,$$

where for each integer $i, 1 \le i \le r$, C_i is an ideal of $\mathcal{R}_i$ given by the following three cases:

(i) *C_1 is one of the following 3 ideals*:

$$C_1 = \langle 2\rangle, \quad C_1 = \langle (x-1)^3, 2(x-1)\rangle,\ C_1 = \langle (x-1)^3 + 2, 2(x-1)\rangle,$$

(ii) *If $2 \le i \le \lambda$, C_i is one of the following $1 + 2^{\frac{m_i}{2}} + 2^{m_i}$ ideals:*

(ii-1) $C_i = \langle 2\rangle$.

(ii-2) $C_i = \langle f_i(x)^2 + 2(h_0(x) + h_1(x)\overline{f}_i(x))\rangle$, *where* $h_0(x) \in \mathcal{W}_i^{(0)}$ *and* $h_1(x) \in \mathcal{W}_{i,h_0(x)}^{(1)}$.

(ii-3) $C_i = \langle f_i(x)^3 + 2h(x), 2\overline{f}_i(x)\rangle$, *where* $h(x) \in \mathcal{V}_i$.

(iii) *If $i = \lambda + j$, where $1 \le j \le \epsilon$, $(C_i, C_{i+\epsilon})$ is one of $4^{m_{\lambda+j}} + 5 \cdot 2^{m_{\lambda+j}} + 9$ pairs of ideals given by the following table:*

$C_i \pmod{f_i(x^4)}$	$C_{i+\epsilon} \pmod{f_{i+\epsilon}(x^4)}$
$\diamond \langle 0\rangle$	$\bullet \langle 1\rangle$
$\diamond \langle 1\rangle$	$\bullet \langle 0\rangle$
$\diamond \langle 2\overline{f}_i(x)^s\rangle\ (s = 0, 1, 2, 3)$	$\bullet \langle f_{i+\epsilon}(x)^{4-s}, 2\rangle$
$\diamond \langle f_i(x)^l, 2\rangle\ (l = 1, 2, 3)$	$\bullet \langle 2\overline{f}_{i+\epsilon}(x)^{4-l}\rangle$
$\diamond \langle f_i(x) + 2h(x)\rangle$	$\bullet \langle f_{i+\epsilon}(x)^3 + 2\overline{f}_{i+\epsilon}(x) \cdot (x^{2m_i} w_{i,0}(x^{-1}) + \widehat{\vartheta}_i(x)\overline{f}_{i+\epsilon}(x))\rangle$ where $\widehat{\vartheta}_i(x) = x^{m_i}\left(w_{i,1}(x^{-1}) + h(x^{-1})\right)$
$\diamond \langle f_i(x)^2 + 2h(x), 2\overline{f}_i(x)\rangle$	$\bullet \langle f_{i+\epsilon}(x)^3 + 2\overline{f}_{i+\epsilon}(x)\widehat{t}_i(x), 2\overline{f}_{i+\epsilon}(x)^2\rangle$ where $\widehat{t}_i(x) = x^{2m_i}\left(w_{i,0}(x^{-1}) + h(x^{-1})\right)$

$C_i \pmod{f_i(x^4)}$	$C_{i+\epsilon} \pmod{f_{i+\epsilon}(x^4)}$
$\diamond \langle f_i(x)^2 + 2(h_0(x) + h_1(x)\bar{f}_i(x))\rangle$	$\bullet \langle f_{i+\epsilon}(x)^2 + 2(\widehat{\delta}_{i,0}(x) + \widehat{\delta}_{i,1}(x)\bar{f}_{i+\epsilon}(x))\rangle$ where $\widehat{\delta}_{i,0}(x) = x^{2m_i}(w_i(x^{-1})^2 + h_0(x^{-1}))$ and $\widehat{\delta}_{i,1}(x) = x^{m_i}h_1(x^{-1})$
$\diamond \langle f_i(x)^3 + 2h(x), 2\bar{f}_i(x)\rangle$	$\bullet \langle f_{i+\epsilon}(x)^3 + 2x^{3m_i}h(x^{-1}), 2\bar{f}_{i+\epsilon}(x)\rangle$
$\diamond \langle f_i(x)^3 + 2\bar{f}_i(x)h(x), 2\bar{f}_i(x)^2\rangle$	$\bullet \langle f_{i+\epsilon}(x)^2 + 2\widehat{t}_i(x), 2\bar{f}_{i+\epsilon}(x)\rangle$ where $\widehat{t}_i(x) = x^{2m_i}\left(w_{i,0}(x^{-1}) + h(x^{-1})\right)$
$\diamond \langle f_i(x)^3 + 2\bar{f}_i(x)(w_{i,0}(x) + h(x)\bar{f}_i(x))\rangle$	$\bullet \langle f_{i+\epsilon}(x) + 2\widehat{\vartheta}_i(x)\rangle$ where $\widehat{\vartheta}_i(x) = x^{m_i}(w_{i,1}(x^{-1}) + h(x^{-1}))$

in which $h(x), h_0(x), h_1(x) \in \mathcal{T}_i$ *arbitrary.*
Therefore, the number of self-dual cyclic codes over $\mathbb{Z}_4$ *of length* $4n$ *is*

$$3 \cdot \prod_{2\le i\le\lambda} (1 + 2^{\frac{m_i}{2}} + 2^{m_i}) \cdot \prod_{j=1}^{\epsilon} (9 + 5 \cdot 2^{m_{\lambda+j}} + 4^{m_{\lambda+j}}).$$

Remark

(i) In [5, Corollary 4.6], the number of self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$ was proposed as:

$$3^{\lambda} \cdot \prod_{1\le j\le\epsilon} (9 + 5 \cdot 2^{m_{\lambda+j}} + 4^{m_{\lambda+j}}).$$

The mistake in this formula occurs in the cases (ii-2) and (ii-3). Obviously, the conclusion of [5, Corollary 4.6] holds when $\lambda = 1$.

(ii) By the table in p. 302 of [5], the number $\mathcal{N}$ of self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$ was proposed by the following table, where n is odd and $12 \le 4n \le 100$:

$4n$	$\mathcal{N}$	$4n$	$\mathcal{N}$	$4n$	$\mathcal{N}$
12, 20, 44, 52, 76	9	28	339	84	4500225
36, 68, 100	27	60	9315	92	12613659

There are mistakes in this table. Now, we correct them as follows:

$4n$	$\mathcal{N}$	corrected
12	$21 = 3 \cdot (1 + 2 + 2^2)$	✓
20	$63 = 3 \cdot (1 + 2^2 + 2^4)$	✓
28	$339 = 3 \cdot (9 + 5 \cdot 2^3 + 4^3)$	
36	$1533 = 3 \cdot (1 + 2 + 2^2) \cdot (1 + 2^3 + 2^6)$	✓

$4n$	$\mathcal{N}$	corrected
44	$3171 = 3 \cdot (1 + 2^5 + 2^{10})$	✓
52	$12483 = 3 \cdot (1 + 2^6 + 2^{12})$	✓
60	$152145 = 3 \cdot (1 + 2 + 2^2) \cdot (1 + 2^2 + 2^4) \cdot (9 + 5 \cdot 2^4 + 4^4)$	✓
68	$223587 = 3 \cdot (1 + 2^4 + 2^8)^2$	✓
76	$787971 = 3 \cdot (1 + 2^9 + 2^{18})$	✓
84	$10500525 = 3 \cdot (1 + 2 + 2^2) \cdot (9 + 5 \cdot 2^3 + 4^3) \cdot (9 + 5 \cdot 2^6 + 4^6)$	✓
92	$12613659 = 3 \cdot (9 + 5 \cdot 2^{11} + 4^{11})$	
100	$66124863 = 3 \cdot (1 + 2^2 + 2^4) \cdot (1 + 2^{10} + 2^{20})$	✓

4 Examples

In this section, we show how to use Theorem 3.4 to construct self-dual codes over $\mathbb{Z}_4$ of length $4n$.

Example 4.1 We construct all 21 self-dual cyclic codes over $\mathbb{Z}_4$ of length 12.

First, we have $y^3 - 1 = f_1(y)f_2(y)$, where $f_1(y) = y - 1$ and $f_2(y) = y^2 + y + 1$. In this case, $\lambda = r = 2$, $\epsilon = 0$. $\tilde{f}_1(y) = c_1 f_1(y)$, $\tilde{f}_2(y) = c_2 f_1(y)$, $c_1 = -1$ and $c_2 = 1$. Obviously, $3 \cdot f_2(y) + (y + 2)f_1(y) = 1$ in $\mathbb{Z}_4[y]$.

Using the notation in Sect. 2, we obtain

$$\varepsilon_1(x) = 3f_2(x^4) = 3x^8 + 3x^4 + 3 \text{ and } \varepsilon_2(x) = (x^4 + 2)f_1(x^4) = x^8 + x^4 + 2.$$

Further, by Theorems 2.5, 2.7 and Lemma 2.6 we have the following:

- $\bar{f}_2(x) = x^2 + x + 1$, $\overline{\mathcal{R}}_2 = \frac{\mathbb{F}_2[x]}{\langle (x^2+x+1)^4 \rangle}$ and $\mathcal{T}_2 = \{a + bx \mid a, b \in \mathbb{F}_2\}$.
- $g_2(x) = \frac{(x^2+x+1)^2 - ((x^2)^2+x^2+1)}{2(x^2+x+1)} = x \in \mathbb{Z}_4[x]$, $w_2(x) = g_2(x) = x \pmod 2$, and $w_2(x)^2 = x^2 = 1 + x + 1 \cdot (x^2 + x + 1)$.
  Hence $w_{i,0}(x) = 1 + x$ and $w_{i,1}(x) = 1$.
- $\mathcal{F}_2 = \frac{\mathbb{F}_2[x]}{\langle x^2+x+1 \rangle} = \{a + bx \mid a, b \in \mathbb{F}_2\}$ and $\mathcal{H}_2 = \{\xi \in \mathcal{F}_2 \mid \xi^{2^1} = \xi\} = \mathbb{F}_2$.
- $\mathrm{Tr}^{-1}_{\mathcal{F}_2/\mathcal{H}_2}(0) = \{\xi \in \mathcal{F}_2 \mid \xi + \xi^2 = 0\} = \{0, 1\}$;
  $\mathrm{Tr}^{-1}_{\mathcal{F}_2/\mathcal{H}_2}(1) = \{\xi \in \mathcal{F}_2 \mid \xi + \xi^2 = 1\} = \{x, 1 + x\}$.
- $\mathcal{V}_2 = \{x^{\frac{3\cdot 2}{2}} \xi \mid \xi \in \mathrm{Tr}^{-1}_{\mathcal{F}_2/\mathcal{H}_2}(0)\} = x^3 \cdot \mathrm{Tr}^{-1}_{\mathcal{F}_2/\mathcal{H}_2}(0) = \{0, 1\} \pmod{x^2 + x + 1}$.
- $\mathcal{W}_2^{(0)} = \{x^2\xi \mid \xi \in \mathrm{Tr}^{-1}_{\mathcal{F}_2/\mathcal{H}_2}(1)\} = \{1, x\}$, since $x^{m_2} w_2(x^{-1})^2 = x^2 x^{-2} = 1$.
- $\mathcal{W}_{2,1}^{(1)} = \{x^{-\frac{2}{2}} \xi \mid \xi \in \mathrm{Tr}^{-1}_{\mathcal{F}_2/\mathcal{H}_2}(0)\} = \{0, x\}$. This conclusion is due to $\varsigma_2(x) = \frac{1+x^4(x^{-2}+1)}{x^2+x+1} = \frac{1+x^2+x^4}{x^2+x+1} = x^2 + x + 1 = 0 \in \mathcal{F}_2$ and $x^{-\frac{2}{2}}\varsigma_2(x) = 0 \in \mathcal{H}_2$.
- $\mathcal{W}_{2,x}^{(1)} = \{x^{-\frac{2}{2}} \xi \mid \xi \in \mathrm{Tr}^{-1}_{\mathcal{F}_2/\mathcal{H}_2}(1)\} = \{1, 1 + x\}$. This conclusion is due to $\varsigma_2(x) = \frac{x+x^4(x^{-2}+x^{-1})}{x^2+x+1} = \frac{x+x^2+x^3}{x^2+x+1} = x \in \mathcal{F}_2$ and $x^{-\frac{2}{2}}\varsigma_2(x) = 1 \in \mathcal{H}_2$.

Then by Theorem 3.4 (i) and (ii), all distinct 21 self-dual cyclic codes over $\mathbb{Z}_4$ of length 12 are given by $\mathcal{C} = \varepsilon_1(x)C_1 \oplus \varepsilon_2(x)C_2$, where C_1 is given by Theorem 3.4 (i) and C_2 is an ideals of the ring $\frac{\mathbb{Z}_4[x]}{\langle x^8+x^4+1\rangle}$ given by:

$C_2 = \langle 2\rangle$.
$C_2 = \langle f_2(x)^2 + 2(h_0(x) + h_1(x)\bar{f}_2(x))\rangle$, $h_1(x) \in \mathcal{W}^{(1)}_{2,h_0(x)}$ and $h_0(x) \in \mathcal{W}^{(0)}_2$.
$C_2 = \langle f_2(x)^3 + 2h(x), 2\bar{f}_2(x)\rangle$, $h(x) \in \mathcal{V}_2$.
Specifically, all these 21 self-dual cyclic codes over $\mathbb{Z}_4$ are the following:

$$\mathcal{C}_{j,k} = \varepsilon_1(x)C_{1,j} \oplus \varepsilon_1(x)C_{2,k},\ j = 1, 2, 3 \text{ and } k = 1, 2, \ldots, 7,$$

where $C_{1,j}$ is an ideals of the ring $\frac{\mathbb{Z}_4[x]}{\langle x^4-1\rangle}$ given by:

$C_{1,1} = \langle 2\rangle$, $C_{1,2} = \langle (x-1)^3, 2(x-1)\rangle$, $C_{1,3} = \langle (x-1)^3 + 2, 2(x-1)\rangle$;
and $C_{2,k}$ is an ideals of the ring $\frac{\mathbb{Z}_4[x]}{\langle x^8+x^4+1\rangle}$ given by:

$C_{2,1} = \langle 2\rangle$, $C_{2,2} = \langle (x^2+x+1)^2 + 2\rangle$,
$C_{2,3} = \langle (x^2+x+1)^2 + 2(1 + x\cdot(x^2+x+1))\rangle$,
$C_{2,4} = \langle (x^2+x+1)^2 + 2(x + (x^2+x+1))\rangle$,
$C_{2,5} = \langle (x^2+x+1)^2 + 2(x + (1+x)(x^2+x+1))\rangle$,
$C_{2,6} = \langle (x^2+x+1)^3, 2(x^2+x+1)\rangle$,
$C_{2,7} = \langle (x^2+x+1)^3 + 2, 2(x^2+x+1)\rangle$.

Now, let

$$G_{1,1} = \left(\begin{array}{cccccccccccc} 2&0&0&0&2&0&0&0&2&0&0&0\\ 0&2&0&0&0&2&0&0&0&2&0&0\\ 0&0&2&0&0&0&2&0&0&0&2&0\\ 0&0&0&2&0&0&0&2&0&0&0&2 \end{array}\right), G_{1,2} = \left(\begin{array}{cccccccccccc} 1&1&3&3&1&1&3&3&1&1&3&3\\ \hline 2&2&0&0&2&2&0&0&2&2&0&0\\ 0&2&2&0&0&2&2&0&0&2&2&0 \end{array}\right),$$

$$G_{1,3} = \left(\begin{array}{cccccccccccc} 3&1&3&3&3&1&3&3&3&1&3&3\\ \hline 2&2&0&0&2&2&0&0&2&2&0&0\\ 0&2&2&0&0&2&2&0&0&2&2&0 \end{array}\right); G_{2,1} = \left(\begin{array}{cccccccccccc} 0&0&0&0&2&0&0&0&2&0&0&0\\ 0&0&0&0&0&2&0&0&0&2&0&0\\ 0&0&0&0&0&0&2&0&0&0&2&0\\ 0&0&0&0&0&0&0&2&0&0&0&2\\ 2&0&0&0&0&0&0&0&2&0&0&0\\ 0&2&0&0&0&0&0&0&0&2&0&0\\ 0&0&2&0&0&0&0&0&0&0&2&0\\ 0&0&0&2&0&0&0&0&0&0&0&2 \end{array}\right),$$

$$G_{2,2} = \left(\begin{array}{cccccccccccc} 3&0&2&0&1&2&3&2&0&2&3&2\\ 2&3&0&2&0&1&2&3&2&0&2&3\\ 3&2&3&0&2&0&1&2&3&2&0&2\\ 2&3&2&3&0&2&0&1&2&3&2&0 \end{array}\right), G_{2,3} = \left(\begin{array}{cccccccccccc} 3&0&2&0&1&0&1&0&0&0&1&0\\ 0&3&0&2&0&1&0&1&0&0&0&1\\ 1&0&3&0&2&0&1&0&1&0&0&0\\ 0&1&0&3&0&2&0&1&0&1&0&0 \end{array}\right),$$

$$G_{2,4} = \left(\begin{array}{cccccccccccc} 3&0&2&0&1&2&1&2&0&2&1&2\\ 2&3&0&2&0&1&2&1&2&0&2&1\\ 1&2&3&0&2&0&1&2&1&2&0&2\\ 2&1&2&3&0&2&0&1&2&1&2&0 \end{array}\right), G_{2,5} = \left(\begin{array}{cccccccccccc} 3&0&2&0&1&0&3&0&0&0&3&0\\ 0&3&0&2&0&1&0&3&0&0&0&3\\ 3&0&3&0&2&0&1&0&3&0&0&0\\ 0&3&0&3&0&2&0&1&0&3&0&0 \end{array}\right),$$

$$G_{2,6} = \left(\begin{array}{cccccccccccc} 0&1&1&2&1&1&0&3&3&2&3&3\\ 3&0&1&1&2&1&1&0&3&3&2&3\\ \hline 0&0&0&0&2&2&2&0&2&2&2&0\\ 0&0&0&0&0&2&2&2&0&2&2&2\\ 2&0&0&0&0&0&2&2&2&0&2&2\\ 2&2&0&0&0&0&0&2&2&2&0&2 \end{array}\right), G_{2,7} = \left(\begin{array}{cccccccccccc} 0&1&1&2&3&1&0&3&1&2&3&3\\ 3&0&1&1&2&3&1&0&3&1&2&3\\ \hline 0&0&0&0&2&2&2&0&2&2&2&0\\ 0&0&0&0&0&2&2&2&0&2&2&2\\ 2&0&0&0&0&0&2&2&2&0&2&2\\ 2&2&0&0&0&0&0&2&2&2&0&2 \end{array}\right).$$

Then by Theorem 3.2, the self-dual cyclic code $\mathcal{C}_{j,k}$ over $\mathbb{Z}_4$ of length 12 is generated by the matrix $\begin{pmatrix} G_{1,j} \\ G_{2,k} \end{pmatrix}$, and the type of $\mathcal{C}_{j,k}$ is given by:

$\mathcal{C}_{1,1} = 2(\mathbb{Z}_4^{12})$ is the trivial self-dual cyclic code of type $4^0 2^{12}$;
$\mathcal{C}_{1,k}$ is of type $4^4 2^4$ for $k = 2, 3, 4, 5$; $\mathcal{C}_{1,k}$ is of type $4^2 2^8$ for $k = 6, 7$;
$\mathcal{C}_{j,k}$ is of type $4^5 2^2$ for $j = 2, 3$ and $k = 2, 3, 4, 5$;
$\mathcal{C}_{j,k}$ is of type $4^3 2^6$ for $j = 2, 3$ and $k = 6, 7$.

Example 4.2 We construct self-dual cyclic codes over $\mathbb{Z}_4$ of length 28.

In this case, $y^7 - 1 = f_1(y)f_2(y)f_3(y)$, where $f_1(y) = y - 1$, $f_2(y) = y^3 + 2y^2 + y + 3$ and $f_3(y) = y^3 + 3y^2 + 2y + 3 = 3\widetilde{f_3}(y)$. These imply $\overline{f}_1(x) = x + 1$, $\overline{f}_2(x) = x^3 + x + 1$ and $\overline{f}_3(x) = x^3 + x^2 + 1$ in $\mathbb{F}_2[x]$.

Using the notations in Sect. 2, we have $r = 3$, $\lambda = 1$, $\epsilon = 1$, $m_1 = 1$ and $m_2 = m_3 = 3$. Hence there are $\prod_{i=1}^{3}(9 + 5 \cdot 2^{m_i} + 4^{m_i}) = 293687$ distinct cyclic codes over $\mathbb{Z}_4$ of length 28.

For each $i = 1, 2, 3$, let $F_i(y) = \frac{x^7-1}{f_i(y)}$ and find polynomials $u_i(y), v_i(y) \in \mathbb{Z}_4[y]$ satisfying $u_i(y)F_i(y) + v_i(y)f_i(y) = 1$. Then set $\varepsilon_i(x) = u_i(x^4)F_i(x^4) \pmod{x^{28} - 1}$. Precisely, we have

$\varepsilon_1(x) = 3x^{24} + 3x^{20} + 3x^{16} + 3x^{12} + 3x^8 + 3x^4 + 3$,
$\varepsilon_2(x) = 2x^{24} + 2x^{20} + 3x^{16} + 2x^{12} + 3x^8 + 3x^4 + 1$,
$\varepsilon_3(x) = 3x^{24} + 3x^{20} + 2x^{16} + 3x^{12} + 2x^8 + 2x^4 + 1$.

- $\mathcal{R}_1 = \frac{\mathbb{Z}_4[x]}{\langle f_1(x^4)\rangle} = \frac{\mathbb{Z}_4[x]}{\langle x^4-1\rangle}$ and $\mathcal{F}_1 = \mathbb{F}_2[x]/\langle \overline{f}_1(x)\rangle = \{0, 1\} = \mathcal{T}_1$.
- $\mathcal{R}_i = \frac{\mathbb{Z}_4[x]}{\langle f_i(x^4)\rangle}$ and $\mathcal{F}_i = \frac{\mathbb{F}_2[x]}{\langle \overline{f}_i(x)\rangle} = \{t_0 + t_1x + t_2x^2 \mid t_0, t_1, t_2 \in \{0, 1\}\} = \mathcal{T}_i$, for $i = 2, 3$.
- $g_2(x) = \frac{(x^3+2x^2+x+3)^2-(x^6+2x^4+x^2+3)}{2(x^3+2x^2+x+3)} = 2x^2 + 2x + 1 \in \mathbb{Z}_4[x]$,

  $w_2(x) = 1 = g_2(x) \pmod 2$, $w_{2,0}(x) = 1$ and $w_{2,1}(x) = 0$ which satisfy
  $w_2(x)^2 = 1 = w_{2,0}(x) + w_{2,1}(x)\overline{f}_2(x)$ in $\overline{\mathcal{R}}_2 = \mathbb{F}_2[x]/\langle \overline{f}_2(x)^4\rangle$.

By Theorem 3.4, all 339 self-dual codes over $\mathbb{Z}_4$ of length 28 are given by:

$$\mathcal{C} = \varepsilon_1(x)C_1 \oplus \varepsilon_2(x)C_2 \oplus \varepsilon_3(x)C_3,$$

where C_i is an ideal of $\mathcal{R}_i$, $1 \le i \le 3$, given by the following:

$\diamond$ C_1 is one of the following 3 ideals in $\mathcal{R}_1$:

$$\langle 2\rangle, \quad \langle (x-1)^3, 2(x-1)\rangle, \quad \langle (x-1)^3 + 2, 2(x-1)\rangle.$$

$\diamond$ (C_2, C_3) is one of the following 113 pairs of ideals, where C_2 is an ideal of $\mathcal{R}_2$ and C_3 is an ideal of $\mathcal{R}_3$:

1. $C_2 = \langle 0 \rangle$ and $C_3 = \langle 1 \rangle$;
2. $C_2 = \langle 1 \rangle$ and $C_3 = \langle 0 \rangle$;
3. $C_2 = \langle 2\bar{f}_2(x)^s \rangle$ and $C_3 = \langle f_3(x)^{4-s}, 2 \rangle$, where $s = 0, 1, 2, 3$;
4. $C_2 = \langle f_2(x)^l, 2 \rangle$ and $C_3 = \langle 2\bar{f}_3(x)^{4-l} \rangle$, where $l = 1, 2, 3$;
5. $C_2 = \langle f_2(x) + 2h(x) \rangle$ and $C_3 = \langle f_3(x)^3 + 2\bar{f}_3(x)(x^6 + \hat{\vartheta}_2(x)\bar{f}_3(x)) \rangle$;
6. $C_2 = \langle f_2(x)^2 + 2h(x), 2\bar{f}_2(x) \rangle$ and $C_3 = \langle f_3(x)^3 + 2\bar{f}_3(x)\hat{t}_2(x), 2\bar{f}_3(x)^2 \rangle$;
7. $C_2 = \langle f_2(x)^2 + 2(h_0(x) + h_1(x)\bar{f}_2(x)) \rangle$ and $C_3 = \langle f_3(x)^2 + 2(\hat{\delta}_{2,0}(x) + \hat{\delta}_{2,1}(x)\bar{f}_3(x)) \rangle$;
8. $C_2 = \langle f_2(x)^3 + 2h(x), 2\bar{f}_2(x) \rangle$ and $C_3 = \langle f_3(x)^3 + 2(ax^2 + bx + c), 2\bar{f}_3(x) \rangle$ in which $ax^2 + bx + c \equiv x^{3\cdot 3}h(x^{-1}) \pmod{\langle 2, \bar{f}_3(x) \rangle}$;
9. $C_2 = \langle f_2(x)^3 + 2\bar{f}_2(x)h(x), 2\bar{f}_2(x)^2 \rangle$ and $C_3 = \langle f_3(x)^2 + 2\hat{t}_2(x), 2\bar{f}_3(x) \rangle$;
10. $C_2 = \langle f_2(x)^3 + 2\bar{f}_2(x)(1 + h(x)\bar{f}_2(x)) \rangle$ and $C_3 = \langle f_3(x) + 2\hat{\vartheta}_2(x) \rangle$,

where

$h(x) = h_0(x) = a + bx + cx^2$ and $h_1(x) = g + ux + vx^2$ with $a, b, c, g, u, v \in \mathbb{F}_2$;
$\hat{\vartheta}_2(x) = (a + b)x^2 + cx + a \equiv x^3(w_{2,1}(x^{-1}) + h(x^{-1})) \equiv x^3h(x^{27})$
$\equiv x^3(a + bx^{27} + cx^{26}) \pmod{\bar{f}_3(x) = x^3 + x^2 + 1}$ in $\mathbb{F}_2[x]$;
$\hat{t}_2(x) = (a + c + 1)x^2 + (a + b + c + 1)x + b + c \equiv x^{2\cdot 3}(w_{2,0}(x^{-1}) + h(x^{-1})) \pmod{\bar{f}_3(x)}$ in $\mathbb{F}_2[x]$;
$\hat{\delta}_{2,0}(x) = bx^5 + (a + c + 1)x^4 + 1 + a \equiv x^{2\cdot 3}(w_2(x^{-1})^2 + h_0(x^{-1})) \pmod{\bar{f}_3(x)^2}$ in $\mathbb{F}_2[x]$;
$\hat{\delta}_{2,1}(x) = (g + u)x^2 + vx + g \equiv x^3h_1(x^{-1}) \pmod{\bar{f}_3(x)}$ in $\mathbb{F}_2[x]$.

Shi et al. obtained some good cyclic codes over $\mathbb{Z}_4$ from $(1 + 2u)$-constacyclic codes over the ring $\mathbb{Z}_4[u]/\langle u^2 - 1 \rangle$ by [22, Tables 1–3]. From self-dual negacyclic codes over the ring $\frac{\mathbb{Z}_4[v]}{\langle v^2+2v \rangle}$ of length 14, 36 new and good self-dual 2-quasi-twisted $\mathbb{Z}_4$-codes with parameters $(28, 2^{28}, d_L = 8, d_E = 12)$ and of type $4^7 2^{14}$ and parameters $(28, 2^{28}, d_L = 6, d_E = 12)$ and of type $4^6 2^{16}$ were given in [9]; From self-dual cyclic codes over $\frac{\mathbb{Z}_4[v]}{\langle v^2+2v \rangle}$ of length 15, 70 new and good self-dual 2-quasi-cyclic $\mathbb{Z}_4$-codes with parameters $(30, 2^{30}, d_L = 12)$ and 92 new and good self-dual 2-quasi-cyclic $\mathbb{Z}_4$-codes with parameters $(30, 2^{30}, d_L = 10)$ were obtained in [10], where d_H, d_L and d_E be the minimum Hamming distance, Lee distance and Euclidean distance of a $\mathbb{Z}_4$-code respectively (cf. [25]).

Now, among the 339 self-dual codes over $\mathbb{Z}_4$ of length 28 listed above, we have the following 50 new and good self-dual cyclic $\mathbb{Z}_4$-codes with basic parameters $(28, |C| = 2^{28}, d_H = 4, d_L = 8, d_E = 8)$:

- 8 self-dual cyclic $\mathbb{Z}_4$-codes of type $4^{12}2^4$ determined by:
  $C_1 = \langle 2 \rangle, C_2 = \langle \bar{f}_2(x) + 2(a + bx + cx^2) \rangle$,
  $C_3 = \langle f_3(x)^3 + 2\bar{f}_3(x)(x^6 + ((a + b)x^2 + cx + a)\bar{f}_3(x)) \rangle$,
  where $a, b, c \in \mathbb{F}_2 = \{0, 1\}$.
- 8 self-dual cyclic $\mathbb{Z}_4$-codes of type $4^{12}2^4$ determined by:
  $C_1 = \langle 2 \rangle, C_2 = \langle \bar{f}_2(x)^3 + 2\bar{f}_2(x)(1 + (a + bx + cx^2)\bar{f}_2(x)) \rangle$,
  $C_3 = \langle f_3(x) + 2((a + b)x^2 + cx + a) \rangle$, where $a, b, c \in \mathbb{F}_2$.
- 4 self-dual cyclic $\mathbb{Z}_4$-codes of type $4^{10}2^8$ determined by:

$C_1 = \langle (x-1)^3, 2(x-1)\rangle$, $C_2 = \langle 2\bar{f}_2(x)^3\rangle$ and $C_3 = \langle f_3(x), 2\rangle$, or $C_2 = \langle f_2(x), 2\rangle$ and $C_3 = \langle 2\bar{f}_3(x)^3\rangle$;
$C_1 = \langle (x-1)^3 + 2, 2(x-1)\rangle$, $C_2 = \langle 2\bar{f}_2(x)^3\rangle$ and $C_3 = \langle f_3(x), 2\rangle$, or $C_2 = \langle f_2(x), 2\rangle$ and $C_3 = \langle 2\bar{f}_3(x)^3\rangle$.

- 2 self-dual cyclic $\mathbb{Z}_4$-codes of type $4^7 2^{14}$ determined by:
  $C_1 = \langle (x-1)^3, 2(x-1)\rangle$, $C_2 = \langle f_2(x)^2, 2\rangle$ and $C_3 = \langle 2\bar{f}_3(x)^2\rangle$;
  $C_1 = \langle (x-1)^3 + 2, 2(x-1)\rangle$, $C_2 = \langle f_2(x)^2, 2\rangle$ and $C_3 = \langle 2\bar{f}_3(x)^2\rangle$.
- 6 self-dual cyclic $\mathbb{Z}_4$-codes of type $4^{13}2^2$ determined by:
  $C_1 = \langle (x-1)^3, 2(x-1)\rangle$, $C_2 = \langle f_2(x)^2 + 2h(x), 2\bar{f}_2(x)\rangle$,
  $C_3 = \langle f_3(x)^3 + 2\bar{f}_3(x)\widehat{t}_2(x), 2\bar{f}_3(x)^2\rangle$,
  where $(h(x), \widehat{t}_2(x)) \in \{(x^2, 1), (x, x^2+1), (x^2+x, x), (x^2+1, x^2+x+1), (x+1, x+1), (x^2+x+1, x^2)\}$.
- 6 self-dual cyclic $\mathbb{Z}_4$-codes of type $4^{13}2^2$ determined by:
  $C_1 = \langle (x-1)^3, 2(x-1)\rangle$, $C_2 = \langle f_2(x)^3 + 2\bar{f}_2(x)(1 + h(x)\bar{f}_2(x))\rangle$,
  $C_3 = \langle f_3(x) + 2\widehat{\vartheta}_2(x)\rangle$,
  where $(h(x), \widehat{\vartheta}_2(x)) \in \{(x^2, x), (x, x^2), (x^2+x, x^2+x), (x^2+1, x^2+x+1), (x+1, 1), (x^2+x+1, x+1)\}$.
- 8 self-dual cyclic $\mathbb{Z}_4$-codes of type $4^{13}2^2$ determined by:
  $C_1 = \langle (x-1)^3 + 2, 2(x-1)\rangle$, $C_2 = \langle f_2(x)^2 + 2(a + bx + cx^2), 2\bar{f}_2(x)\rangle$,
  $C_3 = \langle f_3(x)^3 + 2\bar{f}_3(x)((a+c+1)x^2 + (a+b+c+1)x + b + c), 2\bar{f}_3(x)^2\rangle$,
  where $a, b, c \in \mathbb{F}_2$.
- 8 self-dual cyclic $\mathbb{Z}_4$-codes of type $4^{13}2^2$ determined by:
  $C_1 = \langle (x-1)^3 + 2, 2(x-1)\rangle$, $C_2 = \langle f_2(x)^3 + 2\bar{f}_2(x)(1 + (a + bx + cx^2)\bar{f}_2(x))\rangle$,
  $C_3 = \langle f_3(x) + 2((a+b)x^2 + cx + a)\rangle$, where $a, b, c \in \mathbb{F}_2$.

5 Proofs of Theorems 3.1–3.4

In this section, we give the detail proofs for Theorems 3.1–3.4. First, we prove that ideals of the ring $\mathcal{B}$ are determined by ideals of rings $\mathcal{R}_i$, $i = 1, \ldots, r$.

Proposition 5.1 *Let $\mathcal{C} \subseteq \mathcal{B} = \frac{\mathbb{Z}_4[x]}{\langle x^{4n}-1\rangle}$. Then $\mathcal{C}$ is a cyclic code over $\mathbb{Z}_4$ of length $4n$ if and only if for each integer $i, 1 \le i \le r$, there is a unique ideal C_i of the ring $\mathcal{R}_i$ such that $\mathcal{C} = \bigoplus_{i=1}^{r} \mathcal{C}_i = \sum_{i=1}^{r} \mathcal{C}_i$, where*

$$\mathcal{C}_i = \varepsilon_i(x)C_i = \{\varepsilon_i(x)c_i(x) \mid c_i(x) \in C_i\} \pmod{x^{4n} - 1}.$$

Moreover, the number of codewords in $\mathcal{C}$ is equal to $|\mathcal{C}| = \prod_{i=1}^{r} |C_i|$.

Proof Let $\mathcal{C}$ be a cyclic code over $\mathbb{Z}_4$ of length $4n$. By Lemma 2.1 and properties of isomorphic rings, there is a unique ideal C of the direct product ring $\mathcal{R}_1 \times \cdots \times \mathcal{R}_r$ such that $\mathcal{C} = \psi(C)$. Hence for each integer $i, 1 \le i \le r$, there is a unique ideal C_i of $\mathcal{R}_i$ such that $C = C_1 \times \cdots \times C_r$. This implies

$$\begin{aligned}\mathcal{C} &= \{\psi(c_1(x), \ldots, c_r(x)) \mid c_i(x) \in C_i,\ i = 1, \ldots, r\} \\ &= \sum_{i=1}^{r} \{\varepsilon_i(x)c_i(x) \mid c_i(x) \in C_i\} \pmod{x^{4n} - 1}.\end{aligned}$$

Then the conclusion follows from Lemma 2.1(i), $\mathcal{C}_i = \varepsilon_i(x)C_i \subseteq \mathcal{B}_i$ for all i and $|\mathcal{C}| = |C| = |C_1 \times \cdots \times C_r| = \prod_{i=1}^{r} |C_i|$. □

Then we investigate properties of ideals in the ring $\mathcal{R}_i = \frac{\mathbb{Z}_4[x]}{\langle f_i(x^4)\rangle}$.

Proposition 5.2 *For any integer i, $1 \le i \le r$, let $C_i = \langle f_i(x)^l + 2v(x), 2\bar{f}_i(x)^s\rangle$ be an ideal of $\mathcal{R}_i$, where $v(x) \in \overline{\mathcal{R}}_i$ and $0 \le s \le l \le 4$, and set $\mathcal{C}_i = \varepsilon_i(x)C_i \subseteq \mathcal{B}$. Then we have the following conclusions*:

(i) *The set $\mathcal{C}_i$ is a cyclic code of type $4^{(4-l)m_i}2^{(l-s)m_i}$ over $\mathbb{Z}_4$ with length $4n$.*

(ii) *Using the notation in Eq. (8), let $G = \begin{pmatrix} G_{i,(1)} \\ G_{i,(2)} \end{pmatrix}$, where*

$$G_{i,(1)} = \left[\left(f_i(x)^l + 2v(x)\right)\varepsilon_i(x)\right]_{(4-l)m_i,4n},\quad G_{i,(2)} = \left[2\bar{f}_i(x)\varepsilon_i(x)\right]_{(l-s)m_i,4n}.$$

Then $\mathcal{C}_i = \left\{(\underline{a}, \underline{b})G_i \mid \underline{a} \in \mathbb{Z}_4^{(4-l)m_i}, \underline{b} \in \mathbb{F}_2^{(l-s)m_i}\right\}$.

Proof (i) For any vectors $\underline{a} = (a_0, a_1, \ldots, a_{(4-l)m_i-1}) \in \mathbb{Z}_4^{(4-l)m_i}$ and $\underline{b} = (b_0, b_1, \ldots, b_{(l-s)m_i-1}) \in \mathbb{F}_2^{(l-s)m_i}$, define a map ϱ by

$$\varrho(\underline{a}, \underline{b}) = \sum_{0 \le j \le (4-l)m_i-1} a_j x^j \left(f_i(x)^l + 2v(x)\right) + \sum_{0 \le t \le (l-s)m_i-1} 2b_t x^t \bar{f}_i(x)^s$$

(mod $f_i(x^4)$). Now, we claim that ϱ is a bijection from $\mathbb{Z}_4^{(4-l)m_i} \times \mathbb{F}_2^{(l-s)m_i}$ onto C_i. In fact, since C_i is an ideal of $\mathcal{R}_i$ generated by $f_i(x)^l + 2v(x)$ and $2\bar{f}_i(x)^s$, we see that $\varrho(\underline{a}, \underline{b}) \in C_i$. By Lemma 2.4, it follows that

$$|C_i| = 2^{m_i(8-(l+s))} = 2^{2(4-l)m_i+(l-s)m_i} = |\mathbb{Z}_4^{(4-l)m_i} \times \mathbb{F}_2^{(l-s)m_i}|.$$

Hence we only need to prove that the map ϱ is injective.

In fact, let $\underline{c} = (c_0, c_1, c_2, \ldots, c_{(4-l)m_i-1}) \in \mathbb{Z}_4^{(4-l)m_i}$ and $\underline{d} = (d_0, d_1, \ldots, d_{(l-s)m_i-1}) \in \mathbb{F}_2^{(l-s)m_i}$ satisfying $\varrho(\underline{a}, \underline{b}) = \varrho(\underline{c}, \underline{d})$ (mod $f_i(x^4)$). For each integer j, $0 \le j \le (4-l)m_i - 1$, we write: $a_j = a_{0,j} + 2a_{1,j}$ and $c_j = c_{0,j} + 2c_{1,j}$, where $a_{0,j}, a_{1,j}, c_{0,j}, c_{1,j} \in \mathbb{F}_2$. Then by $\varrho(\underline{a}, \underline{b}) = \varrho(\underline{c}, \underline{d})$ (mod $f_i(x^4)$), we have that $\varrho(\underline{a}, \underline{b})$ (mod $\langle \bar{f}_i(x)^4, 2\rangle) = \varrho(\underline{c}, \underline{d})$ (mod $\langle \bar{f}_i(x)^4, 2\rangle$). This implies

$$\left(\sum_{0 \le j \le (4-l)m_i-1} a_{0,j}x^j\right)\bar{f}_i(x)^l = \left(\sum_{0 \le j \le (4-l)m_i-1} c_{0,j}x^j\right)\bar{f}_i(x)^l \text{ (mod } \bar{f}_i(x)^4).$$

Since both $\sum_{0 \le j \le (4-l)m_i-1} a_{0,j}x^j$ and $\sum_{0 \le j \le (4-l)m_i-1} c_{0,j}x^j$ are polynomials in $\mathbb{F}_2[x]$ of degree $\le (4-l)m_i - 1 < (4-l)\deg(\bar{f}_i(x))$, From the equation above, we can deduce

$\sum_{0\le j\le(4-l)m_i-1} a_{0,j}x^j = \sum_{0\le j\le(4-l)m_i-1} c_{0,j}x^j$ in $\mathbb{F}_2[x]$, by Lemma 2.2 (ii). This implies $a_{0,j} = c_{0,j}$, $\forall j = 0, 1, \ldots, (4-l)m_i - 1$.

Moreover, by $\varrho(\underline{a}, \underline{b}) = \varrho(\underline{c}, \underline{d})$ (mod $f_i(x^4)$) and $2(f_i(x)^l + 2v(x)) = 2\bar{f}_i(x)^l$, we obtain

$$\begin{aligned}
&2\left(\left(\sum_{0\le j\le(4-l)m_i-1} a_{1,j}x^j\right)\left(\bar{f}_i(x)\right)^l + \left(\sum_{0\le t\le(l-s)m_i-1} b_t x^t\right)\left(\bar{f}_i(x)\right)^s\right)\\
=&2\left(\left(\sum_{0\le j\le(4-l)m_i-1} c_{1,j}x^j\right)\left(\bar{f}_i(x)\right)^l + \left(\sum_{0\le t\le(l-s)m_i-1} d_t x^t\right)\left(\bar{f}_i(x)\right)^s\right).
\end{aligned}$$

Since $\sum_{0\le j\le(4-l)m_i-1} a_{1,j}x^j$ and $\sum_{0\le j\le(4-l)m_i-1} c_{1,j}x^j$ are polynomials in $\mathbb{F}_2[x]$ of degree $\le (4-l)m_i - 1 < (4-l)\deg(f_i(x))$, $\sum_{0\le t\le(l-s)m_i-1} b_t x^t$ and $\sum_{0\le t\le(l-s)m_i-1} d_t x^t$ are polynomials in $\mathbb{F}_2[x]$ of degree $\le (l-s)m_i - 1 < (l-s)\deg(f_i(x))$, we see that $\sum_{0\le j\le(4-l)m_i-1} a_{1,j}x^j = \sum_{0\le j\le(4-l)m_i-1} c_{1,j}x^j$ and $\sum_{0\le t\le(l-s)m_i-1} b_t x^t = \sum_{0\le t\le(l-s)m_i-1} d_t x^t$ in $\mathbb{F}_2[x]$. This implies

$$a_{1,j} = c_{1,j},\ 0 \le j \le (4-l)m_i - 1;\ \text{and}\ \ b_t = d_t,\ 0 \le t \le (l-s)m_i - 1.$$

Summing up the results above, we get the following: $\underline{a} = \underline{c}$ and $\underline{b} = \underline{d}$. Therefore, ϱ is injective and hence a bijection. Moreover, it is clear that

$$\varrho((\underline{a}, \underline{b}) + (\underline{c}, \underline{d})) = \varrho((\underline{a} + \underline{c}, \underline{b} + \underline{d}) = \varrho(\underline{a}, \underline{b}) + \varrho(\underline{c}, \underline{d}).$$

Hence ϱ is additive group isomorphism from $(\mathbb{Z}_4^{(4-l)m_i}, +) \times (\mathbb{F}_2^{(l-s)m_i}, +)$ onto $(C_i, +)$. So C_i is an abelian group of type $4^{(4-l)m_i}2^{(l-s)m_i}$.

By Lemma 5.1, $\mathcal{C}_i = \varepsilon_i(x)C_i$ is a cyclic code over $\mathbb{Z}_4$ of length $4n$. Using Lemma 2.1 (iii), the map ψ_i induces an additive group isomorphism from $(C_i, +)$ onto $(\mathcal{C}_i, +)$. Hence, $\mathcal{C}_i$ is an abelian group of type $4^{(4-l)m_i}2^{(l-s)m_i}$.

(ii) For any positive integer k, denote $X_k = (1, x, \ldots, x^{k-1})^{\mathrm{tr}}$ where M^{tr} represents the transpose of a matrix M. Using the notation of Eq. (8), by the proof of (i), each codeword in $\mathcal{C}_i$ can be uniquely expessed as

$$\begin{aligned}
\varepsilon_i(x)\varrho(\underline{a}, \underline{b}) =& \left(\underline{a}X_{(4-l)m_i}\right)\left(f_i(x)^l + 2v(x)\right) + (\underline{b}X_{(l-s)m_i})\bar{f}_i(x)^s\\
=& \underline{a}\left(X_{(4-l)m_i}f_i(x)^l + 2v(x)\right) + \underline{b}(X_{(l-s)m_i}\bar{f}_i(x)^s)\\
=& \underline{a}G_{i,(1)} + \underline{b}G_{i,(2)},
\end{aligned}$$

i.e., $\varepsilon_i(x)\varrho(\underline{a}, \underline{b}) = (\underline{a}, \underline{b})G_i$, where $\underline{a} \in \mathbb{Z}_4^{(4-l)m_i}$ and $\underline{b} \in \mathbb{F}_2^{(l-s)m_i}$.

Therefore, $\mathcal{C}_i = \{(\underline{a}, \underline{b})G_i \mid \underline{a} \in \mathbb{Z}_4^{(4-l)m_i}, \underline{b} \in \mathbb{F}_2^{(l-s)m_i}\}$. □

A. Proof for Theorem 3.1.

By Proposition 5.2, the ideal C_i of $\mathcal{R}_i$ listed in the table of Theorem 3.1 is of the type as given by the table, for all Cases 1–10. Further, as ideals in distinct cases are of different types, any two ideals are distinct in different cases. Obviously, the 7 ideals in Cases 3 and 4 are distinct, as they are of different types. Then we need to consider ideals C_i of $\mathcal{R}_i$ in Cases 5–10.

Case 5. Let $h(x), q(x) \in \mathcal{T}_i = \{\sum_{j=0}^{m_i-1} t_j x^j \mid t_j \in \{0,1\}, j = 0,1,\ldots,m_i-1\}$ be such that $\langle f_i(x) + 2h(x)\rangle = \langle f_i(x) + 2q(x)\rangle$ as ideals of the ring $\mathcal{R}_i$. Then by Lemma 2.4 (iii) and Equation (4), we have $h(x) \equiv q(x) \pmod{\bar{f}_i(x)}$ in $\mathbb{F}_2[x]$. This implies $h(x) = q(x)$. Therefore, the ideals C_i in Case 5 are distinct.

Case 6. Let $h(x), q(x) \in \mathcal{T}_i$ be such that $\langle f_i(x)^2 + 2h(x), 2\bar{f}_i(x)\rangle = \langle f_i(x)^2 + 2q(x), 2\bar{f}_i(x)\rangle$. Then by Eq. (4) in Lemma 2.4, we have that $h(x) \equiv q(x) \pmod{\bar{f}_i(x)}$ in $\mathbb{F}_2[x]$. This implies $h(x) = q(x)$.

Similarly, one can easily verify that the ideals C_i in **Case 8** are distinct.

Case 7. Let $h_0(x), h_1(x), q_0(x), q_1(x) \in \mathcal{T}_i$ be such that $\langle f_i(x)^2 + 2(h_0(x) + h_1(x)\bar{f}_i(x))\rangle = \langle f_i(x)^2 + 2(q_0(x) + q_1(x)\bar{f}_i(x))\rangle$ as ideals of $\mathcal{R}_i$. By Lemma 2.4 (iii) and Eq. (4), we have $h_0(x) + h_1(x)\bar{f}_i(x) \equiv q_0(x) + q_1(x)\bar{f}_i(x) \pmod{\bar{f}_i(x)^2}$ in $\mathbb{F}_2[x]$. This implies $h_0(x) = q_0(x)$ and $h_1(x) = q_1(x)$. Therefore, the ideals C_i in Case 7 are distinct.

Case 9. Let $h(x), q(x) \in \mathcal{T}_i$ be such that $\langle f_i(x)^3 + 2h(x)\bar{f}_i(x), 2\bar{f}_i(x)^2\rangle = \langle f_i(x) + 2q(x)\bar{f}_i(x), 2\bar{f}_i(x)^2\rangle$ as ideals of $\mathcal{R}_i$. By Lemma 2.4 (iii) and Eq. (4), we have $h(x)\bar{f}_i(x) \equiv q(x)\bar{f}_i(x) \pmod{\bar{f}_i(x)^2}$ in $\mathbb{F}_2[x]$. This implies that $h(x) = q(x)$. Therefore, the ideals C_i in Case 9 are distinct.

Case 10. Let $h(x), q(x) \in \mathcal{T}_i$ be such that $\langle f_i(x)^3 + 2\bar{f}_i(x) \cdot (w_{i,0}(x) + h(x)\bar{f}_i(x))\rangle = \langle f_i(x)^3 + 2\bar{f}_i(x) \cdot (w_{i,0}(x) + q(x)\bar{f}_i(x))\rangle$. By Lemma 2.4 (iii) and Eq. (4), we have $\bar{f}_i(x) \cdot (w_{i,0}(x) + h(x)\bar{f}_i(x)) \equiv \bar{f}_i(x) \cdot (w_{i,0}(x) + q(x)\bar{f}_i(x)) \pmod{\bar{f}_i(x)^3}$ in $\mathbb{F}_2[x]$. This implies $w_{i,0}(x) + h(x)\bar{f}_i(x)) \equiv w_{i,0}(x) + q(x)\bar{f}_i(x) \pmod{\bar{f}_i(x)^2}$, and hence $h(x) = q(x)$. So, the ideals C_i in Case 10 are distinct.

As stated above, we conclude that all ideals of $\mathcal{R}_i$ in Cases 1–10 are distinct. Now, let $\mathcal{L}_i$ be the number of all ideals in $\mathcal{R}_i$. Then we have

$$\mathcal{L}_i \geq 9 + 5 \cdot 2^{m_i} + (2^{m_i})^2, \quad i = 1, 2, \ldots, r.$$

Further, by Proposition 5.1 the number of cyclic ideals over $\mathbb{Z}_4$ of length $4n$ is equal to $\prod_{i=1}^{r} \mathcal{L}_i \geq \prod_{i=1}^{r}(9 + 5 \cdot 2^{m_i} + (2^{m_i})^2)$. On the other hand, by [11, Corollary 3.4], we know that the number of cyclic ideals over $\mathbb{Z}_4$ of length $4n$ equals $\prod_{i=1}^{r}(9 + 5 \cdot 2^{m_i} + (2^{m_i})^2)$. From these, we deduce that

$$\mathcal{L}_i = 9 + 5 \cdot 2^{m_i} + (2^{m_i})^2, \quad i = 1, 2, \ldots, r.$$

Therefore, all distinct ideals of $\mathcal{R}_i$ have been listed by the table in Theorem 3.1. The other conclusions follow from Proposition 5.1 immediately.

B. Proof for Theorem 3.2.

The result follows directly from Theorem 3.1 and Proposition 5.2.

C. Proof for Theorem 3.3

As usual, for any $\underline{a} = (a_0, a_1, \ldots, a_{4n-1}) \in \mathbb{Z}_4^{4n}$, we identify $\underline{a}$ with $a(x) = \sum_{j=0}^{4n-1} a_j x^j \in \mathcal{B} = \mathbb{Z}_4[x]/\langle x^{4n} - 1\rangle$ in the following. In the ring $\mathcal{B}$, we have that $x^{4n} = 1$, and hence $x^{-1} = x^{4n-1}$. Moreover, we have $x^{4n} \equiv 1 \pmod{f_i(x^4)}$, since $f_i(x^4)$ is a divisor of $x^{4n} - 1$ in $\mathbb{Z}_4[x]$. This implies $x^{4n} = 1$ and $x^{-1} = x^{4n-1}$ in the ring $\mathcal{R}_i = \mathbb{Z}_4[x]/\langle f_i(x^4)\rangle$ for all i. Define

$$\mu(a(x)) = a(x^{-1}) = a_0 + \sum_{1\le j\le 4n-1} a_j x^{4n-j}, \quad \forall a(x) \in \mathcal{B}.$$

It is clear that μ is a ring automorphism of $\mathcal{B}$ and satisfies $\mu^{-1} = \mu$. Then, by a direct calculation, we get the following lemma.

Lemma 5.3 *Let* $\underline{a}, \underline{b} \in \mathbb{Z}_4^{4n}$ *where* $\underline{b} = (b_0, b_1, \ldots, b_{4n-1})$. *Then* $[\underline{a}, \underline{b}] = 0$ *if* $a(x)\mu(b(x)) = 0$ *in the ring* $\mathcal{B}$ *where* $b(x) = \sum_{j=0}^{4n-1} b_j x^j$.

In Theorem 3.4, we define by μ the permutation on the set $\{1, \ldots, r\}$:

$$\mu(i) = i, \text{ if } 1 \le i \le \lambda;\ \mu(\lambda + j) = \lambda + j + \epsilon \text{ and } \mu(\lambda + j + \epsilon) = \lambda + j,\ \forall j = 1, \ldots, \epsilon.$$

Whether μ denotes the automorphism of $\mathcal{B}$ or this map on the set $\{1, \ldots, r\}$ is determined by the context. By a method paralleling to that above [6, Lemma 7] and its proof, we can prove the following lemma. Here we omit its proof.

Lemma 5.4 *Using the notations in Sect. 2, we have the following*:

(i) *For each integer* $i, 1 \le i \le r$, *there is a unique element* $c_i \in \mathbb{Z}_4^\times = \{1, -1\}$ *such that* $\widetilde{f_i}(x) = c_i f_{\mu(i)}(x)$.
(ii) *For any integer* $i, 1 \le i \le r$, *we have that* $\mu(\varepsilon_i(x)) = \varepsilon_i(x^{-1}) = \varepsilon_{\mu(i)}(x)$ *in the ring* $\mathcal{B}$ *and* $\mu(\mathcal{B}_i) = \mathcal{B}_{\mu(i)}$.
(iii) *Let* $\mu|_{\mathcal{B}_i} : \mathcal{B}_i \to \mathcal{B}_{\mu(i)}$ *be the restriction of* μ *on* $\mathcal{B}_i$, *and define*

$$\mu_i(c(x)) = c(x^{-1}) = c(x^{4n-1}) \left(\mathrm{mod}\, f_{\mu(i)}(x^4)\right),\ \forall c(x) \in \mathcal{R}_i.$$

Using the notation in Lemma 2.1 (iii), we have the following commutative diagram of ring isomorphisms:

$$\begin{array}{ccc} \mathcal{R}_i = \mathbb{Z}_4[x]/\langle f_i(x^4)\rangle & \xrightarrow{\psi_{\mu(i)}^{-1}(\mu|_{\mathcal{B}_i})\psi_i} & \mathcal{R}_{\mu(i)} = \mathbb{Z}_4[x]/\langle f_{\mu(i)}(x^4)\rangle \\ \psi_i \downarrow & & \downarrow \psi_{\mu(i)} \\ \mathcal{B}_i = \varepsilon_i(x)\mathcal{R}_i & \xrightarrow{\mu|_{\mathcal{B}_i}} & \mathcal{B}_{\mu(i)} = \varepsilon_{\mu(i)}(x)\mathcal{R}_i \end{array}$$

Let $\mu_i = \psi_{\mu(i)}^{-1}(\mu|_{\mathcal{B}_i})\psi_i$. *Then* μ_i *is a ring isomorphism from* $\mathcal{R}_i$ *onto* $\mathcal{R}_{\mu(i)}$. *Moreover, we have* $\mu_i^{-1} = \mu_{\mu(i)}$ where $\mu_{\mu(i)} : \mathcal{R}_{\mu(i)} \to \mathcal{R}_i$ *is defined by* $\mu_{\mu(i)}(a(x)) = a(x^{-1}) = a(x^{4n-1}) \,(\mathrm{mod}\, f_i(x^4))$ *for all* $a(x) \in \mathcal{K}_{\mu(i)}$.

For any ideal C_i of the ring $\mathcal{R}_i = \mathbb{Z}_4[x]/\langle f_i(x^4)\rangle$, recall that the *annihilator* of C_i is defined as the ideal $\mathrm{Ann}(C_i) = \{\alpha \in \mathcal{R}_i \mid \alpha\beta = 0, \forall \beta \in C_i\}$ of $\mathcal{R}_i$. The annihilator of each ideal in $\mathcal{R}_i$ is given by the following proposition.

Proposition 5.5 *Using the notation in Sect. 2 and Theorem 3.1, for any integer i, $1 \le i \le r$, the annihilator* $\mathrm{Ann}(C_i)$ *of each ideal C_i in $\mathcal{R}_i$ is given by the following table:*

C_i in Theorem 3.1	$\mathrm{Ann}(C_i)$
Case 1	$\langle 1\rangle$
Case 2	$\langle 0\rangle$
Case 3	$\langle f_i(x)^{4-s}, 2\rangle$
Case 4	$\langle 2\bar{f}_i(x)^{4-l}\rangle$
Case 5	$\left\langle f_i(x)^3 + 2\bar{f}_i(x)\cdot\left(w_{i,0}(x) + (w_{i,1}(x) + h(x))\bar{f}_i(x)\right)\right\rangle$
Case 6	$\langle f_i(x)^3 + 2\bar{f}_i(x)\cdot(w_{i,0}(x) + h(x)), 2\bar{f}_i(x)^2\rangle$
Case 7	$\left\langle f_i(x)^2 + 2\left(w_i(x)^2 + h_0(x) + h_1(x)\bar{f}_i(x)\right)\right\rangle$
Case 8	$\langle f_i(x)^3 + 2h(x), 2\bar{f}_i(x)\rangle$
Case 9	$\langle f_i(x)^2 + 2(w_{i,0}(x) + h(x)), 2\bar{f}_i(x)\rangle$
Case 10	$\langle f_i(x) + 2(w_{i,1}(x) + h(x))\rangle$

where $0 \le s \le 3, 1 \le l \le 3$, and $h(x), h_0(x), h_1(x) \in \mathcal{T}_i$.

Proof Let $\mathcal{S}_i$ be the set of all ideals in $\mathcal{R}_i$ listed in the table of Theorem 3.1, and assume $C_i \in \mathcal{S}_i$. It is clear that $\mathrm{Ann}(C_i) = D$, where $D \in \mathcal{S}_i$ satisfying the following conditions:

$$C_i \cdot D = \{0\} \text{ and } |D| = \mathrm{Max}\{|J| \mid C_i \cdot J = \{0\},\ J \in \mathcal{S}_i\}. \tag{9}$$

By the table in Theorem 3.1, there are 10 cases for all distinct ideals of $\mathcal{R}_i$. Hence we have the following four situations:

(i) Let C_i be given by Case 7 in the table of Theorem 3.1. Then $|C_i| = 2^{4m_i}$. We set $D = \langle f_i(x)^2 + 2(w_i(x)^2 + h_0(x) + h_1(x)\bar{f}_i(x))\rangle$. By Theorem 3.1, we see that D is an ideal of $\mathcal{R}_i$ and $|D| = 2^{4m_i}$. Now, denote

$\alpha = f_i(x)^2 + 2(h_0(x) + h_1(x)\bar{f}_i(x))$,

$\beta = f_i(x)^2 + 2(w_i(x)^2 + h_0(x) + h_1(x)\bar{f}_i(x))$.

Then $C_i = \{\xi\alpha \mid \xi \in \mathcal{R}_i\}$ and $D = \{\eta\beta \mid \eta \in \mathcal{R}_i\}$. By Theorem 2.5 (ii), we have $f_i(x)^4 = 2\bar{f}_i(x)^2 w_i(x)^2 = 2f_i(x)^2 w_i(x)^2$ in $\mathcal{R}_i$. This implies that $\alpha\beta = f_i(x)^4 + 2f_i(x)^2\cdot(h_0(x) + h_1(x)\bar{f}_i(x) + w_i(x)^2 + h_0(x) + h_1(x)\bar{f}_i(x)) = 0$, and hence $C_i \cdot D = \{\xi\alpha\cdot\eta\beta \mid \xi, \eta \in \mathcal{R}_i\} = \{0\}$. Then by Condition (9), we conclude that $D = \mathrm{Ann}(C_i)$.

(ii) Let $C_i = \langle f_i(x)^3 + 2\bar{f}_i(x)h(x), 2\bar{f}_i(x)^2\rangle$ be given by Case 9 in the table of Theorem 3.1. Then $|C_i| = 2^{3m_i}$. We set $D = \langle f_i(x)^2 + 2(w_{i,0}(x) + h(x)), 2\bar{f}_i(x)\rangle$. Then by Theorem 3.1, D is an ideal of $\mathcal{R}_i$ and $|D| = 2^{5m_i}$. As $f_i(x)^4 = 0$ in $\mathcal{R}_i$, we have $2\bar{f}_i(x)^2\cdot f_i(x)^2 = f_i(x)^3\cdot 2\bar{f}_i(x) = 2\bar{f}_i(x)^4 = 0$. This implies

$$2\bar{f}_i(x)^2\cdot(f_i(x)^2 + 2(w_{i,0}(x) + h(x))) = (f_i(x)^3 + 2\bar{f}_i(x)h(x))\cdot 2\bar{f}_i(x) = 0.$$

Since $f_i(x)^4 = 2\bar{f}_i(x)^2 w_i(x)^2 = 2\bar{f}_i(x)^2(w_{i,0}(x) + w_{i,1}(x)\bar{f}_i(x))$ by Theorem 2.5 (ii), it follows that

$$\begin{aligned}&\left(f_i(x)^3+2\overline{f}_i(x)h(x)\right)\cdot\left(f_i(x)^2+2(w_{i,0}(x)+h(x))\right)\\&=f_i(x)^5+2\overline{f}_i(x)^3(w_{i,0}(x)+2h(x))\\&=2\overline{f}_i(x)^3(w_{i,0}(x)+w_{i,1}(x)\overline{f}_i(x))+2\overline{f}_i(x)^3w_{i,0}(x)\\&=0.\end{aligned}$$

This implies $C_i\cdot D=\{0\}$. Then by Condition (9), we have $D=\mathrm{Ann}(C_i)$.

(iii) Let $C_i=\langle f_i(x)^3+2\overline{f}_i(x)(w_{i,0}(x)+h(x)\overline{f}_i(x))\rangle$ be given by Case 10 in the table of Theorem 3.1. Then $|C_i|=2^{2m_i}$. Set $D=\langle f_i(x)+2(w_{i,1}(x)+h(x))\rangle$. By Theorem 3.1, we see that D is an ideal of $\mathcal{R}_i$ and $|D|=2^{6m_i}$.

By Theorem 2.5 (ii), it follows that

$$\begin{aligned}&\left(f_i(x)^3+2\overline{f}_i(x)(w_{i,0}(x)+h(x)\overline{f}_i(x))\right)\cdot\left(f_i(x)+2(w_{i,1}(x)+h(x))\right)\\&=f_i(x)^4+2\overline{f}_i(x)^3(w_{i,1}(x)+h(x))+2\overline{f}_i(x)^2(w_{i,0}(x)+h(x)\overline{f}_i(x))\\&=2\overline{f}_i(x)^2(w_{i,0}(x)+w_{i,1}(x)\overline{f}_i(x))+2\overline{f}_i(x)^3w_{i,1}(x)+2\overline{f}_i(x)^2w_{i,0}(x)\\&=0.\end{aligned}$$

This implies $C_i\cdot D=\{0\}$. Then by Condition (9), we have $D=\mathrm{Ann}(C_i)$.

(iv) If C_i is an ideal of $\mathcal{R}_i$ given by Cases 1–6 and Case 8 in the table of Theorem 3.1, the conclusions for each $\mathrm{Ann}(C_i)$ follow from Theorem 2.5 and direct calculations. Here, we omit these elementary calculations. □

Lemma 5.6 *Let* $a(x)=\sum_{i=1}^r\varepsilon_i(x)\xi_i, b(x)=\sum_{i=1}^r\varepsilon_i(x)\eta_i\in\mathcal{B}$, *where* $\xi_i,\eta_i\in\mathcal{R}_i$. *Then* $a(x)\mu(b(x))=\sum_{i=1}^r\varepsilon_i(x)(\xi_i\cdot\mu_i^{-1}(\eta_{\mu(i)}))$.

Proof By Lemma 5.4 (ii), we have $\mu_i^{-1}(\eta_{\mu(i)})\in\mu_i^{-1}(\mathcal{R}_{\mu(i)})=\mathcal{R}_i$. This implies $\xi_i\cdot\mu_i^{-1}(\eta_{\mu(i)})\in\mathcal{R}_i$ for all i. If $j\neq\mu(i)$, then $i\neq\mu(j)$ and so $\varepsilon_i(x)\varepsilon_{\mu(j)}(x)=0$ in the ring $\mathcal{B}$, by Lemma 2.1 (i). Therefore, by Lemma 5.4 (iii) it follows that

$$\begin{aligned}a(x)\mu(b(x))&=\sum_{i,j=1}^r\varepsilon_i(x)\xi_i\cdot\mu(\varepsilon_j(x)\eta_j)=\sum_{i,j=1}^r\varepsilon_i(x)\xi_i\cdot\mu(\varepsilon_j(x))\mu_j(\eta_j)\\&=\sum_{i,j=1}^r\varepsilon_i(x)\xi_i\cdot\varepsilon_{\mu(j)}(x)\mu_j(\eta_j)=\sum_{i=1}^r\varepsilon_i(x)\xi_i\cdot\varepsilon_i(x)\mu_{\mu(i)}(\eta_{\mu(i)}).\end{aligned}$$

Hence $a(x)\mu(b(x))=\sum_{i=1}^r\varepsilon_i(x)(\xi_i\cdot\mu_i^{-1}(\eta_{\mu(i)}))$ by Lemma 2.1 (i). □

Now, we prove Theorem 3.3 as follows:

Let $\mathcal{C}=\bigoplus_{i=1}^r\varepsilon_i(x)C_i$ be a cyclic code over $\mathbb{Z}_4$ of length $4n$, where C_i is an ideal of the ring $\mathcal{R}_i$ given by Theorem 3.1. For each integer $1\le j\le r$, define

$$H_j=\mu_{\mu(j)}(\mathrm{Ann}(C_{\mu(j)}))=\mu_j^{-1}(\mathrm{Ann}(C_{\mu(j)})),$$

where $\mathrm{Ann}(C_{\mu(j)})$ is the annihilator of $C_{\mu(j)}$ determine by Proposition 5.5, for all $j=1,\ldots,r$. Then by Lemma 5.4 (iii), we have $\mu_{\mu(j)}^{-1}(H_j)=\mu_j(H_j)=\mathrm{Ann}(C_{\mu(j)})$.

Assume $i = \mu(j)$. Then we have $\mu(i) = j$ and $\mu_i^{-1}(H_{\mu(i)}) = \mathrm{Ann}(C_i)$. Now, let $\mathcal{H} = \bigoplus_{i=1}^{r} \varepsilon_{\mu(i)}(x) H_{\mu(i)} = \sum_{j=1}^{r} \varepsilon_j(x) H_j \pmod{x^{4n} - 1}$.

By Proposition 5.1, we know that $\mathcal{H}$ is a cyclic code over $\mathbb{Z}_4$ of length $4n$. As $C_i \cdot \mathrm{Ann}(C_i) = \{0\}$, by Lemma 5.6 it follows that

$$\mathcal{C} \cdot \mu(\mathcal{H}) = \sum_{i=1}^{r} \varepsilon_i(x)\big(C_i \cdot \mu_i^{-1}(H_{\mu(i)})\big) = \sum_{i=1}^{r} \varepsilon_i(x)\big(C_i \cdot \mathrm{Ann}(C_i)\big) = \{0\}.$$

From this and by Lemma 5.3, we deduce that $\mathcal{H} \subseteq \mathcal{C}^{\perp}$. Further, by Theorem 3.1 and Proposition 5.5, we have $|C_i||\mathrm{Ann}(C_i)| = 2^{8m_i}$ for all i. This implies

$$|\mathcal{C}||\mathcal{H}| = \Big(\prod_{i=1}^{r} |C_i|\Big)\Big(\prod_{i=1}^{r} |H_{\mu(i)}|\Big) = \prod_{i=1}^{r} \big(|C_i||\mathrm{Ann}(C_i)|\big) = 2^{8\sum_{i=1}^{r} m_i} = |\mathbb{Z}_4|^{4n},$$

by Proposition 5.1 and $\sum_{i=1}^{r} m_i = n$. Then from the theory of linear codes over $\mathbb{Z}_4$ (cf. [23]), we deduce that $\mathcal{C}^{\perp} = \mathcal{H}$.

To prove Theorem 3.3, it is sufficient to prove $H_{\mu(i)} = D_{\mu(i)}$, where $D_{\mu(i)}$ is an ideal of the ring $\mathcal{R}_{\mu(i)}$ listed in the table of Theorem 3.3, $1 \le i \le r$.

Since $x^{-1} = x^{4n-1}$ in $\mathcal{R}_i$, we have $x \in \mathcal{R}_i^{\times}$, for all i. By Lemma 5.4 (i), we know that $\widetilde{f_i}(x) = c_i f_{\mu(i)}(x)$ where $c_i \in \{1, -1\}$. This implies $2c_i = 2$ in $\mathbb{Z}_4$. Then by the definition of μ_i in Lemma 5.4 (iii), for $k = 1, 2, 3$, we have

$$\begin{aligned}\mu_i(f_i(x)^k) =& (\mu_i(f_i(x)))^k = f_i(x^{-1})^k = x^{-km_i}(x^{m_i} f_i(x^{-1}))^k \\ =& x^{-km_i}(\widetilde{f_i}(x))^k = c_i^k x^{-km_i} f_{\mu(i)}(x)^k,\end{aligned}$$

and so $\mu_i(2\overline{f}_i(x)^k) = \mu_i(2f_i(x)^k) = 2c_i^k x^{-km_i} f_{\mu(i)}(x)^k = 2x^{-km_i}\overline{f}_{\mu(i)}(x)^k$.

(i) Let $\mathrm{Ann}(C_i) = \langle f_i(x)^{4-s}, 2\rangle$ be given in Case 3 of Proposition 5.5. By $x \in \mathcal{R}_{\mu(i)}^{\times}$, it follows that

$$\begin{aligned}H_{\mu(i)} =& \langle \mu_i(f_i(x)^{4-s}), \mu_i(2)\rangle = \langle c_i^{4-s} x^{-(4-s)m_i} f_{\mu(i)}(x)^{4-s}, 2\rangle \\ =& \langle f_{\mu(i)}(x)^{4-s}, 2\rangle = D_{\mu(i)}.\end{aligned}$$

The equations $H_{\mu(i)} = D_{\mu(i)}$ for Cases 1, 2, 4 can be proved similarly as Case 3.

(ii) Let $\mathrm{Ann}(C_i) = \langle f_i(x)^3 + 2\overline{f}_i(x)(w_{i,0}(x) + \vartheta_i(x)\overline{f}_i(x))\rangle$ be given in Case 5 of Proposition 5.5, where $\vartheta_i(x) = w_{i,1}(x) + h(x)$. Then we have

$$\begin{aligned}H_{\mu(i)} =& \Big\langle \mu_i\Big(f_i(x)^3 + 2\overline{f}_i(x)(w_{i,0}(x) + \vartheta_i(x)\overline{f}_i(x))\Big)\Big\rangle \\ =& \langle c_i^3 x^{-3m_i} f_{\mu(i)}(x)^3 \\ &+ 2x^{-m_i}\overline{f}_{\mu(i)}(x) \cdot (w_{i,0}(x^{-1}) + \vartheta_i(x^{-1})x^{-m_i}\overline{f}_{\mu(i)}(x))\rangle \\ =& \Big\langle f_{\mu(i)}(x)^3 + 2\overline{f}_{\mu(i)}(x)\Big(x^{2m_i} w_{i,0}(x^{-1}) + \widehat{\vartheta}_i(x)\overline{f}_{\mu(i)}(x)\Big)\Big\rangle,\end{aligned}$$

where $\widehat{\vartheta}_i(x) = x^{m_i}(w_{i,1}(x^{-1}) + h(x^{-1})) \in \overline{\mathcal{R}}_{\mu(i)}$. Hence $H_{\mu(i)} = D_{\mu(i)}$.

The equation $H_{\mu(i)} = D_{\mu(i)}$ for Case 10 can be proved similarly as Case 5.

(iii) Let $\mathrm{Ann}(C_i) = \langle f_i(x)^3 + 2\overline{f}_i(x)t_i(x), 2\overline{f}_i(x)^2\rangle$ be given in case 6 of Proposition 5.5, where $t_i(x) = w_{i,0}(x) + h(x)$. Then we have

$$\begin{aligned} H_{\mu(i)} =& \left\langle c_i^3 x^{-3m_i} f_{\mu(i)}(x)^3 + 2x^{-m_i}\overline{f}_{\mu(i)}(x)t_i(x^{-1}), 2x^{-2m_i}\overline{f}_{\mu(i)}(x)^2 \right\rangle \\ =& \langle f_{\mu(i)}(x)^3 + 2\overline{f}_{\mu(i)}(x)\widehat{t}_i(x), \overline{f}_{\mu(i)}(x)^2\rangle, \end{aligned}$$

where $\widehat{t}_i(x) = x^{2m_i}(w_{i,0}(x^{-1}) + h(x^{-1})) \in \overline{\mathcal{R}}_{\mu(i)}$. Hence $H_{\mu(i)} = D_{\mu(i)}$.

The equation $H_{\mu(i)} = D_{\mu(i)}$ for Case 9 can be proved similarly as Case 6.

(iv) Let $\mathrm{Ann}(C_i) = \langle f_i(x)^2 + 2(w_i(x)^2 + h_0(x) + h_1(x)\overline{f}_i(x))\rangle$ be given in Case 7 of Proposition 5.5, where $\delta_{i,j}(x) = w_{i,j}(x) + h_j(x)$ for $j = 0, 1$. Then

$$\begin{aligned} H_{\mu(i)} =& \langle c_i^2 x^{-2m_i} f_{\mu(i)}(x)^2 + 2(w_i(x^{-1})^2 + h_0(x^{-1}) + h_1(x^{-1})x^{-m_i}\overline{f}_{\mu(i)}(x))\rangle \\ =& \left\langle f_{\mu(i)}(x)^2 + 2\left(\widehat{\delta}_{i,0}(x) + \widehat{\delta}_{i,1}(x)\overline{f}_{\mu(i)}(x)\right)\right\rangle = D_{\mu(i)}, \end{aligned}$$

where $\widehat{\delta}_{i,0}(x) = x^{2m_i}(w_i(x^{-1})^2 + h_0(x^{-1}))$ and $\widehat{\delta}_{i,1}(x) = x^{m_i}h_1(x^{-1})$ in $\overline{\mathcal{R}}_{\mu(i)}$.

(v) Let $\mathrm{Ann}(C_i) = \langle f_i(x)^3 + 2h(x), 2\overline{f}_i(x)\rangle$ be given in Case 8 of Proposition 5.5. Then we have $H_{\mu(i)} = \langle c_i^3 x^{-3m_i} f_{\mu(i)}(x)^3 + 2h(x^{-1}), 2x^{-m_i}\overline{f}_{\mu(i)}(x)\rangle = \langle f_{\mu(i)}(x)^3 + 2x^{3m_i}h(x^{-1}), 2\overline{f}_{\mu(i)}(x)\rangle = D_{\mu(i)}$.

On the basis of the above discussion, we get $\mathcal{C}^\perp = \bigoplus_{i=1}^r \varepsilon_{\mu(i)}(x)D_{\mu(i)}$, where $D_{\mu(i)}$ is an ideal of $\mathcal{R}_{\mu(i)}$ given in the table of Theorem 3.3 for all $i = 1, \ldots, r$. This proves the theorem 3.3.

D. Proof for Theorem 3.4

Using the notation of Theorem 3.3, by Proposition 5.1, we see that $\mathcal{C}$ is self-dual if and only if the ideal C_i of $\mathcal{R}_i$ satisfies $C_i = D_i$ for all $i = 1, \ldots, r$, where the pair $(C_i, D_{\mu(i)})$ of ideals is listed in the table of Theorem 3.3. Then the latter condition is equivalent to that C_i satisfies the following conditions:

$\diamond$ Let $i = 1$. There are 3 ideals of $\mathcal{R}_1$ satisfies $C_1 = D_1 = D_{\mu(1)}$:

$C_1 = \langle 2\rangle$, $C_1 = \langle (x-1)^3, 2(x-1)\rangle$ and $C_1 = \langle (x-1)^3 + 2, 2(x-1)\rangle$.

$\diamond$ Let $2 \le i \le \lambda$. In this case, $\mu(i) = i$. Then by Theorems 3.1 and 3.3, we see that C_i is one of the following three subcases:

$\triangleright$ $C_i = \langle 2\rangle$.

$\triangleright$ $C_i = \langle f_i(x)^3 + 2h(x), 2\overline{f}_i(x)\rangle$, where $h(x) \in \mathcal{T}_i$ satisfying Eq. (5) in the proof of Theorem 2.7, i.e., $h(x) \in \mathcal{V}_i$ by Theorem 2.7 (i).

$\triangleright$ $C_i = \langle f_i(x)^2 + 2(h_0(x) + h_1(x)\overline{f}_i(x))\rangle$, where $h_0(x), h_1(x) \in \mathcal{T}_i$ satisfying Equation (7) in the proof of Theorem 2.7, i.e., $h_0(x) \in \mathcal{W}_i^{(0)}$ and $h_1(x) \in \mathcal{W}_{i,h_0(x)}^{(1)}$ by Theorem 2.7 (ii) and (iii).

By Theorem 2.7, there are $1 + 2^{\frac{m_i}{2}} + (2^{\frac{m_i}{2}})^2$ ideals C_i of $\mathcal{R}_i$ satisfies $C_i = D_i = D_{\mu(i)}$, for all $i = 2, \ldots, \lambda$.

$\diamond$ Let $i = \lambda + j$ where $1 \le j \le \epsilon$. Then $\mu(i) = i + \epsilon$ and $\mu(i + \epsilon) = i$. In this case, $C_t = D_t$ for all $t = \lambda + 1, \ldots, \lambda + 2\epsilon$ if and only if: C_i is any ideal of $\mathcal{R}_i$ listed in the table of Theorem 3.1 and $C_{i+\epsilon} = D_{\mu(i)}$, where $D_{\mu(i)} = D_{i+\epsilon}$ is given by the table in Theorem 3.3, for all $i = \lambda + j$ and $1 \le j \le \epsilon$.

As stated above, we see that the number of self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$ is $3 \cdot \prod_{2\le i\le\lambda}(1+2^{\frac{m_i}{2}}+2^{m_i}) \cdot \prod_{j=1}^{\epsilon}(9+5\cdot 2^{m_{\lambda+j}}+4^{m_{\lambda+j}})$.

6 Conclusions

We give an explicit representation and enumeration for all distinct cyclic codes over $\mathbb{Z}_4$ of length $4n$ where n is odd. Using this representation, we provide an efficient encoder for each code and determine its type explicitly. Then we give a precise description for the dual codes and listed explicitly all distinct self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$. Compared with the results in the literature, the results in this paper are more simple and practical for constructing self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$, for a given odd positive integer n.

Obtaining some bounds for the minimal distance such as BCH-like of a self-dual cyclic code over $\mathbb{Z}_4$ of length $4n$ by just looking at the representation of such codes are future topics of interest.

Acknowledgements This research is supported in part by the National Natural Science Foundation of China (Grant Nos. 11671235, 11801324, 61971243, 61571243), the Shandong Provincial Natural Science Foundation, China (Grant No. ZR2018BA007) and the Scientific Research Fund of Hubei Provincial Key Laboratory of Applied Mathematics (Hubei University) (Grant Nos. HBAM201906, HBAM201804), the Scientific Research Fund of Hunan Provincial Key Laboratory of Mathematical Modeling and Analysis in Engineering (No. 2018MMAEZD09) and the Nankai Zhide Foundation. Part of this work was done when Yonglin Cao was visiting Chern Institute of Mathematics, Nankai University, Tianjin, China. He would like to thank the institution for the kind hospitality.

References

1. Abualrub, T., Oehmke, R.: On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e. IEEE Trans. Inform. Theory **49**, 2126–2133 (2003)
2. Blackford, T.: Cyclic codes over $\mathbb{Z}_4$ of oddly even length. Discrete Appl. Math. **128**, 27–46 (2003)
3. Calderbank, A.R., Sloane, N.J.A.: Modular and p-adic cyclic codes. Des. Codes Cryptogr. **6**, 21–35 (1995)
4. Calderbank, A.R., Sloane, N.J.A.: Double circulant codes over $\mathbb{Z}_4$ and even unimodular lattices. J. Algebraic Combin. **6**, 119–131 (1997)
5. Cao, Y., Cao, Y., Li, Q.: Concatenated structure of cyclic codes over $\mathbb{Z}_4$ of length $4n$. Appl. Algebra Eng. Commun. Comput. **10**, 279–302 (2016)
6. Cao, Y., Cao, Y., Dougherty, S.T., Ling, S.: Construction and enumeration for self-dual cyclic codes over $\mathbb{Z}_4$ of oddly even length. Des. Codes Cryptogr. **87**, 2419–2446 (2019)
7. Cao, Y.: A class of 1-generator repeated root quasi-cyclic codes. Des. Codes Cryptogr. **72**, 483–496 (2014)
8. Cao, Y., Cao, Y., Fu, F.-W.: On self-duality and hulls of cyclic codes over $\frac{\mathbb{F}_{2^m}[u]}{\langle u^k\rangle}$ with oddly even length. Appl. Algebra Eng. Commun. Comput. (2019). https://doi.org/10.1007/s00200-019-00408-9
9. 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)
10. Cao, Y., Cao, Y.: Complete classification for simple root cyclic codes over the local ring $\mathbb{Z}_4[v]/\langle v^2+2v\rangle$. Cryptogr. Commun. **12**, 301–319 (2020)
11. Dougherty, S.T., Ling, S.: Cyclic codes over $\mathbb{Z}_4$ of even length. Des. Codes Cryptogr. **39**, 127–153 (2006)
12. Gaborit, P., Natividad, A.M., Solé, P.: Eisenstein lattices, Galois rings and quaternary codes. Int. J. Number Theory **2**, 289–303 (2006)

13. Hammons Jr., A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inform. Theory **40**(2), 301–319 (1994)
14. Harada, M.: Self-dual $\mathbb{Z}_4$-codes and Hadamard matrices. Discrete Math. **245**, 273–278 (2002)
15. Harada, M., Kitazume, M., Munemasa, A., Venkov, B.: On some self-dual codes and unimodular lattices in dimension 48. Eur. J. Combin. **26**, 543–557 (2005)
16. Harada, M., Miezaki, T.: An optimal odd unimodular lattice in dimension 72. Arch. Math. **97**(6), 529–533 (2011)
17. Harada M., Solé P., Gaborit P.: Self-dual codes over $\mathbb{Z}_4$ and unimodular lattices: a survey. In: Algebras and Combinatorics, Hong Kong, 1997, pp. 255–275. Springer, Singapore (1999)
18. Kiah, H.M., Leung, K.H., Ling, S.: A note on cyclic codes over GR(p^2, m) of length p^k. Des. Codes Cryptogr. **63**, 105–112 (2012)
19. Jitman, S., Ling, S., Sangwisut, E.: On self-dual cyclic codes of length p^a over GR(p^2, s). Adv. Math. Commun. **10**, 255–273 (2016)
20. Pless, V.S., Qian, Z.: Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. IEEE Trans. Inform. Theory **42**, 1594–1600 (1996)
21. Pless, V.S., Solé, P., Qian, Z.: Cyclic self-dual $\mathbb{Z}_4$-codes. Finite Fields Appl. **3**, 48–69 (1997)
22. 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**, 86–95 (2017)
23. Wan, Z.-X.: Quaternary Codes. World Scientific Pub Co Inc., Singapore (1997)
24. Wan, Z.-X.: Lectures on Finite Fields and Galois Rings. World Scientific Pub Co Inc., Singapore (2003)
25. Database of $\mathbb{Z}_4$ codes [online], http://www.z4codes.info. Accessed 03 Sept 2016