Designs, Codes and Cryptography (2019) 87:2419–2446
https://doi.org/10.1007/s10623-019-00629-6

Construction and enumeration for self-dual cyclic codes over $\mathbb{Z}_4$ of oddly even length

Yuan Cao[1,2,3] · Yonglin Cao[1] · Steven T. Dougherty[4] · San Ling[5]

Received: 2 September 2018 / Revised: 19 January 2019 / Accepted: 11 March 2019 /
Published online: 21 March 2019

Abstract

For any positive odd integer n, a precise representation for cyclic codes over $\mathbb{Z}_4$ of length $2n$ is given in terms of the Chinese Remainder Theorem. Using this representation, an efficient encoder for each of these codes is described. Then the dual codes are determined precisely and this is used to study codes which are self-dual. In particular, the number of self-dual cyclic codes over $\mathbb{Z}_4$ of length $2n$ can be calculated from 2-cyclotomic cosets modulo n directly. Moreover, mistakes in Blackford (Discret Appl Math 128:27–46, 2003) and Dougherty and Ling (Des Codes Cryptogr 39:127–153, 2006) are corrected. As an application, all 315 self-dual cyclic codes over $\mathbb{Z}_4$ of length 30 are listed. Among these codes, there are some new cyclic self-dual $\mathbb{Z}_4$-codes $\mathcal{C}$ with parameters $(30, |\mathcal{C}| = 2^{30}, d_H = 6, d_L = 12)$ and $(30, |\mathcal{C}| = 2^{30}, d_H = 5, d_L = 10)$. From these codes and applying the Gray map from $\mathbb{Z}_4$ onto $\mathbb{F}_2^2$, formally self-dual and 2-quasicyclic binary codes with basic parameters [60, 30, 12] and [60, 30, 10] are derived respectively.

Communicated by J. D. Key.

✉ Yonglin Cao
ylcao@sdut.edu.cn

Yuan Cao
yuancao@sdut.edu.cn

Steven T. Dougherty
prof.steven.dougherty@gmail.com

San Ling
lingsan@ntu.edu.sg

[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] Department of Mathematics, University of Scranton, Scranton, PA 18510, USA

[5] School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, Republic of Singapore

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

Mathematics Subject Classification 94B15 · 94B05 · 11T71

1 Introduction

In [17], it was shown that many interesting binary linear and nonlinear codes were in fact the images under a Gray map of codes over the ring $\mathbb{Z}_4$. This important discovery caused an enormous amount of activity in studying 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. More precisely, $\mathbb{Z}_4$ modules are studied together with the following Gray map ψ from $\mathbb{Z}_4$ onto $\mathbb{F}_2^2$, defined by $0 \mapsto 00$, $1 \mapsto 01$, $2 \mapsto 11$ and $3 \mapsto 10$, to obtain good binary codes. As a consequence of these discoveries, codes over rings have become a widely studied branch of coding theory.

We begin with the necessary definitions for codes over rings. Let A be a commutative finite ring with identity $1 \neq 0$, and let $A^\times$ be the multiplicative group of invertible elements of 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. Specifically, $\mathcal{C}$ is called a $\mathbb{Z}_4$-linear code when $A = \mathbb{Z}_4$. All quaternary codes, i.e., codes over $\mathbb{Z}_4$, in this paper are assumed to be linear. The ambient space A^N is equipped with the usual Euclidian 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 *dual code* is defined by $\mathcal{C}^\perp = \{a \in A^N \mid [a, b] = 0, \forall b \in \mathcal{C}\}$. If $\mathcal{C} = \mathcal{C}^\perp$, $\mathcal{C}$ is called a *self-dual code* over A. Self-dual codes are an important and widely studied family of codes. As an example of the importance of quaternary self-dual codes, see [19], where the authors find extremal unimodular lattices of length 72 using self-dual quaternary codes. For an encyclopedic description of self-dual codes, see [23].

Cyclic codes are one of the most studied families of codes. One important reason for this is that they have a canonical representation in polynomial rings. This representation allows for a classification of these and a description of their structure. We define a code $\mathcal{C}$ 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 the vector $c = (c_0, c_1, \ldots, c_{N-1})$ is viewed as a polynomial $c(x) = \sum_{j=0}^{N-1} c_j x^j$. Under this association, the cyclic code $\mathcal{C}$ is an ideal in the polynomial residue ring $A[x]/\langle x^N - 1\rangle$ since addition and multiplication of a scalar from A follows from the code being linear and multiplication by x corresponds to the cyclic shift. If σ is the cyclic shift operator, then a code $\mathcal{C}$ is said to be *quasicyclic of index k* if k is the smallest integer with $\sigma^k(\mathcal{C}) = \mathcal{C}$.

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} denote 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 [25, Proposition 1.1]).

Cyclic codes over $\mathbb{Z}_4$ of length n were first studied in [4] as a projection of codes over the p-adics. A more detailed study appeared in [21], where specific polynomial representations of cyclic codes were given. In [22], Pless *et al.* characterized nontrivial cyclic self-dual codes over $\mathbb{Z}_4$ of certain length n by describing generators of such codes. In particular, all examples of nontrivial cyclic self-dual codes over $\mathbb{Z}_4$ up to length 39 were given. For example, there is only 1 nontrivial cyclic self-dual code over $\mathbb{Z}_4$ of length 23.

In [12], Dougherty and Fernandez studied the ranks and kernels of cyclic codes over $\mathbb{Z}_4$ of odd length. In [20], Jitman and Sangwisut studied the hulls of cyclic codes over $\mathbb{Z}_4$ of length n, and a characterization for hulls was established in terms of the generators viewed as ideals in the quotient ring $\mathbb{Z}_4[x]/\langle x^n - 1\rangle$. In [16], Gao *et al.* investigated double cyclic codes over $\mathbb{Z}_4$, i.e., $\mathbb{Z}_4[x]$-submodules of $\mathbb{Z}_4[x]/\langle x^r - 1\rangle \times \mathbb{Z}_4[x]/\langle x^s - 1\rangle$, where both r and s are odd positive integers. Some optimal or suboptimal nonlinear binary codes were obtained from this family of codes.

In general, cyclic codes were studied where the length was relatively prime to the characteristic of the ring since this simplified the algebra significantly. Later cyclic codes where the length was not relatively prime to 4 were studied. The first step was done by Abualrub and Oehmke in [1], where they determined the generators for cyclic codes over $\mathbb{Z}_4$ for lengths of the form 2^k. Later, Blackford in [3] and [2] gave a description for cyclic codes over $\mathbb{Z}_4$ of length $2n$ in terms of the discrete Fourier transform and by the following ring isomorphism:

$$\frac{\mathbb{Z}_4[x]}{\langle x^{2n} - 1\rangle} \cong \frac{\mathcal{R}[x]}{\langle x^n - u\rangle} \cong \frac{\mathcal{R}[x]}{\langle g_1(x)\rangle} \times \cdots \times \frac{\mathcal{R}[x]}{\langle g_r(x)\rangle},$$

where

$$\mathcal{R} := \frac{\mathbb{Z}_4[u]}{\langle u^2 - 1\rangle} = \{a + bu \mid a, b \in \mathbb{Z}_4\} \ (u^2 = 1)$$

and $x^n - u = g_1(x)g_2(x)\ldots g_r(x)$ and $g_1(x), g_2(x), \ldots, g_r(x)$ are monic, basic irreducible and pairwise coprime polynomials in $\mathcal{R}[x]$ (see [3, p. 29]). Using this foundation, generator polynomials, parity check matrices, and dual codes over $\mathbb{Z}_4$ of length $2n$ were given in [3].

Completing the remaining cases, as a generalization and further development of [3] and [2], Dougherty and Ling in [13] determined the structure of cyclic codes over $\mathbb{Z}_4$ for arbitrary even length in terms of the discrete Fourier transform.

It is not easy to explicitly give all distinct cyclic codes over $\mathbb{Z}_4$ of length $2n$ (resp. $2^k n$) nor to explicitly give all self-dual cyclic codes by use of expressions for cyclic codes given in [3] (resp. [13]). As an example, see Sect. 2.4 “Examples” in [3, pp. 38–39].

To be precise, there are some mistakes in the description of self-dual cyclic codes over $\mathbb{Z}_4$ of length $2n$ in [13]. We shall explain what these are presently.

Proposition 5.8 of [13] (see p. 151) states: “The number of self-dual cyclic codes over $\mathbb{Z}_4$ of length $2^k n$ is given by $\prod_{\alpha\in\widetilde{\mathcal{J}}} M_\alpha \prod_{\alpha\in K} N_\alpha$.”

For any integer α, $0 \leq \alpha \leq n-1$, let $J_\alpha^{(2)}$ be the 2-cyclotomic coset modulo n containing α, i.e., $J_\alpha^{(2)} = \{2^j\alpha \mid j = 0, 1, \ldots, m_\alpha - 1\} \pmod n$, where $m_\alpha = |J_\alpha^{(2)}|$. In [13, Proposition 5.8], $\widetilde{\mathcal{J}} \cup K$ is a complete set of 2-cyclotomic coset representatives modulo n, satisfying the following conditions:

(1) $0 \in \widetilde{\mathcal{J}}$, and $J_{n-\alpha}^{(2)} = J_\alpha^{(2)}$ for all $0 \neq \alpha \in \widetilde{\mathcal{J}}$;

(2) $J_\alpha^{(2)} \cap J_{n-\alpha}^{(2)} = \emptyset$ for all $\alpha \in K$.

When $k = 1$, $N_\alpha = 5 + 2^{m_\alpha}$ ([13, p. 140] or [3, Corollary 1]) for all $\alpha \in \widetilde{\mathcal{J}} \cup K$, and $M_\alpha = 1$ [13, Corollary 5.7(i)] for all $\alpha \in K$. In this case, [13] claimed the following:

(1) *The number of self-dual cyclic codes over* $\mathbb{Z}_4$ *of length* $2n$ *is given by*

$$\prod_{\alpha\in K}(5 + 2^{m_\alpha}).$$

(2) *If there exists e such that* $-1 \equiv 2^e \bmod n$, *then there is only one cyclic self-dual code over* $\mathbb{Z}_4$ *of length* $2n$ *where* n *is odd, namely* $2(\mathbb{Z}_4)^{2n}$ [13, Corollary 5.9].

Both of these statements require correction. The first statement is missing a term (which proves to be quite important). In Theorem 3 in this paper, we prove the following correction:

- The number of self-dual cyclic codes over $\mathbb{Z}_4$ of length $2n$ is given by

$$\prod_{0 \neq \alpha \in \widetilde{\mathcal{J}}} (1 + 2^{m_\alpha/2}) \prod_{\alpha \in K} (5 + 2^{m_\alpha}).$$

We can compare these two results. As $-1 \equiv 2 \pmod 3$, $-1 \equiv 2^2 \pmod 5$, $-1 \equiv 2^3 \pmod 9$, $-1 \equiv 2^4 \pmod{17}$, $-1 \equiv 2^5 \pmod{33}$, $-1 \equiv 2^5 \pmod{11}$, $-1 \equiv 2^6 \pmod{13}$ and $-1 \equiv 2^7 \pmod{43}$, the results in [13] would imply that there is only one cyclic self-dual code over $\mathbb{Z}_4$ of length $2n$ for $n = 3, 5, 9, 11, 13, 17, 33, 43$. However, the number $\mathcal{N}$ of cyclic self-dual code over $\mathbb{Z}_4$ with length $2n$ for $n = 3, 5, 9, 11, 13, 17, 33, 43$ is given by the following table.

n	$\mathcal{N}$	n	$\mathcal{N}$	n	$\mathcal{N}$	n	$\mathcal{N}$
3	3	9	27	13	65	33	107811
5	5	11	33	17	289	43	2146689

As an initial improvement for the partial results in [13], Cao *et al.* presented a clearer concatenated structure for every cyclic code over $\mathbb{Z}_4$ of length $4n$ using the following ring isomorphism (see [8, Theorem 2.6]):

$$\frac{\mathbb{Z}_4[x]}{\langle x^{4n} - 1 \rangle} \cong \frac{\mathcal{A}[x]}{\langle x^4 - y \rangle} \cong \frac{R_1[x]}{\langle x^4 - y \rangle} \times \cdots \times \frac{R_r[x]}{\langle x^4 - y \rangle}$$

and ideals of each ring $\frac{R_i[x]}{\langle x^4 - y \rangle}$ (see [8, Theorem 3.3]), where

$$\mathcal{A} := \frac{\mathbb{Z}_4[y]}{\langle y^n - 1 \rangle} = \left\{ \sum_{j=0}^{n-1} a_j y^j \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}_4 \right\} \ (y^n = 1),$$

$R_i = \frac{\mathbb{Z}_4[y]}{\langle f_i(y) \rangle}$, $1 \leq i \leq r$, and $f_1(y), \ldots, f_r(y)$ are monic, basic irreducible and pairwise coprime polynomials in $\mathbb{Z}_4[y]$ satisfying $y^n - 1 = f_1(y) \ldots f_r(y)$. It can still be difficult to construct cyclic codes over $\mathbb{Z}_4$ of length $4n$ by use of the representation given in [8], as the expression for ideals of each ring $\frac{R_i[x]}{\langle x^4 - y \rangle}$ is still complicated. Therefore, it is necessary to adopt a new approach for representing all distinct cyclic codes over $\mathbb{Z}_4$ of even length. It is then possible to determine which codes among them are self-dual.

Throughout the rest of this paper, we let n be an positive odd integer. Then, cyclic codes over $\mathbb{Z}_4$ of length $2n$ are viewed as ideals in the polynomial ring $\mathbb{Z}_4[x]/\langle x^{2n} - 1 \rangle$, using the canonical representation. In this paper, we give another description for ideals of $\mathbb{Z}_4[x]/\langle x^{2n} - 1 \rangle$ by the using the following ring isomorphism:

$$\frac{\mathbb{Z}_4[x]}{\langle x^{2n} - 1 \rangle} \cong \frac{\mathbb{Z}_4[x]}{\langle f_1(x^2) \rangle} \times \cdots \times \frac{\mathbb{Z}_4[x]}{\langle f_r(x^2) \rangle},$$

and by examining the ideals in each ring $\frac{\mathbb{Z}_4[x]}{\langle f_i(x^2) \rangle}$, where $f_1(x), \ldots, f_r(x)$ are monic, basic irreducible and pairwise coprime polynomials in $\mathbb{Z}_4[x]$ satisfying $x^n - 1 = f_1(x) \ldots f_r(x)$.

Recall the following easy proposition.

Proposition 1 *Let $\mathcal{C}$ be a quaternary cyclic code of length $2n$. Then $\psi(\mathcal{C})$ is a binary (not necessarily linear) quasicyclic code of length $4n$ and index 2, where $\psi : \mathbb{Z}_4^{2n} \to \mathbb{F}_2^{4n}$ is the Gray map.*

Proof Follows from a straightforward computation. □

We organize the paper as follows. In Sect. 2, we give a new representation and an efficient encoder for each cyclic code over $\mathbb{Z}_4$ of length $2n$ (Theorem 2.1). In Sect. 3, we introduce necessary notation needed in this paper and give a proof for Theorem 1. In Sect. 4, we present the dual code for each of these cyclic codes. In Sect. 5, we list all distinct self-dual cyclic codes over $\mathbb{Z}_4$ of length $2n$ and count the number of these codes. In Sect. 6, we list all 315 self-dual cyclic codes over $\mathbb{Z}_4$ of length 30 explicitly. Among these codes, we obtain 24 new and good cyclic self-dual $\mathbb{Z}_4$-codes $\mathcal{C}$ with parameters $(30, |\mathcal{C}| = 2^{30}, d_H = 6, d_L = 12)$ and $(30, |\mathcal{C}| = 2^{30}, d_H = 5, d_L = 10)$, where d_H and d_L are the minimum Hamming distance and the minimum Lee distance of the code $\mathcal{C}$, respectively. In Sect. 7, we study the lifts of cyclic codes and an isomorphism on the set of cyclic codes.

2 Representation and encoding for cyclic codes over $\mathbb{Z}_4$ of length $2n$

In this section, we give a new representation and an efficient encoder for each cyclic code over $\mathbb{Z}_4$ of length $2n$.

In this paper, we will regard the binary field $\mathbb{F}_2 = \mathbb{Z}_2 = \{0, 1\}$ as a subset of the ring $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, even though $\mathbb{F}_2$ is not a subring of $\mathbb{Z}_4$. Using this, any element a of $\mathbb{Z}_4$ has a unique 2-expansion, namely $a = a_0 + 2a_1$, where $a_0, a_1 \in \mathbb{F}_2$. We define the following projection to the binary field $\overline{a} = a_0 = a \pmod 2$. Then $^{-} : \mathbb{Z}_4 \to \mathbb{F}_2$ is a surjective ring homomorphism. The map extends naturally to $\mathbb{Z}_4[y]$ by applying it to the coefficients of the polynomial. Let y be an indeterminate over $\mathbb{Z}_4$ and $\mathbb{F}_2$. Define

$$\overline{f}(y) = \overline{f(y)} = \sum_{i=0}^{d} \overline{b}_i y^i, \ \forall f(y) = \sum_{i=0}^{d} b_i y^i \in \mathbb{Z}_4[y].$$

The map $^{-}$ is a surjective ring homomorphism from $\mathbb{Z}_4[y]$ onto $\mathbb{F}_2[y]$.

Recall that a monic polynomial $f(y) \in \mathbb{Z}_4[y]$ of positive degree is defined to be *basic irreducible* if $\overline{f}(y)$ is an irreducible polynomial in $\mathbb{F}_2[y]$ (cf. Wan [26, Sect. 13.4]).

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

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

where $f_1(y), f_2(y), \dots, f_r(y)$ are pairwise coprime monic basic irreducible polynomials in $\mathbb{Z}_4[y]$ with degree $\deg(f_i(y)) = m_i$ for all $i = 1, \dots, r$. Additionally, we will adopt the following notation.

(1) The ring $\mathcal{A} = \frac{\mathbb{Z}_4[x]}{\langle x^{2n}-1\rangle} = \{\sum_{j=0}^{2n-1} a_j x^j \mid a_j \in \mathbb{Z}_4,\ j = 0, 1, \dots, 2n-1\}$ where the arithmetic is done modulo $x^{2n} - 1$. Cyclic codes over $\mathbb{Z}_4$ of length $2n$ are viewed as ideals of the ring $\mathcal{A}$.

(2) The ring $\mathcal{K}_i = \frac{\mathbb{Z}_4[x]}{\langle f_i(x^2)\rangle} = \{\sum_{j=0}^{2m_i-1} a_j x^j \mid a_j \in \mathbb{Z}_4,\ j = 0, 1, \dots, 2m_i - 1\}$ where the arithmetic is done modulo $f_i(x^2)$. We regard $\mathcal{K}_i$ as a subset of the ring $\mathcal{A}$.

(3) The set $\mathcal{T}_i = \{\sum_{j=0}^{m_i-1} t_j x^j \mid t_j \in \{0,1\},\ j = 0, \ldots, m_i - 1\}$. Then $|\mathcal{T}_i| = 2^{m_i}$. We regard $\mathcal{T}_i$ as a subset of the ring $\mathcal{K}_i$. Hereafter, the set $\mathcal{T}_i$ will appear frequently in the succeeding results.

(4) Denote by $F_i(y) = \frac{y^n-1}{f_i(y)} \in \mathbb{Z}_4[y]$. Since $\gcd(\overline{F}_i(y), \overline{f}_i(y)) = 1$, we see that $F_i(y)$ and $f_i(y)$ are coprime in $\mathbb{Z}_4[y]$ (cf. [26, Lemma 13.5]). Hence there are polynomials $u_i(y), v_i(y) \in \mathbb{Z}_4[y]$ such that

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

and $\deg(u_i(y)) < \deg(f_i(y)) = m_i$. Then define $\theta_i(x) \in \mathcal{A}$ by the following equation

$$\theta_i(x) \equiv u_i(x^2)F_i(x^2) = 1 - v_i(x^2)f_i(x^2) \pmod{x^{2n} - 1}. \tag{3}$$

(5) There is a unique element $w_i(x)$ in $\mathcal{T}_i$ such that $f_i(x)^2 = 2\overline{f}_i(x)w_i(x)$ in the ring $\mathcal{K}_i$ and $w_i(x) \neq 0$ (see Lemma 5 of this paper).

For any ideal C_i in the ring $\mathcal{K}_i = \mathbb{Z}_4[x]/\langle f_i(x^2)\rangle$, recall that the *annihilating ideal* of C_i is defined as $\mathrm{Ann}(C_i) = \{\alpha \in \mathcal{K}_i \mid \alpha\beta = 0, \forall \beta \in C_i\}$.

The following theorem will give a description of all distinct ideals in $\mathcal{A}$.

Theorem 1 *Every cyclic code $\mathcal{C}$ over $\mathbb{Z}_4$ of length $2n$ is a unique direct sum of its subcodes:*

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

where

$$\mathcal{C}_i = \theta_i(x)C_i = \{\theta_i(x)b(x) \mid b(x) \in C_i\} \pmod{x^{2n} - 1}$$

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

Case	C_i	type of $\mathcal{C}_i$	$\lvert\mathcal{C}_i\rvert$	$\mathrm{Ann}(C_i)$
1.	$\langle 0\rangle$	$4^0 2^0$	1	$\langle 1\rangle$
2.	$\langle 1\rangle$	$4^{2m_i} 2^0$	2^{4m_i}	$\langle 0\rangle$
3.	$\langle 2\rangle$	$4^0 2^{2m_i}$	2^{2m_i}	$\langle 2\rangle$
4.	$\langle 2\overline{f}_i(x)\rangle$	$4^0 2^{m_i}$	2^{m_i}	$\langle f_i(x), 2\rangle$
5.	$\langle f_i(x), 2\rangle$	$4^{m_i} 2^{m_i}$	2^{3m_i}	$\langle 2\overline{f}_i(x)\rangle$
6.	$\langle f_i(x) + 2h(x)\rangle$	$4^{m_i} 2^0$	2^{2m_i}	$\langle f_i(x) + 2(w_i(x) + h(x))\rangle$

where $h(x) \in \mathcal{T}_i$. Then the number of ideals in $\mathcal{K}_i$ is $5 + 2^{m_i}$.

An encoder for each subcode $\mathcal{C}_i$, is given by the following:

Case 1. $\mathcal{C}_i = \{0\}$.
Case 2. $\mathcal{C}_i = \{\sum_{j=0}^{2m_i-1} a_j x^j \theta_i(x) \mid a_j \in \mathbb{Z}_4,\ j = 0, 1, \ldots, 2m_i - 1\}$.
Case 3. $\mathcal{C}_i = \{\sum_{t=0}^{2m_i-1} 2b_t x^t \theta_i(x) \mid b_t \in \{0,1\},\ t = 0, 1, \ldots, 2m_i - 1\}$.
Case 4. $\mathcal{C}_i = \{\sum_{t=0}^{m_i-1} 2b_t x^t \overline{f}_i(x)\theta_i(x) \mid b_t \in \{0,1\},\ t = 0, 1, \ldots, m_i - 1\}$.
Case 5. $\mathcal{C}_i = \{\sum_{j=0}^{m_i-1} a_j x^j f_i(x)\theta_i(x) + \sum_{t=0}^{m_i-1} 2b_t x^t \theta_i(x) \mid a_j \in \mathbb{Z}_4,\ b_t \in \{0,1\},\ j = 0, 1, \ldots, m_i - 1$ and $t = 0, 1, \ldots, m_i - 1\}$.
Case 6. $\mathcal{C}_i = \{\sum_{j=0}^{m_i-1} a_j x^j (f_i(x) + 2h(x))\theta_i(x) \mid a_j \in \mathbb{Z}_4,\ j = 0, 1, 2, \ldots, m_i - 1\}$.

Let $4^{k_{0,i}}2^{k_{1,i}}$ be the type of the subcode $\mathcal{C}_i$ given above for all $1 \leq i \leq r$. Then $\mathcal{C}$ 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 $\prod_{i=1}^{r} |\mathcal{C}_i| = 2^{2\sum_{i=1}^{r} k_{0,i}+\sum_{i=1}^{r} k_{1,i}}$ and the minimum Hamming distance (Lee distance and Euclidean distance) of $\mathcal{C}$ satisfies

$$d_{\min}(\mathcal{C}) \leq \min\{d_{\min}(\theta_i(x)C_i) \mid i = 1, \ldots, r\}.$$

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

Using the notation of Theorem 1, $\mathcal{C} = \bigoplus_{j=1}^{r} \theta_j(x)C_j$ is called the *canonical form decomposition* of the cyclic code $\mathcal{C}$ over $\mathbb{Z}_4$ of length $2n$.

Remark 1 For each integer i, $1 \leq i \leq r$, by Theorem 1, we know that $\mathcal{K}_i = \frac{\mathbb{Z}_4[x]}{\langle f_i(x^2)\rangle}$ is a local ring with unique maximal ideal $\langle f_i(x), 2\rangle$ and a non-principal ideal ring with $5 + 2^{m_i}$ ideals. However, $\frac{\mathbb{Z}_4[x]}{\langle f_i(-x^2)\rangle}$ is a finite chain ring with unique maximal ideal $\langle f_i(x)\rangle$ and a principal ideal ring with 5 ideals (cf. [7, Theorem 3.2]).

3 Proof of Theorem 1

In this section, we give a complete proof of Theorem 1.

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

$$x^{2n} - 1 = f_1(x^2)f_2(x^2)\ldots f_r(x^2) \text{ and } u_i(x^2)F_i(x^2) + v_i(x^2)f_i(x^2) = 1 \qquad (4)$$

in $\mathbb{Z}_4[x]$ respectively, where $F_i(x^2) = \frac{x^{2n}-1}{f_i(x^2)} \in \mathbb{Z}_4[x]$. From this, by Eq. (3) in Sect. 2 and the Chinese Remainder Theorem for commutative rings, one can easily verify the following conclusions. Here we omit the proofs.

Lemma 1 *Let $\mathcal{A} = \frac{\mathbb{Z}_4[x]}{\langle x^{2n}-1\rangle}$ and $\mathcal{K}_i = \frac{\mathbb{Z}_4[x]}{\langle f_i(x^2)\rangle}$.*

(i) In the ring $\mathcal{A}$, we have $\theta_1(x) + \cdots + \theta_r(x) = 1$, $\theta_i(x)^2 = \theta_i(x)$ and $\theta_i(x)\theta_j(x) = 0$ for all $1 \leq i \neq j \leq r$.

(ii) We have that $\mathcal{A} = \mathcal{A}_1 + \cdots + \mathcal{A}_r$, where $\mathcal{A}_i = \mathcal{A}\theta_i(x)$ is the ideal of $\mathcal{A}$ generated by $\theta_i(x)$, and $\mathcal{A}_i$ is a commutative ring with $\theta_i(x)$ as its multiplicative identity for all $i = 1, \ldots, r$. Moreover, $\mathcal{A}$ is a direct sum of rings $\mathcal{A}_1, \ldots, \mathcal{A}_r$ with $\mathcal{A}_i\mathcal{A}_j = \{0\}$ for all $i \neq j$.

(iii) For each integer i, $1 \leq i \leq r$, the map ϕ_i defined by

$$\phi_i : a(x) \mapsto \theta_i(x)a(x) \pmod{x^{2n} - 1}, \ \forall a(x) \in \mathcal{K}_i.$$

is a ring isomorphism from $\mathcal{K}_i$ onto $\mathcal{A}_i$.

(iv) Define a map ϕ by the rule: for any $a_i(x) \in \mathcal{K}_i$, $1 \leq i \leq r$, let

$$\phi(a_1(x), \ldots, a_r(x)) = \sum_{i=1}^{r} \phi_i(a_i(x)) = \sum_{i=1}^{r} \theta_i(x)a_i(x) \pmod{x^{2n} - 1}.$$

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

We now present a canonical form decomposition for any cyclic code over $\mathbb{Z}_4$ of length $2n$, i.e., any ideal of the ring $\mathcal{A} = \mathbb{Z}_4[x]/\langle x^{2n} - 1\rangle$.

Proposition 2 *Let $\mathcal{C} \subseteq \mathcal{A}$. Then $\mathcal{C}$ is a cyclic code over $\mathbb{Z}_4$ of length $2n$ if and only if for each integer i, $1 \leq i \leq r$, there is a unique ideal C_i of the ring $\mathcal{K}_i$ such that $\mathcal{C} = \bigoplus_{i=1}^{r} \mathcal{C}_i = \sum_{i=1}^{r} \mathcal{C}_i$, where*

$$\mathcal{C}_i = \theta_i(x)C_i = \{\theta_i(x)c_i(x) \mid c_i(x) \in C_i\} \pmod{x^{2n}-1}.$$

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 $2n$. By Lemma 1(iv) and the properties of isomorphic rings, there is a unique ideal C of the direct product ring $\mathcal{K}_1 \times \cdots \times \mathcal{K}_r$ such that $\mathcal{C} = \phi(C)$. Hence for each integer i, $1 \leq i \leq r$, there is a unique ideal C_i of $\mathcal{K}_i$ such that $C = C_1 \times \cdots \times C_r$. This implies that

$$\begin{aligned}\mathcal{C} &= \{\phi(c_1(x), \ldots, c_r(x)) \mid c_i(x) \in C_i,\ i = 1, \ldots, r\}\\ &= \sum_{i=1}^{r} \{\theta_i(x)c_i(x) \mid c_i(x) \in C_i\} \pmod{x^{2n}-1}.\end{aligned}$$

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

In order to present all cyclic codes over $\mathbb{Z}_4$ of length $2n$, it is sufficient, using Proposition 2, to determine all ideals of the ring $\mathcal{K}_i = \mathbb{Z}_4[x]/\langle f_i(x^2)\rangle$, where $f_i(x)$ is a monic basic irreducible polynomial in $\mathbb{Z}_4[x]$ of degree m_i and $f_i(x) \mid (x^n - 1)$, $1 \leq i \leq r$.

Let i be a positive integer, $1 \leq i \leq r$. Since $f_i(y)$ is a monic basic irreducible polynomial in $\mathbb{Z}_4[y]$ of degree m_i by the notation of Sect. 2, $\overline{f}_i(y)$ is an irreducible polynomial in $\mathbb{F}_2[y]$ of degree m_i and $\overline{f_i(x^2)} = \overline{f}_i(x)^2$ as polynomials in $\mathbb{F}_2[x]$. We will adopt the following notation from now on.

(1) The ring $\Gamma_i = \frac{\mathbb{Z}_4[y]}{\langle f_i(y)\rangle} = \{\sum_{j=0}^{m_i-1} a_j y^j \mid a_j \in \mathbb{Z}_4,\ j = 0, \ldots, m_i - 1\}$ where the arithmetic is done modulo $f_i(y)$.

(2) The ring $\overline{\Gamma}_i = \frac{\mathbb{F}_2[y]}{\langle \overline{f}_i(y)\rangle} = \{\sum_{j=0}^{m_i-1} b_j y^j \mid b_j \in \mathbb{F}_2,\ j = 0, \ldots, m_i - 1\}$ where the arithmetic is done modulo $\overline{f}_i(y)$.

(3) The ring $\overline{\mathcal{K}}_i = \frac{\mathbb{F}_2[x]}{\langle \overline{f}_i(x^2)\rangle} = \frac{\mathbb{F}_2[x]}{\langle \overline{f}_i(x)^2\rangle} = \{\sum_{j=0}^{2m_i-1} b_j x^j \mid b_j \in \mathbb{F}_2,\ j = 0, 1, 2, \ldots, 2m_i - 1\}$ where the arithmetic is done modulo $\overline{f}_i(x)^2$.

As we regard $\mathbb{F}_2$ as a subset of $\mathbb{Z}_4$, we will regard $\overline{\Gamma}_i$ as a subset of Γ_i even though $\overline{\Gamma}_i$ is not a subring of Γ_i. Similarly, we will regard $\overline{\mathcal{K}}_i$ as a subset of the ring $\mathcal{K}_i = \frac{\mathbb{Z}_4[x]}{\langle f_i(x^2)\rangle}$. If needed, the reader is referred back to this identification of $\overline{\mathcal{K}}_i$ with a subset of $\mathcal{K}_i$.

We collect a few results from [26] and [5] which we will need and we state them as a lemma. The following conclusion depends on that $f_i(x)$ is monic basic irreducible, $f_i(x) | (x^n - 1)$ in $\mathbb{Z}_4[x]$ and n is odd.

Lemma 2 *(i) [26, Theorems 14.1 and 14.8] The ring Γ_i is a Galois ring of characteristic 4 and cardinality 4^{m_i} and $\Gamma_i = \mathbb{Z}_4[\zeta_i]$, where $\zeta_i = y + \langle f_i(y)\rangle \in \Gamma_i$ satisfying $f_i(\zeta_i) = 0$, $\zeta_i^{2^{m_i}-1} = 1$ and $\zeta_i^n = 1$ in Γ_i.*

Denote by $\overline{\zeta}_i = y + \langle \overline{f}_i(y)\rangle \in \overline{\Gamma}_i$. Then $\overline{\Gamma}_i = \mathbb{F}_2[\overline{\zeta}_i]$, which is a finite field of cardinality 2^{m_i}, $\overline{f}_i(x) = \prod_{j=0}^{m_i-1}(x - \overline{\zeta}_i^{2^j})$ over $\overline{\Gamma}_i$. Moreover, the homomorphism $^-$ from $\mathbb{Z}_4[y]$ onto $\mathbb{F}_2[y]$ induces a surjective ring homomorphism from Γ_i onto $\overline{\Gamma}_i$ by the rule that

$$\xi \mapsto \overline{\xi} = \sum_{j=0}^{m_i-1} \overline{a}_j \overline{\zeta}_i^j,\ \forall \xi = \sum_{j=0}^{m_i-1} a_j \zeta_i^j \in \Gamma_i \text{ with } a_0, a_1, \ldots, a_{m_i-1} \in \mathbb{Z}_4.$$

Every element ξ of Γ_i has a unique 2-expansion: $\xi = b_0 + 2b_1,\ b_0, b_1 \in \overline{\Gamma}_i$. Hence $\overline{\xi} = b_0$ and that ξ is an invertible element of Γ_i if and only if $b_0 \neq 0$. Therefore, $|\Gamma_i^{\times}| = (2^{m_i} - 1)2^{m_i}$.

(ii) (cf. [5, Lemma 2.3(ii)]) We have that $f_i(x) = \prod_{j=0}^{m_i-1}(x - \zeta_i^{2^j})$ over Γ_i.

Obviously, $\overline{\mathcal{K}}_i$ is a ring but it is important to note that $\overline{\mathcal{K}}_i$ is not a subring of $\mathcal{K}_i$. Our next lemma is a result from [6].

Lemma 3 (cf. [6, Lemma 3.7])

(i) The ring $\overline{\mathcal{K}}_i$ is a finite chain ring with maximal ideal $\langle \overline{f}_i(x)\rangle = \overline{f}_i(x)\overline{\mathcal{K}}_i$. The nilpotency index of $\overline{f}_i(x)$ in $\overline{\mathcal{K}}_i$ is 2, and $\overline{\mathcal{K}}_i/\langle \overline{f}_i(x)\rangle \cong \mathbb{F}_2[x]/\langle \overline{f}_i(x)\rangle$. Therefore, all ideals of $\overline{\mathcal{K}}_i$ are given by: $\overline{f}_i(x)^l\overline{\mathcal{K}}_i$, $l = 0, 1, 2$.

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

$$\beta = t_0(x) + t_1(x)\overline{f}_i(x),\ t_0(x), t_1(x) \in \mathcal{T}_i.$$

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

(iii) We have $|\overline{f}_i(x)^l\overline{\mathcal{K}}_i| = |\mathbb{F}_2[x]/\langle \overline{f}_i(x)\rangle|^{2-l} = 2^{m_i(2-l)}$, for $l = 0, 1, 2$.

We require two additional lemmas before proceeding to the proof.

Lemma 4 *Every element $a(x)$ of the ring $\mathcal{K}_i$ has a unique 2-expansion:*

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

where $\overline{\mathcal{K}}_i$ is viewed as a subset of $\mathcal{K}_i$. Then $a(x) \in \mathcal{K}_i^{\times}$ if and only if $a_0(x) \in \overline{\mathcal{K}}_i^{\times}$.

Proof Let $a(x) = \sum_{j=0}^{2m_i-1} a_jx^j \in \mathcal{K}_i = \mathbb{Z}_4[x]/\langle f_i(x^2)\rangle$, where $a_j \in \mathbb{Z}_4$. Then each $a_j \in \mathbb{Z}_4$ has a unique 2-expansion: $a_j = a_{j,0} + 2a_{j,1}$ where $a_{j,0}, a_{j,1} \in \mathbb{F}_2$. Let $a_s(x) = \sum_{j=0}^{2m_i-1} a_{j,s}x^j$ for $s = 0, 1$. Then $a_0(x), a_1(x) \in \overline{\mathcal{K}}_i$ and $a(x)$ is uniquely expressed as $a(x) = a_0(x) + 2a_1(x)$.

Now, let $a(x) \in \mathcal{K}_i^{\times}$. Then there exists $b(x) = b_0(x)+2b_1(x) \in \mathcal{K}_i^{\times}$, where $b_0(x), b_1(x) \in \overline{\mathcal{K}}_i$, such that

$$a_0(x)b_0(x) + 2(a_0(x)b_1(x) + a_1(x)b_0(x)) = a(x)b(x) = 1 \text{ in } \mathcal{K}_i.$$

This implies $a_0(x)b_0(x) = 1$ in $\overline{\mathcal{K}}_i$, and hence $a_0(x) \in \overline{\mathcal{K}}_i^{\times}$.

Conversely, let $a_0(x) \in \overline{\mathcal{K}}_i^{\times}$. Then there exist $b_0(x), c(x) \in \overline{\mathcal{K}}_i$ such that $a_0(x)b_0(x) = 1 + 2c(x)$. We select $b_1(x) = a_0(x)^{-1}(a_1(x)b_0(x) + c(x)) \in \overline{\mathcal{K}}_i$ in which $a_0(x)^{-1} \in \mathcal{K}_i$ being the inverse of $a_0(x)$, and set $b(x) = b_0(x) + 2b_1(x) \in \mathcal{K}_i$. Then by $a_0(x)b_1(x) = a_1(x)b_0(x) + c(x)$ (mod 2), we have

$$a(x)b(x) = 1 + 2c(x) + 2((a_0(x)b_1(x) + a_1(x)b_0(x)) = 1 \text{ in } \mathcal{K}_i.$$

This implies that $a(x) \in \mathcal{K}_i^{\times}$. □

Let $1 \leq i \leq r$. As $f_i(x) \in \mathbb{Z}_4[x]$, we have $\overline{f}_i(x) \in \mathbb{Z}_2[x]$ and hence $\overline{f}_i(x)^2 = \overline{f}_i(x^2)$ as polynomials in $\mathbb{Z}_2[x]$. This implies that $f_i(x)^2 - f_i(x^2) \equiv 0 \pmod 2$. Therefore, 2 always divides $f_i(x)^2 - f_i(x^2)$ as polynomials in $\mathbb{Z}[x]$.

Lemma 5 *Let $1 \leq i \leq r$, and $f_i(x)$ be a monic basic irreducible divisor of $x^n - 1$ in $\mathbb{Z}_4[x]$ satisfying Eq. (1) with degree m_i, where n is odd. Then* *(i) There is a polynomial $g_i(x)$ in $\mathbb{Z}_4[x]$ has degree* $\deg(g_i(x)) \leq m_i - 1$ *and satisfies* $f_i(x)^2 = f_i(x^2) + 2f_i(x)g_i(x)$. *Precisely, we have*

$$g_i(x) = \frac{f_i(x)^2 - f_i(x^2)}{2f_i(x)} \pmod 4,$$

where we regard $f_i(x) \in \mathbb{Z}[x]$ and do calculations in the ring $\mathbb{Z}[x]$.

(ii) Let $w_i(x) \in \mathcal{T}_i$ satisfy $w_i(x) \equiv g_i(x) \pmod 2$, i.e. $w_i(x) = \overline{g}_i(x)$. Then

$$f_i(x)^2 = 2\overline{f}_i(x)w_i(x) \text{ in } \mathcal{K}_i \text{ and } w_i(x) \neq 0.$$

Proof (i) Since $f_i(x)$ is monic basic irreducible, $f_i(x)|(x^n - 1)$ in $\mathbb{Z}_4[x]$ and n is odd, by Lemma 2 we have that $\Gamma_i = \mathbb{Z}_4[\zeta_i]$, where $\zeta_i = y + \langle f_i(y) \rangle \in \Gamma_i$ satisfying $\zeta_i^{2^{m_i}-1} = 1$, i.e., $\zeta_i^{2^{m_i}} = \zeta_i$, and $f_i(x) = \prod_{k=0}^{m_i-1}(x - \zeta_i^{2^k})$ in $\Gamma_i[x]$. From this, we deduce that

$$f_i(x^2) = \prod_{k=0}^{m_i-1}(x^2 - \zeta_i^{2^k}) = \prod_{k=0}^{m_i-1}(x^2 - \zeta_i^{2^{k+1}}) = \prod_{k=0}^{m_i-1}\left(x^2 - (\zeta_i^{2^k})^2\right).$$

Then since $x^2 - (\zeta_i^{2^j})^2 = (x - \zeta_i^{2^j})(x + \zeta_i^{2^j})$ and $4 = 0$ in $\mathbb{Z}_4$, we have

$$\begin{aligned} f_i(x)^2 &= \prod_{k=0}^{m_i-1}(x - \zeta_i^{2^k})^2 = \prod_{k=0}^{m_i-1}\left(x^2 - 2\zeta_i^{2^k}x + (\zeta_i^{2^k})^2\right) \\ &= \prod_{k=0}^{m_i-1}\left(\left(x^2 - (\zeta_i^{2^k})^2\right) - 2\zeta_i^{2^k}(x - \zeta_i^{2^k})\right) \\ &= \prod_{k=0}^{m_i-1}\left(x^2 - (\zeta_i^{2^k})^2\right) - 2\sum_{k=0}^{m_i-1}\zeta_i^{2^k}(x - \zeta_i^{2^k}) \prod_{0 \leq j \leq m_i-1, j \neq k}\left(x^2 - (\zeta_i^{2^j})^2\right) \\ &= f_i(x^2) + 2f_i(x)g_i(x), \end{aligned}$$

where

$$g_i(x) = \sum_{k=0}^{m_i-1}\zeta_i^{2^k} \prod_{0 \leq j \leq m_i-1, j \neq k}(x + \zeta_i^{2^j}) \in \Gamma_i[x] \text{ with } \deg(g_i(x)) \leq m_i - 1. \quad (5)$$

This implies $g_i(x) = \frac{f_i(x)^2 - f_i(x^2)}{2f_i(x)}$ which is a polynomial. From these and by $f_i(x)$, $f_i(x)^2$, $f_i(x^2) \in \mathbb{Z}_4[x]$, we deduce that that $g_i(x) \in \mathbb{Z}_4[x]$, since $\mathbb{Z}_4$ is a subring of Γ_i.

(ii) As we viewed the finite field $\mathbb{F}_2$ as the subset $\{0, 1\} \subset \mathbb{Z}_4$, we have that $w_i(x) = \overline{g}_i(x) \in \mathbb{F}_2[x]$. Since $f_i(x)^2 = f_i(x^2) + 2f_i(x)g_i(x)$ and $4 = 0$ in $\mathbb{Z}_4$, it follows that $f_i(x)^2 \equiv 2\overline{f}_i(x)\overline{g}_i(x) \pmod{f_i(x^2)}$. This implies

$$f_i(x)^2 = 2\overline{f}_i(x)\overline{g}_i(x) = 2\overline{f}_i(x)w_i(x) \text{ in } \mathcal{K}_i.$$

By Eq. (5), we have

$$w_i(x) = \overline{g}_i(x) = \sum_{k=0}^{m_i-1}\overline{\zeta}_i^{2^k} \prod_{0 \leq j \leq m_i-1, j \neq k}(x - \overline{\zeta}_i^{2^j}) \in \mathbb{F}_2[x],$$

where $\overline{\zeta}_i$ is a root of the monic irreducible polynomial $\overline{f}_i(x)$ in the finite field $\overline{\Gamma}_i$ satisfying $\overline{\zeta}_i^{2^{m_i}-1} = 1$ by Lemma 2(i). For any integer t, $0 \leq t \leq m_i - 1$, we see that $w_i(\overline{\zeta}_i^{2^t}) =$

$\overline{\zeta}_i^{2^t} \prod_{0\leq j\leq m_i-1, j\neq t}(\overline{\zeta}_i^{2^t} - \overline{\zeta}_i^{2^j}) \neq 0$, since $\overline{\zeta}_i, \overline{\zeta}_i^2, \ldots, \overline{\zeta}_i^{2^{m_i-1}}$ are all distinct roots of $\overline{f}_i(x)$ in the finite field $\overline{\Gamma}_i$. From this, we deduce that $w_i(x)$ and $\overline{f}_i(x)$ are coprime polynomials in $\mathbb{F}_2[x]$. This implies that $w_i(x)$ is an invertible element of the finite field $\frac{\mathbb{F}_2[x]}{\langle \overline{f}_i(x)\rangle}$. From this and since $\deg(w_i(x)) \leq \deg(g_i(x)) < m_i = \deg(\overline{f}_i(x))$, we deduce that $w_i(x) \neq 0$. □

Remark 2 The proof the this lemma depends heavily on Lemma 2(ii). The premise condition of Lemma 2(ii) is that $f_i(x)$ is monic basic irreducible, $f_i(x)$ is a divisor of $x^n - 1$ in $\mathbb{Z}_4[x]$ and n is odd. If this prerequisite is not met, the conclusion does not necessarily hold. For example, let $f(x) = x^3 + x + 1 \in \mathbb{Z}_4[x]$. It is clear that $f(x)$ is monic basic irreducible in $\mathbb{Z}_4[x]$. But

$$g(x) = \frac{(x^3+x+1)^2 - (x^6+x^2+1)}{2(x^3+x+1)} = \frac{x^4+x^3+x}{x^3+x+1} \notin \mathbb{Z}_4[x].$$

In fact, we notice that $x^3 + x + 1$ is a divisor of $x^{14} - 1$ but it is not a divisor of $x^7 - 1$ in $\mathbb{Z}_4[x]$. Hence there is no odd positive integer n such that $(x^3 + x + 1) \mid (x^n - 1)$ in $\mathbb{Z}_4[x]$.

We can now state the proof of Theorem 1.

Proof By Proposition 2, we need to first prove that all distinct ideals of the ring $\mathcal{K}_i$ are given by the table in Theorem 1.

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

$$\tau : a(x) \mapsto \tau(a(x)) = a_0(x) = \overline{a}(x) \ (\text{mod } \overline{f}_i(x^2) = \overline{f}_i(x)^2),$$

for all $a(x) = a_0(x) + 2a_1(x) \in \mathcal{K}_i$ with $a_0(x), a_1(x) \in \overline{\mathcal{K}}_i$ (see Lemma 4).

Let C be an ideal of $\mathcal{K}_i$, and denote by $\tau|_C$ the restriction of τ to the ideal C of $\mathcal{K}_i$. Then $\tau|_C$ is a surjective ring homomorphism from C onto $\tau(C) = \{\tau(c(x)) \mid c(x) \in C\}$. This implies $\tau(C) \cong C/\ker(\tau|_C)$ where $\ker(\tau|_C) = \{c(x) \in C \mid \tau(c(x)) = 0\}$ is the kernel of $\tau|_C$. Therefore, $|C| = |\tau(C)||\ker(\tau|_C)|$.

Let $(C : 2) = \{a(x) \in \mathcal{K}_i \mid 2a(x) \in C\}$. Then $(C : 2)$ is an ideal of $\mathcal{K}_i$ satisfying $C \subseteq (C : 2)$. Since τ is a surjective ring homomorphism, both $\tau(C)$ and $\tau(C : 2)$ are ideals of $\overline{\mathcal{K}}_i$. As $\overline{\mathcal{K}}_i$ is a finite chain ring, by Lemma 3(i) there is a unique pair (l, s) of integers, $0 \leq s \leq l \leq 2$, such that

$$\tau(C) = \overline{f}_i(x)^l\overline{\mathcal{K}}_i \text{ and } \tau(C : 2) = \overline{f}_i(x)^s\overline{\mathcal{K}}_i. \tag{6}$$

By the definition of τ and the fact that $2 \cdot 2 = 0$, we have

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

This implies that $|\ker(\tau|_C)| = |\tau(C : 2)|$. From this, by Eq. (6) and Lemma 3(iii), we deduce that

$$|C| = |\tau(C)||\tau(C : 2)| = 2^{m_i(2-l)} \cdot 2^{m_i(2-s)} = 2^{m_i(4-(l+s))}. \tag{7}$$

Then, since $0 \leq s \leq l \leq 2$, we have the following six cases:

Case 1. $s = l = 2$.

By Eq. (7), we have $|C| = 1$, and hence $C = \langle 0\rangle$.

Case 2. $s = l = 0$.

By Eq. (7), we have that $|C| = 2^{4m_i} = 4^{2m_i} = |\mathcal{K}_i|$. Hence $C = \mathcal{K}_i = \langle 1\rangle$. Then, by the definition of $\mathcal{K}_i$ in Sect. 2, we have that $C = \{\sum_{j=0}^{2m_i-1} a_j x^j \mid a_j \in \mathbb{Z}_4,\ j = 0, 1, \ldots, 2m_i - 1\}$ and C is of type $4^{2m_i}2^0$.

Case 3. $l = 2$ and $s = 0$.

In this case, $\tau(C) = \overline{f}_i(x)^2\overline{\mathcal{K}}_i = \{0\}$ and $\tau(C : 2) = \overline{f}_i(x)^0\overline{\mathcal{K}}_i = \overline{\mathcal{K}}_i$ by Eq. (6). Then by Lemma 4 and the definition of τ, we see that $C = 2\overline{\mathcal{K}}_i = \langle 2\rangle$ and $C = \{2\sum_{t=0}^{2m_i-1} b_t x^t \mid b_t \in \{0, 1\},\ t = 0, 1, \ldots, 2m_i - 1\}$. Hence C is of type $4^0 2^{2m_i}$ and $|C| = 2^{2m_i}$.

Case 4. $l = 2$ and $s = 1$.

In this case, $\tau(C) = \{0\}$ and $\tau(C : 2) = \overline{f}_i(x)^1\overline{\mathcal{K}}_i = \overline{f}_i(x)\overline{\mathcal{K}}_i$ by Eq. (6). Then by Lemma 4 and the definition of τ, we have that $C = 2\overline{f}_i(x)\overline{\mathcal{K}}_i = \langle 2\overline{f}_i(x)\rangle$ and $C = \{2\sum_{t=0}^{m_i-1} b_t x^t \overline{f}_i(x) \mid b_t \in \{0, 1\},\ t = 0, 1, 2, \ldots, 2m_i - 1\}$. Hence C is of type $4^0 2^{m_i}$ and $|C| = 2^{m_i}$.

Case 5. $l = 1$ and $s = 0$.

In this case, $\tau(C) = \overline{f}_i(x)^1\overline{\mathcal{K}}_i = \overline{f}_i(x)\overline{\mathcal{K}_i}$ and $\tau(C : 2) = \overline{\mathcal{K}}_i$ by Eq. (6). The latter implies $2 \in C$ and the former implies $f_i(x) + 2v(x) \in C$ for some $v(x) \in \mathcal{K}_i$. From this, we deduce that $f_i(x) = (f_i(x) + 2v(x)) - 2 \cdot v(x) \in C$. Hence $\langle f_i(x), 2\rangle \subseteq C$.

Conversely, let $c(x) \in C$. By $\overline{c}(x) \in \tau(C) = \overline{f}_i(x)\overline{\mathcal{K}_i}$, there exist $a(x), b(x) \in \mathcal{K}_i$ such that $c(x) = a(x)f_i(x) + 2b(x) = a(x) \cdot f_i(x) + 2 \cdot b(x) \in \langle f_i(x), 2\rangle$. Therefore, we have $C = \langle f_i(x), 2\rangle$, and $|C| = 2^{3m_i}$ by Eq. (7).

By Lemma 5, we have that $f_i(x)^2 = 2\overline{f}_i(x)w_i(x) \equiv 0 \pmod{C}$. From this and since $C = \langle f_i(x), 2\rangle = f_i(x)\mathcal{K}_i + 2\overline{\mathcal{K}}_i$, we deduce that

$$C = \left\{ \sum_{j=0}^{m_i-1} a_j x^j f_i(x) + 2\sum_{t=0}^{m_i-1} b_t x^t \mid a_j \in \mathbb{Z}_4,\ b_t \in \{0, 1\},\ j, t = 0, 1, \ldots, m_i - 1 \right\}.$$

Hence C is of type $4^{m_i}2^{m_i}$.

Case 6. $l = s = 1$.

In this case, $|C| = 2^{2m_i}$ by Eq. (7). Then by Eq. (6), we have $\tau(C) = \overline{f}_i(x)\overline{\mathcal{K}}_i$ and $\tau(C : 2) = \overline{f}_i(x)\overline{\mathcal{K}}_i$. The latter implies $2\overline{f}_i(x) \in C$ and the former implies $f_i(x) + 2v(x) \in C$ for some $v(x) \in \mathcal{K}_i$. By Lemma 4, there is a unique pair $(a(x), b(x))$ of elements in $\overline{\mathcal{K}}_i$ such that $v(x) = a(x) + 2b(x)$. From this, we deduce that $f_i(x) + 2v(x) = f_i(x) + 2(a(x) + 2b(x)) = f_i(x) + 2a(x)$. As $a(x) \in \overline{\mathcal{K}}_i$, by Lemma 3 (ii) there is a unique pair $(h(x), q(x))$ of elements in $\mathcal{T}_i$ such that $a(x) = h(x) + q(x)\overline{f}_i(x)$. Therefore,

$$f_i(x) + 2h(x) = \big(f_i(x) + 2(h(x) + q(x)\overline{f}_i(x))\big) - q(x) \cdot 2\overline{f}_i(x) \in C.$$

This implies that $\langle f_i(x) + 2h(x)\rangle \subseteq C$.

Conversely, let $c(x) \in C$. Since $\overline{c}(x) \in \tau(C) = \overline{f}_i(x)\overline{\mathcal{K}}_i$, there exist $a(x), b(x) \in \mathcal{K}_i$ such that $c(x) = a(x)f_i(x) + 2b(x) = a(x) \cdot (f_i(x) + 2h(x)) + 2d(x)$, where $d(x) = b(x) - a(x)h(x) \in \mathcal{K}_i$ satisfying

$$2d(x) = c(x) - a(x) \cdot (f_i(x) + 2h(x)) \in C,$$

i.e., $d(x) \in (C : 2)$. This implies that $\overline{d}(x) \in \tau(C : 2) = \overline{f}_i(x)\overline{\mathcal{K}}_i$. Hence there exist $u(x), v(x) \in \mathcal{K}_i$ such that $d(x) = u(x)f_i(x) + 2v(x)$. Therefore, we have

$$\begin{aligned} c(x) &= a(x) \cdot (f_i(x) + 2h(x)) + 2(u(x)f_i(x) + 2v(x)) \\ &= a(x) \cdot (f_i(x) + 2h(x)) + 2\overline{u}(x) \cdot \overline{f}_i(x) \\ &= a(x) \cdot (f_i(x) + 2h(x)) + 2\overline{u}(x) \cdot \overline{(f_i(x) + 2h(x))} \\ &= a(x) \cdot (f_i(x) + 2h(x)) + 2\overline{u}(x) \cdot (f_i(x) + 2h(x)) \\ &= (a(x) + 2\overline{u}(x)) \cdot (f_i(x) + 2h(x)) \in \langle f_i(x) + 2h(x)\rangle. \end{aligned}$$

It follows that $C = \langle f_i(x) + 2h(x)\rangle$, where $h(x) \in \mathcal{T}_i$.

By $2\overline{f}_i(x) \in C$ and Lemma 5, we have that $f_i(x)^2 = 2\overline{f}_i(x)w_i(x) \equiv 0 \pmod{C}$. From this, we deduce that

$$\begin{aligned} C &= (f_i(x) + 2h(x))\mathcal{K}_i \\ &= \left\{ \sum_{j=0}^{m_i-1} a_j x^j (f_i(x) + 2h(x)) \mid a_j \in \mathbb{Z}_4,\ j = 0, 1, \ldots, m_i - 1 \right\}. \end{aligned}$$

Hence C is of type $4^{m_i}2^0$.

As stated above, we conclude that all distinct ideals of $\mathcal{K}_i$ are given by the table in Theorem 1.

Now, let $\mathcal{M}_i$ be the set of all ideals in $\mathcal{K}_i$ listed in the table of Theorem 1 and $C_i \in \mathcal{M}_i$. It is clear that $\mathrm{Ann}(C_i) = D_i$, where $D_i \in \mathcal{M}_i$ satisfies the following conditions:

$$C_i \cdot D_i = \{0\} \text{ and } |D_i| = \mathrm{Max}\{|J| \mid C_i \cdot J = \{0\},\ J \in \mathcal{M}_i\}.$$

Then the conclusion for each $\mathrm{Ann}(C_i)$ follows from Lemma 5 and a direct calculation.

Finally, by Lemma 1(iii) we see that $\phi_i|_{C_i}$ is an isomorphism of abelian groups from the ideal C_i of $\mathcal{K}_i$ onto the subcode code $\mathcal{C}_i$ of $\mathcal{C}$. Then the conclusion for the type and an encoder of $\mathcal{C}_i$ follows immediately from the fact that $\mathcal{C}_i = \theta_i(x)C_i$. This concludes the proof of Theorem 1. □

4 Dual codes of cyclic codes over $\mathbb{Z}_4$ of length 2*n*

In this section, we determine the dual code of each cyclic code over $\mathbb{Z}_4$ of length $2n$.

For any $a = (a_0, a_1, \ldots, a_{2n-1}) \in \mathbb{Z}_4^{2n}$, we will identify a with $a(x) = \sum_{j=0}^{2n-1} a_j x^j \in \mathcal{A} = \mathbb{Z}_4[x]/\langle x^{2n} - 1\rangle$. In the ring $\mathcal{A}$, we have that $x^{2n} = 1$, and hence $x^{-1} = x^{2n-1}$. Moreover, we have $x^{2n} \equiv 1 \pmod{f_i(x^2)}$ since $f_i(x^2)$ is a divisor of $x^{2n} - 1$ in $\mathbb{Z}_4[x]$. This implies that $x^{2n} = 1$ and $x^{-1} = x^{2n-1}$ in the ring $\mathcal{K}_i = \mathbb{Z}_4[x]/\langle f_i(x^2)\rangle$ for all i. Define

$$\mu(a(x)) = a(x^{-1}) = a_0 + \sum_{j=1}^{2n-1} a_j x^{2n-j},\ \forall a(x) \in \mathcal{A}.$$

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

Lemma 6 *Let* $a, b \in \mathbb{Z}_4^{2n}$ *where* $b = (b_0, b_1, \ldots, b_{2n-1})$. *Then* $[a, b] = 0$ *if* $a(x)\mu(b(x)) = 0$ *in the ring* $\mathcal{A}$ *where* $b(x) = \sum_{j=0}^{2n-1} b_j x^j$.

For any polynomial $f(y) = \sum_{j=0}^{d} c_j y^j \in \mathbb{Z}_4[y]$ of degree $d \geq 1$, recall that the *reciprocal polynomial* of $f(y)$ is defined as $\widetilde{f}(y) = \widetilde{f(y)} = y^d f(\frac{1}{y}) = \sum_{j=0}^{d} c_j y^{d-j}$, and $f(y)$ is said to be *self-reciprocal* if $\widetilde{f}(y) = \delta f(y)$ for some $\delta \in \mathbb{Z}_4^{\times} = \{1, -1\}$. 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 $f(0), g(0) \in \mathbb{Z}_4^{\times}$. Then by Eq. (1) in Sect. 2, we have

$$y^n - 1 = -(1 - y^n) = -(\widetilde{y^n - 1}) = -\widetilde{f}_1(y)\widetilde{f}_2(y)\ldots\widetilde{f}_r(y).$$

Since $f_1(y), f_2(y), \ldots, f_r(y)$ are pairwise coprime monic basic irreducible polynomials in $\mathbb{Z}_4[y]$, $\widetilde{f}_1(y), \widetilde{f}_2(y), \ldots, \widetilde{f}_r(y)$ are pairwise coprime basic irreducible polynomials in $\mathbb{Z}_4[y]$ as well. Hence, for each integer i, $1 \leq i \leq r$, there is a unique integer i', $1 \leq i' \leq r$, such that $\widetilde{f}_i(y) = \delta_i f_{i'}(y)$ where $\delta_i \in \{1, -1\}$.

Assume that $f_i(y) = \sum_{j=0}^{m_i} c_j y^j$ where $c_j \in \mathbb{Z}_4$. Then $\deg(f_i(x^2)) = 2\deg(f_i(y)) = 2m_i$ and

$$x^{2m_i} f_i(x^{-2}) = (x^2)^{m_i} \sum_{j=0}^{m_i} c_j (x^2)^{-j} = \sum_{j=0}^{m_i} c_j (x^2)^{m_i - j} = \widetilde{f}_i(x^2) = \delta_i f_{i'}(x^2).$$

Then by Eq. (3) in Sect. 2 and $x^{2n} = 1$ in $\mathcal{A}$, we obtain

$$\begin{aligned}\mu(\theta_i(x)) &= 1 - x^{2n-2(\deg(v_i(y))+m_i)}(x^{2\deg(v_i(y))} v_i(x^{-2}))(x^{2m_i} f_i(x^{-2}))\\ &= 1 - x^{2n-2(\deg(v_i(y))+m_i)} \widetilde{v}_i(x^2)\widetilde{f}_i(x^2)\\ &= 1 - h_i(x) f_{i'}(x^2),\end{aligned}$$

where $h_i(x) = \delta_i x^{2n-2(\deg(v_i(y))+m_i)} \widetilde{v}_i(x^2) \in \mathcal{A}$. Similarly, by Eq. (3), it follows that $\mu(\theta_i(x)) = g_i(x) F_{i'}(x^2)$ for some $g_i(x) \in \mathcal{A}$. Then from these and Eq. (3), we deduce that $\mu(\theta_i(x)) = \theta_{i'}(x)$.

As stated above, we see that, for each $1 \leq i \leq r$, there is a unique integer i', $1 \leq i' \leq r$, such that $\mu(\theta_i(x)) = \theta_{i'}(x)$. We continue the use of μ to denote this map $i \mapsto i'$; i.e., $\mu(\theta_i(x)) = \theta_{\mu(i)}(x)$.

Whether μ denotes the automorphism of $\mathcal{A}$ or this map on the set $\{1, \ldots, r\}$ is determined by the context.

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

(i) *The map μ is a permutation on $\{1, \ldots, r\}$ satisfying $\mu^{-1} = \mu$.*

(ii) *After a rearrangement of $\theta_1(x), \ldots, \theta_r(x)$, there are integers λ, ϵ such that $\mu(i) = i$ for all $i = 1, \ldots, \lambda$ and $\mu(\lambda + j) = \lambda + \epsilon + j$ for all $j = 1, \ldots, \epsilon$, where $\lambda \geq 1, \epsilon \geq 0$ and $\lambda + 2\epsilon = r$.*

(iii) *For each integer i, $1 \leq i \leq r$, there is a unique element $\delta_i \in \{1, -1\}$ such that $\widetilde{f}_i(x) = \delta_i f_{\mu(i)}(x)$.*

(iv) *For any integer i, $1 \leq i \leq r$, $\mu(\theta_i(x)) = \theta_{\mu(i)}(x)$ in the ring $\mathcal{A}$, and $\mu(\mathcal{A}_i) = \mathcal{A}_{\mu(i)}$.*

(v) *Let $\mu|_{\mathcal{A}_i} : \mathcal{A}_i \to \mathcal{A}_{\mu(i)}$ be the restriction of μ on $\mathcal{A}_i$, and define*

$$\mu_i(c(x)) = c(x^{-1}) = c(x^{2n-1}) \left(\bmod f_{\mu(i)}(x^2)\right), \ \forall c(x) \in \mathcal{K}_i.$$

Then $\mu_i = \phi_{\mu(i)}^{-1} \mu|_{\mathcal{A}_i} \phi_i$, which is a ring isomorphism from $\mathcal{K}_i$ onto $\mathcal{K}_{\mu(i)}$. Moreover, we have $\mu_i^{-1} = \mu_{\mu(i)}$ where $\mu_{\mu(i)} : \mathcal{K}_{\mu(i)} \to \mathcal{K}_i$ is defined by $\mu_{\mu(i)}(a(x)) = a(x^{-1}) = a(x^{2n-1}) \pmod{f_i(x^2)}$ for all $a(x) \in \mathcal{K}_{\mu(i)}$.

Proof Statements (i)–(iii) follow from the definition of the map μ.

(iv) Since $\mu(\theta_i(x)) = \theta_{\mu(i)}(x)$ and $\mathcal{A}_i = \theta_i(x)\mathcal{A}$, it follows that $\mu(\mathcal{A}_i) = \mu(\theta_i(x))\mu(\mathcal{A}) = \theta_{\mu(i)}(x)\mathcal{A} = \mathcal{A}_{\mu(i)}$.

(v) Let $c(x) \in \mathcal{K}_i$. By Lemma 1(iii) and $\theta_{\mu(i)}(x) = \mu(\theta_i(x)) = 1 - h_i(x)f_{i'}(x^2) = 1 - h_i(x)f_{\mu(i)}(x^2)$, we have

$$\begin{aligned}\left(\phi_{\mu(i)}^{-1}\mu|_{\mathcal{A}_i}\phi_i\right)(c(x)) &= (\phi_{\mu(i)}^{-1}\mu|_{\mathcal{A}_i})(\theta_i(x)c(x)) = \phi_{\mu(i)}^{-1}\left(\mu(\theta_i(x))c(x^{-1})\right)\\ &= \left(1 - h_i(x)f_{\mu(i)}(x^2)\right)c(x^{-1}) \pmod{f_{\mu(i)}(x^2)}\\ &\equiv c(x^{-1}) \pmod{f_{\mu(i)}(x^2)}.\end{aligned}$$

This implies $\mu_i(c(x)) = \left(\phi_{\mu(i)}^{-1}\mu|_{\mathcal{A}_i}\phi_i\right)(c(x))$ for all $c(x) \in \mathcal{K}_i$. Hence $\mu_i = \phi_{\mu(i)}^{-1}\mu|_{\mathcal{A}_i}\phi_i$, which is a ring isomorphism from $\mathcal{K}_i$ onto $\mathcal{K}_{\mu(i)}$ by (iv) and Lemma 1(iii).

Finally, $\mu_i^{-1} = \mu_{\mu(i)}$ follows from the definition of μ_i for any i. □

Lemma 8 *Let $a(x) = \sum_{i=1}^{r}\theta_i(x)\xi_i, b(x) = \sum_{i=1}^{r}\theta_i(x)\eta_i \in \mathcal{A}$, where $\xi_i, \eta_i \in \mathcal{K}_i$. Then $a(x)\mu(b(x)) = \sum_{i=1}^{r}\theta_i(x)(\xi_i \cdot \mu_i^{-1}(\eta_{\mu(i)}))$.*

Proof As $\mu_i^{-1}(\eta_{\mu(i)}) \in \mu_i^{-1}(\mathcal{K}_{\mu(i)}) = \mathcal{K}_i$ by Lemma 7(v), it follows that $\xi_i \cdot \mu_i^{-1}(\eta_{\mu(i)}) \in \mathcal{K}_i$ for all i. If $j \neq \mu(i)$, then $i \neq \mu(j)$ by Lemma 7(i). This implies $\theta_i(x)\theta_{\mu(j)}(x) = 0$ in the ring $\mathcal{A}$ by Lemma 1(i). Therefore,

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

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

Now, we give the dual code of each cyclic code over $\mathbb{Z}_4$ of length $2n$.

Theorem 2 *Let $\mathcal{C}$ be a cyclic code over $\mathbb{Z}_4$ of length $2n$ with canonical form decomposition $\mathcal{C} = \bigoplus_{i=1}^{r}\theta_i(x)C_i$, where C_i is an ideal of $\mathcal{K}_i$. Then the dual code of $\mathcal{C}$ is given by $\mathcal{C}^{\perp} = \bigoplus_{j=1}^{r}\theta_j(x)D_j$, where, for $j = \mu(i)$, D_j is an ideal of $\mathcal{K}_j$ given by the following table.*

Case	$C_i \pmod{f_i(x^2)}$	$D_{\mu(i)} \pmod{f_{\mu(i)}(x^2)}$
1.	$\langle 0\rangle$	$\langle 1\rangle$
2.	$\langle 1\rangle$	$\langle 0\rangle$
3.	$\langle 2\rangle$	$\langle 2\rangle$
4.	$\langle 2\overline{f}_i(x)\rangle$	$\langle f_{\mu(i)}(x), 2\rangle$
5.	$\langle f_i(x), 2\rangle$	$\langle 2\overline{f}_{\mu(i)}(x)\rangle$
6.	$\langle f_i(x) + 2h(x)\rangle$	$\langle f_{\mu(i)}(x) + 2x^{m_i}\left(w_i(x^{-1}) + h(x^{-1})\right)\rangle$

where $h(x) \in \mathcal{T}_i$.

Proof Let $\mathcal{D} = \bigoplus_{i=1}^{r}\theta_{\mu(i)}(x)D_{\mu(i)} = \sum_{j=1}^{r}\theta_j(x)D_j \pmod{x^{2n}-1}$, where $D_{\mu(i)} = \mu_i(\mathrm{Ann}(C_i))$ and $\mathrm{Ann}(C_i)$ is given by Theorem 1 for all $i = 1, \ldots, r$. Then $\mathcal{D}$ is a cyclic code over $\mathbb{Z}_4$ of length $2n$ by Theorem 1, and satisfies

$$\mathcal{C} \cdot \mu(\mathcal{D}) = \sum_{i=1}^{r}\theta_i(x)\left(C_i \cdot \mu_i^{-1}(D_{\mu(i)})\right) = \sum_{i=1}^{r}\theta_i(x)\left(C_i \cdot \mathrm{Ann}(C_i)\right) = \{0\}$$

by Lemma 8. From this and by Lemma 6, we deduce that $\mathcal{D} \subseteq \mathcal{C}^{\perp}$. On the other hand, by Theorem 1 we have $|C_i||\mathrm{Ann}(C_i)| = 2^{4m_i}$ for all $i = 1, \ldots, r$. This implies

$$|\mathcal{C}||\mathcal{D}| = \left(\prod_{i=1}^{r}|C_i|\right)\left(\prod_{i=1}^{r}|D_{\mu(i)}|\right) = \prod_{i=1}^{r}(|C_i||\mathrm{Ann}(C_i)|) = 2^{4\sum_{i=1}^{r}m_i} = |\mathbb{Z}_4|^{2n}$$

by Theorem 1 and $\sum_{i=1}^{r}m_i = n$. Then, from the theory of linear codes over $\mathbb{Z}_4$, we deduce that $\mathcal{C}^{\perp} = \mathcal{D}$.

Finally, we give the precise expression of $D_{\mu(i)} = \mu_i(\mathrm{Ann}(C_i))$, $1 \leq i \leq r$. Obviously, we only need to consider Cases 4–6 in the table of Theorem 1.

By $x^{2n} = 1$ in $\mathcal{K}_i$, we see that $x \in \mathcal{K}_i^{\times}$, for all $i = 1, 2, ..., r$. By Lemma 7(iii), we have $\widetilde{f_i}(x) = \delta_i f_{\mu(i)}(x)$ where $\delta_i \in \{1, -1\}$. Then, by the definition of μ_i, we have

$$\mu_i(f_i(x)) = f_i(x^{-1}) = x^{-m_i}(x^{m_i}f_i(x^{-1})) = x^{-m_i}(\widetilde{f_i}(x)) = \delta_i x^{-m_i}f_{\mu(i)}(x).$$

Case 4: As x is an invertible element of $\mathcal{K}_{\mu(i)}$, we have

$$D_{\mu(i)} = \mu_i(\langle f_i(x), 2\rangle) = \langle \mu_i(f_i(x), \mu_i(2)\rangle = \langle \delta_i x^{-m_i}f_{\mu(i)}(x), 2\rangle = \langle f_{\mu(i)}(x), 2\rangle.$$

Case 5: By $2\overline{f}_i(x) = 2f_i(x)$ in $\mathcal{K}_i$, we have

$$D_{\mu(i)} = \mu_i(\langle 2\overline{f}_i(x)\rangle) = \langle 2\mu_i(f_i(x))\rangle = \langle 2\delta_i x^{-m_i}f_{\mu(i)}(x)\rangle = \langle 2\overline{f}_{\mu(i)}(x)\rangle.$$

Case 6: By $2\delta_i^{-1} = 2$, we have that

$$\begin{aligned} D_{\mu(i)} &= \mu_i(\langle f_i(x) + 2(w_i(x) + h(x))\rangle) = \langle \mu_i(f_i(x) + 2(w_i(x) + h(x)))\rangle \\ &= \langle \delta_i x^{-m_i}f_{\mu(i)}(x) + 2(w_i(x^{-1}) + h(x^{-1}))\rangle \\ &= \langle f_{\mu(i)}(x) + 2x^{m_i}(w_i(x^{-1}) + h(x^{-1}))\rangle \pmod{f_{\mu(i)}(x^2)} \end{aligned}$$

in the ring $\mathcal{K}_{\mu(i)}$. □

5 Self-dual cyclic codes over $\mathbb{Z}_4$ of length $2n$

In this section, we list all distinct self-dual cyclic codes over $\mathbb{Z}_4$ of length $2n$ explicitly.

We assume $f_1(x) = x - 1$. Let i be a positive integer with $2 \leq i \leq \lambda$. Since n is odd, by Lemma 7(ii) and (iii) we know that $\overline{f}_i(x)$ is a self-reciprocal and irreducible polynomial in $\mathbb{F}_2[x]$. It is well known that the degree of m_i must be even and $x^{-1} \equiv x^{2^{\frac{m_i}{2}}} \pmod{\overline{f}_i(x)}$. This implies that $x^{2^{\frac{m_i}{2}}+1} \equiv 1 \pmod{\overline{f}_i(x)}$.

Lemma 9 *Let $2 \leq i \leq \lambda$ and write $m_i = 2d_i$ where d_i is a positive integer. Let $\overline{\Gamma}_i = \mathbb{F}_2[x]/\langle\overline{f}_i(x)\rangle$ as in Sect. 3 and set*

$$\mathcal{F}_i = \{\xi \in \overline{\Gamma}_i \mid \xi^{2^{d_i}} = \xi\}.$$

Then we have the following conclusions.

(i) We have that $\overline{\Gamma}_i$ is a finite field of cardinality $2^{m_i} = (2^{d_i})^2$ and $x^{-1} = x^{2^{\frac{m_i}{2}}}$ in $\overline{\Gamma}_i$.

(ii) The field $\mathcal{F}_i$ is a subfield of $\overline{\Gamma}_i$ of cardinality $2^{d_i} = 2^{\frac{m_i}{2}}$.

(iii) (cf. [26, Corollary 7.17]) Let $\mathrm{Tr}_{\overline{\Gamma}_i/\mathcal{F}_i}$ be the trace function from $\overline{\Gamma}_i$ onto $\mathcal{F}_i$ defined by

$$\mathrm{Tr}_{\overline{\Gamma}_i/\mathcal{F}_i}(\xi) = \xi + \xi^{2^{d_i}}, \ \xi \in \overline{\Gamma}_i.$$

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

(iv) Let $w_i(x)$ be given by Lemma 5. Then $x^{m_i} w_i(x^{-1}) = w_i(x)$ in $\mathbb{F}_2[x]$, and hence $x^{\frac{m_i}{2}} w_i(x^{-1}) \in \mathcal{F}_i$.

(v) The set of solutions in $\mathcal{T}_i = \{\sum_{j=0}^{m_i-1} a_j x^j \mid a_j \in \{0,1\}, j = 0,1,2,\ldots,m_i-1\}$ for the following congruence:

$$h(x) \equiv x^{m_i}\left(w_i(x^{-1}) + h(x^{-1})\right) \pmod{\langle \overline{f}_i(x), 2\rangle} \tag{8}$$

is given by

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

i.e., $\mathcal{W}_i = x^{\frac{m_i}{2}}\mathrm{Tr}^{-1}_{\overline{\Gamma}_i/\mathcal{F}_i}(x^{\frac{m_i}{2}} w_i(x^{-1}))$, and hence $|\mathcal{W}_i| = 2^{\frac{m_i}{2}}$.

Proof Statements (i) and (ii) follow from the classical theory of finite fields (cf. [26, Chap. 6]).

(iv) Using the notation in Sects. 2 and 3, we view $\mathcal{T}_i$ as the same as $\overline{\Gamma}_i$. As $f_i(x)$ is self-reciprocal and $w_i(x) \equiv \frac{f_i(x)^2 - f_i(x^2)}{2f_i(x)}$ mod $\langle \overline{f}_i(x), 2\rangle$, since $f_i(x^{-1}) = \delta_i x^{-m_i} f_i(x)$ and $\delta_i \equiv 1 \pmod 2$ we have that $w_i(x^{-1}) = x^{-m_i} w_i(x)$. This implies that

$$x^{m_i} w_i(x^{-1}) = w_i(x) \text{ in } \mathbb{F}_2[x].$$

From this and by (i), we deduce that

$$(x^{\frac{m_i}{2}} w_i(x^{-1}))^{2^{d_i}} = x^{-\frac{m_i}{2}} w_i(x) = x^{\frac{m_i}{2}} w_i(x^{-1}) \text{ in } \overline{\Gamma}_i.$$

We conclude that $x^{\frac{m_i}{2}} w_i(x^{-1}) \in \mathcal{F}_i$.

(v) As $x \in \overline{\Gamma}_i^{\times}$, we can multiply both sides of Eq. (8) by $x^{-\frac{m_i}{2}}$. Then Eq. (8) is equivalent to

$$x^{-\frac{m_i}{2}} h(x) + x^{\frac{m_i}{2}} h(x^{-1}) = x^{\frac{m_i}{2}} w_i(x^{-1}) \text{ in } \overline{\Gamma}_i.$$

Set $\xi(x) = x^{-\frac{m_i}{2}} h(x) \in \overline{\Gamma}_i$. Then by (i) we have $\xi(x)^{2^{d_i}} = (x^{-\frac{m_i}{2}} h(x))^{2^{d_i}} = x^{\frac{m_i}{2}} h(x^{-1})$. Hence Eq. (8) is equivalent to

$$\xi(x) + \xi(x)^{2^{d_i}} = x^{\frac{m_i}{2}} w_i(x^{-1}), \ \text{i.e.,} \mathrm{Tr}_{\overline{\Gamma}_i/\mathcal{F}_i}(\xi(x)) = x^{\frac{m_i}{2}} w_i(x^{-1}) \in \mathcal{F}_i, \tag{9}$$

and $h(x) = x^{\frac{m_i}{2}}\xi(x) \pmod{\overline{f}_i(x)}$. Therefore, $\mathcal{W}_i$ is the set of all solutions in $\mathcal{T}_i$ for Eq. (8), and $|\mathcal{W}_i| = |\mathrm{Tr}^{-1}_{\overline{\Gamma}_i/\mathcal{F}_i}(x^{\frac{m_i}{2}} w_i(x^{-1}))| = 2^{\frac{m_i}{2}}$ by (iii). □

Finally, by Proposition 2, Lemma 9, and Theorems 2 and 1 , we can list all distinct self-dual cyclic codes over $\mathbb{Z}_4$ of length $2n$.

Theorem 3 *Using the notation in Theorem 2, Lemma 7(ii) and Lemma 9, let $\mathcal{C}$ be a cyclic code over $\mathbb{Z}_4$ of length $2n$ with canonical form decomposition $\mathcal{C} = \bigoplus_{i=1}^{r} \theta_i(x)C_i$, where C_i is an ideal of $\mathcal{K}_i$. Then $\mathcal{C}$ is self-dual if and only if, for each integer i, $1 \le i \le r$, C_i satisfies one of the following conditions:*

(i) $C_1 = \langle 2 \rangle$.

(ii) If $2 \le i \le \lambda$, C_i is given by one of the following $1 + 2^{\frac{m_i}{2}}$ cases: $C_i = \langle 2 \rangle$, *and* $C_i = \langle f_i(x) + 2h(x) \rangle$ *where* $h(x) \in \mathcal{W}_i$ *arbitrary.*

(iii) If $i = \lambda + j$ where $1 \le j \le \epsilon$, $(C_i, C_{i+\epsilon})$ is given by the following table.

$C_i \pmod{f_i(x^2)}$	$C_{i+\epsilon} \pmod{f_{i+\epsilon}(x^2)}$
$\langle 0 \rangle$	$\langle 1 \rangle$
$\langle 1 \rangle$	$\langle 0 \rangle$
$\langle 2 \rangle$	$\langle 2 \rangle$
$\langle 2\overline{f}_i(x) \rangle$	$\langle f_{i+\epsilon}(x), 2 \rangle$
$\langle f_i(x), 2 \rangle$	$\langle 2\overline{f}_{i+\epsilon}(x) \rangle$
$\langle f_i(x) + 2h(x) \rangle \;\; (h(x) \in \mathcal{T}_i)$	$\langle f_{i+\epsilon}(x) + 2x^{m_i}(w_i(x^{-1}) + h(x^{-1})) \rangle$

Therefore, the number of self-dual cyclic codes over $\mathbb{Z}_4$ of length $2n$ is

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

Proof By Theorems 2 and 1, we see that $\mathcal{C}$ is self-dual if and only if the ideal C_i of $\mathcal{K}_i$ satisfies $C_i = D_i$ for all $i = 1, \ldots, r$, where D_i is listed in the table of Theorem 2. The latter is equivalent to the statement that C_i satisfies one of the following conditions for all $i = 1, \ldots, r$.

(i) Let $i = 1$. Then $\mu(1) = 1$, $f_1(x) = x - 1$ and $m_i = 1$. By Lemma 5, we have $w_1(x) = 1$, since $w_1(x) \equiv \frac{f_1(x)^2 - f_1(x^2)}{2f_1(x)} \equiv \frac{(x-1)^2 - (x^2-1)}{2(x-1)} \equiv 1 \pmod{\langle \overline{f}_1(x), 2 \rangle}$. Then from $\mathcal{T}_1 = \{0, 1\}$ and $x \equiv 1 \pmod{\overline{f}_1(x)}$, we deduce that $C_1 = \langle 2 \rangle$ is the only ideal of $\mathcal{K}_1$ that satisfies $C_1 = D_1 = D_{\mu(1)}$.

(ii) Let $2 \le i \le \lambda$. Then $\mu(i) = i$. In this case, by Theorem 2, we see that $C_i = D_i = D_{\mu(i)}$ if and only if C_i is given by one of the following two subcases:
$C_i = \langle 2 \rangle$;
$C_i = \langle f_i(x) + 2h(x) \rangle$, where $h(x) \in \mathcal{T}_i$ satisfies Eq. (8), i.e., $h(x) \in \mathcal{W}_i$ by Lemma 9(v).

(iii) Let $i = \lambda + j$ where $1 \le j \le \epsilon$. Then $\mu(i) = i + \epsilon$ and $\mu(i + \epsilon) = i$. Hence $C_i = D_i$ if and only if $C_{i+\epsilon} = C_{\mu(i)} = D_{\mu(i)}$, where $D_{\mu(i)}$ is given by the table in Theorem 2.

By Lemma 9(v) and Theorem 1, we see that the number of self-dual cyclic codes over $\mathbb{Z}_4$ of length $2n$ is $\prod_{2 \le i \le \lambda}(1 + 2^{\frac{m_i}{2}}) \cdot \prod_{j=1}^{\epsilon}(5 + 2^{m_{\lambda+j}})$. □

Finally, we consider how to calculate the number of self-dual cyclic codes over $\mathbb{Z}_4$ of length $2n$ from the odd positive integer n directly. Let $J_1, J_2, \ldots, J_r$ be all the distinct 2-cyclotomic cosets modulo n corresponding to the factorization $x^n - 1 = \overline{f}_1(x)\overline{f}_2(x) \ldots \overline{f}_r(x)$. Then we have $r = \lambda + 2\epsilon$ and

- $J_1 = \{0\}$, the set J_i satisfies $J_i = -J_i \pmod{n}$ and $|J_i| = m_i$ for all $i = 2, \ldots, \lambda$;

- $J_{\lambda+j+\epsilon} = -J_{\lambda+j} \pmod{n}$ and $|J_{\lambda+j}| = |J_{\lambda+j+\epsilon}| = m_{\lambda+j}$, for all $j = 1, \ldots, \epsilon$.

Therefore, the number of self-dual cyclic codes over $\mathbb{Z}_4$ of length $2n$ can be calculated by the formula in Theorem 3 and the 2-cyclotomic cosets modulo n directly. As an example, we list the number $\mathcal{N}$ of self-dual cyclic codes over $\mathbb{Z}_4$ of length $2n$, where n is odd and $6 \leq 2n \leq 98$, in the following table.

$2n$	$\mathcal{N}$	$2n$	$\mathcal{N}$
6	$3 = 1 + 2$	54	$13851 = (1+2)(1+2^3)(1+2^9)$
10	$5 = 1 + 2^2$	58	$16385 = 1 + 2^{14}$
14	$13 = 5 + 2^3$	62	$50653 = (5+2^5)^3$
18	$27 = (1+2)(1+2^3)$	66	$107811 = (1+2)(1+2^5)^3$
22	$33 = 1 + 2^5$	70	$266565 = (1+2^2)(5+2^3)(5+2^{12})$
26	$65 = 1 + 2^6$	74	$262145 = 1 + 2^{18}$
30	$315 = (1+2)(1+2^2)(5+2^4)$	78	$799695 = (1+2)(1+2^6)(5+2^{12})$
34	$289 = (1+2^4)^2$	82	$1050625 = (1+2^{10})^2$
38	$513 = 1 + 2^9$	86	$2146689 = (1+2^7)^3$
42	$2691 = (1+2)(5+2^3)(5+2^6)$	90	11626335
46	$2053 = 5 + 2^{11}$	94	$8388613 = 5 + 2^{23}$
50	$5125 = (1+2^2)(1+2^{10})$	98	$27263041 = (5+2^3)(5+2^{21})$

where $11626335 = (1+2)(1+2^2)(1+2^3)(5+2^4)(5+2^{12})$.

Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_4$-code. The Gray image $\psi(\mathcal{C})$ may or may not be self-dual, and the binary code $\psi(\mathcal{C})$ is called formally self-dual (see p. 43 in Wan [25]). See [11] for a classification of those which are self-dual, for small lengths. Recall that a code is *formally self-dual* if the code and its dual code have the same weight enumerator.

Proposition 3 *Let $\mathcal{C}$ be a cyclic self-dual code over $\mathbb{Z}_4$. If $\psi(\mathcal{C})$ is linear, then $\psi(\mathcal{C})$ is a formally self-dual quasicyclic code of index 2.*

Proof It is proven in [11] that the image is formally-self dual when the preimage is linear and the fact that it is quasicyclic follows from Proposition 1. □

It is possible for a quaternary cyclic self-dual code to produce a binary self-dual quasicyclic code, for example the code generated by $2I_{2n}$ generates such a code.

6 Self-dual cyclic codes over $\mathbb{Z}_4$ of length 30, 6 and 10

In this section, we consider cyclic codes over $\mathbb{Z}_4$ of length 30, 6 and 10, respectively.

$$n = 15$$

We have that $y^{15} - 1 = f_1(y)f_2(y)f_3(y)f_4(y)f_5(y)$, where

$$f_1(y) = y - 1,\ \ f_2(y) = y^2 + y + 1,\ \ f_3(y) = y^4 + y^3 + y^2 + y + 1,$$
$$f_4(y) = y^4 + 2y^2 + 3y + 1 \ \text{ and } \ f_5(y) = y^4 + 3y^3 + 2y^2 + 1 = \widetilde{f}_4(y).$$

Using the notation of Lemma 7 and Sect. 2, we have $r = 5$, $\lambda = 3$, $\epsilon = 1$, $\delta_4 = 1$, $m_1 = 1$, $m_2 = 2$ and $m_3 = m_4 = m_5 = 4$. Hence, there are $\prod_{i=1}^{5}(5 + 2^{m_i}) = (5+2) \cdot (5+2^2) \cdot$

$(5+2^4)^3 = 583443$ distinct cyclic codes over $\mathbb{Z}_4$ of length 30 (cf. [3, Corollary 1] or [13, Theorem 2.6]).

For each $i = 1, 2, 3, 4, 5$, let $F_i(y) = \frac{x^{15}-1}{f_i(y)}$ 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 $\varepsilon_i(y) = u_i(y)F_i(y) \pmod{y^{15}-1}$ and $\theta_i(x) = \varepsilon_i(x^2) \in \mathbb{Z}_4[x]/\langle x^{30}-1\rangle$. Precisely, we have

$$\begin{aligned}
\theta_1(x) &= 3\,x^{28} + 3\,x^{26} + 3\,x^{24} + 3\,x^{22} + 3\,x^{20} + 3\,x^{18} + 3\,x^{16} + 3\,x^{14} + 3\,x^{12} \\
&\quad + 3\,x^{10} + 3\,x^8 + 3\,x^6 + 3\,x^4 + 3\,x^2 + 3, \\
\theta_2(x) &= x^{28} + x^{26} + 2\,x^{24} + x^{22} + x^{20} + 2\,x^{18} + x^{16} + x^{14} + 2\,x^{12} + x^{10} + x^8 \\
&\quad + 2\,x^6 + x^4 + x^2 + 2, \\
\theta_3(x) &= x^{28} + x^{26} + x^{24} + x^{22} + x^{18} + x^{16} + x^{14} + x^{12} + x^8 + x^6 + x^4 + x^2, \\
\theta_4(x) &= x^{24} + 2\,x^{20} + x^{18} + 3\,x^{16} + x^{12} + 2\,x^{10} + 3\,x^8 + x^6 + 3\,x^4 + 3\,x^2, \\
\theta_5(x) &= 3\,x^{28} + 3\,x^{26} + x^{24} + 3\,x^{22} + 2\,x^{20} + x^{18} + 3\,x^{14} + x^{12} + 2\,x^{10} + x^6.
\end{aligned}$$

Using the notation in Sect. 2, we have

$$\begin{aligned}
&\mathcal{K}_1 = \frac{\mathbb{Z}_4[x]}{\langle f_1(x^2)\rangle} = \frac{\mathbb{Z}_4[x]}{\langle x^2-1\rangle}, \mathcal{T}_1 = \{0, 1\}; \\
&\mathcal{K}_2 = \frac{\mathbb{Z}_4[x]}{\langle f_2(x^2)\rangle} \text{ and } \mathcal{T}_2 = \{t_0 + t_1 x \mid t_0, t_1 \in \{0, 1\}\}; \\
&\mathcal{K}_i = \frac{\mathbb{Z}_4[x]}{\langle f_i(x^2)\rangle} \text{ and } \mathcal{T}_i = \{t_0 + t_1 x + t_2 x^2 + t_3 x^3 \mid t_0, t_1, t_2, t_3 \in \{0, 1\}\}, \text{ for } i = 3, 4, 5.
\end{aligned}$$

By Lemma 5, we have

- $w_2(x) = x$, since

$$\begin{aligned}
w_2(x) &\equiv \frac{f_2(x)^2 - f_2(x^2)}{2 f_2(x)} \equiv \frac{(x^2+x+1)^2 - (x^4+x^2+1)}{2(x^2+x+1)} \\
&\equiv x \pmod{\langle \overline{f}_2(x), 2\rangle}.
\end{aligned}$$

Using the notation in Lemma 9(v), we have $x^{\frac{m_2}{2}} w_2(x^{-1}) = 1$, $\overline{\Gamma}_2 = \mathbb{F}_2[x]/\langle \overline{f}_2(x)\rangle = \{0, 1, x, 1+x\}$, $\mathcal{F}_2 = \mathbb{F}_2$ and $\mathrm{Tr}^{-1}_{\overline{\Gamma}_2/\mathbb{F}_2}(1) = \{x, 1+x\}$. Hence,

$$\mathcal{W}_2 = x^{\frac{m_2}{2}} \mathrm{Tr}^{-1}_{\overline{\Gamma}_2/\mathbb{F}_2}(x^{\frac{m_2}{2}} w_2(x^{-1})) = x \cdot \{x, 1+x\} = \{1, 1+x\}.$$

- $w_3(x) = x + x^3$, since

$$\begin{aligned}
w_3(x) &\equiv \frac{f_3(x)^2 - f_3(x^2)}{2 f_3(x)} \\
&\equiv \frac{(x^4+x^3+x^2+x+1)^2 - (x^8+x^6+x^4+x^2+1)}{2(x^4+x^3+x^2+x+1)} \\
&\equiv x + x^3 \pmod{\langle \overline{f}_3(x), 2\rangle}.
\end{aligned}$$

Using the notation in Lemma 9(v), we have that
$x^{\frac{m_3}{2}} w_3(x^{-1}) = x^2 \cdot (x^{-1} + x^{-3}) = x + x^{-1} = x + x^4$,
$\overline{\Gamma}_3 = \mathbb{F}_2[x]/\langle \overline{f}_3(x)\rangle = \{a_0 + a_1 x + a_2 x^2 + a_3 x^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{F}_2\} \pmod{x^4 + x^3 + x^2 + x + 1}$,
$\mathcal{F}_3 = \{\xi \in \overline{\Gamma}_3 \mid \xi^4 = \xi\} = \{0, 1, x + x^4, x^2 + x^3\}$,

$\mathrm{Tr}^{-1}_{\Gamma_3/\mathcal{F}_3}(x+x^4)=\{x,1+x,x^4,1+x^4\}$ and

$$\mathcal{W}_3=x^{\frac{m_3}{2}}\mathrm{Tr}^{-1}_{\Gamma_3/\mathcal{F}_3}(x^{\frac{m_3}{2}}w_3(x^{-1}))=\{x,x+x^2,x^2+x^3,x^3\}.$$

- $w_4(x)=x$, since

$$w_4(x)\equiv\frac{f_4(x)^2-f_4(x^2)}{2f_4(x)}\equiv\frac{(x^4+2x^2+3x+1)^2-(x^8+2x^4+3x^2+1)}{2(x^4+2x^2+3x+1)}$$
$$\equiv x \pmod{\langle \overline{f}_4(x),2\rangle}.$$

By Theorem 3, all the 315 distinct self-dual codes over $\mathbb{Z}_4$ of length 30 are listed by

$$\mathcal{C}=\theta_1(x)C_1\oplus\theta_2(x)C_2\oplus\theta_3(x)C_3\oplus\theta_4(x)C_4\oplus\theta_5(x)C_5,$$

where C_i is an ideal of $\mathcal{K}_i$, $1\leq i\leq 5$, given by the following:

(1) $C_1=\langle 2\rangle$;
(2) $C_2=\langle 2\rangle$, $C_2=\langle f_2(x)+2h(x)\rangle$ where $h(x)\in\mathcal{W}_2$ arbitrary;
(3) $C_3=\langle 2\rangle$, $C_3=\langle f_3(x)+2h(x)\rangle$ where $h(x)\in\mathcal{W}_3$ arbitrary;
(4) (C_4,C_5) is given by the following table.

C_4 (mod $f_4(x^2)$)	C_5 (mod $f_5(x^2)$)	C_4 (mod $f_4(x^2)$)	C_5 (mod $f_5(x^2)$)
$\langle 0\rangle$	$\langle 1\rangle$	$\langle 2\overline{f}_4(x)\rangle$	$\langle f_5(x),2\rangle$
$\langle 1\rangle$	$\langle 0\rangle$	$\langle f_4(x),2\rangle$	$\langle 2\overline{f}_5(x)\rangle$
$\langle 2\rangle$	$\langle 2\rangle$	$\langle f_4(x)+2h(x)\rangle$	$\langle f_5(x)+2\widehat{h}(x)\rangle$

where $h(x)=a+bx+cx^2+dx^3$ with $a,b,c,d\in\{0,1\}$, and

$$\widehat{h}(x)=a+dx+cx^2+(1+a+b)x^3$$
$$\equiv x^4(w_4(x^{-1})+h(x^{-1})) \pmod{\langle\overline{f}_5(x),2\rangle}.$$

A generator matrix for each of the 315 self-dual codes over $\mathbb{Z}_4$ of length 30 is provided in the Appendix of this paper.

Recently, in [24, Tables 1, 2, 3] , some good cyclic codes over $\mathbb{Z}_4$ were obtained from $(1+2u)$-constacyclic codes over the ring $\mathbb{Z}_4[u]/\langle u^2-1\rangle$, and these codes have either the same parameters as the ones in [9] or they have better parameters. In [7], 36 new and good self-dual 2-quasi-twisted linear codes over $\mathbb{Z}_4$, with basic parameters $(28,2^{28},d_L=8,d_E=12)$ and of type $4^7 2^{14}$ and basic parameters $(28,2^{28},d_L=6,d_E=12)$ and of type $4^6 2^{16}$, which are Gray images of self-dual negacyclic codes over the ring $\frac{\mathbb{Z}_4[v]}{\langle v^2+2v\rangle}$ of length 14, were obtained, where d_H, d_L and d_E is the minimum Hamming distance, Lee distance and Euclidean distance of a $\mathbb{Z}_4$-code, respectively. Recently, in [18], binary extremal singly even self-dual [60, 30, 12]-codes and [60, 30, 10]-codes were constructed by a classification of four-circulant singly even self-dual [60, 30, d]-codes for $d=10$ and 12.

Among the above 315 self-dual codes over $\mathbb{Z}_4$ of length 30, we have the following 24 self-dual cyclic $\mathbb{Z}_4$-codes which do not exist in [7], [20] and [24]:

(1) 16 codes with basic parameters $(30, |C| = 2^{30}, d_H = 6, d_L = 12)$ of type $4^{14}2^2$ determined by

$$\begin{aligned}&C_1 = \langle 2\rangle, \quad C_2 = \langle f_2(x) + 2h(x)\rangle \text{ where } h(x) \in \mathcal{W}_2,\\ &C_3 = \langle f_3(x) + 2h(x)\rangle \text{ where } h(x) \in \mathcal{W}_3,\\ &(C_4, C_5) = (\langle 0\rangle, \langle 1\rangle) \text{ or } (C_4, C_5) = (\langle 1\rangle, \langle 0\rangle).\end{aligned}$$

From the above 16 codes and by the Gray map ψ from $\mathbb{Z}_4$ onto $\mathbb{F}_2^2$, defined by $0 \mapsto 00$, $1 \mapsto 01$, $2 \mapsto 11$ and $3 \mapsto 10$, we obtain 16 formally self-dual and 2-quasicyclic binary codes with basic parameters [60, 30, 12].

(2) 8 codes with basic parameters $(30, |C| = 2^{30}, d_H = 5, d_L = 10)$ of type $4^{12}2^6$ determined by

$$\begin{aligned}&C_1 = \langle 2\rangle, \quad C_2 = \langle 2\rangle, \quad C_3 = \langle f_3(x) + 2h(x)\rangle \text{ where } h(x) \in \mathcal{W}_3,\\ &(C_4, C_5) = (\langle 0\rangle, \langle 1\rangle) \text{ or } (C_4, C_5) = (\langle 1\rangle, \langle 0\rangle).\end{aligned}$$

From the above 8 codes and by the Gray map ψ from $\mathbb{Z}_4$ onto $\mathbb{F}_2^2$, we obtain 8 formally self-dual and 2-quasicyclic binary codes with parameters [60, 30, 10].

$n = 6, 10$

On [13, p. 152], the authors concluded that "there is only one trivial self-dual cyclic code over $\mathbb{Z}_4$ of length 6 and 10, respectively." In fact, there are 3 self-dual cyclic codes over $\mathbb{Z}_4$ of length 6 and there are 5 self-dual cyclic codes over $\mathbb{Z}_4$ of length 10.

(1) All the 3 distinct self-dual cyclic codes over $\mathbb{Z}_4$ of length 6 are given by:

$$\mathcal{C} = \theta_1(x)C_1 \oplus \theta_2(x)C_2,$$

where

$$\theta_1(x) = 3x^4 + 3x^2 + 3,\ C_1 = \langle 2\rangle, \text{ and}$$
$$\theta_2(x) = x^4 + x^2 + 2;\ C_2 = \langle 2\rangle, \langle (x^2 + x + 1) + 2\rangle, \langle (x^2 + x + 1) + 2(1 + x)\rangle.$$

Hence, the 2 nontrivial self-dual cyclic codes over $\mathbb{Z}_4$ of length 6 are generated by the following matrices, respectively:

$$\begin{pmatrix} 2 & 0 & 2 & 0 & 2 & 0\\ 0 & 2 & 0 & 2 & 0 & 2\\ 3 & 2 & 1 & 1 & 0 & 1\\ 1 & 3 & 2 & 1 & 1 & 0\end{pmatrix}, \begin{pmatrix} 2 & 0 & 2 & 0 & 2 & 0\\ 0 & 2 & 0 & 2 & 0 & 2\\ 3 & 2 & 1 & 3 & 0 & 3\\ 3 & 3 & 2 & 1 & 3 & 0\end{pmatrix}.$$

These 2 linear codes over $\mathbb{Z}_4$ are of type $4^2 2^2$.

(2) All the 5 distinct self-dual cyclic codes over $\mathbb{Z}_4$ of length 10 are given by:

$$\mathcal{C} = \theta_1(x)C_1 \oplus \theta_2(x)C_2,$$

where

$$\begin{aligned}\theta_1(x) &= x^8 + x^6 + x^4 + x^2 + 1;\ C_1 = \langle 2\rangle.\\ \theta_2(x) &= 3x^8 + 3x^6 + 3x^4 + 3x^2;\ C_2 = \langle 2\rangle, \langle (x^4 + x^3 + x^2 + x + 1) + 2x\rangle,\\ &\quad \langle (x^4 + x^3 + x^2 + x + 1) + 2(x + x^2)\rangle, \langle (x^4 + x^3 + x^2 + x + 1)\\ &\quad + 2(x^2 + x^3)\rangle, \langle (x^4 + x^3 + x^2 + x + 1) + 2x^3\rangle.\end{aligned}$$

Hence the 4 nontrivial self-dual cyclic codes over $\mathbb{Z}_4$ of length 6 are generated by the following matrices, respectively:

$$\begin{pmatrix} 2&0&2&0&2&0&2&0&2&0\\ 0&2&0&2&0&2&0&2&0&2\\ 2&3&2&1&2&0&1&0&1&0\\ 0&2&3&2&1&2&0&1&0&1\\ 1&0&2&3&2&1&2&0&1&0\\ 0&1&0&2&3&2&1&2&0&1 \end{pmatrix}, \begin{pmatrix} 2&0&2&0&2&0&2&0&2&0\\ 0&2&0&2&0&2&0&2&0&2\\ 0&3&2&1&0&0&3&0&3&0\\ 0&0&3&2&1&0&0&3&0&3\\ 3&0&0&3&2&1&0&0&3&0\\ 0&3&0&0&3&2&1&0&0&3 \end{pmatrix},$$
$$\begin{pmatrix} 2&0&2&0&2&0&2&0&2&0\\ 0&2&0&2&0&2&0&2&0&2\\ 0&1&2&3&0&0&3&0&3&0\\ 0&0&1&2&3&0&0&3&0&3\\ 3&0&0&1&2&3&0&0&3&0\\ 0&3&0&0&1&2&3&0&0&3 \end{pmatrix}, \begin{pmatrix} 2&0&2&0&2&0&2&0&2&0\\ 0&2&0&2&0&2&0&2&0&2\\ 2&1&2&3&2&0&1&0&1&0\\ 0&2&1&2&3&2&0&1&0&1\\ 1&0&2&1&2&3&2&0&1&0\\ 0&1&0&2&1&2&3&2&0&1 \end{pmatrix}.$$

These 4 linear codes over $\mathbb{Z}_4$ are of type $4^4 2^2$.

7 An isomorphism and lifts of cyclic codes

In this section, we study an isomorphism on the family of cyclic codes and lifts of cyclic codes. Recall that a negacyclic code $\mathcal{C}$ satisfies $(c_0, c_1, \ldots, c_{N-1}) \in \mathcal{C}$ implies $(-c_{N-1}, c_0, c_1, \ldots, c_{N-2}) \in \mathcal{C}$. If N is odd, then the map $\Psi(c(x)) = c(-x)$ sends cyclic codes to negacyclic codes. Therefore a description of cyclic codes necessarily gives a description of all negacyclic codes. Moreover, the rank and kernel of the negacyclic code are also determined from the rank and kernel of the cyclic code, see [12] for a complete description. When N is even, this is not the case.

Theorem 4 *The map* $\Psi : \mathbb{Z}_4[x]/\langle x^{2n} - 1\rangle \to \mathbb{Z}_4[x]/\langle x^{2n} - 1\rangle$ *sends cyclic codes to cyclic codes.*

Proof We note that $(-x)^{2n} - 1 = x^{2n} - 1$. Take $(c_0, c_1, \ldots, c_{2n-1}) \in \Psi(\mathcal{C})$. This implies that $(c_0, -c_1, c_2, -c_3 \ldots, -c_{2n-1}) \in \mathcal{C}$. Since $\mathcal{C}$ is cyclic, we have that $\mathbf{v} = (-c_{2n-1}, c_0, -c_1, \ldots, c_{2n-2}) \in \mathcal{C}$, so $-\mathbf{v} = (c_{2n-1}, -c_0, c_1, \ldots, -c_{2n-2}) \in \mathcal{C}$. It follows then that $(c_{2n-1}, c_0, c_1, \ldots, c_{2n-2}) \in \Psi(\mathcal{C})$. Therefore $\Psi(\mathcal{C})$ is cyclic. □

It is possible for the map to fix codes, for example the cyclic code generated by $2I_{2n}$ is fixed by Ψ.

Theorem 5 *If* $\mathcal{C}$ *is a self-dual cyclic code over* $\mathbb{Z}_4$ *then* $\Psi(\mathcal{C})$ *is a self-dual cyclic code.*

Proof If $(c_0, c_1, \ldots, c_{2n-1}), (d_0, d_1, \ldots, d_{2n-1}) \in \mathcal{C}$, then

$$[(c_0, c_1, \ldots, c_{2n-1}), (d_0, d_1, \ldots, d_{2n-1})] = \sum_{i=0}^{2n-1} c_i d_i = 0.$$

Then $(c_0, -c_1, c_2, -c_3 \ldots, c_{2n-1}), (d_0, -d_1, d_2, -d_3, \ldots, d_{2n-1}) \in \Psi(\mathcal{C})$ and

$$[(c_0, -c_1, c_2, -c_3 \ldots, c_{2n-1}), (d_0, -d_1, d_2, -d_3, \ldots, d_{2n-1})] = \sum_{i=0}^{2n-1} c_i d_i = 0.$$

Therefore the code $\Psi(\mathcal{C})$ is self-orthogonal. Since the cardinality of $\Psi(\mathcal{C})$ is

$$|\Psi(\mathcal{C})| = |C| = 4^n,$$

the code is self-dual. □

These results show that the map Ψ sends cyclic codes to cyclic codes and self-dual cyclic codes to self-dual cyclic codes. We summarize this in the following corollary.

Corollary 1 *If $\langle c(x)\rangle$ is a cyclic code over $\mathbb{Z}_4$ of length $2n$, then $\langle c(-x)\rangle$ is a cyclic code of length $2n$. If $\langle c(x)\rangle$ is a self-dual cyclic code over $\mathbb{Z}_4$ of length $2n$, then $\langle c(-x)\rangle$ is a self-dual cyclic code of length $2n$.*

In [14], codes over local Frobenius rings of order 16 were studied. Cyclic codes over these rings were studied in [10] and [15]. Of these rings, seven are extensions of $\mathbb{Z}_4$. Namely, $\mathbb{Z}_4[z]/\langle z^2-2\rangle$, $\mathbb{Z}_4[z]/\langle z^2-2z-2\rangle$ and $\mathbb{Z}_4[z]/\langle z^3-2, 2z\rangle$ are chain rings, and $\mathbb{Z}_4[z]/\langle z^2\rangle$, $\mathbb{Z}_4[z]/\langle z^2-2z\rangle$, $\mathbb{Z}_4[w,z]/\langle w^2, wz-2, z^2, 2w, 2z\rangle$ and $\mathbb{Z}_4[w,z]/\langle w^2-2, 2z-2, z^2, 2w, 2z\rangle$ are non-chain local rings. All of these rings have $\mathbb{Z}_4$ as a subring. For each of these rings, a Gray map ψ_R is defined from R to $\mathbb{F}_2^4$. It is shown in [15] that the image of a cyclic code over R under ψ_R is a quasicyclic code of index 4.

If $\mathcal{C}$ is a code over $\mathbb{Z}_4$, let $L_R(\mathcal{C})$ be the lift of the code $\mathcal{C}$ to R, i.e., $L_R(\mathcal{C})$ is the R-module generated by $\mathcal{C}$.

Lemma 10 *Let R be a local Frobenius extension over $\mathbb{Z}_4$. If $\mathcal{C}$ is a cyclic code over $\mathbb{Z}_4$, then $L_R(\mathcal{C})$ is a cyclic code over R.*

Proof By definition of the lift, $L_R(\mathcal{C})$ is linear over R. If $\mathcal{C}$ is of length N, every $\mathbf{v} \in L_R(\mathcal{C})$ is of the form $\mathbf{v} = (v_0, v_1, \ldots, v_{N-1}) = \sum_{i=1}^{t} r_i(c_{i,0}, c_{i,1}, \ldots, c_{i,N-1})$, where $r_i \in R$ and $(c_{i,0}, c_{i,1}, \ldots, c_{i,N-1}) \in \mathcal{C}$, for all $1 \leq i \leq t$.

Since $\mathcal{C}$ is cyclic, $(c_{i,N-1}, c_{i,0}, c_{i,1}, \ldots, c_{i,N-2}) \in \mathcal{C}$ for each $1 \leq i \leq t$, so $(v_{N-1}, v_0, v_1, \ldots, v_{N-2}) = \sum_{i=1}^{t} r_i(c_{i,N-1}, c_{i,0}, c_{i,1}, \ldots, c_{i,N-2}) \in L_R(\mathcal{C})$. Therefore, the code $L_R(\mathcal{C})$ is a cyclic code. □

Combining this lemma with the result from [15], we have the following result:

Theorem 6 *Let R be a local Frobenius extension over $\mathbb{Z}_4$ and let $\mathcal{C}$ be a cyclic code over $\mathbb{Z}_4$. Then $\psi_R(L_R(\mathcal{C}))$ is a binary quasicyclic code of index 4.*

8 Conclusions

We have presented a new representation for every cyclic code over $\mathbb{Z}_4$ of length $2n$, where n is an odd positive integer. Using this representation, we have provided an efficient encoder for each code and determined its type explicitly. We then gave a precise description for the dual codes and the self-duality of cyclic codes over $\mathbb{Z}_4$ of length $2n$. In particular, the number of self-dual cyclic codes over $\mathbb{Z}_4$ of length $2n$ can be obtained from 2-cyclotomic cosets modulo n directly, correcting mistakes in [3] and [13].

A natural extension of this work is to represent all distinct self-dual cyclic codes over $\mathbb{Z}_4$ of length $2^k n$ precisely, for any integer $k \geq 2$.

Acknowledgements Part of this work was done when Yonglin Cao was visiting Chern Institute of Mathematics, Nankai University, Tianjin, China. Yonglin Cao thanks the institution for the kind hospitality. This research is supported in part by the National Natural Science Foundation of China (Grant Nos. 11671235, 11801324), the Shandong Provincial Natural Science Foundation, China (Grant No. ZR2018BA007), the Nanyang Technological University Research Grant M4080456, the Scientific Research Fund of Hubei Provincial Key Laboratory of Applied Mathematics (Hubei University) (Grant No. AM201804) and the Scientific Research Fund of Hunan Provincial Key Laboratory of Mathematical Modeling and Analysis in Engineering (No. 2018MMAEZD09).

Appendix: Generator matrices for all 315 self-dual cyclic codes over $\mathbb{Z}_4$ of length 30

We identify each polynomial $a(x)=\sum_{j=0}^{29}a_jx^j\in\frac{\mathbb{Z}_4[x]}{\langle x^{30}-1\rangle}$ with the vector $(a_0,a_1,\ldots,a_{29})\in\mathbb{Z}_4^{30}$. Then set

(i)

$$G_1=\begin{pmatrix}2\theta_1(x)\\ 2x\theta_1(x)\end{pmatrix}\in \mathrm{M}_{2\times 2n}(\mathbb{Z}_4),\ k_{0,1}=0 \text{ and } k_{1,1}=2.$$

(ii-1)

$$G_{2,1}=\begin{pmatrix}2\theta_2(x)\\ 2x\theta_2(x)\\ 2x^2\theta_2(x)\\ 2x^3\theta_2(x)\end{pmatrix}\in \mathrm{M}_{4\times 2n}(\mathbb{Z}_4),\ k_{0,2}=0 \text{ and } k_{1,2}=4.$$

(ii-2)

$$G_{2,2}=\begin{pmatrix}(f_2(x)+2h(x))\theta_2(x)\\ x(f_2(x)+2h(x))\theta_2(x)\end{pmatrix}\in \mathrm{M}_{2\times 2n}(\mathbb{Z}_4),\ k_{0,2}=2 \text{ and}$$
$$k_{1,2}=0,\ \text{ where } h(x)\in\mathcal{W}_2=\{1,1+x\}.$$

(iii-1)

$$G_{3,1}=\begin{pmatrix}2\theta_3(x)\\ 2x\theta_3(x)\\ \cdots\\ 2x^7\theta_3(x)\end{pmatrix}\in \mathrm{M}_{8\times 2n}(\mathbb{Z}_4),\ k_{0,2}=0 \text{ and } k_{1,2}=8.$$

(iii-2)

$$G_{3,2}=\begin{pmatrix}(f_3(x)+2h(x))\theta_3(x)\\ x(f_3(x)+2h(x))\theta_3(x)\\ x^2(f_3(x)+2h(x))\theta_3(x)\\ x^3(f_3(x)+2h(x))\theta_3(x)\end{pmatrix}\in \mathrm{M}_{4\times 2n}(\mathbb{Z}_4),\ k_{0,3}=4 \text{ and}$$
$$k_{1,3}=0,\ \text{ where } h(x)\in\mathcal{W}_3=\{x,x+x^2,x^2+x^3,x^3\}.$$

(iv-1)

$$G_{4,1}=0,\ k_{0,4}=k_{1,4}=0;$$
$$G_{5,1}=\begin{pmatrix}\theta_5(x)\\ x\theta_5(x)\\ \cdots\\ x^7\theta_5(x)\end{pmatrix}\in \mathrm{M}_{8\times 2n}(\mathbb{Z}_4),\ k_{0,5}=8 \text{ and } k_{1,5}=0.$$

(iv-2)

$$G_{4,2}=\begin{pmatrix}\theta_4(x)\\ x\theta_4(x)\\ \dots\\ x^7\theta_4(x)\end{pmatrix}\in \mathrm{M}_{8\times 2n}(\mathbb{Z}_4),\, k_{0,4}=8 \text{ and } k_{1,4}=0;$$
$$G_{5,2}=0,\, k_{0,5}=k_{1,5}=0.$$

(iv-3)

$$G_{4,3}=\begin{pmatrix}2\theta_4(x)\\ 2x\theta_4(x)\\ \dots\\ 2x^7\theta_4(x)\end{pmatrix}\in \mathrm{M}_{8\times 2n}(\mathbb{Z}_4),\, k_{0,4}=0 \text{ and } k_{1,4}=8;$$
$$G_{5,3}=\begin{pmatrix}2\theta_5(x)\\ 2x\theta_5(x)\\ \dots\\ 2x^7\theta_5(x)\end{pmatrix}\in \mathrm{M}_{8\times 2n}(\mathbb{Z}_4),\, k_{0,5}=0 \text{ and } k_{1,5}=8.$$

(iv-4)

$$G_{4,4}=\begin{pmatrix}2\overline{f}_4(x)\theta_4(x)\\ 2x\overline{f}_4(x)\theta_4(x)\\ 2x^2\overline{f}_4(x)\theta_4(x)\\ 2x^3\overline{f}_4(x)\theta_4(x)\end{pmatrix}\in \mathrm{M}_{4\times 2n}(\mathbb{Z}_4),\, k_{0,4}=0 \text{ and } k_{1,4}=4;$$
$$G_{5,4}=\begin{pmatrix}f_5(x)\theta_5(x)\\ xf_5(x)\theta_5(x)\\ x^2f_5(x)\theta_5(x)\\ x^3f_5(x)\theta_5(x)\\ 2\theta_5(x)\\ 2x\theta_5(x)\\ 2x^2\theta_5(x)\\ 2x^3\theta_5(x)\end{pmatrix}\in \mathrm{M}_{8\times 2n}(\mathbb{Z}_4),\, k_{0,5}=4 \text{ and } k_{1,5}=4.$$

(iv-5)

$$G_{4,5}=\begin{pmatrix}f_4(x)\theta_4(x)\\ xf_4(x)\theta_4(x)\\ x^2f_4(x)\theta_4(x)\\ x^3f_4(x)\theta_4(x)\\ 2\theta_4(x)\\ 2x\theta_4(x)\\ 2x^2\theta_4(x)\\ 2x^3\theta_4(x)\end{pmatrix}\in \mathrm{M}_{8\times 2n}(\mathbb{Z}_4),\, k_{0,4}=4 \text{ and } k_{1,4}=4;$$
$$G_{5,5}=\begin{pmatrix}2\overline{f}_5(x)\theta_5(x)\\ 2x\overline{f}_5(x)\theta_5(x)\\ 2x^2\overline{f}_5(x)\theta_5(x)\\ 2x^3\overline{f}_5(x)\theta_5(x)\end{pmatrix}\in \mathrm{M}_{4\times 2n}(\mathbb{Z}_4),\, k_{0,5}=0 \text{ and } k_{1,5}=4.$$

(iv-6) Let $a, b, c, d \in \{0, 1\}$.

$$G_{4,6} = \begin{pmatrix} (f_4(x) + 2(a + bx + cx^2 + dx^3)\theta_4(x) \\ x(f_4(x) + 2(a + bx + cx^2 + dx^3)\theta_4(x) \\ x^2(f_4(x) + 2(a + bx + cx^2 + dx^3)\theta_4(x) \\ x^3(f_4(x) + 2(a + bx + cx^2 + dx^3)\theta_4(x) \end{pmatrix}$$
$$\in \mathrm{M}_{4\times 2n}(\mathbb{Z}_4),\ k_{0,4} = 4 \text{ and } k_{1,4} = 0;$$
$$G_{5,6} = \begin{pmatrix} (f_5(x) + 2(a + dx + cx^2 + (1 + a + b)x^3)\theta_5(x) \\ x(f_5(x) + 2(a + dx + cx^2 + (1 + a + b)x^3)\theta_5(x) \\ x^2(f_5(x) + 2(a + dx + cx^2 + (1 + a + b)x^3)\theta_5(x) \\ x^3(f_5(x) + 2(a + dx + cx^2 + (1 + a + b)x^3)\theta_5(x) \end{pmatrix}$$
$$\in \mathrm{M}_{4\times 2n}(\mathbb{Z}_4),\ k_{0,5} = 4 \text{ and } k_{1,5} = 0,$$

Then, by Theorem 1, all of the 315 self-dual codes over $\mathbb{Z}_4$ of length 30 are generated by one of the following 315 matrices:

$$G_{(i,j,l)} = \begin{pmatrix} G_1 \\ G_{2,i} \\ G_{3,j} \\ G_{4,l} \\ G_{5,l} \end{pmatrix},\ 1 \le i, j \le 2,\ 1 \le l \le 6.$$

Precisely, the self-dual codes over $\mathbb{Z}_4$ of length 30 with generator matrix $G_{(i,j,l)}$ are of type $4^{k_{2,0}+k_{3,0}+k_{4,0}}2^{2+k_{2,1}+k_{3,1}+k_{4,1}}$.

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. In: International Workshop on Coding and Cryptography (Paris, 2001), 10 pp. Electron. Notes Discret. Math., 6, Elsevier, Amsterdam (2001).
3. Blackford T.: Cyclic codes over $\mathbb{Z}_4$ of oddly even length. Discret. Appl. Math. **128**, 27–46 (2003).
4. Calderbank A.R., Sloane N.J.A.: Modular and p-adic cyclic codes. Des. Codes Cryptogr. **6**, 21–35 (1995).
5. Cao Y.: On constacyclic codes over finite chain rings. Finite Fields Appl. **24**, 124–135 (2013).
6. Cao Y.: A class of 1-generator repeated root quasi-cyclic codes. Des. Codes Cryptogr. **72**, 483–496 (2014).
7. 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).
8. 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).
9. Database of $\mathbb{Z}_4$ codes. http://www.z4codes.info. Accessed 03 September 2016.
10. Dougherty S.T.: Algebraic Coding Theory Over Finite Commutative Rings. Briefs in Mathematics. Springer, Cham (2017).
11. Dougherty S.T., Fernandez-Cordoba C.: Codes over $\mathbb{Z}_{2^k}$, gray maps and self-dual codes. Adv. Math. Commun. **5**(4), 571–588 (2011).
12. Dougherty S.T., Fernandez-Cordoba C.: Kernels and ranks of cyclic and negacyclic quaternary codes. Des. Codes Cryptogr. **81**(2), 347–364 (2016).
13. Dougherty S.T., Ling S.: Cyclic codes over $\mathbb{Z}_4$ of even length. Des. Codes Cryptogr. **39**, 127–153 (2006).
14. Dougherty S.T., Salturk E., Szabo S.: Codes over local rings of order 16 and binary codes. Adv. Math. Commun. **10**(2), 379–391 (2016).
15. Dougherty S.T., Kaya A., Salturk E.: Cyclic codes over local frobenius rings of order 16. Adv. Math. Commun. **11**(1), 99–114 (2017).
16. Gao J., Shi M., Wu T., Fu F.-W.: On double cyclic codes over $\mathbb{Z}_4$. Finite Fields Appl. **39**, 233–250 (2016).
17. Hammons Jr. A.R., Kumar P.V., Calderbank A.R., Sloane N.J.A., Solé P.: The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inform. Theory **40**(2), 301–319 (1994).

18. Harada M.: Binary extremal self-dual codes of length 60 and related codes, arXiv:1706.01694v1 [math.CO], 6 Jun 2017.
19. Harada M., Miezaki T.: An optimal odd unimodular lattice in dimension 72. Arch. Math. **97**(6), 529–533 (2011).
20. Jitman S., Sangwisut E., Udomkavanich P.: Hulls of cyclic codes over $\mathbb{Z}_4$, arXiv:1806.07590v1 [cs.IT] (20 Jun 2018).
21. Pless V., Qian Z.: Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. IEEE Trans. Inform. Theory **42**, 1594–1600 (1996).
22. Pless V., Solé P., Qian Z.: Cyclic self-dual $\mathbb{Z}_4$-codes. Finite Fields Appl. **3**, 48–69 (1997).
23. Rains F.M., Sloane N.J.A.: Self-dual Codes. Handbook of Coding Theory, vol. I, II, pp. 117–294. North-Holland, Amsterdam (1998).
24. 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).
25. Wan Z.-X.: Quaternary Codes. World Scientific, Singapore (1997).
26. Wan Z.-X.: Lectures on Finite Fields and Galois Rings. World Scientific, Singapore (2003).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.