AAECC (2016) 27:279–302
DOI 10.1007/s00200-015-0283-2

ORIGINAL PAPER

Concatenated structure of cyclic codes over $\mathbb{Z}_4$ of length $4n$

Yonglin Cao[1] · **Yuan Cao**[2] · **Qingguo Li**[2]

Received: 10 July 2015 / Revised: 21 December 2015 / Accepted: 22 December 2015 /
Published online: 8 January 2016

Abstract Let $N = 2^k n$ where n is odd and k a positive integer. We present a canonical form decomposition for every cyclic code over $\mathbb{Z}_4$ of length N, where each subcode is concatenated by a basic irreducible cyclic code over $\mathbb{Z}_4$ of length n as the inner code and a constacyclic code over a Galois extension ring of $\mathbb{Z}_4$ for length 2^k as the outer code. For the case of $k = 2$, by determining their outer codes, we give a precise description for cyclic codes over $\mathbb{Z}_4$, present dual codes and investigate self-duality for cyclic codes over $\mathbb{Z}_4$ of length $4n$. Then we list all self-dual cyclic codes over $\mathbb{Z}_4$ of length 28 and 60, respectively.

Keywords Cyclic code · Concatenated structure · Constacyclic code · Dual code · Self-dual code

Mathematics Subject Classification 94B15 · 94B05 · 11T71

1 Introduction

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

✉ Yonglin Cao
ylcao@sdut.edu.cn

Yuan Cao
yuan_cao@hnu.edu.cn

Qingguo Li
liqingguo@hnu.edu.cn

1 School of Sciences, Shandong University of Technology, Zibo 255091, Shandong, China

2 College of Mathematics and Econometrics, Hunan University, Changsha 410082, China

over $\mathbb{Z}_4$ for lengths of the form $2n$ where n is odd. The case for odd n follows from results in [3] and also appears in more detail in [5]. Dougherty and Ling in [4] determined the structure of cyclic codes over $\mathbb{Z}_4$ for arbitrary even length giving the generator polynomial for these codes, described the number and dual codes of cyclic codes for a given length and presented the form of cyclic codes that are self-dual.

A code over a ring R of length N is a nonempty subset $\mathcal{C}$ of R^N. The code $\mathcal{C}$ is said to be *linear* if $\mathcal{C}$ is an R-submodule. All codes in this paper are assumed to be linear unless otherwise specified. The ambient space R^N is equipped with the usual Euclidian inner product, i.e., $[a, b] = \sum_{j=0}^{N-1} a_j b_j$, where $a = (a_0, a_1, \ldots, a_{N-1}), b = (b_0, b_1, \ldots, b_{N-1}) \in R^N$, and the *dual code* is defined by $\mathcal{C}^{\perp} = \{a \in R^N \mid [a, b] = 0, \forall b \in \mathcal{C}\}$. If $\mathcal{C}^{\perp} = \mathcal{C}$, $\mathcal{C}$ is called a *self-dual code* over R. Let ζ be an invertible element of R. $\mathcal{C}$ is said to be *ζ-constacyclic* if $(c_0, c_1, \ldots, c_{N-1}) \in \mathcal{C}$ implies $(\zeta c_{N-1}, c_0, c_1, \ldots, c_{N-2}) \in \mathcal{C}$. Particularly, $\mathcal{C}$ is called a *negacyclic code* if $\zeta = -1$, and $\mathcal{C}$ is called a *cyclic code* if $\zeta = 1$. We use the natural connection of ζ-constacyclic codes to polynomial rings, where $c = (c_0, c_1, \ldots, c_{N-1})$ is viewed as $c(x) = \sum_{j=0}^{N-1} c_j x^j$ and the ζ-constacyclic code $\mathcal{C}$ is an ideal in the polynomial residue ring $R[x]/\langle x^N - \zeta \rangle$.

Let $N = 2^k n$ where n is odd and k a positive integer. Then cyclic codes over $\mathbb{Z}_4$ of length N are viewed as ideals of the ring $\mathbb{Z}_4[x]/\langle x^N - 1\rangle$. Let m be a positive integer, and $h(x)$ a monic basic irreducible polynomial in $\mathbb{Z}_4$ of degree m that divides $x^{2^m-1} - 1$. As in [4], we denote $\mathrm{GR}(4, m) = \mathbb{Z}_4[x]/\langle h(x)\rangle$, which is an extension Galois ring of $\mathbb{Z}_4$ with cardinality 4^m, and set $R_4(u, m) = \mathrm{GR}(4, m)[u]/\langle u^{2^k} - 1\rangle$. The main important contribution in [4] is the complete description for cyclic codes over $\mathrm{GR}(4, m)$ of length 2^k, i.e., ideals of the ring $R_4(u, m)$. Then ideals of the ring $\mathbb{Z}_4[x]/\langle x^N - 1\rangle$ are described by a ring isomorphism from $\mathbb{Z}_4[x]/\langle x^N - 1\rangle$ onto $\oplus_{\alpha \in J} R_4(u, m_\alpha)$ (see [4, Theorem 3.2]) using a discrete Fourier transformation, and then connecting cyclic codes over $\mathbb{Z}_4$ of length N to a direction sum of some cyclic codes over $\mathrm{GR}(4, m_\alpha)$ of length 2^k (see [4, Corollary 3.3]). But the expressions for codes in [4] are not clear enough for the purpose of designing and encoding codes.

In this paper, we focus our attention on cyclic codes of length $4n$ where n is odd, and attempt to give a precise description for these cyclic codes over $\mathbb{Z}_4$ in terms of concatenated structure of codes. By use of this description, one can easily to design codes for their requirements and encode presented codes by constructing their generator matrices from the concatenated structure directly.

The present paper is organized as follows. In Sect. 2, we present a canonical form decomposition for every cyclic code over $\mathbb{Z}_4$ of length $2^k n$, where each subcode is concatenated by a basic irreducible cyclic code over $\mathbb{Z}_4$ of length n as the inner code and a constacyclic code over a Galois extension ring over $\mathbb{Z}_4$ of length 2^k as the outer code. In Sect. 3, we give a precise description for each cyclic code by determining its outer code when $k = 2$. Using the canonical form decomposition, we present dual codes and investigate self-duality in Sect. 4. Finally, we list all self-dual cyclic codes over $\mathbb{Z}_4$ of length 28 and 60 in Sect. 5.

2 The concatenated structure of cyclic codes over $\mathbb{Z}_4$ of length $2^k n$

In this section, we give a canonical form decomposition for every cyclic code over $\mathbb{Z}_4$ of length $2^k n$ where n is odd.

It is known that any element a of $\mathbb{Z}_4$ is unique expressed as $a = a_0 + 2a_1$ where $a_0, a_1 \in \mathbb{F}_2 = \{0, 1\}$ in which we regard $\mathbb{F}_2$ as a subset of $\mathbb{Z}_4$. Denote $\overline{a} = a_0 \in \mathbb{F}_2$. 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 $\mathbb{Z}_4[x]$ onto $\mathbb{F}_2[x]$ by $\overline{f}(x) = \overline{f(x)} = \sum_{i=0}^{m} \overline{b}_i x^i$ for any $f(x) = \sum_{i=0}^{m} b_i x^i \in \mathbb{Z}_4[x]$. Recall that a monic polynomial $f(x) \in \mathbb{Z}_4[x]$ of positive degree is said to be *basic irreducible* if $\overline{f}(x)$ is an irreducible polynomial in $\mathbb{F}_2[x]$ (cf. [7, Chapter 5]). In the rest of this paper, we adopt the following notations.

Notation 2.1 Let n be an odd positive integer, denote $\mathcal{A} = \mathbb{Z}_4[y]/\langle y^n - 1\rangle$ and assume

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

where $f_1(y), f_2(y), \ldots, f_r(y)$ are pairwise coprime monic basic irreducible polynomials in $\mathbb{Z}_4[y]$. We assume $\deg(f_i(y)) = m_i$ and denote $R_i = \mathbb{Z}_4[y]/\langle f_i(y)\rangle = \{\sum_{j=0}^{m_i-1} b_j y^j \mid b_0, b_1, \ldots, b_{m_i-1} \in \mathbb{Z}_4\}$, for all $i = 1, \ldots, r$.

For each integer i, $1 \leq i \leq r$, by [7, Chapter 6] we know that R_i is a Galois ring of characteristic 4 and cardinality 4^{m_i} with the usual polynomial addition and multiplication modulo $f_i(y)$. The Teichmüller set of R_i is

$$\mathcal{T}_i = \left\{ \sum_{j=0}^{m_i-1} t_j y^j \mid t_0, t_1, \ldots, t_{m_i-1} \in \mathbb{F}_2 \right\},$$

and every element α of R_i has a unique 2-adic expansion: $\alpha = r_0 + 2r_1$, $r_0, r_1 \in \mathcal{T}_i$. Moreover, α is invertible if and only if $r_0 \neq 0$.

Denote $F_i(y) = \frac{y^n-1}{f_i(y)} \in \mathbb{Z}_4[y]$ in the following. Since $F_i(y)$ and $f_i(y)$ are coprime, there are polynomials $u_i(y), v_i(y) \in \mathbb{Z}_4[y]$ such that $u_i(y)F_i(y) + v_i(y)f_i(y) = 1$. In the rest of this paper, we denote by $\varepsilon_i(y)$ the unique element of $\mathcal{A}$ satisfying

$$\varepsilon_i(y) \equiv u_i(y)F_i(y) = 1 - v_i(y)f_i(y) \ \left(\text{mod } y^n - 1\right). \tag{2}$$

Then from classical ring theory, we deduce the following lemma.

Lemma 2.2 (cf. [6, Theorem 2.7]) *The ring $\mathcal{A}$ satisfies the following properties.*

(i) $\varepsilon_1(y) + \cdots + \varepsilon_r(y) = 1$, $\varepsilon_i(y)^2 = \varepsilon_i(y)$ *and* $\varepsilon_i(y)\varepsilon_j(y) = 0$ *for all* $1 \leq i \neq j \leq r$.

(ii) $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_r$, *where* $\mathcal{A}_i = \varepsilon_i(y)\mathcal{A}$ *is a ring with multiplicative identity* $\varepsilon_i(y)$. *Moreover, this decomposition is a direct sum of rings in that* $\mathcal{A}_i\mathcal{A}_j = \{0\}$ *for all i and j*, $1 \leq i \neq j \leq r$.

(iii) *For each* $1 \leq i \leq r$, *define a mapping* $\varphi_i : g(y) \mapsto \varepsilon_i(y)g(y)$ $(\forall g(y) \in R_i)$. *Then* φ_i *is a ring isomorphism from* R_i *onto* $\mathcal{A}_i$. *Hence* $|\mathcal{A}_i| = 4^{m_i}$.

(iv) *For each* $1 \le i \le r$, $\mathcal{A}_i$ *is a basic irreducible cyclic code over* $\mathbb{Z}_4$ *of length* n *having parity check polynomial* $f_i(y)$.

For convenience and self-sufficiency of the paper, we restate the concatenated structure of codes over rings.

Definition 2.3 Using the notations above, let C be a linear code over R_i of length l, i.e., C is an R_i-submodule of $R_i^l = \{(r_0, r_1, \ldots, r_{l-1}) \mid r_j \in R_i,\ j = 0, 1, \ldots, l-1\}$. The *concatenated code* of $\mathcal{A}_i$ and C is defined by

$$\mathcal{A}_i \Box_{\varphi_i} C = \{(\varphi_i(c_0), \varphi_i(c_1), \ldots, \varphi_i(c_{l-1})) \mid (c_0, c_1, \ldots, c_{l-1}) \in C\} \subseteq \mathbb{Z}_4^{nl},$$

where the cyclic code $\mathcal{A}_i$ over $\mathbb{Z}_4$ of length n is called the *inner code* and C is called the *outer code*.

Lemma 2.4 $\mathcal{A}_i \Box_{\varphi_i} C$ *is a linear code over* $\mathbb{Z}_4$ *of length* nl. *The number of codewords in this concatenated code is equal to* $|\mathcal{A}_i \Box_{\varphi_i} C| = |C|$ *and*

$$d_{\min}(\mathcal{A}_i \Box_{\varphi_i} C) \ge d_{\min}(\mathcal{A}_i) \cdot d_{\min}(C),$$

where $d_{\min}(\mathcal{A}_i \Box_{\varphi_i} C)$ *is the minimum distance of* $\mathcal{A}_i \Box_{\varphi_i} C$ *as a linear code over* $\mathbb{Z}_4$, $d_{\min}(\mathcal{A}_i)$ *is the minimum distance of* $\mathcal{A}_i$ *as a linear code over* $\mathbb{Z}_4$ *of length* n *and* $d_{\min}(C)$ *is the minimum distance of* C *as a linear code over the Galois ring* R_i *of length* l.

Proof Every nonzero codeword ξ in $\mathcal{A}_i \Box_{\varphi_i} C$ is given by $\xi = (\varphi_i(c_0), \varphi_i(c_1), \ldots, \varphi_i(c_{l-1}))$ with $c = (c_0, c_1, \ldots, c_{l-1}) \in C \subseteq R_i^l$ and $c \neq 0$. Then the Hamming weight $\mathrm{w}_H(c)$ of c satisfies $\mathrm{w}_H(c) = |\{i \mid c_i \neq 0,\ i = 0, 1, \ldots, l-1\}| \ge d_{\min}(C)$. Now, let $\mathrm{w}_H(\varphi_i(c_i))$ be the Hamming weight of $\varphi_i(c_i) \in \mathcal{A}_i \subseteq \mathcal{A} = \mathbb{Z}_4[y]/\langle y^n - 1\rangle$ (in which we regard $\varphi_i(c_i)$ as a vector in $\mathbb{Z}_4^n$). Then $\mathrm{w}_H(\varphi_i(c_i)) \ge d_{\min}(\mathcal{A}_i)$ for all $c_i \neq 0, 0 \le i \le l-1$. Therefore, as a vector in $\mathbb{Z}_4^{nl}$ the Hamming weight of ξ satisfies

$$\mathrm{w}_H(\xi) = \sum_{c_i \neq 0,\ 0 \le i \le l-1} \mathrm{w}_H(\varphi_i(c_i)) \ge \mathrm{w}_H(c) \cdot d_{\min}(\mathcal{A}_i) \ge d_{\min}(C) \cdot d_{\min}(\mathcal{A}_i).$$

Hence $d_{\min}(\mathcal{A}_i \Box_{\varphi_i} C) \ge d_{\min}(\mathcal{A}_i) \cdot d_{\min}(C)$. □

By the following lemma, we see that a generator matrix of the concatenated code $\mathcal{A}_i \Box_{\varphi_i} C$ as a $\mathbb{Z}_4$-submodule can be constructed from a generator matrix of the cyclic code $\mathcal{A}_i$ over $\mathbb{Z}_4$ and a generator matrix of the linear code C over R_i straightforwardly.

Theorem 2.5 *Let* $\varepsilon_i(y) = \sum_{j=0}^{n-1} e_{i,j} y^j$ *with* $e_{i,j} \in \mathbb{Z}_4$, *and* C *be a linear code over the Galois ring* R_i *of length* l *with a generator matrix* $G_C = (\alpha_{j,s})_{1 \le j \le t, 1 \le s \le l}$ *where* $\alpha_{j,s} \in R_i$, *i.e.,* C *is an* R_i*-submodule of* R_i^l *generated by the row vectors of* G_C. *Then we have the following*

(i) *A generator matrix of the cyclic code $\mathcal{A}_i$ over $\mathbb{Z}_4$ of length n is given by*

$$G_{\mathcal{A}_i} = \begin{pmatrix} e_{i,0} & e_{i,1} & \dots & e_{i,n-2} & e_{i,n-1} \\ e_{i,n-1} & e_{i,0} & \dots & e_{i,n-3} & e_{i,n-2} \\ \dots & \dots & \dots & \dots & \dots \\ e_{i,n-m_i+1} & e_{i,n-m_i+2} & \dots & e_{i,n-m_i-1} & e_{i,n-m_i} \end{pmatrix}.$$

(ii) *Assume $f_i(y) = \sum_{j=0}^{m_i} f_{i,j} y^j$ with $f_{i,j} \in \mathbb{Z}_4$ and $f_{i,m_i} = 1$, and let $M_{f_i} = \begin{pmatrix} 0 & I_{m_i-1} \\ -f_{i,0} & V_i \end{pmatrix}$ be the companion matrix of $f_i(y)$ where I_{m_i-1} is the identity matrix of order $m_i - 1$ and $V_i = (-f_{i,1}, \dots, -f_{i,m_i-1})$. For any $\alpha = \alpha(y) = \sum_{j=0}^{m_i-1} r_j y^j \in R_i$ with $r_j \in \mathbb{Z}_4$, denote $A_\alpha = \alpha(M_{f_i}) = \sum_{j=0}^{m_i-1} r_j (M_{f_i})^j \in \mathrm{M}_{m_i \times m_i}(\mathbb{Z}_4)$ in the rest of the paper. Then*

$$\alpha Y = A_\alpha Y, \text{ where } Y = \begin{pmatrix} 1 \\ y \\ \dots \\ y^{m_i-1} \end{pmatrix}.$$

(iii) *Let $G_C = (\alpha_{j,s})_{1 \le j \le t, 1 \le s \le l}$ with $\alpha_{j,s} \in R_i$. Then a generator matrix of the concatenated code $\mathcal{A}_i \Box_{\varphi_i} C$ is given by*

$$G_{\mathcal{A}_i \Box_{\varphi_i} C} = \begin{pmatrix} A_{\alpha_{1,1}} G_{\mathcal{A}_i} & \dots & A_{\alpha_{1,l}} G_{\mathcal{A}_i} \\ \dots & \dots & \dots \\ A_{\alpha_{t,1}} G_{\mathcal{A}_i} & \dots & A_{\alpha_{t,l}} G_{\mathcal{A}_i} \end{pmatrix}.$$

Hence $\mathcal{A}_i \Box_{\varphi_i} C = \{\underline{w} G_{\mathcal{A}_i \Box_{\varphi_i} C} \mid \underline{w} \in \mathbb{Z}_4^{m_i t}\}$.

Proof (i) Since $f_i(y)$ is a monic basic irreducible polynomial in $\mathbb{Z}_4[y]$ of degree m_i, $\{1, y, \dots, y^{m_i-1}\}$ is a $\mathbb{Z}_4$-basis of the Galois ring $R_i = \mathbb{Z}_4[y]/\langle f_i(y)\rangle$ (See [7, Chapter 6]). As φ_i is a $\mathbb{Z}_4$-module isomorphism from R_i onto $\mathcal{A}_i$ by Lemma 2.2(iii), we conclude that $\{\varepsilon_i(y), y\varepsilon_i(y), \dots, y^{m_i-1}\varepsilon_i(y)\}$ is a $\mathbb{Z}_4$-basis of $\mathcal{A}_i$. Hence $G_{\mathcal{A}_i}$ is a generator matrix of $\mathcal{A}_i$ as a $\mathbb{Z}_4$-submodule of $\mathbb{Z}_4^n$.

(ii) It is obvious that $yY = M_{f_i} Y$, which implies that $y^j Y = (M_{f_i})^j Y$ for all $j = 0, 1, \dots, m_i - 1$. Hence $\alpha Y = \sum_{j=0}^{m_i-1} r_j (y^j Y) = A_\alpha Y$.

(iii) Let $\mathcal{C}$ be the $\mathbb{Z}_4$-submodule of $\mathbb{Z}_4^{nl}$ generated by the row vectors of $G_{\mathcal{A}_i \Box_{\varphi_i} C}$, i.e., $\mathcal{C} = \{\underline{w} G_{\mathcal{A}_i \Box_{\varphi_i} C} \mid \underline{w} \in \mathbb{Z}_4^{m_i t}\}$. By Definition 2.3, $\xi \in \mathcal{A}_i \Box_{\varphi_i} C$ if and only if there exists a unique codeword $c = (c_1, \dots, c_l) \in C$ such that $\xi = (\varphi_i(c_1), \dots, \varphi_i(c_l))$. Since G_C is a generator matrix of C, $c \in C$ if and only if c is an R_i-combination of the row vectors $(\alpha_{1,1}, \dots, \alpha_{1,l}), \dots, (\alpha_{t,1}, \dots, \alpha_{t,l})$ of G_C, which is equivalent that there exist $\beta_1, \dots, \beta_t \in R_i$ such that

$$\begin{aligned} \xi &= \left(\varphi_i\left(\beta_1\alpha_{1,1} + \dots + \beta_t\alpha_{t,1}\right), \dots, \varphi_i\left(\beta_1\alpha_{1,l} + \dots + \beta_t\alpha_{t,l}\right)\right) \\ &= \left(\varphi_i\left(\beta_1\alpha_{1,1}\right) + \dots + \varphi_i\left(\beta_t\alpha_{t,1}\right), \dots, \varphi_i\left(\beta_1\alpha_{1,l}\right) + \dots + \varphi_i\left(\beta_t\alpha_{t,l}\right)\right), \end{aligned}$$

since φ_i is a $\mathbb{Z}_4$-module isomorphism. For each integer j, $1 \leq j \leq t$, by $\beta_j \in R_i$ there is a unique row vector $\underline{b}_j \in \mathbb{Z}_4^{m_i}$ such that $\beta_j = \underline{b}_j Y$. From this and by (ii) we deduce that $\beta_j \alpha_{j,s} = \underline{b}_j(\alpha_{j,s}Y) = \underline{b}_j A_{\alpha_{j,s}} Y$ for all $s = 1, \ldots, l$. Also, since φ_i is a $\mathbb{Z}_4$-module isomorphism, we have

$$\begin{aligned}\xi &= \big(\underline{b}_1 A_{\alpha_{1,1}}\varphi_i(Y) + \cdots + \underline{b}_t A_{\alpha_{t,1}}\varphi_i(Y), \ldots, \\ &\quad \underline{b}_1 A_{\alpha_{1,l}}\varphi_i(Y) + \cdots + \underline{b}_t A_{\alpha_{t,l}}\varphi_i(Y)\big) \\ &= \underline{w}\begin{pmatrix} A_{\alpha_{1,1}}\varphi_i(Y) & \ldots & A_{\alpha_{1,l}}\varphi_i(Y) \\ \ldots & \ldots & \ldots \\ A_{\alpha_{t,1}}\varphi_i(Y) & \ldots & A_{\alpha_{t,l}}\varphi_i(Y) \end{pmatrix},\end{aligned}$$

where $\underline{w} = (\underline{b}_1, \ldots, \underline{b}_t) \in \mathbb{Z}_4^{m_i t}$. Then from

$$\varphi_i(Y) = \begin{pmatrix} \varphi_i(1) \\ \varphi_i(y) \\ \ldots \\ \varphi_i(y^{m_i-1}) \end{pmatrix} = \begin{pmatrix} \varepsilon_i(y) \\ y\varepsilon_i(y) \\ \ldots \\ y^{m_i-1}\varepsilon_i(y) \end{pmatrix} = G_{\mathcal{A}_i}\begin{pmatrix} 1 \\ y \\ \ldots \\ y^{n-1} \end{pmatrix}$$

and the identification of $\mathbb{Z}_4[y]\langle y^n - 1\rangle$ with $\mathbb{Z}_4^n$, we deduce $\xi = \underline{w}G_{\mathcal{A}_i \Box_{\varphi_i} C} \in \mathcal{C}$. Therefore, $\mathcal{A}_i \Box_{\varphi_i} C = \mathcal{C}$. □

Now, we give the concatenated structure of cyclic codes over $\mathbb{Z}_4$. From now on, let $N = 2^k n$ where k is a positive integer. As usual, we will identify $\mathbb{Z}_4^N$ with $\mathbb{Z}_4[x]/\langle x^N - 1\rangle$ under the natural $\mathbb{Z}_4$-module isomorphism: $(c_0, c_1, \ldots, c_{N-1}) \mapsto c_0 + c_1 x + \cdots + c_{N-1}x^{N-1}$ ($c_j \in \mathbb{Z}_4$, $j = 0, 1, \ldots, N-1$).

Using the notations of Lemma 2.2, every element of the ring $\mathcal{A}$ can be uniquely expressed as $a(y) = \sum_{j=0}^{n-1} a_j y^j$ with $a_j \in \mathbb{Z}_4$. Then every element of the quotient ring $\mathcal{A}[x]/\langle x^{2^k} - y\rangle$ can be uniquely expressed as $\alpha(x, y) = \sum_{i=0}^{n-1}\sum_{j=0}^{2^k-1} c_{i,j} y^i x^j$, $c_{i,j} \in \mathbb{Z}_4$. Now, define

$$\Psi(\alpha(x, y)) = \alpha\left(x, x^{2^k}\right) = \sum_{i=0}^{n-1}\sum_{j=0}^{2^k-1} c_{i,j} x^{i2^k+j}.$$

It is clear that Ψ is a ring isomorphism from $\mathcal{A}[x]/\langle x^{2^k} - y\rangle$ onto $\mathbb{Z}_4[x]/\langle x^N - 1\rangle$. In the rest of this paper, we will identify $\mathcal{A}[x]/\langle x^{2^k} - y\rangle$ with $\mathbb{Z}_4[x]/\langle x^N - 1\rangle$ under this isomorphism Ψ.

Theorem 2.6 *Using the notations in Notation 2.1 and Lemma 2.2, let $\mathcal{C} \subseteq \mathbb{Z}_4[x]/\langle x^N - 1\rangle$. The following are equivalent:*

(i) *$\mathcal{C}$ is a cyclic code over $\mathbb{Z}_4$ of length N.*
(ii) *$\mathcal{C}$ is an ideal of the ring $\mathcal{A}[x]/\langle x^{2^k} - y\rangle$.*
(iii) *For each integer i, $1 \leq i \leq r$, there is a unique ideal $\mathcal{C}_i$ of the ring $\mathcal{A}_i[x]/\langle \varepsilon_i(y)x^{2^k} - \varepsilon_i(y)y\rangle$ such that $\mathcal{C} = \oplus_{i=1}^r \mathcal{C}_i$.*

(iv) *For each integer i, $1 \le i \le r$, there is a unique y-constacyclic code C_i over R_i of length 2^k, i.e., C_i is an ideal of the ring $R_i[x]/\langle x^{2^k} - y\rangle$, such that*

$$\mathcal{C} = \left(\mathcal{A}_1 \Box_{\varphi_1} C_1\right) \oplus \cdots \oplus \left(\mathcal{A}_r \Box_{\varphi_r} C_r\right),$$

where $\mathcal{A}_i \Box_{\varphi_i} C_i = \{\varepsilon_i(y)\alpha(x) \mid \alpha(x) \in C_i\}$ *for all* $i = 1, \ldots, r$.

Proof (i)⇔(ii) It follows from $\mathbb{Z}_4[x]/\langle x^N - 1\rangle = \mathcal{A}[x]/\langle x^{2^k} - y\rangle$.

(ii)⇔(iii) By Lemma 2.2 (i) and (ii) it follows that

$$\mathcal{A}[x]/\left\langle x^{2^k} - y\right\rangle = \oplus_{i=1}^{r} \left(\mathcal{A}_i[x]/\left\langle \varepsilon_i(y)x^{2^k} - \varepsilon_i(y)y\right\rangle\right)$$

and $(\mathcal{A}_i[x]/\langle \varepsilon_i(y)x^{2^k} - \varepsilon_i(y)y\rangle)(\mathcal{A}_j[x]/\langle \varepsilon_j(y)x^{2^k} - \varepsilon_j(y)y\rangle) = \{0\}$ for all $i \neq j$. Hence $\mathcal{C}$ is an ideal of the ring $\mathbb{Z}_4[x]/\langle x^N - 1\rangle$ if and only if for each integer i, $1 \le i \le r$, there is a unique ideal $\mathcal{C}_i$ of the ring $\mathcal{A}_i[x]/\langle \varepsilon_i(y)x^{2^k} - \varepsilon_i(y)y\rangle$ such that $\mathcal{C} = \oplus_{i=1}^{r}\mathcal{C}_i$.

(iii)⇔(iv) By Lemma 2.2(iii), $\varphi_i : g(y) \mapsto \varepsilon_i(y)g(y)$ ($\forall g(y) \in R_i$) is a ring isomorphism from R_i onto $\mathcal{A}_i$. It is clear that φ_i induces a ring isomorphism from $R_i[x]/\langle x^{2^k} - y\rangle$ onto $\mathcal{A}_i[x]/\langle \varepsilon_i(y)x^{2^k} - \varepsilon_i(y)y\rangle$ by the rule that: $\forall \alpha(x) = \sum_{j=0}^{2^k-1} \alpha_j x^j \in R_i[x]/\langle x^{2^k} - y\rangle$ with $\alpha_0, \alpha_1, \ldots, \alpha_{2^k-1} \in R_i$,

$$\varphi_i(\alpha(x)) = \sum_{j=0}^{2^k-1} \varphi_i(\alpha_j)x^j \leftrightarrow \left(\varphi_i(\alpha_0), \varphi_i(\alpha_1), \ldots, \varphi_i(\alpha_{2^k-1})\right) \in \mathcal{A}_i^{2^k}.$$

Therefore, for each integer i, $1 \le i \le r$, and an ideal $\mathcal{C}_i$ of $\mathcal{A}_i[x]/\langle \varepsilon_i(y)x^{2^k} - \varepsilon_i(y)y\rangle$, there is a unique ideal C_i of $R_i[x]/\langle x^{2^k} - y\rangle$ such that $\mathcal{C}_i = \varphi_i(C_i)$. Hence $\mathcal{C}_i = \mathcal{A}_i \Box_{\varphi_i} C_i$ by Definition 2.3. It is clear that C_i is a y-constacyclic code over the Galois ring R_i of length 2^k. □

By Theorem 2.6, in order to present all cyclic codes over $\mathbb{Z}_4$ of length N it is sufficient to determine all ideals of the ring $R_i[x]/\langle x^{2^k} - y\rangle$, for all $i = 1, \ldots, r$.

3 Representation of cyclic codes over $\mathbb{Z}_4$ of length $4n$

In this section, following [4] we give another precise description for cyclic codes over $\mathbb{Z}_4$ of length $4n$ by determining their outer codes in the concatenated structure of subcodes.

Since n is odd, there is a positive integer e, $1 \le e < n$, such that $2^k e \equiv -1$ (mod n). By Eq. (1) it follows that $y^n \equiv 1$ (mod $f_i(y)$), i.e., $y^n = 1$ in R_i. From these we deduce that $(y^e)^{2^k} = y^{-1}$ in R_i.

Lemma 3.1 *Using the notations above, define a mapping* $\sigma_i : R_i[u]/\langle u^{2^k} - 1\rangle \to R_i[x]/\langle x^{2^k} - y\rangle$ *by*

$$\sigma_i(a(u)) = a\left(y^e x\right), \ \forall a(u) \in R_i[u]/\left\langle u^{2^k} - 1\right\rangle.$$

Then σ_i is a ring isomorphism from $R_i[u]/\langle u^{2^k} - 1\rangle$ onto $R_i[x]/\langle x^{2^k} - y\rangle$ preserving R_i-Hamming weight.

Proof For any $b(u) = \sum_j b_j u^j \in R_i[u]$ where $b_j \in R_i$, define $\sigma_i(b(u)) = \sum_j b_j (y^e x)^j \in R_i[x]$. Since y^e is an invertible element of R_i, σ_i is a ring isomorphism from $R_i[u]$ onto $R_i[x]$. From this and by $\sigma_i(u^{2^k} - 1) = (y^e x)^{2^k} - 1 = y^{e2^k} x^{2^k} - 1 = y^{-1}(x^{2^k} - y)$ in $R_i[x]$, we deduce the conclusions. □

In the rest of this paper, we denote

$$\pi_i = y^e x - 1 = \sigma_i(u - 1) \in R_i[x]/\left\langle x^{2^k} - y\right\rangle. \tag{3}$$

Now, we denote $\Gamma_4(u, m) = R_i[u]/\langle u^{2^k} - 1\rangle$ where $R_i = \mathrm{GR}(4, m_i)$ (cf. Eq. (7) in Page 130 of [4]). Recall that ideals of the ring $\Gamma_4(u, m)$ are in fact cyclic codes over the Galois ring R_i of length 2^k. These cyclic codes have been studied in [4]. For the purpose of this paper, we list some conclusions from [4].

Lemma 3.2 ([4, Theorem 2.6]) *The number of ideals of $R_i[u]/\langle u^{2^k} - 1\rangle$, where $R_i = \mathrm{GR}(4, m_i)$, is equal to*

$$N_{(4,m_i;k)} = 5 + \left(2^{m_i}\right)^{2^{k-1}} + \left(5 \cdot 2^{m_i} - 1\right)\left(2^{m_i}\right) \frac{(2^{m_i})^{2^{k-1}-1} - 1}{(2^{m_i} - 1)^2} - 4 \cdot \frac{2^{k-1} - 1}{2^{m_i} - 1}.$$

Especially, $N_{(4,m_i;k)} = 9 + 5 \cdot 2^{m_i} + 2^{2m_i}$ when $k = 2$.

By Theorem 2.6, Lemmas 3.1 and 3.2, we see that the number of cyclic codes over $\mathbb{Z}_4$ of length $2^k n$ is equal to $\prod_{i=1}^{r} N_{(4,m_i;k)}$ ([4, Corollary 3.4]).

For any ideal C_i of the ring $R_i[x]/\langle x^{2^k} - y\rangle$, recall that the *annihilating ideal* of C_i is $\mathrm{Ann}(C_i) = \{\alpha \in R_i[x]/\langle x^{2^k} - y\rangle \mid \alpha\beta = 0, \forall \beta \in C_i\}$.

Then by Lemma 3.1 and [4, Theorem 5.3] or by direct calculations, we list all distinct y-constacyclic codes over the Galois ring R_i of length 4, i.e., ideals of the ring $R_i[x]/\langle x^4 - y\rangle$, by the following theorem.

Theorem 3.3 *All distinct y-constacyclic codes C_i over the Galois ring R_i of length 4 and their annihilating ideals are given by one of the following cases:*

Case	C_i	$\|C_i\|$	$\mathrm{Ann}(C_i)$	L_C
1.	$\langle 0\rangle$	1	$\langle 1\rangle$	1
2.	$\langle 1\rangle$	2^{8m_i}	$\langle 0\rangle$	1
3.	$\langle \pi_i^j\rangle$ $(j=1,2)$	$2^{2m_i(4-j)}$	$\langle \pi_i^{4-j}+2\pi_i^{2-j}\rangle$	2
4.	$\langle 2\rangle$	2^{4m_i}	$\langle 2\rangle$	1
5.	$\langle 2\pi_i^s\rangle$ $(s=1,2,3)$	$2^{m_i(4-s)}$	$\langle \pi_i^{4-s},2\rangle$	3
6.	$\langle \pi_i+2h\rangle$ $(h\in\mathcal{T}_i\backslash\{0\})$	2^{6m_i}	$\langle \pi_i^3+2\pi_i(1+\pi_i h)\rangle$	$2^{m_i}-1$
7.	$\langle \pi_i^2+2\pi_i h\rangle$ $(h\in\mathcal{T}_i\backslash\{0\})$	2^{4m_i}	$\langle \pi_i^2+2(1+\pi_i h)\rangle$	$2^{m_i}-1$
8.	$\langle \pi_i^2+2(h+\pi_i g)\rangle$ $(h\in\mathcal{T}_i\backslash\{0,1\}, g\in\mathcal{T}_i)$	2^{4m_i}	$\langle \pi_i^2+2(1+h+\pi_i g)\rangle$	$2^{2m_i}-2^{m_i+1}$
9.	$\langle \pi_i^2+2(1+\pi_i h)\rangle$ $(h\in\mathcal{T}_i\backslash\{0\})$	2^{4m_i}	$\langle \pi_i^2+2\pi_i h\rangle$	$2^{m_i}-1$
10.	$\langle \pi_i^3+2\pi_i(3+\pi_i h)\rangle$ $(h\in\mathcal{T}_i\backslash\{0\})$	2^{2m_i}	$\langle \pi_i+2h\rangle$	$2^{m_i}-1$
11.	$\langle \pi_i^3+2h\rangle$ $(h\in\mathcal{T}_i)$	2^{4m_i}	$\langle \pi_i^3+2h\rangle$	2^{m_i}
13.	$\langle \pi_i^j+2\pi_i^{j-2}\rangle$ $(j=2,3)$	$2^{2m_i(4-j)}$	$\langle \pi_i^{4-j}\rangle$	2
14.	$\langle \pi_i^j,2\rangle$ $(j=1,2,3)$	$2^{m_i(8-j)}$	$\langle 2\pi_i^{4-j}\rangle$	3
15.	$\langle \pi_i^2+2,2\pi_i\rangle$	2^{5m_i}	$\langle \pi_i^3,2\pi_i^2\rangle$	1
16.	$\langle \pi_i^3,2\pi_i^2\rangle$	2^{3m_i}	$\langle \pi_i^2+2,2\pi_i\rangle$	1
17.	$\langle \pi_i^3+2\pi_i,2\pi_i^2\rangle$	2^{3m_i}	$\langle \pi_i^2,2\pi_i\rangle$	1
18.	$\langle \pi_i^2,2\pi_i\rangle$	2^{5m_i}	$\langle \pi_i^3+2\pi_i,2\pi_i^2\rangle$	1
19.	$\langle \pi_i^2+2h,2\pi_i\rangle$ $(h\in\mathcal{T}_i\backslash\{0,1\})$	2^{5m_i}	$\langle \pi_i^3+2\pi_i(1+h),2\pi_i^2\rangle$	$2^{m_i}-2$
20.	$\langle \pi_i^3+2\pi_i h,2\pi_i^2\rangle$ $(h\in\mathcal{T}_i\backslash\{0,1\})$	2^{3m_i}	$\langle \pi_i^2+2(1+h),2\pi_i\rangle$	$2^{m_i}-2$

where $\mathcal{T}_i=\{\sum_{j=0}^{m_i-1}t_jy^j \mid t_0,t_1,\ldots,t_{m_i-1}\in\{0,1\}\}$ *and* L_C *is the number of codes in the same row.*

Proof In [4] Theorem 5.3, all distinct ideals of $\Gamma_4(u,m)=R_i[u]/\langle u^{2^k}-1\rangle$ and their annihilating ideals are listed in terms of $u-1$. By Lemma 3.1, all distinct ideals of $R_i[x]/\langle x^{2^k}-y\rangle$ and their annihilating ideals can be obtained by replacing $u-1$ to $\sigma_i(u-1)=y^ex-1=\pi_i$ from [4] Theorem 5.3. Particularly, we get the conclusions for the special case of $k=2$. □

Example 3.4 We know that $y^{15}-1=f_1(y)f_2(y)f_3(y)f_4(y)f_5(y)$, where

- $f_1(y)=y-1$, $f_2(y)=1+y+y^2$, $f_3(y)=1+y+y^2+y^3+y^4$;
- $f_4(y)=1+3y+2y^2+y^4$, $f_5(y)=1+2y^2+3y^3+y^4$,

and $f_1(y)$, $f_2(y)$, $f_3(y)$, $f_4(y)$, $f_5(y)$ are pairwise coprime monic basic irreducible polynomials in $\mathbb{Z}_4[y]$. Hence $r=5$, $m_1=1$, $m_2=2$ and $m_3=m_4=m_5=4$. Now, let $N=60=2^k\cdot 15$ where $k=2$. Then the number of cyclic codes over $\mathbb{Z}_4$ of length 60 is equal to

$$\prod_{i=1}^{5}N_{(4,m_i;2)}=\prod_{i=1}^{5}\left(9+5\cdot 2^{m_i}+2^{2m_i}\right)=23\cdot 45\cdot 345^3=42,500,851,875.$$

For each integer i, $1\leq i\leq 5$, let $R_i=\mathbb{Z}_4[y]/\langle f_i(y)\rangle$, which is a Galois ring of characteristic 4 and cardinality 4^{m_i}. By $4\cdot 11\equiv -1$, (mod 15), it follows that $(y^{11})^4=y^{-1}$ in every R_i. We select $e=11$. Using Eq. (3), we have the following.

- $\pi_1=y^{11}x-1=x-1\in R_1[x]/\langle x^4-y\rangle=R_1[x]/\langle x^4-1\rangle$, since $y^{11}\equiv y\equiv 1$ (mod $y-1$), i.e., $y^e=1$ in R_1, and $R_1=\mathbb{Z}_4[y]/\langle y-1\rangle=\mathbb{Z}_4$.
- $\pi_2=y^{11}x-1=(3+3y)x-1\in R_2[x]/\langle x^4-y\rangle$, since $y^{11}\equiv 3+3y$ (mod $f_2(y)$), i.e., $y^e=3+3y$ in R_2.
- $\pi_3=y^{11}x-1=yx-1\in R_3[x]/\langle x^4-y\rangle$, since $y^{11}\equiv y$ (mod $f_3(y)$), i.e., $y^e=y$ in R_3.
- $\pi_4=y^{11}x-1=(2+y+y^2+3y^3)x-1\in R_4[x]/\langle x^4-y\rangle$, since $y^{11}\equiv 2+y+y^2+3y^3$ (mod $f_4(y)$), i.e., $y^e=2+y+y^2+3y^3$ in R_4.
- $\pi_5=y^{11}x-1=(3+3y^2+3y^3)x-1\in R_5[x]/\langle x^4-y\rangle$, since $y^{11}\equiv 3+3y^2+3y^3$ (mod $f_5(y)$), i.e., $y^e=3+3y^2+3y^3$ in R_5.

Then by Theorem 3.3, one can list all cyclic codes over $\mathbb{Z}_4$ of length 60.

Finally, from Theorems 2.6, 3.3 and 2.5 we deduce the following corollary.

Corollary 3.5 *Every cyclic code $\mathcal{C}$ over $\mathbb{Z}_4$ of length $4n$ can be constructed by the following two steps:*

(i) *For each $i=1,\ldots,r$, choose a y-constacyclic code C_i over R_i of length 4 listed in Theorem 3.3.*
(ii) *Set $\mathcal{C}=\oplus_{i=1}^{r}\mathcal{C}_i$ with $\mathcal{C}_i=\mathcal{A}_i\Box_{\varphi_i}C_i$.*

The number of codewords in $\mathcal{C}$ is equal to $|\mathcal{C}|=\prod_{i=1}^{r}|C_i|$ and the minimal Hamming distance of $\mathcal{C}$ satisfies

$$d_{\min}(\mathcal{C})\leq \min\left\{d_{\min}(\mathcal{C}_i)\mid i=1,\ldots,r\right\},$$

where $d_{\min}(\mathcal{C}_i)$ is the minimal $\mathbb{Z}_4$-Hamming weight of $\mathcal{C}_i$. Moreover, a generator matrix of $\mathcal{C}$ is given by $G_{\mathcal{C}}=\begin{pmatrix}G_{\mathcal{A}_1\Box_{\varphi_1}C_1}\\ \cdots\\ G_{\mathcal{A}_r\Box_{\varphi_r}C_r}\end{pmatrix}$.

Using the notations of Corollary 3.5(ii), $\mathcal{C}=\oplus_{i=1}^{r}\mathcal{C}_i$ is called the *canonical form decomposition* of the cyclic code $\mathcal{C}$ over $\mathbb{Z}_4$ of length $4n$.

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

In this section, we give the dual code of each cyclic code over $\mathbb{Z}_4$ of length N where $N=4n$, and investigate the self-duality of these codes.

As usual, we will identify $a = (a_0, a_1, \ldots, a_{N-1}) \in \mathbb{Z}_4^N$ with $a(x) = \sum_{j=0}^{N-1} a_j x^j \in \mathbb{Z}_4[x]/\langle x^N - 1\rangle$. In this paper, we define

$$\mu(a(x)) = a\left(x^{-1}\right) = a_0 + \sum_{j=1}^{N-1} a_j x^{N-j},\ \forall a(x) \in \mathbb{Z}_4[x]/\left\langle x^N - 1\right\rangle.$$

Then μ is a ring automorphism of $\mathbb{Z}_4[x]/\langle x^N - 1\rangle$ satisfying $\mu^{-1} = \mu$ and $\mu(c) = c$ for all $c \in \mathbb{Z}_4$. The following lemma is well known.

Lemma 4.1 *Let* $a, b \in \mathbb{Z}_4^N$. *Then* $[a, b] = 0$ *if* $a(x)\mu(b(x)) = 0$ *in the ring* $\mathbb{Z}_4[x]/\langle x^N - 1\rangle$.

Using the notations of Sect. 3, we have $\mathbb{Z}_4[x]/\langle x^N - 1\rangle = \mathcal{A}[x]/\langle x^4 - y\rangle$ under the substitution $y = x^4$, where $\mathcal{A} = \mathbb{Z}_4[y]/\langle y^n - 1\rangle$. Hence

$$\mu(y) = \left(x^{-1}\right)^4 = y^{-1} \text{ in } \mathcal{A}[x]/\left\langle x^4 - y\right\rangle.$$

Therefore, the restriction of μ to $\mathcal{A}$ is given by

$$\mu(f(y)) = f\left(y^{-1}\right)\ (\forall f(y) \in \mathcal{A}),$$

which is a ring automorphism of $\mathcal{A}$. For notations simplicity, we still denote this restriction by μ. From this and by Notation 2.1, we deduce

$$\mu(\varepsilon_i(y)) = u_i\left(y^{-1}\right) F_i\left(y^{-1}\right) = 1 - v_i\left(y^{-1}\right) f_i\left(y^{-1}\right) \text{ in } \mathcal{A}. \tag{4}$$

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

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

Since $f_1(y), f_2(y), \ldots, f_r(y)$ are pairwise coprime monic basic polynomials in $\mathbb{Z}_4[y]$, for each $1 \leq i \leq r$ there is a unique integer i', $1 \leq i' \leq r$, such that $\widetilde{f}_i(y) = \delta_i f_{i'}(y)$ for some $\delta_i \in \{1, -1\}$. From this, by Eq. (4) and $y^n = 1$ in the ring $\mathcal{A}$, we deduce

$$\begin{aligned}\mu\left(\varepsilon_i(y)\right) &= 1 - y^{n-\deg(v_i(y))-m_i}\left(y^{\deg(v_i(y))} v_i(y^{-1})\right)\left(y^{m_i} f_i\left(y^{-1}\right)\right)\\ &= 1 - y^{n-\deg(v_i(y))-m_i}\widetilde{v}_i(y)\widetilde{f}_i(y)\\ &= 1 - h_i(y) f_{i'}(y)\end{aligned}$$

where $h_i(y) = \delta_i y^{n-\deg(v_i(y))-m_i}\widetilde{v}_i(y) \in \mathcal{A}$. Similarly, by (4) it follows that $\mu(\varepsilon_i(y)) = g_i(y)F_{i'}(y)$ for some $g_i(y) \in \mathcal{A}$. Then from these and by Eq. (2) in Sect. 2, we deduce that $\mu(\varepsilon_i(y)) = \varepsilon_{i'}(y)$.

As stated above, we see that for each $1 \le i \le r$ there is a unique integer i', $1 \le i' \le r$, such that $\mu(\varepsilon_i(y)) = \varepsilon_{i'}(y)$. We still use μ to denote this map $i \mapsto i'$, i.e., $\mu(\varepsilon_i(y)) = \varepsilon_{\mu(i)}(y)$. Whether μ denotes the automorphism of $\mathcal{A}$ or this map on the set $\{1, \ldots, r\}$ is determined by the context. The next lemma shows the compatibility of the two uses of μ.

Lemma 4.2 *With the notations above, we have the following conclusions.*

(i) *μ is a permutation on the set $\{1, \ldots, r\}$ satisfying $\mu^{-1} = \mu$.*
(ii) *After a rearrangement of $\varepsilon_1(y), \ldots, \varepsilon_r(y)$, there are integers λ, ρ such that $\mu(i) = i$ for all $i = 1, \ldots, \lambda$ and $\mu(\lambda + j) = \lambda + \rho + j$ for all $j = 1, \ldots, \rho$, where $\lambda \ge 1$, $\rho \ge 0$ and $\lambda + 2\rho = r$.*
(iii) *For each integer i, $1 \le i \le r$, there is a unique element δ_i of $\{1, -1\}$ such that $\widetilde{f}_i(y) = \delta_i f_{\mu(i)}(y)$.*
(iv) *For any integer i, $1 \le i \le r$, $\mu(\varepsilon_i(y)) = \varepsilon_{\mu(i)}(y)$ in the ring $\mathcal{A}$, and $\mu(\mathcal{A}_i) = \mathcal{A}_{\mu(i)}$. Then μ induces a ring isomorphism from $\mathcal{A}_i$ onto $\mathcal{A}_{\mu(i)}$.*

Proof (i)–(iii) follow from the definition of the map μ, and (iv) follows from that $\mathcal{A}_i = \varepsilon_i(y)\mathcal{A}$ immediately. □

Lemma 4.3 *Using the notations above, the following hold for any $1 \le i \le r$.*

(i) *For any $\xi \in R_i$, we define $\widehat{\xi} = (\varphi_{\mu(i)}^{-1}\mu\varphi_i)(\xi)$. Then $\widehat{}$ is a ring isomorphism from R_i onto $R_{\mu(i)}$ such that the following diagram commutes*

$$\begin{array}{ccc} R_i = \mathbb{Z}_4[y]/\langle f_i(y)\rangle & \stackrel{\widehat{}}{\longrightarrow} & R_{\mu(i)} = \mathbb{Z}_4[y]/\langle f_{\mu(i)}(y)\rangle \\ \varphi_i \downarrow & & \downarrow \varphi_{\mu(i)} \\ \mathcal{A}_i & \stackrel{\mu}{\longrightarrow} & \mathcal{A}_{\mu(i)} \end{array}$$

Specifically, we have $\widehat{\xi} = a(y^{-1}) \in R_{\mu(i)}$ for all $\xi = a(y) \in R_i$.
(ii) *For any $\alpha(x) = \sum_{j=0}^{3} \alpha_j x^j \in R_i[x]/\langle x^4 - y\rangle$ where $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in R_i$, define $\widehat{\alpha}(x) = \sum_{j=0}^{3} \widehat{\alpha_j} x^j$. Then μ induces a ring isomorphism from $R_i[x]/\langle x^4 - y\rangle$ onto $R_{\mu(i)}[x]/\langle x^4 - y\rangle$ by the rule that*

$$\mu : \alpha(x) = \sum_{j=0}^{3} \alpha_j x^j \mapsto \widehat{\alpha}\left(x^{-1}\right) = \widehat{\alpha_0} + y^{-1}\sum_{j=1}^{3} \widehat{\alpha_j} x^{4-j}.$$

Proof (i) By Lemma 2.2(iii) and Lemma 4.2(iv), we see that $\varphi_{\mu(i)}^{-1}\mu\varphi_i$ is a ring isomorphism from R_i onto $R_{\mu(i)}$ such that the following diagram commutes

$$\begin{array}{ccc} R_i = \mathbb{Z}_4[y]/\langle f_i(y)\rangle & \stackrel{\varphi_{\mu(i)}^{-1}\mu\varphi_i}{\longrightarrow} & R_{\mu(i)} = \mathbb{Z}_4[y]/\langle f_{\mu(i)}(y)\rangle \\ \varphi_i \downarrow & & \downarrow \varphi_{\mu(i)} \\ \mathcal{A}_i & \stackrel{\mu}{\longrightarrow} & \mathcal{A}_{\mu(i)} \end{array}$$

Then for any $\xi = a(y) \in R_i$, by $\varepsilon_{\mu(i)}(y) = 1 - h_i(y) f_{\mu(i)}(y)$ we have

$$\begin{aligned}\widehat{\xi} &= \left(\varphi_{\mu(i)}^{-1}\mu\varphi_i\right)(\xi) = \varphi_{\mu(i)}^{-1}\mu(\varepsilon_i(y)a(y))) \\ &= \varphi_{\mu(i)}^{-1}\left(\varepsilon_{\mu(i)}(y)a(y^{-1})\right) = \left(1 - h_i(y) f_{\mu(i)}(y)\right) a\left(y^{-1}\right) \\ &\equiv a\left(y^{-1}\right) \left(\text{mod } f_{\mu(i)}(y)\right),\end{aligned}$$

which implies $\widehat{\xi} = a(y^{-1}) \in R_{\mu(i)}$.

(ii) As $y \in R_i$, by (i) we deduce that $\widehat{y} = y^{-1} \in R_{\mu(i)}$ and $y^{-1} = y^{n-1}$ (mod $f_{\mu(i)}(y)$). Since x and y are invertible elements of $R_{\mu(i)}[x]/\langle x^4 - y\rangle$, we have $\langle \mu(x^4 - y)\rangle = \langle (x^{-1})^4 - y^{-1}\rangle = \langle -x^{-4}y^{-1}(x^4 - y)\rangle = \langle x^4 - y\rangle$ as ideals of the ring $R_{\mu(i)}[x]/\langle x^4 - y\rangle$. Hence μ induces a ring isomorphism from $R_i[x]/\langle x^4 - y\rangle$ onto $R_{\mu(i)}[x]/\langle x^4 - y\rangle$ by the rule that $\mu(\alpha(x)) = \widehat{\alpha}(x^{-1}) = \sum_{j=0}^{3} \widehat{\alpha}_j x^{-j}$. Finally, by $x^4 = y$, i.e., $y^{-1}x^4 = 1$ in $R_{\mu(i)}[x]/\langle x^4 - y\rangle$ it follows that $\mu(\alpha(x)) = \widehat{\alpha}_0 + y^{-1}\sum_{j=1}^{3} \widehat{\alpha}_j x^{4-j}$ as required. □

Lemma 4.4 *Let* $a(x) = \sum_{i=1}^{r} a_i(x)$, $b(x) = \sum_{i=1}^{r} b_i(x) \in \mathcal{A}[x]/\langle x^4 - y\rangle$, *where* $a_i(x), b_i(x) \in \mathcal{A}_i[x]/\langle \varepsilon_i(y)x^4 - \varepsilon_i(y)y\rangle$. *Then*

$$a(x)\mu(b(x)) = \sum_{i=1}^{r} a_i(x)\mu(b_{\mu(i)}(x)).$$

Proof By Lemma 4.2(iv), we have

$$\mu\left(b_{\mu(i)}(x)\right) \in \mu\left(\mathcal{A}_{\mu(i)}[x]/\left\langle \varepsilon_{\mu(i)}(y)x^4 - \varepsilon_{\mu(i)}y\right\rangle\right) = \mathcal{A}_i[x]/\left\langle \varepsilon_i(y)x^4 - \varepsilon_i(y)y\right\rangle.$$

Hence $a_i(x)\mu(b_{\mu(i)}(x)) \in \mathcal{A}_i[x]/\langle \varepsilon_i(y)x^4 - \varepsilon_i(y)y\rangle$ for all i. If $j \neq \mu(i)$, then $i \neq \mu(j)$, which implies $\mathcal{A}_i\mathcal{A}_{\mu(j)} = \{0\}$ by Lemma 2.2(ii). Therefore,

$$\left(\mathcal{A}_i[x]/\langle \varepsilon_i(y)x^4 - \varepsilon_i(y)y\rangle\right)\left(\mathcal{A}_{\mu(j)}[x]/\langle \varepsilon_{\mu(j)}(y)x^4 - \varepsilon_{\mu(j)}(y)y\rangle\right) = \{0\},$$

and so $a_i(x)\mu(b_j(x)) = 0$ since $\mu(b_j(x)) \in \mathcal{A}_{\mu(j)}[x]/\langle \varepsilon_{\mu(j)}(y)x^4 - \varepsilon_{\mu(j)}(y)y\rangle$. Hence $a(x)\mu(b(x)) = \sum_{i=1}^{r}\sum_{j=1}^{r} a_i(x)\mu(b_j(x)) = \sum_{i=1}^{r} a_i(x)\mu(b_{\mu(i)}(x))$. □

Now, we can give the dual code of each cyclic code over $\mathbb{Z}_4$ of length $4n$.

Theorem 4.5 *Let* $\mathcal{C}$ *be a cyclic code over* $\mathbb{Z}_4$ *of length* $4n$ *with concatenated structure* $\mathcal{C} = \oplus_{i=1}^{r}(\mathcal{A}_i \Box_{\varphi_i} C_i)$, *where* C_i *is an ideal of the ring* $R_i[x]/\langle x^4 - y\rangle$ *listed by Theorem 3.3 for all* $i = 1, \ldots, r$. *Using the notations of Theorem 3.3, the dual code* $\mathcal{C}^{\perp}$ *is given by*

$$\mathcal{C}^{\perp} = \oplus_{i=1}^{r}\left(\mathcal{A}_{\mu(i)}\Box_{\varphi_{\mu(i)}} D_{\mu(i)}\right),$$

where $D_{\mu(i)} = \mu(\mathrm{Ann}(C_i))$, which is an ideal of the ring $R_{\mu(i)}[x]/\langle x^4 - y\rangle$ given in the following table.

Case	$C_i \pmod{x^4 - y, f_i(y)}$	$D_{\mu(i)} = \mu(\mathrm{Ann}(C_i)) \pmod{x^4 - y, f_{\mu(i)}(y)}$
1.	$\langle 0\rangle$	$\langle 1\rangle$
2.	$\langle 1\rangle$	$\langle 0\rangle$
3.	$\langle \pi_i^j\rangle$ $(j = 1, 2)$	$\langle \pi_{\mu(i)}^{4-j} + 2\pi_{\mu(i)}^{2-j} y^{2e} x^2\rangle$
4.	$\langle 2\rangle$	$\langle 2\rangle$
5.	$\langle 2\pi_i^s\rangle$ $(s = 1, 2, 3)$	$\langle \pi_{\mu(i)}^{4-s}, 2\rangle$
6.	$\langle \pi_i + 2h\rangle$ $(h \in \mathcal{T}_i\backslash\{0\})$	$\langle \pi_{\mu(i)}^3 + 2\pi_{\mu(i)}(1 + \pi_{\mu(i)}\widehat{h} y^{n-e} x^{4n-1}) y^{2e} x^2\rangle$
7.	$\langle \pi_i^2 + 2\pi_i h\rangle$ $(h \in \mathcal{T}_i\backslash\{0\})$	$\langle \pi_{\mu(i)}^2 + 2(1 + \pi_{\mu(i)}\widehat{h} y^{n-e} x^{4n-1}) y^{2e} x^2\rangle$
8.	$\langle \pi_i^2 + 2(h + \pi_i g)\rangle$ $(h \in \mathcal{T}_i\backslash\{0, 1\}, g \in \mathcal{T}_i)$	$\langle \pi_{\mu(i)}^2 + 2(1 + \widehat{h} + \pi_{\mu(i)}\widehat{g} y^{n-e} x^{4n-1}) y^{2e} x^2\rangle$
9.	$\langle \pi_i^2 + 2(1 + \pi_i h)\rangle$ $(h \in \mathcal{T}_i\backslash\{0\})$	$\langle \pi_{\mu(i)}^2 + 2\pi_{\mu(i)}\widehat{h} y^e x\rangle$
10.	$\langle \pi_i^3 + 2\pi_i(1 + \pi_i h)\rangle$ $(h \in \mathcal{T}_i\backslash\{0\})$	$\langle \pi_{\mu(i)} + 2\widehat{h} y^e x\rangle$
11.	$\langle \pi_i^3 + 2h\rangle$ $(h \in \mathcal{T}_i)$	$\langle \pi_{\mu(i)}^3 + 2\widehat{h} y^{3e} x^3\rangle$
13.	$\langle \pi_i^j + 2\pi_i^{j-2}\rangle$ $(j = 2, 3)$	$\langle \pi_{\mu(i)}^{4-j}\rangle$
14.	$\langle \pi_i^j, 2\rangle$ $(j = 1, 2, 3)$	$\langle 2\pi_{\mu(i)}^{4-j}\rangle$
15.	$\langle \pi_i^2 + 2, 2\pi_i\rangle$	$\langle \pi_{\mu(i)}^3, 2\pi_{\mu(i)}^2\rangle$
16.	$\langle \pi_i^3, 2\pi_i^2\rangle$	$\langle \pi_{\mu(i)}^2 + 2y^{2e} x^2, 2\pi_{\mu(i)}\rangle$
17.	$\langle \pi_i^3 + 2\pi_i, 2\pi_i^2\rangle$	$\langle \pi_{\mu(i)}^2, 2\pi_{\mu(i)}\rangle$
18.	$\langle \pi_i^2, 2\pi_i\rangle$	$\langle \pi_{\mu(i)}^3 + 2\pi_{\mu(i)} y^{2e} x^2, 2\pi_{\mu(i)}^2\rangle$
19.	$\langle \pi_i^2 + 2h, 2\pi_i\rangle$ $(h \in \mathcal{T}_i\backslash\{0, 1\})$	$\langle \pi_{\mu(i)}^3 + 2\pi_{\mu(i)}(1 + \widehat{h}) y^{2e} x^2, 2\pi_{\mu(i)}^2\rangle$
20.	$\langle \pi_i^3 + 2\pi_i h, 2\pi_i^2\rangle$ $(h \in \mathcal{T}_i\backslash\{0, 1\})$	$\langle \pi_{\mu(i)}^2 + 2(1 + \widehat{h}) y^{2e} x^2, 2\pi_{\mu(i)}\rangle$

where $\widehat{h} = b_0 + \sum_{j=1}^{m_i-1} b_j y^{n-j} \pmod{f_{\mu(i)}(y)}$ and $\widehat{g} = g_0 + \sum_{j=1}^{m_i-1} g_j y^{n-j} \pmod{f_{\mu(i)}(y)}$ for any $h = \sum_{j=0}^{m_i-1} b_j y^j$, $g = \sum_{j=0}^{m_i-1} g_j y^j \in \mathcal{T}_i$.

Proof For any integer i, $1 \le i \le r$, let $D_{\mu(i)} = \mu(\mathrm{Ann}(C_i))$. Then $D_{\mu(i)}$ is an ideal of the ring $R_{\mu(i)}[x]/\langle x^4 - y\rangle$. Set $\mathcal{D} = \oplus_{i=1}^r(\mathcal{A}_{\mu(i)} \Box_{\varphi_{\mu(i)}} D_{\mu(i)}) = \oplus_{j=1}^r(\mathcal{A}_j \Box_{\varphi_j} D_j)$, where $D_j = \mu(\mathrm{Ann}(C_{\mu(j)}))$. Then $\mathcal{D}$ is an ideal of $\mathcal{A}[x]/\langle x^4 - y\rangle$. Since $(\mathcal{A}_i \Box_{\varphi_i} C_i) \cdot \mu(\mathcal{A}_{\mu(i)} \Box_{\varphi_{\mu(i)}} D_{\mu(i)}) = (\mathcal{A}_i \Box_{\varphi_i} C_i) \cdot (\mathcal{A}_i \Box_{\varphi_i} \mathrm{Ann}(C_i)) = \varepsilon_i(y)(C_i \cdot \mathrm{Ann}(C_i)) = \{0\}$, by Lemma 4.4 we have $\mathcal{C} \cdot \mu(\mathcal{D}) = \sum_{i=1}^r (\mathcal{A}_i \Box_{\varphi_i} C_i) \cdot \mu(\mathcal{A}_{\mu(i)} \Box_{\varphi_{\mu(i)}} D_{\mu(i)}) = \{0\}$. Hence $\mathcal{D} \subseteq \mathcal{C}^{\perp}$ by Lemma 4.1.

On the other hand, by Theorem 3.3 we see that $|C_i||\mathrm{Ann}(C_i)| = 2^{8m_i}$ for all $i = 1, \ldots, r$, which implies

$$
\begin{aligned}
|\mathcal{C}||\mathcal{D}| &= \prod_{i=1}^{r} |\mathcal{A}_i \Box_{\varphi_i} C_i||\mathcal{A}_{\mu(i)} \Box_{\varphi_{\mu(i)}} D_{\mu(i)}| = \prod_{i=1}^{r} |C_i||D_{\mu(i)}| \\
&= \prod_{i=1}^{r} |C_i||\mathrm{Ann}(C_i)| = 4^{4\sum_{i=1}^{r} m_i} = 4^{4n} \\
&= |\mathbb{Z}_4[x]/\langle x^{4n} - 1\rangle|.
\end{aligned}
$$

As stated above, we conclude that $\mathcal{C}^{\perp} = \mathcal{D}$ since $\mathbb{Z}_4$ is a finite chain ring.

It is clear that $x^{4n} = y^n = 1$ in $R_i[x]/\langle x^4 - y\rangle$ for any $i = 1, \ldots, r$. Now, for any integer l, $1 \le l \le 3$, by Eq. (3) we have

$$
\begin{aligned}
\mu\left(\pi_i^l\right) &= \left(\mu\left(y^e x - 1\right)\right)^l = \left(\left(y^{-1}\right)^e x^{-1} - 1\right)^l = (-1)^l y^{-el} x^{-l} \left(y^e x - 1\right)^l \\
&= (-1)^l y^{-el} x^{-l} \pi_{\mu(i)}^l = (-1)^l y^{n-el} x^{4n-l} \pi_{\mu(i)}^l \in R_{\mu(i)}[x]/\left\langle x^4 - y\right\rangle.
\end{aligned}
$$

Then the conclusions follow from Theorem 3.3, Lemma 4.3 and direct calculations. □

Finally, we list all distinct self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$ by the following corollary.

Corollary 4.6 *Using the notations in Theorem 4.5 and Lemma 4.2*(ii)*, let $\mathcal{C}$ be a cyclic code over $\mathbb{Z}_4$ of length $4n$ with $\mathcal{C} = \oplus_{i=1}^{r}(\mathcal{A}_i \Box_{\varphi_i} C_i)$, where C_i is an ideal of $R_i[x]/\langle x^4 - y\rangle$. Then $\mathcal{C}$ is self-dual if and only if for each integer i, $1 \le i \le r$, C_i satisfies the following conditions:*

(i) *If $1 \le i \le \lambda$, C_i is given by one of the following three cases:*

$$\langle 2\rangle, \ \left\langle \pi_i^2 + 2\left(1 + \pi_i\right)\right\rangle, \ \left\langle \pi_i^3\right\rangle.$$

(ii) *If $i = \lambda + j$ where $1 \le j \le \rho$, then C_i is an ideal of $R_i[x]/\langle x^4 - y\rangle$ and $C_{i+\rho} = \mu(\mathrm{Ann}(C_i))$ which is given in the table of Theorem 4.5.*

Hence the number of all self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$ is equal to

$$3^{\lambda} \prod_{j=\lambda+1}^{\lambda+\rho} \left(9 + 5 \cdot 2^{m_i} + 2^{2m_i}\right).$$

Proof Using the notations in Lemma 4.2(ii), by Theorem 4.5 we have

$$
\begin{aligned}
\mathcal{C} &= \oplus_{i=1}^{\lambda}(\mathcal{A}_i \Box_{\varphi_i} C_i) \oplus \left(\oplus_{i=\lambda+1}^{\lambda+\rho}\left((\mathcal{A}_i \Box_{\varphi_i} C_i) \oplus (\mathcal{A}_{i+\rho} \Box_{\varphi_{i+\rho}} C_{i+\rho})\right)\right), \\
\mathcal{C}^{\perp} &= \oplus_{i=1}^{\lambda}(\mathcal{A}_i \Box_{\varphi_i} D_i) \oplus \left(\oplus_{i=\lambda+1}^{\lambda+\rho}\left((\mathcal{A}_i \Box_{\varphi_i} D_i) \oplus (\mathcal{A}_{i+\rho} \Box_{\varphi_{i+\rho}} D_{i+\rho})\right)\right),
\end{aligned}
$$

where $D_i = D_{\mu(i)} = \mu(\mathrm{Ann}(C_i))$ for all $i = 1, \ldots, \lambda$, $D_i = D_{\mu(i+\rho)} = \mu(\mathrm{Ann}(C_{i+\rho}))$ and $D_{i+\rho} = D_{\mu(i)} = \mu(\mathrm{Ann}(C_i))$ for all $i = \lambda + 1, \ldots, \lambda + \rho$.

Now, by Theorem 2.6 we conclude that $\mathcal{C} = \mathcal{C}^{\perp}$ if and only if $C_i = D_i$ for all $i = 1, \ldots, \lambda + 2\rho$. Precisely, $C_i = D_i$ if and only if C_i satisfies the following conditions:

(i) Let $1 \leq i \leq \lambda$. Then $C_i = D_{\mu(i)} = \mu(\mathrm{Ann}(C_i))$. By Theorem 4.5, C_i must be given by one of the following five cases:
- $\langle 2 \rangle$.
- $\langle \pi_i^2 + 2\pi_i h \rangle$, where $h \in \mathcal{T}_i \backslash \{0\}$ satisfying $h - (1 + \pi_i \widehat{h} y^{-e} x^{-1}) y^{2e} x^2 \equiv 0 \pmod{x^4 - y, f_i(y), 2}$, i.e., $((1 + \widehat{h}) y^{2e}) x^2 + (\widehat{h} y^e) x + h \equiv 0 \pmod{x^4 - y, f_i(y), 2}$. It is clear that there is no $h \in \mathcal{T}_i \backslash \{0\}$ satisfying this condition.
- $\langle \pi_i^2 + 2(h + \pi_i g) \rangle$, where $h \in \mathcal{T}_i \backslash \{0, 1\}$ and $g \in \mathcal{T}_i$ satisfying $h + \pi_i g - (1 + \widehat{h} + \pi_i \widehat{g} y^{-e} x^{-1}) y^{2e} x^2 \equiv 0 \pmod{x^4 - y, f_i(y), 2}$, i.e., $((1 + \widehat{h} + \widehat{g}) y^{2e}) x^2 + ((g + \widehat{g}) y^e) x + (h + g) \equiv 0 \pmod{x^4 - y, f_i(y), 2}$. It is clear that there is no $h \in \mathcal{T}_i \backslash \{0, 1\}$ and $g \in \mathcal{T}_i$ satisfying this condition.
- $\langle \pi_i^2 + 2(1 + \pi_i h) \rangle$, where $h \in \mathcal{T}_i \backslash \{0\}$ satisfying $1 + \pi_i h - \pi_i \widehat{h} y^e x \equiv 0 \pmod{x^4 - y, f_i(y), 2}$, i.e., $((h + \widehat{h}) y^e) x + (1 + h) \equiv 0 \pmod{x^4 - y, f_i(y), 2}$. It is clear that the condition is equivalent to $h = 1$.
- $\langle \pi_i^3 + 2h \rangle$, where $h \in \mathcal{T}_i$ satisfying $h - \widehat{h} y^{3e} x^3 \equiv 0 \pmod{x^4 - y, f_i(y), 2}$. It is clear that the condition is equivalent to $h = 0$.

As stated above, we conclude that C_i must be given by one of the following three cases: $\langle 2 \rangle$, $\langle \pi_i^2 + 2(1 + \pi_i) \rangle$, $\langle \pi_i^3 \rangle$.

(ii) Let $i = \lambda + j$ where $1 \leq j \leq \rho$. Then $C_{i+\rho} = D_{i+\rho} = D_{\mu(i)} = \mu(\mathrm{Ann}(C_i))$ as $\mu(i) = i + \rho$. Furthermore, $C_{i+\rho} = D_{i+\rho} = \mu(\mathrm{Ann}(C_i))$ implies $D_i = D_{\mu(i+\rho)} = \mu(\mathrm{Ann}(C_{i+\rho})) = \mu(\mathrm{Ann}(\mu(\mathrm{Ann}(C_i))) = C_i$.

Therefore, $(C_i, C_{i+\rho})$ is determined completely by the ideal C_i of $R_i[x]/\langle x^4 - y \rangle$ and the relation $C_{i+\rho} = \mu(\mathrm{Ann}(C_i))$. Hence the number of pairs of $(C_i, C_{i+\rho})$ is equal to $N_{(4,m_i,2)} = 9 + 5 \cdot 2^{m_i} + 2^{2m_i}$ by Lemma 3.2.

Finally, from (i) and (ii) we deduce that number of all self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$ is equal to $3^{\lambda} \prod_{i=\lambda+1}^{\lambda+\rho} (9 + 5 \cdot 2^{m_i} + 2^{2m_i})$. □

5 Examples

In this section, we give all self-dual cyclic codes over $\mathbb{Z}_4$ of length 28 and 60.

◇ In the case of $N = 28 = 4n$ where $n = 7$, it is known that $y^7 - 1 = f_1(y) f_2(y) f_3(y)$, where $f_1(y) = y - 1$, $f_2(y) = y^3 + 2y^2 + y + 3$ and $f_3(y) = y^3 + 3y^2 + 2y + 3$ are pairwise coprime monic basic irreducible polynomials in $\mathbb{Z}_4[y]$. Obviously, $\widetilde{f_1}(y) = \delta_1 f_1(y)$ and $\widetilde{f_2}(y) = \delta_2 f_3(y)$ where $\delta_1 = \delta_2 = -1$, which implies that $\mu(1) = 1$ and $\mu(2) = 3$. Hence $m_1 = 1$, $m_2 = m_3 = 3$, $r = 3$ and $\lambda = \rho = 1$. By Lemma 3.2 and Corollary 4.6, the number of cyclic codes and the number of self-dual cyclic codes over $\mathbb{Z}_4$ of length 28 is equal to

$\prod_{i=1}^{3} N_{(4,m_i;2)} = \prod_{i=1}^{3}(9+5\cdot 2^{m_i}+2^{2m_i}) = 23\cdot 113^2 = 293,687$ and $3\cdot 113 = 339$, respectively.

Using the notations in Sect. 2, for each integer i, $1 \leq i \leq 3$, we denote $F_i(y) = \frac{y^7-1}{f_i(y)}$, 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 $\varepsilon_i(y) \equiv u_i(y)F_i(y) \pmod{y^7-1}$. Precisely, we have

$$\varepsilon_1(y) = 3+3y+3y^2+3y^3+3y^4+3y^5+3y^6;$$
$$\varepsilon_2(y) = 1+3y+3y^2+2y^3+3y^4+2y^5+2y^6;$$
$$\varepsilon_3(y) = 1+2y+2y^2+3y^3+2y^4+3y^5+3y^6.$$

Let $\mathcal{A} = \mathbb{Z}_4[y]/\langle y^7-1\rangle$ and $\mathcal{A}_i = \mathcal{A}\varepsilon_i(y)$. Then $\mathcal{A}_i$ is a basic irreducible cyclic code over $\mathbb{Z}_4$ of length 7 with parity check polynomial $f_i(y)$ for $i = 1, 2, 3$. Precisely, we know that

- $\mathcal{A}_1$ is a free $\mathbb{Z}_4$-submodule of $\mathbb{Z}_4^7$, $\mathrm{rank}_{\mathbb{Z}_4}(\mathcal{A}_1) = 1$, and a generator matrix is given by $G_{\mathcal{A}_1} = (3,3,3,3,3,3,3)$. Hence $\mathcal{A}_1 = \{(a,a,a,a,a,a,a) \mid a \in \mathbb{Z}_4\}$ and $d_{\min}(\mathcal{A}_1) = 7$.
- $\mathcal{A}_2$ is a free $\mathbb{Z}_4$-submodule of $\mathbb{Z}_4^7$, $\mathrm{rank}_{\mathbb{Z}_4}(\mathcal{A}_2) = 3$, and a generator matrix is given by $G_{\mathcal{A}_2} = \begin{pmatrix} 1&3&3&2&3&2&2\\ 2&1&3&3&2&3&2\\ 2&2&1&3&3&2&3 \end{pmatrix}$. Hence $\mathcal{A}_2 = \{wG_{\mathcal{A}_2} \mid w \in \mathbb{Z}_4^3\}$ and $d_{\min}(\mathcal{A}_2) = 4$.
- $\mathcal{A}_3$ is a free $\mathbb{Z}_4$-submodule of $\mathbb{Z}_4^7$, $\mathrm{rank}_{\mathbb{Z}_4}(\mathcal{A}_3) = 3$, and a generator matrix is given by $G_{\mathcal{A}_3} = \begin{pmatrix} 1&2&2&3&2&3&3\\ 3&1&2&2&3&2&3\\ 3&3&1&2&2&3&2 \end{pmatrix}$. Hence $\mathcal{A}_3 = \{wG_{\mathcal{A}_3} \mid w \in \mathbb{Z}_4^3\}$ and $d_{\min}(\mathcal{A}_3) = 4$.

Denote $R_i = \mathbb{Z}_4[y]/\langle f_i(y)\rangle$. Obviously, $4\cdot 5 \equiv -1 \pmod 7$, which implies $(y^5)^4 = y^{-1}$ by $y^7 = 1$ in R_i for all $i = 1, 2, 3$. Using the notations in Sect. 3, we have $e = 5$. Therefore, by Corollary 4.6 we conclude that all distinct self-dual cyclic codes over $\mathbb{Z}_4$ of length 28 are given by

$$\mathcal{C} = (\mathcal{A}_1 \Box_{\varphi_1} C_1) \oplus (\mathcal{A}_2 \Box_{\varphi_2} C_2) \oplus (\mathcal{A}_3 \Box_{\varphi_3} C_3),$$

where C_i is a y-constacyclic code over R_i of length 4, i.e., an ideal of the ring $R_i[x]/\langle x^4-y\rangle$, satisfying the following conditions:

- C_1 is is an ideal of $\mathbb{Z}_4/\langle x^4-1\rangle$ given by one of the following 3 cases:

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

- (C_2, C_3) is given by one of the following 113 cases, since $y^{-5}x^{-1} = yx^3$, $(y^5x)^2 = y^3x^2$ and $(y^5x)^3 = yx^3$:

Case	C_2 (mod x^4-y, $f_2(y)$)	C_3 (mod x^4-y, $f_3(y)$)	L_C
1.	$\langle 0\rangle$	$\langle 1\rangle$	1
2.	$\langle 1\rangle$	$\langle 0\rangle$	1
3.	$\langle \pi_2^j\rangle$ $(j=1,2)$	$\langle \pi_3^{4-j}+2\pi_3^{2-j}y^3x^2\rangle$	2
4.	$\langle 2\rangle$	$\langle 2\rangle$	1
5.	$\langle 2\pi_2^s\rangle$ $(s=1,2,3)$	$\langle \pi_3^{4-s},2\rangle$	3
6.	$\langle \pi_2+2h\rangle$ $(h\in\mathcal{T}_2\backslash\{0\})$	$\langle \pi_3^3+2\pi_3(1+\pi_3\widehat{h}yx^3)y^3x^2\rangle$	7
7.	$\langle \pi_2^2+2\pi_2h\rangle$ $(h\in\mathcal{T}_2\backslash\{0\})$	$\langle \pi_3^2+2(1+\pi_3\widehat{h}yx^3)y^3x^2\rangle$	7
8.	$\langle \pi_2^2+2(h+\pi_2g)\rangle$ $(h\in\mathcal{T}_2\backslash\{0,1\},g\in\mathcal{T}_2)$	$\langle \pi_3^2+2(1+\widehat{h}+\pi_3\widehat{g}yx^3)y^3x^2\rangle$	48
9.	$\langle \pi_2^2+2(1+\pi_2h)\rangle$ $(h\in\mathcal{T}_2\backslash\{0\})$	$\langle \pi_3^2+2\pi_3\widehat{h}y^5x\rangle$	7
10.	$\langle \pi_2^3+2\pi_2(1+\pi_2h)\rangle$ $(h\in\mathcal{T}_2\backslash\{0\})$	$\langle \pi_3+2\widehat{h}y^5x\rangle$	7
11.	$\langle \pi_2^3+2h\rangle$ $(h\in\mathcal{T}_2)$	$\langle \pi_3^3+2\widehat{h}yx^3\rangle$	8
13.	$\langle \pi_2^j+2\pi_2^{j-2}\rangle$ $(j=2,3)$	$\langle \pi_3^{4-j}\rangle$	2
14.	$\langle \pi_2^j,2\rangle$ $(j=1,2,3)$	$\langle 2\pi_3^{4-j}\rangle$	3
15.	$\langle \pi_2^2+2,2\pi_2\rangle$	$\langle \pi_3^3,2\pi_3^2\rangle$	1
16.	$\langle \pi_2^3,2\pi_2^2\rangle$	$\langle \pi_3^2+2y^3x^2,2\pi_3\rangle$	1
17.	$\langle \pi_2^3+2\pi_2,2\pi_2^2\rangle$	$\langle \pi_3^2,2\pi_3\rangle$	1
18.	$\langle \pi_2^2,2\pi_2\rangle$	$\langle \pi_3^3+2\pi_3y^3x^2,2\pi_3^2\rangle$	1
19.	$\langle \pi_2^2+2h,2\pi_2\rangle$ $(h\in\mathcal{T}_2\backslash\{0,1\})$	$\langle \pi_3^3+2\pi_3(1+\widehat{h})y^3x^2,2\pi_3^2\rangle$	6
20.	$\langle \pi_2^3+2\pi_2h,2\pi_2^2\rangle$ $(h\in\mathcal{T}_2\backslash\{0,1\})$	$\langle \pi_3^2+2(1+\widehat{h})y^3x^2,2\pi_3\rangle$	6

where $\mathcal{T}_2=\{\sum_{j=0}^{2}t_jy^j \mid t_0,t_1,t_2\in\{0,1\}\}$ and L_C is the number of pairs (C_2,C_3) in the same row. Furthermore, we have the following

- $\pi_1=y^5x-1=x-1\in R_1[x]/\langle x^4-1\rangle$ where $R_1=\mathbb{Z}_4[y]/\langle f_1(y)\rangle=\mathbb{Z}_4$;
- $\pi_2=y^5x-1=(y^2+3y+3)x-1\in R_2[x]/\langle x^4-y\rangle$ since $y^5\equiv y^2+3y+3$ (mod $f_2(y)$);
- $\pi_3=y^5x-1=(2y^2+3y+3)x-1\in R_3[x]/\langle x^4-y\rangle$ since $y^5\equiv 2y^2+3y+3$ (mod $f_3(y)$),

and $\varphi_i:R_i\to\mathcal{A}_i$ is given by

- $\varphi_1(a)=a\varepsilon_1(y)$ for all $a\in R_1$;
- $\varphi_i(a(y))=a(y)\varepsilon_i(y)$ for all $a(y)\in R_i$, $i=2,3$.

Next, by an example we describe how to obtain an encoder for each self-dual code over $\mathbb{Z}_4$ of length 28 listed above. Choose $\mathcal{C}=(\mathcal{A}_1\Box_{\varphi_1}C_1)\oplus(\mathcal{A}_2\Box_{\varphi_2}C_2)\oplus(\mathcal{A}_3\Box_{\varphi_3}C_3)$, where $C_1=\langle(x-1)^3\rangle$, $C_2=\langle\pi_2^2+2(1+\pi_2h)\rangle$ and $C_3=\langle\pi_3^2+2\pi_3\widehat{h}y^5x\rangle$ in which $h=y+y^2$. As $y^7=1$ we have $\widehat{h}=y^{-1}+(y^{-1})^2=y^5+y^6$.

By Cases 11 and 9 in Theorem 3.3, it follows that $|C_1| = 2^{4m_1} = 4^2$ and $|C_2| = |C_3| = 2^{4m_2} = 4^6$, which implies $|\mathcal{C}| = |C_1||C_2||C_3| = 4^{14}$. Furthermore, we have the following:

- $C_1 = \langle 3+3x+x^2+x^3\rangle$. Then a generator matrix of the cyclic code C_1 over R_1 is $G_{C_1} = \begin{pmatrix} 3&3&1&1\\ 1&3&3&1\\ 1&1&3&3\\ 3&1&1&3 \end{pmatrix}$. Since the companion matrix of $f_1(y) = y-1$ is $M_{f_1} = (1)$, by Theorem 2.5 a generator matrix of $\mathcal{A}_1\Box_{\varphi_1}C_1$ is given by

$$G_{\mathcal{A}_1\Box_{\varphi_1}C_1} = \begin{pmatrix} 3G_{\mathcal{A}_1} & 3G_{\mathcal{A}_1} & G_{\mathcal{A}_1} & G_{\mathcal{A}_1}\\ G_{\mathcal{A}_1} & 3G_{\mathcal{A}_1} & 3G_{\mathcal{A}_1} & G_{\mathcal{A}_1}\\ G_{\mathcal{A}_1} & G_{\mathcal{A}_1} & 3G_{\mathcal{A}_1} & 3G_{\mathcal{A}_1}\\ 3G_{\mathcal{A}_1} & G_{\mathcal{A}_1} & G_{\mathcal{A}_1} & 3G_{\mathcal{A}_1} \end{pmatrix}$$
$$= \left(\begin{array}{c|c|c|c} 1\,1\,1\,1\,1\,1\,1 & 1\,1\,1\,1\,1\,1\,1 & 3\,3\,3\,3\,3\,3\,3 & 3\,3\,3\,3\,3\,3\,3\\ \hline 3\,3\,3\,3\,3\,3\,3 & 1\,1\,1\,1\,1\,1\,1 & 1\,1\,1\,1\,1\,1\,1 & 3\,3\,3\,3\,3\,3\,3\\ \hline 3\,3\,3\,3\,3\,3\,3 & 3\,3\,3\,3\,3\,3\,3 & 1\,1\,1\,1\,1\,1\,1 & 1\,1\,1\,1\,1\,1\,1\\ \hline 1\,1\,1\,1\,1\,1\,1 & 3\,3\,3\,3\,3\,3\,3 & 3\,3\,3\,3\,3\,3\,3 & 1\,1\,1\,1\,1\,1\,1 \end{array}\right).$$

- $C_2 = \langle (3+2y+2y^2)+(2+2y)x+(1+3y+2y^2)x^2\rangle$. Then a generator matrix of the y-constacyclic code C_2 over R_2 is given by

$$G_{C_2} = \begin{pmatrix} \alpha_2 & \beta_2 & \gamma_2 & 0\\ 0 & \alpha_2 & \beta_2 & \gamma_2\\ y\gamma_2 & 0 & \alpha_2 & \beta_2\\ y\beta_2 & y\gamma_2 & 0 & \alpha_2 \end{pmatrix},$$

where $\alpha_2 = 3+2y+2y^2$, $\beta_2 = 2+2y$, $\gamma_2 = 1+3y+2y^2$, $y\beta_2 = 2y+2y^2$ and $y\gamma_2 = 2+3y+3y^2$. Using the notations of Theorem 2.5, we have

$$A_{\alpha_2} = 3I_3 + 2M_{f_2} + 2M_{f_2}^2 = \begin{pmatrix} 3&2&2\\ 2&1&2\\ 2&0&1 \end{pmatrix},$$
$$A_{\beta_2} = 2I_3 + 2M_{f_2} = \begin{pmatrix} 2&2&0\\ 0&2&2\\ 2&2&2 \end{pmatrix},$$
$$A_{\gamma_2} = I_3 + 3M_{f_2} + 2M_{f_2}^2 = \begin{pmatrix} 1&3&2\\ 2&3&3\\ 3&3&1 \end{pmatrix},$$
$$A_{y\beta_2} = 2M_{f_2} + 2M_{f_2}^2 = \begin{pmatrix} 0&2&2\\ 2&2&2\\ 2&0&2 \end{pmatrix},$$

$$A_{y\gamma_2} = 2I_3 + 3M_{f_2} + 3M_{f_2}^2 = \begin{pmatrix} 2 & 3 & 3 \\ 3 & 3 & 1 \\ 1 & 2 & 1 \end{pmatrix}.$$

Since the companion matrix of $f_2(y)$ is $M_{f_2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 3 & 2 \end{pmatrix}$, by Theorem 2.5 a generator matrix of $\mathcal{A}_2 \Box_{\varphi_2} C_2$ is given by

$$G_{\mathcal{A}_2 \Box_{\varphi_2} C_2} = \begin{pmatrix} A_{\alpha_2} G_{\mathcal{A}_2} & A_{\beta_2} G_{\mathcal{A}_2} & A_{\gamma_2} G_{\mathcal{A}_2} & 0 \\ 0 & A_{\alpha_2} G_{\mathcal{A}_2} & A_{\beta_2} G_{\mathcal{A}_2} & A_{\gamma_2} G_{\mathcal{A}_2} \\ A_{y\gamma_2} G_{\mathcal{A}_2} & 0 & A_{\alpha_2} G_{\mathcal{A}_2} & A_{\beta_2} G_{\mathcal{A}_2} \\ A_{y\beta_2} G_{\mathcal{A}_2} & A_{y\gamma_2} G_{\mathcal{A}_2} & 0 & A_{\alpha_2} G_{\mathcal{A}_2} \end{pmatrix}$$

$$= \left(\begin{array}{ccccccc|ccccccc|ccccccc|ccccccc}
3&3&1&2&3&0&0&2&0&0&2&2&2&0&3&2&2&1&3&3&2&0&0&0&0&0&0&0 \\
0&3&3&1&2&3&0&0&2&0&0&2&2&2&2&3&2&2&1&3&3&0&0&0&0&0&0&0 \\
0&0&3&3&1&2&3&2&0&2&0&0&2&2&3&2&3&2&2&1&3&0&0&0&0&0&0&0 \\ \hline
0&0&0&0&0&0&0&3&3&1&2&3&0&0&2&0&0&2&2&2&0&3&2&2&1&3&3&2 \\
0&0&0&0&0&0&0&0&3&3&1&2&3&0&0&2&0&0&2&2&2&2&3&2&2&1&3&3 \\
0&0&0&0&0&0&0&0&0&3&3&1&2&3&2&0&2&0&0&2&2&3&2&3&2&2&1&3 \\ \hline
2&3&2&2&1&3&3&0&0&0&0&0&0&0&3&3&1&2&3&0&0&2&0&0&2&2&2&0 \\
3&2&3&2&2&1&3&0&0&0&0&0&0&0&0&3&3&1&2&3&0&0&2&0&0&2&2&2 \\
3&3&2&3&2&2&1&0&0&0&0&0&0&0&0&0&3&3&1&2&3&2&0&2&0&0&2&2 \\ \hline
0&2&0&0&2&2&2&2&3&2&2&1&3&3&0&0&0&0&0&0&0&3&3&1&2&3&0&0 \\
2&0&2&0&0&2&2&3&2&3&2&2&1&3&0&0&0&0&0&0&0&0&3&3&1&2&3&0 \\
2&2&0&2&0&0&2&3&3&2&3&2&2&1&0&0&0&0&0&0&0&0&0&3&3&1&2&3
\end{array}\right).$$

- $C_3 = \langle 1 + 2x + (1 + 3y^2)x^2 \rangle$. Then a generator matrix of the y-constacyclic code C_3 over R_3 is given by

$$G_{C_3} = \begin{pmatrix} 1 & 2 & \alpha_3 & 0 \\ 0 & 1 & 2 & \alpha_3 \\ y\alpha_3 & 0 & 1 & 2 \\ 2y & y\alpha_3 & 0 & 1 \end{pmatrix},$$

  where $\alpha_3 = 1 + 3y^2$, $y\alpha_3 = 3 + 3y + 3y^2$. Using the notations in Theorem 2.5, we have $A_y = M_{f_3}$ and

$$A_{\alpha_3} = I_3 + 3M_{f_3}^2 = \begin{pmatrix} 1 & 0 & 3 \\ 3 & 3 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$A_{y\alpha_3} = 3I_3 + 3M_{f_3} + 3M_{f_3}^2 = \begin{pmatrix} 3 & 3 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 3 \end{pmatrix}.$$

Since the companion matrix of $f_3(y)$ is $M_{f_3} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 2 & 1 \end{pmatrix}$, by Theorem 2.5 a generator matrix of $\mathcal{A}_3\Box_{\varphi_2}C_3$ is given by

$$G_{\mathcal{A}_3\Box_{\varphi_2}C_3} = \begin{pmatrix} G_{\mathcal{A}_3} & 2G_{\mathcal{A}_3} & A_{\alpha_3}G_{\mathcal{A}_3} & 0 \\ 0 & G_{\mathcal{A}_3} & 2G_{\mathcal{A}_3} & A_{\alpha_3}G_{\mathcal{A}_3} \\ A_{y\alpha_3}G_{\mathcal{A}_3} & 0 & G_{\mathcal{A}_3} & 2G_{\mathcal{A}_3} \\ 2M_{f_3}G_{\mathcal{A}_3} & A_{y\alpha_3}G_{\mathcal{A}_3} & 0 & G_{\mathcal{A}_3} \end{pmatrix}$$
$$= \left(\begin{array}{c|c|c|c} 1\,2\,2\,3\,2\,3\,3 & 2\,0\,0\,2\,0\,2\,2 & 2\,3\,1\,1\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0 \\ 3\,1\,2\,2\,3\,2\,3 & 2\,2\,0\,0\,2\,0\,2 & 1\,2\,3\,1\,1\,0\,0 & 0\,0\,0\,0\,0\,0\,0 \\ 3\,3\,1\,2\,2\,3\,2 & 2\,2\,2\,0\,0\,2\,0 & 0\,1\,2\,3\,1\,1\,0 & 0\,0\,0\,0\,0\,0\,0 \\ \hline 0\,0\,0\,0\,0\,0\,0 & 1\,2\,2\,3\,2\,3\,3 & 2\,0\,0\,2\,0\,2\,2 & 2\,3\,1\,1\,0\,0\,1 \\ 0\,0\,0\,0\,0\,0\,0 & 3\,1\,2\,2\,3\,2\,3 & 2\,2\,0\,0\,2\,0\,2 & 1\,2\,3\,1\,1\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0 & 3\,3\,1\,2\,2\,3\,2 & 2\,2\,2\,0\,0\,2\,0 & 0\,1\,2\,3\,1\,1\,0 \\ \hline 1\,2\,3\,1\,1\,0\,0 & 0\,0\,0\,0\,0\,0\,0 & 1\,2\,2\,3\,2\,3\,3 & 2\,0\,0\,2\,0\,2\,2 \\ 0\,1\,2\,3\,1\,1\,0 & 0\,0\,0\,0\,0\,0\,0 & 3\,1\,2\,2\,3\,2\,3 & 2\,2\,0\,0\,2\,0\,2 \\ 0\,0\,1\,2\,3\,1\,1 & 0\,0\,0\,0\,0\,0\,0 & 3\,3\,1\,2\,2\,3\,2 & 2\,2\,2\,0\,0\,2\,0 \\ \hline 2\,2\,0\,0\,2\,0\,2 & 1\,2\,3\,1\,1\,0\,0 & 0\,0\,0\,0\,0\,0\,0 & 1\,2\,2\,3\,2\,3\,3 \\ 2\,2\,2\,0\,0\,2\,0 & 0\,1\,2\,3\,1\,1\,0 & 0\,0\,0\,0\,0\,0\,0 & 3\,1\,2\,2\,3\,2\,3 \\ 0\,2\,2\,2\,0\,0\,2 & 0\,0\,1\,2\,3\,1\,1 & 0\,0\,0\,0\,0\,0\,0 & 3\,3\,1\,2\,2\,3\,2 \end{array}\right).$$

Then by Corollary 3.5, a generator matrix of the self-dual cyclic code $\mathcal{C}$ over $\mathbb{Z}_4$ of length 28 is given by $G_{\mathcal{C}} = \begin{pmatrix} G_{\mathcal{A}_1\Box_{\varphi_1}C_1} \\ G_{\mathcal{A}_2\Box_{\varphi_2}C_2} \\ G_{\mathcal{A}_3\Box_{\varphi_3}C_3} \end{pmatrix}$. Now, by performing a reduction on $G_{\mathcal{C}}$ we obtain a standard generator matrix of the self-dual cyclic code $\mathcal{C}$ over $\mathbb{Z}_4$ of length 28 given by $\mathbf{G} = \begin{pmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \cdots \\ \mathbf{g}_{14} \end{pmatrix}$, where

$$\mathbf{g}_1 = (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3);$$

$$\begin{aligned}
\mathbf{g}_2 &= (3,3,3,3,3,3,3,1,1,1,1,1,1,1,1,1,1,1,1,1,1,3,3,3,3,3,3,3);\\
\mathbf{g}_3 &= (3,3,1,2,3,0,0,2,0,0,2,2,2,0,3,2,2,1,3,3,2,0,0,0,0,0,0,0);\\
\mathbf{g}_4 &= (0,3,3,1,2,3,0,0,2,0,0,2,2,2,2,3,2,2,1,3,3,0,0,0,0,0,0,0);\\
\mathbf{g}_5 &= (0,0,3,3,1,2,3,2,0,2,0,0,2,2,3,2,3,2,2,1,3,0,0,0,0,0,0,0);\\
\mathbf{g}_6 &= (0,0,0,0,0,0,0,3,3,1,2,3,0,0,2,0,0,2,2,2,0,3,2,2,1,3,3,2);\\
\mathbf{g}_7 &= (0,0,0,0,0,0,0,0,3,3,1,2,3,0,0,2,0,0,2,2,2,2,3,2,2,1,3,3);\\
\mathbf{g}_8 &= (0,0,0,0,0,0,0,0,0,3,3,1,2,3,2,0,2,0,0,2,2,3,2,3,2,2,1,3);\\
\mathbf{g}_9 &= (1,2,2,3,2,3,3,2,0,0,2,0,2,2,2,3,1,1,0,0,1,0,0,0,0,0,0,0);\\
\mathbf{g}_{10} &= (3,1,2,2,3,2,3,2,2,0,0,2,0,2,1,2,3,1,1,0,0,0,0,0,0,0,0,0);\\
\mathbf{g}_{11} &= (3,3,1,2,2,3,2,2,2,2,0,0,2,0,0,1,2,3,1,1,0,0,0,0,0,0,0,0);\\
\mathbf{g}_{12} &= (0,0,0,0,0,0,0,1,2,2,3,2,3,3,2,0,0,2,0,2,2,2,3,1,1,0,0,1);\\
\mathbf{g}_{13} &= (0,0,0,0,0,0,0,3,1,2,2,3,2,3,2,2,0,0,2,0,2,1,2,3,1,1,0,0);\\
\mathbf{g}_{14} &= (0,0,0,0,0,0,0,3,3,1,2,2,3,2,2,2,2,0,0,2,0,0,1,2,3,1,1,0).
\end{aligned}$$

Therefore, $\mathcal{C}$ is encoded by

$$\mathcal{C} = \left\{\underline{u}\mathbf{G} \mid \underline{u} \in \mathbb{Z}_4^{14}\right\} = \left\{\sum_{j=1}^{14} u_j \mathbf{g}_j \mid u_1, \ldots, u_{14} \in \mathbb{Z}_4\right\}.$$

Precisely, the Hamming weight enumerator of the self-dual cyclic code $\mathcal{C}$ over $\mathbb{Z}_4$ of length 28 is given by

$$\begin{aligned}
W_C^{(H)}(Y) = 1 &+ 14Y^2 + 91Y^4 + 364Y^6 + 448Y^7 + 1001Y^8 + 4032Y^9\\
&+18130Y^{10} + 41216Y^{11} + 154875Y^{12} + 344064Y^{13} + 890472Y^{14}\\
&+1828736Y^{15} + 3660475Y^{16} + 6340992Y^{17} + 9985234Y^{18}\\
&+13558272Y^{19} + 17731945Y^{20} + 19586560Y^{21} + 20430956Y^{22}\\
&+16488640Y^{23} + 11621211Y^{24} + 6754496Y^{25} + 3548174Y^{26}\\
&+1112832Y^{27} + 114497Y^{28}.
\end{aligned}$$

◇ In the case of $N = 60 = 4 \cdot 15$. Using the notations of Lemma 4.2, by Example 3.4 we see that

$$\widetilde{f_1}(y) = -f_1(y),\ \widetilde{f_2}(y) = f_2(y),\ \widetilde{f_3}(y) = f_3(y) \text{ and } \widetilde{f_4}(y) = f_5(y),$$

which imply $\mu(4) = 5$ and $\mu(i) = i$ for $i = 1, 2, 3$. Hence $\lambda = 3$ and $\rho = 1$. From these and by Corollary 4.6, we deduce that the number of self-dual cyclic codes over $\mathbb{Z}_4$ of length 60 is equal to $3^3 \cdot 345 = 9315$.

Specifically, all distinct self-dual cyclic codes over $\mathbb{Z}_4$ of length 60 are the following:

$$(\mathcal{A}_1 \Box_{\varphi_1} C_1) \oplus (\mathcal{A}_2 \Box_{\varphi_2} C_2) \oplus (\mathcal{A}_3 \Box_{\varphi_3} C_3) \oplus (\mathcal{A}_4 \Box_{\varphi_4} C_4) \oplus (\mathcal{A}_5 \Box_{\varphi_5} C_5),$$

- For each integer i, $1 \le i \le 3$, C_i is given by one of the following cases:

$$\langle 2 \rangle\,,\ \left\langle \pi_i^2 + 2(1+\pi_i) \right\rangle,\ \left\langle \pi_i^3 \right\rangle,$$

  which are y-constacyclic codes over R_i of length 4.
- As $x^{-1} = x^{59} = (x^4)^{14}x^3 = y^{14}x^3$, we have $y^{-11}x^{-1} = y^3x^3$ and $y^{22} = y^7$. By Theorem 4.5 and Corollary 4.6, (C_4, C_5) is given by one of the following cases:

Case	C_4 (mod $x^4 - y,\ f_4(y)$)	C_5 (mod $x^4 - y,\ f_5(y)$)	L_C
1.	$\langle 0 \rangle$	$\langle 1 \rangle$	1
2.	$\langle 1 \rangle$	$\langle 0 \rangle$	1
3.	$\langle \pi_4^j \rangle$ $(j = 1, 2)$	$\langle \pi_5^{4-j} + 2\pi_5^{2-j} y^7 x^2 \rangle$	2
4.	$\langle 2 \rangle$	$\langle 2 \rangle$	1
5.	$\langle 2\pi_4^s \rangle$ $(s = 1, 2, 3)$	$\langle \pi_5^{4-s}, 2 \rangle$	3
6.	$\langle \pi_4 + 2h \rangle$ $(h \in \mathcal{T}_4\backslash\{0\})$	$\langle \pi_5^3 + 2\pi_5(1 + \pi_5\widehat{h}y^3x^3)y^7x^2 \rangle$	15
7.	$\langle \pi_4^2 + 2\pi_4 h \rangle$ $(h \in \mathcal{T}_4\backslash\{0\})$	$\langle \pi_5^2 + 2(1 + \pi_5\widehat{h}y^3x^3)y^7x^2 \rangle$	15
8.	$\langle \pi_4^2 + 2(h + \pi_4 g) \rangle$ $(h \in \mathcal{T}_4\backslash\{0, 1\}, g \in \mathcal{T}_4)$	$\langle \pi_5^2 + 2(1 + \widehat{h} + \pi_5\widehat{g}y^3x^3)y^7x^2 \rangle$	224
9.	$\langle \pi_4^2 + 2(1 + \pi_4 h) \rangle$ $(h \in \mathcal{T}_4\backslash\{0\})$	$\langle \pi_5^2 + 2\pi_5\widehat{h}y^{11}x \rangle$	15
10.	$\langle \pi_4^3 + 2\pi_4(1 + \pi_4 h) \rangle$ $(h \in \mathcal{T}_4\backslash\{0\})$	$\langle \pi_5 + 2\widehat{h}y^{11}x \rangle$	15
11.	$\langle \pi_4^3 + 2h \rangle$ $(h \in \mathcal{T}_4)$	$\langle \pi_5^3 + 2\widehat{h}y^3x^3 \rangle$	16
13.	$\langle \pi_4^j + 2\pi_4^{j-2} \rangle$ $(j = 2, 3)$	$\langle \pi_5^{4-j} \rangle$	2
14.	$\langle \pi_4^j, 2 \rangle$ $(j = 1, 2, 3)$	$\langle 2\pi_5^{4-j} \rangle$	3
15.	$\langle \pi_4^2 + 2, 2\pi_4 \rangle$	$\langle \pi_5^3, 2\pi_5^2 \rangle$	1
16.	$\langle \pi_4^3, 2\pi_4^2 \rangle$	$\langle \pi_5^2 + 2y^7x^2, 2\pi_5 \rangle$	1
17.	$\langle \pi_4^3 + 2\pi_4, 2\pi_4^2 \rangle$	$\langle \pi_5^2, 2\pi_5 \rangle$	1
18.	$\langle \pi_4^2, 2\pi_4 \rangle$	$\langle \pi_5^3 + 2\pi_5 y^7x^2, 2\pi_5^2 \rangle$	1
19.	$\langle \pi_4^2 + 2h, 2\pi_4 \rangle$ $(h \in \mathcal{T}_4\backslash\{0, 1\})$	$\langle \pi_5^3 + 2\pi_5(1 + \widehat{h})y^7x^2, 2\pi_5^2 \rangle$	14
20.	$\langle \pi_4^3 + 2\pi_4 h, 2\pi_4^2 \rangle$ $(h \in \mathcal{T}_4\backslash\{0, 1\})$	$\langle \pi_5^2 + 2(1 + \widehat{h})y^7x^2, 2\pi_5 \rangle$	14

where $\mathcal{T}_4 = \{\sum_{j=0}^{3} t_j y^j \mid t_0, t_1, t_2, t_3 \in \{0, 1\}\}$ and L_C is the number of pairs (C_4, C_5) in the same row.

Finally, we list the number $\mathcal{N}$ of self-dual cyclic codes over $\mathbb{Z}_4$ of length $4n$, where n is odd and $12 \le 4n \le 100$, by the following table.

$4n$	$\mathcal{N}$	$4n$	$\mathcal{N}$	$4n$	$\mathcal{N}$
12, 20, 44, 52, 76	9	28	339	84	4,500,225
36, 68, 100	27	60	9315	92	12,613,659

6 Conclusions

We have given precise description for cyclic codes over $\mathbb{Z}_4$, present precisely dual codes and investigate self-duality for cyclic codes over $\mathbb{Z}_4$ of length $4n$. These codes enjoy a rich algebraic structure compared to arbitrary linear codes (which makes the search process much simpler). Obtaining some bounds for minimal distance such as BCH-like of a cyclic code over the ring $\mathbb{Z}_4$ by just looking at the concatenated structure would be rather interesting.

Acknowledgments Part of this work was done when Yonglin Cao was visiting Chern Institute of Mathematics, Nankai University, Tianjin, China. Yonglin Cao would like to thank the institution for the kind hospitality. This research is supported in part by the National Key Basic Research Program of China (Grant No. 2013CB834204) and the National Natural Science Foundation of China (Grant Nos. 11471255, 61171082).

References

1. Abualrub, T., Oehmke, R.: On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e. IEEE-IT **49**(9), 2126–2133 (2003)
2. Blackford, T.: Cyclic codes over $\mathbb{Z}_4$ of oddly even length. Discret. 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. Dougherty, S.T., Ling, S.: Cyclic codes over $\mathbb{Z}_4$ of even length. Des. Codes Cryptogr. **39**, 127–153 (2006)
5. Pless, V.S., Qian, Z.: Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. IEEE-IT **42**(5), 1594–1600 (1996)
6. Wan, Z.-X.: Cyclic codes over Galois rings. Algebra Colloq. **6**(3), 291–304 (1999)
7. Wan, Z.-X.: Quaternary Codes. World Scientific, Hackensack (1997)