AAECC (2021) 32:459–493
https://doi.org/10.1007/s00200-019-00408-9

ORIGINAL PAPER

On self-duality and hulls of cyclic codes over $\frac{\mathbb{F}_{2^m}[u]}{\langle u^k\rangle}$ with oddly even length

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

Received: 18 December 2018 / Revised: 12 November 2019 / Accepted: 26 November 2019 / Published online: 5 December 2019

Abstract

Let $\mathbb{F}_{2^m}$ be a finite field of 2^m elements and denote $R=\mathbb{F}_{2^m}[u]/\langle u^k\rangle=\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}+\cdots+u^{k-1}\mathbb{F}_{2^m}$ ($u^k=0$), where k is an integer satisfying $k\geq 2$. For any odd positive integer n, an explicit representation for every self-dual cyclic code over R of length $2n$ and a mass formula to count the number of these codes are given. In particular, a generator matrix is provided for the self-dual 2-quasi-cyclic code of length $4n$ over $\mathbb{F}_{2^m}$ derived by an arbitrary self-dual cyclic code of length $2n$ over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ and a Gray map from $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ onto $\mathbb{F}_{2^m}^2$. Finally, the hull of each cyclic code with length $2n$ over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ is determined and all distinct self-orthogonal cyclic codes of length $2n$ over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ are listed.

Keywords Cyclic code · Self-dual code · Hull · Self-orthogonal code · Finite chain ring

Mathematics Subject Classification 94B15 · 94B05 · 11T71

✉ Yuan Cao
yuancao@sdut.edu.cn

Yonglin Cao
ylcao@sdut.edu.cn

Fang-Wei Fu
fwfu@nankai.edu.cn

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

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

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

4 Chern Institute of Mathematics and LPMC, and Tianjin Key Laboratory of Network and Data Security Technology, Nankai University, Tianjin 300071, China

1 Introduction and preliminaries

The class of self-dual codes is an interesting topic in coding theory due to their connections to other fields of mathematics such as lattices, cryptography, invariant theory, block designs [5], etc. In many instances, self-dual codes have been found by first finding a code over a ring and then mapping this code onto a code over a subring through a map that preserves duality. In the literatures, the mappings typically map to codes over $\mathbb{F}_2$, $\mathbb{F}_4$ and $\mathbb{Z}_4$ since codes over these rings have had the most use.

Throughout this paper, let $\mathbb{F}_{2^m}$ be a finite field of 2^m elements and denote

$$R = \frac{\mathbb{F}_{2^m}[u]}{\langle u^k\rangle} = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + \cdots + u^{k-1}\mathbb{F}_{2^m} \ (u^k = 0),$$

where $k \in \mathbb{Z}^+$ satisfying $k \geq 2$. Then R is a finite chain ring. Let N be a fixed positive integer and denote $R^N = \{(a_0, a_1, \ldots, a_{N-1}) \mid a_0, a_1, \ldots, a_{N-1} \in R\}$. Then R^N is a free R-module with the usual componentwise addition and scalar multiplication by elements of R. Any R-submodule $\mathcal{C}$ of R^N is called a *linear code* over R of length N. Moreover, the linear code $\mathcal{C}$ is said to be *cyclic* if $(c_{N-1}, c_0, \ldots, c_{N-2}) \in \mathcal{C}$ for all $(c_0, \ldots, c_{N-2}, c_{N-1}) \in \mathcal{C}$. The usual Euclidean inner product on R^N is defined by: $[\alpha, \beta] = \sum_{i=0}^{N-1} a_i b_i \in R$ for all $\alpha = (a_0, a_1, \ldots, a_{N-1}), \beta = (b_0, b_1, \ldots, b_{N-1}) \in R^N$. Then the *dual code* of $\mathcal{C}$ is defined by $\mathcal{C}^{\perp} = \{\beta \in R^N \mid [\alpha, \beta] = 0, \ \forall \alpha \in \mathcal{C}\}$, and $\mathcal{C}$ is said to be *self-dual* (resp. *self-orthogonal*) if $\mathcal{C} = \mathcal{C}^{\perp}$ (resp. $\mathcal{C} \subseteq \mathcal{C}^{\perp}$).

When $k = 2$ and $m = 1$, cyclic codes, self-dual codes and Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$ were studied by [6] and [10]. Ling and Solé studied Type II codes over the ring $\mathbb{F}_4 + u\mathbb{F}_4$ in [16], which was later generalized to the ring $R = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ in [4]. The common theme in the aforementioned works is that the map ϕ, defined by $\phi(a + bu) = (b, a + b)$ for all $a, b \in \mathbb{F}_{2^m}$, is a distance and duality preserving Gray map from R onto $\mathbb{F}_{2^m}^2$. The map ϕ takes codes over R of length N to codes over $\mathbb{F}_{2^m}$ of length $2N$. There were many literatures on the construction of binary self-dual codes from various kind of codes over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ for $m = 1, 2$. Please refer to the literature [12–15].

When $k \geq 3$, for any finite field $\mathbb{F}_q$ of q elements, several different Gray type maps were defined, in similar fashion obtaining different notions of distance for linear codes over $\frac{\mathbb{F}_q[u]}{\langle u^k\rangle}$, and a method to obtain explicitly new self-dual codes over $\mathbb{F}_q$ of larger length was presented from self-dual codes over $\frac{\mathbb{F}_q[u]}{\langle u^k\rangle}$ in [3]. Hence the construction and enumeration for self-dual codes over $\frac{\mathbb{F}_q[u]}{\langle u^k\rangle}$ for various prime power q and positive integer k becomes a central topic in coding theory over finite rings.

Let $\frac{R[x]}{\langle x^N-1\rangle} = R[x]/\langle x^N - 1\rangle = \{\sum_{0\leq i\leq N-1} a_i x^i \mid a_0, a_1, \ldots, a_{N-1} \in R\}$ in which the arithmetic is done modulo $x^N - 1$. In this paper, cyclic codes over R of length N are identified with ideals of the ring $\frac{R[x]}{\langle x^N-1\rangle}$, under the map

$$\sigma : R^N \to R[x]/\langle x^N - 1\rangle \text{ via } \sigma : (a_0, a_1, \ldots, a_{N-1}) \mapsto \sum_{i=0}^{N-1} a_i x^i$$

($\forall a_0, a_1, \ldots, a_{N-1} \in R$). Moreover, ideals of $\frac{R[x]}{\langle x^N-1\rangle}$ are called *simple-root cyclic codes* over R when N is relatively prime to the characteristic of R and called *repeated-root cyclic codes* otherwise.

There were many literatures on cyclic codes of length N over finite chain rings $R=\mathbb{F}_{2^m}[u]/\langle u^k\rangle$ for various positive integers m, k, N. For example: When $k=2$, cyclic codes and self-dual codes over $\mathbb{F}_2+u\mathbb{F}_2$ of odd length N were investigated in [6]. Norton and Sălăgean [17] discussed simple-root cyclic codes over an arbitrary finite chain ring R systematically. Dinh [9] studied constacyclic codes over Galois extension rings of $\mathbb{F}_2+u\mathbb{F}_2$ of length $N=2^s$.

When $k\geq 3$, in 2007 Abualrub and Siap [1] studied cyclic codes over the rings $\mathbb{Z}_2+u\mathbb{Z}_2$ and $\mathbb{Z}_2+u\mathbb{Z}_2+u^2\mathbb{Z}_2$ of the length n, where either n is odd or $n=2k$ (k is odd) or n is a power of 2. This paper did not investigate self-dual cyclic codes over rings $\mathbb{Z}_2+u\mathbb{Z}_2$ and $\mathbb{Z}_2+u\mathbb{Z}_2+u^2\mathbb{Z}_2$, but asked a question:

◇ Open problems include the study of self-dual codes and their properties.

In 2011, Al-Ashker and Hamoudeh [2] extended some of the results in [1], and studied cyclic codes of an arbitrary length over the ring $\mathbb{Z}_2+u\mathbb{Z}_2+u^2\mathbb{Z}_2+\cdots+u^{k-1}\mathbb{Z}_2$ with $u^k=0$. The rank and minimal spanning set of this family of codes were studied and two open problems were asked:

◇ The study of cyclic codes of an arbitrary length over $\mathbb{Z}_p+u\mathbb{Z}_p+u^2\mathbb{Z}_p+\cdots+u^{k-1}\mathbb{Z}_p$, where p is a prime integer, $u^k=0$, and the study of dual and self-dual codes and their properties over these rings.

In 2015, Singh et al. [19] studied cyclic code over the ring $R_{k,p}=\mathbb{Z}_p[u]/\langle u^k\rangle$ $=\mathbb{Z}_p+u\mathbb{Z}_p+u^2\mathbb{Z}_p+\cdots+u^{k-1}\mathbb{Z}_p$ for any prime integer p and positive integer N, where N allows that $p|N$. However, the dual code and self-duality for each cyclic code over $R_{k,p}$ were not considered in [19].

In 2016, Chen et al. [8] gave some new necessary and sufficient conditions for the existence of nontrivial self-dual simple-root cyclic codes over finite commutative chain rings and studied explicit enumeration formulas for these codes. But self-dual repeated-root cyclic codes over finite commutative chain rings were not considered in [8].

In 2015, Sangwisut et al. [18] studied the hulls of simple-root cyclic and negacyclic codes over a finite field $\mathbb{F}_q$. Based on the characterization of their generator polynomials, the dimensions of the hulls of cyclic and negacyclic codes over $\mathbb{F}_q$ were determined and the enumerations for hulls of cyclic codes and negacyclic codes over $\mathbb{F}_q$ were established. However, in the literature, the representation for the hulls of repeated-root cyclic codes over the ring $\mathbb{F}_q+u\mathbb{F}_q$ ($u^2=0$) have not been well studied.

In 2016, we [7] gave a different approach from [1], [2] and [19] to study cyclic code over $R=\frac{\mathbb{F}_{2^m}[u]}{\langle u^k\rangle}$ of length $2n$ for any odd positive integer n. We provided an explicit representation for each cyclic code, gave clear formulas to calculate the number of codewords in each code and the number of all these cyclic codes respectively. In particular, we determined the dual code for each code and presented a criterion to judge whether a cyclic code over R of length $2n$ is self-dual. Based on that, we study the self-duality and hulls of cyclic codes over $\frac{\mathbb{F}_{2^m}[u]}{\langle u^k\rangle}$ with oddly even length in this paper.

The present paper is organized as follows. In Sect. 2, we introduce necessary notations and sketch known results for cyclic codes over R of length $2n$ needed in this paper. In Sect. 3, we give an explicit representation and enumeration for self-dual cyclic codes over R of length $2n$. Moreover, we obtain a clear Mass formula to count all these codes. In Sect. 4, we provide a generator matrix for each self-dual 2-quasi-cyclic code of length $4n$ over $\mathbb{F}_{2^m}$ derived by a self-deal cyclic code of length $2n$ over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$. As an application, we list all 945 self-dual cyclic codes of length 30 over $\mathbb{F}_2+u\mathbb{F}_2$. In Sect. 5, we determine the hull of each cyclic code of length $2n$ over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$, and give an explicit representation and enumeration for all distinct self-orthogonal cyclic codes of length $2n$ over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$. Section 6 concludes the paper.

2 Known results for cyclic codes over *R* of length 2*n*

In this section, we list the necessary notations and known results for cyclic codes of length $2n$ over the ring $R=\frac{\mathbb{F}_{2^m}[u]}{\langle u^k\rangle}$ needed in the following sections.

As n is odd, there are pairwise coprime monic irreducible polynomials $f_1(x)=x-1, f_2(x),\ldots,f_r(x)$ in $\mathbb{F}_{2^m}[x]$ such that

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

Then we have $x^{2n}-1=(x^n-1)^2=f_1(x)^2\ldots f_r(x)^2$.

Let $1\leq j\leq r$. We assume $\deg(f_j(x))=d_j$ and denote $F_j(x)=\frac{x^{2n}-1}{f_j(x)^2}$. Then $\gcd(F_j(x),f_j(x)^2)=1$, and hence there exist $a_j(x),b_j(x)\in\mathbb{F}_{2^m}[x]$ such that $a_j(x)F_j(x)+b_j(x)f_j(x)^2=1$.

As in [7], we adopt the following notations in this paper:

- $\mathcal{A}=\frac{\mathbb{F}_{2^m}[x]}{\langle x^{2n}-1\rangle}=\{\sum_{i=0}^{2n-1}a_ix^i\mid a_i\in\mathbb{F}_{2^m},\ i=0,1,\ldots,2n-1\}$ in which the arithmetic is done modulo $x^{2n}-1$.
- Let $\varepsilon_j(x)\in\mathcal{A}$ be defined by

$$\varepsilon_j(x)\equiv a_j(x)F_j(x)=1-b_j(x)f_j(x)^2 \pmod{x^{2n}-1}.$$

  Then $\varepsilon_j(x)^2=\varepsilon_j(x)$ and $\varepsilon_j(x)\varepsilon_l(x)=0$ in the ring $\mathcal{A}$ for all $j\neq l$ and $j,l=1,\ldots,r$ (cf. [7, Theorem 2.3]).
- $\mathcal{K}_j=\frac{\mathbb{F}_{2^m}[x]}{\langle f_j(x)^2\rangle}=\{\sum_{i=0}^{2d_j-1}a_ix^i\mid a_i\in\mathbb{F}_{2^m},\ i=0,1,\ldots,2d_j-1\}$ in which the arithmetic is done modulo $f_j(x)^2$.
- $\mathcal{F}_j=\frac{\mathbb{F}_{2^m}[x]}{\langle f_j(x)\rangle}=\{\sum_{i=0}^{d_j-1}a_ix^i\mid a_i\in\mathbb{F}_{2^m},\ i=0,1,\ldots,d_j-1\}$ in which the arithmetic is done modulo $f_j(x)$. Then $\mathcal{F}_j$ is an extension field of $\mathbb{F}_{2^m}$ with 2^{md_j} elements.
- For each $\Upsilon\in\{\mathcal{A},\mathcal{K}_j,\mathcal{F}_j\}$, we set

$$\frac{\Upsilon[u]}{\langle u^k\rangle}=\{\alpha_0+u\alpha_1+\cdots+u^{k-1}\alpha_{k-1}\mid \alpha_0,\alpha_1,\ldots,\alpha_{k-1}\in\Upsilon\}\ (u^k=0).$$

Remark $\mathcal{F}_j$ is a finite field with operations defined by the usual polynomial operations modulo $f_j(x)$, $\mathcal{K}_j$ is a finite chain ring with operations defined by the usual polynomial operations modulo $f_j(x)^2$ (cf. [7, Lemma 2.4(v)]) and $\mathcal{A}$ is a finite principal ideal ring with operations defined by the usual polynomial operations modulo $x^{2n}-1$. As in [7], we adopt the following points of view:

$$\mathcal{F}_j \subseteq \mathcal{K}_j \subseteq \mathcal{A} \text{ and } \frac{\mathcal{F}_j[u]}{\langle u^k\rangle} \subseteq \frac{\mathcal{K}_j[u]}{\langle u^k\rangle} \subseteq \frac{\mathcal{A}[u]}{\langle u^k\rangle}$$

only as sets. Obviously, $\mathcal{F}_j$ is not a subfield of $\mathcal{K}_j$, $\mathcal{K}_j$ is not a subring of $\mathcal{A}$, $\frac{\mathcal{F}_j[u]}{\langle u^k\rangle}$ is not a subring of $\frac{\mathcal{K}_j[u]}{\langle u^k\rangle}$ and $\frac{\mathcal{K}_j[u]}{\langle u^k\rangle}$ is not a subring of $\frac{\mathcal{A}[u]}{\langle u^k\rangle}$, when $n \geq 2$.

For any $\alpha(x) = \sum_{i=0}^{2n-1} \alpha_i x^i \in \frac{R[x]}{\langle x^{2n}-1\rangle}$, where $\alpha_i = \sum_{j=0}^{k-1} a_{i,j}u^j \in R$ with $a_{i,j} \in \mathbb{F}_{2^m}$ for all $i = 0, 1, \ldots, 2n-1$ and $j = 0, 1, \ldots, k-1$, we define

$$\Psi(\alpha(x)) = a_0(x) + a_1(x)u + \cdots + a_{k-1}(x)u^{k-1} \in \frac{\mathcal{A}[u]}{\langle u^k\rangle}$$

where $a_j(x) = \sum_{i=0}^{2n-1} a_{i,j}x^i \in \mathcal{A}$ for all $j = 0, 1, \ldots, k-1$. Then the map Ψ is a ring isomorphism from $\frac{R[x]}{\langle x^{2n}-1\rangle}$ onto $\frac{\mathcal{A}[u]}{\langle u^k\rangle}$ (cf. [7], Lemma 2.2).

As in [7], we identify $\frac{R[x]}{\langle x^{2n}-1\rangle}$ with $\frac{\mathcal{A}[u]}{\langle u^k\rangle}$ under this ring isomorphism Ψ in the rest of this paper. From this, we deduce that $\mathcal{C}$ is a cyclic code over R of length $2n$, i.e. $\mathcal{C}$ is an ideal of $\frac{R[x]}{\langle x^{2n}-1\rangle}$, if and only if $\mathcal{C}$ is an ideal of the ring $\frac{\mathcal{A}[u]}{\langle u^k\rangle}$. Then in order to determine cyclic codes over R of length $2n$, it is sufficient to determine ideals of the ring $\frac{\mathcal{A}[u]}{\langle u^k\rangle}$.

First, every ideal of the ring $\frac{\mathcal{A}[u]}{\langle u^k\rangle}$ can be determined by a unique ideal of $\frac{\mathcal{K}_j[u]}{\langle u^k\rangle}$ for each $j = 1, \ldots, r$. See the following lemma.

Lemma 2.1 (cf. [7, Theorem 2.3]) *Let $\mathcal{C} \subseteq \frac{\mathcal{A}[u]}{\langle u^k\rangle}$. Then $\mathcal{C}$ is a cyclic code over R of length $2n$ if and only if for each integer j, $1 \leq j \leq r$, there is a unique ideal C_j of the ring $\frac{\mathcal{K}_j[u]}{\langle u^k\rangle}$ such that*

$$\mathcal{C} = \bigoplus_{j=1}^{r} \varepsilon_j(x)C_j = \sum_{j=1}^{r} \varepsilon_j(x)C_j \ (\mathrm{mod}\ x^{2n}-1),$$

where $\varepsilon_j(x)C_j = \{\varepsilon_j(x)c_j(x) \ (\mathrm{mod}\ x^{2n}-1) \mid c_j(x) \in C_j\} \subseteq \frac{\mathcal{A}[u]}{\langle u^k\rangle}$ for all $j = 1, \ldots, r$. Moreover, the number of codewords in $\mathcal{C}$ is equal to $\prod_{j=1}^{r} |C_j|$.

To present all distinct ideals of the ring $\mathcal{K}_j[u]/\langle u^k\rangle$ for all $j = 1, \ldots, r$, we need the following lemma.

Lemma 2.2 (cf. [7, Lemma 2.4 (ii)–(iv)]) *Using the notations above, for any integers j, s: $1 \leq j \leq r$ and $1 \leq s \leq k$, we have the following:*

(i) *The ring* $\frac{\mathcal{F}_j[u]}{\langle u^s\rangle}$ *is a finite commutative chain ring with the unique maximal ideal* $u(\frac{\mathcal{F}_j[u]}{\langle u^s\rangle})$*, the nilpotency index of* u *is equal to* s *and the residue field of* $\frac{\mathcal{F}_j[u]}{\langle u^s\rangle}$ *is* $(\frac{\mathcal{F}_j[u]}{\langle u^s\rangle})/u(\frac{\mathcal{F}_j[u]}{\langle u^s\rangle}) \cong \mathcal{F}_j$.

(ii) *Every element* α *of* $\frac{\mathcal{F}_j[u]}{\langle u^s\rangle}$ *has a unique* u*-adic expansion:*

$$\alpha = b_0(x) + ub_1(x) + \cdots + u^{s-1}b_{s-1}(x),\ b_0(x), b_1(x), \ldots, b_{s-1}(x) \in \mathcal{F}_j$$

Moreover, α *is an invertible element of* $\frac{\mathcal{F}_j[u]}{\langle u^s\rangle}$ *if and only if* $b_0(x) \neq 0$. *The set of all invertible elements of* $\frac{\mathcal{F}_j[u]}{\langle u^s\rangle}$ *is denoted by* $(\frac{\mathcal{F}_j[u]}{\langle u^s\rangle})^\times$.

(iii) $|(\frac{\mathcal{F}_j[u]}{\langle u^s\rangle})^\times| = (2^{md_j} - 1)2^{(s-1)md_j}$.

Using the notation of Lemma 2.2, all ideals of $\frac{\mathcal{K}_j[u]}{\langle u^k\rangle}$ are listed as follows:

Lemma 2.3 ([7, Theorem 2.6]) *Let* $1 \leq j \leq r$. *Then all distinct ideals of the ring* $\frac{\mathcal{K}_j[u]}{\langle u^k\rangle}$ *are given by the following table:*

Number of ideals	C_j (ideal of $\frac{\mathcal{K}_j[u]}{\langle u^k\rangle}$)	$\|C_j\|$
$k+1$	• $\langle u^i\rangle$ $(0 \leq i \leq k)$	$2^{2md_j(k-i)}$
k	• $\langle u^s f_j(x)\rangle$ $(0 \leq s \leq k-1)$	$2^{md_j(k-s)}$
$\Omega_1(2^{md_j}, k)$	• $\langle u^i + u^t f_j(x)\omega\rangle$ $(\omega \in (\frac{\mathcal{F}_j[u]}{\langle u^{i-t}\rangle})^\times, t \geq 2i-k,$ $0 \leq t < i \leq k-1)$	$2^{2md_j(k-i)}$
$\Omega_2(2^{md_j}, k)$	• $\langle u^i + u^t f_j(x)\omega\rangle$ $(\omega \in (\frac{\mathcal{F}_j[u]}{\langle u^{k-i}\rangle})^\times, t < 2i-k,$ $0 \leq t < i \leq k-1)$	$2^{md_j(k-t)}$
$\frac{1}{2}k(k-1)$	• $\langle u^i, u^s f_j(x)\rangle$ $(0 \leq s < i \leq k-1)$	$2^{md_j(2k-(i+s))}$
$(2^{md_j}-1) \cdot\Gamma(2^{md_j}, k)$	• $\langle u^i + u^t f_j(x)\omega, u^s f_j(x)\rangle$ $(\omega \in (\frac{\mathcal{F}_j[u]}{\langle u^{s-t}\rangle})^\times, i+s \leq k+t-1,$ $0 \leq t < s < i \leq k-2)$	$2^{md_j(2k-(i+s))}$

where $|C_j|$ *is the number of elements in* C_j*, and*

$$\diamond\ \Omega_1(2^{md_j}, k) = \begin{cases} \frac{2^{md_j(\frac{k}{2}+1)} + 2^{md_j \cdot \frac{k}{2}} - 2}{2^{md_j} - 1} - (k+1), & \text{if } k \text{ is even;} \\ \frac{2(2^{md_j \cdot \frac{k+1}{2}} - 1)}{2^{md_j} - 1} - (k+1), & \text{if } k \text{ is odd.} \end{cases}$$

$$\diamond\ \Omega_2(2^{md_j}, k) = \begin{cases} (2^{md_j} - 1)\sum_{i=\frac{k}{2}+1}^{k-1}(2i-k)2^{md_j(k-i-1)}, & \text{if } k \text{ is even;} \\ (2^{md_j} - 1)\sum_{i=\frac{k+1}{2}}^{k-1}(2i-k)2^{md_j(k-i-1)}, & \text{if } k \text{ is odd.} \end{cases}$$

◇ *$\Gamma(2^{md_j},k)$ can be calculated by the following recurrence formula:*

$\Gamma(2^{md_j},\rho)=0$ *for* $\rho=1,2,3$; $\Gamma(2^{md_j},\rho)=1$ *for* $\rho=4$;

$\Gamma(2^{md_j},\rho)=\Gamma(2^{md_j},\rho-1)+\sum_{s=1}^{\lfloor\frac{\rho}{2}\rfloor-1}(\rho-2s-1)2^{md_j(s-1)}$ *for* $\rho\geq 5$.

Therefore, the number of all distinct ideals of the ring $\mathcal{K}_j[u]/\langle u^k\rangle$ is equal to

$$N_{(2^m,d_j,k)}=1+\frac{k(k+3)}{2}+\Omega_1(2^{md_j},k)+\Omega_2(2^{md_j},k)+(2^{md_j}-1)\Gamma(2^{md_j},k).$$

As the end of this section, we give an explicit formula to count the number of all cyclic codes over R of length $2n$.

Theorem 2.4 *Using the notation above, let $1\leq j\leq r$.*

(i) *The number of all distinct ideals of the ring $\mathcal{K}_j[u]/\langle u^k\rangle$ is*

$$N_{(2^m,d_j,k)}=\begin{cases}\sum_{i=0}^{\frac{k}{2}}(1+4i)2^{(\frac{k}{2}-i)md_j}, & \text{if } k \text{ is even;}\\ \sum_{i=0}^{\frac{k-1}{2}}(3+4i)2^{(\frac{k-1}{2}-i)md_j}, & \text{if } k \text{ is odd.}\end{cases}\tag{2}$$

Precisely, we have

$N_{(2^m,d_j,k)}=\frac{(2^{md_j}+3)2^{(\frac{k}{2}+1)md_j}-2^{md_j}(2k+5)+2k+1}{(2^{md_j}-1)^2}$, *when k is even;*

$N_{(2^m,d_j,k)}=\frac{(3\cdot 2^{md_j}+1)2^{(\frac{k-1}{2}+1)md_j}-2^{md_j}(2k+5)+2k+1}{(2^{md_j}-1)^2}$, *when k is odd.*

(ii) *The number of cyclic codes over $\mathbb{F}_{2^m}[u]/\langle u^k\rangle$ of length $2n$ is equal to*

$\prod_{j=1}^{r}\frac{(2^{md_j}+3)2^{(\frac{k}{2}+1)md_j}-2^{md_j}(2k+5)+2k+1}{(2^{md_j}-1)^2}$, *when k is even;*

$\prod_{j=1}^{r}\frac{(3\cdot 2^{md_j}+1)2^{(\frac{k-1}{2}+1)md_j}-2^{md_j}(2k+5)+2k+1}{(2^{md_j}-1)^2}$, *when k is odd.*

Proof (i) By the mathematical induction on k, one can easily verify that the equation (2) holds.

Now, let $k=2s+1$ where s is a positive integer, and denote $q=2^{md_j}$. Then we have $N_{(2^m,d_j,k)}=\sum_{i=0}^{s}(3+4i)q^{s-i}=3\sum_{i=0}^{s}q^{s-i}+4q^s\sum_{i=0}^{s}iq^{-i}$ in which $\sum_{i=0}^{s}q^{s-i}=\frac{q^{s+1}-1}{q-1}$. Then by

$$\sum_{i=1}^{s}ix^{i-1}=\frac{d}{dx}\left(\sum_{i=0}^{s}x^i\right)=\frac{d}{dx}\left(\frac{x^{s+1}-1}{x-1}\right)=\frac{(s+1)x^s(x-1)-(x^{s+1}-1)}{(x-1)^2},$$

we have

$$q^s\sum_{i=0}^{s} iq^{-i} = q^{s-1}\sum_{i=1}^{s} i(q^{-1})^{i-1} = q^{s-1}\cdot\frac{(s+1)q^{-s}(q^{-1}-1)-(q^{-(s+1)}-1)}{(q^{-1}-1)^2}$$
$$= q^{s-1}\cdot\frac{q^{-s+1}}{(q-1)^2}\left(q^{s+1}-q(s+1)+s\right).$$

From these, we deduce $N_{(2^m,d_j,k)} = 3\cdot\frac{q^{s+1}-1}{q-1} + 4\cdot\frac{1}{(q-1)^2}\left(q^{s+1}-q(s+1)+s\right)$, and hence $N_{(2^m,d_j,k)} = \frac{(3q+1)q^{s+1}-q(4s+7)+4s+3}{(q-1)^2}$ where $s=\frac{k-1}{2}$.

When k is even, the conclusion can be proved similarly. We omit this here.

(ii) It follows from (i) and Lemma 2.1. □

For the special cases of $k = 2, 3, 4, 5$, we have the following conclusions.

Corollary 2.5 *Let $2 \le k \le 5$. The number of all ideals in $\mathcal{K}_j[u]/\langle u^k\rangle$ is*

$$N_{(2^m,d_j,k)} = \begin{cases} 5+2^{d_jm}, & \text{when } k=2;\\ 9+5\cdot 2^{d_jm}+2^{2d_jm}, & \text{when } k=4;\\ 7+3\cdot 2^{d_jm}, & \text{when } k=3;\\ 11+7\cdot 2^{d_jm}+3\cdot 2^{2d_jm}, & \text{when } k=5. \end{cases}$$

Finally, let $n=1$ and $m=1$. Then $r=1$ and $d_1=1$ in this case. We denote by L_k the number of ideals in the ring $\frac{(\mathbb{F}_2+u\mathbb{F}_2+\cdots+u^{k-1}\mathbb{F}_2)[x]}{\langle x^2-1\rangle}$, where $k\ge 2$. By Theorem 2.4, we have that

$$L_k = N_{(2,1,k)} = \begin{cases} 10\cdot 2^{\frac{k}{2}}-2k-9 & \text{if } 2\mid k;\\ 14\cdot 2^{\frac{k-1}{2}}-2k-9 & \text{if } 2\nmid k. \end{cases}$$

For examples, we have $L_2=7$, $L_4=23$, $L_6=59$, $L_8=135$; $L_3=13$, $L_5=37$, $L_7=89$ and $L_9=197$.

3 An explicit representation and enumeration for self-dual cyclic codes over *R* of length 2*n*

In this section, we give an explicit representation for self-dual cyclic codes over R of length $2n$ and a precise mass formula to count the number of these codes.

For any polynomial $f(x)=\sum_{l=0}^{d} a_lx^l \in \mathbb{F}_{2^m}[x]$ of degree $d\ge 1$, recall that the *reciprocal polynomial* of $f(x)$ is defined as $\widetilde{f}(x) = x^d f(\frac{1}{x}) = \sum_{l=0}^{d} a_lx^{d-l}$, and $f(x)$ is said to be *self-reciprocal* if $\widetilde{f}(x)=\delta f(x)$ for some $\delta\in\mathbb{F}_{2^m}^{\times}$. Then by Eq. (1) in Sect. 2, it follows that

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

Since $f_1(x)=x+1$, $f_2(x),\ldots,f_r(x)$ are pairwise coprime monic irreducible polynomials in $\mathbb{F}_{2^m}[x]$, $\widetilde{f}_1(x)=x+1$, $\widetilde{f}_2(x),\ldots,\widetilde{f}_r(x)$ are pairwise coprime irreducible polynomials in $\mathbb{F}_{2^m}[x]$ as well. Hence for each integer j, $1 \le j \le r$, there is a unique integer j', $1 \le j' \le r$, such that

$$\widetilde{f}_j(x) = \delta_j f_{j'}(x) \text{ where } \delta_j \in \mathbb{F}_{2^m}^{\times}.$$

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

- $\lambda + 2\epsilon = r$ where $\lambda \ge 1$ and $\epsilon \ge 0$;
- $\widetilde{f}_j(x) = \delta_j f_j(x)$, where $\delta_j \in \mathbb{F}_{2^m}^{\times}$, for all $j = 1, \ldots, \lambda$;
- $\widetilde{f}_j(x) = \delta_j f_{j+\epsilon}(x)$, where $\delta_j \in \mathbb{F}_{2^m}^{\times}$, for all $j = \lambda + 1, \ldots, \lambda + \epsilon$.

Let $1 \le j \le r$. Since $f_j(x)^2$ is a divisor of $x^{2n} - 1$, we have $x^{2n} \equiv 1 \pmod{f_j(x)^2}$, i.e. $x^{2n} = 1$ in the ring $\mathcal{K}_j = \frac{\mathbb{F}_{2^m}[x]}{\langle f_j(x)^2 \rangle}$. This implies that

$$x^{-d} = x^{2n-d} \text{ in } \mathcal{K}_j[u]/\langle u^k \rangle,\ 1 \le d \le 2n - 1.$$

For any integer s, $1 \le s \le k$, and $\omega = \omega(x) \in \frac{\mathcal{F}_j[u]}{\langle u^s \rangle}$, by Lemma 2.2(ii) we know that $\omega(x)$ has a unique u-adic expansion:

$$\omega(x) = \sum_{i=0}^{s-1} u^i a_i(x),\ a_0(x), a_1(x), \ldots, a_{s-1}(x) \in \mathcal{F}_j.$$

To simplify the expressions, we adopt the following notation in this paper:

- $\widehat{\omega} = \omega(x^{-1}) = a_0(x^{-1}) + ua_1(x^{-1}) + \cdots + u^{s-1}a_{s-1}(x^{-1}) \pmod{f_j(x)}$, when $1 \le j \le \lambda$;
- $\widehat{\omega} = \omega(x^{-1}) = a_0(x^{-1}) + ua_1(x^{-1}) + \cdots + u^{s-1}a_{s-1}(x^{-1}) \pmod{f_{j+\epsilon}(x)}$, when $\lambda + 1 \le j \le \lambda + \epsilon$.
- $\Theta_{j,s} = \{\omega \in (\frac{\mathcal{F}_j[u]}{\langle u^s \rangle})^{\times} \mid \omega + \delta_j x^{2n-d_j}\widehat{\omega} \equiv 0 \pmod{f_j(x)}\}$, where $1 \le j \le \lambda$ and $1 \le s \le k - 1$.

For self-dual cyclic codes over R, using the notation above and by [7, Theorem 3.6], we have the following conclusion.

Theorem 3.1 *Using the notations above, all distinct self-dual cyclic codes over the ring R of length $2n$ are given by:*

$$\mathcal{C} = \left(\oplus_{j=1}^{\lambda} \varepsilon_j(x) C_j\right) \oplus \left(\oplus_{j=\lambda+1}^{\lambda+\epsilon} (\varepsilon_j(x) C_j \oplus \varepsilon_{j+\epsilon}(x) C_{j+\epsilon})\right),$$

where C_j is an ideal of $\mathcal{K}_j[u]/\langle u^k \rangle$ determined by the following conditions:

(i) *If $1 \le j \le \lambda$, C_j is determined by the following conditions:*

(†) When k is even, C_j is given by one of the following six cases:

(†-1) $C_j = \langle u^{\frac{k}{2}} \rangle$.
(†-2) $C_j = \langle f_j(x) \rangle$.
(†-3) $C_j = \langle u^{\frac{k}{2}} + u^t f_j(x)\omega \rangle$, *where* $\omega \in \Theta_{j,\frac{k}{2}-t}$ *and* $0 \le t \le \frac{k}{2} - 1$.

(†-4) $C_j = \langle u^i + f_j(x)\omega\rangle$, *where* $\omega \in \Theta_{j,k-i}$ *and* $\frac{k}{2}+1 \le i \le k-1$.
(†-5) $C_j = \langle u^i, u^{k-i} f_j(x)\rangle$, *where* $\frac{k}{2}+1 \le i \le k-1$.
(†-6) $C_j = \langle u^i + u^t f_j(x)\omega, u^{k-i} f_j(x)\rangle$, *where* $\omega \in \Theta_{j,k-i-t}$, $1 \le t < k-i$ *and* $\frac{k}{2}+1 \le i \le k-2$.

(‡) When k is odd, C_j *is given by one of the following four cases:*
(‡-1) $C_j = \langle f_j(x)\rangle$.
(‡-2) $C_j = \langle u^i + f_j(x)\omega\rangle$, *where* $\omega \in \Theta_{j,k-i}$ *and* $\frac{k+1}{2} \le i \le k-1$.
(‡-3) $C_j = \langle u^i, u^{k-i} f_j(x)\rangle$, *where* $\frac{k+1}{2} \le i \le k-1$.
(‡-4) $C_j = \langle u^i + u^t f_j(x)\omega, u^{k-i} f_j(x)\rangle$, *where* $\omega \in \Theta_{j,k-i-t}$, $1 \le t < k-i$ *and* $\frac{k+1}{2} \le i \le k-2$.

(ii) *If* $\lambda+1 \le j \le \lambda+\epsilon$, *then* $(C_j, C_{j+\epsilon})$ *is given by one of the* $N_{(2^m,d_j,k)}$ *pairs listed in the below table:*

C_j (mod $f_j(x)^2$)	$C_{j+\epsilon}$ (mod $f_{j+\epsilon}(x)^2$)
• $\langle u^i\rangle$ $(0 \le i \le k)$	◇ $\langle u^{k-i}\rangle$
• $\langle u^s f_j(x)\rangle$ $(0 \le s \le k-1)$	◇ $\langle u^{k-s}, f_{j+\epsilon}(x)\rangle$
• $\langle u^i + u^t f_j(x)\omega\rangle$ $(\omega \in (\frac{\mathcal{F}_j[u]}{\langle u^{i-t}\rangle})^\times$, $t \ge 2i-k, 0 \le t < i \le k-1)$	◇ $\langle u^{k-i} + u^{k+t-2i} f_{j+\epsilon}(x)\omega'\rangle$ $\omega' = \delta_j x^{2n-d_j}\widehat{\omega}$ (mod $f_{j+\epsilon}(x)$)
• $\langle u^i + f_j(x)\omega\rangle$ $(\omega \in (\frac{\mathcal{F}_j[u]}{\langle u^{k-i}\rangle})^\times$, $2i > k, 0 < i \le k-1)$	◇ $\langle u^i + f_{j+\epsilon}(x)\omega'\rangle$ $\omega' = \delta_j x^{2n-d_j}\widehat{\omega}$ (mod $f_{j+\epsilon}(x)$)
• $\langle u^i + u^t f_j(x)\omega\rangle$ $(\omega \in (\frac{\mathcal{F}_j[u]}{\langle u^{k-i}\rangle})^\times$, $t < 2i-k, 1 \le t < i \le k-1)$	◇ $\langle u^{i-t} + f_{j+\epsilon}(x)\omega', u^{k-i} f_{j+\epsilon}(x)\rangle$ $\omega' = \delta_j x^{2n-d_j}\widehat{\omega}$ (mod $f_{j+\epsilon}(x)$)
• $\langle u^i, u^s f_j(x)\rangle$ $(0 \le s < i \le k-1)$	◇ $\langle u^{k-s}, u^{k-i} f_{j+\epsilon}(x)\rangle$
• $\langle u^i + f_j(x)\omega, u^s f_j(x)\rangle$ $(\omega \in (\frac{\mathcal{F}_j[u]}{\langle u^s\rangle})^\times$, $i+s \le k-1, 1 \le s < i \le k-1)$	◇ $\langle u^{k-s} + u^{k-i-s} f_{j+\epsilon}(x)\omega'\rangle$ $\omega' = \delta_j x^{2n-d_j}\widehat{\omega}$ (mod $f_{j+\epsilon}(x)$)
• $\langle u^i + u^t f_j(x)\omega, u^s f_j(x)\rangle$ $(\omega \in (\frac{\mathcal{F}_j[u]}{\langle u^{s-t}\rangle})^\times$, $i+s \le k+t-1$, $1 \le t < s < i \le k-2)$	◇ $\langle u^{k-s} + u^{k+t-i-s} f_{j+\epsilon}(x)\omega'$, $u^{k-i} f_{j+\epsilon}(x)\rangle$ $\omega' = \delta_j x^{2n-d_j}\widehat{\omega}$ (mod $f_{j+\epsilon}(x)$)

To listed all self-dual cyclic codes over R of length $2n$, by Theorem 3.1 we need to determine the set $\Theta_{j,s}$ of elements $\omega \in (\mathcal{F}_j[u]/\langle u^s\rangle)^\times$ satisfying

$$\omega + \delta_j x^{2n-d_j}\widehat{\omega} \equiv 0 \ (\mathrm{mod}\ f_j(x)) \quad (3)$$

for some integer s, $1 \le s \le k-1$, and for all $j = 1, \ldots, \lambda$. To do this, we need the following lemma.

Lemma 3.2 *Using the notation above, let $1 \le j \le r$. We have the following:*

(i) $\delta_j = 1$ *for all* $j = 1, \ldots, \lambda$.
(ii) $d_1 = 1$, *and* $2 \mid d_j$ *for all* $j = 2, \ldots, \lambda$.

Proof (i) As $1 \le j \le \lambda$, we have $\widetilde{f_j}(x) = \delta_j f_j(x)$ where $\delta_j \in \mathbb{F}_{2^m}^{\times}$. Since $f_j(x)$ is a monic irreducible divisor of $x^n - 1$ in $\mathbb{F}_{2^m}[x]$, we have that $f_j(x) = \widetilde{\widetilde{f_j}}(x) = \delta_j \widetilde{f_j}(x) = \delta_j^2 f_j(x)$. This implies $\delta_j^2 = 1$, and hence $\delta_j = 1$ in $\mathbb{F}_{2^m}$.

(ii) Assume that $a \in \mathbb{F}_{2^m}^{\times}$ and $f(x) = x - a$ is a self-reciprocal polynomial. Then there exists $\delta \in \mathbb{F}_{2^m}^{\times}$ such that $\delta x - \delta a = \delta f(x) = \widetilde{f}(x) = 1 - ax$. This implies that $\delta = -a$ and $-\delta a = 1$. From this, we deduce that $a^2 = 1$, and hence $a = 1$. Therefore, $f_1(x) = x - 1$ is the only self-reciprocal and monic irreducible divisor of $x^n - 1$ in $\mathbb{F}_{2^m}[x]$ with degree 1.

Now, let $2 \le j \le r$. Then $f_j(x)$ is a self-reciprocal and monic irreducible divisor of $x^n - 1$ in $\mathbb{F}_{2^m}[x]$ with degree $\deg(f_j(x)) = d_j > 1$. This implies that d_j is even from finite field theory. □

Now, all distinct self-dual cyclic codes over R of length $2n$ can be listed explicitly by Theorem 3.1 and the following theorem.

Theorem 3.3 *Using the notation above, let $1 \le j \le r$ and $1 \le s \le k-1$. Then the set $\Theta_{j,s}$ is determined as follows:*

(i) *If $j = 1$, then*

$$\Theta_{1,s} = \left(\frac{\mathbb{F}_{2^m}[u]}{\langle u^s \rangle}\right)^{\times} = \left\{ \sum_{i=0}^{s-1} a_i u^i \mid a_0 \neq 0,\ a_i \in \mathbb{F}_{2^m}, i = 0, 1, \ldots, s-1 \right\}.$$

Hence $|\Theta_{1,s}| = (2^m - 1)2^{(s-1)m}$.

(ii) *Let $2 \le j \le r$, and let $\varrho_j(x)$ be a primitive element of the finite field $\mathcal{F}_j = \frac{\mathbb{F}_{2^m}[x]}{\langle f_j(x) \rangle}$. Then we have*

$$\Theta_{j,1} = \left\{ x^{-\frac{d_j}{2}} \varrho_j(x)^{l(2^{\frac{d_j}{2}m}+1)} \mid l = 0, 1, \ldots, 2^{\frac{d_j}{2}m} - 2 \right\} \subseteq \mathcal{F}_j;$$

and for any integer s, $2 \le s \le k-1$, we have

$$\Theta_{j,s} = \left\{ \sum_{i=0}^{s-1} a_i(x) u^i \mid a_0(x) \in \Theta_{j,1};\ a_i(x) \in \{0\} \cup \Theta_{j,1}, 1 \le i \le s-1 \right\}.$$

Therefore, $|\Theta_{j,s}| = (2^{\frac{d_j}{2}m} - 1)2^{(s-1)\frac{d_j}{2}m}$ for all $s = 1, 2, \ldots, k-1$.

Proof (i) Let $j=1$. By $f_1(x)=x-1$ and Lemma 2.2(ii), we have that $x\equiv 1$ (mod $f_1(x)$), $\mathcal{F}_1=\frac{\mathbb{F}_{2^m}[x]}{\langle x-1\rangle}=\mathbb{F}_{2^m}$ and

$$(\mathcal{F}_j[u]/\langle u^s\rangle)^{\times}=\left\{\sum_{i=0}^{s-1}a_iu^i \mid a_0\neq 0,\ a_i\in\mathbb{F}_{2^m}, i=0,1,\ldots,s-1\right\}.$$

In this case, by Lemma 3.2, Condition (3) is simplified to

$$\omega+\widehat{\omega}=\omega+\omega\equiv 0 \ (\mathrm{mod}\ x-1). \tag{4}$$

It is clear that every elements $\omega\in(\mathcal{F}_j[u]/\langle u^s\rangle)^{\times}$ satisfies the above condition. Hence $\Theta_{1,s}=(\mathcal{F}_j[u]/\langle u^s\rangle)^{\times}$ and $|\Theta_{1,s}|=(2^m-1)2^{(s-1)m}$.

(ii) Let $2\leq j\leq\lambda$. Then d_j is even and it is well known that

$$x^{-1}=x^{2^{m\frac{d_j}{2}}} \text{ in } \mathcal{F}_j. \tag{5}$$

Let $\omega=\omega(x)\in(\mathcal{F}_j[u]/\langle u^s\rangle)^{\times}$. By Lemma 2.2(ii), $\omega(x)$ has a unique u-adic expansion: $\omega(x)=\sum_{i=0}^{s-1}u^ia_i(x),\ a_0(x)\neq 0$, where $a_0(x),a_1(x),\ldots,a_{s-1}(x)\in\mathcal{F}_j=\frac{\mathbb{F}_{2^m}[x]}{\langle f_j(x)\rangle}$.

As $\gcd(x,f_j(x))=1$, Condition (3) for $\omega=\omega(x)\in(\mathcal{F}_j[u]/\langle u^s\rangle)^{\times}$ is transformed to $x^{\frac{d_j}{2}}\omega(x)+x^{-\frac{d_j}{2}}\omega(x^{-1})\equiv 0$ (mod $f_j(x)$) by Lemma 3.2(i). Let's write it down specifically: $\sum_{i=0}^{s-1}u^i\left(x^{\frac{d_j}{2}}a_i(x)\right)+\sum_{i=0}^{s-1}u^i\left(x^{-\frac{d_j}{2}}a_i(x^{-1})\right)\equiv 0$ (mod $f_j(x)$). This is equivalent to the following congruence relations

$$x^{\frac{d_j}{2}}a_i(x)+x^{-\frac{d_j}{2}}a_i(x^{-1})\equiv 0 \ (\mathrm{mod}\ f_j(x)),\ \ i=0,1,\ldots,s-1. \tag{6}$$

For each $0\leq i\leq s-1$, let $\xi_i(x)=x^{\frac{d_j}{2}}a_i(x)\in\mathcal{F}_j$. Then

$$a_i(x)=x^{-\frac{d_j}{2}}\xi_i(x)\in\mathcal{F}_j. \tag{7}$$

For any $b\in\mathbb{F}_{2^m}$, by $b^{2^m}=b$ we have $b^{2^{\frac{d_j}{2}m}}=b^{(2^m)^{\frac{d_j}{2}}}=b$ in $\mathbb{F}_{2^m}\subset\mathcal{F}_j$. Then by $x^{-1}=x^{2^{\frac{d_j}{2}m}}$ and $\xi_i(x)=x^{\frac{d_j}{2}}a_i(x)\in\mathcal{F}_j$, it follows that

$$x^{-\frac{d_j}{2}}a_i(x^{-1})=\xi_i(x^{-1})=\xi_i(x)^{2^{\frac{d_j}{2}m}}.$$

Therefore, Eq. (6) is equivalent to

$$\xi_i(x)\left(\xi_i(x)^{2^{\frac{d_j}{2}m}-1}-1\right)=\xi_i(x)+(\xi_i(x))^{2^{\frac{d_j}{2}m}}=0 \text{ in } \mathcal{F}_j,\ i=0,1,\ldots,s-1.$$

From the latter condition, we deduce that $\xi_i(x) = 0$ when $s \geq 2$ or $\xi_i(x) \in \mathcal{F}_j$ satisfying $\xi_i(x)^{2^{\frac{d_j}{2}m}-1} = 1$ for all s.

Since $\varrho_j(x)$ is a primitive element of $\mathcal{F}_j$, the multiplicative order of $\varrho_j(x)$ is $2^{d_j m} - 1 = (2^{\frac{d_j}{2}m} + 1)(2^{\frac{d_j}{2}m} - 1)$. This implies that $\varrho_j(x)^{2^{\frac{d_j}{2}m}+1}$ is a primitive $(2^{\frac{d_j}{2}m} - 1)$th root of unity. Hence $\xi_i(x)^{2^{\frac{d_j}{2}m}-1} = 1$ if and only if

$$\xi_i(x) = \left(\varrho_j(x)^{2^{\frac{d_j}{2}m}+1}\right)^l = \varrho_j(x)^{l(2^{\frac{d_j}{2}m}+1)},\ 0 \leq l \leq 2^{\frac{d_j}{2}m} - 2.$$

Therefore, the conclusion for $\Theta_{j,s}$ follows from Eq. (7) immediately. Moreover, we have $|\Theta_{j,s}| = |\Theta_{j,1}| \prod_{i=2}^{s}(|\Theta_{j,1}| + 1) = (2^{\frac{d_j}{2}m} - 1)2^{(s-1)\frac{d_j}{2}m}$ for all $s = 1, 2, \ldots, k-1$. □

Now is the time to give an explicit formula to count the number of all distinct self-dual cyclic codes over the ring R of length $2n$.

Corollary 3.4 *Let $\mathcal{N}_S(2^m, k, n)$ be the number of all distinct self-dual cyclic codes over the ring R of length $2n$. Then*

$$\mathcal{N}_S(2^m, k, n) = \left(\sum_{s=0}^{\frac{k}{2}} 2^{ms}\right)\left(\prod_{j=2}^{\lambda}\sum_{s=0}^{\frac{k}{2}} 2^{\frac{d_j}{2}ms}\right)\left(\prod_{j=\lambda+1}^{\lambda+\epsilon} N_{(2^m,d_j,k)}\right), \text{ when } 2 \mid k;$$

$$\mathcal{N}_S(2^m, k, n) = \left(\sum_{s=0}^{\frac{k-1}{2}} 2^{ms}\right)\left(\prod_{j=2}^{\lambda}\sum_{s=0}^{\frac{k-1}{2}} 2^{\frac{d_j}{2}ms}\right)\left(\prod_{j=\lambda+1}^{\lambda+\epsilon} N_{(2^m,d_j,k)}\right), \text{ when } 2 \nmid k.$$

Proof Let k be even and $1 \leq j \leq \lambda$. Then the number of ideals C_j listed in (†) of Theorem 3.1(i) is equal to

$$\begin{aligned} N_j &= 2 + \sum_{t=0}^{\frac{k}{2}-1} |\Theta_{j,\frac{k}{2}-t}| + \sum_{i=\frac{k}{2}+1}^{k-1} |\Theta_{j,k-i}| + k - 1 - \frac{k}{2} + \sum_{i=\frac{k}{2}+1}^{k-1}\sum_{t=1}^{k-1-i} |\Theta_{j,k-i-t}| \\ &= 1 + \frac{k}{2} + \frac{k}{2}|\Theta_{j,1}| + \left(\frac{k}{2} - 1\right)|\Theta_{j,2}| + \left(\frac{k}{2} - 2\right)|\Theta_{j,3}| + 2|\Theta_{j,\frac{k}{2}-1}| + |\Theta_{j,\frac{k}{2}}| \\ &= 1 + \frac{k}{2} + \sum_{s=1}^{\frac{k}{2}}\left(\frac{k}{2} - s + 1\right)|\Theta_{j,s}|. \end{aligned}$$

By Theorem 3.3 (i) and (ii) respectively, we know $|\Theta_{1,s}| = (2^m - 1)2^{(s-1)m}$ and $|\Theta_{j,s}| = (2^{\frac{d_j}{2}m} - 1)2^{(s-1)\frac{d_j}{2}m}$ when $2 \leq j \leq \lambda$. Now, we set $q_1 = 2^m$ and denote

$q_j = 2^{\frac{d_j}{2}m}$ when $2 \le j \le \lambda$, in the following. Then we have $|\Theta_{j,s}| = q_j^s - q_j^{s-1}$ for all integers j, $1 \le j \le \lambda$. From this, we obtain

$$\begin{aligned} N_j &= 1 + \frac{k}{2} + \frac{k}{2}(q_j - 1) + \left(\frac{k}{2} - 1\right)(q_j^2 - q_j) + \left(\frac{k}{2} - 2\right)(q_j^3 - q_j^2) \\ &\quad + \left(\frac{k}{2} - 3\right)(q_j^4 - q_j^3) + \cdots + 2\left(q_j^{\frac{k}{2}-1} - q_j^{\frac{k}{2}-2}\right) + \left(q_j^{\frac{k}{2}} - q_j^{\frac{k}{2}-1}\right) \\ &= \sum_{s=0}^{\frac{k}{2}} q_j^s. \end{aligned}$$

Therefore, $\mathcal{N}_S(2^m, k, n) = N_1(\prod_{j=2}^{\lambda} N_j)(\prod_{j=\lambda+1}^{\lambda+\epsilon} N_{(2^m,d_j,k)})$ by Theorem 3.1.

The conclusion for any odd integer k, $k \ge 3$, can by proved similarly. Here, we omit it. □

4 Self-dual 2-quasi-cyclic codes of length 4*n* over $\mathbb{F}_{2^m}$ derived from self-dual cyclic codes of length 2*n* over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$

In this section, We focus on self-dual cyclic codes of length $2n$ over $R = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ ($u^2 = 0$), where n is odd. By Lemma 2.3, Corollary 2.5, Theorem 3.1, Theorem 3.3 and Corollary 3.4, we obtain the following conclusion.

Corollary 4.1 *The number of self-dual cyclic codes of length* $2n$ *over the ring* $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ ($u^2 = 0$) *is* $(1+2^m) \cdot \prod_{j=2}^{\lambda}(1+2^{\frac{d_j}{2}m}) \cdot \prod_{j=\lambda+1}^{\lambda+\epsilon}(5+2^{d_j m})$. *Precisely, all these codes are given by*

$$\mathcal{C} = \left(\oplus_{j=1}^{\lambda} \varepsilon_j(x)C_j\right) \oplus \left(\oplus_{j=\lambda+1}^{\lambda+\epsilon}(\varepsilon_j(x)C_j \oplus \varepsilon_{j+\epsilon}(x)C_{j+\epsilon})\right),$$

where C_j *is an ideal of* $\mathcal{K}_j + u\mathcal{K}_j$ ($u^2 = 0$) *listed as follows:*

(i) C_1 *is one of the following* $1 + 2^m$ *ideals:*
$\langle u\rangle$, $\langle x - 1\rangle$, $\langle u + (x - 1)\omega\rangle$ *where* $\omega \in \mathbb{F}_{2^m}$ *and* $\omega \ne 0$.

(ii) *Let* $2 \le j \le \lambda$, *and* $\varrho_j(x)$ *is a primitive element of the finite field* $\mathcal{F}_j = \frac{\mathbb{F}_{2^m}[x]}{\langle f_j(x)\rangle}$.
Then C_j *is one of the following* $1 + 2^{\frac{d_j}{2}m}$ *ideals:*
$\langle u\rangle$, $\langle f_j(x)\rangle$;
$\langle u + f_j(x)\omega(x)\rangle$, *where* $\omega(x) \in \Theta_{j,1}$ *and*

$$\Theta_{j,1} = \left\{x^{-\frac{d_j}{2}}\varrho_j(x)^{l(2^{\frac{d_j}{2}m}+1)} \pmod{f_j(x)} \mid l = 0, 1, \ldots, 2^{\frac{d_j}{2}m} - 2\right\}.$$

(iii) *Let* $\lambda + 1 \le j \le \lambda + \epsilon$. *Then the pair* $(C_j, C_{j+\epsilon})$ *of ideals is one of the following* $5+2^{d_j m}$ *cases in the following table: where* $\mathcal{L}$ *is the number of pairs* $(C_j, C_{j+\epsilon})$ *in the same row,*

$\mathcal{L}$	$C_j \pmod{f_j(x)^2}$	$\lvert C_j\rvert$	$C_{j+\epsilon} \pmod{f_{j+\epsilon}(x)^2}$
3	$\bullet\ \langle u^i\rangle\ \ (i=0,1,2)$	$4^{(2-i)d_jm}$	$\diamond\ \langle u^{2-i}\rangle$
2	$\bullet\ \langle u^s f_j(x)\rangle\ (s=0,1)$	$2^{(2-s)d_jm}$	$\diamond\ \langle u^{2-s}, f_{j+\epsilon}(x)\rangle$
$2^{d_jm}-1$	$\bullet\ \langle u+f_j(x)\omega\rangle$	4^{d_jm}	$\diamond\ \langle u+f_{j+\epsilon}(x)\omega'\rangle$
1	$\bullet\ \langle u, f_j(x)\rangle$	2^{3d_jm}	$\diamond\ \langle uf_{j+\epsilon}(x)\rangle$

$\omega=\omega(x)\in\mathcal{F}_j=\{\sum_{i=0}^{d_j-1}a_ix^i\mid a_0,a_1,\ldots,a_{d_j-1}\in\mathbb{F}_{2^m}\}$ *and* $\omega\neq 0$,
$\omega'=\delta_jx^{-d_j}\omega(x^{-1}) \pmod{f_{j+\epsilon}(x)}$.

Remark For the cases of $k=3,4,5$, we list all distinct self-dual cyclic codes of length $2n$ over the ring $\frac{\mathbb{F}_{2^m}[u]}{\langle u^k\rangle}$ in Appendix of this paper.

Now, let's consider how to calculate the number of self-dual cyclic codes of length $2n$ over the ring $R=\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ directly from the odd positive integer n. Let $J_1, J_2, \ldots, J_r$ be all the distinct 2^m-cyclotomic cosets modulo n corresponding to the factorization $x^n-1=f_1(x)f_2(x)\ldots f_r(x)$, where $f_1(x)=x-1$, $f_2(x),\ldots,f_r(x)$ are distinct monic irreducible polynomials in $\mathbb{F}_{2^m}[x]$. Then we have $r=\lambda+2\epsilon$ and

- $J_1=\{0\}$, the set J_j satisfies $J_j=-J_j \pmod{n}$ and $|J_j|=d_j$ for all $j=2,\ldots,\lambda$;
- $J_{\lambda+l+\epsilon}=-J_{\lambda+l} \pmod{n}$ and $|J_{\lambda+l}|=|J_{\lambda+l+\epsilon}|=d_{\lambda+l}$, for all $l=1,\ldots,\epsilon$.

From this and by Corollary 4.1, we deduce that the number of self-dual cyclic codes over R of length $2n$ is

$$(1+2^m)\cdot\prod_{j=2}^{\lambda}(1+2^{\frac{|J_j|}{2}m})\cdot\prod_{j=\lambda+1}^{\lambda+\epsilon}(5+2^{|J_j|m}).$$

As an example, we list the number $\mathcal{N}$ of self-dual cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$ of length $2n$, where n is odd and $6\leq 2n\leq 98$, in the following table: where

$2n$	$\mathcal{N}$	$2n$	$\mathcal{N}$
6	$9=3(1+2)$	54	$41553=3(1+2)(1+2^3)(1+2^9)$
10	$15=3(1+2^2)$	58	$49155=3(1+2^{14})$
14	$39=3(5+2^3)$	62	$151959=3(5+2^5)^3$
18	$81=3(1+2)(1+2^3)$	66	$323433=3(1+2)(1+2^5)^3$
22	$99=3(1+2^5)$	70	$799695=3(1+2^2)(5+2^3)(5+2^{12})$
26	$195=3(1+2^6)$	74	$786435=3(1+2^{18})$
30	$945=3(1+2)(1+2^2)(5+2^4)$	78	$2399085=3(1+2)(1+2^6)(5+2^{12})$
34	$867=3(1+2^4)^2$	82	$3151875=3(1+2^{10})^2$
38	$1539=3(1+2^9)$	86	$6440067=3(1+2^7)^3$
42	$8073=3(1+2)(5+2^3)(5+2^6)$	90	34879005
46	$6159=3(5+2^{11})$	94	$25165839=3(5+2^{23})$
50	$15375=3(1+2^2)(1+2^{10})$	98	$81789123=3(5+2^3)(5+2^{21})$

$34879005=3(1+2)(1+2^2)(1+2^3)(5+2^4)(5+2^{12})$.

Then we consider how to construct self-dual 2-quasi-cyclic codes of length $4n$ over $\mathbb{F}_{2^m}$ from self-dual cyclic codes of length $2n$ over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$.

Let $\alpha = a + bu \in R$ where $a, b \in \mathbb{F}_{2^m}$. As in [4], we define $\phi(\alpha) = (b, a + b)$ and define the *Lee weight* of α by $\mathrm{w}_L(\alpha) = \mathrm{w}_H(b, a + b)$, where $\mathrm{w}_H(b, a + b)$ is the Hamming weight of the vector $(b, a + b) \in \mathbb{F}_{2^m}^2$. Then ϕ is an isomorphism of $\mathbb{F}_{2^m}$-linear spaces from R onto $\mathbb{F}_{2^m}^2$, and can be extended to an isomorphism of $\mathbb{F}_{2^m}$-linear spaces from $\frac{R[x]}{\langle x^{2n}-1\rangle}$ onto $\mathbb{F}_{2^m}^{4n}$ by the rule:

$$\phi(\xi) = (b_0, b_1, \ldots, b_{2n-1}, a_0 + b_0, a_1 + b_1, \ldots, a_{2n-1} + b_{2n-1}), \tag{8}$$

for all $\xi = \sum_{i=0}^{2n-1} \alpha_i x^i \in \frac{R[x]}{\langle x^{2n}-1\rangle}$, where $\alpha_i = a_i + b_i u$ with $a_i, b_i \in \mathbb{F}_{2^m}$ and $i = 0, 1, \ldots, 2n - 1$.

The following conclusion can be derived from [4, Corollary 14].

Lemma 4.2 *Using the notation above, let $\mathcal{C}$ be an ideal of the ring $\frac{R[x]}{\langle x^{2n}-1\rangle}$ and set $\phi(\mathcal{C}) = \{\phi(\xi) \mid \xi \in \mathcal{C}\} \subseteq \mathbb{F}_{2^m}^{4n}$. Then*

(i) *$\phi(\mathcal{C})$ is a 2-quasi-cyclic code over $\mathbb{F}_{2^m}$ of length $4n$, i.e.,*

$$(b_{2n-1}, b_0, b_1, \ldots, b_{2n-2}, c_{2n-1}, c_0, c_1, \ldots, c_{2n-2}) \in \phi(\mathcal{C})$$

for all $(b_0, b_1, \ldots, b_{2n-2}, b_{2n-1}, c_0, c_1, \ldots, c_{2n-2}, c_{2n-1}) \in \phi(\mathcal{C})$.

(ii) *The Hamming weight distribution of $\phi(\mathcal{C})$ is exactly the same as the Lee weight distribution of $\mathcal{C}$.*

(iii) *$\phi(\mathcal{C})$ is a self-dual code over $\mathbb{F}_{2^m}$ of length $4n$ if $\mathcal{C}$ is a self-dual code over R of length $2n$.*

By Corollary 4.1, we can get a class of self-dual 2-quasi-cyclic codes over $\mathbb{F}_{2^m}$ of length $4n$ from the class of self-dual cyclic code over R of length $2n$ and the Gray map ϕ defined by Eq. (8). In the following, we consider how to give an efficient encoder for each self-dual 2-quasi-cyclic code $\phi(\mathcal{C})$ of length $4n$ over $\mathbb{F}_{2^m}$ derived from a self-dual cyclic code $\mathcal{C}$ of length $2n$ over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$. We denote by A^{tr} the transpose of a matrix A in this paper.

To simplify the symbol, in the following we identify each polynomial $a(x) = a_0 + a_1 x + \cdots + a_{2n-1} x^{2n-1} \in \frac{\mathbb{F}_{2^m}[x]}{\langle x^{2n}-1\rangle}$ with the vector $(a_0, a_1, \ldots, a_{2n-1}) \in \mathbb{F}_{2^m}^{2n}$. Moreover, for any integer $1 \leq s \leq n - 1$ we denote:

$$[a(x)]_s = \begin{pmatrix} a(x) \\ xa(x) \\ \cdots \\ x^{s-1}a(x) \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & \ldots & a_{2n-2} & a_{2n-1} \\ a_{2n-1} & a_0 & \ldots & a_{2n-3} & a_{2n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{2n-s+1} & a_{2n-s+2} & \ldots & a_{2n-s-1} & a_{2n-s} \end{pmatrix} \tag{9}$$

which is a matrix over $\mathbb{F}_{2^m}$ of size $s \times 2n$.

Theorem 4.3 *Using the notation above, every self-dual 2-quasi-cyclic code $\phi(\mathcal{C})$ of length $4n$ over $\mathbb{F}_{2^m}$ derived from a self-dual cyclic code $\mathcal{C}$ of length $2n$ over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$*

has an $\mathbb{F}_{2^m}$*-generator matrix given by:* $G = \begin{pmatrix} G_1 \\ G_2 \\ \ldots \\ G_{\lambda+\epsilon} \end{pmatrix}$ *in which for each integer* j, $1 \leq j \leq r$, G_j *is a matrix over* $\mathbb{F}_{2^m}$ *listed in the following:*

(i) G_1 *is one of the following* $1 + 2^m$ *matrices with size* $2 \times 4n$*:*
$\begin{pmatrix} \varepsilon_1(x) & \varepsilon_1(x) \\ (x-1)\varepsilon_1(x) & (x-1)\varepsilon_1(x) \end{pmatrix}$, $\begin{pmatrix} 0 & (x-1)\varepsilon_1(x) \\ (x-1)\varepsilon_1(x) & (x-1)\varepsilon_1(x) \end{pmatrix}$,
$\begin{pmatrix} \varepsilon_1(x) & \varepsilon_1(x) + (x-1)\varepsilon_1(x)\omega \\ (x-1)\varepsilon_1(x) & (x-1)\varepsilon_1(x) \end{pmatrix}$ *where* $\omega \in \mathbb{F}_{2^m}$ *and* $\omega \neq 0$.

(ii) *Let* $2 \leq j \leq \lambda$. *Then* G_j *is one of the following* $1 + 2^{\frac{d_j}{2}m}$ *matrices with size* $2d_j \times 4n$*:*
$\begin{pmatrix} [\varepsilon_j(x)]_{d_j} & [\varepsilon_j(x)]_{d_j} \\ [f_j(x)\varepsilon_j(x)]_{d_j} & [f_j(x)\varepsilon_j(x)]_{d_j} \end{pmatrix}$, $\begin{pmatrix} 0 & [f_j(x)\varepsilon_j(x)]_{d_j} \\ [f_j(x)\varepsilon_j(x)]_{d_j} & [f_j(x)\varepsilon_j(x)]_{d_j} \end{pmatrix}$,
$\begin{pmatrix} [\varepsilon_j(x)]_{d_j} & [(1 + f_j(x)\omega(x))\varepsilon_j(x)]_{d_j} \\ [f_j(x)\varepsilon_j(x)]_{d_j} & [f_j(x)\varepsilon_j(x)]_{d_j} \end{pmatrix}$ *where*

$$\omega(x) = x^{-\frac{d_j}{2}} \varrho_j(x)^{l(2^{\frac{d_j}{2}m}+1)} \pmod{f_j(x)},\ l = 0, 1, \ldots, 2^{\frac{d_j}{2}m} - 2.$$

(iii) *Let* $\lambda + 1 \leq j \leq \lambda + \epsilon$. *Then* G_j *is one of the following* $5 + 2^{d_j m}$ *matrices with size* $4d_j \times 4n$*:*

$$\begin{pmatrix} 0 & [\varepsilon_j(x)]_{d_j} \\ 0 & [f_j(x)\varepsilon_j(x)]_{d_j} \\ [\varepsilon_j(x)]_{d_j} & [\varepsilon_j(x)]_{d_j} \\ [f_j(x)\varepsilon_j(x)]_{d_j} & [f_j(x)\varepsilon_j(x)]_{d_j} \end{pmatrix},$$

$$\left(\begin{array}{cc} [\varepsilon_j(x)]_{d_j} & [\varepsilon_j(x)]_{d_j} \\ [f_j(x)\varepsilon_j(x)]_{d_j} & [f_j(x)\varepsilon_j(x)]_{d_j} \\ \hline [\varepsilon_{j+\epsilon}(x)]_{d_j} & [\varepsilon_{j+\epsilon}(x)]_{d_j} \\ [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} & [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} \end{array}\right);$$

$$\begin{pmatrix} 0 & [\varepsilon_{j+\epsilon}(x)]_{d_j} \\ 0 & [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} \\ [\varepsilon_{j+\epsilon}(x)]_{d_j} & [\varepsilon_{j+\epsilon}(x)]_{d_j} \\ [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} & [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} \end{pmatrix};$$

$$\left(\begin{array}{cc} 0 & [f_j(x)\varepsilon_j(x)]_{d_j} \\ [f_j(x)\varepsilon_j(x)]_{d_j} & [f_j(x)\varepsilon_j(x)]_{d_j} \\ \hline 0 & [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} \\ [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} & [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} \end{array}\right),$$

$$\left(\begin{array}{cc} [f_j(x)\varepsilon_j(x)]_{d_j} & [f_j(x)\varepsilon_j(x)]_{d_j} \\ \hline [\varepsilon_{j+\epsilon}(x)]_{d_j} & [\varepsilon_{j+\epsilon}(x)]_{d_j} \\ [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} & [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} \\ 0 & [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} \end{array}\right);$$

$$\left(\begin{array}{cc} [\varepsilon_j(x)]_{d_j} & [\varepsilon_j(x)]_{d_j} \\ [f_j(x)\varepsilon_j(x)]_{d_j} & [f_j(x)\varepsilon_j(x)]_{d_j} \\ 0 & [f_j(x)\varepsilon_j(x)]_{d_j} \\ \hline [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} & [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} \end{array}\right);$$

$$\left(\begin{array}{cc} [\varepsilon_j(x)]_{d_j} & [(1+f_j(x)\omega(x))\varepsilon_j(x)]_{d_j} \\ [f_j(x)\varepsilon_j(x)]_{d_j} & [f_j(x)\varepsilon_j(x)]_{d_j} \\ \hline [\varepsilon_{j+\epsilon}(x)]_{d_j} & [(1+f_{j+\epsilon}(x)\omega'(x))\varepsilon_{j+\epsilon}(x)]_{d_j} \\ [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} & [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} \end{array}\right)$$

where $\omega'(x) = \delta_j x^{-d_j} w(x^{-1}) \pmod{f_{j+\epsilon}(x))}$, $\omega(x) \in \mathcal{F}_j$ *and* $\omega(x) \neq 0$.

Proof Let $\mathcal{C}$ be a self-dual cyclic code over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ of length $2n$. By Corollary 4.1, $\mathcal{C}$ has a unique direct decomposition:

$$\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2 \oplus \ldots \oplus \mathcal{C}_{\lambda+\epsilon}, \tag{10}$$

where $\mathcal{C}_j = \varepsilon_j(x)C_j = \{\varepsilon_j(x)\xi \mid \xi \in C_j\} \pmod{x^{2n}-1}$ for all $j = 1, \ldots, \lambda$, $\mathcal{C}_j = \varepsilon_j(x)C_j \oplus \varepsilon_{j+\epsilon}(x)C_{j+\epsilon} \pmod{x^{2n}-1}$ for all $j = \lambda+1, \ldots, \lambda+\epsilon$, and

- C_1 is given by Corollary 4.1(i);
- C_j is given by Corollary 4.1(ii) for all $j = 2, \ldots \lambda$;
- $(C_j, C_{j+\epsilon})$ is given by Corollary 4.1(iii) for all $j = \lambda+1, \ldots, \lambda+\epsilon$.

Now, let $\alpha(x)$ be an arbitrary element in the ring $\mathcal{K}_j + u\mathcal{K}_j$ $(u^2 = 0)$ where $\mathcal{K}_j = \frac{\mathbb{F}_{2^m}[x]}{\langle f_j(x)^2\rangle}$. Then there is a unique tuple $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ of elements in $\mathcal{F}_j = \frac{\mathbb{F}_{2^m}[x]}{\langle f_j(x)\rangle} \subset \mathcal{K}_j$ such that

$$\alpha = \left(\alpha_0 + \alpha_1 f_j(x)\right) + u\left(\alpha_2 + \alpha_3 f_j(x)\right). \tag{11}$$

Since $\{1, x, \ldots, x^{d_j-1}\}$ is an $\mathbb{F}_{2^m}$-basis of $\mathcal{F}_j$, for each integer $0 \le t \le 3$ there is a unique row matrix $\underline{a}_t = (a_{t,0}, a_{t,1}, \ldots, a_{t,d_j-1}) \in \mathbb{F}_{2^m}^{d_j}$ such that

$$\alpha_t = a_{t,0} + a_{t,1}x + \cdots + a_{t,d_j-1}x^{d_j-1} = \underline{a}_t X_{d_j}, \tag{12}$$

where $X_{d_j} = (1, x, \ldots, x^{d_j-1})^{\mathrm{tr}}$.

Let $D_j = D_{j;(g(x),h(x))} = \langle g(x)+uh(x)\rangle$ be an ideal of the ring $\mathcal{K}_j + u\mathcal{K}_j$ generated by $g(x)+uh(x)$, where $g(x), h(x) \in \mathcal{K}_j = \frac{\mathbb{F}_{2^m}[x]}{\langle f_j(x)^2\rangle}$, and denote $\mathcal{D}_j = \varepsilon_j(x)D_j$. Then $\mathcal{D}_j$ is an $\mathbb{F}_{2^m}$-subspace of $\mathcal{A} + u\mathcal{A}$, where $\mathcal{A} = \frac{\mathbb{F}_{2^m}[x]}{\langle x^{2n}-1\rangle}$, and the $\mathbb{F}_{2^m}$-dimension of $\mathcal{D}_j$ is $\log_{2^m}|D_j|$. Hence $\dim_{\mathbb{F}_{2^m}}(\mathcal{D}_j) = l$ if $|D_j| = 2^{ml}$. Now, we claim that a generator matrix of the $\mathbb{F}_{2^m}$-subspace $\phi(\mathcal{D}_j)$ is the following:

$$G_{j;(g(x),h(x))} = \left(\begin{array}{cc} [h(x)\varepsilon_j(x)]_{d_j} & [(g(x)+h(x))\varepsilon_j(x)]_{d_j} \\ [f_j(x)h(x)\varepsilon_j(x)]_{d_j} & [f_j(x)(g(x)+h(x))\varepsilon_j(x)]_{d_j} \\ [g(x)\varepsilon_j(x)]_{d_j} & [g(x)\varepsilon_j(x)]_{d_j} \\ [f_j(x)g(x)\varepsilon_j(x)]_{d_j} & [f_j(x)g(x)\varepsilon_j(x)]_{d_j} \end{array}\right). \tag{13}$$

In fact, by Eq. (11), each element ξ of D_j is of the form:

$$\begin{aligned}\xi &= \alpha(g(x)+uh(x))\\ &= (\alpha_0+\alpha_1 f_j(x))g(x)+u\left((\alpha_0+\alpha_1 f_j(x))h(x)+(\alpha_2+\alpha_3 f_j(x))g(x)\right).\end{aligned}$$

Then by Eq. (8) in Sect. 4 and Eq. (12), we have

$$\begin{aligned}\phi(\varepsilon_j(x)\xi) &= \big((\alpha_0+\alpha_1 f_j(x))h(x)\varepsilon_j(x)+(\alpha_2+\alpha_3 f_j(x))g(x)\varepsilon_j(x),\\ &\qquad (\alpha_0+\alpha_1 f_j(x))(g(x)+h(x))\varepsilon_j(x)+(\alpha_2+\alpha_3 f_j(x))g(x)\varepsilon_j(x)\big)\\ &= (\alpha_0,\alpha_1,\alpha_2,\alpha_3)\begin{pmatrix} h(x)\varepsilon_j(x) & (g(x)+h(x))\varepsilon_j(x)\\ f_j(x)h(x)\varepsilon_j(x) & f_j(x)(g(x)+h(x))\varepsilon_j(x)\\ g(x)\varepsilon_j(x) & g(x)\varepsilon_j(x)\\ f_j(x)g(x)\varepsilon_j(x) & f_j(x)g(x)\varepsilon_j(x)\end{pmatrix}\\ &= (\underline{a}_0,\underline{a}_1,\underline{a}_2,\underline{a}_3)G_{j;(g(x),h(x))}.\end{aligned}$$

From this, we deduce that the $\mathbb{F}_{2^m}$-subspace $\phi(\mathcal{D}_j)$ is generated by the row vectors of $G_{j;(g(x),h(x))}$. Hence $G_{j;(g(x),h(x))}$ is a generator matrix over $\mathbb{F}_{2^m}$.

$\diamond$ Let consider Case (ii) first. Let $2\leq j\leq\lambda$ and C_j be an ideal of $\mathcal{K}_j+u\mathcal{K}_j$ given by Corollary 4.1(ii). Then we have one of the following three cases:

(ii-1) $C_j=\langle u\rangle=D_{j;(0,1)}$. In this case, we have $g(x)=0$ and $h(x)=1$. Then by Eq. (13), $G_{j;(0,1)}$ is a generator matrix of $\phi(\mathcal{C}_j)$ over $\mathbb{F}_{2^m}$. By deleting the bottom zero row vectors of $G_{j;(0,1)}$, a generator matrix of $\phi(\mathcal{C}_j)$ over $\mathbb{F}_{2^m}$ is given by $G_j=\begin{pmatrix}[\varepsilon_j(x)]_{d_j} & [\varepsilon_j(x)]_{d_j}\\ [f_j(x)\varepsilon_j(x)]_{d_j} & [f_j(x)\varepsilon_j(x)]_{d_j}\end{pmatrix}$. Then by $|C_j|=2^{md_j}$, we have $\dim_{\mathbb{F}_{2^m}}(\phi(\mathcal{C}_j))=2d_j$.

(ii-2) $C_j=\langle f_j(x)\rangle=D_{j;(f_j(x),0)}$. In this case, we have $g(x)=f_j(x)$ and $h(x)=0$. Then by Eq. (13), $G_{j;(f_j(x),0)}$ is a generator matrix of $\phi(\mathcal{C}_j)$ over $\mathbb{F}_{2^m}$. As $f_j(x)^2=0$ in $\mathcal{K}_j$, both the second row and the 4th row of the block matrix $G_{j;(f_j(x),0)}$ are zero vector. By deleting the two zero row vectors of $G_{j;(f_j(x),0)}$, a generator matrix of $\phi(\mathcal{C}_j)$ over $\mathbb{F}_{2^m}$ is given by $G_j=\begin{pmatrix}0 & [f_j(x)\varepsilon_j(x)]_{d_j}\\ [f_j(x)\varepsilon_j(x)]_{d_j} & [f_j(x)\varepsilon_j(x)]_{d_j}\end{pmatrix}$. Then by $|C_j|=2^{md_j}$, we have $\dim_{\mathbb{F}_{2^m}}(\phi(\mathcal{C}_j))=2d_j$.

(ii-3) $C_j=\langle u+f_j(x)\omega(x)\rangle=D_{j;(f_j(x)\omega(x),1)}$. In this case, we have $g(x)=f_j(x)\omega(x)$ and $h(x)=1$. Then by Eq. (13), $G_{j;(f_j(x)\omega(x),1)}$ is a generator matrix of $\phi(\mathcal{C}_j)$ over $\mathbb{F}_{2^m}$. As $f_j(x)^2=0$ in $\mathcal{K}_j$, we have $f_j(x)g(x)=0$ and $f_j(x)(g(x)+h(x))=f_j(x)$. Hence

$$G_{j;(f_j(x)\omega(x),1)}=\begin{pmatrix}[\varepsilon_j(x)]_{d_j} & [(f_j(x)\omega(x)+1)\varepsilon_j(x)]_{d_j}\\ [f_j(x)\varepsilon_j(x)]_{d_j} & [f_j(x)\varepsilon_j(x)]_{d_j}\\ [f_j(x)\omega(x)\varepsilon_j(x)]_{d_j} & [f_j(x)\omega(x)\varepsilon_j(x)]_{d_j}\\ 0 & 0\end{pmatrix}.$$

Since $\omega(x)$ is a polynomial in $\mathbb{F}_{2^m}[x]$ of degree less than d_j-1 by $\omega(x)\in\mathcal{F}_j^{\times}$, we see that every row vector of the matrix $[f_j(x)\omega(x)\varepsilon_j(x)]_{d_j}$ is an $\mathbb{F}_{2^m}$-linear combination of the row vectors of $[f_j(x)\varepsilon_j(x)]_{d_j}$. Hence a generator matrix of $\phi(\mathcal{C}_j)$ over $\mathbb{F}_{2^m}$ is given by $G_j=\begin{pmatrix}[\varepsilon_j(x)]_{d_j} & [(1+f_j(x)\omega(x))\varepsilon_j(x)]_{d_j}\\ [f_j(x)\varepsilon_j(x)]_{d_j} & [f_j(x)\varepsilon_j(x)]_{d_j}\end{pmatrix}$.

◇ The conclusions in Case (i) can be proved similarly as that in Case (ii) above.

◇ We consider Case (iii). Let $\mathcal{C}_j=\varepsilon_j(x)C_j\oplus\varepsilon_{j+\epsilon}(x)C_{j+\epsilon}$, where $\lambda+1\leq j\leq\lambda+\epsilon$ and the pair $(C_j, C_{j+\epsilon})$ of ideals is given by the table in Corollary 4.1. Then we have $\phi(\mathcal{C}_j)=\phi(\varepsilon_j(x)C_j)\oplus\phi(\varepsilon_{j+\epsilon}(x)C_{j+\epsilon})$ and $\dim_{\mathbb{F}_{2^m}}(\phi(\mathcal{C}_j)=4d_j$. Therefore, a generator matrix of $\phi(\mathcal{C}_j)$ over $\mathbb{F}_{2^m}$ is given by $G_j=\left(\frac{A}{B}\right)$, where A and B are generator matrices of $\phi(\varepsilon_j(x)C_j)$ and $\phi(\varepsilon_{j+\epsilon}(x)C_{j+\epsilon})$ over $\mathbb{F}_{2^m}$ respectively. Using Eq. (13), matrices A and B can be determined similarly as that in Case (ii) above. Here are some cases:

▹ Let $C_j=\langle 1\rangle=D_{j;(1,0)}$ and $C_{j+\epsilon}=\{0\}$. Then $B=0$, and by Eq. (13) we have

$$A=\begin{pmatrix}0 & [\varepsilon_j(x)]_{d_j}\\ 0 & [f_j(x)\varepsilon_j(x)]_{d_j}\\ [\varepsilon_j(x)]_{d_j} & [\varepsilon_j(x)]_{d_j}\\ [f_j(x)\varepsilon_j(x)]_{d_j} & [f_j(x)\varepsilon_j(x)]_{d_j}\end{pmatrix}.$$

▹ Let $C_j=\langle u\rangle=D_{j;(0,1)}$ and $C_{j+\epsilon}=\langle u\rangle=D_{j+\epsilon;(0,1)}$. Then by the proof of (ii) and $d_{j+\epsilon}=d_j$, we deduce that $A=\begin{pmatrix}[\varepsilon_j(x)]_{d_j} & [\varepsilon_j(x)]_{d_j}\\ [f_j(x)\varepsilon_j(x)]_{d_j} & [f_j(x)\varepsilon_j(x)]_{d_j}\end{pmatrix}$ and $B=\begin{pmatrix}[\varepsilon_{j+\epsilon}(x)]_{d_j} & [\varepsilon_{j+\epsilon}(x)]_{d_j}\\ [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} & [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j}\end{pmatrix}$.

▹ Let $C_j=\langle uf_j(x)\rangle=D_{j;(0,f_j(x))}$ and $C_{j+\epsilon}=\langle u, f_{j+\epsilon}(x)\rangle=\langle u\rangle+\langle f_{j+\epsilon}(x)\rangle=D_{j+\epsilon;(0,1)}+D_{j+\epsilon;(f_{j+\epsilon}(x),0)}$. Then by the proof of (ii), we see that $B_1=\begin{pmatrix}[\varepsilon_{j+\epsilon}(x)]_{d_j} & [\varepsilon_{j+\epsilon}(x)]_{d_j}\\ [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} & [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j}\end{pmatrix}$ is a generator matrix of $\phi(\varepsilon_{j+\epsilon}(x)D_{j+\epsilon;(0,1)})$ and $B_2=\begin{pmatrix}0 & [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j}\\ [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} & [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j}\end{pmatrix}$ is a generator matrix of $\phi(\varepsilon_{j+\epsilon}(x)D_{j+\epsilon;(f_{j+\epsilon}(x),0)})$. Since the last row of the block matrices B_1 and B_2 are the same, a generator matrix of $\phi(\varepsilon_j(x)C_{j+\epsilon})$ is given by

$$B=\begin{pmatrix}[\varepsilon_{j+\epsilon}(x)]_{d_j} & [\varepsilon_{j+\epsilon}(x)]_{d_j}\\ [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j} & [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j}\\ 0 & [f_{j+\epsilon}(x)\varepsilon_{j+\epsilon}(x)]_{d_j}\end{pmatrix}.$$

From Eq. (13), we deduce that $A=\left([f_j(x)\varepsilon_j(x)]_{d_j}, [f_j(x)\varepsilon_j(x)]_{d_j}\right)$ is a a generator matrix of $\phi(\varepsilon_j(x)C_j)=\phi(\varepsilon_j(x)D_{j;(0,f_j(x))})$, since $u^2=0$ and $f_j(x)^2=0$.

▹ The other conclusion in Case (iii) can be proved similarly. Here, we omit these details. □

As the end of this section, we list all distinct self-dual cyclic codes $\mathcal{C}$ over $\mathbb{F}_2+u\mathbb{F}_2$ of length 30. We have $x^{15}-1=f_1(x)f_2(x)f_3(x)f_4(x)f_5(x)$, where

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

are irreducible polynomials in $\mathbb{F}_2[x]$ satisfying $\widetilde{f_j}(x)=f_j(x)$ for all $j=1,2,3$, and $\widetilde{f_4}(x)=f_5(x)$ with $\delta_4=1$. Hence $r=5$, $\lambda=3$, $\epsilon=1$, $d_1=1$, $d_2=2$ and $d_3=d_4=d_5=4$.

Using the notation in Sect. 2, we have

$$\begin{aligned}
\varepsilon_1(x) =& x^{28}+x^{26}+x^{24}+x^{22}+x^{20}+x^{18}+x^{16}+x^{14}+x^{12}+x^{10}+x^8+x^6\\
&+x^4+x^2+1,\\
\varepsilon_2(x) =& x^{28}+x^{26}+x^{22}+x^{20}+x^{16}+x^{14}+x^{10}+x^8+x^4+x^2,\\
\varepsilon_3(x) =& x^{28}+x^{26}+x^{24}+x^{22}+x^{18}+x^{16}+x^{14}+x^{12}+x^8+x^6+x^4+x^2,\\
\varepsilon_4(x) =& x^{24}+x^{18}+x^{16}+x^{12}+x^8+x^6+x^4+x^2,\\
\varepsilon_5(x) =& x^{28}+x^{26}+x^{24}+x^{22}+x^{18}+x^{14}+x^{12}+x^6.
\end{aligned}$$

Obviously, x is a primitive element of the finite field $\mathcal{F}_2=\frac{\mathbb{F}_2[x]}{\langle f_2(x)\rangle}$ and

$$\Theta_{2,1}=\{x^{-\frac{2}{2}}x^{l(2^{\frac{2}{2}}+1)}\mid l=2^{\frac{2}{2}}-2=0\}=\{x+1\}\ (\mathrm{mod}\ f_2(x));$$

$x+1$ is a primitive element of the finite field $\mathcal{F}_3=\frac{\mathbb{F}_2[x]}{\langle f_3(x)\rangle}$ and

$$\begin{aligned}
\Theta_{3,1}&=\{x^{-\frac{4}{2}}(x+1)^{l(2^{\frac{4}{2}}+1)}\mid l=0,1,2^{\frac{4}{2}}-2=2\}\ (\mathrm{mod}\ f_3(x))\\
&=\{x^3,x^3+x+1,x+1\}.
\end{aligned}$$

Moreover, for any $\omega(x)=a+bx+cx^2+dx^3\in\mathcal{F}_3=\frac{\mathbb{F}_2[x]}{\langle f_4(x)\rangle}$ satisfying $(a,b,c,d)\in\mathbb{F}_2^4\setminus\{(0,0,0,0)\}$, we have

$$\begin{aligned}
\omega'(x)&=\delta_4x^{-4}\omega(x^{-1})=x^{11}\omega(x^{14})\ (\mathrm{mod}\ f_5(x)=x^4+x^3+1)\\
&=(a+b+d)x^3+(a+c+d)x^2+(b+d)x+a+c.
\end{aligned}$$

Let $\mathcal{K}_j=\frac{\mathbb{F}_2[x]}{\langle f_j(x)^2\rangle}$ for all $j=1,2,3,4,5$. By Corollary 4.1, all 945 self-dual cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$ of length 30 are given by

$$\mathcal{C}=\mathcal{C}_1\oplus\mathcal{C}_2\oplus\mathcal{C}_3\oplus\mathcal{C}_4,$$

where

- $\mathcal{C}_1=\varepsilon_1(x)C_1$, C_1 is one of the following 3 ideals of the ring $\mathcal{K}_1+u\mathcal{K}_1$: $\langle u\rangle$, $\langle (x-1)\rangle$, $\langle u+(x-1)\rangle$.
- $\mathcal{C}_2=\varepsilon_2(x)C_2$, C_2 is one of the following 3 ideals of the ring $\mathcal{K}_2+u\mathcal{K}_2$: $\langle u\rangle$, $\langle (x^2+x+1)\rangle$, $\langle u+(x^2+x+1)\cdot(x+1)\rangle$.
- $\mathcal{C}_3=\varepsilon_3(x)C_3$, C_3 is one of the following 5 ideals of the ring $\mathcal{K}_3+u\mathcal{K}_3$: $\langle u\rangle$, $\langle (x^4+x^3+x^2+x+1)\rangle$, $\langle u+(x^4+x^3+x^2+x+1)\cdot\omega(x)\rangle$ with $\omega(x)\in\Theta_{3,1}$.
- $\mathcal{C}_4=\varepsilon_4(x)C_4\oplus\varepsilon_5(x)C_5$, C_j is an ideal of the ring $\mathcal{K}_j+u\mathcal{K}_j$ for $j=4,5$, and the pair (C_4,C_5) is one of the following 21 cases:

  $C_4=\langle u^i\rangle$ and $C_5=\langle u^{2-i}\rangle$, where $i=0,1,2$;
  $C_4=\langle f_4(x)\rangle$ and $C_5=\langle f_5(x)\rangle$;

$C_4 = \langle uf_4(x)\rangle$ and $C_5 = \langle u, f_5(x)\rangle$;
$C_4 = \langle u, f_4(x)\rangle$ and $C_5 = \langle uf_5(x)\rangle$;
$C_4 = \langle u + f_4(x)(a+bx+cx^2+dx^3)\rangle$ and $C_5 = \langle u + f_5(x)((a+b+d)x^3 + (a+c+d)x^2 + (b+d)x + a + c)\rangle$, where $(a, b, c, d) \in \mathbb{F}_2^4 \setminus \{(0, 0, 0, 0)\}$.

Finally, by Lemma 4.2 and Theorem 4.3 we obtain 945 binary self-dual 2-quasi-cyclic codes $\phi(\mathcal{C})$ of length 60. For example, among these codes we have the following 48 self-dual and 2-quasi-cyclic codes $\phi(\mathcal{C})$ with basic parameters [60, 30, 8], which are determined by:

- C_2 is $\langle u\rangle$ or $\langle u + (x^2 + x + 1) \cdot (x + 1)\rangle$.
- The pair (C_4, C_5) is $(\langle u^i\rangle, \langle u^{2-i}\rangle)$, for $i = 0, 2$.
- The pair (C_1, C_3) is one of the following 12 cases:

  ▷ $C_1 = \langle u\rangle$, and C_3 is one of the following 4 ideals:
  $\langle(x^4+x^3+x^2+x+1)\rangle$, $\langle u+(x^4+x^3+x^2+x+1)\cdot\omega(x)\rangle$ with $\omega(x) \in \Theta_{3,1}$;
  ▷ $C_1 = \langle(x - 1)\rangle$, and C_3 is one of the following 4 ideals:
  $\langle u\rangle$, $\langle u + (x^4 + x^3 + x^2 + x + 1) \cdot \omega(x)\rangle$ with $\omega(x) \in \Theta_{3,1}$;
  ▷ $C_1 = \langle u + (x - 1)\rangle$, and C_3 is one of the following 4 ideals:
  $\langle u\rangle$, $\langle(x^4 + x^3 + x^2 + x + 1)\rangle$, $\langle u + (x^4 + x^3 + x^2 + x + 1) \cdot \omega(x)\rangle$ with $\omega(x) \in \{x^3, x^3 + x + 1\}$.

5 The hull of every cyclic code with length 2*n* over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$

In this section, we determine the hull of each cyclic code over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ with length $2n$ where n is odd.

As a generalization for the hull of a linear code over finite field, for any linear code $\mathcal{C}$ of length $2n$ over the ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$, the hull of $\mathcal{C}$ is defined by $\mathrm{Hull}(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^{\perp}$.

Let ϕ be the isomorphism of $\mathbb{F}_{2^m}$-linear spaces from $\frac{(\mathbb{F}_{2^m}+u\mathbb{F}_{2^m})[x]}{\langle x^{2n}-1\rangle}$ onto $\mathbb{F}_{2^m}^{4n}$ defined by Eq. (8) in Sect. 4. Then from properties for ideals in a ring and Lemma 4.2, we deduce the following conclusion immediately.

Proposition 5.1 *Let $\mathcal{C}$ be a cyclic code of length $2n$ over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ and $\phi(\mathcal{C})$ be defined as in Lemma 4.2. Then*

(i) $\mathrm{Hull}(\mathcal{C})$ *is a cyclic code over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ of length $2n$.*
(ii) $\mathrm{Hull}(\phi(\mathcal{C})) = \phi(\mathcal{C}) \cap (\phi(\mathcal{C}))^{\perp}$ *is a 2-quasi-cyclic code over $\mathbb{F}_{2^m}$ of length $4n$, and* $\mathrm{Hull}(\phi(\mathcal{C})) = \phi(\mathrm{Hull}(\mathcal{C}))$.
(iii) *The Hamming weight distribution of* $\mathrm{Hull}(\phi(\mathcal{C}))$ *is exactly the same as the Lee weight distribution of* $\mathrm{Hull}(\mathcal{C})$.

It is known that a class of entanglement-assisted quantum error correcting codes (EAQECCs) can be constructed from classical codes and their basic parameters are related to the hulls of classical codes ([11, Corollary 3.1]):

Let $\mathcal{C}$ be a classical $[n,k,d]_q$ linear code and $\mathcal{C}^{\perp}$ its Euclidean dual with parameters $[n, n-k, d^{\perp}]_q$. Then there exist $[[n, k-\dim(\mathrm{Hull}(\mathcal{C})), d; n-k-\dim(\mathrm{Hull}(\mathcal{C}))]]_q$ and $[[n, n-k-\dim(\mathrm{Hull}(\mathcal{C})), d^{\perp}; k-\dim(\mathrm{Hull}(\mathcal{C}))]]_q$ EAQECCs. Further, if C is MDS then the two EAQECCs are also MDS.

Using the notation in the beginning of Sect. 3, we denote

$$\varrho(j)=\begin{cases} j, & \text{when } 1\leq j\leq \lambda;\\ j+\epsilon, & \text{when } \lambda+1\leq j\leq \lambda+\epsilon;\\ j-\epsilon, & \text{when } \lambda+\epsilon+1\leq j\leq \lambda+2\epsilon.\end{cases}$$

The dual code for every cyclic code of length $2n$ over $\frac{\mathbb{F}_{2^m}[u]}{\langle u^k\rangle}$, where $k\geq 2$, has been determined by [7, Theorem 3.5]. In particular, we have the following:

Lemma 5.2 *Let $\mathcal{C}$ be a cyclic code of length $2n$ over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ $(u^2=0)$ with canonical form decomposition $\mathcal{C}=\bigoplus_{j=1}^{r}\varepsilon_j(x)C_j$, where C_j is an ideal of $\mathcal{K}_j+u\mathcal{K}_j$. Then*

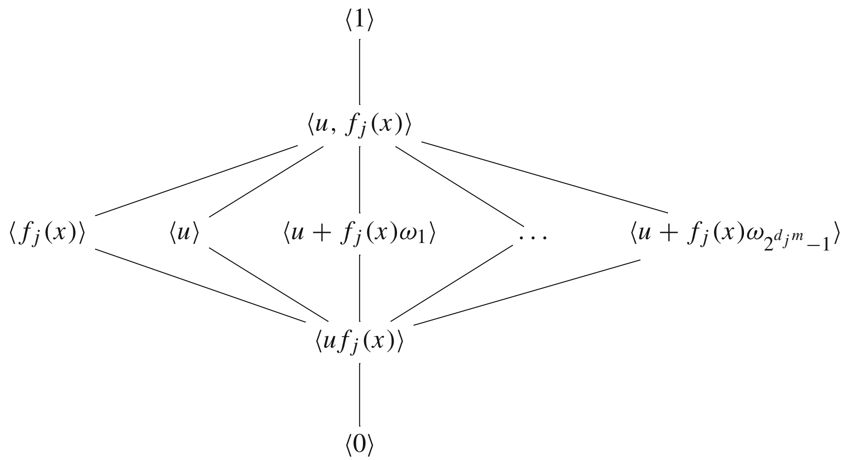
- $|\mathcal{C}|=\prod_{j=1}^{r}|C_j|$ *and* $\dim_{\mathbb{F}_{2^m}}(\mathcal{C})=\sum_{j=1}^{r}\dim_{\mathbb{F}_{2^m}}(C_j)$.
- *The dual code of $\mathcal{C}$ is given by $\mathcal{C}^{\perp}=\bigoplus_{j=1}^{r}\varepsilon_j(x)D_j$, where D_j is an ideal of $\mathcal{K}_j+u\mathcal{K}_j$ determined by the following table for all $j=1,\ldots,r$: where*

$\mathcal{L}$	C_j (mod $f_j(x)^2$)	$\lvert C_j\rvert$	κ_j	$D_{\varrho(j)}$ (mod $f_{\varrho(j)}(x)^2$)
1	• $\langle 0\rangle$	1	0	⋄ $\langle 1\rangle$
1	• $\langle 1\rangle$	4^{2d_jm}	$4d_j$	⋄ $\langle 0\rangle$
1	• $\langle u\rangle$	4^{d_jm}	$2d_j$	⋄ $\langle u\rangle$
1	• $\langle f_j(x)\rangle$	4^{d_jm}	$2d_j$	⋄ $\langle f_{\varrho(j)}(x)\rangle$
1	• $\langle uf_j(x)\rangle$	2^{d_jm}	d_j	⋄ $\langle u, f_{\varrho(j)}(x)\rangle$
$2^{d_jm}-1$	• $\langle u+f_j(x)\omega\rangle$	4^{d_jm}	$2d_j$	⋄ $\langle u+f_{\varrho(j)}(x)\omega'\rangle$
1	• $\langle u, f_j(x)\rangle$	2^{3d_jm}	$3d_j$	⋄ $\langle uf_{\varrho(j)}(x)\rangle$

$\kappa_j=\dim_{\mathbb{F}_{2^m}}(C_j)$, *$\mathcal{L}$ is the number of pairs $(C_j, D_{\varrho(j)})$ in the same row, and*

$\omega=\omega(x)\in\mathcal{F}_j=\{\sum_{i=0}^{d_j-1}a_ix^i \mid a_0,a_1,\ldots,a_{d_j-1}\in\mathbb{F}_{2^m}\}$ *and* $\omega\neq 0$,
$\omega'=\delta_jx^{-d_j}\omega(x^{-1})$ (mod $f_{\varrho(j)}(x)$).

For each integer j, $1\leq j\leq r$, let $\mathcal{F}_j\setminus\{0\}=\{\omega_1,\ldots,\omega_{2^{d_jm}-1}\}$. Then the ideal lattice of the ring $\mathcal{K}_j+u\mathcal{K}_j$ is the following figure.



Then we have the following conclusion.

Theorem 5.3 *Let $\mathcal{C}$ be a cyclic code of length $2n$ over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ with canonical form decomposition $\mathcal{C}=\bigoplus_{j=1}^{r}\varepsilon_j(x)C_j$, where C_j is an ideal of $\mathcal{K}_j+u\mathcal{K}_j$. Then the Hull of $\mathcal{C}$ is given by*

$$\mathrm{Hull}(\mathcal{C})=\bigoplus_{j=1}^{r}\varepsilon_j(x)H_j,$$

where H_j is an ideal of $\mathcal{K}_j+u\mathcal{K}_j$ determined by the following conditions for all $j=1,\ldots,r$:

(i) *Let $j=1$. Then*

$$H_1=\begin{cases}\langle 0\rangle, & \text{if } C_1=\langle 0\rangle \text{ or } \langle 1\rangle;\\ \langle u(x-1)\rangle, & \text{if } C_1=\langle u(x-1)\rangle \text{ or } \langle u, x-1\rangle;\\ \langle x-1\rangle, & \text{if } C_1=\langle x-1\rangle;\\ \langle u+(x-1)a\rangle, & \text{if } C_1=\langle u+(x-1)a\rangle \text{ where } a\in\mathbb{F}_{2^m}.\end{cases}$$

(ii) *Let $2\le j\le\lambda$. Then*

$$H_j=\begin{cases}\langle 0\rangle, & \text{if } C_j=\langle 0\rangle \text{ or } \langle 1\rangle;\\ \langle uf_j(x)\rangle, & \text{if } C_j=\langle uf_j(x)\rangle \text{ or } \langle u, f_j(x)\rangle;\\ \langle f_j(x)\rangle, & \text{if } C_j=\langle f_j(x)\rangle;\\ \langle u+f_j(x)\omega\rangle, & \text{if } C_j=\langle u+f_j(x)\omega\rangle \text{ where } \omega\in\{0\}\cup\Theta_{j,1};\\ \langle uf_j(x)\rangle, & \text{if } C_j=\langle u+f_j(x)\omega\rangle \text{ where } 0\neq\omega\in\mathcal{F}_j\setminus\Theta_{j,1}.\end{cases}$$

(iii) *Let* $\lambda+1\leq j\leq\lambda+\epsilon$. *Then the pair* $(H_j, H_{j+\epsilon})$ *of ideals is given by one of the following six cases, where* $\mathcal{S}_{j+\epsilon}$ *is the set of all* $5+2^{d_jm}$ *ideals in the ring* $\mathcal{K}_{j+\epsilon}+u\mathcal{K}_{j+\epsilon}$ *listed by Lemma 5.2.*

1. *Let* $C_j=\langle 0\rangle$. *Then*
$\diamond$ $H_j=\langle 0\rangle$ *and* $H_{j+\epsilon}=C_{j+\epsilon}$, *for every* $C_{j+\epsilon}\in\mathcal{S}_{j+\epsilon}$.

2. *Let* $C_j=\langle uf_j(x)\rangle$. *Then*
$\diamond$ $H_j=\langle 0\rangle$ *and* $H_{j+\epsilon}=\langle u, f_{j+\epsilon}(x)\rangle$, *if* $C_{j+\epsilon}=\langle 1\rangle$;
$\diamond$ $H_j=\langle uf_j(x)\rangle$ *and* $H_{j+\epsilon}=C_{j+\epsilon}$, *if* $C_{j+\epsilon}\in\mathcal{S}_{j+\epsilon}$ *and* $C_{j+\epsilon}\neq\langle 1\rangle$.

3. *Let* $C_j=\langle f_j(x)\rangle$. *Then*
$\diamond$ $H_j=\langle f_j(x)\rangle$ *and* $H_{j+\epsilon}=\langle f_{j+\epsilon}(x)\rangle$, *if* $C_{j+\epsilon}=\langle f_{j+\epsilon}(x)\rangle$;
$\diamond$ $H_j=\langle uf_j(x)\rangle$ *and* $H_{j+\epsilon}=\langle f_{j+\epsilon}(x)\rangle$, *if* $C_{j+\epsilon}=\langle u, f_{j+\epsilon}(x)\rangle$;
$\diamond$ $H_j=\langle 0\rangle$ *and* $H_{j+\epsilon}=\langle f_{j+\epsilon}(x)\rangle$, *if* $C_{j+\epsilon}=\langle 1\rangle$;
$\diamond$ $H_j=\langle f_j(x)\rangle$ *and* $H_{j+\epsilon}=C_{j+\epsilon}$, *if* $C_{j+\epsilon}=\langle uf_{j+\epsilon}(x)\rangle, \langle 0\rangle$;
$\diamond$ $H_j=\langle uf_j(x)\rangle$ *and* $H_{j+\epsilon}=\langle uf_{j+\epsilon}(x)\rangle$,
if $C_{j+\epsilon}=\langle u+f_{j+\epsilon}(x)\omega'\rangle$ *for any* $\omega'\in\mathcal{F}_{j+\epsilon}$.

4. *Let* $C_j=\langle u+f_j(x)\omega_0\rangle$, *where* $\omega_0=\omega_0(x)\in\mathcal{F}_j$. *Denote* $\omega_0'=\omega_0'(x)=\delta_jx^{-d_j}\omega_0(x^{-1})\ (\mathrm{mod}\ f_{j+\epsilon}(x))$ *in the following. Especially, we have* $\omega_0'=0$ *when* $\omega_0=0$. *Then*
$\diamond$ $H_j=\langle u+f_j(x)\omega_0\rangle$ *and* $H_{j+\epsilon}=C_{j+\epsilon}$,
if $C_{j+\epsilon}=\langle uf_{j+\epsilon}(x)\rangle, \langle u+f_{j+\epsilon}(x)\omega_0'\rangle, \langle 0\rangle$;
$\diamond$ $H_j=\langle uf_j(x)\rangle$ *and* $H_{j+\epsilon}=\langle u+f_{j+\epsilon}(x)\omega_0'\rangle$, *if* $C_{j+\epsilon}=\langle u, f_{j+\epsilon}(x)\rangle$;
$\diamond$ $H_j=\langle 0\rangle$ *and* $H_{j+\epsilon}=\langle u+f_{j+\epsilon}(x)\omega_0'\rangle$, *if* $C_{j+\epsilon}=\langle 1\rangle$;
$\diamond$ $H_j=\langle uf_j(x)\rangle$ *and* $H_{j+\epsilon}=\langle uf_{j+\epsilon}(x)\rangle$, *if* $C_{j+\epsilon}=\langle f_{j+\epsilon}(x)\rangle, \langle u+f_{j+\epsilon}(x)\omega'\rangle$ *where* $\omega'\in\mathcal{F}_{j+\epsilon}\setminus\{\omega_0'\}$.

5. *Let* $C_j=\langle u, f_j(x)\rangle$. *Then*
$\diamond$ $H_j=\langle u, f_j(x)\rangle$ *and* $H_{j+\epsilon}=\langle 0\rangle$, *if* $C_{j+\epsilon}=\langle 0\rangle$;
$\diamond$ $H_j=D_{\varrho(j+\epsilon)}$ *and* $H_{j+\epsilon}=\langle uf_{j+\epsilon}(x)\rangle$, *if* $C_{j+\epsilon}\in\mathcal{S}_{j+\epsilon}\setminus\{\langle 0\rangle\}$.

6. *Let* $C_j=\langle 1\rangle$. *Then*
$\diamond$ $H_j=D_{\varrho(j+\epsilon)}$ *and* $H_{j+\epsilon}=\langle 0\rangle$, *for every* $C_{j+\epsilon}\in\mathcal{S}_{j+\epsilon}$.

Moreover, we have that $\dim_{\mathbb{F}_{2^m}}(\mathrm{Hull}(\mathcal{C}))=\sum_{j=1}^{r}\dim_{\mathbb{F}_{2^m}}(H_j)$.

Remark (†) In Cases 5 and 6 of (iii) above, by Lemma 5.2 and $\varrho(j+\epsilon)=j$ the ideal $D_{\varrho(j+\epsilon)}$ in the ring $\mathcal{K}_j+u\mathcal{K}_j$ is determined by the following table: *where* $\mathcal{L}$ *is*

$\mathcal{L}$	$C_{j+\epsilon}\ (\mathrm{mod}\ f_{j+\epsilon}(x)^2)$	$\lvert C_{j+\epsilon}\rvert$	$D_{\varrho(j)}=D_j\ (\mathrm{mod}\ f_j(x)^2)$
1	• $\langle 0\rangle$	1	$\diamond$ $\langle 1\rangle$
1	• $\langle 1\rangle$	4^{2d_jm}	$\diamond$ $\langle 0\rangle$
1	• $\langle u\rangle$	4^{d_jm}	$\diamond$ $\langle u\rangle$
1	• $\langle f_{j+\epsilon}(x)\rangle$	4^{d_jm}	$\diamond$ $\langle f_j(x)\rangle$
1	• $\langle uf_{j+\epsilon}(x)\rangle$	2^{d_jm}	$\diamond$ $\langle u, f_j(x)\rangle$
$2^{d_jm}-1$	• $\langle u+f_{j+\epsilon}(x)\omega\rangle$	4^{d_jm}	$\diamond$ $\langle u+f_j(x)\omega'\rangle$
1	• $\langle u, f_{j+\epsilon}(x)\rangle$	2^{3d_jm}	$\diamond$ $\langle uf_j(x)\rangle$

the number of pairs $(C_{j+\epsilon}, D_j)$ *in the same row,* $d_j = d_{j+\epsilon}$ *and*

$$\omega = \omega(x) \in \mathcal{F}_{j+\epsilon} = \{\sum_{i=0}^{d_j-1} a_i x^i \mid a_0, a_1, \ldots, a_{d_j-1} \in \mathbb{F}_{2^m}\} \text{ and } \omega \neq 0,$$
$$\omega' = \delta_{j+\epsilon} x^{-d_j} \omega(x^{-1}) (\mathrm{mod}\ f_j(x)).$$

(‡) The $\mathbb{F}_{2^m}$-dimension $\dim_{\mathbb{F}_{2^m}}(H_j)$ can be obtained easily through the table in Lemma 5.2.

Proof Let $\mathcal{C}^\perp = \bigoplus_{j=1}^r \varepsilon_j(x) D_j$, where D_j is an ideal of the ring $\mathcal{K}_j + u\mathcal{K}_j$ determined by Lemma 5.2 for $j = 1, \ldots, r$. Since $\varepsilon_j(x)^2 = \varepsilon_j(x)$ and $\varepsilon_j(x)\varepsilon_l(x) = 0$ in the ring $\mathcal{A}$ for all $j \neq l$ and $j, l = 1, \ldots, r$, by Lemma 2.1 it follows that $\mathrm{Hull}(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^\perp = \bigoplus_{j=1}^r \varepsilon_j(x) H_j$ where $H_j = C_j \cap D_j$ for all $j = 1, \ldots, r$. Then by Lemma 5.2 we have the following three cases.

Case i: $j = 1$. In this case, we have $\varrho(1) = 1$, $f_1(x) = x - 1$ and $\mathcal{F}_1 = \mathbb{F}_{2^m}$. By Lemma 3.2, we know that $\delta_1 = 1$, $d_1 = 1$ and $\omega' = \omega$ for any $\omega \in \mathbb{F}_{2^m} \setminus \{0\}$. Then we have one of the following four subcases:

(i-1) Let $C_1 = \langle 0 \rangle$ or $\langle 1 \rangle$. Then $H_1 = C_1 \cap D_1 = \langle 0 \rangle$.
(i-2) Let $C_1 = \langle u(x-1) \rangle$ or $\langle u, x-1 \rangle$. Then $H_1 = C_1 \cap D_1 = \langle u(x-1) \rangle$.
(i-3) Let $C_1 = \langle x-1 \rangle$. Then $H_1 = C_1 \cap D_1 = \langle x-1 \rangle$.
(i-4) Let $C_1 = \langle u + (x-1)a \rangle$, where $a \in \mathcal{F}_{2^m}$. Then $D_1 = \langle u + (x-1)a \rangle$ by Lemma 5.2. This implies $H_1 = C_1 \cap D_1 = \langle u + (x-1)a \rangle$.

Case ii: $2 \leq j \leq \lambda$. In this case, we have $\varrho(j) = j$, $\mathcal{F}_j = \frac{\mathbb{F}_{2^m}[x]}{\langle f_j(x) \rangle}$. By Lemma 3.2, we know that $\delta_j = 1$. Then we have one of the following five subcases:

(ii-1) Let $C_j = \langle 0 \rangle$ or $\langle 1 \rangle$. Then $H_j = C_j \cap D_j = \langle 0 \rangle$.
(ii-2) Let $C_j = \langle u f_j(x) \rangle$ or $\langle u, f_j(x) \rangle$. Then $H_j = C_j \cap D_j = \langle u f_j(x) \rangle$.
(ii-3) Let $C_j = \langle f_j(x) \rangle$. Then $H_j = C_j \cap D_j = \langle f_j(x) \rangle$.
(ii-4) Let $C_j = \langle u + f_j(x)\omega \rangle$, where $\omega = \omega(x) \in \{0\} \cup \Theta_{j,1}$. For any $\omega \in \Theta_{j,1}$, by the definition of the set $\Theta_{j,1}$ before Theorem 3.1, we have that $\omega = \delta_j x^{-d_j} \widehat{\omega} = \omega'$ in the finite field $\mathcal{F}_j$. This implies $D_j = \langle u + f_j(x)\omega \rangle$ for all $\omega \in \{0\} \cup \Theta_{j,1}$. Hence $H_j = C_j \cap D_j = \langle u + f_j(x)\omega \rangle$.
(ii-5) Let $C_j = \langle u + f_j(x)\omega \rangle$, where $\omega \neq 0$ and $\omega \in \mathcal{F}_j \setminus \Theta_{j,1}$. By Lemma 5.2, we have that $D_j = \langle u + f_j(x)\omega' \rangle$ and $\omega \neq \omega'$. From this, we deduce that $H_j = C_j \cap D_j = \langle u f_j(x) \rangle$.

Case iii: $\lambda + 1 \leq j \leq \lambda + \epsilon$. In this case, we have $\varrho(j) = j + \epsilon$, $\varrho(j+\epsilon) = j$, $\mathcal{F}_j = \frac{\mathbb{F}_{2^m}[x]}{\langle f_j(x) \rangle}$ and $\mathcal{F}_{j+\epsilon} = \frac{\mathbb{F}_{2^m}[x]}{\langle f_{j+\epsilon}(x) \rangle}$. Then we have one of the following seven subcases:

(iii-1) $C_j = \langle 0 \rangle$. In this case, by Lemma 5.2 we have $D_{j+\epsilon} = \langle 1 \rangle$. This implies $H_j = C_j \cap D_j = \langle 0 \rangle$ and $H_{j+\epsilon} = C_{j+\epsilon} \cap D_{j+\epsilon} = C_{j+\epsilon}$ for any ideal $C_{j+\epsilon}$ of $\mathcal{K}_{j+\epsilon} + u\mathcal{K}_{j+\epsilon}$ by Lemma 5.2.

(iii-2) $C_j = \langle u f_j(x) \rangle$. In this case, we have $D_{j+\epsilon} = \langle u, f_{j+\epsilon}(x) \rangle$. Then by Lemma 5.2 we have the following conclusions:

- ▷ If $C_{j+\epsilon} = \langle 1 \rangle$, then $D_j = D_{\varrho(j+\epsilon)} = \langle 0 \rangle$ by Lemma 5.2. Hence $H_j = C_j \cap D_j = \langle 0 \rangle$ and $H_{j+\epsilon} = C_{j+\epsilon} \cap D_{j+\epsilon} = D_{j+\epsilon} = \langle u, f_{j+\epsilon}(x) \rangle$.

- ▹ If $C_{j+\epsilon} \neq \langle 1 \rangle$, we have $C_{j+\epsilon} \subseteq \langle u, f_{j+\epsilon}(x) \rangle$, and that $D_j = D_{\varrho(j+\epsilon)} \supseteq \langle u f_j(x) \rangle$ by Lemma 5.2. Hence $H_j = C_j \cap D_j = C_j = \langle u f_j(x) \rangle$, and $H_{j+\epsilon} = C_{j+\epsilon} \cap D_{j+\epsilon} = C_{j+\epsilon}$ for any ideal $C_{j+\epsilon}$ of $\mathcal{K}_{j+\epsilon} + u\mathcal{K}_{j+\epsilon}$ satisfying $C_{j+\epsilon} \neq \langle 1 \rangle$.

(iii-3) $C_j = \langle f_j(x) \rangle$. In this case, we have $D_{j+\epsilon} = \langle f_{j+\epsilon}(x) \rangle$. Then by Lemma 5.2 we have the following conclusions:

- ▹ If $C_{j+\epsilon} = \langle f_{j+\epsilon}(x) \rangle$, $\langle u, f_{j+\epsilon}(x) \rangle$ or $\langle 1 \rangle$, then $D_j = D_{\varrho(j+\epsilon)} = \langle f_j(x) \rangle$, $\langle u f_j(x) \rangle$ or $\langle 0 \rangle$ respectively. Hence $H_j = C_j \cap D_j = D_j$ and $H_{j+\epsilon} = C_{j+\epsilon} \cap D_{j+\epsilon} = D_{j+\epsilon} = \langle f_{j+\epsilon}(x) \rangle$.
- ▹ If $C_{j+\epsilon} = \langle u f_{j+\epsilon}(x) \rangle$ or $\langle 0 \rangle$, then $D_j = D_{\varrho(j+\epsilon)} = \langle u, f_j(x) \rangle$ or $\langle 1 \rangle$ respectively. Hence $H_j = C_j \cap D_j = C_j = \langle f_j(x) \rangle$ and $H_{j+\epsilon} = C_{j+\epsilon} \cap D_{j+\epsilon} = C_{j+\epsilon}$.
- ▹ If $C_{j+\epsilon} = \langle u + f_{j+\epsilon}(x)\omega' \rangle$ where $\omega' = \omega'(x) \in \mathcal{F}_{j+\epsilon}$, then $D_j = D_{\varrho(j+\epsilon)} = \langle u + f_j(x)\omega \rangle$ where $\omega = \omega(x) \in \mathcal{F}_j$ satisfying

$$\omega'(x) = \delta_j x^{-d_j} \omega(x^{-1}) \pmod{f_{j+\epsilon}(x)}.$$

  Hence $H_j = C_j \cap D_j = \langle f_j(x) \rangle \cap \langle u + f_j(x)\omega \rangle = \langle u f_j(x) \rangle$ and $H_{j+\epsilon} = C_{j+\epsilon} \cap D_{j+\epsilon} = \langle u + f_{j+\epsilon}(x)\omega' \rangle \cap \langle f_{j+\epsilon}(x) \rangle = \langle u f_{j+\epsilon}(x) \rangle$.

(iii-4) $C_j = \langle u \rangle$. In this case, we have $D_{j+\epsilon} = \langle u \rangle$. Similar to the case (iii-3), by Lemma 5.2 we have the following conclusions:

- ▹ If $C_{j+\epsilon} = \langle u \rangle$, $\langle u, f_{j+\epsilon}(x) \rangle$ or $\langle 1 \rangle$, then $D_j = D_{\varrho(j+\epsilon)} = \langle u \rangle$, $\langle u f_j(x) \rangle$ or $\langle 0 \rangle$ respectively. Hence $H_j = C_j \cap D_j = D_j$ and $H_{j+\epsilon} = D_{j+\epsilon} = \langle u \rangle$.
- ▹ If $C_{j+\epsilon} = \langle u f_{j+\epsilon}(x) \rangle$ or $\langle 0 \rangle$, then $D_j = D_{\varrho(j+\epsilon)} = \langle u, f_j(x) \rangle$ or $\langle 1 \rangle$ respectively. Hence $H_j = C_j \cap D_j = C_j = \langle u \rangle$ and $H_{j+\epsilon} = C_{j+\epsilon} \cap D_{j+\epsilon} = C_{j+\epsilon}$.
- ▹ If $C_{j+\epsilon} = \langle f_{j+\epsilon}(x) \rangle$ or $\langle u + f_{j+\epsilon}(x)\omega' \rangle$ where $\omega' = \omega'(x) \in \mathcal{F}_{j+\epsilon} \setminus \{0\}$, then $D_j = D_{\varrho(j+\epsilon)} = \langle f_j(x) \rangle$ or $\langle u + f_j(x)\omega \rangle$ where $\omega = \omega(x) \in \mathcal{F}_j \setminus \{0\}$ satisfying $\omega'(x) = \delta_j x^{-d_j} \omega(x^{-1}) \pmod{f_{j+\epsilon}(x)}$. Hence $H_j = C_j \cap D_j = \langle u \rangle \cap D_j = \langle u f_j(x) \rangle$ and $H_{j+\epsilon} = C_{j+\epsilon} \cap D_{j+\epsilon} = C_{j+\epsilon} \cap \langle u \rangle = \langle u f_{j+\epsilon}(x) \rangle$.

(iii-5) $C_j = \langle u + f_j(x)\omega_0 \rangle$ where $\omega_0 = \omega_0(x) \in \mathcal{F}_j \setminus \{0\}$. In this case, we have $D_{j+\epsilon} = \langle u + f_{j+\epsilon}(x)\omega_0' \rangle$ where $\omega_0' \in \mathcal{F}_{j+\epsilon} \setminus \{0\}$ satisfying $\omega_0' = \omega_0'(x) = \delta_j x^{-d_j} \omega_0(x^{-1}) \pmod{f_{j+\epsilon}(x)}$. Then by Lemma 5.2 we have the following conclusions:

- ▹ If $C_{j+\epsilon} = \langle u + f_{j+\epsilon}(x)\omega_0' \rangle$, $\langle u, f_{j+\epsilon}(x) \rangle$ or $\langle 1 \rangle$, then $D_j = D_{\varrho(j+\epsilon)} = \langle u + f_j(x)\omega_0 \rangle$, $\langle u f_j(x) \rangle$ or $\langle 0 \rangle$ respectively. Hence $H_j = C_j \cap D_j = D_j$ and $H_{j+\epsilon} = C_{j+\epsilon} \cap D_{j+\epsilon} = C_{j+\epsilon} = \langle u + f_{j+\epsilon}(x)\omega_0' \rangle$.
- ▹ If $C_{j+\epsilon} = \langle u f_{j+\epsilon}(x) \rangle$ or $\langle 0 \rangle$, then $D_j = D_{\varrho(j+\epsilon)} = \langle u, f_j(x) \rangle$ or $\langle 1 \rangle$ respectively. Hence $H_j = C_j = \langle u + f_j(x)\omega_0 \rangle$ and $H_{j+\epsilon} = C_{j+\epsilon} \cap D_{j+\epsilon} = C_{j+\epsilon}$.
- ▹ If $C_{j+\epsilon} = \langle f_{j+\epsilon}(x) \rangle$, $\langle u \rangle$ or $\langle u + f_{j+\epsilon}(x)\omega' \rangle$ where $\omega' = \omega'(x) \in \mathcal{F}_{j+\epsilon} \setminus \{\omega_0'\}$, then $D_j = D_{\varrho(j+\epsilon)} = \langle f_j(x) \rangle$, $\langle u \rangle$ or $\langle u + f_j(x)\omega \rangle$ where $\omega = \omega(x) \in \mathcal{F}_j \setminus \{\omega_0\}$ satisfying $\omega'(x) = \delta_j x^{-d_j} \omega(x^{-1}) \pmod{f_{j+\epsilon}(x)}$. Hence $H_j = C_j \cap D_j = \langle u + f_j(x)\omega_0 \rangle \cap D_j = \langle u f_j(x) \rangle$ and $H_{j+\epsilon} = C_{j+\epsilon} \cap D_{j+\epsilon} = C_{j+\epsilon} \cap \langle u + f_{j+\epsilon}(x)\omega_0' \rangle = \langle u f_{j+\epsilon}(x) \rangle$.

(iii-6) $C_j = \langle u, f_j(x) \rangle$. In this case, we have $D_{j+\epsilon} = \langle u f_{j+\epsilon}(x) \rangle$. Then by Lemma 5.2 we have the following conclusions:

- ▷ If $C_{j+\epsilon} = \langle 0\rangle$, then $D_j = D_{\varrho(j+\epsilon)} = \langle 1\rangle$ by Lemma 5.2. Hence $H_j = C_j \cap D_j = C_j = \langle u, f_j(x)\rangle$ and $H_{j+\epsilon} = C_{j+\epsilon} \cap D_{j+\epsilon} = \langle 0\rangle$.
- ▷ If $C_{j+\epsilon} \neq \langle 0\rangle$, we have $C_{j+\epsilon} \supseteq \langle uf_{j+\epsilon}(x)\rangle$, and that $D_j = D_{\varrho(j+\epsilon)} \subseteq \langle u, f_j(x)\rangle$ by Lemma 5.2. Hence $H_j = C_j \cap D_j = D_j$, and $H_{j+\epsilon} = C_{j+\epsilon} \cap D_{j+\epsilon} = C_{j+\epsilon} = \langle uf_{j+\epsilon}(x)\rangle$ for any ideal $C_{j+\epsilon}$ of $\mathcal{K}_{j+\epsilon} + u\mathcal{K}_{j+\epsilon}$ satisfying $C_{j+\epsilon} \neq \langle 0\rangle$.

(iii-7) $C_j = \langle 1\rangle$. In this case, we have $D_{j+\epsilon} = \langle 0\rangle$. This implies $H_j = C_j \cap D_j = D_j = D_{\varrho(j+\epsilon)}$ and $H_{j+\epsilon} = C_{j+\epsilon} \cap D_{j+\epsilon} = \langle 0\rangle$ for any ideal $C_{j+\epsilon}$ of $\mathcal{K}_{j+\epsilon} + u\mathcal{K}_{j+\epsilon}$ by Lemma 5.2.

When $\omega_0 = \omega_0(x) = 0$, we have $\omega_0' = \omega_0'(x) = \delta_j x^{-d_j}\omega_0(x^{-1}) = 0$ as well. Hence the Case (iii-4) and Case (iii-5) can be combined into one case where $\omega_0 \in \mathcal{F}_j$. □

For any cyclic code $\mathcal{C}$ of length $2n$ over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$, it is clear that $\mathcal{C}$ is self-orthogonal if and only if $\mathcal{C} \subseteq \mathcal{C}^{\perp}$. The latter is equivalent to that $\mathrm{Hull}(\mathcal{C}) = \mathcal{C}$. From this and by Theorem 5.3, we deduce the following corollary immediately.

Corollary 5.4 *Using the notation in Theorem 5.3, all distinct self-orthogonal cyclic codes of length $2n$ over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ are given by*

$$\mathcal{C} = \bigoplus_{j=1}^{r} \varepsilon_j(x)C_j \pmod{x^{2n}-1},$$

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

(i) *C_1 is one of the following $3 + 2^m$ ideals:*

$$\langle 0\rangle, \langle u(x-1)\rangle, \langle x-1\rangle, \langle u+(x-1)a\rangle \text{ where } a \in \mathbb{F}_{2^m}.$$

(ii) *Let $2 \le j \le \lambda$. Then C_j is one of the following $3 + 2^{\frac{d_j}{2}m}$ ideals:*

$$\langle 0\rangle, \langle uf_j(x)\rangle, \langle f_j(x)\rangle, \langle u + f_j(x)\omega\rangle \text{ where } \omega \in \{0\} \cup \Theta_{j,1}.$$

(iii) *Let $\lambda + 1 \le j \le \lambda + \epsilon$. Then the pair $(C_j, C_{j+\epsilon})$ of ideals is given by one of the following five subcases:*

◇ $5 + 2^{d_j m}$ *pairs:* $\begin{cases} C_j = \langle 0\rangle, \\ C_{j+\epsilon} \in \mathcal{S}_{j+\epsilon}. \end{cases}$

◇ $4 + 2^{d_j m}$ *pairs:* $\begin{cases} C_j = \langle uf_j(x)\rangle, \\ C_{j+\epsilon} \in \mathcal{S}_{j+\epsilon} \text{ and } C_{j+\epsilon} \neq \langle 1\rangle. \end{cases}$

◇ 3 *pairs:* $\begin{cases} C_j = \langle f_j(x)\rangle, \\ C_{j+\epsilon} = \langle f_{j+\epsilon}(x)\rangle,\ \langle uf_{j+\epsilon}(x)\rangle,\ \langle 0\rangle. \end{cases}$

◇ $3 \cdot 2^{d_j m}$ *pairs:* $\begin{cases} C_j = \langle u + f_j(x)\omega_0\rangle, \\ C_{j+\epsilon} = \langle u + f_{j+\epsilon}(x)\omega_0'\rangle,\ \langle uf_{j+\epsilon}(x)\rangle,\ \langle 0\rangle; \end{cases}$ $\forall \omega_0 \in \mathcal{F}_j$.

◇ 2 *pairs:* $\begin{cases} C_j = \langle u, f_j(x)\rangle,\ \langle 1\rangle \\ C_{j+\epsilon} = \langle 0\rangle. \end{cases}$

Therefore, the number of self-orthogonal cyclic codes of length $2n$ *over* $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ *is* $(3+2^m)\cdot\prod_{j=2}^{\lambda}(3+2^{\frac{d_j}{2}m})\cdot\prod_{j=\lambda+1}^{\lambda+\epsilon}(14+5\cdot 2^{d_j m})$.

Now, we list the number $\mathcal{NO}$ of self-orthogonal cyclic codes $\mathcal{C}$ over $\mathbb{F}_2 + u\mathbb{F}_2$ of length $2n$, where n is odd and $6 \le 2n \le 98$, in the following table.

$2n$	$\mathcal{NO}$	$2n$	$\mathcal{NO}$
6	$25 = 5(3+2)$	54	$141625 = 5(3+2)(3+2^3)(3+2^9)$
10	$45 = 5(3+2^2)$	58	$81935 = 5(3+2^{14})$
14	$270 = 5(14+5\cdot 2^3)$	62	$26340120 = 5(14+5\cdot 2^5)^3$
18	$275 = 5(3+2)(3+2^3)$	66	$982600 = 5(3+2)(3+2^5)^3$
22	$175 = 5(3+2^5)$	70	38733660
26	$335 = 5(3+2^6)$	74	$1310735 = 5(3+2^{18})$
30	$16450 = 25(3+2^2)(14+5\cdot 2^4)$	78	$34327450 = 25(3+2^6)(14+5\cdot 2^{12})$
34	$1805 = 5(3+2^4)^2$	82	$5273645 = 5(3+2^{10})^2$
38	$2575 = 5(3+2^9)$	86	$11240455 = 5(3+2^7)^3$
42	$450900 = 25(14+5\cdot 2^3)(14+5\cdot 2^6)$	90	3708389300
46	$51270 = 5(14+5\cdot 2^{11})$	94	$209715270 = 5(14+5\cdot 2^{23})$
50	$35945 = 5(3+2^2)(3+2^{10})$	98	2831158980

where $38733660 = 5(3+2^2)(14+5\cdot 2^3)(14+5\cdot 2^{12})$ and

$$3708389300 = 5(3+2)(3+2^2)(3+2^3)(14+5\cdot 2^4)(14+5\cdot 2^{12}),$$
$$2831158980 = 5(14+5\cdot 2^3)(14+5\cdot 2^{21}).$$

Remark (i) Let $\mathcal{C}$ be a cyclic code of length $2n$ over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$. Then $\mathcal{C}$ is orthogonal self-contained if and only if $\mathrm{Hull}(\mathcal{C}) = \mathcal{C}^{\perp}$. All distinct orthogonal self-contained cyclic codes of length $2n$ over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ can be determined by Theorem 5.3 similar to the case of self-orthogonal cyclic codes. Furthermore, we can obtain orthogonal self-contained and 2-quasi-cyclic codes of length $4n$ over $\mathbb{F}_{2^m}$ by Eq. (8) in Sect. 4. A class of EAQECCs has been constructed from orthogonal self-contained cyclic codes and LCD codes in literatures (see [11, Proposition 4.2] and [20], for example).

(ii) Let ϕ be the isomorphism of $\mathbb{F}_{2^m}$-linear spaces from $\frac{(\mathbb{F}_{2^m}+u\mathbb{F}_{2^m})[x]}{\langle x^{2n}-1\rangle}$ onto $\mathbb{F}_{2^m}^{4n}$ defined by Eq. (8). By Proposition 5.1, we see that $\phi(\mathcal{C})$ is a self-orthogonal 2-quasi-cyclic code of length $4n$ over the finite field $\mathbb{F}_{2^m}$ for every self-orthogonal cyclic code $\mathcal{C}$ over the ring $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ of length $2n$. In particular, The Hamming weight distribution of $\phi(\mathcal{C})$ is the same as the Lee weight distribution of $\mathcal{C}$ by Lemma 4.2(ii).

(iii) On the last line of the three tables in Pages 265, 272 and 274 of [7], the range $0 \le t < s < i \le k-1$ (resp. $1 \le t < s < i \le k-1$) for the triple (t, s, i) of integers should be changed to $0 \le t < s < i \le k-2$ (resp. $1 \le t < s < i \le k-2$). Because there is no triple (t, s, i) of integers satisfying all the conditions: $i = k-1$, $i+s \le k+t-1$ (i.e., $s \le t$) and $t < s$.

6 Conclusions and further research

We have given an explicit representation for self-dual cyclic codes of length $2n$ over the ring $R=\mathbb{F}_{2^m}[u]/\langle u^k\rangle=\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}+\cdots+u^{k-1}\mathbb{F}_{2^m}$ $(u^k=0)$ and a clear Mass formula to count the number of these codes, for any integer $k\geq 2$ and positive odd integer n. Then, all self-dual 2-quasi-cyclic codes over finite field $\mathbb{F}_{2^m}$ of length $4n$ derived from self-dual cyclic codes of length $2n$ over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ $(u^2=0)$ are determined by providing their generator matrices precisely. Moreover, we determine the hull of each cyclic code of length $2n$ over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$, and give an explicit representation and enumeration for self-orthogonal cyclic codes of length $2n$ over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$.

Giving an explicit representation and enumeration for self-dual cyclic codes over R for arbitrary even length and considering the construction of EAQECCs from the class of self-orthogonal (resp. orthogonal self-contained) 2-quasi-cyclic codes of length $4n$ over $\mathbb{F}_{2^m}$ derived from self-orthogonal (resp. orthogonal self-contained) cyclic codes of length $2n$ over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ are future topics of interest.

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

Appendix: All distinct self-dual cyclic codes of length 2*n* over the ring $R=\frac{\mathbb{F}_{2^m}[u]}{\langle u^k\rangle}$, where $3\leq k\leq 5$ and *n* is odd

By Lemma 2.3, Corollary 2.5, Theorem 3.1 and Theorem 3.3, we have the follows conclusions.

Case $k=4$

Using the notation in Theorem 3.3(ii), the number of self-dual cyclic codes of length $2n$ over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}+u^2\mathbb{F}_{2^m}+u^3\mathbb{F}_{2^m}$ $(u^4=0)$ is

$$(1+2^m+4^m)\cdot\prod_{j=2}^{\lambda}(1+2^{\frac{d_j}{2}m}+2^{d_jm})\cdot\prod_{j=\lambda+1}^{\lambda+\epsilon}(9+5\cdot 2^{d_jm}+4^{d_jm}).$$

Precisely, all these codes are given by

$$\mathcal{C}=\left(\oplus_{j=1}^{\lambda}\varepsilon_j(x)C_j\right)\oplus\left(\oplus_{j=\lambda+1}^{\lambda+\epsilon}(\varepsilon_j(x)C_j\oplus\varepsilon_{j+\epsilon}(x)C_{j+\epsilon})\right),$$

where C_j is an ideal of $\mathcal{K}_j + u\mathcal{K}_j + u^2\mathcal{K}_j + u^3\mathcal{K}_j$ ($u^4 = 0$) listed as follows:

(i) C_1 is one of the following $1 + 2^m + 4^m$ ideals:

$$\langle u^2\rangle, \langle (x-1)\rangle;$$
$$\langle u^2 + u(x-1)\omega\rangle \text{ where } \omega \in \mathbb{F}_{2^m} \text{ and } \omega \neq 0;$$
$$\langle u^2 + (x-1)\omega\rangle \text{ where } \omega = a_0 + ua_1, a_0, a_1 \in \mathbb{F}_{2^m} \text{ and } a_0 \neq 0;$$
$$\langle u^3 + (x-1)\omega\rangle \text{ where } \omega \in \mathbb{F}_{2^m} \text{ and } \omega \neq 0;$$
$$\langle u^3, u(x-1)\rangle.$$

(ii) Let $2 \leq j \leq \lambda$. Then C_j is one of the following $1 + 2^{\frac{d_j}{2}m} + 2^{d_j m}$ ideals:

$$\langle u^2\rangle, \langle f_j(x)\rangle;$$
$$\langle u^2 + uf_j(x)\omega\rangle \text{ where } \omega \in \Theta_{j,1};$$
$$\langle u^2 + f_j(x)\omega\rangle \text{ where } \omega = a_0(x) + ua_1(x), a_0(x) \in \Theta_{j,1} \text{ and } a_1(x) \in \{0\} \cup \Theta_{j,1};$$
$$\langle u^3 + f_j(x)\omega\rangle \text{ where } \omega \in \Theta_{j,1};$$
$$\langle u^3, uf_j(x)\rangle.$$

(iii) Let $\lambda+1 \leq j \leq \lambda+\epsilon$. Then the pair $(C_j, C_{j+\epsilon})$ of ideals is one of the following $9 + 5\cdot 2^{d_j m} + 4^{d_j m}$ cases listed in the following table:

$\mathcal{L}$	C_j (mod $f_j(x)^2$)	$\lvert C_j\rvert$	$C_{j+\epsilon}$ (mod $f_{j+\epsilon}(x)^2$)
5	• $\langle u^i\rangle$ $(0 \leq i \leq 4)$	$4^{(4-i)d_j m}$	◇ $\langle u^{k-i}\rangle$
4	• $\langle u^s f_j(x)\rangle$ $(0 \leq s \leq 3)$	$2^{(4-s)d_j m}$	◇ $\langle u^{4-s}, f_{j+\epsilon}(x)\rangle$
$3(2^{d_j m}-1)$	• $\langle u^i + u^{i-1}f_j(x)\omega\rangle$ $(i = 1, 2, 3)$	$4^{(4-i)d_j m}$	◇ $\langle u^{4-i} + u^{3-i}f_{j+\epsilon}(x)\omega'\rangle$
$4^{d_j m} - 2^{d_j m}$	• $\langle u^2 + f_j(x)\vartheta\rangle$	$4^{2d_j m}$	◇ $\langle u^2 + f_{j+\epsilon}(x)\vartheta'\rangle$
$2^{d_j m}-1$	• $\langle u^3 + f_j(x)\omega\rangle$	$2^{4d_j m}$	◇ $\langle u^3 + f_{j+\epsilon}(x)\omega'\rangle$
$2^{d_j m}-1$	• $\langle u^3 + uf_j(x)\omega\rangle$	$2^{3d_j m}$	◇ $\langle u^2 + f_{j+\epsilon}(x)\omega', uf_{j+\epsilon}(x)\rangle$
6	• $\langle u^i, u^s f_j(x)\rangle$ $(0 \leq s < i \leq 3)$	$2^{(8-(i+s))d_j m}$	◇ $\langle u^{4-s}, u^{4-i}f_{j+\epsilon}(x)\rangle$
$2^{d_j m}-1$	• $\langle u^2 + f_j(x)\omega, uf_j(x)\rangle$	$2^{5d_j m}$	◇ $\langle u^3 + uf_{j+\epsilon}(x)\omega'\rangle$

where $\mathcal{L}$ is the number of pairs $(C_j, C_{j+\epsilon})$ in the same row, and

$$\omega = \omega(x) \in \mathcal{F}_j = \frac{\mathbb{F}_{2^m}[x]}{\langle f_j(x)\rangle}, \omega \neq 0 \text{ and}$$
$$\omega' = \delta_j x^{-d_j}\omega(x^{-1}) \text{ (mod } f_{j+\epsilon}(x));$$

$\vartheta = a_0(x) + ua_1(x)$ with $a_0(x), a_1(x) \in \mathcal{F}_j$ and $a_0(x) \neq 0$, and

$$\vartheta' = \delta_j x^{-d_j}\left(a_0(x^{-1}) + ua_1(x^{-1})\right) \pmod{f_{j+\epsilon}(x)}.$$

Case $k = 3$

Using the notation in Theorem 3.3(ii), the number of self-dual cyclic codes of length $2n$ over the ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + u^2\mathbb{F}_{2^m}$ ($u^3 = 0$) is

$$(1 + 2^m) \cdot \prod_{j=2}^{\lambda}(1 + 2^{\frac{d_j}{2}m}) \cdot \prod_{j=\lambda+1}^{\lambda+\epsilon}(7 + 3 \cdot 2^{d_j m}).$$

Precisely, all these codes are given by

$$\mathcal{C} = \left(\oplus_{j=1}^{\lambda}\varepsilon_j(x)C_j\right) \oplus \left(\oplus_{j=\lambda+1}^{\lambda+\epsilon}(\varepsilon_j(x)C_j \oplus \varepsilon_{j+\epsilon}(x)C_{j+\epsilon})\right),$$

where C_j is an ideal of $\mathcal{K}_j + u\mathcal{K}_j + u^2\mathcal{K}_j$ ($u^3 = 0$) listed as follows:

(i) C_1 is one of the following $1 + 2^m$ ideals:

$$\langle (x-1)\rangle, \langle u^2, u(x-1)\rangle;$$
$$\langle u^2 + (x-1)\omega\rangle \text{ where } \omega \in \mathbb{F}_{2^m} \text{ and } \omega \neq 0.$$

(ii) Let $2 \leq j \leq \lambda$. Then C_j is one of the following $1 + 2^{\frac{d_j}{2}m}$ ideals:

$$\langle f_j(x)\rangle, \langle u^2, uf_j(x)\rangle;$$
$$\langle u^2 + f_j(x)\omega\rangle \text{ where } \omega \in \Theta_{j,1}.$$

(iii) Let $\lambda+1 \leq j \leq \lambda+\epsilon$. Then the pair $(C_j, C_{j+\epsilon})$ of ideals is one of the following $7 + 3 \cdot 2^{d_j m}$ cases listed in the following table:

$\mathcal{L}$	$C_j \pmod{f_j(x)^2}$	$\|C_j\|$	$C_{j+\epsilon} \pmod{f_{j+\epsilon}(x)^2}$
4	• $\langle u^i\rangle$ $(i = 0, 1, 2, 3)$	$4^{(3-i)d_j m}$	◇ $\langle u^{3-i}\rangle$
3	• $\langle u^s f_j(x)\rangle$ $(0 \leq s \leq 2)$	$2^{(3-s)d_j m}$	◇ $\langle u^{3-s}, f_{j+\epsilon}(x)\rangle$
$2^{d_j m} - 1$	• $\langle u + f_j(x)\omega\rangle$	$4^{2d_j m}$	◇ $\langle u^2 + uf_{j+\epsilon}(x)\omega'\rangle$
$2^{d_j m} - 1$	• $\langle u^2 + uf_j(x)\omega\rangle$	$4^{d_j m}$	◇ $\langle u + f_{j+\epsilon}(x)\omega'\rangle$
$2^{d_j m} - 1$	• $\langle u^2 + f_j(x)\omega\rangle$	$2^{3d_j m}$	◇ $\langle u^2 + f_{j+\epsilon}(x)\omega'\rangle$
3	• $\langle u^i, u^s f_j(x)\rangle$ $(0 \leq s < i \leq 2)$	$2^{(6-(i+s))d_j m}$	◇ $\langle u^{3-s}, u^{3-i} f_{j+\epsilon}(x)\rangle$

where $\mathcal{L}$ is the number of pairs $(C_j, C_{j+\epsilon})$ in the same row, $\omega = \omega(x) \in \mathcal{F}_j = \frac{\mathbb{F}_{2^m}[x]}{\langle f_j(x)\rangle}$ with $\omega \neq 0$, and $\omega' = \delta_j x^{-d_j}\omega(x^{-1}) \pmod{f_{j+\epsilon}(x)}$.

Case $k = 5$

◇ Using the notation in Theorem 3.3(ii), the number of self-dual cyclic codes of length $2n$ over the ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + u^2\mathbb{F}_{2^m} + u^3\mathbb{F}_{2^m} + u^4\mathbb{F}_{2^m}$ $(u^5 = 0)$ is

$$(1 + 2^m + 4^m) \cdot \prod_{j=2}^{\lambda}(1 + 2^{\frac{d_j}{2}m} + 2^{d_j m}) \cdot \prod_{j=\lambda+1}^{\lambda+\epsilon}(11 + 7 \cdot 2^{d_j m} + 3 \cdot 4^{d_j m}).$$

Precisely, all these codes are given by

$$\mathcal{C} = \left(\oplus_{j=1}^{\lambda}\varepsilon_j(x)C_j\right) \oplus \left(\oplus_{j=\lambda+1}^{\lambda+\epsilon}(\varepsilon_j(x)C_j \oplus \varepsilon_{j+\epsilon}(x)C_{j+\epsilon})\right),$$

where C_j is an ideal of $\mathcal{K}_j + u\mathcal{K}_j + u^2\mathcal{K}_j + u^3\mathcal{K}_j + u^4\mathcal{K}_j$ $(u^5 = 0)$ listed as follows:

(i) Let $\lambda + 1 \le j \le \lambda + \epsilon$. Then the pair $(C_j, C_{j+\epsilon})$ of ideals is one of the following $11 + 7 \cdot 2^{d_j m} + 3 \cdot 4^{d_j m}$ cases listed in the following table:

$\mathcal{L}$	$C_j \pmod{f_j(x)^2}$	$\lvert C_j\rvert$	$C_{j+\epsilon} \pmod{f_{j+\epsilon}(x)^2}$
6	• $\langle u^i\rangle$ $(0 \le i \le 5)$	$4^{(5-i)d_j m}$	◇ $\langle u^{5-i}\rangle$
5	• $\langle u^s f_j(x)\rangle$ $(0 \le s \le 4)$	$2^{(5-s)d_j m}$	◇ $\langle u^{5-s}, f_{j+\epsilon}(x)\rangle$
$4(2^{d_j m} - 1)$	• $\langle u^i + u^{i-1} f_j(x)\omega\rangle$ $(i = 1, 2, 3, 4)$	$4^{(5-i)d_j m}$	◇ $\langle u^{4-i} f_{j+\epsilon}(x)\omega' + u^{5-i}\rangle$
$4^{d_j m} - 2^{d_j m}$	• $\langle u^2 + f_j(x)\vartheta\rangle$	$4^{3d_j m}$	◇ $\langle u^3 + uf_{j+\epsilon}(x)\vartheta'\rangle$
$4^{d_j m} - 2^{d_j m}$	• $\langle u^3 + uf_j(x)\vartheta\rangle$	$4^{2d_j m}$	◇ $\langle u^2 + f_{j+\epsilon}(x)\vartheta'\rangle$
$4^{d_j m} - 2^{d_j m}$	• $\langle u^3 + f_j(x)\vartheta\rangle$	$2^{5d_j m}$	◇ $\langle u^3 + f_{j+\epsilon}(x)\vartheta'\rangle$
$2^{d_j m} - 1$	• $\langle u^4 + f_j(x)\omega\rangle$	$2^{5d_j m}$	◇ $\langle u^4 + f_{j+\epsilon}(x)\omega'\rangle$
$2^{d_j m} - 1$	• $\langle u^4 + uf_j(x)\omega\rangle$	$2^{4d_j m}$	◇ $\langle u^3 + f_{j+\epsilon}(x)\omega', uf_{j+\epsilon}(x)\rangle$
$2^{d_j m} - 1$	• $\langle u^4 + u^2 f_j(x)\omega\rangle$	$2^{3d_j m}$	◇ $\langle u^2 + f_{j+\epsilon}(x)\omega', uf_{j+\epsilon}(x)\rangle$
10	• $\langle u^i, u^s f_j(x)\rangle$ $(0 \le s < i \le 4)$	$2^{(10-(i+s))d_j m}$	◇ $\langle u^{5-s}, u^{5-i} f_{j+\epsilon}(x)\rangle$
$2^{d_j m} - 1$	• $\langle u^2 + f_j(x)\omega, uf_j(x)\rangle$	$2^{7d_j m}$	◇ $\langle u^4 + u^2 f_{j+\epsilon}(x)\omega'\rangle$
$2^{d_j m} - 1$	• $\langle u^3 + f_j(x)\omega, uf_j(x)\rangle$	$2^{6d_j m}$	◇ $\langle u^4 + uf_{j+\epsilon}(x)\omega'\rangle$
$2^{d_j m} - 1$	• $\langle u^3 + uf_j(x)\omega, u^2 f_j(x)\rangle$	$2^{5d_j m}$	◇ $\langle u^3 + uf_{j+\epsilon}(x)\omega', u^2 f_{j+\epsilon}(x)\rangle$

where $\mathcal{L}$ is the number of pairs $(C_j, C_{j+\epsilon})$ in the same row;
$\omega = \omega(x) \in \mathcal{F}_j = \frac{\mathbb{F}_{2^m}[x]}{\langle f_j(x)\rangle}$, $\omega \neq 0$ and

$$\omega' = \delta_j x^{-d_j}\omega(x^{-1}) \pmod{f_{j+\epsilon}(x)};$$

$\vartheta = a_0(x) + ua_1(x)$ with $a_0(x), a_1(x) \in \mathcal{F}_j$ and $a_0(x) \neq 0$, and

$$\vartheta' = \delta_j x^{-d_j}\left(a_0(x^{-1}) + ua_1(x^{-1})\right) \pmod{f_{j+\epsilon}(x)}.$$

(ii) C_1 is one of the following $1 + 2^m + 4^m$ ideals:
$\langle (x-1)\rangle$;
$\langle u^3 + (x-1)\omega\rangle$ where $\omega = a_0 + ua_1$, $a_0, a_1 \in \mathbb{F}_{2^m}$ and $a_0 \neq 0$;
$\langle u^4 + (x-1)\omega\rangle$ where $\omega \in \mathbb{F}_{2^m}$ and $\omega \neq 0$;
$\langle u^3, u^2(x-1)\rangle$, $\langle u^4, u(x-1)\rangle$;
$\langle u^3 + u(x-1)\omega, u^2(x-1)\rangle$ where $\omega \in \mathbb{F}_{2^m}$ and $\omega \neq 0$.

(iii) Let $2 \leq j \leq \lambda$. Then C_j is one of the following $1 + 2^{\frac{d_j}{2}m} + 2^{d_j m}$ ideals:
$\langle f_j(x)\rangle$;
$\langle u^3 + f_j(x)\omega\rangle$ where $\omega = a_0(x) + ua_1(x)$, $a_0(x) \in \Theta_{j,1}$ and $a_1(x) \in \{0\} \cup \Theta_{j,1}$;
$\langle u^4 + f_j(x)\omega\rangle$ where $\omega \in \Theta_{j,1}$;
$\langle u^3, u^2 f_j(x)\rangle$, $\langle u^4, uf_j(x)\rangle$;
$\langle u^3 + uf_j(x)\omega, u^2 f_j(x)\rangle$ where $\omega \in \Theta_{j,1}$.

References

1. Abualrub, T., Siap, I.: Cyclic codes over the ring $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$. Des. Codes Cryptogr. **42**, 273–287 (2007)
2. Al-Ashker, M., Hamoudeh, M.: Cyclic codes over $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2 + \ldots + u^{k-1}\mathbb{Z}_2$. Turk. J. Math. **35**(4), 737–749 (2011)
3. Alfaro, R., Dhul-Qarnayn, K.: Constructing self-dual codes over $\mathbb{F}_q[u]/(u^t)$. Des. Codes Cryptogr. **74**, 453–465 (2015)
4. Betsumiya, K., Ling, S., Nemenzo, F.R.: Type II codes over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$. Discrete Math. **275**(1–3), 43–65 (2004)
5. Bonnecaze, A., Rains, E., Solé, P.: 3-colored 5-designs and $\mathbb{Z}_4$-codes. J. Stat. Plan. Inference **86**(2), 349–368 (2000). Special issue in honor of Professor Ralph Stanton. MR 1768278 (2001g:05021)
6. Bonnecaze, A., Udaya, P.: Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE Trans. Inf. Theory **45**, 1250–1255 (1999)
7. Cao, Y., Cao, Y., Fu, F.-W.: Cyclic codes over $\mathbb{F}_{2^m}[u]/\langle u^k\rangle$ of oddly even length. Appl. Algebra Eng. Commun. Comput. **27**, 259–277 (2016)
8. Chen, B., Ling, S., Zhang, G.: Enumeration formulas for self-dual cyclic codes. Finite Fields Appl. **42**, 1–22 (2016)
9. Dinh, H.Q.: Constacyclic codes of length 2^s over Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE Trans. Inf. Theory **55**, 1730–1740 (2009)
10. Dougherty, S.T., Gaborit, P., Harada, M., Solé, P.: Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE. Trans. Inf. Theory **45**(1), 32–45 (1999). MR 1677846 (2000h:94053)
11. Guenda, K., Jitman, S., Gulliver, T.A.: Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr. **86**, 121–136 (2018)
12. Han, S., Lee, H., Lee, Y.: Construction of self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. Bull. Korean Math. Soc. **49**(1), 135–143 (2012)

13. Karadeniz, S., Yildiz, B., Aydin, N.: Extremal binary self-dual codes of lengths 64 and 66 from four-circulant constructions over $\mathbb{F}_2 + u\mathbb{F}_2$. Filomat **28**(5), 937–945 (2014)
14. Kaya, A., Yildiz, B., Siap, I.: New extremal binary self-dual codes from $\mathbb{F}_4 + u\mathbb{F}_4$-lifts of quadratic double circulant codes over $\mathbb{F}_4$. Finite Fields Appl. **35**, 318–329 (2015)
15. Kaya, A., Yildiz, B.: Various constructions for self-dual codes over rings and new binary self-dual codes. Discrete Math. **339**(2), 460–469 (2016)
16. Ling, S., Solé, P.: Type II codes over $\mathbb{F}_4 + u\mathbb{F}_4$. Eur. J. Comb. **22**, 983–997 (2001)
17. Norton, G., Sălăgean-Mandache, A.: On the structure of linear and cyclic codes over finite chain rings. Appl. Algebra Eng. Commun. Comput. **10**, 489–506 (2000)
18. Sangwisut, E., Jitman, S., Ling, S., Udomkavanich, P.: Hulls of cyclic and negacyclic codes over finite fields. Finite Fields Appl. **33**, 232–257 (2015)
19. Singh, A.K., Kewat, P.K.: On cyclic codes over the ring $\mathbb{Z}_p[u]/\langle u^k \rangle$. Des. Codes Cryptogr. **74**, 1–13 (2015)
20. Sok, L., Shi, M., Solé, P.: Construction of optimal LCD codes over large finite fields. Finite Fields Appl. **50**, 138–153 (2018)