Cyclic codes over Z4 of even length

Dougherty, Steven T.; Ling, San

2006

Dougherty, S. T., & Ling, S. (2006). Cyclic Codes Over Z4 of Even Length. Designs, Codes and Cryptography, 39(2), 127-153.

https://hdl.handle.net/10356/96404

https://doi.org/10.1007/s10623-005-2773-x

Cyclic Codes Over $\mathbb{Z}_4$ of Even Length

STEVEN T. DOUGHERTY[†] doughertys1@scranton.edu
Department of Mathematics, University of Scranton, Scranton, PA 18510, USA

SAN LING[*] lingsan@ntu.edu.sg
Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Block 5, Level 3, 1 Nanyang Walk, Singapore 637616, Republic of Singapore

Communicated by: T. Helleseth

Abstract. We determine the structure of cyclic codes over $\mathbb{Z}_4$ for arbitrary even length giving the generator polynomial for these codes. We determine the number of cyclic codes for a given length. We describe the duals of the cyclic codes, describe the form of cyclic codes that are self-dual and give the number of these codes. We end by examining specific cases of cyclic codes, giving all cyclic self-dual codes of length less than or equal to 14.

Keywords: cyclic codes, codes over rings

1. Introduction

Cyclic codes are an important class of codes from both a theoretical and a practical viewpoint. The key to describing the structure of cyclic codes over a ring R is to view cyclic codes as ideals in the polynomial ring $R[X]/\langle X^n - 1\rangle$, where n is the length of the code. For this purpose, it is useful to obtain the divisors of $X^n - 1$, but this becomes difficult when the characteristic of the ring is not relatively prime to the length of the code, i.e., the repeated-root case, because then $X^n - 1$ does not factor uniquely over the ring. For codes over $\mathbb{Z}_4$, this case corresponds to the case when the length is even.

In [1], Abualrub and Oehmke determine the generators for cyclic codes over $\mathbb{Z}_4$ for lengths of the form 2^k and in [2], Blackford determines the generators for cyclic codes over $\mathbb{Z}_4$ for lengths of the form $2n$ where n is odd. The case for odd n follows from results in [3] and also appears in more detail in [7]. In this paper, we shall complete the classification by examining cyclic codes over $\mathbb{Z}_4$ of length $N = 2^k n$, where n is odd. Our results will generalize the results of Refs. 1 and 2. Moreover, allowing $k = 0$, we get the results given in [7] for the odd case. From this perspective we see that our work in fact can handle all lengths.

[*]The research of the second named author is partially supported by research Grants MOE-ARF R-146-000-029-112 and DSTA R-394-000-011-422.
[†]Corresponding author.

We shall build an isomorphism between the standard polynomial ring and another polynomial ring and show that cyclic codes in the former correspond to constacyclic codes in the latter. Using the Discrete Fourier Transform, we give the structure of the second polynomial ring as the direct sum of rings and show that the ideal corresponding to a cyclic code can be described as the direct sum of ideals under this decomposition. We use this to find all generators of cyclic codes and determine the structure and size of their dual codes.

We begin with some definitions. A code over a ring R of length n is a non-empty subset of R^n. If the code is a submodule, then we say that the code is linear. All codes in this work are assumed to be linear unless otherwise specified. The ambient space is equipped with the standard inner-product, i.e., $[v, w] = \sum v_i w_i$, where $v = (v_1, \ldots, v_n)$ and $w = (w_1, \ldots, w_n)$, and the dual is defined by $C^\perp = \{w \mid [w, v] = 0 \text{ for all } v \in C\}$. If $(c_0, c_1, \ldots, c_{n-1}) \in C$ implies that $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$, then we say that the code is cyclic. We use the natural connection of cyclic codes to polynomial rings, where $(c_0, c_1, \ldots, c_{n-1})$ is viewed as $c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$ and the code C is an ideal in the ring $R[X]/\langle X^n - 1\rangle$. A code over a ring is constacyclic if, for some unit a, we have $(c_0, c_1, \ldots, c_{n-1}) \in C$ implies that $(ac_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$.

If C is a code of length n over a finite chain ring R of characteristic 4 with unique maximal ideal m, then we can define the torsion and residue codes over the residue field $F := R/\mathsf{m}$ of characteristic 2 by

$$\mathrm{Tor}(C) = \{\mathbf{v} \in F^n \mid 2\mathbf{v} \in C\} \tag{1}$$

and

$$\mathrm{Res}(C) = \{\mathbf{v} \in F^n \mid \text{ there exists } \mathbf{u} \text{ such that } \mathbf{v} + 2\mathbf{u} \in C\}. \tag{2}$$

(Here, the residue field $F = R/\mathsf{m}$ is identified with the Teichmüller set of R.)

We can describe the generator matrices of these codes over $\mathbb{Z}_4$. A linear code over $\mathbb{Z}_4$ has a generator matrix that is permutation-equivalent to

$$\begin{pmatrix} I_{k_1} & A & A' \\ 0 & 2I_{k_2} & 2A'' \end{pmatrix}, \tag{3}$$

where I_k is the identity matrix of size k, A and A'' are matrices with entries from $\{0, 1\}$, and A' is a matrix with entries from $\mathbb{Z}_4$. A code of this form is said to be of type $\{k_1, k_2\}$. It contains $4^{k_1} 2^{k_2}$ elements.

The code over $\mathbb{F}_2$ with generator matrix

$$\begin{pmatrix} I_{k_1} & A & \overline{A'} \end{pmatrix}, \tag{4}$$

where $\overline{A'}$ is the reduction modulo 2 of A', is the *residue code*. The code over $\mathbb{F}_2$ with generator matrix

$$\begin{pmatrix} I_{k_1} & A & \overline{A'} \\ 0 & I_{k_2} & A'' \end{pmatrix}, \tag{5}$$

is the *torsion code*.

Notice that $|\mathrm{Tor}(C)||\mathrm{Res}(C)| = 2^{k_1}2^{k_1+k_2} = 4^{k_1}2^{k_2} = |C|$. This same equality holds for another ring we describe later (see Lemma 2.4). We shall use this fact to determine the cardinality of codes by determining the torsion and residue codes from the generators.

2. Rings

We shall describe a ring and relate this ring to the standard description of cyclic codes over $\mathbb{Z}_4$ to find the generator polynomials. We assume throughout the rest of this paper that n is an odd integer and $N = 2^k n$ will denote the length of a cyclic code over $\mathbb{Z}_4$.

Define the ring $\mathcal{R} = \mathbb{Z}_4[u]/\langle u^{2^k} - 1\rangle$. We have a module isomorphism $\Psi: \mathcal{R}^n \to (\mathbb{Z}_4)^{2^k n}$ defined by

$$\begin{aligned}\Psi\Big(&a_{0,0} + a_{0,1}u + a_{0,2}u^2 + \cdots + a_{0,2^k-1}u^{2^k-1}, \ldots,\\ &a_{n-1,0} + a_{n-1,1}u + a_{n-1,2}u^2 + \cdots + a_{n-1,2^k-1}u^{2^k-1}\Big)\\ =&(a_{0,0}, a_{1,0}, a_{2,0}, a_{3,0}, \ldots, a_{n-1,0}, a_{0,1}, a_{1,1}, a_{2,1}, \ldots, a_{0,2^k-1},\\ &a_{1,2^k-1}, \ldots, a_{n-1,2^k-1}).\end{aligned}$$

We have that

$$\begin{aligned}&\Psi\left(u\left(\sum_{j=0}^{2^k-1} a_{n-1,j}u^j\right), \sum_{j=0}^{2^k-1} a_{0,j}u^j, \sum_{j=0}^{2^k-1} a_{1,j}u^j, \ldots, \sum_{j=0}^{2^k-1} a_{n-2,j}u^j\right)\\ &= (a_{n-1,2^k-1}, a_{0,0}, a_{1,0}, \ldots, a_{n-2,2^k-1}).\end{aligned}$$

This gives that a cyclic shift in $(\mathbb{Z}_4)^{2^k n}$ corresponds to a constacyclic shift in $\mathcal{R}^n$ by u.

This gives the following theorem.

THEOREM 2.1. *Cyclic codes over $\mathbb{Z}_4$ of length $N = 2^k n$ correspond to constacyclic codes over $\mathcal{R}$ modulo $X^n - u$ via the map Ψ, i.e., the following diagram commutes, where ϕ_i are the canonical maps between polynomials and codewords.*

$$\begin{array}{ccc}\mathcal{R}[X]/\langle X^n - u\rangle & \xrightarrow[\Psi]{} & \mathbb{Z}_4[X]/\langle X^{2^k n} - 1\rangle\\ \phi_1 \downarrow & & \phi_2 \downarrow\\ \mathcal{R}^n & \xrightarrow[\Psi]{} & (\mathbb{Z}_4)^{2^k n}\end{array}$$

A helpful way to regard a cyclic code over $\mathbb{Z}_4$ is to use its spectral decomposition, obtained via the Discrete Fourier Transform (see Theorem 3.2). This interpretation allows for easier description of these codes as well as their enumeration. To this end, rings of the type given in (7) are needed.

For a positive integer m, we define the following Galois ring:

$$GR(4, m) = \mathbb{Z}_4[X]/\langle h_m(X)\rangle, \tag{6}$$

where $h_m(X)$ is a monic basic irreducible polynomial in $\mathbb{Z}_4[X]$ of degree m that divides $X^{2^m-1}-1$. This ring is local with maximal ideal $\langle 2\rangle$ and residue field $\mathbb{F}_{2^m}$. The polynomial h_m is chosen so that $\xi = X + \langle h(X)\rangle$ is a primitive (2^m-1)st root of unity. The Teichmüller set of representatives is a complete set of coset representatives of the ring modulo 2 and is $\mathcal{T}_m = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^m-2}\}$. Each $z \in GR(4,m)$ has a unique 2-adic expansion $z = z_0 + 2z_1$, with $z_0, z_1 \in \mathcal{T}_m$, and we define $z^f = z_0^2 + 2z_1^2$, where z^f denotes the Frobenius image of z.

Define the ring

$$R_4(u,m) = GR(4,m)[u]/\langle u^{2^k}-1\rangle. \tag{7}$$

(In the latter parts of this paper, the rings $GR(4,m)$ and $R_4(u,m)$ are used in two different ways with slight modifications in the notations – $GR(4,M)$ and $R_4(u,M)$, where M is the order of 2 modulo n, and $GR(4,m_\alpha)$ and $R_4(u,m_\alpha)$, where m_α is the size of the 2-cyclotomic coset modulo n containing α. The notations $GR(4,m)$ and $R_4(u,m)$ are reserved for the general context.)

We begin with a simple observation that proves to be rather useful throughout this paper.

LEMMA 2.2. *In $R_4(u,m)$, we have $(u-1)^{2^k} = 2(u-1)^{2^{k-1}}$.*

Proof. The proof is similar to that for [1] Lemma 1. It is easy to show, by induction, that $(u-1)^{2^e}+1 = u^{2^e} + 2(u-1)^{2^{e-1}}$, for all positive integers e. Setting $e=k$ yields the lemma. ■

LEMMA 2.3. *Let $S = R_4(u,m)$.*

(i) *Every element $z \in S$ is uniquely written as*

$$\begin{aligned} z &= (z_{0,0}+2z_{0,1}) + (z_{1,0}+2z_{1,1})(u-1) + \cdots + (z_{2^k-1,0}+2z_{2^k-1,1})(u-1)^{2^k-1} \\ &= \sum_{i=0}^{2^k-1} (z_{i,0}+2z_{i,1})(u-1)^i, \quad z_{i,j} \in \mathcal{T}_m. \end{aligned} \tag{8}$$

(ii) *An element $z \in S$, written as in* (8)*, is a unit if and only if $z_{0,0} \neq 0$.*

(iii) *S is a local ring with maximal ideal $\langle 2, u-1\rangle$ and residue field $\mathbb{F}_{2^m}$.*

(iv) *The ideals of S are*

- $\langle 0\rangle$,
- $\langle 1\rangle$,
- $\langle 2(u-1)^i\rangle$, *where* $0 \le i \le 2^k-1$,
- $\left\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j (u-1)^j \right\rangle$, *where* $1 \le i \le 2^k-1$ *and* $s_j \in \mathcal{T}_m$ *for all* j,
- $\left\langle 2(u-1)^\ell, (u-1)^i + 2\sum_{j=0}^{\ell-1} s_j (u-1)^j \right\rangle$, *where* $1 \le i \le 2^k-1$, $\ell < i$ *and* $s_j \in \mathcal{T}_m$ *for all* j.

Proof.

(i) This statement is obvious. We choose to expand in $(u-1)$ rather than in u to make what follows clearer and to make the computations easier.

(ii) If $z \in S$ is a unit, then $z \bmod 2$ is clearly a unit in $\mathbb{F}_{2^m}[u]/\langle (u-1)^{2^k} \rangle$, which is equivalent to $z_{0,0} \neq 0$.
Conversely, for an element $z = x + 2y \in S$, suppose $z \bmod 2$ is a unit in $\mathbb{F}_{2^m}[u]/\langle (u-1)^{2^k} \rangle$. Then there exists $x' \in S$ such that $x'x \equiv 1 \bmod 2$, i.e., $x'x = 1 + 2\mu$, for some $\mu \in S$. Then

$$\begin{aligned}(x+2y)(x'+2(-\mu-x'y)x') &= xx' + 2(yx' + xx'(-\mu - x'y)) \\ &= 1 + 2(yx' - \mu - x'y + \mu) = 1,\end{aligned}$$

so $x' + 2(-\mu - x'y)x'$ is an inverse of z, i.e., z is a unit in S.

(iii) We have that $S/\langle 2, u-1 \rangle \cong \mathbb{F}_{2^m}$ a field, so $\langle 2, u-1 \rangle$ is maximal. To show this ideal is the unique maximal ideal, we shall show that any element not in the ideal $\langle 2, u-1 \rangle$ is a unit.
If $z = \sum_{i=0}^{2^k-1} (z_{i,0} + 2z_{i,1})(u-1)^i \notin \langle 2, u-1 \rangle$, then $z_{0,0} \neq 0$ and therefore z is a unit by (ii).

(iv) We have the trivial ideals $\langle 0 \rangle$ and $S = \langle 1 \rangle$.
Let I be an ideal of S, distinct from $\langle 0 \rangle$ and $\langle 1 \rangle$.
If $I \subseteq \langle 2 \rangle$, any element in I can be written in the form:

$$2s_0 + 2s_1(u-1) + \cdots + 2s_{2^k-1}(u-1)^{2^k-1}, \qquad \text{where } s_j \in \mathcal{T}_m.$$

Let $s \in I$ be an element with the smallest i with $s_i \neq 0$. For all $t \in I$, $t = 2(u-1)^i(t_i + t_{i+1}(u-1) + \ldots t_{2^k-1}(u-1)^{2^k-1-i})$, where $t_j \in \mathcal{T}_m$. Therefore, $I \subseteq \langle 2(u-1)^i \rangle$.

Since $s = 2(u-1)^i(s_i + s_{i+1}(u-1) + \ldots s_{2^k-1}(u-1)^{2^k-1-i})$, where $s_j \in \mathcal{T}_m$ and $s_i \neq 0$, this means that $(s_i + s_{i+1}(u-1) + \ldots s_{2^k-1}(u-1)^{2^k-1-i})$ is invertible and hence $2(u-1)^i \in I$, which implies $I = \langle 2(u-1)^i \rangle$. Hence all ideals contained in $\langle 2 \rangle$ are of the form $\langle 2(u-1)^i \rangle$, $0 \leq i \leq 2^k - 1$.

Now assume I is not contained in $\langle 2 \rangle$. Let $\overline{I} = \{v \mid v \equiv w \bmod 2, w \in I\}$. Then $\overline{I}$ is an ideal in $\mathbb{F}_{2^m}[u]/\langle (u-1)^{2^k} \rangle$. Since I is not contained in $\langle 2 \rangle$, $\overline{I}$ is not the zero ideal $\langle 0 \rangle$.

The nonzero ideals in $\mathbb{F}_{2^m}[u]/\langle (u-1)^{2^k} \rangle$, distinct from $\langle 1 \rangle$, are of the form $\langle (u-1)^i \rangle$, $1 \leq i \leq 2^k - 1$. Therefore $\overline{I} = \langle (u-1)^i \rangle$ with $1 \leq i \leq 2^k - 1$. Hence there exists an element $(u-1)^i + 2s \in I$, for some $s \in S$. Without any loss of generality, we may write

$$(u-1)^i + 2s = (u-1)^i + 2\sum_{j=0}^{2^k-1} s_j(u-1)^j, \qquad \text{where } s_j \in \mathcal{T}_m.$$

Since $2(u-1)^i = 2((u-1)^i + 2s) \in I$, it follows that $2s_j(u-1)^j \in I$ for all $i \le j \le 2^k - 1$. Therefore

$$(u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \in I.$$

Now we divide into two subcases.
Subcase I:

$$I = \left\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \right\rangle.$$

This is the fourth type of ideals in the list of Lemma 2.3(iv).
Subcase II:

$$\left\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \right\rangle \subset I.$$

Let $g = (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j$. Let $r \in I \setminus \left\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \right\rangle$. There exists r' such that, expressing elements of S in the form of (8), $z := r - r'g \in I$ can be written as

$$z = (z_{0,0} + 2z_{0,1}) + (z_{1,0} + 2z_{1,1})(u-1) + \cdots + (z_{i-1,0} + 2z_{i-1,1})(u-1)^{i-1}.$$

Denoting the image of z in $\mathbb{F}_{2^m}[u]/\langle (u-1)^{2^k} \rangle$ by $\bar{z}$, we have $\bar{z} \in \langle (u-1)^i \rangle$, so

$$z_{0,0} = z_{1,0} = \cdots = z_{i-1,0} = 0.$$

Thus we have

$$z = 2(u-1)^\lambda (z_{\lambda,1} + z_{\lambda+1,1}(u-1) + \cdots + z_{i-1,1}(u-1)^{i-1-\lambda}) \quad \text{with } z_{\lambda,1} \neq 0 \tag{9}$$

for some $\lambda < i$. Since $z_{\lambda,1} \neq 0$, (ii) shows that $z_{\lambda,1} + z_{\lambda+1,1}(u-1) + \cdots + z_{i-1,1}(u-1)^{i-1-\lambda}$ is a unit. Consequently, $2(u-1)^\lambda \in I$. For each $r \in I \setminus \left\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \right\rangle$, we obtain such a λ. Let ℓ be the smallest of these λ. Then

$$\left\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j, 2(u-1)^\ell \right\rangle \subseteq I.$$

By (9) and the definition of ℓ, for every $r \in I$, there exists some $r' \in I$ such that $r - r'g \in \langle 2(u-1)^\ell \rangle$ (when $r \in \left\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \right\rangle$, there exists r' such that $r - r'g = 0 \in \langle 2(u-1)^\ell \rangle$), so

$$r \in \left\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j, 2(u-1)^\ell \right\rangle.$$

Therefore,

$$I = \left\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j (u-1)^j, 2(u-1)^\ell \right\rangle.$$

Since $2(u-1)^\ell \in I$, it follows that, for $\ell \le j \le i-1$, we have $2s_j(u-1)^j \in I$. Therefore, it follows that:

$$I = \left\langle (u-1)^i + 2\sum_{j=0}^{\ell-1} s_j (u-1)^j, 2(u-1)^\ell \right\rangle. \qquad \blacksquare$$

As a corollary to Lemma 2.3, when $k=1$, we get the ideals as given in [2], Lemma 1. If $m=n=1$, then $S=\mathbb{Z}_4[X]/\langle X^{2^k}-1\rangle$ and we get the ideals given in [1]. If N is odd then $N=2^0 n$, i.e. $N=n$ and $k=0$. The ring $\mathcal{R}$ is then $\mathbb{Z}_4[u]/\langle u-1\rangle = \mathbb{Z}_4$ and $\mathcal{R}[X]/\langle X^n-u\rangle$ is isomorphic to $\mathbb{Z}_4[X]/\langle X^n-1\rangle$. Now X^n-1 factors uniquely, since n is odd, over $\mathbb{Z}_4$ into a product $\prod_{i=0}^{|J|-1} f_i = X^n-1$ of basic irreducible polynomials, where J denotes a complete set of representatives of the 2-cyclotomic cosets modulo n. Since $u=1$, the only ideals in $R_4(1,m)=GR(4,m)$ are $\langle 0\rangle$, $\langle 1\rangle$ and $\langle 2\rangle$. This is Lemma 3 in [7].

We also note that an ideal of the type $\left\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j (u-1)^j \right\rangle$, where $0 \le i \le 2^k - 1$ and $s_j \in \mathcal{T}_m$ for all j, can be written in the form $\left\langle (u-1)^i + 2(u-1)^t h(u) \right\rangle$, where $0 \le t \le i-1$ and $h(u)$ is either 0 or a unit. Furthermore, we may write $h(u) = \sum_j h_j (u-1)^j$, where $h_j \in \mathcal{T}_m$ for all j. In particular, when $h(u)$ is a unit, then one of the following must hold:

(i) $h(u)=1$;

(ii) $h(u) = 1 + (u-1)^\tau \tilde{h}(u)$, where $\tau \ge 1$ and $\tilde{h}(u)$ is a unit;

(iii) $h(u) = \sum_{j=0}^{i-t-1} h_j (u-1)^j$, with $h_0 \in \mathcal{T}_m \setminus \{0, 1\}$.

Suppose that T is the smallest integer such that $2(u-1)^T \in \left\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j (u-1)^j \right\rangle$. For an ideal of the type $\left\langle 2(u-1)^\ell, (u-1)^i + 2\sum_{j=0}^{i-1} s_j (u-1)^j \right\rangle$, we may assume, without loss of generality, that $\ell < T$. Otherwise, this ideal is actually $\left\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j (u-1)^j \right\rangle$.

Notice that ideals in the ring S may be viewed equivalently as cyclic codes of length 2^k over $GR(4,m)$. Hence, they have residue and torsion codes as given in (1) and (2).

LEMMA 2.4. *Let C be an ideal in S (or equivalently, a cyclic code of length 2^k over $GR(4,m)$). Then we have that* $|\mathrm{Res}(C)||\mathrm{Tor}(C)| = |C|$.

Proof. Consider the (clearly surjective) reduction mod 2 map $C \to \mathrm{Res}(C)$. The kernel of this map is $\{\mathbf{c} \in C \mid \mathbf{c} = 2\mathbf{v} \text{ for some } \mathbf{v}\}$. By identifying $\mathbb{F}_{2^m}$ with the Teichmüller set $\mathcal{T}_m$ in $GR(4,m)$, it follows that there is a natural bijection

between this kernel and $\mathrm{Tor}(C)$. Hence, by the First Isomorphism Theorem of finite groups, we have $|\mathrm{Tor}(C)| = |C|/|\mathrm{Res}(C)|$. ■

PROPOSITION 2.5. *For the ideals in S, the corresponding residue and torsion codes are given as follows:*

(i) *If* $C = \langle 0 \rangle$, *then* $\mathrm{Res}(C) = \langle 0 \rangle$ *and* $\mathrm{Tor}(C) = \langle 0 \rangle$.

(ii) *If* $C = \langle 1 \rangle$, *then* $\mathrm{Res}(C) = \langle 1 \rangle$ *and* $\mathrm{Tor}(C) = \langle 1 \rangle$.

(iii) *If* $C = \langle 2(u-1)^i \rangle$ $(0 \le i \le 2^k - 1)$, *then* $\mathrm{Res}(C) = \langle 0 \rangle$ *and* $\mathrm{Tor}(C) = \langle (u-1)^i \rangle$.

(iv) *If* $C = \langle (u-1)^i + 2(u-1)^t h(u) \rangle$ $(1 \le i \le 2^k - 1,\ 0 \le t \le i-1)$, *then* $\mathrm{Res}(C) = \langle (u-1)^i \rangle$ *and* $\mathrm{Tor}(C) = \langle (u-1)^T \rangle$, *where*

$$T = \begin{cases} \min\{2^{k-1}, i\} & \text{if } h(u) = 0, \\ i & \text{if } h(u) = 1 \quad \text{and} \quad 2^{k-1} - i + t = 0, \\ \min\{i, 2^{k-1} + \tau\} & \text{if } h(u) = 1 + (u-1)^\tau \tilde{h}(u) \quad \text{and} \quad 2^{k-1} - i + t = 0, \\ 2^{k-1} & \text{if } h(u) = \sum_j h_j (u-1)^j \text{ with } h_0 \ne 0, 1 \\ & \text{and} \quad 2^{k-1} - i + t = 0, \\ \min\{2^{k-1}, i, 2^k - i + t\} & \text{if } 2^{k-1} - i + t \ne 0 \quad \text{and} \quad h(u) \ne 0. \end{cases}$$

(v) *If* $C = \langle 2(u-1)^\ell, (u-1)^i + 2(u-1)^t h(u) \rangle$, *where* $\ell < T$ *with* T *as in* (iv), *then* $\mathrm{Res}(C) = \langle (u-1)^i \rangle$ *and* $\mathrm{Tor}(C) = \langle (u-1)^\ell \rangle$.

Proof. The statements on the residue codes are obvious, and so are the statements on the torsion codes in (i)–(iii).

(iv) Let $\mathrm{Tor}(C) = \langle (u-1)^T \rangle$, so T is the smallest integer such that $2(u-1)^T \in C$.

Note first that $2(u-1)^i = 2\left((u-1)^i + 2(u-1)^t h(u)\right) \in C$, so

$$T \le i. \tag{10}$$

By definition of T, there exists

$$g(u) = \sum_{j=0}^{2^k-1} g_j (u-1)^j + 2 \sum_{j=0}^{2^k-1} g'_j (u-1)^j \tag{11}$$

so that

$$2(u-1)^T = ((u-1)^i + 2(u-1)^t h(u)) g(u). \tag{12}$$

Reducing (12) modulo 2 and using (11), it follows that $g_j = 0$ for $0 \le j \le 2^k - i - 1$. Hence, by Lemma 2.2,

$$2(u-1)^T = 2(u-1)^{2^{k-1}} \sum_{j=0}^{i-1} g_{j+2^k-i}(u-1)^j + 2(u-1)^i \sum_{j=0}^{2^k-i-1} g'_j (u-1)^j$$
$$+ 2(u-1)^{2^k-i+t} h(u) \sum_{j=0}^{i-1} g_{j+2^k-i}(u-1)^j. \tag{13}$$

In particular, noting that $i \geq 2^{k-1}$ when $2^{k-1} - i + t = 0$, we have

$$T \geq \begin{cases} \min\{2^{k-1}, i\} & \text{if } h(u) = 0, \\ i & \text{if } h(u) = 1 \quad \text{and} \quad 2^{k-1} - i + t = 0, \\ \min\{i, 2^{k-1} + \tau\} & \text{if } h(u) = 1 + (u-1)^\tau \tilde{h}(u) \text{ and } 2^{k-1} - i + t = 0, \\ 2^{k-1} & \text{if } h(u) = \sum_j h_j (u-1)^j \text{ with } h_0 \neq 0, 1 \\ & \quad \text{and} \quad 2^{k-1} - i + t = 0, \\ \min\{2^{k-1}, i, 2^k - i + t\} & \text{if } 2^{k-1} - i + t \neq 0 \quad \text{and} \quad h(u) \neq 0. \end{cases} \tag{14}$$

If $h(u) = 0$, then in fact $C = \langle (u-1)^i \rangle$ and $2(u-1)^{2^{k-1}} = (u-1)^{2^k} \in C$, so $T \leq 2^{k-1}$. Together with (10) and (14), we obtain $T = \min\{2^{k-1}, i\}$.

If $h(u) = 1$ and $2^{k-1} - i + t = 0$, (10) and (14) immediately yield $T = i$.

If $h(u) = 1 + (u-1)^\tau \tilde{h}(u)$ and $2^{k-1} - i + t = 0$, we have

$$\left((u-1)^i + 2(u-1)^t h(u) \right) (u-1)^{2^k - i} = 2(u-1)^{2^{k-1} + \tau} \tilde{h}(u).$$

Since $\tilde{h}(u)$ is a unit, it follows that $2(u-1)^{2^{k-1}+\tau} \in C$, so $T \leq 2^{k-1} + \tau$. Therefore, $T = \min\{i, 2^{k-1} + \tau\}$ follows from (10) and (14).

If $h(u) = \sum_j h_j (u-1)^j$ with $h_0 \neq 0, 1$ and $2^{k-1} - i + t = 0$, we have

$$\left((u-1)^i + 2(u-1)^t h(u) \right) (u-1)^{2^k - i} = 2(u-1)^{2^{k-1}} (1 + h(u)).$$

Note that the constant term of $1 + h(u)$ is $1 + h_0$, which is a unit. Hence, $2(u-1)^{2^{k-1}} \in C$, i.e., $T \leq 2^{k-1}$. Together with (14), we obtain $T = 2^{k-1}$.

Finally, assume $2^{k-1} - i + t \neq 0$ and $h(u) \neq 0$ (and is hence a unit). We have

$$\left((u-1)^i + 2(u-1)^t h(u) \right) (u-1)^{2^k - i} = 2(u-1)^{2^{k-1}} + 2(u-1)^{2^k - i + t} h(u),$$

so $2(u-1)^{\min\{2^{k-1}, 2^k - i + t\}} \in C$. Therefore, $T \leq \min\{2^{k-1}, 2^k - i + t\}$. Using (10) and (14) again, we obtain $T = \min\{2^{k-1}, i, 2^k - i + t\}$.

(v) Since $\ell < T$, with T as in (iv), it is clear that $\mathrm{Tor}(C) = \langle (u-1)^\ell \rangle$. ■

Remark 1.

(i) As remarked earlier, in Proposition 2.5(v), if $\ell \geq T$, then we have $C = \langle 2(u-1)^\ell, (u-1)^i + 2(u-1)^t h(u) \rangle = \langle (u-1)^i + 2(u-1)^t h(u) \rangle$, so it is covered by (iv).

(ii) In Proposition 2.5(iv), we may assume without loss of generality that $t + \deg(h) < T$, i.e., $\deg(h) \leq T - t - 1$. Similarly, in Proposition 2.5(v), we may assume that $\deg(h) \leq \ell - t - 1$.

(iii) For Proposition 2.5(iv), it is not difficult to see that the possible values of T are given as follows:

- for $1 \le i \le 2^{k-1}$, we have $T = i$;
- for $2^{k-1} < i < 2^{k-1} + t$ $(t > 0)$, we have $T = 2^{k-1}$;
- for $i = 2^{k-1} + t$ $(t > 0)$, we have $2^{k-1} \le T \le 2^{k-1} + t = i$;
- for $i > 2^{k-1} + t$, we have $T = 2^{k-1}$ or $2^k - i + t$.

THEOREM 2.6. *The number of distinct ideals in* $S = R_4(u, m)$ *is*

$$5 + (2^m)^{2^{k-1}} + (5 \cdot 2^m - 1)(2^m)\frac{(2^m)^{2^{k-1}-1} - 1}{(2^m - 1)^2} - 4 \cdot \frac{2^{k-1} - 1}{2^m - 1}.$$

Proof. We shall count the number of distinct ideals of each type in Proposition 2.5.

Clearly, $\langle 0 \rangle$ and $\langle 1 \rangle$ account for two distinct ideals.

There are obviously 2^k distinct ideals of the type $\langle 2(u-1)^i \rangle$.

To count the number of distinct ideals of the type $\langle (u-1)^i + 2(u-1)^t h(u) \rangle$, with $1 \le i \le 2^k - 1$, we further divide into subcases.

If $h(u) = 0$, then the ideals are of the form $\langle (u-1)^i \rangle$ with $1 \le i \le 2^k - 1$. There are $2^k - 1$ ideals of this form.

If $h(u) = 1$ and $2^{k-1} - i + t = 0$, then the ideals are of the form $\langle (u-1)^i + 2(u-1)^{i-2^{k-1}} \rangle$, with $2^{k-1} \le i \le 2^k - 1$. Hence, there are 2^{k-1} ideals of this kind.

Next consider the case where $h(u) = 1 + (u-1)^\tau \tilde{h}(u)$ (where $\tilde{h}(u)$ is a unit) and $2^{k-1} - i + t = 0$. In this case, we have $2^{k-1} \le i \le 2^k - 1$. Clearly, in order for the ideals to be distinct, we should also have $t + \tau < i$, so $1 \le \tau \le 2^{k-1} - 1$. Writing $\tilde{h}(u) = \sum_j \tilde{h}_j (u-1)^j$, it is easy to see that the fact that $\tilde{h}(u)$ is a unit implies $\tilde{h}_0 \ne 0$, while, in order for the ideals to be distinct, we should also assume $t + \tau + j \le T - 1$, with T as in Proposition 2.5(iv). In other words, $j \le 2^{k-1} - i + T - \tau - 1$. Hence, the number of ideals of this form is given by

$$\sum_{i=2^{k-1}}^{2^k-1} \left\{ \sum_{\tau=1}^{i-2^{k-1}} (2^m)^{2^k-i-1}(2^m - 1) + \sum_{\tau=i-2^{k-1}+1}^{2^{k-1}-1} (2^m)^{2^{k-1}-\tau-1}(2^m - 1) \right\}$$
$$= 2(2^m - 1)\left\{ \frac{(2^m)^{2^{k-1}} - 1}{(2^m - 1)^2} - \frac{2^{k-1}}{2^m - 1} \right\}.$$

Now let $h(u) = \sum_j h_j (u-1)^j$ be a unit such that $h_0 \ne 0, 1$, and suppose $2^{k-1} - i + t = 0$. Once again, we have $2^{k-1} \le i \le 2^k - 1$. In order not to double count any of the ideals, we need $j + i - 2^{k-1} < T = 2^{k-1}$, i.e., $j < 2^k - i$. Hence, noting that $h_0 \ne 0, 1$, the number of distinct ideals of this form is given by

$$\sum_{i=2^{k-1}}^{2^k-1} (2^m)^{2^k-i-1}(2^m - 2) = (2^m - 2)\frac{(2^m)^{2^{k-1}} - 1}{2^m - 1}.$$

If $2^{k-1}+t\neq i$ and $h(u)\neq 0$, recall that $T=\min\{2^{k-1}, i, 2^k-i+t\}$. In order to account only for distinct ideals, we need $j+t<T$, i.e., $0\leq j\leq T-t-1$. Consequently, the number of distinct ideals of this kind is

$$\sum_{i=1}^{2^{k-1}-1}\sum_{t=0}^{i-1}(2^m)^{i-t-1}(2^m-1)+\sum_{i=2^{k-1}}^{2^k-1}\left\{\sum_{t=0}^{i-2^{k-1}-1}(2^m)^{2^k-i-1}(2^m-1)\right.$$
$$\left.+\sum_{t=i-2^{k-1}+1}^{2^{k-1}-1}(2^m)^{2^{k-1}-t-1}(2^m-1)\right\}=3\left\{\frac{(2^m)^{2^{k-1}}-1}{2^m-1}-2^{k-1}\right\}.$$

Therefore, the number of distinct ideals of the type $\langle (u-1)^i+2(u-1)^t h(u)\rangle$, with $1\leq i\leq 2^k-1$, is

$$2^k-1+2^{k-1}+2(2^m-1)\left\{\frac{(2^m)^{2^{k-1}}-1}{(2^m-1)^2}-\frac{2^{k-1}}{2^m-1}\right\}+(2^m-2)\frac{(2^m)^{2^{k-1}}-1}{2^m-1}$$
$$+3\left\{\frac{(2^m)^{2^{k-1}}-1}{2^m-1}-2^{k-1}\right\}$$
$$=4\cdot\frac{(2^m)^{2^{k-1}}-1}{2^m-1}+(2^m)^{2^{k-1}}-2^k-2.$$

Finally, we consider ideals of the type $\langle 2(u-1)^\ell, (u-1)^i+2(u-1)^t h(u)\rangle$, which are not of the type $\langle (u-1)^i+2(u-1)^t h(u)\rangle$ (i.e., not principal). This condition means that $\ell<T$, where T is as in Proposition 2.5(iv). Once again, we divide into several subcases.

When $h(u)=0$, the ideals are of the form $\langle 2(u-1)^\ell, (u-1)^i\rangle$ with $0\leq\ell<T=\min\{2^{k-1}, i\}$. Hence, the number of distinct ideals of this kind is

$$\sum_{i=1}^{2^{k-1}} i+\sum_{i=2^{k-1}+1}^{2^k-1}2^{k-1}=\frac{(2^{k-1}-1)2^{k-1}}{2}+2^{2(k-1)}.$$

If $h(u)\neq 0$, then we need to assume $t<\ell$. Indeed, if $\ell\leq t$, then by subtracting a suitable multiple of $2(u-1)^\ell$ from $(u-1)^i+2(u-1)^t h(u)$, we see that such an ideal is also of the form $\langle 2(u-1)^\ell, (u-1)^i\rangle$, which has already been accounted for above.

If $h(u)=1$ and $2^{k-1}-i+t=0$, we have $i\geq 2^{k-1}$ and $T=i$, it follows that the number of distinct ideals of this type is

$$\sum_{i=2^{k-1}}^{2^k-1}(T-t-1)=\sum_{i=2^{k-1}}^{2^k-1}\left(2^{k-1}-1\right)=2^{k-1}(2^{k-1}-1).$$

Next consider the case where $h(u)=1+(u-1)^\tau\tilde{h}(u)$ and $2^{k-1}-i+t=0$. Note that, if $t+\tau\geq\ell$, then, by subtracting a suitable multiple of $2(u-1)^\ell$ from $(u-1)^i+2(u-1)^t h(u)$, we see that the ideal $\langle 2(u-1)^\ell, (u-1)^i+2(u-1)^t h(u)\rangle$ is also of the form $\langle 2(u-1)^\ell, (u-1)^i+2(u-1)^t\rangle$, which is already accounted

for in the previous case. Hence, we assume further that $t+\tau<\ell$, i.e., $i-2^{k-1}<\ell<T$. In order not to double count any ideal, writing $\tilde{h}_j(u)=\sum_j \tilde{h}_j(u-1)^j$, we need $t+\tau+j<\ell$, i.e., $0\le j\le \ell-\tau-i+2^{k-1}-1$. The total number of distinct ideals of this kind is then given by

$$\sum_{i=2^{k-1}}^{2^k-1}\left\{\sum_{\tau=1}^{i-2^{k-1}}\sum_{\ell=i-2^{k-1}+\tau+1}^{2^{k-1}+\tau-1}(2^m-1)(2^m)^{\ell-1-\tau-i+2^{k-1}}+\sum_{\tau=i-2^{k-1}+1}^{2^{k-1}-1}\sum_{\ell=i-2^{k-1}+\tau+1}^{i-1}(2^m-1)(2^m)^{\ell-1-\tau-i+2^{k-1}}\right\}$$
$$=2\left\{\frac{(2^m)^{2^{k-1}}-1}{(2^m-1)^2}-\frac{2^{k-1}}{2^m-1}\right\}-2^{k-1}(2^{k-1}-1).$$

Next, let $h(u)=\sum_j h_j(u-1)^j$ be a unit such that $h_0\neq 0,1$, and suppose $2^{k-1}-i+t=0$. Once again, we have $2^{k-1}\le i\le 2^k-1$. If we write $h(u)=\sum_j h_j(u-1)^j$, in order not to double count any ideal of this type, we need $t+j\le \ell-1$, i.e., $0\le j\le \ell-i+2^{k-1}-1$. Hence, the number of distinct ideals of this type is given by

$$\sum_{i=2^{k-1}}^{2^k-1}\sum_{\ell=i-2^{k-1}+1}^{2^{k-1}-1}(2^m-2)(2^m)^{\ell-i+2^{k-1}-1}=(2^m-2)\left\{\frac{(2^m)^{2^{k-1}}-1}{(2^m-1)^2}-\frac{2^{k-1}}{2^m-1}\right\}.$$

Finally, assume that $i\neq t+2^{k-1}$ and $h(u)\neq 0$. In order to avoid double counting, with $h(u)=\sum_j h_j(u-1)^j$, we need $t+j\le \ell-1$, i.e., $0\le j\le \ell-t-1$. Hence, the total number of ideals of this kind is

$$\sum_{i=1}^{2^{k-1}-1}\sum_{t=0}^{i-1}\left((2^m)^{i-t-1}-1\right)+\sum_{i=2^{k-1}}^{2^k-1}\left\{\sum_{t=0}^{i-2^{k-1}-1}\left((2^m)^{2^k-i-1}-1\right)+\sum_{t=i-2^{k-1}+1}^{2^{k-1}-1}\left((2^m)^{2^{k-1}-t-1}-1\right)\right\}$$
$$=3\left\{\frac{(2^m)^{2^{k-1}}-1}{(2^m-1)^2}-\frac{2^{k-1}}{2^m-1}-\frac{(2^{k-1}-1)2^{k-1}}{2}\right\}.$$

Therefore, the number of distinct ideals of the type $\langle 2(u-1)^\ell,(u-1)^i+2(u-1)^t h(u)\rangle$, which are not of the type $\langle (u-1)^i+2(u-1)^t h(u)\rangle$ (i.e., not principal), is

given by

$$\frac{(2^{k-1}-1)2^{k-1}}{2}+2^{2(k-1)}+2^{k-1}(2^{k-1}-1)+2\left\{\frac{(2^m)^{2^{k-1}}-1}{(2^m-1)^2}-\frac{2^{k-1}}{2^m-1}\right\}$$
$$-2^{k-1}(2^{k-1}-1)+(2^m-2)\left\{\frac{(2^m)^{2^{k-1}}-1}{(2^m-1)^2}-\frac{2^{k-1}}{2^m-1}\right\}$$
$$+3\left\{\frac{(2^m)^{2^{k-1}}-1}{(2^m-1)^2}-\frac{2^{k-1}}{2^m-1}-\frac{(2^{k-1}-1)2^{k-1}}{2}\right\}$$
$$=(2^m+3)\left\{\frac{(2^m)^{2^{k-1}}-1}{(2^m-1)^2}-\frac{2^{k-1}}{2^m-1}\right\}+2^{k-1}.$$

The total number of ideals in $S=R_4(u,m)$ now follows by summing the number of ideals for each type. ■

3. Discrete Fourier Transform

Let M be the order of 2 modulo n and let ζ denote a primitive nth root of unity in $GR(4,M)$.

Definition 1. Let $\mathbf{c}=(c_{0,0}, c_{1,0},\ldots,c_{n-1,0}, c_{0,1}, c_{1,1},\ldots,c_{0,2^k-1}, c_{1,2^k-1},\ldots, c_{n-1,2^k-1}) \in (\mathbb{Z}_4)^{2^k n}$, with $c(X)=\sum_{i=0}^{n-1}\sum_{j=0}^{2^k-1} c_{i,j}X^{i+jn}$ the corresponding polynomial. The Discrete Fourier Transform of $c(X)$ is the vector

$$(\widehat{c}_0,\widehat{c}_1,\ldots,\widehat{c}_{n-1})\in R_4(u,M)^n$$

with

$$\widehat{c}_h=c(u^{n'}\zeta^h)=\sum_{i=0}^{n-1}\sum_{j=0}^{2^k-1} c_{i,j}u^{n'i+j}\zeta^{hi} \tag{15}$$

for $0\le h<n$, where $nn'\equiv 1 \bmod 2^k$.

Define the Mattson–Solomon polynomial of c to be

$$\widehat{c}(Z)=\sum_{h=0}^{n-1}\widehat{c}_{n-h}Z^h. \tag{16}$$

(Here, we have identified $\widehat{c}_0$ with $\widehat{c}_n$.)

LEMMA 3.1 (Inversion formula). *Let $\mathbf{c}\in(\mathbb{Z}_4)^{2^k n}$ with $\widehat{c}(Z)$ its Mattson–Solomon polynomial as defined above. Then*

$$\mathbf{c}=\Psi[(1,u^{-n'},u^{-2n'},\ldots,u^{-(n-1)n'})*\frac{1}{n}(\widehat{c}(1),\widehat{c}(\zeta),\ldots,\widehat{c}(\zeta^{n-1}))], \tag{17}$$

where $*$ indicates componentwise multiplication.

Proof. Let $0 \le t \le n-1$. Then

$$\begin{aligned}
\widehat{c}(\zeta^t) &= \sum_{h=0}^{n-1} \widehat{c}_h \zeta^{-ht} \\
&= \sum_{h=0}^{n-1} \Big(\sum_{i=0}^{n-1} \sum_{j=0}^{2^k-1} c_{i,j} u^{n'i+j} \zeta^{hi} \Big) \zeta^{-ht} \\
&= \sum_{i=0}^{n-1} \sum_{j=0}^{2^k-1} c_{i,j} u^{n'i+j} \sum_{h=0}^{n-1} \zeta^{h(i-t)} \\
&= (nu^{n't}) \sum_{j=0}^{2^k-1} c_{t,j} u^j .
\end{aligned}$$

The rest follows from a straightforward computation from the definition of the map Ψ. ∎

Let J denote a complete set of representatives of the 2-cyclotomic cosets modulo n and, for each $\alpha \in J$, let m_α denote the size of the 2-cyclotomic coset containing α.

The following theorem is proved in [2] in a less general form but the proof is the same. This theorem allows us to describe cyclic codes which are ideals in $\mathbb{Z}_4[X]/\langle X^{2^k n} - 1 \rangle$ in terms of ideals of $R_4(u, m_\alpha)$ which we have previously described.

THEOREM 3.2. *The map* $\gamma : \mathbb{Z}_4[X]/\langle X^{2^k n} - 1 \rangle \to \oplus_{\alpha \in J} R_4(u, m_\alpha)$ *is a ring isomorphism, where* $\gamma(c(X)) = [\widehat{c}_\alpha]_{\alpha \in J}$ *for* $c(X) \in \mathbb{Z}_4[X]/\langle X^{2^k n} - 1 \rangle$.

Since a cyclic code of length $2^k n$ over $\mathbb{Z}_4$ can be regarded as an ideal in $\mathbb{Z}_4[X]/\langle X^{2^k n} - 1 \rangle$, we have the following corollary.

COROLLARY 3.3. *If C is a cyclic code of length $2^k n$ over $\mathbb{Z}_4$, then C is isomorphic to $\oplus_{\alpha \in J} C_\alpha$, where, for each $\alpha \in J$, C_α is an ideal in $R_4(u, m_\alpha)$.*

For every $\alpha \in J$, let N_α denote the number of distinct ideals in $R_4(u, m_\alpha)$, as given in Theorem 2.6. Then, the following enumeration result follows immediately from Theorem 3.2.

COROLLARY 3.4. *The number of distinct cyclic codes over $\mathbb{Z}_4$ of length $N = 2^k n$ (n odd) is $\prod_{\alpha \in J} N_\alpha$.*

If $N = 2^k$, then $J = \{0\}$. In this case $m_0 = 1$, then the number of cyclic codes of length 2^k is $5 + 2^{2^{k-1}} + (9)(2)(2^{2^{k-1}-1} - 1) - 4(2^{k-1} - 1) = 10 \cdot 2^{2^{k-1}} - 4 \cdot 2^{k-1} - 9$.

When $k = 1$, then the number of ideals in $R_4(u, m_\alpha)$ is $5 + 2^{m_\alpha}$. Hence the number of cyclic codes of length $2n$ is $\prod_{\alpha \in J} (5 + 2^{m_\alpha})$ (cf. [2, Corollary 1]).

EXAMPLE 3.1. (i) Consider cyclic codes of length 16 over $\mathbb{Z}_4$. Here, $k=4$ and $n=1$, so J is $\{0\}$. From Theorem 2.6, it follows that there are 2519 cyclic codes of length 16 over $\mathbb{Z}_4$.

(ii) Consider cyclic codes of length 28 over $\mathbb{Z}_4$. Here, $k=2$ and $n=7$, so J can be taken to be $\{0, 1, 6\}$. From Theorem 2.6, it is easy to check that $N_0=23$ and $N_1=N_6=113$, so there are $23\cdot 113\cdot 113=293687$ cyclic codes of length 28 over $\mathbb{Z}_4$.

4. Polynomial Representation

Recall that ζ is a primitive nth root of unity in $GR(4, M)$. Since n is odd, the polynomial $X^n-1\in\mathbb{Z}_4[X]$ factors uniquely into the product of $|J|$ monic basic irreducible polynomials. For each $0\le\alpha\le n-1$, ζ^α is the root of exactly one such polynomial — we shall call this polynomial the minimal polynomial of ζ^α. (If α and β belong to the same 2-cyclotomic coset modulo n, then ζ^α and ζ^β share the same minimal polynomial.) Note that $f_\alpha(u^{n'}\zeta^\alpha)\in GR(4, M)[u]/\langle u^{2^k}-1\rangle = R_4(u, M)$.

LEMMA 4.1. *Let f_α be the minimal polynomial of ζ^α in $\mathbb{Z}_4[X]$ and let n' be as defined before. Then*

(i) $f_\alpha(u^{n'}\zeta^\alpha)\not\equiv 0 \bmod 2$.

(ii) $f_\alpha(u^{n'}\zeta^\alpha)\equiv 0 \bmod \langle(u-1)\rangle$ *and* $f_\alpha(u^{n'}\zeta^\alpha)\not\equiv 0 \bmod \langle(u-1)^2\rangle$.

(iii) $f_\alpha((u^{n'}\zeta^\alpha)^{2^k})=0$.

(iv) *If $g(X)\in\mathbb{Z}_4[X]$ is a monic polynomial such that $g=f_\alpha^i+2e$, where $\deg(e)<\deg(f_\alpha^i)$, then $g(u^{n'}\zeta^\alpha)\equiv 0 \bmod \left\langle(u-1)^i+2\sum_{j=0}^{i-1}s_j(u-1)^j\right\rangle$ for some ideal $\left\langle(u-1)^i+2\sum_{j=0}^{i-1}s_j(u-1)^j\right\rangle$.*

(v) *For $0\le\beta\le n-1$, if $f_\alpha\ne f_\beta$, then $f_\alpha(u^{n'}\zeta^\beta)$ is a unit.*

Proof. (i) Write $f_\alpha(X)=\sum_{j=0}^{2^k-1}X^j f_{\alpha,j}(X)$, where each $f_{\alpha,j}(X)$ is a polynomial such that the exponents of all its terms are congruent to 0 mod 2^k. Hence, the exponents in $X^j f_{\alpha,j}(X)$ are congruent to j mod 2^k. Observe that, since $f_\alpha(X)$ is not a constant polynomial, we cannot have $f_\alpha(X)=f_{\alpha,0}(X)$, for otherwise, this polynomial becomes reducible modulo 2. Then

$$f_\alpha(u^{n'}\zeta^\alpha)=f_{\alpha,0}(\zeta^\alpha)+\sum_{j=1}^{2^k-1}u^{n'j}\zeta^{j\alpha}f_{\alpha,j}(\zeta^\alpha).$$

If $f_\alpha(u^{n'}\zeta^\alpha)\equiv 0 \bmod 2$, by comparing the terms without u, it follows that $f_{\alpha,0}(X)$ is a polynomial with ζ^α as a solution. Reducing modulo 2, we have $f_{\alpha,0}(X)\equiv g_{\alpha,0}(X)^{2^k} \bmod 2$, for some $g_{\alpha,0}(X)$ whose degree is strictly less than

$\deg(f_\alpha)$. It follows that $g_{\alpha,0}(X)$ has ζ^α as a root, which is a contradiction. Therefore, $f_\alpha(u^{n'}\zeta^\alpha) \not\equiv 0 \bmod 2$.

(ii) Since $f_\alpha(u^{n'}\zeta^\alpha) \equiv f_\alpha(\zeta^\alpha) \bmod \langle u-1\rangle$, we have $f_\alpha(u^{n'}\zeta^\alpha) \equiv 0 \bmod \langle u-1\rangle$. If $f_\alpha(u^{n'}\zeta^\alpha) \in \langle (u-1)^2\rangle$, then, reducing modulo 2, we see that

$$0 \equiv f_\alpha(u^{n'}\zeta^\alpha) \equiv \sum_{j \text{ even}} \zeta^{j\alpha} f_{\alpha,j}(\zeta^\alpha) + u \sum_{j \text{ odd}} \zeta^{j\alpha} f_{\alpha,j}(\zeta^\alpha) \bmod \langle 2, u^2-1\rangle.$$

In particular,

$$\sum_{j \text{ even}} \zeta^{j\alpha} f_{\alpha,j}(\zeta^\alpha) \equiv 0 \bmod 2. \tag{18}$$

Now, observe that, since all the exponents of X are even in $\sum_{j \text{ even}} X^j f_{\alpha,j}(X)$, it follows that:

$$\sum_{j \text{ even}} X^j f_{\alpha,j}(X) \equiv (g(X))^2 \bmod 2,$$

for some polynomial $g(X)$, and $\deg(g) < \deg(f_\alpha)$. Therefore, by (18), it follows that $g(\zeta^\alpha) \equiv 0 \bmod 2$, which contradicts the minimality of f_α. Hence, $f_\alpha(u^{n'}\zeta^\alpha) \notin \langle (u-1)^2\rangle$.

(iii) Since $\alpha \cdot 2^k$ lies in the same 2-cyclotomic coset as α, it follows that $(\zeta^\alpha)^{2^k}$ is also a root of f_α. Hence, $f_\alpha((u^{n'}\zeta^\alpha)^{2^k}) = f_\alpha((\zeta^\alpha)^{2^k}) = 0$.

(iv) Note that $g(u^{n'}\zeta^\alpha) = \left(f_\alpha(u^{n'}\zeta^\alpha)\right)^i + 2e(u^{n'}\zeta^\alpha)$.

By (i), there is some $w \notin \langle u-1\rangle$ such that $f_\alpha(u^{n'}\zeta^\alpha) = w(u-1)$.

We claim that w is a unit.

From Lemma 2.3, $R_4(u, M)$ is local with maximal ideal $\langle 2, u-1\rangle$. Hence, if w is not a unit, then $w \in \langle 2, u-1\rangle$, so there exist $x, y \in R_4(u, M)$ such that $w = 2x + (u-1)y$. Then $f_\alpha(u^{n'}\zeta^\alpha) = 2x(u-1) + y(u-1)^2$, implying that $f_\alpha(u^{n'}\zeta^\alpha) \equiv 0 \bmod \langle 2, u^2-1\rangle$. We have seen in the proof of (ii) that this leads to a contradiction.

Hence, we have $\left(f_\alpha(u^{n'}\zeta^\alpha)\right)^i = w^i(u-1)^i$, w a unit. Now, there exist $s'_j \in \mathcal{T}_m$ $(0 \le j \le 2^k - 1)$ such that

$$\begin{aligned} g(u^{n'}\zeta^\alpha) &= \left(f_\alpha(u^{n'}\zeta^\alpha)\right)^i + 2e(u^{n'}\zeta^\alpha) \\ &= w^i(u-1)^i + 2\left(\sum_{j=0}^{2^k-1} s'_j(u-1)^j\right). \end{aligned}$$

Since w is a unit, this is an element of $\left\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \right\rangle$, where $s_j = w^{-i}s'_j$.

(v) Suppose, on the contrary, that $f_\alpha(u^{n'}\zeta^\beta) \in \langle 2, u-1\rangle$. Then we have

$$f_\alpha(u^{n'}\zeta^\beta) \equiv f_\alpha(\zeta^\beta) \equiv 0 \bmod \langle 2, u-1\rangle.$$

This means that $f_\alpha = f_\beta$, which contradicts the assumption. ■

THEOREM 4.2. *Let n be odd and let C be an ideal in $\mathbb{Z}_4[X]/\langle X^{2^k n}-1\rangle$. Then C is of the form:*

$$\left\langle p(X^{2^k})\prod_{i=0}^{2^k-1} q_i(X^{2^k})\prod_{i=1}^{2^k-1}\left(\prod_T \widetilde{r_{i,T}(X)}^{\,i}\right)\prod_{i=1}^{2^k-1}\left(\prod_{\ell=0}^{i-1}\widetilde{s_{i,\ell}(X)}^{\,i}\right),\right.$$
$$\left. 2p(X^{2^k})\prod_{i=0}^{2^k-1} q_i(X)^i\prod_{i=1}^{2^k-1}\left(\prod_T r_{i,T}(X)^T\right)\prod_{i=1}^{2^k-1}\left(\prod_{\ell=0}^{i-1} s_{i,\ell}(X)^\ell\right)\right\rangle, \tag{19}$$

where

$$X^n-1 = p(X)\left(\prod_{i=0}^{2^k-1} q_i(X)\right)\left(\prod_{i=1}^{2^k-1}\left(\prod_T r_{i,T}(X)\right)\right)\left(\prod_{i=1}^{2^k-1}\left(\prod_{\ell=0}^{i-1} s_{i,\ell}(X)\right)\right) y(X),$$

and $\widetilde{r_{i,T}(X)}$ and $\widetilde{s_{i,\ell}(X)}$ are lifts of $r_{i,T}(X)$ and $s_{i,\ell}(X)$, respectively, i.e., $\widetilde{r_{i,T}(X)}\equiv r_{i,T}(X) \bmod 2$ and $\widetilde{s_{i,\ell}(X)}\equiv s_{i,\ell}(X) \bmod 2$. (Here, for each i, the product $\prod_T$ is taken over all possible corresponding values of T as in Remark 1(iii).)

Proof. By Theorem 3.2, C is isomorphic to a direct sum of ideals $\oplus_{\alpha\in J} C_\alpha$ of the ring $\oplus_{\alpha\in J} R_4(u, m_\alpha)$.

The polynomials are given by the following rules:

- $f_\alpha | p$ if $C_\alpha = \langle 0\rangle$,
- $f_\alpha | y$ if $C_\alpha = \langle 1\rangle$,
- $f_\alpha | q_i$ if $C_\alpha = \langle 2(u-1)^i\rangle$, $i = 0, \ldots, 2^k-1$,
- $f_\alpha | r_{i,T}$ if $C_\alpha = \langle (u-1)^i + 2(u-1)^t h(u)\rangle$ with $\mathrm{Tor}(C_\alpha) = \langle (u-1)^T\rangle$, where T is as in Proposition 2.5(iv),
- $f_\alpha | s_{i,\ell}$ if $C_\alpha = \langle 2(u-1)^\ell, (u-1)^i + 2(u-1)^t h(u)\rangle$, $\ell < T$ with T as in Proposition 2.5(iv).

For $\ell \geq T$, we set $s_{i,\ell}(X) = 1 = \widetilde{s_{i,\ell}(X)}$. ∎

Remark 2. Note that the exact forms of the lifts $\widetilde{r_{i,T}(X)}$ and $\widetilde{s_{i,\ell}(X)}$ vary according to the code C and depend on the local components C_α.

THEOREM 4.3. *If C is given with generators as in Theorem* 4.2*, then*

$$|C| = (4^{\deg(t)})^{2^k}\prod_{0\leq i\leq 2^k-1}(2^{\deg(q_i)})^{2^k-i}\prod_{1\leq i\leq 2^k-1}\left(\prod_T (2^{\deg(r_{i,T})})^{2\cdot 2^k-i-T}\right)$$
$$\times\prod_{1\leq i\leq 2^k-1}\left(\prod_{0\leq \ell\leq i-1}(2^{\deg(s_{i,\ell})})^{2\cdot 2^k-\ell-i}\right).$$

Proof. This theorem follows from Theorem 4.2, Proposition 2.5 and the observation that, for $\langle (u-1)^j \rangle \subseteq \mathbb{F}_{2^{m_\alpha}}[u]/\langle (u-1)^{2^k} \rangle$, we have $|\langle (u-1)^j \rangle| = (2^{m_\alpha})^{2^k - j}$. ∎

5. Duals

Recall from Theorem 2.1 that cyclic codes in $(\mathbb{Z}_4)^{2^k n}$ correspond to constacyclic codes over $\mathcal{R} = \mathbb{Z}_4[u]/\langle u^{2^k} - 1 \rangle$ via the map Ψ. In fact, this identification is the same as the one given in [5], Section 3 (the ϕ there is our Ψ^{-1}).

Let $\bar{}: \mathcal{R} \to \mathcal{R}$ denote the "conjugation" map defined by $\overline{\sum_{i=0}^{2^k-1} a_i u^i} = \sum_{i=0}^{2^k-1} a_i u^{-i}$. (Note that $u^{-i} = u^{2^k - i}$ in $\mathcal{R}$.) This map is also extended to $R_4(u, m)$ in the obvious way. For any subset E of $\mathcal{R}$ or $R_4(u, m)$, we also denote by $\overline{E}$ the image of E under the conjugation map. On $\mathcal{R}^n$, we define the Hermitian inner product as follows: for $\mathbf{d} = (d_0, \ldots, d_{n-1}) \in \mathcal{R}^n$ and $\mathbf{d}' = (d'_0, \ldots, d'_{n-1}) \in \mathcal{R}^n$,

$$\langle \mathbf{d}, \mathbf{d}' \rangle = \sum_{j=0}^{n-1} d_j \overline{d'_j}. \tag{20}$$

The following lemma is essentially ([5], Proposition 3.2) translated into our present context:

LEMMA 5.1. *Let notation be as above, let σ denote the cyclic shift in $(\mathbb{Z}_4)^{2^k n}$ and let $\cdot$ denote the Euclidean inner product in $(\mathbb{Z}_4)^{2^k n}$. Then $\langle \mathbf{d}, \mathbf{d}' \rangle = 0$ if and only if $\sigma^{nj}(\Psi(\mathbf{d})) \cdot \Psi(\mathbf{d}') = 0$ for all $0 \le j \le 2^k - 1$.*

Let C and C' be constacyclic codes over $\mathcal{R}$ of length n. By [5], Corollary 3.3 (see also [4, Corollary 3.3]), C and C' are duals of each other (under the Hermitian inner product) if and only if $\Psi(C)$ and $\Psi(C')$ are duals of each other (under the Euclidean inner product).

We now consider how the Hermitian inner product in $\mathcal{R}^n$ is related to the coefficients of the Discrete Fourier Transforms.

Let $\mathbf{d} = (d_0, \ldots, d_{n-1}) \in \mathcal{R}^n$ and $\mathbf{d}' = (d'_0, \ldots, d'_{n-1}) \in \mathcal{R}^n$, and suppose that, for $0 \le t \le n-1$,

$$d_t = \sum_{j=0}^{2^k-1} c_{t,j} u^j \quad \text{and} \quad d'_t = \sum_{j=0}^{2^k-1} c'_{t,j} u^j.$$

Then $\Psi(\mathbf{d}) = \mathbf{c}$ and $\Psi(\mathbf{d}') = \mathbf{c}'$, where

$$\mathbf{c} = (c_{0,0}, c_{1,0}, \ldots, c_{n-1,0}, c_{0,1}, c_{1,1}, \ldots, c_{0,2^k-1}, c_{1,2^k-1}, \ldots, c_{n-1,2^k-1}) \in (\mathbb{Z}_4)^{2^k n}$$

and

$$\mathbf{c}' = (c'_{0,0}, c'_{1,0}, \ldots, c'_{n-1,0}, c'_{0,1}, c'_{1,1}, \ldots, c'_{0,2^k-1}, c'_{1,2^k-1}, \ldots, c'_{n-1,2^k-1}) \in (\mathbb{Z}_4)^{2^k n}.$$

Let $\widehat{c}(Z)=\sum_{h=0}^{n-1}\widehat{c}_{n-h}Z^h$ and $\widehat{c}'(Z)=\sum_{h=0}^{n-1}\widehat{c}'_{n-h}Z^h$ be the Mattson–Solomon polynomials of $\mathbf{c}$ and $\mathbf{c}'$, respectively. Then, by Lemma 3.1,

$$\begin{aligned}\sum_{t=0}^{n-1} d_t\overline{d'_t} &= \frac{1}{n^2}\sum_{t=0}^{n-1}\widehat{c}(\zeta^t)\overline{\widehat{c}'(\zeta^t)}\\ &= \frac{1}{n^2}\sum_{t=0}^{n-1}\left(\sum_{j=0}^{n-1}\widehat{c}_j\zeta^{-jt}\right)\left(\overline{\sum_{i=0}^{n-1}\widehat{c}'_i\zeta^{-it}}\right)\\ &= \frac{1}{n^2}\sum_{j=0}^{n-1}\widehat{c}_j\sum_{i=0}^{n-1}\overline{\widehat{c}'_i}\sum_{t=0}^{n-1}\zeta^{-(i+j)t}\\ &= \frac{1}{n}\sum_{i=0}^{n-1}\widehat{c}_i\overline{\widehat{c}'_{n-i}}. \end{aligned} \tag{21}$$

Definition 2. For an ideal C of $S=R_4(u,m)$, the annihilator $A(C)$ of C is defined to be the ideal

$$A(C)=\{g(u)\mid g(u)f(u)=0 \text{ for all } f(u)\in C\}.$$

For every $\alpha\in J$, let α' denote the representative in J of the coset containing $n-\alpha$.

LEMMA 5.2. *Let C, D be cyclic codes over $\mathbb{Z}_4$ of length $2^k n$ and let $C=\oplus_{\alpha\in J}C_\alpha$ and $D=\oplus_{\alpha\in J}D_\alpha$, where $D_\alpha=\overline{A(C_{\alpha'})}$. Then, $D\subseteq C^\perp$.*

Proof. This lemma follows from (21) and Lemma 5.1. ■

THEOREM 5.3. *The annihilator $A(C)$ of the ideal C in $S=R_4(u,m)$ is of the following form (notation as in Proposition 2.5):*

Case	C	$A(C)$
1.	$\langle 0\rangle$	$\langle 1\rangle$
2.	$\langle 1\rangle$	$\langle 0\rangle$
3.	$\langle 2\rangle$	$\langle 2\rangle$
4.	$\langle 2(u-1)^i\rangle$ $(1\le i\le 2^k-1)$	$\langle 2,(u-1)^{2^k-i}\rangle$
5.	$\langle (u-1)^i\rangle$ $(1\le i\le 2^{k-1})$	$\langle (u-1)^{2^k-i}+2(u-1)^{2^{k-1}-i}\rangle$
6.	$\langle (u-1)^i\rangle$ $(2^{k-1}+1\le i\le 2^k-1)$	$\langle 2(u-1)^{2^k-i},(u-1)^{2^{k-1}}+2\rangle$
7.	$\langle (u-1)^i+2(u-1)^{i-2^{k-1}}\rangle$ $(2^{k-1}\le i\le 2^k-1)$	$\langle (u-1)^{2^k-i}\rangle$

8.	$\left\langle (u-1)^i + 2(u-1)^{i-2^{k-1}}(1+(u-1)^\tau \tilde{h}(u)) \right\rangle$ $(2^{k-1} \le i \le 2^{k-1}+\tau,\ \tau \ge 1)$	$\left\langle (u-1)^{2^k-i} + 2(u-1)^{2^{k-1}+\tau-i}\tilde{h}(u) \right\rangle$
9.	$\left\langle (u-1)^i + 2(u-1)^{i-2^{k-1}}(1+(u-1)^\tau \tilde{h}(u)) \right\rangle$ $(2^{k-1}+\tau < i \le 2^k-1,\ \tau \ge 1)$	$\left\langle 2(u-1)^{2^k-i}, (u-1)^{2^{k-1}-\tau} + 2\tilde{h}(u) \right\rangle$
10.	$\left\langle (u-1)^{2^{k-1}} + 2h(u) \right\rangle$ $(h_0 \ne 0, 1)$	$\left\langle (u-1)^{2^{k-1}} + 2(1+h(u)) \right\rangle$
11.	$\left\langle (u-1)^i + 2(u-1)^{i-2^{k-1}}h(u) \right\rangle$ $(2^{k-1}+1 \le i \le 2^k-1, h_0 \ne 0, 1)$	$\left\langle 2(u-1)^{2^k-i}, (u-1)^{2^{k-1}} + 2(1+h(u)) \right\rangle$
12.	$\left\langle (u-1)^i + 2(u-1)^t h(u) \right\rangle$ $(2^{k-1}-i+t \ne 0, i \le 2^{k-1}, h(u) \ne 0)$	$\left\langle (u-1)^{2^k-i} + 2(u-1)^{2^{k-1}-i}(1+(u-1)^{2^{k-1}-i+t}h(u)) \right\rangle$
13.	$\left\langle (u-1)^i + 2(u-1)^t h(u) \right\rangle$ $(2^{k-1}-i+t \ne 0,$ $2^{k-1} < i < 2^{k-1}+t, h(u) \ne 0)$	$\left\langle 2(u-1)^{2^k-i}, (u-1)^{2^{k-1}} + 2(1+(u-1)^{2^{k-1}-i+t}h(u)) \right\rangle$
14.	$\left\langle (u-1)^i + 2(u-1)^t h(u) \right\rangle$ $(2^{k-1}-i+t \ne 0, 2^{k-1}+t < i,$ $t > 0, h(u) \ne 0)$	$\left\langle 2(u-1)^{2^k-i}, (u-1)^{i-t} + 2(h(u)+(u-1)^{i-t-2^{k-1}}) \right\rangle$
15.	$\left\langle (u-1)^i + 2h(u) \right\rangle$ $(2^{k-1} < i,\ h(u) \ne 0)$	$\left\langle (u-1)^i + 2(h(u)+(u-1)^{i-2^{k-1}}) \right\rangle$
16.	$\left\langle 2, (u-1)^i \right\rangle$ $(1 \le i \le 2^k-1)$	$\left\langle 2(u-1)^{2^k-i} \right\rangle$
17.	$\left\langle 2(u-1)^\ell, (u-1)^{2^{k-1}} + 2 \right\rangle$ $(1 \le \ell \le 2^{k-1}-1)$	$\left\langle (u-1)^{2^k-\ell} \right\rangle$
18.	$\left\langle 2(u-1)^\ell, (u-1)^{2^{k-1}} + 2(1+(u-1)^\tau \tilde{h}(u) \right\rangle$ $(1 \le \ell \le 2^{k-1}-1,\ 1 \le \tau \le \ell-1)$	$\left\langle (u-1)^{2^k-\ell} + 2(u-1)^{2^{k-1}-\ell+\tau}\tilde{h}(u) \right\rangle$
19.	$\left\langle 2(u-1)^\ell, (u-1)^{2^{k-1}} + 2h(u) \right\rangle$ $(1 \le \ell \le 2^{k-1}-1,\ h_0 \ne 0, 1)$	$\left\langle (u-1)^{2^k-\ell} + 2(u-1)^{2^{k-1}-\ell}(1+h(u)) \right\rangle$
20.	$\left\langle 2(u-1)^\ell, (u-1)^i + 2h(u) \right\rangle$ $(2^{k-1}+1 \le i \le 2^k-1,\ h(u) \ne 0,$ $1 \le \ell \le 2^k-i-1)$	$\left\langle (u-1)^{2^k-\ell} + 2(u-1)^{2^k-\ell-i}(h(u)+(u-1)^{i-2^{k-1}}) \right\rangle$
21.	$\left\langle 2(u-1)^\ell, (u-1)^i + 2h(u) \right\rangle$ $(1 \le i \le 2^{k-1}-1,\ h(u) \ne 0$ $1 \le \ell \le i-1)$	$\left\langle (u-1)^{2^k-\ell} + 2(u-1)^{2^{k-1}-\ell}(1+(u-1)^{2^{k-1}-i}h(u)) \right\rangle$
22.	$\left\langle 2(u-1)^\ell, (u-1)^i \right\rangle$ $(1 \le i \le 2^k-1\ ,$ $i-2^{k-1}+1 \le \ell \le \min\{i, 2^{k-1}\}-1)$	$\left\langle 2(u-1)^{2^k-i}, (u-1)^{2^k-\ell} + 2(u-1)^{2^{k-1}-\ell} \right\rangle$
23.	$\left\langle 2(u-1)^\ell, (u-1)^i \right\rangle$ $(2^{k-1}+1 \le i \le 2^k-1,\ 1 \le \ell \le i-2^{k-1})$	$\left\langle 2(u-1)^{2^k-i}, (u-1)^{2^k-\ell} \right\rangle$

Case	C	$A(C)$
24.	$\left\langle 2(u-1)^{\ell}, (u-1)^{i}+2(u-1)^{i-2^{k-1}}\right\rangle$ $(2^{k-1}+1\le i\le 2^k-1,\ i-2^{k-1}<\ell<i)$	$\left\langle 2(u-1)^{2^k-i}, (u-1)^{2^k-\ell}\right\rangle$
25.	$\left\langle 2(u-1)^{\ell}, (u-1)^{i}+2(u-1)^{i-2^{k-1}}(1+(u-1)^{\tau}\tilde{h}(u))\right\rangle$ $(2^{k-1}+1\le i\le 2^k-1,$ $i-2^{k-1}<\ell<\min\{i, 2^{k-1}+\tau\})$	$\left\langle 2(u-1)^{2^k-i}, (u-1)^{2^k-\ell}+2(u-1)^{2^{k-1}-\ell+\tau}\tilde{h}(u)\right\rangle$
26.	$\left\langle 2(u-1)^{\ell}, (u-1)^{i}+2(u-1)^{i-2^{k-1}}h(u)\right\rangle$ $(2^{k-1}+1\le i\le 2^k-1,\ i-2^{k-1}<\ell<2^{k-1},$ $h_0\neq 0, 1)$	$\left\langle 2(u-1)^{2^k-i},$ $(u-1)^{2^k-\ell}+2(u-1)^{2^{k-1}-\ell}(1+h(u))\right\rangle$
27.	$\left\langle 2(u-1)^{\ell}, (u-1)^{i}+2(u-1)^{t}h(u)\right\rangle$ $(2^{k-1}+t<i<2^{k-1}+\ell,\ h(u)\neq 0,$ $0<t<\ell<2^k-i+t)$	$\left\langle 2(u-1)^{2^k-i},$ $(u-1)^{2^k-\ell}+2(u-1)^{2^k-\ell-i+t}((u-1)^{i-t-2^{k-1}}$ $+h(u))\right\rangle$
28.	$\left\langle 2(u-1)^{\ell}, (u-1)^{i}+2(u-1)^{t}h(u)\right\rangle$ $(2^{k-1}+\ell\le i,\ h(u)\neq 0,$ $0<t<\ell<2^k-i+t)$	$\left\langle 2(u-1)^{2^k-i}, (u-1)^{2^k-\ell}+2(u-1)^{2^k-\ell-i+t}h(u)\right\rangle$
29.	$\left\langle 2(u-1)^{\ell}, (u-1)^{i}+2(u-1)^{t}h(u)\right\rangle$ $(1\le i\le 2^{k-1}+t-1,\ h(u)\neq 0\ ,$ $0<t<\ell<\min\{2^{k-1}, i, 2^k\})$	$\left\langle 2(u-1)^{2^k-i},$ $(u-1)^{2^k-\ell}+2(u-1)^{2^{k-1}-\ell}(1+(u-1)^{2^{k-1}}$ $-i+t\ h(u))\right\rangle$

Proof. For each C, let D denote the corresponding ideal in the right-most column. A simple verification shows that $D\subseteq A(C)$ and that $|D|=(4^m)^{2^k}/|C|$. An argument similar to the one for Lemma 5.2 (with C a cyclic code of length 2^k over $GR(4,m)$) proves that $\overline{A(C)}\subseteq C^{\perp}$, so (cf. [6, Theorem 3.10(iii)])

$$(4^m)^{2^k}/|C|=|D|\le|A(C)|=|\overline{A(C)}|\le|C^{\perp}|=(4^m)^{2^k}/|C|.$$

Therefore, $D=A(C)$ and $\overline{A(C)}=C^{\perp}$. ∎

The following description of the dual code now follows from Lemma 5.2 and the proof of Theorem 5.3.

COROLLARY 5.4. *Let C be a cyclic code over $\mathbb{Z}_4$ of length $2^k n$ and let $C=\oplus_{\alpha\in J}C_{\alpha}$. Then $C^{\perp}=\oplus_{\alpha\in J}\overline{A(C_{\alpha'})}$.*

Therefore, to understand self-dual codes, it is first necessary to identify the ideals $C\subseteq R_4(u,m)$ such that $C=\overline{A(C)}$.

PROPOSITION 5.5. *With notation as in Theorem 5.3, if $C=\overline{A(C)}$, then C must belong to one of the following types:*

- $\langle 2 \rangle$ (*Case 3*);
- $\left\langle (u-1)^i + 2h(u) \right\rangle$, $(2^{k-1} < i,\ h(u) \neq 0)$ (*Case 15*);
- $\left\langle 2(u-1)^{2^k-i}, (u-1)^i \right\rangle$, $(3 \cdot 2^{k-2} \leq i \leq 2^k - 1)$ (*Case 23*);
- $\left\langle 2(u-1)^{2^k-i}, (u-1)^i + 2(u-1)^t h(u) \right\rangle$, $(2^{k-1} + t < i,\ h(u) \neq 0,\ 0 < t < 2^k - i)$ (*Cases 27 & 28*).

Remark 3. For Cases 15, 27 and 28, additional conditions on the coefficients of $h(u)$ may be necessary in order for $C = \overline{A(C)}$.

Proof. First, we eliminate the other cases. It is clear that C in Cases 1 and 2 cannot satisfy $C = \overline{A(C)}$. For Cases 4,6,7,9,11,13,14,16–21, C and $\overline{A(C)}$ are clearly of different types (e.g., in all cases except for Case 7, one ideal is principal while the other is not).

Some other cases are eliminated by showing an element is in C, if we assume $C = \overline{A(C)}$, while it really should not. This approach works for Cases 5, 8, 10 and 12. We illustrate with Case 8 (one of the more involved among these cases). Note that $\mathrm{Res}(C) = \mathrm{Res}(\overline{A(C)})$ implies that $i = 2^{k-1}$. Now write $h(u) = \sum h_j (u-1)^j$. By Proposition 2.5, $\mathrm{Tor}(C) = \langle (u-1)^{2^{k-1}} \rangle$ in this case. The assumption $C = \overline{A(C)}$ implies that

$$\begin{aligned} C &= \left\langle (u-1)^{2^{k-1}} + 2\left(1 + \sum h_j (u-1)^{j+\tau}\right) \right\rangle \\ &= \left\langle (u-1)^{2^{k-1}} + 2(u-1)^\tau \left(\sum h_j (u-1)^j u^{2^{k-1}-\tau-j}\right) \right\rangle, \end{aligned}$$

which implies that

$$2\left(1 + \sum h_j (u-1)^{j+\tau}\right) + 2(u-1)^\tau \left(\sum h_j (u-1)^j u^{2^{k-1}-\tau-j}\right) \in C.$$

This means that

$$\left(1 + \sum h_j (u-1)^{j+\tau}\right) + (u-1)^\tau \left(\sum h_j (u-1)^j u^{2^{k-1}-\tau-j}\right) \in \mathrm{Tor}(C) = \langle (u-1)^{2^{k-1}} \rangle,$$

which cannot be true since $\tau \geq 1$. Cases 5, 10 and 12 can be eliminated in a similar fashion.

The remaining cases to eliminate, i.e., Cases 22, 24, 25, 26 and 29, can be proved by showing that the assumption $C = \overline{A(C)}$ leads to a contradiction to some of the conditions on i, ℓ and t. E.g., consider Case 25. With $\tilde{h}(u) = \sum \tilde{h}_j (u-1)^j$, the assumption $C = \overline{A(C)}$ means that

$$\begin{aligned} &\left\langle 2(u-1)^\ell, (u-1)^i + 2(u-1)^{i-2^{k-1}} (1 + (u-1)^\tau \sum \tilde{h}_j (u-1)^j) \right\rangle \\ &\quad = \left\langle 2(u-1)^{2^k-i}, (u-1)^{2^k-\ell} + 2(u-1)^{2^{k-1}-\ell+\tau} (\sum \tilde{h}_j (u-1)^j u^{2^{k-1}-\tau-j}) \right\rangle, \end{aligned}$$

which implies that $i+\ell=2^k$ and (hence)

$$2(u-1)^{i-2^{k-1}}\left(1+(u-1)^{\tau}\sum\tilde{h}_j(u-1)^j\right)$$
$$+2(u-1)^{i-2^{k-1}+\tau}\left(\sum\tilde{h}_j(u-1)^j u^{2^{k-1}-\tau-j}\right)\in C,$$

so

$$(u-1)^{i-2^{k-1}}\left(1+(u-1)^{\tau}\sum\tilde{h}_j(u-1)^j+(u-1)^{\tau}\sum\tilde{h}_j(u-1)^j u^{2^{k-1}-\tau-j}\right)$$
$$\in \mathrm{Tor}(C)=\left\langle(u-1)^{\ell}\right\rangle.$$

This means that $i-2^{k-1}\geq\ell$, but this case assumes that $i-2^{k-1}<\ell$. Cases 22, 24, 26 and 29 may be dealt with in a similar way.

Consequently, only cases 3, 15, 23, 27 and 28 remain plausible for C. The additional constraint for Case 23 in the statement of the Proposition follows because $i+\ell=2^k$ and $\ell\leq i-2^{k-1}$. ■

Note that this proposition is not an "if and only if" result, for C simply being one of these cases does not ensure that $C=\overline{A(C)}$.

COROLLARY 5.6. *For $k\in\{1,2,3,4\}$ and C an ideal in $R_4(u,m)$, we have $C=\overline{A(C)}$ if and only if C is*

(i) $(k=1)$ $\langle 2\rangle$;

(ii) $(k=2)$ $\langle 2\rangle$, $\langle (u-1)^3+2h_0\rangle$ $(h_0\in\mathcal{T}_m\setminus\{0\})$, *or* $\langle 2(u-1),(u-1)^3\rangle$;

(iii) $(k=3)$ $\langle 2\rangle$, $\langle (u-1)^5+2(1+h_1(u-1)+h_2(u-1)^2)\rangle$, $\langle (u-1)^6+2(h_0+h_1(u-1))\rangle$, $\langle (u-1)^7+2h_0\rangle$, $\langle 2(u-1),(u-1)^7\rangle$, $\langle 2(u-1)^2,(u-1)^6\rangle$, *or* $\langle 2(u-1)^2,(u-1)^6+2(u-1)h_0\rangle$ $(h_0\in\mathcal{T}_m\setminus\{0\},\ h_1,h_2\in\mathcal{T}_m)$;

(iv) $(k=4)$ $\langle 2\rangle$, $\langle (u-1)^{15}+2h_0\rangle$, $\langle (u-1)^{14}+2(h_0+h_1(u-1))\rangle$, $\langle (u-1)^{12}+2(h_0+h_2(u-1)^2+h_3(u-1)^3)\rangle$, $\langle (u-1)^{10}+2(h_0+(1+h_0)(u-1)+h_2(u-1)^2+h_4(u-1)^4+h_5(u-1)^5)\rangle$, $\langle 2(u-1)^4,(u-1)^{12}\rangle$, $\langle 2(u-1)^3,(u-1)^{13}\rangle$, $\langle 2(u-1)^2,(u-1)^{14}\rangle$, $\langle 2(u-1),(u-1)^{15}\rangle$, $\langle 2(u-1)^6,(u-1)^{10}+2(u-1)(1+h_1(u-1)+h_3(u-1)^3+h_4(u-1)^4)\rangle$, $\langle 2(u-1)^5,(u-1)^{11}+2(u-1)(h_0+(1+h_0)(u-1)+h_2(u-1)^2+h_3(u-1)^3)\rangle$, $\langle 2(u-1)^5,(u-1)^{11}+2(u-1)^2(1+h_1(u-1)+h_2(u-1)^2)\rangle$, $\langle 2(u-1)^2,(u-1)^{14}+2(u-1)h_0\rangle$, $\langle 2(u-1)^3,(u-1)^{13}+2(u-1)(h_0+h_1(u-1))\rangle$, $\langle 2(u-1)^3,(u-1)^{13}+2(u-1)^2h_0\rangle$, $\langle 2(u-1)^4,(u-1)^{12}+2(u-1)^2(h_0+h_1(u-1))\rangle$, *or* $\langle 2(u-1)^4,(u-1)^{12}+2(u-1)^3h_0\rangle$ $(h_0\in\mathcal{T}_m\setminus\{0\},\ h_1,h_2,h_3,h_4,h_5\in\mathcal{T}_m)$.

Proof. By Proposition 5.5, it suffices to deduce the additional conditions satisfied by the coefficients of $h(u)$ in Cases 15, 27 and 28.

When $k=1$, it is clear that Cases 15, 23, 27 and 28 do not exist.

When $k=2$, Cases 27 and 28 cannot exist because the conditions imply that $i=3$ and $t=0$, contradicting the assumption that $t>0$. For Case 15, the condition on i shows that $i=3$ (so $\mathrm{Tor}(C)=\langle(u-1)\rangle$ and hence we may assume

$h(u) = h_0$ where $h_0 \in \mathcal{T}_m \setminus \{0\}$), and therefore $C = \overline{A(C)}$ if and only if

$$\langle (u-1)^3 + 2h_0 \rangle = \langle (u-1)^3 + 2(u^3 h_0 + u^2(u-1)) \rangle,$$

which is equivalent to

$$2(h_0 + u^3 h_0 + u^2(u-1)) \in C,$$

i.e.,

$$h_0 + u^3 h_0 + u^2(u-1) \in \mathrm{Tor}(C) = \langle (u-1) \rangle.$$

This last condition is true for all $h_0 \in \mathcal{T}_m \setminus \{0\}$. This completes the case $k = 2$.

Now consider the case $k = 3$. A necessary condition for Case 15 is $5 \le i \le 7$ (so $\mathrm{Tor}(C) = \langle (u-1)^{8-i} \rangle$ and hence we may assume that $h(u) = \sum_{j=0}^{7-i} h_j (u-1)^j$). Noting that $u^e = (1 + (u-1))^e = \sum_{m=0}^{e} \binom{e}{m} (u-1)^m$, the same kind of argument as in the case $k = 2$ shows that $C = \overline{A(C)}$ if and only if $C = \langle (u-1)^5 + 2(1 + h_1(u-1) + h_2(u-1)^2) \rangle$, $\langle (u-1)^6 + 2(h_0 + h_1(u-1)) \rangle$ or $\langle (u-1)^7 + 2h_0 \rangle$, where $h_0 \in \mathcal{T}_m \setminus \{0\}$ and $h_1, h_2 \in \mathcal{T}_m$.

For Cases 27 and 28, writing $\ell = 2^k - i$, we see that the conditions imply that $0 < t < 2$ (i.e., $t = 1$), so $i > 5$ and $\ell < 3$. However, Case 27 can only exist if $\ell \ge t + 2 = 3$ (see the conditions in Theorem 5.3). As for Case 28, $t = 1$ must imply $\ell = 2$, so $i = 6$. Arguing as in the case $k = 2$, we see that $C = \overline{A(C)}$ if and only if $C = \langle 2(u-1)^2, (u-1)^6 + 2(u-1)h_0 \rangle$.

Finally, let $k = 4$. The condition in Case 15 means that $i \ge 9$. Using the same approach as for $k = 3$, it is easy to see that, when $i = 9$, 11 or 13, we must have $h_0 = 0$ (this can be seen by considering the coefficient of $(u-1)$ in $h(u) + u^i h(u^{-1}) + u^8 (u-1)^{i-8}$). The conditions on the coefficients of $h(u)$ when $i = 10, 12, 14, 15$ can also be obtained using the same consideration.

For Case 27, we must have $i < 12$ and $4 > i - 8 > t$, so only $t = 1$ and 2 are feasible. If $t = 1$, then $i \in \{10, 11\}$; while $t = 2$ implies that $i = 11$. An argument similar to the one in the case $k = 3$ yields the desired ideals.

As for Case 28, the conditions imply that $i \ge 12$ and $0 < t < 16 - i$. Therefore, the only possibilities are: $i = 14$ and $t = 1$; $i = 13$ and $i = 1, 2$; and $i = 12$ and $t = 1, 2, 3$. Applying the same argument as above, the conditions for the coefficients of $h(u)$ are obtained, except that the case $i = 12$ and $t = 1$ yields the condition $h_0 = 0$ and is thus inadmissible.

This completes the proof of the corollary. ■

COROLLARY 5.7. *For $1 \le k \le 4$, the number of ideals $C \subseteq R_4(u, m)$ such that $C = \overline{A(C)}$ is*

(i) 1 (*when $k = 1$*);

(ii) $2^m + 1$ (*when $k = 2$*);

(iii) $2 \cdot (2^m)^2 + 2^m + 1$ (*when $k = 3$*); *and*

(iv) $(2^m)^4 + 2 \cdot (2^m)^3 + (2^m)^2 + 2^m + 2$ (*when $k = 4$*).

For $\alpha \in J$, recall that N_α denotes the number of ideals in $R_4(u, m_\alpha)$. Let M_α denote the number of ideals C in $R_4(u, m_\alpha)$ such that $C = \overline{A(C)}$ (when $1 \le k \le 4$, this value is given in Corollary 5.7).

Let $\tilde{J}$ denote the subset of J consisting of those α such that $\alpha = \alpha'$, where $\alpha' \in J$ is the representative of the cyclotomic coset containing $n - \alpha$. We also further partition $J \backslash \tilde{J}$ into two parts K, K' of equal size such that $\alpha \in K$ if and only if α' belongs to K'.

The following enumeration of self-dual cyclic codes over $\mathbb{Z}_4$ follows immediately from Corollary 5.4.

PROPOSITION 5.8. *The number of self-dual cyclic codes over $\mathbb{Z}_4$ of length $2^k n$ is given by $\prod_{\alpha \in K} N_\alpha \prod_{\alpha \in \tilde{J}} M_\alpha$.*

EXAMPLE 5.1. For cyclic codes of length 28 over $\mathbb{Z}_4$, we have $k = 2$ and $n = 7$. Note that $\tilde{J} = \{0\}$ and that we may take $K = \{1\}$ and $K' = \{6\}$. By Corollary 5.7, Proposition 5.8 and Theorem 2.6, there are $3 \cdot 113 = 339$ self-dual cyclic codes of length 28.

As a corollary, we also retrieve [2, Corollary 2].

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

Proof. If $N = 2n$, then $k = 1$. We have that $\mathbb{Z}_4[X]/\langle X^{2^k n} - 1 \rangle \cong \oplus_{\alpha \in J} R_4(u, m_\alpha)$. The condition that $-1 \equiv 2^e \bmod n$ for some e implies that $\alpha = \alpha'$ for all $\alpha \in J$, i.e., $J = \tilde{J}$. Since $k = 1$, the only self-dual ideal in each $R_4(u, m_\alpha)$ is $\langle 2 \rangle$. Therefore there is only one cyclic self-dual code and it is $\oplus_{\alpha \in J} \langle 2 \rangle = 2(\mathbb{Z}_4)^{2n}$. ∎

6. Examples

We shall give examples of cyclic codes for lengths less than or equal to 14.

$N = 2$.

If $N = 2$, then $n = 1, k = 1, J = \{0\}$, and $m_0 = 1$. There are seven ideals for this case. We shall list them together with the vectors that generate the code over $\mathbb{Z}_4$:

$$\langle 0 \rangle \leftrightarrow \begin{pmatrix} 0 & 0 \end{pmatrix}, \quad \langle 1 \rangle \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \langle 2 \rangle \leftrightarrow \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix},$$

$$\langle 2(u-1) \rangle \leftrightarrow \begin{pmatrix} 2 & 2 \end{pmatrix}, \quad \langle (u-1) \rangle \leftrightarrow \begin{pmatrix} 1 & 3 \end{pmatrix}, \quad \langle (u-1)+2 \rangle \leftrightarrow \begin{pmatrix} 1 & 1 \end{pmatrix},$$

$$\langle (u-1), 2 \rangle \leftrightarrow \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}.$$

There is only one cyclic self-dual code of length 2, namely $\langle 2 \rangle$.

$N = 4$.

If $N=4$, then $n=1, k=2, J=\{0\}$, and $m_0=1$. There are 23 ideals for this case. There are three cyclic self-dual codes of this length. We shall list them:

$$\langle 2\rangle \leftrightarrow 2(\mathbb{Z}_4)^4,$$

$$\langle (u-1)^3+2\rangle \leftrightarrow \begin{pmatrix} 1 & 1 & 3 & 1 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{pmatrix},$$

$$\langle 2(u-1), (u-1)^3\rangle \leftrightarrow \begin{pmatrix} 1 & 1 & 3 & 3 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix}.$$

$N=6$.

If $N=6$, then $n=3, k=1, J=\{0,1\}$, $m_0=1$ and $m_1=2$. We have $\mathbb{Z}_4[X]/\langle X^6-1\rangle \cong R_4(u,1)\oplus R_4(u,2)$. There are $7\cdot 9=63$ ideals in this case. There is only one cyclic self-dual code, namely $\langle 2\rangle \oplus \langle 2\rangle \leftrightarrow 2(\mathbb{Z}_4)^6$.

$N=8$.

If $N=8$, then $n=1, k=3, J=\{0\}$, and $m_0=1$. There are 135 ideals in this case.

There are 11 cyclic self-dual codes of length 8. They are: $\langle 2\rangle$, $\langle (u-1)^5+2\rangle$, $\langle (u-1)^5+2(1+(u-1))\rangle$, $\langle (u-1)^5+2(1+(u-1)^2)\rangle$, $\langle (u-1)^5+2(1+(u-1)+(u-1)^2)\rangle$, $\langle (u-1)^6+2\rangle$, $\langle (u-1)^6+2(1+(u-1))\rangle$, $\langle (u-1)^7+2\rangle$, $\langle 2(u-1)^2, (u-1)^6\rangle$, $\langle 2(u-1), (u-1)^7\rangle$ and $\langle 2(u-1)^2, (u-1)^6+2(u-1)\rangle$. (The list given in Ref. 1, Section IV is incorrect.)

$N=10$.

If $N=10$, then $n=5, k=1, J=\{0,1\}$, $m_0=1$ and $m_1=4$. There are $7\cdot 21=84$ ideals in this case. There is only 1 cyclic self-dual code, namely $\langle 2\rangle \oplus \langle 2\rangle \leftrightarrow 2(\mathbb{Z}_4)^{10}$.

$N=12$.

If $N=12$, then $n=3, k=2, J=\{0,1\}$, $m_0=1$ and $m_1=2$. We have $\mathbb{Z}_4[X]/\langle X^{12}-1\rangle \cong R_4(u,1)\oplus R_4(u,2)$. We have seen that $R_4(u,1)$ has 23 distinct ideals and $R_4(u,2)$ has 45 distinct ideals making 1035 distinct cyclic codes of length 12 over $\mathbb{Z}_4$.

Corollary 5.6 gives the possible self-dual ideals in the rings. There are three self-dual ideals in $R_4(u,1)$ and they are:

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

There are five self-dual ideals in $R_4(u,2)$ and they are:

$$\langle 2\rangle, \langle (u-1)^3+2\rangle, \langle (u-1)^3+2\xi\rangle, \langle (u-1)^3+2\xi^2\rangle, \langle 2(u-1), (u-1)^3\rangle,$$

where $\mathcal{T}_2 = \{0, 1, \xi, \xi^2\}$ is the Teichmüller set of $GR(4, 2)$.

Hence there are 15 self-dual codes of the form $C_0 \oplus C_1$, where C_0 is an ideal in the first list and C_1 is an ideal in the second list.

$$N = 14.$$

If $N = 14$, then $n = 7, k = 1, J = \{0, 1, 6\}$, $m_0 = 1$, $m_1 = 3$ and $m_6 = 3$. There are $7 \cdot 13 \cdot 13 = 1183$ ideals in this case. There is only one ideal C_0 in $R_4(u, 1)$ such that $C_0 = \overline{A(C_0)}$, while there are 13 distinct ideals C_1 in $R_4(u, 3)$. Any self-dual code in $\mathbb{Z}_4[X]/\langle X^{14} - 1\rangle$ is of the form $C_0 \oplus C_1 \oplus \overline{A(C_1)}$, so there are altogether 13 self-dual codes of length 14.

7. Conclusion

We have determined the structure of cyclic codes over $\mathbb{Z}_4$ for arbitrary even lengths, giving the generator polynomial for these codes. The number of cyclic codes for a given length is also obtained. A spectral description of these codes has been given, which enabled us to describe the duals of the cyclic codes and the form of cyclic codes that are self-dual, as well as to enumerate self-dual cyclic codes over $\mathbb{Z}_4$. All cyclic self-dual codes of length less than or equal to 14 were also studied.

A natural open problem is to study the structure of cyclic codes of arbitrary lengths over $\mathbb{Z}_{p^e}$, where p is a prime and $e \geq 2$ is a positive integer.

References

1. T. Abualrub and R. Oehmke, On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e, *IEEE-IT*, Vol. 49, No. 9, September (2003) pp. 2126–2133.
2. T. Blackford, Cyclic codes over $\mathbb{Z}_4$ of oddly even length, *Discrete Applied Mathematics*, Vol. 128 (2003) pp. 27–46.
3. A. R. Calderbank and N. J. A. Sloane, Modular and p-adic cyclic codes, *Designs, Codes and Cryptography*, Vol. 6 (1995) pp. 21–35.
4. S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes I: finite fields, *IEEE-IT*, Vol. 47, No. 7, November (2001) pp. 2751–2760.
5. S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes II: chain rings, *Designs, Codes Cryptography*, Vol. 30 (2003) pp. 113–130.
6. G. H. Norton and A. Sălăgean, On the structure of linear and cyclic codes over a finite chain ring, *Appl. Alg. Engrg. Comm. Comput.*, Vol. 10 (2000) pp. 489–506.
7. V. S. Pless and Z. Qian, Cyclic codes and quadratic residue codes over Z_4, *IEEE-IT*, Vol. 42, No. 5, September (1996) pp. 1594–1600.