Available online at www.sciencedirect.com
ScienceDirect

FINITE FIELDS AND THEIR APPLICATIONS

ELSEVIER

Finite Fields and Their Applications 13 (2007) 31–57
http://www.elsevier.com/locate/ffa

On modular cyclic codes

Steven T. Dougherty[a], Young Ho Park[b,*]

[a]*Department of Mathematics, University of Scranton, Scranton, PA 18510, USA*
[b]*Department of Mathematics, Kangwon National University, Chuncheon 200-701, Republic of Korea*

Received 22 November 2004; revised 2 June 2005

Communicated by Vera Pless

Available online 26 July 2005

Abstract

We study cyclic codes of arbitrary length N over the ring of integers modulo M. We first reduce this to the study of cyclic codes of length $N = p^k n$ (n prime to p) over the ring $\mathbb{Z}_{p^e}$ for prime divisors p of N. We then use the discrete Fourier transform to obtain an isomorphism γ between $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$ and a direct sum $\oplus_{i\in I}\mathcal{S}_i$ of certain local rings which are ambient spaces for codes of length p^k over certain Galois rings, where I is the complete set of representatives of p-cyclotomic cosets modulo n. Via this isomorphism we may obtain all codes over $\mathbb{Z}_{p^e}$ from the ideals of $\mathcal{S}_i$. The inverse isomorphism of γ is explicitly determined, so that the polynomial representations of the corresponding ideals can be calculated. The general notion of higher torsion codes is defined and the ideals of $\mathcal{S}_i$ are classified in terms of the sequence of their torsion codes.

MSC: 94B15; 94B05; 11T71; 14H20

Keywords: Cyclic codes; Constacyclic codes; Galois rings; Discrete Fourier transforms; Local rings; Torsion codes

[*] Corresponding author.
E-mail addresses: doughertys1@scranton.edu (S.T. Dougherty), yhpark@kangwon.ac.kr (Y.H. Park).

1071-5797/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2005.06.004

1. Introduction

Cyclic codes are a widely studied family of codes that are very important from both a theoretical and an applied standpoint. Cyclic-codes over $\mathbb{Z}_{p^e}$ of length N where p does not divide N are a well-understood object; see [3,7] for example and the references therein. Cyclic codes over $\mathbb{Z}_4$ of odd length were studied in [12], of length 2^k were studied in [1] and of length $2n$, n odd, were studied in [2]. In [5], this work was completed by studying cyclic codes of length $2^k n$.

Cyclic codes of length N over a ring R are identified with the ideals of $R[X]/\langle X^N-1\rangle$ by identifying the vectors with the polynomials of degree less than N. Cyclic codes over a finite field $\mathbb{F}_q$ are well-known [11]. Indeed every cyclic code C over $\mathbb{F}_q$ is generated by a nonzero monic polynomial of the minimal degree in C, which must be a divisor of X^N-1 by the minimality of degree. Since $\mathbb{F}_q[X]$ is a UFD, cyclic codes over $\mathbb{F}_q$ are completely determined by the factorization of X^N-1 whether or not N is prime to the characteristic of the field, even though when they are not relatively prime we are in the repeated root case [4,9]. This is true for cyclic codes over $\mathbb{Z}_{p^e}$ if the length N is prime to p, since X^N-1 factors uniquely over $\mathbb{Z}_{p^e}$ by Hensel's Lemma in this case. In fact, all cyclic codes over $\mathbb{Z}_{p^e}$ of length N prime to p have the form $\langle f_0, pf_1, p^2f_2, \ldots, p^{e-1}f_{e-1}\rangle$, where $f_{e-1} \mid f_{e-2} \mid \cdots \mid f_0 \mid X^N-1$ [3,7]. Therefore, cyclic codes of length N prime to p are again easily determined by the unique factorization of X^N-1. The case of the characteristic of the ring dividing the length N is more difficult because there is no unique factorization of X^N-1.

We begin with some definitions. A code C of length N over a ring R is said to be *constacyclic* if there exists a unit $u \in R$, such that

$$(c_0, c_1, \ldots, c_{N-1}) \in C \Rightarrow (uc_{N-1}, c_0, c_1, \ldots, c_{N-2}) \in C.$$

If $u=1$, then C is a *cyclic* code. In general, linear constacyclic codes are identified with ideals of $R[X]/\langle X^N-u\rangle$ by the identification

$$(c_0, c_1, \ldots, c_{N-1}) \mapsto c_0 + c_1X + c_2X^2 + \cdots + c_{N-1}X^{N-1}. \tag{1}$$

In this paper, all codes are linear and the ambient space R^N for constacyclic codes of length N over R is identified with $R[X]/\langle X^N-u\rangle$.

Let C be a (linear) cyclic code of length N over the ring $\mathbb{Z}_M$, where M and N are arbitrary positive integers. First we use the Chinese Remainder Theorem to decompose the code C, i.e. an ideal of $\mathbb{Z}_M[X]/\langle X^N-1\rangle$, into a direct sum of ideals over $\mathbb{Z}_{p_i^{e_i}}$ according to the prime factorization of $M = p_1^{e_1}p_2^{e_2}\ldots p_r^{e_r}$ as follows. For each prime divisor p_i of M, let $C^{(p_i)} = C \pmod{p_i^{e_i}}$. By the Chinese Remainder Theorem, we have an isomorphism

$$\psi_M : C \simeq \bigoplus_{i=1}^{r} C^{(p_i)} \tag{2}$$

by the map $\psi_M(v) = (v \pmod{p_1^{e_1}}, v \pmod{p_2^{e_2}}, \ldots, v \pmod{p_r^{e_r}})$. Conversely, if $C^{(p_i)}$ are cyclic codes over $\mathbb{Z}_{p_i^{e_i}}$ then the Chinese Remainder Theorem again gives us a cyclic code $C = CRT(C^{(p_1)}, C^{(p_2)}, \ldots, C^{(p_r)})$, called a Chinese product [6], over $\mathbb{Z}_M$, such that $\psi_M(C) = \oplus_{i=1}^{r} C^{(p_i)}$. Therefore, it is enough to study cyclic codes over the rings $\mathbb{Z}_{p^e}$ for a prime p.

Fix a prime p and write $N = p^k n$, p not dividing n. We shall examine cyclic codes over $\mathbb{Z}_{p^e}$ of length N. In our case the factorization of $X^N - 1$ is not unique so we take the discrete Fourier transform approach which is a generalization of the approach in [2,5]. We define an isomorphism between $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$ and a direct sum, $\oplus_{i\in I} \mathcal{S}_{p^e}(m_i, u)$, of certain local rings defined in (9). This shows that any cyclic code over $\mathbb{Z}_{p^e}$ can be described by a direct sum of ideals using this decomposition. We also give the inverse isomorphism so that the corresponding ideal in $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$ can be computed explicitly. This will clarify the correspondence of ideals described in [2,5]. The ideals of local rings that occur are classified in the final section.

2. Cyclic codes over $\mathbb{Z}_{p^e}$

Let p be a prime. Throughout this paper we let $R = \mathbb{Z}_{p^e}$ and write $R_N = \mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$, so that $R_N = R^N$ after the identification (1). We shall consider cyclic codes over R of length $N = p^k n$, where p does not divide n. By introducing an auxiliary variable u, we first define the ring

$$\mathcal{R} = \mathbb{Z}_{p^e}[u]/\langle u^{p^k} - 1\rangle.$$

There is a natural $\mathbb{Z}_{p^e}$-module isomorphism $\Psi : \mathcal{R}^n \to \mathbb{Z}_{p^e}^N$ defined by

$$\begin{aligned}&\Psi(a^{(0)}, a^{(1)}, \ldots, a^{(n-1)})\\ &\quad = (a_0^{(0)}, a_0^{(1)}, \ldots, a_0^{(n-1)}, a_1^{(0)}, a_1^{(1)}, \ldots, a_1^{(n-1)}, \ldots, a_{p^k-1}^{(0)}, a_{p^k-1}^{(1)}, \ldots, a_{p^k-1}^{(n-1)}),\end{aligned} \tag{3}$$

where $a^{(i)} = a_0^{(i)} + a_1^{(i)} u + \cdots + a_{p^k-1}^{(i)} u^{p^k-1} \in \mathcal{R}$ for $0 \leqslant i \leqslant n-1$. It is easy to see that the constacyclic shift by u in $\mathcal{R}^n$ corresponds to a cyclic shift in $\mathbb{Z}_{p^e}^N$. As before we identify $\mathcal{R}^n$ with $\mathcal{R}[X]/\langle X^n - u\rangle$. If we view Ψ as a map from $\mathcal{R}[X]/\langle X^n - u\rangle$ to $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$, we have that

$$\Psi\left(\sum_{i=0}^{n-1}\left(\sum_{j=0}^{p^k-1} a_j^{(i)} u^j\right) X^i\right) = \sum_{i=0}^{n-1}\sum_{j=0}^{p^k-1} a_j^{(i)} X^{i+jn}. \tag{4}$$

It is straightforward to prove the following lemma:

Lemma 2.1. *Ψ is an $\mathbb{Z}_{p^e}$-algebra isomorphism between $\mathcal{R}[X]/\langle X^n - u\rangle$ and $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$. Furthermore, the cyclic codes over $\mathbb{Z}_{p^e}$ of length N correspond to constacyclic codes of length n over $\mathcal{R}$ via the map Ψ.*

$$\begin{tikzcd}
\mathcal{R}[X]/\langle X^n - u\rangle \arrow[r, "\Psi"] \arrow[d, equal] & \mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle \arrow[d, equal] \\
\mathcal{R}^n \arrow[r, "\Psi"] & \mathbb{Z}_{p^e}^N
\end{tikzcd}$$

The ring $\mathcal{R}$ is shortly proved to be a finite local ring, and hence the regular polynomial $X^n - u$ has a unique factorization in $\mathcal{R}[X]$

$$X^n - u = g_1 g_2 \ldots g_l \tag{5}$$

into monic, irreducible and pairwise relatively prime polynomials $g_i \in \mathcal{R}[X]$, and by the Chinese Remainder Theorem

$$\mathcal{R}[X]/\langle X^n - u\rangle \simeq \mathcal{R}[X]/\langle g_1\rangle \oplus \cdots \oplus \mathcal{R}[X]/\langle g_l\rangle. \tag{6}$$

This isomorphism will give us a decomposition of $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$ via the map Ψ. However, the corresponding decomposition of $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$ seems difficult to manage. We will examine this isomorphism in more detail later. Instead we will use the discrete Fourier transform to obtain another decomposition, which is more natural and manageable.

3. Extension rings

$\mathbb{Z}_{p^e}$ is a local ring with maximal ideal $p\mathbb{Z}_{p^e}$ and residue field $\mathbb{Z}_p$. Let

$$\mu : \mathbb{Z}_{p^e}[X] \to \mathbb{Z}_p[X], \quad \mu(f) = f \pmod p$$

denote the ring homomorphism that maps f to $f \pmod p$.

Let m be a positive integer and let $GR(p^e, m) = \mathbb{Z}_{p^e}[X]/\langle h(X)\rangle$ be the Galois extension of degree m over $\mathbb{Z}_{p^e}$, called a *Galois ring*. Here $h(X)$ is a monic basic irreducible polynomial in $\mathbb{Z}_{p^e}[X]$ of degree m that divides $X^{p^m-1} - 1$, and it can be chosen so that $\zeta = X + \langle h(X)\rangle$ is a primitive $(p^m - 1)$th root of unity. $GR(p^e, m) = \mathbb{Z}_{p^e}[\zeta]$ is a local ring with maximal ideal $\langle p\rangle$ and residue field $\mathbb{F}_{p^m}$. In fact, $GR(p^e, m)$ is a finite chain ring since every ideal in $GR(p^e, m)$ has the form $\langle p^i\rangle$ for $0 \leqslant i \leqslant m$. We recall that the Galois extensions are unique and simple. The map μ naturally extends to the canonical projection

$$\begin{aligned}\mu : \mathbb{Z}_{p^e}[X]/\langle h(X)\rangle &\rightarrow \mathbb{Z}_p[X]/\langle \mu(h)(X)\rangle \simeq \mathbb{F}_{p^m},\\ f+\langle h(X)\rangle &\mapsto \mu(f)+\langle \mu(h)(X)\rangle.\end{aligned}$$

The set $\mathcal{T}_m = \{0, 1, \zeta, \ldots, \zeta^{p^m-2}\}$ is a complete set, known as Teichmüller set, of coset representatives of $GR(p^e, m)$ modulo $\langle p\rangle$. Any $a \in GR(p^e, m)$ can be uniquely written as a finite sum $a = a_0 + a_1 p + a_2 p^2 + \cdots + a_{e-1} p^{e-1}$ with $a_i \in \mathcal{T}_m$. Slightly abusing notation, we sometimes write $\mu(a) = a_0$. Note that a is a unit if and only if $\mu(a) \neq 0$ by the following lemma.

Lemma 3.1. *Suppose $a - b$ is nilpotent in a ring. Then a is a unit if and only if b is a unit.*

Elements of $GR(p^e, m)$ can also be written in the ζ-adic expansion $b_0 + b_1\zeta + \cdots + b_{m-1}\zeta^{m-1}$ with $b_i \in \mathbb{Z}_{p^e}$. The Galois group of isomorphisms of $GR(p^e, m)$ over $\mathbb{Z}_{p^e}$ is a cyclic group of order m generated by the Frobenius automorphism Fr given by

$$\mathtt{Fr}\left(\sum_{i=0}^{m-1} b_i\zeta^i\right) = \sum_{i=0}^{m-1} b_i\zeta^{ip} \quad (b_i \in \mathbb{Z}_{p^e}) \tag{7}$$

in ζ-adic expansion. We recall that $l \mid m$ if and only if $GR(p^e, l) \subset GR(p^e, m)$. Moreover, the Galois group of $GR(p^e, m)$ over $GR(p^e, l)$ is generated by $\mathtt{Fr}^l$ and hence

$$GR(p^e, l) = \{a \in GR(p^e, m) \mid \mathtt{Fr}^l(a) = a\}. \tag{8}$$

We denote by $\zeta_{[l]}$ the $(p^l - 1)$th root of unity $\zeta^{(p^m-1)/(p^l-1)}$.

Next, we define another extension ring

$$\mathcal{S} = \mathcal{S}_{p^e}(m, u) = GR(p^e, m)[u]/\langle u^{p^k} - 1\rangle \tag{9}$$

of $GR(p^e, m)$. For an appropriate m, this $\mathcal{S}$ will be the ambient space for codes of length p^k over the Galois ring which contains the nth root of unity. Note that

$$\mathcal{S} = \mathbb{Z}_{p^e}[\zeta][u]/\langle u^{p^k} - 1\rangle = \mathbb{Z}_{p^e}[u]/\langle u^{p^k} - 1\rangle[\zeta] = \mathcal{R}[\zeta].$$

Since $u^{p^k} - 1$ is monic, the division algorithm implies that every element s of $\mathcal{S}$ may be uniquely represented by a polynomial in $u - 1$ of degree less than p^k

$$s = s(u) = s_0 + s_1(u-1) + s_2(u-1)^2 + \cdots + s_{p^k-1}(u-1)^{p^k-1} \tag{10}$$

with $s_i \in GR(p^e, m)$. Note that $s_0 = s(1)$. The map μ naturally extends to $\mathcal{S} \to \mathcal{S}/p\mathcal{S}$ by the additional property $\mu(u) = u$. We also extend the Frobenius automorphism $\mathtt{Fr}$ to $\mathcal{S}$ by setting $\mathtt{Fr}(u) = u$. As usual, the trace map from $\mathcal{S}_{p^e}(m, u)$ to $\mathcal{R}$ is defined by

$$T_m(z) = \sum_{r=0}^{m-1} \mathtt{Fr}^r(z). \tag{11}$$

In passing, we warn that p remains prime in $GR(p^e, m)$, but it is no longer a prime in $\mathcal{S}$. The reason for this is that $GR(p^e, m)/\langle p \rangle = \mathbb{F}_{p^m}$ is a field, but $\mathcal{S}/p\mathcal{S} = \mathbb{F}_{p^m}[u]/\langle (u-1)^{p^k} \rangle$ is not an integral domain.

Theorem 3.2. *As before, we let* $\mathcal{R} = \mathbb{Z}_{p^e}[u]/\langle u^{p^k} - 1 \rangle$ *and* $\mathcal{S} = \mathbb{Z}_{p^e}[\zeta][u]/\langle u^{p^k} - 1 \rangle = \mathcal{R}[\zeta]$.

(i) $s \in \mathcal{S}$, *written as in* (10), *is a unit if and only if* $\mu(s_0) \neq 0$.
(ii) $\mathcal{S}$ *is a local ring with maximal ideal* $\langle p, u-1 \rangle$ *and residue field* $\mathbb{F}_{p^m}$.
(iii) $\mathcal{R}$ *is a local ring with maximal ideal* $\langle p, u-1 \rangle$ *and residue field* $\mathbb{Z}_p$.
(iv) $\mathcal{S}$ *is a Galois extension of* $\mathcal{R}$. *In particular, the set of elements in* $\mathcal{S}$ *fixed by* $\mathtt{Fr}$ *is* $\mathcal{R}$, *i.e.* $\mathcal{S}^{\mathtt{Fr}} = \{s \in \mathcal{S} \mid \mathtt{Fr}(s) = s\} = \mathcal{R}$.

Proof. (i) By Lemma 3.1, $s = x + py$ is a unit in $\mathcal{S}$ if and only if x is a unit in $\mathcal{S}$. If x is a unit in $\mathcal{S}$, then clearly $\mu(x)$ is a unit in $\mathcal{S}/p\mathcal{S}$. Conversely, if μx is a unit in $\mathcal{S}/p\mathcal{S}$, then $xx' = 1 + ps'$ for some $x', s' \in \mathcal{S}$ which implies that xx' is a unit in $\mathcal{S}$, and then x is a unit in $\mathcal{S}$. Hence s is a unit if and only if $\mu(s)$ is a unit. Note that $\mu(u-1) = u-1$ is nilpotent in $\mathcal{S}/p\mathcal{S}$. If $s = s_0 + (u-1)s'$ in the $(u-1)$-adic expansion, then $\mu(s) = \mu(s_0) + (u-1)\mu(s')$. Hence $\mu(s)$ is a unit in $\mathcal{S}/p\mathcal{S}$ if and only if $\mu(s_0)$ is a unit in $\mathcal{S}/p\mathcal{S}$ if and only if $\mu(s_0) \neq 0$.

(ii) As before $\mathcal{S}/p\mathcal{S} = \mathbb{F}_{p^m}[u]/\langle (u-1)^{p^k} \rangle$, and hence $\mathcal{S}/\langle p, u-1 \rangle \simeq \mathbb{F}_{p^m}$ is a field, which implies that $\langle p, u-1 \rangle$ is a maximal ideal. Furthermore, elements not in the ideal $\langle p, u-1 \rangle$ are exactly those elements s with $\mu(s_0) \neq 0$. By (i), they are exactly the units. Thus $\langle p, u-1 \rangle$ is the unique maximal ideal.

(iii) The proof is similar to (ii).

(iv) It follows from the fact that $\mathcal{S}$ is unramified, i.e. the maximal ideal of $\mathcal{S} = \mathcal{R}[\zeta]$ is generated by the maximal ideal of $\mathcal{R}$. □

4. Discrete Fourier transforms

From now on we fix m to be the order of p modulo n. Then $n \mid p^m - 1$ and hence the Galois ring $GR(p^e, m)$ contains a primitive nth root of unity $\zeta_n = \zeta^{(p^m-1)/n}$, where ζ is the $(p^m - 1)$th root of unity as before. Again we set $\mathcal{S} = \mathcal{S}_{p^e}(m, u) = \mathbb{Z}_{p^e}[\zeta][u]/\langle u^{p^k} - 1 \rangle$. As always, we identify vectors with polynomials.

Definition 4.1. Let $c = (c_j) \in \mathbb{Z}_{p^e}^N$. The *discrete Fourier transform* of c is the vector $\hat{c} = \big(\hat{c}_0, \hat{c}_1, \dots, \hat{c}_{n-1}\big) \in \mathcal{S}^n$, where

$$\hat{c}_i = \sum_{j=0}^{N-1} c_j u^j \zeta_n^{ij} = c(u\zeta_n^i)$$

for all integers i. The reciprocal polynomial of $\hat{c}(Z)$

$$\mathcal{M}_c(Z) = \sum_{i=0}^{n-1} \hat{c}_{n-i} Z^i \in \mathcal{S}^n$$

is called the *Mattson–Solomon polynomial* of c.

Let n' be the multiplicative inverse of n mod p^k, i.e. $nn' \equiv 1 \pmod{p^k}$. For each t, $0 \leqslant t \leqslant n-1$, we define a permutation π_t of the set $\{0, 1, \dots, p^k - 1\}$ as

$$\pi_t(\ell) \equiv (\ell - t)n' \pmod{p^k},$$

i.e. $\pi_t(t + \ell n) = \ell$. This permutation induces a $\mathbb{Z}_{p^e}$-isomorphism $\pi_t : \mathcal{S} \to \mathcal{S}$ given by

$$\pi_t\big(a_0 + a_1 u + \dots + a_{p^k-1} u^{p^k-1}\big) = a_0 u^{\pi_t(0)} + a_1 u^{\pi_t(1)} + \dots + a_{p^k-1} u^{\pi_t(p^k-1)},$$

where $a_j \in \mathbb{Z}_{p^e}[\zeta]$. For any $s = s(u) \in \mathcal{S}$, we have that

$$\pi_t s(u) = u^{-n't} s(u^{n'}), \quad \pi_t^{-1} s(u) = u^t s(u^n). \tag{12}$$

Theorem 4.2 (*Inversion formula*). *Let $c \in R^N$. Then c is recovered from $\mathcal{M}_c$ by*

$$c = \Psi\left(\frac{1}{n}\Big(\pi_0 \mathcal{M}_c(1), \pi_1 \mathcal{M}_c(\zeta_n), \pi_2 \mathcal{M}_c(\zeta_n^2), \dots, \pi_{n-1} \mathcal{M}_c(\zeta_n^{n-1})\Big)\right).$$

Proof. For $0 \leqslant t \leqslant n-1$, we have that

$$\begin{aligned}
\mathcal{M}_c(\zeta_n^t) &= \sum_{i=0}^{n-1} \hat{c}_i \zeta_n^{-it} = \sum_{i=0}^{n-1} \sum_{j=0}^{N-1} c_j u^j \zeta_n^{ij} \zeta_n^{-it} = \sum_{j=0}^{N-1} c_j u^j \sum_{i=0}^{n-1} \zeta_n^{i(j-t)} = n \sum_{\ell=0}^{p^k-1} c_{t+\ell n} u^{t+\ell n} \\
&= n\big(c_t u^t + c_{t+n} u^{t+n} + c_{t+2n} u^{t+2n} + \dots + c_{t+(p^k-1)n} u^{t+(p^k-1)n}\big) \\
&= n\pi_t^{-1}\big(c_t + c_{t+n} u + c_{t+2n} u^2 + \dots + c_{t+(p^k-1)n} u^{p^k-1}\big).
\end{aligned}$$

Here, we used the well-known fact that $\sum_{i=0}^{n-1} \zeta_n^{ij} = 0$ unless $j \equiv 0 \pmod{n}$. □

We make $\mathcal{S}^n$ into a ring by defining the product

$$A * B = (A_0B_0, A_1B_1, \dots, A_{n-1}B_{n-1})$$

for two elements $A = (A_0, A_1, \dots, A_{n-1})$, $B = (B_0, B_1, \dots, B_{n-1})$ in $\mathcal{S}^n$. $(\mathcal{S}^n, *)$ is not only a ring but also a $\mathbb{Z}_{p^e}$-algebra with componentwise addition and multiplication, and the obvious scalar multiplication $a(A_0, A_1, \dots, A_{n-1}) = (aA_0, aA_1, \dots, aA_{n-1})$.

It is easy to prove the following properties of the Mattson–Solomon polynomials.

Theorem 4.3. *Let $c, d \in \mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$. Then*

(i) $\mathcal{M}_0 = 0$ *and* $\mathcal{M}_1(Z) = \sum_{i=0}^{n-1} Z^i$.
(ii) $\mathcal{M}_{ac}(Z) = a\mathcal{M}_c(Z)$ *for* $a \in \mathbb{Z}_{p^e}$.
(iii) $\mathcal{M}_{c+d}(Z) = \mathcal{M}_c(Z) + \mathcal{M}_d(Z)$.
(iv) $\mathcal{M}_{cd}(Z) = \mathcal{M}_c(Z) * \mathcal{M}_d(Z)$.

We view $\mathcal{M}$ as a map $\mathcal{M} : \mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle \to \mathcal{S}^n$ sending c to $\mathcal{M}_c(Z)$. We would like to determine the image space of $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$ under this map. For all i, $0 \leqslant i \leqslant n-1$, we have that

$$\hat{c}_{ip} = \mathtt{Fr}(\hat{c}_i), \quad \mathcal{M}_{c,ip} = \mathtt{Fr}(\mathcal{M}_{c,i}), \tag{13}$$

where subscripts are calculated mod n. Let

$$\mathcal{A} = \{(A_0, A_1, \dots, A_{n-1}) \in \mathcal{S}^n \mid A_{ip} = \mathtt{Fr}(A_i) \text{ for all } i\}.$$

Then $\mathcal{A}$ is a $\mathbb{Z}_{p^e}$-subalgebra of $\mathcal{S}^n$.

Lemma 4.4. *Let $A(Z) = A_0 + A_1Z + \cdots + A_{n-1}Z^{n-1} \in \mathcal{S}[Z]/\langle Z^n - 1\rangle$ be a polynomial of degree less than n. If $A(\zeta_n^t) = 0$ for all $0 \leqslant t \leqslant n-1$, then $A(Z) = 0$.*

Proof. We have

$$\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta_n & (\zeta_n)^2 & \dots & (\zeta_n)^{n-1} \\ 1 & \zeta_n^2 & (\zeta_n^2)^2 & \dots & (\zeta_n^2)^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \zeta_n^{n-1} & (\zeta_n^{n-1})^2 & \dots & (\zeta_n^{n-1})^{n-1} \end{bmatrix} \begin{bmatrix} A_0 \\ A_1 \\ A_2 \\ \vdots \\ A_{N-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

The determinant of the Vandermonde matrix is $\prod_{0 \leqslant i < j \leqslant n-1}(\zeta_n^j - \zeta_n^i)$. Since each $\zeta_n^j - \zeta_n^i$ is a unit in $\mathcal{S}$, the Vandermonde determinant is also a unit in $\mathcal{S}$. Thus $A_i = 0$ for all i. □

We recall the cyclotomic cosets. Let $0 \leqslant i \leqslant \ell - 1$. The *p-cyclotomic coset* modulo ℓ which contains i is the set

$$cl_p(i, \ell) = \{i, ip, ip^2, \ldots, ip^{m_i - 1}\},$$

where m_i is the smallest positive integer such that $ip^{m_i} \equiv i \pmod{\ell}$. We have that $m_i = |cl_p(i, \ell)|$ and m_i divides $m_1 = m$.

Theorem 4.5. *The map $\mathcal{M} : \mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle \to \mathcal{A}$ is a $\mathbb{Z}_{p^e}$-algebra isomorphism.*

Proof. Theorem 4.2 and 4.3 together with (13) show that the map is a well-defined one-to-one $\mathbb{Z}_{p^e}$-algebra homomorphism. Thus it only remains to show that the map is surjective. Let $A = (A_0, A_1, \ldots, A_{n-1}) \in \mathcal{A}$ and $A(Z) = \sum_{i=0}^{n-1} A_i Z^i$. For $0 \leqslant t \leqslant n-1$,

$$A(\zeta_n^t) = \sum_{i=0}^{n-1} A_i \zeta_n^{ti} = \sum_{i \in I} \sum_{j \in cl_p(i,n)} A_j \zeta_n^{tj}.$$

Now note that

$$\mathtt{Fr}\left(\sum_{j \in cl_p(i,n)} A_j \zeta_n^{tj} \right) = \sum_{j \in cl_p(i,n)} \mathtt{Fr}(A_j) \zeta_n^{tjp} = \sum_{j \in cl_p(i,n)} A_{jp} \zeta_n^{tjp} = \sum_{j \in cl_p(i,n)} A_j \zeta_n^{tj},$$

which shows that $\sum_{j \in cl_p(i,n)} A_j \zeta_n^{tj} \in \mathcal{S}^{\mathtt{Fr}} = \mathcal{R}$. Thus $A(\zeta_n^t) \in \mathcal{R}$. Therefore

$$B = \frac{1}{n} \Big(\pi_0 A(1), \pi_1 A(\zeta_n), \pi_2 A(\zeta_n^2), \ldots, \pi_{n-1} A(\zeta_n^{n-1}) \Big) \in \mathcal{R}^n.$$

Set $c = \Psi(B)$. By Theorem 4.2, we then have $\mathcal{M}_c(\zeta_n^t) = A(\zeta_n^t)$ for all $0 \leqslant t \leqslant n-1$. Now the previous lemma shows that $\mathcal{M}_c(Z) = A(Z)$, and the proof is completed. □

Lemma 4.6. *Let I be a complete set of p-cyclotomic representatives modulo n. Then the map $(A_0, A_1, \ldots, A_{n-1}) \mapsto (A_i)_{i \in I}$ is a $\mathbb{Z}_{p^e}$-algebra isomorphism from $\mathcal{A}$ to $\bigoplus_{i \in I} \mathcal{S}_{p^e}(m_i, u)$.*

Proof. Any element $(A_0, A_1, \ldots, A_{n-1}) \in \mathcal{A}$ is completely determined by $(A_i)_{i \in I}$ by the property $A_{jp} = \mathtt{Fr}(A_j)$ for all j, which implies that $A_{ip^r} = \mathtt{Fr}^r(A_i)$ for $i \in I$ and $0 \leqslant r \leqslant m_i - 1$. In particular, $\mathtt{Fr}^{m_i}(A_i) = A_i$ for all $i \in I$ and thus $A_i \in \mathcal{S}^{\mathtt{Fr}^{m_i}} = \mathcal{S}_{p^e}(m_i, u)$. Now the rest of the assertion is clear. □

Theorem 4.5 and Lemma 4.6 give the following:

Theorem 4.7. *The map* $\gamma : \mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle \to \bigoplus_{i\in I} \mathcal{S}_{p^e}(m_i, u)$ *defined by* $\gamma(c) = (\hat{c}_i)_{i\in I}$ *is a* $\mathbb{Z}_{p^e}$*-algebra isomorphism: in particular, if* C *is an ideal of* $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$*, then* $C \simeq \bigoplus_{i\in I} C_i$*, where* C_i *is the ideal* $\{c(u\zeta_n^i) \mid c \in C\}$ *of* $\mathcal{S}_{p^e}(m_i, u)$*.*

Going back to the most general modulus and using the isomorphisms given in (2) and Theorem 4.7 we have the following:

Theorem 4.8. *Let* $M = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ *and let* C *be a cyclic code over* $\mathbb{Z}_M$ *of length* N*. Write* $N = p_i^{k_i} n_i$ *for each* $1 \leqslant i \leqslant r$*. Let* I_i *be the complete set of* p_i*-cyclotomic cosets modulo* n_i *and let* $m_{ij} = |cl_{p_i}(j, n_i)|$*. Then* $C \simeq \bigoplus_{i=1}^r \bigoplus_{j\in I_i} C_{ij}$*, where* $C_{ij} \subset \mathcal{S}_{p_i^{e_i}}(m_{ij}, u_i)$ *is the ideal* $\{c(u_i\zeta_n^j) \pmod{p_i^{e_i}} \mid c \in C\}$*.*

5. Polynomial representations

In this section, we shall compute the inverse map γ^{-1} to obtain the polynomial representation of the ideal in $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$. Given an element

$$(d_i)_{i\in I} \in \oplus_{i\in I} \mathcal{S}_{p^e}(m_i, u),$$

we obtain the corresponding element $d = (d_0, d_1, \dots, d_{n-1}) \in \mathcal{A}$, where $d_{ip^j} = \mathtt{Fr}^j(d_i)$. Let $A(Z) = \sum_{j=0}^{n-1} d_{n-j} Z^j$. The inverse image of $(d_i)_{i\in I}$ under γ is then

$$\gamma^{-1}((d_i)_{i\in I}) = \Psi\left(\frac{1}{n}\left(\pi_0 A(1), \pi_1 A(\zeta_n), \pi_2 A(\zeta_n^2), \dots, \pi_{n-1} A(\zeta_n^{n-1})\right)\right), \tag{14}$$

which is a element in $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$. We shall compute these inverse images in more detail. We fix an integer $i \in I$ and take an element $s \in \mathcal{S}_{p^e}(m_i, u)$. Consider the element

$$d_i(s) = (0, \dots, 0, s, 0, \dots, 0) \in \oplus_{j\in I} \mathcal{S}_{p^e}(m_j, u),$$

where s is the i-component. For notational convenience we let $F_{i,s}(X) = \gamma^{-1}(d_i(s))$. In other words, $F_{i,s}(X)$ is an element in $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$, such that

$$F_{i,s}(u\zeta_n^j) = \begin{cases} s & \text{if } j = i \\ 0 & \text{otherwise} \end{cases} \quad (j \in I).$$

We remark that each of these $F_{i,s}(X)$ is a generator for a minimal cyclic code.

Lemma 5.1. *Let $T_{m_i} : \mathcal{S}_{p^e}(m_i, u) \to \mathcal{R}$ be the trace map defined in* (11). *Then*

$$F_{i,s}(X) = \Psi\left(\frac{1}{n}\left(\pi_0 T_{m_i}(s), \pi_1 T_{m_i}(s\zeta_n^{-i}), \pi_2 T_{m_i}(s\zeta_n^{-2i}), \ldots, \pi_{n-1} T_{m_i}(s\zeta_n^{-(n-1)i})\right)\right).$$

Proof. It follows from (14), since we have

$$\begin{aligned} A(\zeta_n^t) &= \sum_{j=0}^{n-1} d_j \zeta_n^{-tj} = \sum_{j \in cl_p(i,n)} d_j \zeta_n^{-tj} = \sum_{r=0}^{m_i-1} \mathtt{Fr}^r(s)\zeta_n^{-tip^r} \\ &= \sum_{r=0}^{m_i-1} \mathtt{Fr}^r(s)\mathtt{Fr}^r(\zeta_n^{-it}) = \sum_{r=0}^{m_i-1} \mathtt{Fr}^r(s\zeta_n^{-it}) = T_{m_i}(s\zeta_n^{-it}). \qquad \Box \end{aligned}$$

The map $s \mapsto F_{i,s}(X)$ is a $\mathbb{Z}_{p^e}$-algebra homomorphism from $\mathcal{S}_{p^e}(m_i, u)$ to $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$ and hence $\gamma^{-1}((s_i)_{i \in I}) = \sum_{i \in I} F_{i,s_i}(X)$. Therefore, it is sufficient to compute $F_{i,s}(X)$ for $s = 1, u$ and $\zeta_{[m_i]} = \zeta^{(p^m-1)/(p^{m_i}-1)}$. Let

$$E_i(X) = F_{i,1}(X),$$

which will play an important role in the sequel. Let

$$\tau_{i,j} = T_{m_i}(\zeta_n^{-ij}), \quad \tau_{i,j}^* = T_{m_i}(\zeta_{[m_i]}\zeta_n^{-ij}).$$

Note that these are elements in $\mathbb{Z}_{p^e}$ and that $T_{m_i}(bs) = bT_{m_i}(s)$ for any $b \in \mathcal{R}$. Recall that $n'n \equiv 1 \pmod{p^k}$.

Lemma 5.2. (i) $E_i(X) = \frac{1}{n}\sum_{j=0}^{n-1} \tau_{i,j} X^{j(1-n'n)}$.

(ii) $F_{i,u}(X) = X^{nn'} E_i(X)$.

(iii) $F_{i,\zeta_{[m_i]}}(X) = \frac{1}{n}\sum_{j=0}^{n-1} \tau_{i,j}^* X^{j(1-n'n)}$.

Proof. For any constant polynomial $b \in \mathcal{R}$, we have that $\pi_t(b) = bu^{-n't}$ and $\pi_t(bu) = bu^{(1-t)n'}$. By Lemma 5.1 and (4), we have that

$$\begin{aligned} E_i(X) &= \Psi\left(\frac{1}{n}\left(\pi_0(\tau_{i,0}), \ldots, \pi_t(\tau_{i,t}), \ldots, \pi_{n-1}(\tau_{i,n-1})\right)\right) \\ &= \Psi\left(\frac{1}{n}\left(\tau_{i,0}, \ldots, \tau_{i,t}u^{-tn'}, \ldots, \tau_{i,n-1}u^{-(n-1)n'}\right)\right) = \frac{1}{n}\sum_{t=0}^{n-1} \tau_{i,t} X^{t(1-n'n)}, \end{aligned}$$

which proves (i). Secondly,

$$\begin{aligned}
F_{i,u}(X) &= \Psi\left(\frac{1}{n}\left(\pi_0(\tau_{i,0}u), \dots, \pi_t(\tau_{i,t}u), \dots, \pi_{n-1}(\tau_{i,n-1}u)\right)\right) \\
&= \Psi\left(\frac{1}{n}\left(\tau_{i,0}u^{n'}, \dots, \tau_{i,t}u^{(1-t)n'}, \dots, \tau_{i,n-1}u^{-nn'}\right)\right) \\
&= \frac{1}{n}\sum_{t=0}^{n-1}\tau_{i,t}X^{t+(1-t)n'n} = X^{nn'}\frac{1}{n}\sum_{t=0}^{n-1}\tau_{i,t}X^{t(1-n'n)} = X^{nn'}E_i(X).
\end{aligned}$$

Finally, a similar computation yields (iii). □

Since $\tau_{i,t} = \tau_{i,tp}$, we can write

$$E_i(X) = \frac{1}{n}\sum_{j\in I}\tau_{i,j}\varepsilon_j\left(X^{1-n'n}\right) \quad \text{with } \varepsilon_j(X) = \sum_{t\in cl_p(j,n)} X^t. \tag{15}$$

For any element $s = \sum_j \sum_k a_{jk}\zeta_{[m_i]}^k u^j \in \mathcal{S}_{p^e}(m_i, u)$ with $a_{jk} \in \mathbb{Z}_{p^e}$, we denote by

$$s\left(F_{i,\zeta_{[m_i]}}(X), X^{nn'}\right) = \sum_j \sum_k a_{jk}F_{i,\zeta_{[m_i]}}(X)^k\left(X^{nn'}\right)^j \in \mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle,$$

the polynomial obtained by substituting $\zeta_{[m_i]}$, u in s by $F_{i,\zeta_{[m_i]}}(X)$, $X^{nn'}$, respectively.

Theorem 5.3. $F_{i,s}(X) = s(F_{i,\zeta_{[m_i]}}(X), X^{nn'})E_i(X)$.

Proof. This follows from Lemma 5.2 together with the facts that $s \mapsto F_{i,s}$ is a $\mathbb{Z}_{p^e}$-algebra homomorphism and $E_i(X)F_{i,s}(X) = F_{i,s}(X)$. □

We introduce another inverse image, which is convenient for dealing with multiplication. For $s \in \mathcal{S}_{p^e}(m_i, u)$, let

$$d_i^*(s) = (1, \dots, 1, s, 1, \dots, 1) \in \oplus_{j\in I}\mathcal{S}_{p^e}(m_j, u),$$

where s is the i-component, and let $G_{i,s}(X) = \gamma^{-1}(d_i^*(s)) \in \mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$, i.e.

$$G_{i,s}(u\zeta_n^t) = \begin{cases} 1 & \text{if } t \neq i \\ s & \text{if } t = i \end{cases} \quad (t \in I). \tag{16}$$

Since $d_i^*(s) = (1, \ldots, 1) - d_i(1) + d_i(s)$, we have that

$$G_{i,s}(X) = 1 - E_i(X) + F_{i,s}(X). \tag{17}$$

Theorem 5.4. *Let $C_i \subset \mathcal{S}_{p^e}(m_i, u)$ be ideals for $i \in I$. Without loss of generality we may assume that C_i's have the form $C_i = \langle b_1 s_{i1}, b_2 s_{i2}, \ldots, b_l s_{il}\rangle$ with $b_j \in \mathbb{Z}_{p^e}$, independent of i, and $s_{ij} \in \mathcal{S}_{p^e}(m_i, u)$. Then*

$$\gamma^{-1}\left(\oplus_{i\in I} C_i\right) = \langle b_1 \prod_{i\in I} G_{i,s_{i1}}(X), b_2 \prod_{i\in I} G_{i,s_{i2}}(X), \ldots, b_l \prod_{i\in I} G_{i,s_{il}}(X)\rangle.$$

Proof. By (16), $b_j \prod_{i\in I} G_{i,s_{ij}}(u\zeta_n^t) = b_j s_{tj}$ for each $t \in I$ and for each $1 \leqslant j \leqslant l$. □

Theorem 5.4 and (17) provide us an explicit way of computing the generator polynomials of the corresponding ideal of $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$ to an ideal of $\oplus_i \mathcal{S}_i(m_i, u)$ whose generators are given.

The coefficients $\tau_{i,t}$ can be easily computed, once the minimal polynomials of ζ_n^t's are known. Since $(n, p^e) = 1$, $X^n - 1 \in \mathbb{Z}_{p^e}[X]$ factors into monic, basic irreducible polynomials in a unique way as $X^n - 1 = \prod_{i\in I} f_i$, where f_i is an irreducible polynomial over $\mathbb{Z}_{p^e}$ having ζ_n^i as a root. In fact, $f_i(X) = \prod_{j\in cl_p(i,n)}(X - \zeta_n^j)$. We call f_i the *minimal polynomial* of ζ_n^i over $\mathbb{Z}_{p^e}$.

Let $-a_j$ be the coefficient of $X^{m_j - 1}$ in $f_j(X)$. As is well-known, $a_j = T_{m_j}(\zeta_n^j)$. Suppose j is the representative of the p-cyclotomic coset of $-it$. Since $\zeta_n^{-it} \in \mathcal{S}(m_i, u)$, we have that $\zeta_n^j \in \mathcal{S}(m_i, u)$, which implies that $jp^{m_i} \equiv j \pmod{n}$. Since m_j is the smallest integer satisfying the congruence $jp^{m_j} \equiv j \pmod{n}$, we must have that $m_j \mid m_i$. Since $\mathtt{Fr}^{m_j}(s) = s$ for $s \in \mathcal{S}(m_j, u)$, we have that

$$T_{m_i}(\zeta_n^j) = \sum_{r=0}^{m_i - 1} \zeta_n^{jp^r} = \frac{m_i}{m_j} \sum_{r=0}^{m_j - 1} \zeta_n^{jp^r} = \frac{m_i}{m_j} T_{m_j}(\zeta_n^j) = \frac{m_i}{m_j} a_j. \tag{18}$$

The coefficients $\tau_{i,t}^*$ can be computed in a similar manner. We first note that

$$\tau_{i,t}^* = T_{m_i}(\zeta_{[m_i]}\zeta_n^{-it}) = T_{m_i}\left(\zeta_{[m_i]}^{1 - \frac{ip^{m_i} - i}{n} t}\right) = T_{m_i}\left(\zeta^{\frac{p^m - 1}{p^{m_i} - 1} - \frac{ip^m - i}{n} t}\right).$$

Let I_m be the complete set of representatives of the p-cyclotomic cosets modulo $p^m - 1$. Then the factorization $X^{p^m - 1} - 1 = \prod_{j\in I_m} \bar{\phi}_j(X)$ into monic irreducible coprime polynomials over $\mathbb{Z}_p$ lifts to the corresponding factorization $X^{p^m - 1} - 1 = \prod_{j\in I_m} \phi_j(X)$ over $\mathbb{Z}_{p^e}$, such that $\mu(\phi_j) = \bar{\phi}_j$ and $\phi_j(X) = \prod_{t\in cl_p(j, p^m - 1)}(X - \zeta^t)$ is the minimal polynomial of ζ^j over $\mathbb{Z}_{p^e}$. Let m_j' be the degree of ϕ_j, which is $|cl_p(j, p^m - 1)|$.

Then m'_j is the smallest integer, such that $\zeta^j \in \mathcal{S}(m'_j, u)$ and $-b_j = -T_{m'_j}(\zeta^j)$ is the coefficient of $X^{m'_j - 1}$ in $\phi_j(X)$. If $\zeta^j \in \mathcal{S}(m_i, u)$, then $\mathbb{Z}_{p^e}[\zeta^j] \subset \mathbb{Z}_{p^e}[\zeta_{[m_i]}]$ and hence $m'_j \mid m_i$ and

$$T_{m_i}(\zeta^j) = \frac{m_i}{m'_j} T_{m'_j}(\zeta^j) = \frac{m_i}{m'_j} b_j. \tag{19}$$

We could have used the factorization of $X^{p^{m_i}-1} - 1$ to compute $\tau^*_{i,t}$, but (19) works for all i.

We shall now relate $f_i(X)$ with certain $G_{i,s}(X)$. For two elements a, b in a ring, we write $a \sim b$ if $a = bv$ for some unit v.

Lemma 5.5. *Let $f_i(X)$ be the minimal polynomial of ζ_n^i over $\mathbb{Z}_{p^e}$.*

(i) $f_i(u\zeta_n^j) \sim 1$ if $j \notin cl_p(i, n)$.
(ii) $f_i(u\zeta_n^i) \sim u^n - 1 \sim u - 1$.

Proof. (i) $f_i(u\zeta_n^j) = \prod_{\ell \in cl_p(i,n)} (u\zeta_n^j - \zeta_n^\ell)$, and each factor $u\zeta_n^j - \zeta_n^\ell = (\zeta_n^j - \zeta_n^\ell) + \zeta_n^j(u-1)$ is a unit, since $\zeta_n^j - \zeta_n^\ell \neq 0$.

(ii) We have $X^n - 1 = \prod_j f_j(X)$. Thus $(u\zeta_n^i)^n - 1 = \prod_j f_j(u\zeta_n^i)$, or $u^n - 1 = \prod_j f_j(u\zeta_n^i)$. Since each $f_j(u\zeta_n^i)$ is a unit for $j \neq i$, $f_i(u\zeta_n^i) \sim u^n - 1$. Write $u^n - 1 = (u-1)s(u)$. Then $s(1) = n$. Since n is relatively prime to p, we have that $\mu(n) \neq 0$, which implies that $s(u)$ is a unit by Theorem 3.2(i), and hence $u^n - 1 \sim u - 1$. □

Theorem 5.6. *Let $f_i(X)$ be the minimal polynomial of ζ_n^i over $\mathbb{Z}_{p^e}$.*

(i) $f_i(X) \sim G_{i,u-1}(X) = 1 + (X^{nn'} - 2)E_i(X)$.
(ii) $f_i(X^{p^k}) \sim G_{i,0}(X) = 1 - E_i(X)$.

Proof. (i) By the Lemma 5.5, it is clear that $\gamma(f_i(X)) \sim d_i^*(u-1)$. Now $G_{i,u-1}(X) = 1 - E_i(X) + (X^{nn'} - 1)E_i(X) = 1 + (X^{nn'} - 2)E_i(X)$.

(ii) Recall that $f_i(X) = \prod_{r=0}^{m_i}(X - \zeta_n^{ip^r})$ and $\zeta_n^{jp^k} - \zeta_n^{ip^r} \neq 0$ is a unit for every r unless $j \in cl_p(i, n)$. Thus $f_i((u\zeta_n^j)^{p^k}) = f_i(\zeta_n^{jp^k})$ is a unit for $j \notin cl_p(i, n)$ and zero if $j \in cl_p(i, n)$. Therefore $f_i(X^{p^k}) \sim G_{i,0}(X) = 1 - E_i(X)$. □

In the next section, it is shown that the ideals of $\mathcal{S}_{p^e}(m, u)$ have the form

$$\langle s_0, ps_1, p^2 s_2, \ldots, p^{e-1} s_{e-1} \rangle,$$

where $s_i = 0$ or $s_i = (u-1)^{t_i} + pz_i$ with $0 \leqslant t_i < p^k - 1$ and $z_i \in \mathcal{S}_{p^e}(m, u)$. In [2,5], the generators of the corresponding ideals in $\mathbb{Z}_{p^e}[X]/\langle X^N - 1 \rangle$ are given in terms of $f_i(X)^t$, $f_i(X^{p^k})$ and $\tilde{f}_i(X) = f_i(X) + pg_i(X)$, which is called a *lift*, with

$g_i(X) \in \mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$. However the exact forms of the lifts are not studied. We can now describe their lifts in more detail by expressing $G_{i,(u-1)^t+pz}$ in terms of $f_i(X)$. Recall that $G_{i,u-1}(X) \sim f_i(X)$, say $G_{i,u-1}(X)H_i(X) = f_i(X)$ for some unit $H_i(X)$. Thus we have that

$$G_{i,(u-1)^t+pz}(X) = G_{i,(u-1)^t}(X) + pF_{i,z}(X) \sim f_i(X)^t + pH_i(X)^t F_{i,z}(X). \tag{20}$$

To determine $H_i(X)$, let $\gamma(H_i) = (s_j)_{j\in I}$ and apply γ to $G_{i,u-1}(X)H_i(X) = f_i(X)$ to obtain

$$s_j = f_i(u\zeta_n^j)\text{for } j \neq i \quad (u-1)s_i = f_i(u\zeta_n^i).$$

Although $u-1$ is not a unit, we can still take $s_i = f_i(u\zeta_n^i)/(u-1)$ since $f_i(\zeta_n^i) = 0$ so that $u-1$ divides $f_i(u\zeta_n^i)$. Therefore

$$H_i(X) = \sum_{j\in I-\{i\}} F_{j, f_i(u\zeta_n^j)} + F_{i, f_i(u\zeta_n^i)/(u-1)}. \tag{21}$$

Hence the lifts of $f_i(X)$ can be explicitly given by (20).

Recall that the multiplication of the ring $\mathcal{A}$ is the componentwise multiplication. Hence, it is quite natural that the idempotent elements in $\mathcal{A}$ are rather easy to determine, while those in $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$ are not. However, the isomorphism γ will be of great help in this matter. Recall that $E_i(X) = \gamma^{-1}(0,\dots,0,1,0,\dots,0)$, where 1 is the i-component.

Theorem 5.7. *Let $R_N = \mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$.*

(i) *Each E_i is idempotent, i.e. $E_i^2 = E_i$.*
(ii) *$E_iE_j = 0$ for $i \neq j$, and $\sum_{i\in I} E_i = 1$.*
(iii) *The only idempotents in R_N are $\sum_{j\in J} E_j$ for some subset J of I. In particular, there are $2^{|I|}$ idempotent elements in R_N.*
(iv) *R_N is a direct sum of the ideals $\langle E_i\rangle$:*

$$R_N = \bigoplus_{i\in I} \langle E_i\rangle \simeq \bigoplus_{i\in I} R_N/\langle 1 - E_i\rangle. \tag{22}$$

Proof. (i) and (ii) follow from the fact that γ is an isomorphism.

(iii) In a local ring, the only idempotents are 0 and 1. Indeed, if a is an idempotent which is different from 0 and 1, then $a(1-a) = 0$ shows that a and $1-a$ are nonunits, which implies that $1 = a + (1-a)$ is in the maximal ideal consisting of nonunits, a contradiction. Since each $\mathcal{S}_{p^e}(m_i, u)$ is a local ring, the only idempotents in $\oplus\mathcal{S}_{p^e}(m_i, u)$ are $(a_i)_{i\in I}$, where $a_i = 0$ or 1. Take $J = \{j \in I \mid a_j = 1\}$.

(iv) The decomposition follows from (ii). Consider the homomorphism $R_N \to \langle E_i \rangle$ mapping f to $E_i f$. If $E_i f = 0$, then $f = (1 - E_i)f + E_i f = (1 - E_i)f$. Thus, the kernel of the map is $\langle 1 - E_i \rangle$ and $R_N / \langle 1 - E_i \rangle \simeq \langle E_i \rangle$. □

Corollary 5.8. *Let $N = p^k n$ as before and let $X^n - 1 = \prod_{i \in I} f_i(X)$ be the factorization into monic, basic irreducible, coprime polynomials over $\mathbb{Z}_{p^e}$. Then*

(i)
$$\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle \simeq \bigoplus_{i \in I} \mathbb{Z}_{p^e}[X]/\langle f_i(X^{p^k})\rangle. \tag{23}$$

(ii) *Any ideal C of $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$ having an idempotent generator has the form $\langle f(X^{p^k})\rangle$ for some divisor $f(X)$ of $X^n - 1$. If $f(X) = \prod_{j \in J} f_j(X)$, then the unique idempotent generator of C is $\sum_{j \notin J} E_j$. Furthermore, C is isomorphic to $\oplus_{j \notin J} \mathcal{S}_{p^e}(m_j, u)$.*

Proof. (i) This follows from Theorem 5.6(ii) and 5.7(iv).

(ii) We know that the only idempotents are $\sum_{j \in J} E_j$ for some subset J of I. Note that $\sum_{j \in J} E_j = 1 - \sum_{j \notin J} E_j = \prod_{j \notin J}(1 - E_j) \sim \prod_{j \notin J} f_j(X^{p^k})$. Replacing J with its complement, we obtain the result. □

We are now in good position to examine the isomorphism (6) more closely. Let $v = u^{n'} \in \mathcal{R}$ so that $v^n = u^{nn'} = u$. It is easy to see that the factorization given in (5) is exactly $X^n - u = \prod_{i \in I} g_i$, where $g_i(X) = \prod_{j \in cl_p(i,n)}(X - v\zeta_n^j) \in \mathcal{R}[X]$. Recalling that $\Psi(u^j X^i) = X^{i+jn}$, we have that

$$\Psi(g_i)(X) = \prod_{j \in cl_p(i,n)} (X - X^{n'n}\zeta_n^j) \in \mathbb{Z}_{p^e}[X].$$

We compute $\Psi(g_i)(u\zeta_n^j)$ to find its image on $\oplus_{i \in I} \mathcal{S}_{p^e}(m_i, u)$:

$$\Psi(g_i)(u\zeta_n^j) = \prod_{\ell \in cl_p(i,n)} (u\zeta_n^j - u\zeta_n^\ell) = u^{m_i} \prod_{\ell \in cl_p(i,n)} (\zeta_n^j - \zeta_n^\ell) = \begin{cases} 0 & \text{if} j \in cl_p(i,n), \\ \text{a unit} & \text{if } j \notin cl_p(i,n). \end{cases}$$

This means that $\Psi(g_i)(X) \sim G_{i,0}(X) = 1 - E_i(X)$ and hence Ψ induces an isomorphism

$$\mathcal{R}[X]/\langle g_i \rangle \simeq R_N / \langle 1 - E_i \rangle, \tag{24}$$

where $R_N = \mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$. Collecting previous isomorphisms, we have that

$$\mathcal{R}[X]/\langle g_i \rangle \simeq R_N/\langle 1 - E_i \rangle \simeq \langle E_i \rangle \simeq \mathcal{S}_{p^e}(m_i, u) \simeq \mathbb{Z}_{p^e}[X]/\langle f_i(X^{p^k}\rangle. \tag{25}$$

Hence the factorizations in (6), (22), (23) and Theorem 4.7 are all equivalent. However, we find that $\mathcal{S}_{p^e}(m_i, u)$ is most convenient to describe the structures and ideals.

Example 5.9. We consider the case $p = 2$ and $n = 15$. We have $cl_2(0, 15) = \{0\}$, $cl_2(1, 15) = \{1, 2, 4, 8\}$, $cl_2(3, 15) = \{3, 6, 12, 9\}$, $cl_2(5, 15) = \{5, 10\}$, and $cl_2(7, 15) = \{7, 14, 13, 11\}$. Thus $I = \{0, 1, 3, 5, 7\}$ and

$$\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle \simeq \mathcal{S}_{p^e}(1,u) \oplus \mathcal{S}_{p^e}(4,u) \oplus \mathcal{S}_{p^e}(4,u) \oplus \mathcal{S}_{p^e}(2,u) \oplus \mathcal{S}_{p^e}(4,u).$$

Since $m = 4$, we have that $\zeta = \zeta_{[4]} = \zeta_{15} = \zeta_n$.

Let $e = 2$ and $k = 1$, so that $N = 2 \cdot 15 = 30$. Then $n' = 1$ and $1 - nn' = -14 \equiv 16 \pmod N$. Recall that $\varepsilon_j(X) = \sum_{t \in cl_p(j,n)} X^t$, so that $\varepsilon_0(X) = 1$, $\varepsilon_1(X) = X + X^2 + X^4 + X^8$, etc. The irreducible polynomial of the primitive element $\bar{\zeta}$ over $\mathbb{Z}_2$ is $\bar{f}_1(X) = X^4 + X + 1$, which lifts to $f_1(X) = X^4 + 2X^2 + 3X + 1 \in \mathbb{Z}_4[X]$ by Hensel's Lemma [8,10]. Thus we choose $\zeta = X + \langle f_1(X)\rangle$. We know that $X^{15} - 1$ has the factorization of the form $X^{15} - 1 = f_0(X) f_1(X) f_3(X) f_5(X) f_7(X)$ over $\mathbb{Z}_4$ where $f_i(X)$ is the irreducible polynomial of ζ^i of degree m_i over $\mathbb{Z}_4$. To obtain this factorization, we first factor $X^{15} - 1$ over $\mathbb{Z}_2$ as

$$X^{15} - 1 = (X + 1)(X^2 + X + 1)(X^4 + X + 1)(X^4 + X^3 + 1)(X^4 + X^3 + X^2 + X + 1)$$

and then lift over $\mathbb{Z}_4$ as

$$\begin{aligned} X^{15} - 1 = {} & (X + 3)(X^2 + X + 1)(X^4 + 2X^2 + 3X + 1)(X^4 + 3X^3 + 2X^2 + 1) \\ & \times (X^4 + X^3 + X^2 + X + 1). \end{aligned}$$

It is not difficult to find $f_0(X) = X + 3$, $f_3(X) = X^4 + X^3 + X^2 + X + 1$, $f_5(X) = X^2 + X + 1$, and $f_7(X) = X^4 + 3X^3 + 2X^2 + 1$. By (18) and from the fact that $\frac{1}{n} \pmod 4 = 3$, we obtain

$$\begin{pmatrix} E_0(X) \\ E_1(X) \\ E_3(X) \\ E_5(X) \\ E_7(X) \end{pmatrix} = 3 \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 3 & 2 & 0 \\ 0 & 3 & 3 & 0 & 3 \\ 2 & 3 & 2 & 3 & 3 \\ 0 & 0 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} \varepsilon_0(X^{16}) \\ \varepsilon_1(X^{16}) \\ \varepsilon_3(X^{16}) \\ \varepsilon_5(X^{16}) \\ \varepsilon_7(X^{16}) \end{pmatrix}.$$

Explicitly the polynomials $E_i(X)$ are

$$E_0(X) = 3\sum_{t=0}^{14} X^{2t},$$

$$E_1(X) = 3(X^2 + X^4 + 3\,X^6 + X^8 + 2\,X^{10} + 3\,X^{12} + X^{16} + 3\,X^{18} + 2\,X^{20} + 3\,X^{24}),$$

$$\begin{aligned}
E_3(X) &= 3(3X^2+3X^4+3X^6+3X^8+3X^{12}+3X^{14}+3X^{16}\\
&\quad +3X^{18}+3X^{22}+3X^{24}+3X^{26}+3X^{28}),\\
E_5(X) &= 3(2+3X^2+3X^4+2X^6+3X^8+3X^{10}+2X^{12}+3X^{14}\\
&\quad +3X^{16}+2X^{18}+3X^{20}+3X^{22}+2X^{24}+3X^{26}+3X^{28}),\\
E_7(X) &= 3(3X^6+2X^{10}+3X^{12}+X^{14}+3X^{18}+2X^{20}+X^{22}\\
&\quad +3X^{24}+X^{26}+X^{28}).
\end{aligned}$$

Recall that these E_i's determine all 2^5 idempotents of $\mathbb{Z}_{p^e}[X]/\langle X^N-1\rangle = \mathbb{Z}_4[X]/\langle X^{30}-1\rangle$. Furthermore, $F_{i,u}(X) = X^{15}E_i(X)$. Keeping $\zeta_{[0]}=1$, $\zeta_{[4]}=\zeta$ and $\zeta_{[2]}=\zeta^5$ in mind, and using (19), we similarly find that

$$\begin{aligned}
F_{0,1}(X) &= E_0(X),\\
F_{1,\zeta}(X) &= 3(X^2+3X^4+2X^6+3X^{10}+X^{18}+X^{20}+3X^{22}+X^{24}\\
&\quad +2X^{26}+3X^{28}),\\
F_{3,\zeta}(X) &= 3(2X^2+X^6+X^8+2X^{12}+X^{16}+X^{18}+2X^{22}+X^{26}+X^{28}),\\
F_{5,\zeta^5}(X) &= 3(3+3X^2+2X^4+3X^6+3X^8+2X^{10}+3X^{12}+3X^{14}+2X^{16}\\
&\quad +3X^{18}+3X^{20}+2X^{22}+3X^{24}+3X^{26}+2X^{28}),\\
F_{7,\zeta}(X) &= 3(3X^4+2X^8+3X^{10}+X^{12}+3X^{16}+2X^{18}+X^{20}\\
&\quad +3X^{22}+X^{24}+X^{26}).
\end{aligned}$$

Now the generators for the corresponding ideals of R_N can be explicitly found using these polynomials. For example, take the ideal

$$C = \langle 1\rangle \times \langle 2(u-1)\rangle \times \langle u-1+2\zeta\rangle \times \langle u-1,2\rangle \times \langle 0\rangle \subset \oplus_{i\in I}\mathcal{S}_4(m_i,u).$$

Write each factor ideal in the form $C_i = \langle s_{i1}, 2s_{i2}\rangle$ for $i \in I$. By Theorem 5.4, this ideal corresponds to the ideal

$$C = \langle G_{0,1}G_{1,0}G_{3,u-1+2\zeta}G_{5,u-1}G_{7,0},\, 2G_{0,0}G_{1,u-1}G_{3,0}G_{5,1}G_{7,0}\rangle$$

of $\mathbb{Z}_{p^e}[X]/\langle X^N-1\rangle$. This gives an explicit polynomial representation of the ideal.

To compare with the generators given in [2], we recall that $G_{i,0}(X) \sim f_i(X^2)$, $G_{i,1}(X)=1$ and $G_{i,u-1}(X) \sim f_i(X)$. Thus

$$C = \langle f_1(X^2)G_{3,u-1+2\zeta}(X)f_5(X)f_7(X^2),\, 2f_0(X^2)f_1(X)f_3(X^2)f_7(X^2)\rangle. \tag{26}$$

As before, $G_{3,u-1+2\zeta}(X) = G_{3,u-1}(X) + 2F_{3,\zeta}(X) \sim f_3(X) + 2H_3(X)F_{3,\zeta}(X)$. Using the notation as in [2], we let $\tilde{f_3}(X) = f_3(X)+2H_3(X)F_{3,\zeta}(X)$. According to the recipe in (21), we find that

$$\begin{aligned} H_3(X) = {} & 1 + 3\,X^3 + 3\,X^4 + 2\,X^5 + 2\,X^6 + X^7 + X^8 + 3\,X^{11} + 3\,X^{12} \\ & +2\,X^{13} + 2\,X^{14} + 2\,X^{15} + 2\,X^{16} + X^{17} + X^{18} + 3\,X^{21} \\ & +3\,X^{22} + 2\,X^{23} + 2\,X^{24} + 2\,X^{25} + 2\,X^{26} + X^{27} + X^{28}. \end{aligned}$$

Replacing $G_{3,u-1+2\zeta}(X)$ by $\tilde{f_3}(X)$ in (26), we obtain the explicit polynomial representation of C in terms of the minimal polynomials.

6. Ideals of $\mathcal{S}_{p^e}(m,u)$

In this section we classify ideals of $\mathcal{S}_{p^e}(m,u) = \mathbb{Z}_{p^e}[\zeta][u]/\langle u^{p^k} - 1\rangle$. To emphasize the underlying ring $\mathbb{Z}_{p^e}$, we temporarily write $\mathcal{S}_{p^e}$ for $\mathbb{Z}_{p^e}[\zeta][u]/\langle u^{p^k} - 1\rangle$ (m and k are fixed).

Note that $\mathcal{S}_{p^e}$ is an ambient space for cyclic codes of length p^k over $\mathbb{Z}_{p^e}[\zeta]$. For any code C over the local ring $\mathbb{Z}_{p^e}[\zeta]$, we introduce the following torsion codes over the residue field $\mathbb{Z}_{p^e}[\zeta]/p\mathbb{Z}_{p^e}[\zeta] = \mathbb{F}_{p^m}$ by reading the elements of $\mathcal{S}_{p^e}$ modulo p.

Definition 6.1. Let C be a code of length l over the local ring $\mathbb{Z}_{p^e}[\zeta]$. For $0 \leqslant i \leqslant e-1$, define

$$Tor_i(C) = \{\mu(v) \mid p^i v \in C,\ \ v \in \mathbb{Z}_{p^e}[\zeta]^l\}. \tag{27}$$

$Tor_i(C)$ is called the ith *torsion code* of C. $Tor_0(C) = \mu(C)$ is usually called the *residue code* and sometimes denoted by $Res(C)$.

Let us view elements of $\mathbb{F}_{p^m} = S/pS$ as elements of S. Then

$$v_0 \in Tor_i(C) \iff p^i(v_0 + pz) \in C \text{ for some } z \in \mathbb{Z}_{p^e}[\zeta]^l.$$

Moreover, it is clear that $Tor_i(C) \subset Tor_{i+1}(C)$.

One use for torsion codes is for computing the size of the code. If C is the code with generator matrix of the standard form

$$\begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & \dots & A_{0,e-1} \\ 0 & pI_{k_1} & pA_{1,2} & \dots & pA_{1,e-1} \\ 0 & 0 & p^2 I_{k_2} & \dots & p^2 A_{2,e-1} \\ \vdots & & & & \\ 0 & 0 & \dots & p^{e-1} I_{k_{e-1}} & p^{e-1} A_{e-1,e-1} \end{pmatrix}, \tag{28}$$

the code $Tor_i(C)$ is the code over $\mathbb{F}_{p^m}$ generated by

$$\mu\begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & \dots & A_{0,e-1} \\ 0 & I_{k_1} & A_{1,2} & \dots & A_{1,e-1} \\ \vdots & & & & \\ 0 & 0 & \dots & I_{k_i} & A_{i,e-1} \end{pmatrix}. \tag{29}$$

Note that $|\mathbb{Z}_{p^e}[\zeta]| = p^{me}$ and $|p^j\mathbb{Z}_{p^e}[\zeta]| = p^{m(e-j)}$ for $0 \leqslant j \leqslant e$ in general. We can compute the cardinality of C with generator matrix as in (28) in general by

$$|C| = \prod_{j=0}^{e-1} |p^j\mathbb{Z}_{p^e}[\zeta]|^{k_j} = p^{m\sum_{j=0}^{e-1}(e-j)k_j}.$$

But, by (29) we have that $|Tor_i(C)| = \prod_{j=0}^{i} p^{mk_j}$, which gives

$$\prod_{i=0}^{e-1} |Tor_i(C)| = \prod_{i=0}^{e-1}\prod_{j=0}^{i} p^{mk_j} = p^{m\sum_{i=0}^{e-1}\sum_{j=0}^{i}k_j} = p^{m\sum_{j=0}^{e-1}(e-j)k_j} = |C|.$$

This gives the following:

Theorem 6.2. *For a code C over $\mathbb{Z}_{p^e}[\zeta]$, we have that*

$$|C| = \prod_{i=0}^{e-1} |Tor_i(C)|.$$

For any integer $1 \leqslant j \leqslant e-1$, let $\mu_j : \mathbb{Z}_{p^e} \to \mathbb{Z}_{p^j}$ be the canonical map sending a to $a \pmod{p^j}$. For convenience we view elements of $\mathbb{Z}_{p^j}$ as elements of $\mathbb{Z}_{p^e}$ for $j < e$. If C is a code over $\mathbb{Z}_{p^e}[\zeta]$, then $\mu_j(C)$ is a code over $\mathbb{Z}_{p^j}[\zeta]$ such that for any $c \in \mu_j(C)$, there exists some w such that $c + p^j w \in C$. Note that $\mathbb{Z}_{p^j}[\zeta]/p\mathbb{Z}_{p^j}[\zeta] = \mathbb{F}_{p^m}$ for any j.

Lemma 6.3. *Let C be a code over $\mathbb{Z}_{p^e}[\zeta]$. Then $Tor_i(C) = Tor_i(\mu_j(C))$ for all $j > i$.*

Proof. Suppose $v_0 \in Tor_i(C)$. Then there exists some z such that $p^i(v_0 + pz) \in C$. Hence $\mu_j(p^i(v_0 + pz)) = p^i(v_0 + p\mu_j(z)) \in \mu_j(C)$, which implies that $\mu(v_0 + p\mu_j(z)) = v_0 \in Tor_i(\mu_j(C))$. Conversely, suppose that $v_0 \in Tor_i(\mu_j(C))$, i.e. $p^i(v_0 + pz) \in \mu_j(C)$ for some z. Then $p^i(v_0 + pz) + p^j w \in C$ for some w, which implies that $v_0 \in Tor_i(C)$. □

Suppose C is an ideal of $\mathcal{S}_{p^e}(m,u)$. Then $Tor_i(C) = \langle (u-1)^j \rangle$ for some j, since any ideal of $\mathbb{F}_{p^m}[u]/\langle (u-1)^{p^k}\rangle$ has such form. The following lemma is somewhat useful when we compute the torsion codes.

Lemma 6.4. *Let $0 \leqslant i \leqslant e-1$ and $0 \leqslant j \leqslant p^k - 1$.*

(i) *If $g(u) \in \mathbb{Z}_{p^e}[\zeta][u]$, such that $\deg g(u) < p^k$ and $p^i g(u) = 0$ in $\mathbb{Z}_{p^e}[\zeta][u]/\langle u^{p^k} - 1\rangle$, then $g(u) = p^{e-i}h(u)$ for some $h(u) \in \mathbb{Z}_{p^e}[\zeta][u]$.*

(ii) *If $f(u) \in \mathbb{F}_{p^m}[u]$, such that $(u-1)^j f(u) = 0$ in $\mathbb{F}_{p^m}[u]/\langle (u-1)^{p^k}\rangle$, then $f(u) = (u-1)^{p^k - j} f_1(u)$ for some $f_1(u) \in \mathbb{F}_{p^m}[u]$.*

Proof. (i) Write $g(u) = \sum_{t=0}^{p^k-1} g_t(u-1)^t$ with $g_t \in \mathbb{Z}_{p^e}[\zeta]$. Then $p^i g(u) = \sum_{t=0}^{p^k-1} p^i g_t(u- \ 1)^t = 0$, which implies $p^i g_t = 0$ in $\mathbb{Z}_{p^e}[\zeta]$ for every t, which implies that $g_t = p^{e-i}h_t$. Now set $h = \sum_{t=0}^{p^k-1} h_t(u-1)^t$.

(ii) If $(u-1)^j f(u) = 0$ in $\mathbb{F}_{p^m}[u]/\langle (u-1)^{p^k}\rangle$, there exists a polynomial $f_1(u) \in \mathbb{F}_{p^m}[u]$ such that $(u-1)^j f(u) = f_1(u)(u-1)^{p^k}$ in $\mathbb{F}_{p^m}[u]$, which implies that $f(u) = (u-1)^{p^k-j} f_1(u)$. □

As a corollary, we obtain that

$$\left|\langle (u-1)^j \rangle\right| = p^{m(p^k - j)} \tag{30}$$

for $0 \leqslant j \leqslant p^k - 1$. Therefore, once we find all torsion codes $Tor_i(C)$ of an ideal C, it is straightforward to find the cardinality of C.

Theorem 6.5. *Any ideal C of $\mathcal{S}_{p^e} = \mathbb{Z}_{p^e}[\zeta][u]/\langle u^{p^k} - 1\rangle$ has the form*

$$C = \langle s_0, ps_1, \ldots, p^{e-1}s_{e-1}\rangle, \tag{31}$$

such that

(i) *either $s_j = 0$, or $s_j = (u-1)^{t_j} + pz_j$ for some $z_j \in \mathcal{S}_{p^e}$ and $0 \leqslant t_j < p^k$,*
(ii) *$s_j \neq 0$ if and only if $Tor_j(C) \neq \{0\}$ and $Tor_j(C) \neq Tor_{j-1}(C)$,*
(iii) *if $s_j \neq 0$, then $Tor_j(C) = \langle (u-1)^{t_j}\rangle$.*

In particular, the set $\{j \mid s_j \neq 0\}$ is uniquely determined by C and the partial sequence $\{t_j\}_{s_j \neq 0}$ is strictly decreasing.

Proof. We prove this by induction on e. Assume $e = 1$. The ring in this case is $\mathcal{S}_{p^1} = \mathbb{Z}_p[\zeta][u]/\langle u^{p^k} - 1\rangle = \mathbb{F}_{p^m}[u]/\langle u^{p^k} - 1\rangle = \mathbb{F}_{p^m}[u]/\langle (u-1)^{p^k}\rangle$. Since $\mathbb{F}_{p^m}$ is a field, ideals of $\mathcal{S}_{p^1}$ have the form $\langle (u-1)^{t_0}\rangle$ for some $0 \leqslant t_0 \leqslant p^k$. If $t_0 = p^k$, then $(u-1)^{p^k} \equiv u^{p^k} - 1 \equiv 0 \pmod p$, so in this case we take $s_0 = 0$. Thus the statement is true for $e = 1$.

Now suppose that any ideal of $\mathcal{S}_{p^e}$ has the form given in (31) and an ideal C of $\mathcal{S}_{p^{e+1}}$ is given. Clearly $\mu_e(C)$ is an ideal of $\mathcal{S}_{p^e}$, and hence, by the induction hypothesis, $\mu_e(C)$ has the form $\langle s_0', ps_1', \ldots, p^{e-1}s_{e-1}'\rangle$ satisfying the conditions (i)–(iii) in the theorem. If $s_j' = 0$, we take $s_j = 0$. If $s_j' \neq 0$, then we take any element $s_j = (u-1)^{t_j} + pz_j$ in $\mathcal{S}_{p^{e+1}}$ such that $p^j s_j \in C$ and $\mu_e(p^j s_j) = p^j s_j'$. Such an element exists since C contains an element of the form $p^j s_j' + p^e y_j = p^j((u-1)^{t_j} + pz_j)$ with $z_j = z_j' + p^{e-j-1}y_j \in \mathcal{S}_{p^{e+1}}$.

By Lemma 6.3 we have that $Tor_j(C) = Tor_j(\mu_e(C))$, and hence every s_j, $0 \leqslant j \leqslant e-1$, satisfies the conditions in the theorem.

Now $Tor_e(C)$ is an ideal of $\mathbb{F}_{p^m}[u]/\langle (u-1)^{p^k}\rangle$, say $\langle (u-1)^{t_e}\rangle$ for some $1 \leqslant t_e \leqslant p^k$. We take $s_e = (u-1)^{t_e}$. We claim that $C = \langle s_0, ps_1, \ldots, p^e s_e\rangle$. First of all, there exists an element $v \in Tor_e(C)$ such that $v \equiv (u-1)^{t_e} \pmod p$, which implies that $p^e(u-1)^{t_e} \in C$. Hence $\langle s_0, ps_1, \ldots, p^e s_e\rangle \subset C$. Conversely, suppose $c \in C$. Then $\mu_e(c) = \sum_{i=0}^{e-1} x_i' p^i s_i'$ for some $x_i' \in \mathcal{S}_{p^e}$. Since $p^j s_j' = p^j s_j - p^e y_j$ for $j < e$, we have that $c = \sum_{i=0}^{e-1} x_i p^i s_i + p^e x$ for some $x_i, x \in \mathcal{S}_{p^{e+1}}$. Then $x \in Tor_e(C)$, and hence $x \equiv b(u-1)^{t_e} \pmod p$ for some $b \in \mathcal{S}_{p^1}$, which implies that $c \in \langle s_0, ps_1, \ldots, p^e s_e\rangle$. Thus, we have shown that $C = \langle s_0, ps_1, \ldots, p^e s_e\rangle$ as claimed.

Notice that if $s_e = (u-1)^{p^k} = 0$, then C itself has to be $\{0\}$ and then the theorem is clear. So assume that $C \neq \{0\}$ so that $s_e \neq 0$. If $s_j = 0$ for all $j < e$, then again we are done. So assume that $s_j \neq 0$ for some j. Let $Tor_{e-1}(C) = \langle (u-1)^t\rangle$. It is clear that $t_e \leqslant t$ since $Tor_i(C) \subset Tor_{i+1}(C)$ for any i. If $t_e < t$, then we are done. Suppose $t_e = t$. There exists some $l \leqslant e-1$ such that $s_l = (u-1)^t + pz_l$. Then $p^e s_e = p^e(u-1)^{t_e} = p^{e-l}p^l(u-1)^t = p^{e-l}p^l s_l$, which implies that $C = \langle s_0, ps_1, \ldots, p^e s_e\rangle = \langle s_0, ps_1, \ldots, p^{e-1}s_{e-1}\rangle$. We replace s_e with 0 in this case. In any case s_e satisfies the conditions in the theorem.

Clearly the set $\{j \mid s_j \neq 0\}$ is uniquely determined by (ii), and the partial sequence $\{t_j\}_{s_j \neq 0}$ is strictly decreasing since $Tor_{j-1}(C) \subsetneqq Tor_j(C) = \langle (u-1)^{t_j}\rangle$ when $s_j \neq 0$. The proof is completed. □

Definition 6.6. The representation of C in terms of the generators as in the theorem is called the *torsional form*. If $Tor_j(C) = \langle (u-1)^{t_j}\rangle$, then t_j is called the jth *torsional degree* of C and denoted by $tdeg_j(C)$ (if $Tor_j(C) = 0$, then $tdeg_j(C) = p^k$). The partial sequence $\{t_j\}_{s_j \neq 0}$ is called the *reduced* sequence of torsional degrees and written as $\{(t_j)_j\}_{s_j \neq 0}$.

Note that the reduced sequence is simply the sequence of t_j's which are actually appearing in the torsional form. For example, if $C = \langle (u-1)^5, p^3((u-1)^3 + pz_3), p^4((u-1) + pz_4)\rangle$, then the reduced sequence is $5_0, 3_3, 1_4$.

The sequence of the torsional degrees completely determines the reduced sequence of torsional degrees and vice versa. Indeed, if the sequence of torsional degrees is

$$t_0 = \cdots = t_{i_1-1} > t_{i_1} = \cdots = t_{i_2-1} > t_{i_2} = \cdots = t_{i_3-1} > t_{i_3} = \cdots,$$

then $s_j \neq 0$ if and only if $t_j \neq p^k$ and $j = i_l$ for some l. For example, if the torsional degrees of a code $C \subset \mathbb{Z}_{2^8}[\zeta][u]/\langle u^{2^5} - 1\rangle$ are $2^5, 2^5, 3, 3, 2, 2, 2, 0$, then

$s_0 = s_1 = s_3 = s_5 = s_6 = 0$ and the reduced sequence is $3_2, 2_4, 0_7$. Conversely, it is easy to see that the reduced sequence $3_2, 2_4, 0_7$ gives the torsional degrees $2^5, 2^5, 3, 3, 2, 2, 2, 0$.

Moreover, if the ideal C of $\mathcal{S}_{p^e}$ has the torsional form $C = \langle s_0, ps_1, \dots, p^{e-1}s_{e-1}\rangle$ then it is easy to see that its torsion codes are

$$Tor_i(C) = \mu\langle s_0, s_1, \dots, s_i\rangle. \tag{32}$$

The proof of Theorem 6.5 is actually constructive and uses the inductive process. The torsional form of $\mu_{i+1}(C)$ is obtained from that of $\mu_i(C)$ and the ith torsion of C:

$$\begin{tikzcd}
tdeg & t_0 & t_1 & t_2 & & t_{i-1} & t_i & t_{i+1}\ \cdots \\
\mu_{i+1}(C) = & \langle s_{i+1,0}, \arrow[d] & ps_{i+1,1}, \arrow[d] & p^2 s_{i+1,2}, \arrow[d] & \cdots, & p^{i-1}s_{i+1,i-1}, \arrow[d] & p^i s_{i+1,i}\rangle & \\
\mu_i(C) = & \langle s_{i,0}, & ps_{i,1}, & p^2 s_{i,2}, & \cdots, & p^{i-1}s_{i,i-1}\rangle & &
\end{tikzcd}$$

Here $t_j = tdeg_j(C)$, $\downarrow$ indicates the map μ_i. Moreover, each $s_{i+1,j}$ for $j < i$ and $s_{i+1,i}$ are determined as follows.

(i) if $s_{i,j} = 0$, then $s_{i+1,j} = 0$,
(ii) if $s_{i,j} = (u-1)^{t_j} + pz_{ij}$, then $s_{i+1,j} = (u-1)^{t_j} + pz_{i+1,j} \in \mathcal{S}_{p^e}$, such that

$$p^j s_{i+1,j} \in \mu_{i+1}(C), \text{ and } \mu_i(p^j s_{i+1,j}) = p^j s_{ij},$$

(iii) $s_{i+1,i} = (u-1)^{t_i}$ if $t_i \neq p^k$ and $t_i \neq t_{i-1}$; otherwise $s_{i+1,i} = 0$.

Since $Tor_i(C) = (u-1)^{t_i}$, there exists some $s_i = (u-1)^{t_i} + pz_i$ in $\mathcal{S}_{p^e}$ such that $p^i s_i \in C$. We take such an s_i if $t_i \neq p^k$ and $t_i \neq t_{i-1}$, and $s_i = 0$ otherwise. Then $s_{l,i} = \mu_l(s_i)$ will work for all $l > i$, since $\mu_l(s_{l+1,i}) = \mu_l(\mu_{l+1}(s_i)) = \mu_l(s_i) = s_{l,i}$. Thus the inductive steps (i)–(iii) collapse to the direct algorithm:

- for each $i = 0, 1, \dots, e-1$, take an element $p^i s_i$ of the form

$$p^i s_i = \begin{cases} p^i((u-1)^{t_i} + pz_i) \in C \text{ for some } z_i \in \mathcal{S}_{p^e} & \text{if } t_i \neq p^k \text{ and } t_i \neq t_{i-1}, \\ 0 & \text{otherwise.} \end{cases} \tag{33}$$

We give an example of finding the torsional form of a code.

Example 6.7. Let $C = \langle (u-1) + 2\zeta\rangle$ be an ideal of $\mathcal{S}_8 = \mathbb{Z}_8[\zeta][u]/\langle u^2 - 1\rangle$. We shall find the torsional form of C. We first need to compute the torsion codes of C. Clearly $Tor_0(C) = \langle u-1\rangle$. To compute $Tor_1(C)$, assume $2v \in C$, namely $2v = (u-1+2\zeta)g$ for some $g \in \mathcal{S}_8$. Then $0 = (u-1)\mu(g)$. It follows from Lemma 6.4(ii) that $g = (u-1)f_1 + 2w_1 = (u+1)f_1 + 2w$ for some $f_1, w_1, w \in \mathcal{S}_8$. Then

$2v = 2(u-1)w + 2(u+1)\zeta f_1 + 4\zeta w$, which implies that $v \equiv (u-1)w + (u+1)\zeta f_1 + 2\zeta w \pmod 4$. Thus $\mu(v) \in \langle u-1, u+1\rangle = \langle u-1\rangle$. Consequently, $Tor_1(C) = \langle u-1\rangle$. Next it can be shown that

$$4 \cdot 1 = (u-1+2\zeta)(2\zeta^{-1} + 4(\zeta+1)^{-1} - 4\zeta^{-1} - (\zeta^2+\zeta)^{-1}(u-1)) \in C,$$

which implies that $Tor_2(C) = \langle 1\rangle$ (see Example 6.10(i) for detail). Thus C is not written in torsional form, which must be of the form $\langle s_0, 0, 4\cdot 1\rangle$.

To find the torsional form of C, we may start with $tdeg_0(C) = 1$, so we take $s_0 = (u-1)^1 + 2z \in C$ for some $z \in \mathcal{S}_8$, say $z = \zeta$. Next, $tdeg_2(C) = 1 = tdeg_0(C)$, and hence $s_1 = 0$. Finally, $tdeg_2(C) = 0$, and hence we take $2^2 s_2 = 2^2(1+2z) \in C$, say $z = 0$. Thus $C = \langle (u-1)+2\zeta, 0, 4\rangle$ is the torsional representation of C.

Remark. As Example 6.10 will show, $\langle u-1+2\cdot 1\rangle$ is in torsional form. Therefore $\langle u-1+2z\rangle$ can be a torsional form for some z, but not a torsional form for other z.

The ideals of $\mathbb{Z}_4[\zeta][u]/\langle u^p - 1\rangle$ are listed in [2] and those of $\mathbb{Z}_4[\zeta][u]/\langle u^{p^k} - 1\rangle$ for arbitrary k are listed in [5]. The following corollary is the direct generalization of their results to arbitrary prime p.

Corollary 6.8. *The ideals of* $\mathbb{Z}_{p^2}[\zeta][u]/\langle u^{p^k} - 1\rangle$ *consist of*

- $\langle 0\rangle$,
- $\langle p(u-1)^\alpha\rangle$ *with* $tdeg_0 = 0$, $tdeg_1 = \alpha$,
- $\langle (u-1)^\alpha + pz\rangle$ *with* $tdeg_0 = \alpha = tdeg_1$,
- $\langle (u-1)^\beta + pz, p(u-1)^\alpha\rangle$ *with* $tdeg_0 = \beta > tdeg_1 = \alpha$.

Here $0 \leqslant \alpha, \beta \leqslant p^k - 1$, *and z may be assumed to have the form* $\sum_{j=0}^{\alpha-1} s_j (u-1)^j$ *with* $s_j \in \mathbb{Z}_{p^2}[\zeta]$.

Proof. The list of ideals now easily follows from Theorem 6.5 by listing all possible reduced sequence of torsional degrees $t_i = tdeg_i(C)$ as in the following table, where empty degree indicates $s_i = 0$.

t_0	t_1	Sequence of *tdeg*	Ideal
		p^k, p^k	$\langle 0\rangle$
α		α, α	$\langle (u-1)^\alpha + pz\rangle$for some z
	α	p^k, α	$\langle p(u-1)^\alpha\rangle$
β	α	β, α	$\langle (u-1)^\beta + pz, p(u-1)^\alpha\rangle$ for some z

Note that if $(u-1)^\alpha + pz$ is in the ideal, then $p((u-1)^\alpha + pz) = p(u-1)^\alpha$ is in the ideal, which justifies the form of z. □

Table 1
Torsional forms in $\mathbb{Z}_8[\zeta][u]/\langle u^2-1\rangle$

t_0	t_1	t_2	Sequence of *tdeg*	Ideal C	$\|C\|$
			2,2,2	$\langle 0\rangle$	1
0			0,0,0	$\langle 1\rangle$	2^{6m}
	0		2,0,0	$\langle 2\rangle$	2^{4m}
		0	2,2,0	$\langle 4\rangle$	2^{2m}
1			1,1,1	$\langle (u-1)+2z_0\rangle$	2^{3m}
	1		2,1,1	$\langle 2(u-1)+4z_1\rangle$	2^{2m}
		1	2,2,1	$\langle 4(u-1)\rangle$	2^{m}
1	0		1,0,0	$\langle (u-1)+2z_0, 2\rangle$	2^{5m}
1		0	1,1,0	$\langle (u-1)+2z_0, 4\rangle$	2^{4m}
	1	0	2,1,0	$\langle 2(u-1)+4z_1, 4\rangle$	2^{3m}

Again, the actual torsional forms of ideals $\langle (u-1)^\alpha + pz\rangle$ and $\langle (u-1)^\beta + pz, p(u-1)^\alpha\rangle$ in Corollary 6.8 depend on z. The explicit classification for $p=2$ is done in [5].

Example 6.9. We list the ideals of $\mathcal{S}_8 = \mathbb{Z}_8[\zeta][u]/\langle u^2-1\rangle$ in Table 1, which correspond to the direct summands of cyclic codes over $\mathbb{Z}_8$ of length $2n$, where n is odd. Note that if $t_i = tdeg_i(C) = 0$ then s_i is a unit. Since $0 \leqslant t_i \leqslant 1$, it is easy to list the ideals according to the possible reduced sequence of torsional degrees as in the following table, where empty t_i corresponds to $s_i = 0$. Here, z_0, z_1 are elements in $\mathcal{S}_8$ such that the given ideal has the corresponding sequence of torsional degrees. The exact forms of z_0, z_1 are determined in Example 6.10. The cardinality of C is obtained by Theorem 6.2 and (30). Note that $\langle (u-1)+2z_0, 2\rangle = \langle (u-1), 2\rangle$ and $\langle 2(u-1)+4z_1, 4\rangle = \langle 2(u-1), 4\rangle$.

The torsional forms given in Example 6.9 are the forms that the codes must have in order to have the given torsional degrees. However, as shown in Example 6.7, the ideals of the given form can have different torsional degrees. In the next example, we compute the torsion codes of all forms given in Table 1. As a result, torsional forms of all ideals are determined. Table 2 is the 'converse' to Table 1. In this table, z represents an arbitrary element of $\mathcal{S}_8$. Notice that there is only one type, namely $\langle (u-1)+2z\rangle$, that does not have the unique torsional degrees in this case.

Example 6.10. Most of the torsion codes in Table 2 are easy to get, except for the codes containing $(u-1)+2z$ or $2(u-1)+4z$.

We start with noting that $(u-1)^2 = u^2 - 2u + 1 = 6(u-1)$ in $\mathbb{Z}_8[\zeta][u]/\langle u^2-1\rangle$. Write $z = z_0 + z_1(u-1)$ with $z_0, z_1 \in \mathbb{Z}_8[\zeta]$.

We will compute torsion codes for $C = \langle (u-1)+2z\rangle$. Other torsion codes can be verified in a similar way. As in Example 6.7, $Tor_1(C) = \langle u-1\rangle$. Next, $Tor_2(C) = \langle 1\rangle$

Table 2
Torsion codes for ideals of $\mathbb{Z}_8[\zeta][u]/\langle u^2-1\rangle$

C	$tdeg_0(C)$	$tdeg_1(C)$	$tdeg_2(C)$
$\langle 0\rangle$	2	2	2
$\langle 1\rangle$	0	0	0
$\langle 2\rangle$	2	0	0
$\langle 4\rangle$	2	2	0
$\langle (u-1)+2z\rangle$	1	1	$\begin{cases} 0 & \text{if } z \text{ and } z+1 \text{ are units} \\ 1 & \text{otherwise} \end{cases}$
$\langle 2(u-1)+4z\rangle$	2	1	1
$\langle 4(u-1)\rangle$	2	2	1
$\langle (u-1),2\rangle$	1	0	0
$\langle (u-1)+2z,4\rangle$	1	1	0
$\langle 2(u-1),4\rangle$	2	1	0

if and only if there exists $g_0+g_1(u-1)$ with $g_0g_1\in\mathbb{Z}_8[\zeta]$, such that

$$\begin{aligned} 4\cdot 1 &= ((u-1)+2(z_0+z_1(u-1)))(g_0+g_1(u-1)) \\ &= 2z_0g_0+(2z_0g_1+g_0+2z_1g_0+6g_1+4z_1g_1)(u-1), \end{aligned}$$

equivalently

$$4=2z_0g_0,\quad (2z_0+6+4z_1)g_1+(1+2z_1)g_0=0. \tag{34}$$

Multiplying the second equation by $2z_0$, we get $4(z_0^2+z_0)g_1+4=0$. If $\mu(z_0^2+z_0)=\mu(z_0)\mu(z_0+1)=0$, then $z_0^2+z_0=2w$, which implies that $4=0$, a contradiction. Therefore we assume that $\mu(z_0)\neq 0$ and $\mu(z_0+1)\neq 0$, meaning z_0 and z_0+1 are invertible or equivalently z and $z+1$ are invertible. Let $g_0=2z_0^{-1}+4a$, $g_1=-(z_0^2+z_0)^{-1}$, where a is to be determined. We have $2z_0g_0=4$ and

$$\begin{aligned} &(2z_0+6+4z_1)g_1+(1+2z_1)g_0 \\ &\quad = 2(z_0+1)^{-1}+2z_0^{-1}(z_0+1)^{-1}+2z_0^{-1}-4(z_0+1)^{-1} \\ &\qquad -4z_1z_0^{-1}(z_0+1)^{-1}+4a+4z_1z_0^{-1}. \end{aligned}$$

Since

$$2(z_0+1)^{-1}+2z_0^{-1}(z_0+1)^{-1}+2z_0^{-1}=2(z_0+1)^{-1}z_0^{-1}(z_0+1+(z_0+1))=4z_0^{-1},$$

we have that

$$\begin{aligned} &(2z_0+6+4z_1)g_1+(1+2z_1)g_0 \\ &\quad = 4z_0^{-1}-4(z_0+1)^{-1}-4z_1z_0^{-1}(z_0+1)^{-1}+4a+4z_1z_0^{-1}. \end{aligned}$$

Taking $a = -z_0^{-1} + (z_0 + 1)^{-1} + z_1 z_0^{-1}(z_0 + 1)^{-1} - z_1 z_0^{-1}$, we get $g_0 + g_1(u - 1)$ satisfying Eq. (34). Thus $Tor_2(C) = \langle 1 \rangle$.

Acknowledgments

Y.H. Park thanks the Department of Mathematics, University of Scranton for their hospitality while writing this paper during his stay in 2004. The research of Y.H. Park is accomplished with Research Fund provided by Kangwon National University, Support for 2003 Faculty Research Abroad.

References

[1] T. Abualrub, R. Oehmke, On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e, IEEE Trans. Inform. Theory 49 (9) (2003) 2126–2133.

[2] T. Blackford, Cyclic codes over $\mathbb{Z}_4$ of oddly even length, Discrete Appl. Math. 128 (2003) 27–46.

[3] A.R. Calderbank, N.J.A. Sloane, Modular and p-adic cyclic codes, Design Codes Cryptogr. 6 (1995) 21–35.

[4] G. Castagnoli, J.L. Massey, P.A. Schoeller, N. von Seemann, On repeated-root cyclic codes, IEEE Trans. Inform. Theory 37 (2) (1991) 337–342.

[5] S.T. Dougherty, S. Ling, Cyclic codes over $\mathbb{Z}_4$ of even length, 2004, in preparation.

[6] S.T. Dougherty, K. Shiromoto, MDR codes over $\mathbb{Z}_k$, IEEE Trans. Inform. Theory 46 (1) (2000) 265–269.

[7] P. Kanwar, S.R. López-Permouth, Cyclic codes over the integers modulo p^m, Finite Fields Appl. 3 (1997) 334–352.

[8] S.Y. Kim, Liftings of the ternary Golay code, Master's Thesis, Kangwon National University, 2004.

[9] J.H. van Lint, Repeated-root cyclic codes, IEEE Trans. Inform. Theory 37 (2) (1991) 343–345.

[10] B.R. McDonald, Finite Rings with Identity, Dekker, New York, 1974.

[11] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-correcting Codes, North-Holland, Amsterdam, 1977.

[12] V.S. Pless, Z. Qian, Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 42 (5) (1996) 1594–1600.