On the Structure of Constacyclic Codes of Length $p^s$ over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} + \cdots + u^{m-1}\mathbb{F}_{p^k}$

Somphong Jitman$^a$ and Patanee Udomkavanich$^b$

Department of Mathematics, Faculty of Science
Chulalongkorn University, Bangkok, 10330, Thailand

$^asomphong.c@student.chula.ac.th$, $^bpattanee.u@chula.ac.th$

Abstract

We study the structure of constacyclic codes of length $p^s$ over the ring $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} + \cdots + u^{m-1}\mathbb{F}_{p^k}$ in terms of ideals in the quotient ring $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} + \cdots + u^{m-1}\mathbb{F}_{p^k})[x]/(x^{p^s} - \lambda)$, where $\lambda$ is a unit element in $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} + \cdots + u^{m-1}\mathbb{F}_{p^k}$. In particular, we complete a structural classification of constacyclic codes of length $p^s$ over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ and determine their minimum Hamming distances.

Mathematics Subject Classification: 94B15, 94B60

Keywords: constacyclic code, finite chain ring, Hamming distance

1 Introduction

Formerly, cyclic and constacyclic codes over rings are almost studied on the case where the characteristic of rings and the code length are relatively prime. The structure of cyclic codes has been studied over $\mathbb{F}_2 + u\mathbb{F}_2$ in [6] and over $\mathbb{F}_p + u\mathbb{F}_p + \cdots + u^{k}\mathbb{F}_p$ in [4]. Later, a result on constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ has been established in [5].

Recently, constacyclic codes whose length is not relatively prime to the characteristic of the alphabet ring become much interest. The structure of constacyclic codes whose length is a power of 2 has been studied over Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$ in [2].

In this paper, we focus on determining the structure of constacyclic codes of length $p^s$ over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} + \cdots + u^{m-1}\mathbb{F}_{p^k}$. Moreover, a result in [2] is generalized to arbitrary prime numbers. Some properties of $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} + \cdots + u^{m-1}\mathbb{F}_{p^k}$ are explained in Section 2, along with definitions concerning codes over finite rings. In Section 3, we classify the structure of some constacyclic codes of length $p^s$ over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} + \cdots + u^{m-1}\mathbb{F}_{p^k}$. Finally, we complete a structural classification of constacyclic codes of length $p^s$ over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ in Section 4.
2 Preliminaries

A code of length $n$ over a finite ring $R$ is a nonempty subset of $R^n$. A code $C$ is said to be linear if $C$ is a submodule of the $R$-module $R^n$. In this paper, any codes are assumed to be linear unless otherwise stated. For a given unit $\alpha \in R$, a code $C$ is said to be constacyclic, or specifically, $\lambda$-constacyclic if

$$(\lambda r_{n-1}, r_0, r_1, \ldots, r_{n-2}) \in C$$

whenever $(r_0, r_1, \ldots, r_{n-1}) \in C$.

Especially, a $\lambda$-constacyclic code is called a cyclic code when $\lambda = 1$. It is well-known that $\lambda$-constacyclic codes over $R$ are in correspondence with ideals in $R[x]/\langle x^n - \lambda \rangle$.

A finite commutative ring with $1 \neq 0$ is said to be local if it has a unique maximal ideal and is called a chain ring if its ideals are linearly ordered by inclusion. The following facts are known.

**Proposition 2.1.** A finite commutative ring $R$ with identity is a local ring if and only if the set of all non-invertible elements in $R$ forms a maximal ideal.

**Proposition 2.2.** A finite local ring $R$ is a chain ring if and only if its maximal ideal is principal.

Let $R(p^k, m)$ denote the ring $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} + \cdots + u^{m-1}\mathbb{F}_{p^k}$, where $p$ is prime, $k, m \in \mathbb{N}$ and $u^m = 0$. Note that $R(p^k, m)$ is a finite chain ring with nilpotency index $m$, characteristic $p$, maximal ideal $uR(p^k, m)$ and residue field $\mathbb{F}_{p^k}$. An element $r \in R(p^k, m)$ is uniquely expressed as $r = a_0 + u a_1 + \cdots + u^{m-1} a_{m-1}$, where $a_i \in \mathbb{F}_{p^k}$. In particular, every unit element in $R(p^k, m)$ is of the form $a_0 + u a_1 + \cdots + u^{m-1} a_{m-1}$, where $a_i \in \mathbb{F}_{p^k}$ and $a_0 \neq 0$.

3 Constacyclic Codes of Length $p^s$ over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} + \cdots + u^{m-1}\mathbb{F}_{p^k}$

In this section, we give a description of constacyclic codes of length $p^s$ over $R(p^k, m)$ in terms of ideals in $R(p^k, m)[x]/\langle x^{p^s} - \lambda \rangle$, where $\lambda$ is a unit in $R(p^k, m)$.

For a given unit $a_0 + u a_1 + \cdots + u^{m-1} a_{m-1} \in R(p^k, m)$, let $\alpha_{a_0} = a_0^{-p^s}$, where $r$ is the nonnegative residue of $s$ modulo $k$. Then $\alpha_{a_0}^p = a_0^{-1}$. Define

$$\psi_{\alpha_{a_0}} : R(p^k, m)[x]/\langle x^{p^s} - (1 + a_0^{-1}(u a_1 + \cdots + u^{m-1} a_{m-1})) \rangle$$

$$\rightarrow R(p^k, m)[x]/\langle x^{p^s} - (a_0 + u a_1 + \cdots + u^{m-1} a_{m-1}) \rangle$$

by

$$f(x) \mapsto f(\alpha_{a_0} x).$$

Then, by an application of the proof of [2, Proposition 5.1], the map $\psi_{\alpha_{a_0}}$ is shown to be a ring isomorphism.
Proposition 3.1. The map $\psi_{a_0}$ is a ring isomorphism from $R(p^k, m)[x]/\langle x^{p^s} - (1 + a_0^{-1}(ua_1 + \cdots + u^{m-1}a_{m-1})) \rangle$ onto $R(p^k, m)[x]/\langle x^{p^s} - (a_0 + ua_1 + \cdots + u^{m-1}a_{m-1}) \rangle$.

Note that $R(p^k, m)[x]/\langle x^{p^s} - a_0 \rangle$ is isomorphic to $R(p^k, m)[x]/\langle x^{p^s} - 1 \rangle$. Similarly, for $1 \leq \ell \leq m-1$, $R(p^k, m)[x]/\langle x^{p^s} - (1+a_0^{-1}(u^{\ell}a_{\ell} + \cdots + u^{m-1}a_{m-1})) \rangle$ and $R(p^k, m)[x]/\langle x^{p^s} - (a_0 + u^\ell a_{\ell} + \cdots + u^{m-1}a_{m-1}) \rangle$ are isomorphic as rings. Denote by $1 + u\ell A_{\ell}$ the unit $1 + u^{\ell}a_{\ell} + \cdots + u^{m-1}a_{m-1}$, where $A_{\ell} = a_{\ell} + a_{\ell+1}u + \cdots + u^{m-\ell-1}a_{m-1}$ is a unit in $R(p^k, m)$. Then it suffices to determine only the ideals in $R(p^k, m)[x]/\langle x^{p^s} - 1 \rangle$ and $R(p^k, m)[x]/\langle x^{p^s} - (1 + u^\ell A_{\ell}) \rangle$.

The following propositions and lemma are useful tools.

Proposition 3.2. In $R(p^k, m)[x]/\langle x^{p^s} - 1 \rangle$, the element $x - 1$ is nilpotent of nilpotency index $p^s$.

Proof. Since the characteristic of $R(p^k, m)$ is $p$, we have $(x - 1)^{p^s} = x^{p^s} - 1$. The computation in $R(p^k, m)[x]/\langle x^{p^s} - 1 \rangle$ gives $(x - 1)^{p^s} = 0$. Hence $x - 1$ is nilpotent of nilpotency index $\leq p^s$. Since $\deg((x - 1)^{p^s-1})$ is less than $\deg(x^{p^s} - 1)$, by the Division Algorithm, $(x - 1)^{p^s-1}$ cannot be zero in $R(p^k, m)[x]/\langle x^{p^s} - 1 \rangle$. Therefore, the nilpotency index of $x - 1$ is $p^s$. \qed

Proposition 3.3. For each $1 \leq \ell \leq m-1$, the element $x - 1$ is nilpotent of nilpotency index $\lceil \frac{m}{p} \rceil p^s$ in $R(p^k, m)[x]/\langle x^{p^s} - (1 + u^\ell A_{\ell}) \rangle$.

Proof. In $R(p^k, m)[x]/\langle x^{p^s} - (1 + u^\ell A_{\ell}) \rangle$, we have

$$(x - 1)^{p^s} = x^{p^s} - 1 = u^\ell A_{\ell} \in R(p^k, m)[x]/\langle x^{p^s} - (1 + u^\ell A_{\ell}) \rangle.$$ 

Since $A_{\ell}$ is a unit and $u^\ell$ is nilpotent of nilpotency index $\lceil \frac{m}{p} \rceil$, it follows that $x - 1$ is nilpotent of nilpotency index $\leq \lceil \frac{m}{p} \rceil p^s$.

Finally, we show that $(x - 1)^{\lceil \frac{m}{p} \rceil p^s - 1} \neq 0 \in R(p^k, m)[x]/\langle x^{p^s} - (1 + u^\ell A_{\ell}) \rangle$. As $A_{\ell}$ is invertible, it is sufficient to show that $u^\ell((\lceil \frac{m}{p} \rceil - 1)(x - 1)^{p^s-1} \neq 0 \in R(p^k, m)[x]/\langle x^{p^s} - (1 + u^\ell A_{\ell}) \rangle$, or equivalently, for all $h(x) \in R(p^k, m)[x]$, $u^\ell((\lceil \frac{m}{p} \rceil - 1)(x - 1)^{p^s-1} \neq h(x)(x^{p^s} - (1 + u^\ell A_{\ell}))$ in $R(p^k, m)[x]$. This follows from the monicity of $x^{p^s} - (1 + u^\ell A_{\ell})$ and $\deg((x - 1)^{p^s-1}) < \deg(x^{p^s} - (1 + u^\ell A_{\ell}))$. \qed

Corollary 3.4. For each $1 \leq \ell \leq m - 1$ and $0 \leq t \leq (\lceil \frac{m}{p} \rceil - 1)p^s$, $(x - 1)^{p^s+t} = (u^\ell(x - 1)^{t})$ in $R(p^k, m)[x]/\langle x^{p^s} - (1 + u^\ell A_{\ell}) \rangle$.

Lemma 3.5. For $1 \leq \ell \leq m-1$, let $f(x) \in R(p^k, m)[x]/\langle x^{p^s} - (1 + u^\ell A_{\ell}) \rangle$. Then $f(x)$ is invertible if and only if its constant term is a unit.

Proof. A polynomial $f(x)$ can be uniquely viewed as

$$f(x) = \sum_{i=0}^{p^s-1} c_i(x - 1)^i = c_0 + (x - 1) \sum_{i=1}^{p^s-1} c_i(x - 1)^{i-1}.$$
First, suppose that \( c_0 \) is a unit. Let \( h(x) = c_0^{-1}(x-1) \sum_{i=1}^{p^s-1} c_i(x-1)^{i-1} \). Then \( h(x) \) is nilpotent and \( c_0^{-1}f(x) = 1 + h(x) \). Let \( m \) be an odd integer such that \( h(x)^m = 0 \). Then

\[
1 = 1 + h(x)^m = (1 + h(x))(1 - h(x) + \cdots + h(x)^{m-1}) = c_0^{-1}f(x)(1 - h(x) + \cdots + h(x)^{m-1}).
\]

This means \( f(x) \) is invertible.

Conversely, suppose that \( c_0 \) is not a unit. Then \( c_0 = 0 \) or \( c_0 \) is a zero-divisor. If \( c_0 = 0 \), then \( f(x) = (x - 1) \sum_{i=1}^{p^s-1} c_i(x-1)^{i-1} \) is not invertible as \( x - 1 \) is nilpotent. Suppose that \( c_0 \) is a zero-divisor. Then \( c_0 = u^j a \) for some unit \( a \) in \( R(p^k, m) \) and \( 1 \leq j \leq m - 1 \). Thus \( f(x) = u^j a + (x - 1) \sum_{i=1}^{p^s-1} c_i(x-1)^{i-1} \), which is not invertible because \( u \) and \( x - 1 \) are nilpotent.

**Proposition 3.6.** For each \( 1 \leq \ell \leq m - 1 \), \( R(p^k, m)[x]/\langle x^{p^s} - (1 + u^\ell A_\ell) \rangle \) is a local ring with maximal ideal \( \langle u, x - 1 \rangle \).

**Proof.** Let \( f(x) \) be an element in \( R(p^k, m)[x]/\langle x^{p^s} - (1 + u^\ell A_\ell) \rangle \). Then \( f(x) \) can be uniquely viewed as

\[
f(x) = \sum_{i=0}^{p^s-1} c_i(x-1)^i = c_0 + (x - 1) \sum_{i=1}^{p^s-1} c_i(x-1)^{i-1}.
\]

By Proposition 2.1, it suffices to show that \( f(x) \in \langle u, x - 1 \rangle \) if and only if \( f(x) \) is non-invertible. The first implication is clear since \( u \) and \( x - 1 \) are nilpotent.

Suppose that \( f(x) \) is non-invertible. It follows from Lemma 3.5 that \( c_0 = 0 \) or \( c_0 \) is a zero-divisor. If \( c_0 = 0 \), then \( f(x) = (x - 1) \sum_{i=1}^{p^s-1} c_i(x-1)^{i-1} \in \langle u, x - 1 \rangle \).

If \( c_0 \) is a zero-divisor, then

\[
f(x) = u^j a + (x - 1) \sum_{i=1}^{p^s-1} c_i(x-1)^{i-1} \in \langle u, x - 1 \rangle,
\]

for some unit \( a \) in \( R(p^k, m) \) and \( 1 \leq j \leq m - 1 \). In both cases, we have \( f(x) \in \langle u, x - 1 \rangle \).

Hence \( R(p^k, m)[x]/\langle x^{p^s} - (1 + u^\ell A_\ell) \rangle \) is a local ring having \( \langle u, x - 1 \rangle \) as its maximal ideal. \( \square \)
The next corollary follows from replacing \( u^\ell A_\ell \) by 0 in the previous proof.

**Corollary 3.7.** The ring \( R(p^k, m)[x]/\langle x^{p^s} - 1 \rangle \) is a local ring with maximal ideal \( \langle u, x - 1 \rangle \).

The structures of \( R(p^k, m)[x]/\langle x^{p^s} - 1 \rangle \) and \( R(p^k, m)[x]/\langle x^{p^s} - (1 + u^\ell A_\ell) \rangle \) are characterized as follows.

**Theorem 3.8.** The followings hold:

i) The ring \( R(p^k, m)[x]/\langle x^{p^s} - (1 + uA_1) \rangle \) is a finite chain ring with maximal ideal \( x - 1 \), and residue field \( \mathbb{F}_{p^s} \).

ii) For each \( 2 \leq \ell \leq m - 1 \), the ring \( R(p^k, m)[x]/\langle x^{p^s} - (1 + u^\ell A_\ell) \rangle \) is not a chain ring.

iii) The ring \( R(p^k, m)[x]/\langle x^{p^s} - 1 \rangle \) is not a chain ring.

**Proof.** By Proposition 3.6, \( R(p^k, m)[x]/\langle x^{p^s} - (1 + u^\ell A_\ell) \rangle \) is a local ring with maximal ideal \( \langle u, x - 1 \rangle \).

When \( \ell = 1 \), the application of Corollary 3.4 implies \( \langle u, x - 1 \rangle = \langle x - 1 \rangle \). Therefore, by Proposition 2.2, \( R(p^k, m)[x]/\langle x^{p^s} - (1 + uA_1) \rangle \) is a finite chain ring with maximal ideal \( \langle x - 1 \rangle \). This proves i).

In order to prove ii), suppose \( 2 \leq \ell \leq m - 1 \). Assume that \( u \in \langle x - 1 \rangle \). Then there exist \( f(x) \) and \( g(x) \) in \( R(p^k, m)[x] \) such that \( u = (x - 1)f(x) + (x^{p^s} - (1 + u^\ell A_\ell))g(x) \) in \( R(p^k, m)[x] \). When \( x = 1 \), we have \( u = u^\ell A_\ell g(1) \) which is impossible since the nilpotency index of \( u \) is \( m \) but the nilpotency index of \( u^\ell A_\ell g(1) \) is at most \( \left\lceil \frac{m}{\ell} \right\rceil \) \( \leq \left\lceil \frac{m}{2} \right\rceil < m \). Hence, \( u \notin \langle x - 1 \rangle \).

Next, assume that \( x - 1 \notin \langle u \rangle \). Then \( x - 1 = u f(x) + (x^{p^s} - (1 + u^\ell A_\ell))g(x) \) in \( R(p^k, m)[x] \) for some \( f(x), g(x) \in R(p^k, m)[x] \). Comparing the coefficients, we get \(-1 = u f_0 - g_0(1 + u^\ell A_\ell) \) which implies \( 1 = g_0 \) modulo \( u \). Also, \( 0 = u f_{p^s} + g_{0}(1 + u^\ell A_\ell) \) which implies \( g_0 = g_{p^s} \) modulo \( u \). In general, we have \( 0 = u f_{kp^s} + g_{(k-1)p^s - kp^s}(1 + u^\ell A_\ell) \) for all \( k > 1 \). So, \( g_{kp^s} \neq 0 \) for \( k \geq 0 \) which contradicts a finiteness of the degree of \( g(x) \). Hence, \( x - 1 \notin \langle u \rangle \). This shows that the maximal ideal \( \langle u, x - 1 \rangle \) is not principal. Hence, by Proposition 2.2, \( R(p^k, m)[x]/\langle x^{p^s} - (1 + u^\ell A_\ell) \rangle \) is not a chain ring.

Replacing \( u^\ell A_\ell \) by 0 in the proof of ii), the statement iii) follows. \( \square \)

As \( R(p^k, m)[x]/\langle x^{p^s} - (1 + uA_1) \rangle \) is a chain ring, all \( (1 + uA_1) \)-constacyclic codes of length \( p^s \) over \( R(p^k, m) \) are determined in the following theorem.

**Theorem 3.9.** The number of \( (1 + uA_1) \)-constacyclic codes of length \( p^s \) over \( R(p^k, m) \) is \( mp^s + 1 \). Each \( (1 + uA_1) \)-constacyclic code corresponds to an ideal \( \langle (x - 1)^i \rangle \subseteq R(p^k, m)[x]/\langle x^{p^s} - (1 + uA_1) \rangle \) containing \( p^{k(mp^s - i)} \) codewords, where \( 0 \leq i \leq mp^s \).
4 Constacyclic Codes of Length $p^s$ over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$

In order to avoid tedious computation, we restrict our study to the case $m = 2$ and characterize the structure of constacyclic codes of length $p^s$ over $R(p^k, 2) = \mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$. We complete their structural classification along with their Hamming distances.

We recall some basic tools for determining the Hamming distances of codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$. Denote by $d_H(C)$ the Hamming distance of a code $C$. The Hamming weight of $v \in (\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})^n$, denoted $\text{wt}(v)$, is defined to be the number of non-zero components of $v$. For each code $C$ of length $n$ over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$, we define $\text{Res}(C) = \mu(C)$ and $\text{Tor}(C) = \mu(\{v \in (\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})^n \mid uv \in C\})$, where $\mu : (\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})^n \to \mathbb{F}_{p^k}$ is the componentwise reduction modulo $u$. The sets $\text{Res}(C)$ and $\text{Tor}(C)$ are called the residue and torsion codes of $C$, respectively.

**Lemma 4.1.** Let $C$ be a code of length $n$ over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$. Then $d_H(C) = d_H(\text{Tor}(C))$.

**Proof.** Note that $\text{Res}(C) \subseteq \text{Tor}(C)$ and $u\mu^{-1}(\text{Tor}(C)) \subseteq C$. These yields $d_H(C) \leq d_H(u\mu^{-1}(\text{Tor}(C))) = d_H(\text{Tor}(C))$.

On the other direction, let $v$ be a non-zero codeword in $C$. If $\mu(v) = 0$, then $v = uw$ for some $w \in (\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})^n$ such that $\mu(w) \in \text{Tor}(C) \setminus \{0\}$ and hence $\text{wt}_H(v) = \text{wt}_H(uw) = \text{wt}_H(\mu(w)) \geq d_H(\text{Tor}(C))$. If $\mu(v) \neq 0$, then $\mu(v) \in \text{Res}(C) \subseteq \text{Tor}(C)$ and hence $\text{wt}_H(v) \geq \text{wt}_H(\mu(v)) \geq d_H(\text{Tor}(C))$. \hfill \square

The following Hamming distances of cyclic codes of length $p^s$ over $\mathbb{F}_{p^k}$ [7] is key to determine the Hamming distances of codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$.

**Theorem 4.2 ([7, Theorem 6.4]).** Let $C$ be a $p^k$-ary cyclic code of length $p^s$. Then $C = \langle (x-1)^i \rangle \subseteq \mathbb{F}_{p^k}[x]/(x^{p^s}-1)$, for some $i \in \{0, 1, \ldots, p^s\}$. The Hamming distance $\Delta_i := d_H(C)$ is determined by

$$
\Delta_i = \begin{cases} 
1 & \text{if } i = 0, \\
(t + 1) & \text{if } (t - 1)p^{s-1} + 1 \leq i \leq tp^{s-1} \text{ where } 1 \leq t \leq p - 1, \\
(t + 1)p^\ell & \text{if } p^s - p^{s-\ell} + (t - 1)p^{s-\ell-1} + 1 \leq i \leq p^s - p^{s-\ell} + tp^{s-\ell-1} \\
\infty & \text{if } i = 2p^s.
\end{cases}
$$

According to Proposition 3.1, it is enough to determine the structure of cyclic and $(1 + ua)$-constacyclic codes of length $p^s$ over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$.

For cyclic codes of length $p^s$ over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$, the following theorem can also be proved by modifying the corresponding results in [2, Theorems 4.3-4.5 and 4.9] to work for an arbitrary prime $p$. 
Theorem 4.3. The ideals and the corresponding residue and torsion codes in \((\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})[x]/(x^n - 1)\) are of the following forms:

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

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

iii) If \(C = \langle u(x-1)^i \rangle\), where \(0 \leq i < p^s\), then \(\text{Res}(C) = \langle 0 \rangle\) and \(\text{Tor}(C) = \langle (x-1)^i \rangle\).

iv) If \(C = \langle (x-1)^i + u(x-1)^j \rangle\), where \(1 \leq i < p^s\), \(0 \leq t < i\), and \(\textbf{h}(x)\) is the zero polynomial or a unit, then \(\text{Res}(C) = \langle (x-1)^i \rangle\) and \(\text{Tor}(C) = \langle (x-1)^T \rangle\) where

\[
T = \begin{cases} 
  i & \text{if } \textbf{h}(x) = 0 \\
  \min\{i, p^s - i + t\} & \text{if } \textbf{h}(x) \text{ is a unit.}
\end{cases}
\]

v) \(\langle (x-1)^i + u(x-1)^j \textbf{h}(x), u(x-1)^\kappa \rangle\), where \(1 \leq i < p^s\), \(0 \leq t < \kappa\), \(\kappa < T\) with \(T\) as in case iv) and \(\textbf{h}(x)\) is the zero polynomial or a unit, then \(\text{Res}(C) = \langle (x-1)^i \rangle\) and \(\text{Tor}(C) = \langle (x-1)^\kappa \rangle\).

The cardinalities and the Hamming distances of cyclic codes of length \(p^s\) over \(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}\) are determined in the following theorem:

Theorem 4.4. The cardinalities and the Hamming distances of cyclic codes of length \(p^s\) over \(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}\) are given as in Table 4.1:

<table>
<thead>
<tr>
<th>Ideal</th>
<th>Condition(s)</th>
<th>(T)</th>
<th>Cardinality</th>
<th>(d_H)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\langle 0 \rangle)</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>(\langle 1 \rangle)</td>
<td>-</td>
<td>-</td>
<td>(p^{2mp})</td>
<td>1</td>
</tr>
<tr>
<td>(\langle u(x-1)^i \rangle)</td>
<td>(0 \leq i &lt; p^s)</td>
<td>-</td>
<td>(p^{2(mp - i)})</td>
<td>(\Delta_i)</td>
</tr>
<tr>
<td>(\langle (x-1)^i \rangle)</td>
<td>(1 \leq i &lt; p^s)</td>
<td>(i)</td>
<td>(p^{2(mp - i)})</td>
<td>(\Delta_i)</td>
</tr>
<tr>
<td>(\langle (x-1)^i + u(x-1)^j \rangle), (\textbf{h}(x)) is a unit</td>
<td>(1 \leq i &lt; p^s)</td>
<td>(i)</td>
<td>(p^{2(mp - i)})</td>
<td>(\Delta_i)</td>
</tr>
<tr>
<td>(\langle (x-1)^i, u(x-1)^\kappa \rangle), (\kappa &lt; T)</td>
<td>(1 \leq i &lt; p^s)</td>
<td>(i)</td>
<td>(p^{2(mp - i)})</td>
<td>(\Delta_i)</td>
</tr>
<tr>
<td>(\langle (x-1)^i + u(x-1)^j \rangle), (\kappa &lt; T) and (\textbf{h}(x)) is a unit</td>
<td>(1 \leq i &lt; p^s)</td>
<td>(i)</td>
<td>(p^{2(mp - i)})</td>
<td>(\Delta_i)</td>
</tr>
</tbody>
</table>

Table 4.1: The structure of cyclic codes of length \(p^s\) over \(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}\)

Proof. The third column is derived from the definition of \(T\). The cardinality of each ideal follows directly from the fact that \(|C| = |\text{Res}(C)||\text{Tor}(C)|\), where the residue and torsion codes are determined in Theorem 4.3 and their cardinalities can be computed via \([7, \text{Theorem 6.2}]\).

For the last column, by Lemma 4.1, \(d_H(C) = d_H(\text{Tor}(C))\); therefore, the Hamming distance of \(C\) follows from Theorem 4.3 and 4.2. \(\square\)
For the case \( p \) is an arbitrary odd prime number, the number of cyclic codes of length \( p^s \) over \( \mathbb{F}_{p^k} + u\mathbb{F}_{p^k} \) can be generalized from the idea in [2, Theorem 4.7]

**Theorem 4.5.** The number of cyclic codes of length \( p^s \) over \( \mathbb{F}_{p^k} + u\mathbb{F}_{p^k} \)

\[
2 + p^{m(\frac{p^s-1}{2})} + \frac{(2p^k + 3)p^{m(\frac{p^s-1}{2})} - 2p^s - 1}{p^k - 1} + \frac{2(p^k + 1)p^{m(\frac{p^s-1}{2})} - 2p^{2m} - 2}{(p^k - 1)^2}.
\]

**Proof.** The number of trivial codes \( \langle 0 \rangle \) and \( \langle 1 \rangle \) is 2. The number of \( \langle u(x-1)^i \rangle \), where \( 0 \leq i < p^s \), is \( p^s \). The number of \( \langle (x-1)^i \rangle \), where \( 1 \leq i < p^s \), is \( p^s - 1 \).

Next, we compute the number of \( \langle (x-1)^i + u(x-1)^i \mathfrak{h}(x) \rangle \), where \( 1 \leq i < p^s \), \( 0 \leq t < i \) and \( \mathfrak{h}(x) = \sum_j \alpha_j(x-1)^j \) is a unit. This means \( \alpha_0 \neq 0, \alpha_j \in \mathbb{F}_{p^k} \).

In order to obtain the number of distinct ideals, \( t + j < T = \min\{i, p^s - i + t\} \). That is \( 0 \leq j \leq T - t - 1 \). Hence the number of distinct ideals of this form is

\[
\sum_{i=1}^{p^s-1} \sum_{t=0}^{i-1} (p^k - 1)(p^k)^{i-t-1} + \sum_{t=0}^{2i-1} \sum_{i=p^s+1}^{p^s-1} (p^k - 1)(p^k)^{p^s-i-1} + \sum_{i=p^s+1}^{p^s-1} \sum_{t=2i-1}^{p^s} (p^k - 1)(p^k)^{i-t-1}
\]

\[
= \frac{2(p^k + 1)p^{m(\frac{p^s-1}{2})} - 4}{p^k - 1} + p^{m(\frac{p^s-1}{2})} - 2p^s - 1.
\]

The number of \( \langle (x-1)^i, u(x-1)^\kappa \rangle \), where \( 1 \leq i < p^s \) and \( 0 \leq \kappa < T = i \), is

\[
\sum_{i=1}^{p^s-1} i = \frac{(p^s - 1)p^s}{2}.
\]

Finally, we demonstrate the number of ideals of the form \( \langle (x-1)^i + u(x-1)^i \mathfrak{h}(x), u(x-1)^\kappa \rangle \), where \( 1 \leq i < p^s \), \( 0 \leq t < i \) \( 0 \leq \kappa < T \) and \( \mathfrak{h}(x) \) is a unit. In order to obtain the number of distinct ideals, \( t + j < \kappa \). That is \( 0 \leq j \leq \kappa - t - 1 \). Hence the number of ideals of this form is

\[
\sum_{i=2}^{p^s-2} \sum_{t=0}^{i-1} \sum_{\kappa=t+1}^{i-1} (p^k - 1)(p^k)^{i-t-1} + \sum_{t=0}^{2i-1} \sum_{i=p^s+1}^{p^s-1} \sum_{\kappa=t+1}^{i-1} (p^k - 1)(p^k)^{p^s-i-1} + \sum_{i=p^s+1}^{p^s-1} \sum_{t=2i-1}^{p^s} \sum_{\kappa=t+1}^{p^s} (p^k - 1)(p^k)^{i-t-1}
\]

\[
= \frac{2(p^k + 1)p^{m(\frac{p^s-1}{2})} - 2p^{2m} - 2}{(p^k - 1)^2} + \frac{p^{m(\frac{p^s-1}{2})} - 2p^s + 3}{p^k - 1} - p^s - \frac{p^{2s} - 3p^s}{2} + 2.
\]

The total number follows from summing the number of ideals for each type. \( \square \)
Putting $m = 2$ in Theorem 3.8 i), the next proposition is concluded.

**Proposition 4.6.** The ring $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})/(x^{p^k} - (1 + ua))$ is a finite chain ring with maximal ideal $\langle x - 1 \rangle$ residue filed $\mathbb{F}_{p^k}$, and nilpotency index $2p^s$.

**Corollary 4.7.** The number of $(1 + ua)$-constacyclic codes of length $p^s$ over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ is $2p^s + 1$. Each $(1 + ua)$-constacyclic code is corresponding to the ideal $\langle (x - 1)^i \rangle \subseteq (\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})/(x^{p^s} - (1 + ua))$, where $0 \leq i \leq 2p^s$.

Finally, we compute the Hamming distances of $(1 + ua)$-constacyclic codes of length $p^s$ over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$, or equivalently, the Hamming distances of ideals in $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})/(x^{p^s} - (1 + ua))$.

**Theorem 4.8.** For each $i \in \{0, 1, \ldots, 2p^s\}$, the Hamming distance of a $(1 + ua)$-constacyclic code $\langle (x - 1)^i \rangle \subseteq (\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})/(x^{p^s} - (1 + ua))$ is

$$
\begin{aligned}
1 & \text{ if } 0 \leq i \leq p^s, \\
(t + 1) & \text{ if } p^s + (t - 1)p^s - 1 + 1 \leq i \leq p^s + tp^{s-1} \text{ where } 1 \leq t \leq p - 1, \\
(t + 1)p^N & \text{ if } 2p^s - p^s - N + (t - 1)p^s - N - 1 + 1 \leq i \leq 2p^s - p^s - N + tp^{s-N-1} \text{ where } 1 \leq t \leq p - 1 \text{ and } 1 \leq \ell \leq s - 1, \\
\infty & \text{ if } i = 2p^s.
\end{aligned}
$$

**Proof.** By Corollary 3.4, $\langle u \rangle = \langle (x - 1)^{p^s} \rangle \subseteq (\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})/(x^{p^s} - (1 + ua))$. This means $1 = d_H((\mathbb{F}_{p^k} + u\mathbb{F}_{p^k})/(x^{p^s} - (1 + ua))) \leq d_H((\langle x - 1 \rangle^{p^s})) = 1$. Hence $d_H((\langle x - 1 \rangle^i)) = 1$ for all $0 \leq i \leq p^s$.

Suppose that $p^s < i$, that is, $i = p^s + t$ for some $1 \leq t \leq p^s$. Then, by Corollary 3.4, $\langle (x - 1)^{p^s+t} \rangle = \langle u(x - 1)^{t} \rangle$ and hence Tor($\langle (x - 1)^{p^s+t} \rangle$) = $\langle (x - 1)^{t} \rangle \subseteq \mathbb{F}_{p^k}[x]/(x^{p^s} - 1)$. Therefore, a result follows from Lemma 4.1 and Theorem 4.2.

5 Conclusion

The structure of constacyclic codes of length $p^s$ over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} + \cdots + u^{m-1}\mathbb{F}_{p^k}$ is studied in terms of ideals in the quotient ring $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} + \cdots + u^{m-1}\mathbb{F}_{p^k})[x]/(x^{p^s} - \lambda)$, where $\lambda$ is a unit element in $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} + \cdots + u^{m-1}\mathbb{F}_{p^k}$. Their structures depend on the representation of $\lambda$. All of $(\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} + \cdots + u^{m-1}\mathbb{F}_{p^k})[x]/(x^{p^s} - \lambda)$ are local rings. Moreover, some of them are again finite chain rings. In particular, we complete a structural classification of constacyclic codes of length $p^s$ over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ and determine their minimum Hamming distances.
References


Received: November, 2009