J. Korean Math. Soc. **51** (2014), No. 4, pp. 853–866
http://dx.doi.org/10.4134/JKMS.2014.51.4.853

SOME CLASSES OF REPEATED-ROOT CONSTACYCLIC CODES OVER $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$

Xiusheng Liu and Xiaofang Xu

Abstract. Constacyclic codes of length p^s over $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$ are precisely the ideals of the ring $\frac{R[x]}{\langle x^{p^s}-1\rangle}$. In this paper, we investigate constacyclic codes of length p^s over R. The units of the ring R are of the forms γ, $\alpha + u\beta$, $\alpha + u\beta + u^2\gamma$ and $\alpha + u^2\gamma$, where α, β and γ are nonzero elements of $\mathbb{F}_{p^m}$. We obtain the structures and Hamming distances of all $(\alpha+u\beta)$-constacyclic codes and $(\alpha+u\beta+u^2\gamma)$-constacyclic codes of length p^s over R. Furthermore, we classify all cyclic codes of length p^s over R, and by using the ring isomorphism we characterize γ-constacyclic codes of length p^s over R.

1. Introduction

Constacyclic codes over finite rings are an important class of codes from both a theoretical and practical viewpoint. In the 1990s, it was shown that certain good nonlinear binary codes can be constructed from cyclic codes over $\mathbb{Z}_4$ via the Gray map [10]. Since then, constacyclic codes over finite chain rings have been studied by many authors [8, 12, 17]. In these studies, the code length n is relatively prime to the characteristic of the residue field of a finite chain ring. The case when the code length n is divisible by the characteristics p of the residue field of a finite chain ring yields the so-called repeated-root codes, which were studied since 2003 by several authors such as Abualrub and Oehmke [1], Blackford [2, 3], Noton and Sălăgean [14], Sălăgean [16], Ling et al. [13], Zhu and Kai [18, 19]. In recent years, Dinh and Dougherty have studied the description of several classes of constacyclic codes, such as cyclic and negacyclic codes over various types of finite rings [4, 5, 6, 7, 8, 9]. In this paper, we continue to study repeated-root constacyclic codes over the chain ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$.

Received December 25, 2013.
2010 *Mathematics Subject Classification.* 94B15, 94B05.
Key words and phrases. constacyclic codes, cyclic codes, Hamming distance, repeated-root codes.
This work was supported by the Natural Science Foundation of Hubei Province (D20144401) and the Natural Science Foundation of Hubei Polytechnic University (12xjz14A).

The paper is organized as follows. In Section 2, we will recall some notations and properties about constacyclic codes over finite chain rings, and the structure and Hamming distance of α-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$, where α is a nonzero element of $\mathbb{F}_{p^m}$. Using the structure and Hamming distances of constacyclic codes over $\mathbb{F}_{p^m}$, we investigate the structure and Hamming distance of $(\alpha+u\beta)$-constacyclic codes and $(\alpha+u\beta+u^2\gamma)$-constacyclic codes of length p^s over $R=\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$ in Section 3. We show that $R_{\alpha+u\beta}=\frac{R[x]}{\langle x^{p^s}-(\alpha+u\beta)\rangle}$ or $R_{\alpha+u\beta+u^2\gamma}=\frac{R[x]}{\langle x^{p^s}-(\alpha+u\beta+u^2\gamma)\rangle}$ is a finite chain ring with maximal ideal of $\langle \alpha_0 x-1\rangle$, where α_0 is completely determined by α, s and m. In Section 4, we address the cyclic codes of length p^s over R. These cyclic codes are the ideals of the ring $R_1=\frac{R[x]}{\langle x^{p^s}-1\rangle}$, which is a local ring with the maximal ideal $\langle x-1,u\rangle$. We classify all such cyclic codes by categorizing the ideals of the local ring R_1 into 8 types, and provide a detailed structure of ideals in each type. In the last section, we build a one-to-one correspondence between cyclic and γ-constacyclic codes of length p^s over R_1 via the ring isomorphism ψ, which allows us to apply our results about cyclic codes in Section 4 to γ-constacyclic codes over R.

2. Preliminaries

Let $\mathbb{F}_{p^m}$ be a finite field with p^m elements, where p is a prime and m is an integer number. Let R be the commutative ring $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}=\{a+bu+cu^2 \mid a,b,c\in\mathbb{F}_{p^m}\}$ with $u^3=0$. The ring R is a chain ring, it has a unique maximal ideal $\langle u\rangle=\{au \mid a\in\mathbb{F}_{p^m}\}$. A code of length n over R is a nonempty subset of R^n, and a code is linear over R if it is an R-submodule of R^n. Let C be a code of length n over R and $P(C)$ be its polynomial representation, i.e.,

$$P(C)=\{\sum_{i=0}^{n-1} c_i x^i \mid (c_0,c_1,\ldots,c_{n-1})\in C\}.$$

For a unit λ of R, the λ-constacyclic (λ-twisted) shift τ_λ on R^n is the shift

$$\tau_\lambda(a_0,a_1,\ldots,a_{n-1})=(\lambda a_{n-1},a_0,\ldots,a_{n-2}).$$

A linear code C is said to be λ-constacyclic if $\tau_\lambda(C)=C$, i.e., C is closed under the λ-constacyclic shift τ_λ. In the case $\lambda=1$, these λ-constacyclic codes are called cyclic codes and in the case $\lambda=-1$, these λ-constacyclic codes are called negacyclic codes. A code C of length n over R is λ-constacyclic if and only if $P(C)$ is an ideal of $\frac{R[x]}{\langle x^n-\lambda\rangle}$, and a code C of length n over R is cyclic if and only if $P(C)$ is an ideal of $\frac{R[x]}{\langle x^n-1\rangle}$, and a code C of length n over R is negacyclic if and only if $P(C)$ is an ideal of $\frac{R[x]}{\langle x^n+1\rangle}$.

Let $x=(x_0,x_1,\ldots,x_{n-1})$ and $y=(y_0,y_1,\ldots,y_{n-1})\in R^n$. The Euclidean inner product or dot product of x and y in R^n is defined as $x\cdot y=x_0y_0+x_1y_1+\cdots+x_{n-1}y_{n-1}$, where the operation is performed in R. The dual code of C is defined as $C^{\perp} = \{x \in R^n \mid x \cdot y = 0, \forall y \in C\}$. A code C is called self-orthogonal if $C \subseteq C^{\perp}$, and it is called self-dual if $C = C^{\perp}$. It is well known that the dual of a λ-constacyclic code is a λ^{-1}-constacyclic code [7].

The following equivalent conditions are known for the class of finite commutative chain rings [8].

Proposition 2.1. *Let R be a finite commutative ring. Then the following conditions are equivalent*:

(i) *R is a local ring and the maximal ideal M of R is principal, i.e., $M = \langle r \rangle$ for some $r \in R$;*

(ii) *R is a local principal ideal ring;*

(iii) *R is a chain ring with ideals $\langle r^i \rangle$, and $|\langle r^i \rangle| = |\bar{R}|^{N(r)-i}$, $0 \le i \le N(r)$, where $|\bar{R}| = \frac{R}{M}$ and $N(r)$ is the nilpotency of r.*

The following proposition can be found in [11, 15].

Proposition 2.2. *Let p be a prime and R be a finite chain ring of size p^{α}. The number of codewords in any linear code C of length n over R is p^k for some integer $k \in \{0, 1, \ldots, \alpha n\}$. Moreover, the dual code $C^{\perp}$ has p^l codewords, where $k + l = \alpha n$, i.e., $|C||C^{\perp}| = |R|^n$.*

Let λ be a nonzero element of the field $\mathbb{F}_{p^m}$. Let C be a λ-constacyclic code of length p^s over $\mathbb{F}_{p^m}$. Then $\lambda^{-p^m} = \lambda^{-1}$. By the division algorithm, there exist nonnegative integers λ_q, λ_r such that $s = \lambda_q m + \lambda_r$, where $s, m > 0, 0 \le \lambda_r \le m - 1$. Let $\lambda_0 = -\lambda^{-p^{(\lambda_q+1)m-s}} = -\lambda^{-p^{m-\lambda_r}}$. Then $\lambda_0^{p^s} = -\lambda^{-p^{(\lambda_q+1)m}} = -\lambda^{-1}$. We will use the following.

Proposition 2.3 ([5, Theorem 4.11])**.** *Let C be a λ-constacyclic code of length p^s over $\mathbb{F}_{p^m}$. Then $C = \langle (\lambda_0 x + 1)^i \rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s} - \lambda \rangle}$ for $i \in \{0, 1, \ldots, p^s\}$, and its Hamming distance $d(C)$ is completely determined by*

$$d(C) = \begin{cases} 1, & \text{if } i = 0, \\ l + 2, & \text{if } lp^{s-1} + 1 \le i \le (l+1)p^{s-1}, \text{ where } 0 \le l \le p - 2, \\ (t+1)p^k, & \text{if } p^s - p^{s-k} + (t-1)p^{s-k-1} + 1 \le i \le p^s - p^{s-k} + tp^{s-k-1}, \\ & \text{where } 1 \le t \le p - 1, \text{and } 1 \le k \le s - 1, \\ 0, & \text{if } i = p^s. \end{cases}$$

3. $(\alpha + u\beta)$ or $(\alpha + u\beta + u^2\gamma)$-constacyclic codes of length p^s over ring R

Let α, β and γ be nonzero elements of the field $\mathbb{F}_{p^m}$. Then $\alpha + u\beta$ and $\alpha + u\beta + u^2\gamma$ are units of R. The $(\alpha + u\beta)$-constacyclic codes of length p^s over R are ideals of the ring $R_{\alpha+u\beta} = \frac{R[x]}{\langle x^{p^s} - (\alpha + u\beta) \rangle}$, and the $(\alpha + u\beta + u^2\gamma)$-constacyclic codes of length p^s over R are ideals of the ring $R_{\alpha+u\beta+u^2\gamma} = \frac{R[x]}{\langle x^{p^s} - (\alpha + u\beta + u^2\gamma) \rangle}$. By the division algorithm, there exist nonnegative integers α_q, α_r such that

$s = \alpha_q m + \alpha_r$, where $0 \leq \alpha_r \leq m-1$. Let $\alpha_0 = \alpha^{-p^{(\alpha_q+1)m-s}} = \alpha^{-p^{m-\alpha_r}}$. Then $\alpha_0^{p^s} = \alpha^{-p^{(\alpha_q+1)m}} = \alpha^{-1}$.

Lemma 3.1. *In $R_{\alpha+u\beta}$ or $R_{\alpha+u\beta+u^2\gamma}$, $\langle(\alpha_0 x-1)^{p^s}\rangle = \langle u\rangle$. In particular, $\alpha_0 x - 1$ is nilpotent in $R_{\alpha+u\beta}$ or $R_{\alpha+u\beta+u^2\gamma}$ with nilpotency index $3p^s$.*

Proof. If $1 \leq i \leq p^s-1$, then $p \mid \binom{p^s}{i}$.

(i) By computing in $R_{\alpha+u\beta}$,

$$\begin{aligned}(\alpha_0 x-1)^{p^s} &= (\alpha_0 x)^{p^s} - 1 + \sum_{i=1}^{p^s-1} \binom{p^s}{i} (\alpha_0 x)^i (-1)^{p^s-i} \\ &= \alpha^{-1} x^{p^s} - 1 = \alpha^{-1}(\alpha+u\beta) - 1 = u\beta\alpha^{-1}.\end{aligned}$$

So $\langle(\alpha_0 x-1)^{p^s}\rangle = \langle u\rangle$.

(ii) By computing in $R_{\alpha+u\beta+u^2\gamma}$,

$$\begin{aligned}(\alpha_0 x-1)^{p^s} &= (\alpha_0 x)^{p^s} - 1 + \sum_{i=1}^{p^s-1} \binom{p^s}{i} (\alpha_0 x)^i (-1)^{p^s-i} \\ &= \alpha^{-1} x^{p^s} - 1 = \alpha^{-1}(\alpha+u\beta+u^2\gamma) - 1 \\ &= u\beta\alpha^{-1} + u^2\gamma\alpha^{-1} = u(\beta\alpha^{-1} + u\gamma\alpha^{-1}).\end{aligned}$$

So $\langle(\alpha_0 x-1)^{p^s}\rangle = \langle u\rangle$.

The last statement is straightforward because u has nilpotency index 3 in $R_{\alpha+u\beta}$ or $R_{\alpha+u\beta+u^2\gamma}$. □

Theorem 3.2. *The ring $R_{\alpha+u\beta}$ or $R_{\alpha+u\beta+u^2\gamma}$ is a chain ring whose ideal is separately*

$$R_{\alpha+u\beta} = \langle 1\rangle \supsetneq \langle\alpha_0 x-1\rangle \supsetneq \cdots \supsetneq \langle(\alpha_0 x-1)^{3p^s-1}\rangle \supsetneq \langle(\alpha_0 x-1)^{3p^s}\rangle = \langle 0\rangle,$$

or

$$R_{\alpha+u\beta+u^2\gamma} = \langle 1\rangle \supsetneq \langle\alpha_0 x-1\rangle \supsetneq \cdots \supsetneq \langle(\alpha_0 x-1)^{3p^s-1}\rangle \supsetneq \langle(\alpha_0 x-1)^{3p^s}\rangle = \langle 0\rangle.$$

Proof. Let $f(x)$ be an element in $R_{\alpha+u\beta}$ or $R_{\alpha+u\beta+u^2\gamma}$. Then $f(x)$ can be represented as

$$f(x) = \sum_{i=0}^{p^s-1} a_{0i}(\alpha_0 x-1)^i + u\sum_{i=0}^{p^s-1} a_{1i}(\alpha_0 x-1)^i + u^2\sum_{i=0}^{p^s-1} a_{2i}(\alpha_0 x-1)^i,$$

where $a_{0i}, a_{1i}, a_{2i} \in \mathbb{F}_{p^m}$. By Lemma 3.1, $u = (\alpha_0 x-1)^{p^s}\alpha\beta^{-1}$, so $f(x) = a_{00} + (\alpha_0 x-1)g(x)$ for some polynomial $g(x) \in R_{\alpha+u\beta}$ or $g(x) \in R_{\alpha+u\beta+u^2\gamma}$. Because $\alpha_0 x-1$ is nilpotent in $R_{\alpha+u\beta}$ or $R_{\alpha+u\beta+u^2\gamma}$, $f(x)$ is not invertible if and only if $a_{00} = 0$. It is equivalent to the fact that $f(x)$ is in $\langle\alpha_0 x-1\rangle$. Therefore, $R_{\alpha+u\beta}$ or $R_{\alpha+u\beta+u^2\gamma}$ is a local ring with maximal ideal $\langle\alpha_0 x-1\rangle$. That means that $R_{\alpha+u\beta}$ or $R_{\alpha+u\beta+u^2\gamma}$ is a chain ring whose ideals are $\langle(\alpha_0 x-1)^i\rangle$, $0 \leq i \leq 3p^s$. □

We have $(\alpha + u\beta + u^2\gamma)^{p^{2m}} = (\alpha^{p^m})^{p^m} = \alpha^{p^m} = \alpha$, hence $(\alpha + u\beta + u^2\gamma)^{p^{2m}}\alpha^{-1} = 1$. Therefore,

$$\begin{aligned}(\alpha + u\beta + u^2\gamma)^{-1} &= (\alpha + u\beta + u^2\gamma)^{p^{2m}-1}\alpha^{-1}\\ &= [(\alpha + u\beta)^{p^{m+1}-1} + (p^{m+1} - 1)(\alpha + u\beta)^{p^{m+1}-2}u^2\gamma]\alpha^{-1}\\ &= [\alpha^{p^{2m}-1} - u\beta\alpha^{p^{2m}-2} + \frac{(p^{2m} - 1)(p^{2m} - 2)}{2}u^2\beta^2\alpha^{p^{2m}-3}\\ &\quad - (\alpha + u\beta)^{p^{2m}-2}u^2\gamma]\alpha^{-1}\\ &= [1 - u\beta\alpha^{-1} - u^2\gamma\alpha^{-1} + u^2\beta^2\alpha^{-2}]\alpha^{-1}\\ &= \alpha^{-1} - u\beta\alpha^{-2} - u^2(\gamma\alpha^{-2} - \beta^2\alpha^{-3}).\end{aligned}$$

This implies that if $C = \langle(\alpha_0 x - 1)^i\rangle$ is a $(\alpha + u\beta + u^2\gamma)$-constacyclic code of length p^s over R, then its dual $C^\perp$ is a $[\alpha^{-1} - u\beta\alpha^{-2} - u^2(\gamma\alpha^{-2} - \beta^2\alpha^{-3})]$-constacyclic code of length p^s over R. That means $C^\perp$ is an ideal of the chain ring $R_{\alpha^{-1}-u\beta\alpha^{-2}-u^2(\gamma\alpha^{-2}-\beta^2\alpha^{-3})} = \frac{R[x]}{\langle x^{p^s}-(\alpha^{-1}-u\beta\alpha^{-2}-u^2(\gamma\alpha^{-2}-\beta^2\alpha^{-3}))\rangle}$. Since $|C| = p^{m(3p^s-i)}$, it follows that $|C^\perp| = p^{mi}$ and $C^\perp = \langle(\alpha_0^{-1}x - 1)^{3p^s-i}\rangle \subset R_{\alpha^{-1}-u\beta\alpha^{-2}-u^2(\gamma\alpha^{-2}-\beta^2\alpha^{-3})}$. We obtain the following theorem.

Theorem 3.3. *For each $(\alpha + u\beta + u^2\gamma)$-constacyclic code of length p^s over R, $C = \langle(\alpha_0 x - 1)^i\rangle \subset R_{\alpha+u\beta+u^2\gamma}$, its dual is the $[\alpha^{-1} - u\beta\alpha^{-2} - u^2(\gamma\alpha^{-2} - \beta^2\alpha^{-3})]$-constacyclic code*

$$C^\perp = \langle(\alpha_0^{-1}x - 1)^{3p^s-i}\rangle \subset R_{\alpha^{-1}-u\beta\alpha^{-2}-u^2(\gamma\alpha^{-2}-\beta^2\alpha^{-3})},$$

which contains p^{mi} codewords.

Similarly, we have the following theorem.

Theorem 3.4. *For each $(\alpha + u\beta)$-constacyclic code of length p^s over R, $C = \langle(\alpha_0 x - 1)^i\rangle \subset R_{\alpha+u\beta}$, its dual is the $(\alpha^{-1} - u\beta\alpha^{-2} + u^2\beta^2\alpha^{-3})$-constacyclic code $C^\perp = \langle(\alpha_0^{-1}x - 1)^{3p^s-i}\rangle \subset R_{\alpha^{-1}-u\beta\alpha^{-2}+u^2\beta^2}$, which contains p^{mi} codewords.*

In the following, we consider the Hamming distance of $(\alpha + u\beta)$-constacyclic codes or $(\alpha + u\beta + u^2\gamma)$-constacyclic codes of length p^s over R.

Theorem 3.5. *Let C be a $(\alpha + u\beta)$-constacyclic code or $(\alpha + u\beta + u^2\gamma)$-constacyclic code of length p^s over R. Then $C = \langle(\alpha_0 x - 1)^i\rangle \subset R_{\alpha+u\beta}$ or $R_{\alpha+u\beta+u^2\gamma}$ for $i \in \{0, 1, 2, \ldots, 3p^s\}$, and the Hamming distance $d(C)$ is completely determined by*

$$d(C) = \begin{cases} 1, & \text{if } 0 \le i \le 2p^s,\\ l + 2, & \text{if } 2p^s + lp^{s-1} + 1 \le i \le 2p^s + (l + 1)p^{s-1}, \text{ where } 0 \le l \le p - 2,\\ (t+1)p^k, & \text{if } 3p^s - p^{s-k} + (t-1)p^{s-k-1} + 1 \le i \le 3p^s - p^{s-k} + tp^{s-k-1},\\ & \text{where } 1 \le t \le p - 1, \text{and } 1 \le k \le s - 1,\\ 0, & \text{if } i = 3p^s.\end{cases}$$

Proof. By Lemma 3.1, $\langle(\alpha_0 x-1)^{2p^s}\rangle = \langle u^2\rangle$ in $R_{\alpha+u\beta}$ or $R_{\alpha+u\beta+u^2\gamma}$. We consider the following two cases.

Case 1: $1 \le i \le 2p^s$. Then $u^2 \in \langle(\alpha_0 x-1)^i\rangle$, and thus $\langle(\alpha_0 x-1)^i\rangle$ has a Hamming distance of 1.

Case 2: $2p^s+1 \le i \le 3p^s-1$. Then $\langle(\alpha_0 x-1)^i\rangle = \langle u^2(\alpha_0 x-1)^{i-2p^s}\rangle$, which means that the codewords of the code $\langle(\alpha_0 x-1)^i\rangle$ in $R_{\alpha+u\beta}$ or $R_{\alpha+u\beta+u^2\gamma}$ are precisely the codewords of the code $\langle(\alpha_0 x-1)^{i-2p^s}\rangle$ in $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-\alpha\rangle}$, multiplied with u, which have the same Hamming weights. Moreover, the codes $\langle(\alpha_0 x-1)^{i-2p^s}\rangle$ in $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-\alpha\rangle}$ are α-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$, with the Hamming distance computed as Proposition 2.3. We complete the proof of the theorem. □

4. Cyclic codes of length p^s over R

Cyclic codes of length p^s over R are ideals of the residue ring $R_1 = \frac{R[x]}{\langle x^{p^s}-1\rangle}$. It is easy to prove the following lemma.

Lemma 4.1. *The followings hold in* R_1:

(i) *For any nonnegative integer* t, $(x-1)^{p^t} = x^{p^t}-1$.

(ii) $x-1$ *is nilpotent with the nilpotency index* p^s.

Unlike $R_{\alpha+u\beta}$, the ring R_1 is not a chain ring. It is a local ring whose maximal ideal is not principal.

Proposition 4.2. *The ring* R_1 *is a local ring with the maximal ideal* $\langle u, x-1\rangle$, *but it is not a chain ring.*

Proof. Any $f(x) \in R_1$ can be represented as

$$\begin{aligned} f(x) &= \sum_{i=0}^{p^s-1} b_{0i}(x-1)^i + u\sum_{i=0}^{p^s-1} b_{1i}(x-1)^i + u^2\sum_{i=0}^{p^s-1} b_{2i}(x-1)^i \\ &= b_{00} + (x-1)\sum_{i=1}^{p^s-1} b_{0i}(x-1)^{i-1} + u\sum_{i=0}^{p^s-1} b_{1i}(x-1)^i + u^2\sum_{i=0}^{p^s-1} b_{2i}(x-1)^i, \end{aligned}$$

where $b_{0i}, b_{1i}, b_{2i} \in \mathbb{F}_{p^m}$. Note that $x-1, u$ and u^2 are nilpotent in R_1. It follows that $f(x)$ is not invertible if and only if $b_{00}=0$, and $\langle u, x-1\rangle$ is precisely the set of non-invertible elements of R_1. Hence R_1 is a local ring with the maximal ideal $\langle u, x-1\rangle$. Suppose that $u \in \langle x-1\rangle$. Then there must exist $f_1(x), f_2(x) \in R[x]$ such that $u = (x-1)f_1(x) + (x^{p^s}-1)f_2(x)$. But this is impossible because $u=0$ of $x=1$. Hence $u \notin \langle x-1\rangle$. Obviously, $x-1 \notin \langle u\rangle$, because $x-1$ has nilpotency index p^s and $u^3=0$. Therefore, the maximal ideal $\langle u, x-1\rangle$ of R_1 is not principal. It means R_1 is not a chain ring. □

We can list all cyclic codes of length p^s over R_1 as follows.

Theorem 4.3. *Cyclic codes of length p^s over R, i.e., ideals of the ring R_1 are*

- *Type* 1 : $\langle 0\rangle, \langle 1\rangle$.
- *Type* 2 : $I = \langle u^2(x-1)^k\rangle$, *where* $0 \le k \le p^s - 1$.
- *Type* 3 : $I = \langle u(x-1)^l + u^2 \sum_{j=0}^{l-1} c_{2j}(x-1)^j\rangle$, *where* $0 \le l \le p^s - 1, c_{2j} \in \mathbb{F}_{p^m}$; *or equivalently,* $I = \langle u(x-1)^l + u^2(x-1)^t h(x)\rangle$, *where* $0 \le l \le p^s - 1, 0 \le t < l$, *and either* $h(x)$ *is 0 or* $h(x)$ *is a unit where it can be represented as* $h(x) = \sum_j h_j(x-1)^j$ *with* $h_j \in \mathbb{F}_{p^m}$, *and* $h_0 \ne 0$.
- *Type* 4 : $I = \langle u(x-1)^l + u^2 \sum_{j=0}^{w-1} c_{2j}(x-1)^j, u^2(x-1)^w\rangle$, *where* $0 \le l \le p^s - 1, c_{2j} \in \mathbb{F}_{p^m}, w < l$ *and* $w < T$, *where* T *is the smallest integer such that* $u^2(x-1)^T \in \langle u(x-1)^l + u^2 \sum_{j=0}^{l-1} c_{2j}(x-1)^j\rangle$; *or equivalent,* $\langle u(x-1)^l + u^2(x-1)^t h(x), u(x-1)^w\rangle$, *with* $h(x)$ *as in Type* 3, *and* $\deg(h) \le w - t - 1$.
- *Type* 5 : $I = \langle (x-1)^i + u(x-1)^t h_1(x) + u^2(x-1)^z h_2(x)\rangle$, *where* $0 \le i \le p^s - 1, 0 \le t < i, 0 \le z < i$ *and* $h_1(x), h_2(x)$ *are similar to* $h(x)$ *in Type* 3.
- *Type* 6 : $I = \langle (x-1)^i + u \sum_{j=0}^{q-1} c_{1j}(x-1)^j + u^2 \sum_{j=0}^{q-1} c_{2j}(x-1)^j, u(x-1)^q + u^2 \sum_{j=0}^{q-1} e_{2j}(x-1)^j\rangle$, *where* $0 \le i \le p^s - 1, q \le i$ *and* $c_{1j}, c_{2j}, e_{2j} \in \mathbb{F}_{p^m}$.
- *Type* 7 : $I = \langle (x-1)^i + u \sum_{j=0}^{\sigma-1} c_{1j}(x-1)^j + u^2 \sum_{j=0}^{\sigma-1} c_{2j}(x-1)^j, u(x-1)^q + u^2 \sum_{j=0}^{\sigma-1} e_{2j}(x-1)^j, u^2(x-1)^\sigma\rangle$, *where* $0 \le i \le p^s - 1, \sigma < q \le i, c_{1j}, c_{2j}, e_{2j} \in \mathbb{F}_{p^m}$, *and* T *is the smallest integer such that* $u^2(x-1)^T \in \langle u(x-1)^q + u^2 \sum_{j=0}^{q-1} e_{2j}(x-1)^j\rangle = \langle u(x-1)^q + u^2(x-1)^z h(x)\rangle$, *with* $h(x)$ *as in Type* 3, *and* $\deg(h(x)) \le w - z - 1$.
- *Type* 8 : $I = \langle (x-1)^i + u \sum_{j=0}^{i-1} c_{0j}(x-1)^j + u^2 \sum_{j=0}^{\eta-1} c_{2j}(x-1)^j, u^2(x-1)^\eta\rangle$, *where* $0 \le i \le p^s - 1$, $\eta < i$, $c_{0j}, c_{2j} \in \mathbb{F}_{p^m}$.

Proof. Ideals of Type 1 are the trivial ideals. Consider an arbitrary nontrivial ideal of R_1.

Case 1. $I \subset \langle u^2\rangle$. Any element of I must have the form $u^2 \sum_{j=0}^{p^s-1} b_{2j}(x-1)^j$, where $b_{2j} \in \mathbb{F}_{p^m}$. Let $b \in I$ be an element that has the smallest k such that $b_{2k} \ne 0$. Hence all elements $a(x) \in I$ have the form

$$a(x) = u^2(x-1)^k \sum_{j=k}^{p^s-1} a_{2j}(x-1)^{j-k},$$

which implies $I \subset \langle u^2(x-1)^k\rangle$. On the other hand, we have $b \in I$ with

$$b = u^2(x-1)^k \sum_{j=k}^{p^s-1} b_{2j}(x-1)^{j-k} = u^2(x-1)^k(b_{2k} + \sum_{j=k+1}^{p^s-1} b_{2j}(x-1)^{j-k}).$$

As $b_{2k} \ne 0$, $b_{2k} + \sum_{j=k+1}^{p^s-1} b_{2j}(x-1)^{j-k}$ is invertible, it follows that $u^2(x-1)^k \in I$. That is to say, the ideals of R_1 contained in $\langle u^2\rangle$ are $\langle u^2(x-1)^k\rangle$, $0 \le k \le p^s - 1$.

Case 2. $\langle u^2\rangle \subsetneq I \subset \langle u\rangle$. Any element of I must have the form

$$u\sum_{j=0}^{p^s-1} e_{1j}(x-1)^j + u^2\sum_{j=0}^{p^s-1} e_{2j}(x-1)^j,$$

and there exists a polynomial $u\sum_{j=0}^{p^s-1} p_{1j}(x-1)^j + u^2\sum_{j=0}^{p^s-1} e_{2j}(x-1)^j$ in I such that $\sum_{j=0}^{p^s-1} p_{1j}(x-1)^j \neq 0$. Let $M = \{u\sum_{j=0}^{p^s-1} e_{1j}(x-1)^j + u^2\sum_{j=0}^{p^s-1} e_{2j}(x-1)^j \in I \mid \sum_{j=0}^{p^s-1} e_{1j}(x-1)^j \neq 0\}$ and $N = \{u^2\sum_{j=0}^{p^s-1} e_{2j}(x-1)^j \in I \mid e_{2j} \in \mathbb{F}_{p^m}\}$. We take $\delta = \min\{\deg(h(x)) \mid h(x) \in M\}$. Suppose that $H = \{h(x) \in M \mid \deg(h(x)) = \delta\}$. Then there is an element $h_1(x) = u\sum_{j=0}^{p^s-1} h_{1j}(x-1)^j + u^2\sum_{j=0}^{p^s-1} h_{2j}(x-1)^j$ in H that has the smallest l such that $h_{1l} \neq 0$. Hence we have

$$h_1(x) = u(x-1)^l(h_{1l} + \sum_{j=l+1}^{p^s-1} h_{1j}(x-1)^{j-l}) + u^2\sum_{j=0}^{p^s-1} h_{2j}(x-1)^j \in I.$$

Let $h_2(x) = (x-1)^l(h_{1l} + \sum_{j=l+1}^{p^s-1} h_{1j}(x-1)^{j-l}) + u\sum_{j=0}^{p^s-1} h_{2j}(x-1)^j$. Then $h_1(x) = uh_2(x)$. We now have two subcases.

Case 2a. $N \subset \langle h_1(x)\rangle$. For any $f(x) \in M$, obviously, $f(x)$ can be written as $f(x) = uf_1(x)$, where $f_1(x) = \sum_{j=0}^{p^s-1} e_{1j}(x-1)^j + u\sum_{j=0}^{p^s-1} e_{2j}(x-1)^j$. By the Euclidean algorithm for finite commutative local rings, $f_1(x)$ can be written as

$$f_1(x) = q(x)h_2(x) + r(x),$$

where $q(x), r(x) \in R_1$ and $r(x) = 0$ or $\deg(r(x)) < \deg(h_1(x))$. It implies that $uf_1(x) = q(x)h_1(x) + ur(x)$. Suppose that $ur(x) \notin N$. Then $ur(x) \neq 0$. Hence $ur(x) = f(x) - q(x)h_1(x) \in M$, which contradicts the assumption of $h_1(x)$. Thus $ur(x) \in N$. Therefore, $I = \langle h_1(x)\rangle$. Because $uh_1(x) = u^2(x-1)^l[h_{1l} + \sum_{j=l+1}^{p^s-1} h_{1j}(x-1)^{j-l}] \in I$ and $h_{1l} + \sum_{j=l+1}^{p^s-1} h_{1j}(x-1)^{j-l}$ is an invertible element in R_1, it follows that $u^2(x-1)^l \in I$ and

$$\tilde{h}(x) = u(x-1)^l(h_{1l} + \sum_{j=l+1}^{p^s-1} h_{1j}(x-1)^{j-l}) + u^2\sum_{j=0}^{l-1} h_{2j}(x-1)^j \in I.$$

Thus $c(x) = \tilde{h}(x)(h_{1l} + \sum_{j=l+1}^{p^s-1} h_{1j}(x-1)^{j-l})^{-1} \in I$ and $c(x)$ can be expressed as $c(x) = u(x-1)^l + u^2\sum_{j=0}^{l-1} c_{2j}(x-1)^j$, where $c_{2j} \in \mathbb{F}_{p^m}$.

Therefore,

$$I = \langle u(x-1)^l + u^2\sum_{j=0}^{l-1} c_{2j}(x-1)^j\rangle.$$

Case 2b. $N \not\subseteq \langle\tilde{h}(x)\rangle = \langle c(x)\rangle$. For any $n(x) \in N$, there exists the smallest integer w such that $n(x) = u^2(x-1)^w n_1(x)$ for $n_1(x) \in R_1$. Obviously, $u^2(x-$

$1)^w \in N$, but $u^2(x-1)^w \notin \langle \tilde{h}(x)\rangle = \langle c(x)\rangle$. Hence

$$I = \langle u(x-1)^l + u^2\sum_{j=0}^{l-1} c_{2j}(x-1)^j, u^2(x-1)^w\rangle.$$

Suppose that $w \geq l$. Then

$$u^2(x-1)^w = u(x-1)^{w-l}[u(x-1)^l + u^2\sum_{j=0}^{l-1} c_{2j}(x-1)^j] \in \langle c(x)\rangle,$$

which is a contradiction. Thus $w < l$. Hence

$$I = \langle u(x-1)^l + u^2\sum_{j=0}^{w-1} c_{2j}(x-1)^j, u^2(x-1)^w\rangle.$$

Let T be the smallest integer such that $u^2(x-1)^T \in \langle c(x)\rangle$. If $w \geq T$, then $u^2(x-1)^w = (x-1)^{w-T}u^2(x-1)^T \in \langle c(x)\rangle$, which contradicts the assumption of $u^2(x-1)^w \notin \langle c(x)\rangle$. Hence $w < T$.

Case 3. $I \nsubseteq \langle u\rangle$. Let I_u denote the set of elements in I reduced modulo u. Then I_u is a nonzero ideal of the ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$. According to [5, Theorem 6.2], it is a chain ring with ideals $\langle (x-1)^j\rangle$, where $0 \leq j \leq p^s$. Hence there is an integer $i \in \{0, 1, \ldots, p^s-1\}$ such that $I_u = \langle (x-1)^i\rangle \subset \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$. Therefore, there are two elements $c_i(x) = \sum_{j=0}^{p^s-1} c_{0j}^{(i)}(x-1)^j + u\sum_{j=0}^{p^s-1} c_{1j}^{(i)}(x-1)^j + u^2\sum_{j=0}^{p^s-1} c_{2j}^{(i)}(x-1)^j \in R_1$ for $i = 1, 2$ such that $(x-1)^i + uc_1(x) + u^2c_2(x) \in I$, where $c_{0j}^{(i)}, c_{1j}^{(i)}, c_{2j}^{(i)} \in \mathbb{F}_{p^m}$. Note that

$$\begin{aligned}
&(x-1)^i + uc_1(x) + u^2c_2(x) \\
&= (x-1)^i + u\sum_{j=0}^{p^s-1} c_{0j}^{(1)}(x-1)^j + u^2\sum_{j=0}^{p^s-1} c_{1j}^{(1)}(x-1)^j + u^2\sum_{j=0}^{p^s-1} c_{0j}^{(2)}(x-1)^j \\
&= (x-1)^i + u\sum_{j=0}^{p^s-1} c_{0j}^{(1)}(x-1)^j + u^2\sum_{j=0}^{p^s-1} c_{2j}(x-1)^j \in I,
\end{aligned}$$

where $c_{2j} = c_{1j}^{(1)} + c_{0j}^{(1)}$, and for all l with $i \leq l \leq p^s-1$,

$$u^2(x-1)^l = u^2[(x-1)^i + u\sum_{j=0}^{p^s-1} c_{0j}^{(1)}(x-1)^j + u^2\sum_{j=0}^{p^s-1} c_{2j}(x-1)^j](x-1)^{l-i} \in I.$$

It follows that

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

Hence it can be assumed without loss of generality that $c(x) = (x-1)^i + u\sum_{j=0}^{i-1} c_{0j}^{(1)}(x-1)^j + u^2\sum_{j=0}^{i-1} c_{2j}(x-1)^j \in I$, where $c_{0j}^{(1)}, c_{2j} \in \mathbb{F}_{p^m}$. We now have two subcases.

Case 3a: $I = \langle (x-1)^i + u\sum_{j=0}^{i-1} c_{0j}^{(1)}(x-1)^j + u^2\sum_{j=0}^{i-1} c_{2j}(x-1)^j\rangle$. I can be express as $I = \langle (x-1)^i + u(x-1)^t h_1(x) + u^2(x-1)^z h_2(x)\rangle$, such that either $h_1(x)$, $h_2(x)$ are 0 or $h_1(x)$, $h_2(x)$ are units that can be represented as $h_1(x) = \sum_j h_{1j}(x-1)^j$, $h_2(x) = \sum_j h_{2j}(x-1)^j$, with $h_{1j}, h_{2j} \in \mathbb{F}_{p^m}$, and $h_{10} \neq 0$, $h_{20} \neq 0$. It means that I is in Type 5.

Case 3b: $\langle (x-1)^i + u\sum_{j=0}^{i-1} c_{0j}^{(1)}(x-1)^j + u^2\sum_{j=0}^{i-1} c_{2j}(x-1)^j\rangle \subsetneq I$. For every $f(x) \in I \setminus \langle (x-1)^i + u\sum_{j=0}^{i-1} c_{0j}^{(1)}(x-1)^j + u^2\sum_{j=0}^{i-1} c_{2j}(x-1)^j\rangle$, there is a polynomial $g(x) \in R_1$ such that

$$0 \neq h_f(x) = f(x) - g(x)[(x-1)^i + u\sum_{j=0}^{i-1} c_{0j}^{(1)}(x-1)^j + u^2\sum_{j=0}^{i-1} c_{2j}(x-1)^j] \in I,$$

and $h_f(x)$ can be expressed as

$$h_f(x) = \sum_{j=1}^{i-1} h_{0j}(x-1)^j + u\sum_{j=1}^{i-1} h_{1j}(x-1)^j + u^2\sum_{j=1}^{i-1} h_{2j}(x-1)^j \in I,$$

where $h_{0j}, h_{1j}, h_{2j} \in \mathbb{F}_{p^m}$. Now, $h_f(x)$ reduced modulo u is in $I_u = \langle (x-1)^i\rangle \subset \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$, and thus $h_{0j} = 0$ for all $0 \leq j \leq i-1$, i.e., $h_f(x) = u\sum_{j=1}^{i-1} h_{1j}(x-1)^j + u^2\sum_{j=1}^{i-1} h_{2j}(x-1)^j = uh_{f_u}(x) + u^2 h_{f_{u^2}}(x)$, where $h_{f_u}(x) = \sum_{j=1}^{i-1} h_{1j}(x-1)^j, h_{f_{u^2}}(x) = \sum_{j=1}^{i-1} h_{2j}(x-1)^j$.

Let $M_f = \{h_f(x) = uh_{f_u}(x) + u^2 h_{f_{u^2}}(x) \in I \mid f \in I \setminus \langle (x-1)^i + u\sum_{j=0}^{i-1} c_{0j}^{(1)}(x-1)^j + u^2\sum_{j=0}^{i-1} c_{2j}(x-1)^j\rangle,\ h_{f_u}(x) \neq 0\}$ and $N_f = \{u^2 h_{f_{u^2}}(x) \in I \mid f \in I \setminus \langle (x-1)^i + u\sum_{j=0}^{i-1} c_{0j}^{(1)}(x-1)^j + u^2\sum_{j=0}^{i-1} c_{2j}(x-1)^j\rangle,\ h_{f_u}(x) = 0\}$.

Suppose that $M_f \neq \Phi$. We take $\varsigma = \min\{\deg(h_f(x)) \mid h_f(x) \in M_f\}$. It is easy to prove that there is a polynomial $\tilde{h}_f(x) \in M_f$ with $\deg(\tilde{h}_f(x)) = \varsigma$ that has the smallest q such that $\tilde{h}_{1q} \neq 0$. Hence we have

$$\tilde{h}_f(x) = u(x-1)^q(\tilde{h}_{1q} + \sum_{j=q+1}^{i-1} \tilde{h}_{1j}(x-1)^{j-q}) + u^2\sum_{j=0}^{i-1} \tilde{h}_{2j}(x-1)^j \in I.$$

Similarly with Case 2, we have

$$c_f(x) = u(x-1)^q + u^2\sum_{j=0}^{q-1} e_{2j}(x-1)^j \in I,$$

where $q \leq i$.

If $N_f \subset \langle c_f(x)\rangle$, then

$$I = \langle (x-1)^i + u\sum_{j=0}^{q-1} c_{1j}(x-1)^j + u^2\sum_{j=0}^{q-1} c_{2j}(x-1)^j, u(x-1)^q + u^2\sum_{j=0}^{q-1} e_{2j}(x-1)^j\rangle,$$

where $q \le i$. Hence I is in Type 6.

If $N_f \not\subseteq \langle c_f(x)\rangle$, then there exists the smallest integer $\sigma < i$ such that $h_{f_{u^2}}(x) = u^2(x-1)^\sigma n_{f_{u^2}}(x)$ for any $h_{f_{u^2}}(x) \in N_f$. It is easy to verify that $u^2(x-1)^\sigma \in N_f$, but $u^2(x-1)^\sigma \notin \langle c_f(x)\rangle$. Hence

$$I = \langle (x-1)^i + u\sum_{j=0}^{i-1} c_{1j}(x-1)^j + u^2\sum_{j=0}^{i-1} c_{2j}(x-1)^j,$$
$$u(x-1)^q + u^2\sum_{j=0}^{q-1} e_{2j}(x-1)^j, u^2(x-1)^\sigma\rangle.$$

Suppose that $\sigma \ge q$. Then $u^2(x-1)^\sigma \in \langle c_f(x)\rangle$, which is a contradiction. Hence $\sigma < q \le i$. Therefore,

$$I = \langle (x-1)^i + u\sum_{j=0}^{\sigma-1} c_{1j}(x-1)^j + u^2\sum_{j=0}^{\sigma-1} c_{2j}(x-1)^j,$$
$$u(x-1)^q + u^2\sum_{j=0}^{\sigma-1} e_{2j}(x-1)^j, u^2(x-1)^\sigma\rangle.$$

Let T be the smallest integer such that $u^2(x-1)^T \in \langle u(x-1)^q + u^2\sum_{j=0}^{\sigma-1} e_{2j}(x-1)^j\rangle$. If $\sigma \ge T$, then $u^2(x-1)^\sigma \in \langle c_f(x)\rangle$, which is a contradiction. Hence $\sigma < T$, and therefore, I is in Type 7.

Suppose that $M_f = \Phi$. Then there exists the smallest integer $\eta < i$ such that $h_{f_{u^2}}(x) = u^2(x-1)^\eta \tilde{h}_{f_{u^2}}$ for any $h_{f_{u^2}}(x) \in N_f$. It is easy to verify that $u^2(x-1)^\eta \in N_f$, but $u^2(x-1)^\eta \notin \langle (x-1)^i + u\sum_{j=0}^{i-1} c_{0j}^{(1)}(x-1)^j + u^2\sum_{j=0}^{i-1} c_{2j}(x-1)^i\rangle$. Hence

$$I = \langle (x-1)^i + u\sum_{j=0}^{i-1} c_{0j}^{(1)}(x-1)^j + u^2\sum_{j=0}^{i-1} c_{2j}(x-1)^i, u^2(x-1)^\eta\rangle.$$

Therefore, I is in Type 8. □

For cyclic codes of Types 4 and 7 according to the classification in the Theorem 4.3, the number T plays a very important role. We now determine T for Type 4 and 7.

Proposition 4.4. *In Type* 4, *let T be the smallest integer such that $u^2(x-1)^T \in C = \langle u(x-1)^l + u^2(x-1)^t h(x)\rangle$. Then*

$$T = \begin{cases} l, & \text{if } h(x) = 0,\\ \min\{l, p^s - l + t\}, & \text{if } h(x) \ne 0,\end{cases}$$

Proof. Firstly $T \leq l$, because $u^2(x-1)^l = u[u(x-1)^l + u^2 \sum_{j=0}^{w-1} c_{2j}(x-1)^j] \in C$. In case $h(x) = 0$, $C = \langle u(x-1)^l \rangle$ and it implies $T = l$.

We consider the case $h(x) \neq 0$ and know $h(x)$ is a unit. Because $u^2(x-1)^T \in \langle u(x-1)^l + u^2(x-1)^t h(x) \rangle$, there exists $f(x) \in R_1$ such that $u^2(x-1)^T = f(x)[u(x-1)^l + u^2(x-1)^t h(x)]$. Writing $f(x)$ as

$$f(x) = \sum_{j=0}^{p^s-1} a_{0j}(x-1)^j + u \sum_{j=0}^{p^s-1} a_{1j}(x-1)^j + u^2 \sum_{j=0}^{p^s-1} a_{2j}(x-1)^j,$$

where $a_{0j}, a_{1j}, a_{2j} \in \mathbb{F}_{p^m}$, we have

$$\begin{aligned}
&u^2(x-1)^T \\
=& [\sum_{j=0}^{p^s-1} a_{0j}(x-1)^j + u \sum_{j=0}^{p^s-1} a_{1j}(x-1)^j + u^2 \sum_{j=0}^{p^s-1} a_{2j}(x-1)^j] \\
&[u(x-1)^l + u^2(x-1)^t h(x)] \\
=& u(x-1)^l \sum_{j=0}^{p^s-1} a_{0j}(x-1)^j + u^2(x-1)^t h(x) \sum_{j=0}^{p^s-1} a_{0j}(x-1)^j \\
&+ u^2(x-1)^l \sum_{j=0}^{p^s-1} a_{1j}(x-1)^j \\
=& u(x-1)^l \sum_{j=0}^{p^s-l-1} a_{0j}(x-1)^j + u(x-1)^{p^s} \sum_{j=p^s-l}^{p^s-1} a_{0j}(x-1)^{j+l-p^s} \\
&+ u^2(x-1)^l \sum_{j=0}^{p^s-l-1} a_{1j}(x-1)^j + u^2(x-1)^{p^s} \sum_{j=p^s-l}^{p^s-1} a_{1j}(x-1)^{j+l-p^s} \\
&+ u^2(x-1)^t h(x) \sum_{j=0}^{p^s-l-1} a_{0j}(x-1)^j + u^2(x-1)^t h(x) \sum_{j=p^s-l}^{p^s-1} a_{0j}(x-1)^j \\
=& u^2(x-1)^l \sum_{j=0}^{p^s-l-1} a_{1j}(x-1)^j + u^2(x-1)^{p^s-l+t} h(x) \sum_{j=0}^{l-1} a_{0,p^s-l+j}(x-1)^j.
\end{aligned}$$

So $T \geq \min\{l, p^s - l + t\}$. Moreover,

$$[u(x-1)^l + u^2(x-1)^t h(x)] \cdot (x-1)^{p^s-l} = u^2(x-1)^{p^s-l+t} h(x).$$

Hence $u^2(x-1)^{p^s-l+t} = [u(x-1)^l + u^2(x-1)^t h(x)] h^{-1}(x) \in C$. Thus $T \leq p^s - l + t$, which means that $T = \min\{l, p^s - l + t\}$. □

Similarly, we can prove the following proposition.

Proposition 4.5. *In Type* 7*, we have*

$$T = \begin{cases} q, & \text{if } h(x) = 0, \\ \min\{q, p^s - q + z\}, & \text{if } h(x) \neq 0. \end{cases}$$

5. γ-constacyclic codes of length p^s over R

In this section, we discuss the γ-constacyclic codes by constructing a one-to-one correspondence between cyclic and γ-constacyclic code to apply our results from Section 5 to γ-constacyclic code.

Since γ is a nonzero element of the field $\mathbb{F}_{p^m}$, there exists γ_0 such that $\gamma_0^{p^s} = \gamma^{-1}$. Similarly with Proposition 6.1 of [7], we have the following proposition.

Proposition 5.1. *The map* $\psi : \frac{R[x]}{\langle x^{p^s}-1\rangle} \to \frac{R[x]}{\langle x^{p^s}-\gamma\rangle}$ *given by* $f(x) \mapsto f(\gamma_0 x)$ *is a ring isomorphism. In particular, for* $A \subseteq \frac{R[x]}{\langle x^{p^s}-1\rangle}, B \subseteq \frac{R[x]}{\langle x^{p^s}-\gamma\rangle}$ *with* $\psi(A) = B$*. Then* A *is an ideal of* $\frac{R[x]}{\langle x^{p^s}-1\rangle}$ *if and only if* B *is an ideal of* $\frac{R[x]}{\langle x^{p^s}-\gamma\rangle}$*. Equivalently,* A *is a cyclic code of length* p^s *over* R *if and only if* B *is a* γ*-constacyclic code of length* p^s *over* R*.*

Using the isomorphism ψ, we can apply the results about cyclic code of length p^s over R in Section 4 to corresponding γ-constacyclic codes of length p^s over R. Indeed, the results in Section 4 for cyclic codes hold with γ-constacyclic codes by replacing x by $\gamma_0 x$ and writing $h(x), h_1(x)$ and $h_2(x)$ more explicitly.

References

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

[2] T. Blackford, *Cyclic code over* $\mathbb{Z}_4$ *of oddly even length*, Discrete Appl. Math. **138** (2003), no. 1, 27–40.

[3] ———, *Negacyclic codes over* $\mathbb{Z}_4$ *of even length*, IEEE Trans. Inform. Theory **49** (2003), no. 6, 1417–1424.

[4] H. Q. Dinh, *Negacyclic codes of length* 2^s *over Galois rings*, IEEE Trans. Inform. Theory **51** (2005), no. 12, 4252–4262.

[5] ———, *On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions*, Finite Field Appl. **14** (2008), no. 1, 22–40.

[6] ———, *Constacyclic codes of length* 2^s *over Galois exlension rings of* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory **55** (2009), no. 4, 1730–1740.

[7] ———, *Constacyclic codes of length* p^s *over* $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, J. Algebra **324** (2010), no. 5, 940–950.

[8] H. Q. Dinh and S. R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory **50** (2004), no. 8, 1728–1744.

[9] S. T. Dougherty and S. Ling, *Cyclic codes over* $\mathbb{Z}_4$ *of even length*, Des. Codes Cryptogr. **39** (2006), no. 2, 127–153.

[10] A. R. Hammous, Jr., P. V. Kumar, A. R. Calderbark, J. A. Sloame, and P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kordock, Preparata, Goethals, and releted codes*, IEEE Trans. Inform. Theory **40** (1994), 301–319.

[11] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.

[12] P. Kanwar and S. R. Lopez-Permouth, *Cyclic codes over the integers modulo* $\mathbb{Z}_{p^m}$, Finite Field Appl. **3** (1997), no. 4, 334–352.

[13] S. Ling, H. Niederreiter, and P. Solé, *On the algebraic structure of quasi-cyclic codes. IV*, Repeated root, Des. Codes. Cryplogr. **38** (2006), no. 3, 337–361.

[14] G. H. Norton and A. Sálăgean, *On the struture of linear and cyclic codes over a finite chain ring*, AAECC **10** (2000), no. 6, 489–506.

[15] V. Pless and W. C. Huffman, *Handbook of Coding Theory*, Elsevier, Amsterdam, 1998.

[16] A. Sălăgean, *Repelated-root cyclic and negacyclic codes over finite chain rings*, Discrete Appl. Math. **154** (2006), 413–419.

[17] J. Wolfmann, *Negacyclic and cyclic codes over* $\mathbb{Z}_4$, IEEE Trans. Inform. Theory. **45** (1999), no. 7, 2527–2532.

[18] S. Zhu and X. Kai, *Dual and self-dual negacyclic codes of even length over* $\mathbb{Z}_{2^a}$, Discrete Math. **309** (2009), no. 8, 2382–2391.

[19] ———, *A class of constacyclic codes over* $\mathbb{Z}_{p^m}$, Finite Field Appl. **16** (2010), no. 4, 243–254.

Xiusheng Liu
School of Mathematics and Physics
Hubei Polytechnic University
Huangshi, Hubei 435003, P. R. China
E-mail address: lxs6682@163.com

Xiaofang Xu
School of Mathematics and Physics
Hubei Polytechnic University
Huangshi, Hubei 435003, P. R. China
E-mail address: yenxingxxf@yahoo.com.cn