Journal of Algebra 324 (2010) 940–950

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

Hai Q. Dinh

Department of Mathematical Sciences, Kent State University, 4314 Mahoning Avenue, Warren, OH 44483, USA

ARTICLE INFO

Article history:
Received 31 January 2008
Available online 16 June 2010
Communicated by Gerhard Hiss

Keywords:
Cyclic codes
Constacyclic codes
Repeated-root codes
Codes over rings
Hamming distance

ABSTRACT

For any prime p, all constacyclic codes of length p^s over the ring $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ are considered. The units of the ring $\mathcal{R}$ are of the forms γ and $\alpha + u\beta$, where α, β, and γ are nonzero elements of $\mathbb{F}_{p^m}$, which provides $p^m(p^m - 1)$ such constacyclic codes. First, the structure and Hamming distances of all constacyclic codes of length p^s over the finite field $\mathbb{F}_{p^m}$ are obtained; they are used as a tool to establish the structure and Hamming distances of all $(\alpha + u\beta)$-constacyclic codes of length p^s over $\mathcal{R}$. We then classify all cyclic codes of length p^s over $\mathcal{R}$ and obtain the number of codewords in each of those cyclic codes. Finally, a one-to-one correspondence between cyclic and γ-constacyclic codes of length p^s over $\mathcal{R}$ is constructed via ring isomorphism, which carries over the results regarding cyclic codes corresponding to γ-constacyclic codes of length p^s over $\mathcal{R}$.

1. Introduction

The class of constacyclic codes plays a very significant role in the theory of error-correcting codes. The most important class of these codes is that of cyclic codes, which have been well studied since the late 1950s. However, most of this research is concentrated on the situation in which the code length n is relatively prime to the characteristics of the field F. In such cases, λ-constacyclic codes of length n are classified as ideals $\langle f(x)\rangle$ of $\frac{F[x]}{\langle x^n-\lambda\rangle}$, where $f(x)$ is a divisor of $x^n - \lambda$. The case when the code length n is divisible by the characteristics p of the field yields the so-called repeated-root codes, which were first studied in 1967 by Berman [4] and then in the 1970s and 1980s by authors such as Massey et al. [18], Falkner et al. [13], and Roth and Seroussi [23]. Repeated-root codes were investigated in the most generality in the 1990s by Castagnoli et al. [9] and van Lint [28]. They showed that repeated-root cyclic codes have a concatenated construction and are asymptotically bad.

E-mail address: hdinh@kent.edu.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2010.05.027

Nevertheless, such codes are optimal in a few cases, which has motivated researchers to further study this class of codes ([26,20,29]).

After the realization in the 1990s [8,14,19] that many important yet seemingly non-linear codes over finite fields are actually closely related to linear codes over $\mathbb{Z}_4$ in particular, and codes over finite rings in general; these codes have received a great deal of attention. Since 2003, special classes of repeated-root constacyclic codes over certain classes of finite chain rings have been studied by numerous authors [1,5,6,21,24]. In recent years, we have studied the description of several classes of constacyclic codes, such as cyclic and negacyclic codes, over various types of finite rings. In this paper, we continue to study repeated-root constacyclic codes over the chain ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$.

The class of finite rings of the form $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ has been used widely as alphabets in certain constacyclic codes. For example, the structure of $\mathbb{F}_2 + u\mathbb{F}_2$ is interesting, as it lies between $\mathbb{F}_4$ and $\mathbb{Z}_4$ in the sense that it is additively analogous to $\mathbb{F}_4$ and multiplicatively analogous to $\mathbb{Z}_4$. It has been studied by many researchers [7,27,25,3,2,15]. The purpose of this paper is to investigate all constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ in general, i.e., for any prime p and positive integer m. Among other results, such constacyclic codes are classified, and their structures are established.

After presenting preliminary concepts and results in Section 2, we proceed by first obtaining the structure and Hamming distances of all constacyclic codes of length p^s over the finite field $\mathbb{F}_{p^m}$ in Section 3. This step is accomplished by simply constructing a one-to-one correspondence between negacyclic and constacyclic codes of length p^s over $\mathbb{F}_{p^m}$ to apply results regarding negacyclic codes over $\mathbb{F}_{p^m}$ obtained in [11] to constacyclic codes. The structure and Hamming distances of those constacyclic codes over $\mathbb{F}_{p^m}$ are then used as one of the tools to establish the structure and Hamming distances of $(\alpha + u\beta)$-constacyclic codes of length p^s over $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ in Section 4. We show that such $(\alpha + u\beta)$-constacyclic codes are linearly ordered under set theory inclusion as ideals of the chain ring $\mathcal{R}_{\alpha,\beta} = \frac{\mathcal{R}[x]}{\langle x^{p^s} - (\alpha + u\beta)\rangle}$, which has a maximal ideal of $\langle \alpha_0 x - 1\rangle$ and where α_0 is completely determined by α, s, and m. Section 5 addresses the cyclic codes of length p^s over $\mathcal{R}$. These cyclic codes are the ideals of the ring $\mathcal{R}_1 = \frac{\mathcal{R}[x]}{\langle x^{p^s} - 1\rangle}$, 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 $\mathcal{R}_1$ into 4 types, namely, trivial ideals, principal ideals with nonmonic polynomial generators, principal ideals with monic polynomial generators, and nonprincipal ideals. We provide a detailed structure of ideals in each type. Among other results, we are able to obtain the number of codewords in each cyclic code. Finally, in Section 6, we build a one-to-one correspondence between cyclic and γ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$ via the ring isomorphisms Ψ, which allows us to apply our results about cyclic codes in Sections 5 to γ-constacyclic codes over $\mathcal{R}$.

2. Preliminary concepts

All rings are commutative rings. An ideal I of a ring R is called *principal* if it is generated by one element. A ring R is a principal ideal ring if its ideals are principal. R is called a local ring if $R/rad\, R$ is a division ring or, equivalently, if R has a unique maximal ideal. Furthermore, a ring R is called a chain ring if the set of all ideals of R is linearly ordered under set theory inclusion.

The following equivalence conditions are known for the class of finite commutative rings (see [12, Proposition 2.1]).

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 $\langle r^i\rangle$, $0 \leqslant i \leqslant N(r)$, where $N(r)$ is the nilpotency of r.*

Let R be a finite ring. A code C of length n over R is a nonempty subset of R^n, and the ring R is referred to as the alphabet of the code. If this subset is also an R-submodule of R^n, then C is called *linear*. For a unit λ of R, the λ-constacyclic (λ-twisted) shift τ_λ on R^n is the shift

$$\tau_\lambda(x_0, x_1, \ldots, x_{n-1}) = (\lambda x_{n-1}, x_0, x_1, \ldots, x_{n-2}).$$

A code C is said to be λ-constacyclic if $\tau_\lambda(C) = C$, i.e., if C is closed under the λ-constacyclic shift τ_λ. In the case that $\lambda = 1$, these λ-constacyclic codes are called cyclic codes, and when $\lambda = -1$, these λ-constacyclic codes are called negacyclic codes.

Each codeword $c = (c_0, c_1, \ldots, c_{n-1})$ is customarily identified with its polynomial representation $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$, and the code C is in turn identified with the set of all polynomial representations of its codewords. Then in the ring $\frac{R[x]}{\langle x^n - \lambda\rangle}$, $xc(x)$ corresponds to a λ-constacyclic shift of $c(x)$. From that, the following proposition is well known [17,16] and straightforward:

Proposition 2.2. *A linear code C of length n is λ-constacyclic over R if and only if C is an ideal of $\frac{R[x]}{\langle x^n - \lambda\rangle}$.*

Given n-tuples $x = (x_0, x_1, \ldots, x_{n-1})$, $y = (y_0, y_1, \ldots, y_{n-1}) \in R^n$, their inner product or dot product is defined as usual, with $x \cdot y = x_0y_0 + x_1y_1 + \cdots + x_{n-1}y_{n-1}$, which is evaluated in R. Two n-tuples x and y are called *orthogonal* if $x \cdot y = 0$. For a linear code C over R, its *dual code* $C^\perp$ is the set of n-tuples over R that are orthogonal to all codewords of C, i.e., $C^\perp = \{x \mid x \cdot y = 0,\ \forall y \in C\}$. A code C is called *self-orthogonal* if $C \subseteq C^\perp$, and it is called *self-dual* if $C = C^\perp$. The following proposition is well known [17,10,16,22].

Proposition 2.3. *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., $|C| \cdot |C^\perp| = |R|^n$.*

In general, the dual of a λ-constacyclic code implies the following proposition.

Proposition 2.4. *The dual of a λ-constacyclic code is a λ^{-1}-constacyclic code.*

Proof. Let C be a λ-constacyclic code of length n over R. Consider arbitrary elements $x \in C^\perp$ and $y \in C$. Because C is λ-constacyclic, $\tau_\lambda^{n-1}(y) \in C$. Thus, $0 = x \cdot \tau_\lambda^{n-1}(y) = \lambda\tau_{\lambda^{-1}}(x) \cdot y = \tau_{\lambda^{-1}}(x) \cdot y$, which means that $\tau_{\lambda^{-1}}(x) \in C^\perp$. Therefore, $C^\perp$ is closed under the $\tau_{\lambda^{-1}}$-shift; i.e., $C^\perp$ is a λ^{-1}-constacyclic code. □

For a codeword $x = (x_0, x_1, \ldots, x_{n-1}) \in R^n$, the *Hamming weight* of x, denoted by $\mathrm{wt}(x)$, is the number of nonzero components of x. The Hamming distance $d(x, y)$ of two codewords x and y equals the number of components in which they differ, which is the Hamming weight $\mathrm{wt}(x - y)$ of $x - y$. For a nonzero linear code C, the Hamming weight and the Hamming distance $d(C)$ are the same and defined as the smallest Hamming weight of nonzero codewords of C:

$$d(C) = \min\{\mathrm{wt}(x) \mid x \neq \mathbf{0},\ x \in C\}.$$

The zero code is conventionally said to have Hamming distance 0.

In this paper, we consider all constacyclic codes of length p^s with alphabet $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. The ring $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ consists of all p^m-ary polynomials of degree 0 and 1 in an indeterminate u, and it is closed under p^m-ary polynomial addition and multiplication modulo u^2. Thus, $\mathcal{R} = \frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle} = \{a + ub \mid a, b \in \mathbb{F}_{p^m}\}$ is a local ring with maximal ideal $u\mathbb{F}_{p^m}$. Therefore, by Proposition 2.1, it is a chain ring. The ring $\mathcal{R}$ has precisely $p^m(p^m - 1)$ units, which are of the forms $\alpha + u\beta$ and γ, where α, β, and γ are nonzero elements of the field $\mathbb{F}_{p^m}$.

For a code C of length n over $\mathcal{R}$, their torsion and residue codes are codes over $\mathbb{F}_{p^m}$, defined as follows.

$$\mathrm{Tor}(C) = \{\mathbf{a} \in \mathbb{F}_{p^m}^n \mid u\mathbf{a} \in C\}, \qquad \mathrm{Res}(C) = \{\mathbf{a} \in \mathbb{F}_{p^m}^n \mid \exists \mathbf{b}\colon\ \mathbf{a} + u\mathbf{b} \in C\}.$$

The reduction modulo u from C to $\mathrm{Res}(C)$ is given by $\phi : C \longrightarrow \mathrm{Res}(C)$, $\phi(\mathbf{a} + u\mathbf{b}) = \mathbf{a}$. Clearly, ϕ is well defined and onto, with $\mathrm{Ker}(\phi) = \mathrm{Tor}(C)$, and $\phi(C) = \mathrm{Res}(C)$. Therefore, $|\mathrm{Res}(C)| = \frac{|C|}{|\mathrm{Tor}(C)|}$. Thus, we obtain:

Proposition 2.5. *Let C be a constacyclic code of length n over $\mathcal{R}$, whose torsion and residue codes are* $\mathrm{Tor}(C)$ *and* $\mathrm{Res}(C)$. *Then* $|C| = |\mathrm{Tor}(C)| \cdot |\mathrm{Res}(C)|$.

3. Constacyclic codes of length p^s over $\mathbb{F}_{p^m}$

In [11], the structure and Hamming distances of negacyclic codes of length p^s over $\mathbb{F}_{p^m}$ were established. We now apply all these results to λ-constacyclic codes over $\mathbb{F}_{p^m}$ by providing a one-to-one correspondence between negacyclic and λ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$.

Because λ is a nonzero element of the field $\mathbb{F}_{p^m}$, $\lambda^{-p^m} = \lambda^{-1}$. Using the positive integers s and m as the dividend and divisor, by the division algorithm, there exist nonnegative integers λ_q, λ_r such that $s = \lambda_q m + \lambda_r$, and $0 \leqslant \lambda_r \leqslant m-1$. Let $\lambda_0 = -\lambda^{-p^{(\lambda_q+1)m-s}} = -\lambda^{-p^{m-\lambda_r}}$. Then $\lambda_0^{p^s} = -\lambda^{-p^{(\lambda_q+1)m}} = -\lambda^{-1}$.

Proposition 3.1. *Let Φ be the map $\Phi : \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^m}+1\rangle} \longrightarrow \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^m}-\lambda\rangle}$, given by $\Phi(f(x)) = f(\lambda_0 x)$. Then Φ is a ring isomorphism, and it is Hamming weight preserving.*

Proof. For polynomials $f(x)$ and $g(x) \in \mathbb{F}_{p^m}[x]$, $f(x) \equiv g(x) \pmod{x^{p^s}+1}$ if and only if there exists a polynomial $h(x) \in \mathbb{F}_{p^m}[x]$ such that $f(x) - g(x) = h(x)(x^{p^s}+1)$, if and only if

$$f(\lambda_0 x) - g(\lambda_0 x) = h(\lambda_0 x)\big[(\lambda_0 x)^{p^s} + 1\big] = -\lambda^{-1} h(\lambda_0 x)\big(x^{p^s} - \lambda\big),$$

which is equivalent to $f(\lambda_0 x) \equiv g(\lambda_0 x) \pmod{x^{p^s} - \lambda}$. This means that for $f, g \in \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^m}+1\rangle}$, $\Phi(f(x)) = \Phi(g(x))$ if and only if $f(x) = g(x)$. Therefore, Φ is well defined and one-to-one. It is obvious that Φ is onto and weight-preserving, and it is easy to verify that Φ is a ring homomorphism. Thus, Φ is a ring isomorphism. □

The ring isomorphism Φ provides a one-to-one correspondence between negacyclic and λ-constacyclic code of length p^s over $\mathbb{F}_{p^m}$:

Corollary 3.2. *Let $A \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^m}+1\rangle}$, $B \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^m}-\lambda\rangle}$ be such that $\Phi(A) = B$. Then A is an ideal of $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^m}+1\rangle}$ if and only if B is an ideal of $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^m}-\lambda\rangle}$. Equivalently, A is a negacyclic code of length p^s over $\mathbb{F}_{p^m}$ if and only if B is a λ-constacyclic code of length p^s over $\mathbb{F}_{p^m}$.*

Thus, our results about negacyclic codes of length p^s over $\mathbb{F}_{p^m}$ in [11] can be carried over correspondingly to λ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$ via the isomorphism Φ.

Theorem 3.3. *(See [11, 3.1, 3.2, 3.3].) $\lambda_0 x + 1$ is a nilpotent element of $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^m}-\lambda\rangle}$ with nilpotency index p^s. The ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^m}-\lambda\rangle}$ is a chain ring with the maximal ideal of $\langle \lambda_0 x + 1\rangle$. λ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$ are precisely the ideals $\langle(\alpha_0 x + 1)^i\rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^m}-\lambda\rangle}$, where $0 \leqslant i \leqslant p^s$, which forms the strictly inclusive chain*

$$\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^m} - \lambda\rangle} = \langle 1\rangle \supsetneq \langle \lambda_0 x + 1\rangle \supsetneq \cdots \supsetneq \big\langle (\lambda_0 x + 1)^{p^s-1}\big\rangle \supsetneq \big\langle (\lambda_0 x + 1)^{p^s}\big\rangle = \langle 0\rangle.$$

Each λ-constacyclic code $\langle(\lambda_0 x + 1)^i\rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^m}-\lambda\rangle}$ has $p^{m(p^s-i)}$ codewords.

Theorem 3.4. *(Cf. [11, 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*

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

4. $(\alpha + u\beta)$-Constacyclic codes of length p^s over $\mathcal{R}$

Let α, β be nonzero elements of the field $\mathbb{F}_{p^m}$, then $\alpha + u\beta$ is a unit of $\mathcal{R}$. The $(\alpha + u\beta)$-constacyclic codes of length p^s over $\mathcal{R}$ are ideals of the ring $\mathcal{R}_{\alpha,\beta} = \frac{\mathcal{R}[x]}{\langle x^{p^s} - (\alpha + u\beta) \rangle}$. As in Section 3, by the division algorithm, there exist nonnegative integers α_q, α_r such that $s = \alpha_q m + \alpha_r$, and $0 \leqslant \alpha_r \leqslant m-1$. 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 4.1. *In $\mathcal{R}_{\alpha,\beta}$, $\langle (\alpha_0 x - 1)^{p^s} \rangle = \langle u \rangle$. In particular, $\alpha_0 x - 1$ is nilpotent in $\mathcal{R}_{\alpha,\beta}$ with nilpotency index $2p^s$.*

Proof. For $1 \leqslant i \leqslant p^s - 1$, $p \mid \binom{p^s}{i}$, hence, computing in $\mathcal{R}_{\alpha,\beta}$,

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

Thus, $\langle (\alpha_0 x - 1)^{p^s} \rangle = \langle u \rangle$. The last statement is straightforward because u has nilpotency index 2 in $\mathcal{R}_{\alpha,\beta}$. □

Each element $r \in \mathcal{R}$ has a unique presentation as $r = r_1 + ur_2$, where $r_1, r_2 \in \mathbb{F}_{p^m}$. This means that each polynomial $f(x)$ of degree less than n in $\mathcal{R}[x]$ can be (uniquely) represented as

$$f(x) = \sum_{i=0}^{n-1} b_{0i} (\alpha_0 x - 1)^i + u \sum_{i=0}^{n-1} b_{1i} (\alpha_0 x - 1)^i,$$

where $b_{0i}, b_{1i} \in \mathbb{F}_{p^m}$. Thus, each codeword $\mathbf{c}$ of a $(\alpha + u\beta)$-constacyclic code of length p^s over $\mathcal{R}$ has its polynomial representation $c(x) \in \mathcal{R}_{\alpha,\beta}$ expressed as

$$\begin{aligned} c(x) &= \sum_{i=0}^{p^s-1} c_{0i} (\alpha_0 x - 1)^i + u \sum_{i=0}^{p^s-1} c_{1i} (\alpha_0 x - 1)^i \\ &= c_{00} + (\alpha_0 x - 1) \sum_{i=1}^{p^s-1} c_{0i} (\alpha_0 x - 1)^{i-1} + u \sum_{i=0}^{p^s-1} c_{1i} (\alpha_0 x - 1)^i, \end{aligned}$$

where $c_{0i}, c_{1i} \in \mathbb{F}_{p^m}$. Because $\alpha_0 x - 1$ and u are nilpotent in $\mathcal{R}_{\alpha,\beta}$, $c(x)$ is invertible if and only if $c_{00} \neq 0$. Moreover, by Lemma 4.1, $\langle u \rangle = \langle (\alpha_0 x - 1)^{p^s} \rangle$; hence, in the case that $c(x)$ is not invertible (i.e., $c_{00} = 0$), $c(x)$ must be in $\langle \alpha_0 x - 1 \rangle$. Thus, $\langle \alpha_0 x - 1 \rangle$ is the ideal consisting of all noninvertible elements of $\mathcal{R}_{\alpha,\beta}$. Therefore, $\mathcal{R}_{\alpha,\beta}$ is a local ring with maximal ideal $\langle \alpha_0 x - 1 \rangle$. In light of Proposition 2.1, $\mathcal{R}_{\alpha,\beta}$ is a chain ring. We summarize this important fact in the following theorem.

Theorem 4.2. *$\mathcal{R}_{\alpha,\beta}$ is a chain ring with ideals that are precisely*

$$\mathcal{R}_{\alpha,\beta} = \langle 1\rangle \supsetneq \langle(\alpha_0 x-1)\rangle \supsetneq \cdots \supsetneq \left\langle(\alpha_0 x-1)^{2p^s-1}\right\rangle \supsetneq \left\langle(\alpha_0 x-1)^{2p^s}\right\rangle = \langle 0\rangle.$$

$(\alpha+u\beta)$-constacyclic codes of length p^s over $\mathcal{R}$ are the ideals $\langle(\alpha_0 x-1)^i\rangle$, $0\leqslant i\leqslant 2p^s$, of the chain ring $\mathcal{R}_{\alpha,\beta}$. Each code $\langle(\alpha_0 x-1)^i\rangle$ contains $p^{m(2p^s-i)}$ codewords.

We have $(\alpha+u\beta)^{p^m} = \alpha^{p^m} = \alpha$; hence, $(\alpha+u\beta)^{p^m}\alpha^{-1} = 1$. Therefore, $(\alpha+u\beta)^{-1} = (\alpha+u\beta)^{p^m-1}\alpha^{-1} = (\alpha^{p^m-1}+u\beta\alpha^{p^m-2})\alpha^{-1} = (1+u\beta\alpha^{-1})\alpha^{-1} = \alpha^{-1}+u\beta\alpha^{-2}$. Thus, by Proposition 2.4, for a $(\alpha+u\beta)$-constacyclic code of length p^s over $\mathcal{R}$, $C = \langle(\alpha_0 x+1)^i\rangle \subseteq \mathcal{R}_{\alpha,\beta}$, its dual $C^\perp$ is a $(\alpha^{-1}+u\beta\alpha^{-2})$-constacyclic code of length p^s over $\mathcal{R}$. That means $C^\perp$ is an ideal of the chain ring $\mathcal{R}_{\alpha^{-1},\beta\alpha^{-2}} = \frac{\mathcal{R}[x]}{\langle x^{p^s}-(\alpha^{-1}+u\beta\alpha^{-2})\rangle}$. However, because $|C| = p^{m(2p^s-i)}$, $|C^\perp| = p^{mi}$. Hence, $C^\perp = \langle(\alpha_0^{-1}x-1)^{2p^s-i}\rangle \subseteq \mathcal{R}_{\alpha^{-1},\beta\alpha^{-2}}$. Thus, we have proven the following theorem about the duals of $(\alpha+u\beta)$-constacyclic codes.

Theorem 4.3. *For each $(\alpha+u\beta)$-constacyclic code of length p^s over $\mathcal{R}$, $C = \langle(\alpha_0 x-1)^i\rangle \subseteq \mathcal{R}_{\alpha,\beta}$, its dual is the $(\alpha^{-1}+u\beta\alpha^{-2})$-constacyclic code $C^\perp = \langle(\alpha_0^{-1}x-1)^{2p^s-i}\rangle \subseteq \mathcal{R}_{\alpha^{-1},\beta\alpha^{-2}}$, which contains p^{mi} codewords.*

We now consider the Hamming distances of $(\alpha+u\beta)$-constacyclic codes of length p^s over $\mathcal{R}$. By Lemma 4.1, $\langle(\alpha_0 x-1)^{p^s}\rangle = \langle u\rangle$ in $\mathcal{R}_{\alpha,\beta}$. We consider two cases.

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

Case 2: $p^s+1\leqslant i\leqslant 2p^s-1$. Then $\langle(\alpha_0 x-1)^i\rangle = \langle u(\alpha_0 x-1)^{i-p^s}\rangle$, which means that the codewords of the code $\langle(\alpha_0 x-1)^i\rangle$ in $\mathcal{R}_{\alpha,\beta}$ are precisely the codewords of the code $\langle(\alpha_0 x-1)^{i-p^s}\rangle$ 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 $\langle(\alpha_0 x-1)^{i-p^s}\rangle$ 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 distances computed as Theorem 3.4.

Hence, we have the Hamming distances of all $(\alpha+u\beta)$-constacyclic codes of length p^s over $\mathcal{R}$:

Theorem 4.4. *Let C be a $(\alpha+u\beta)$-constacyclic code of length p^s over $\mathcal{R}$. Then $C = \langle(\alpha_0 x-1)^i\rangle \subseteq \mathcal{R}_{\alpha,\beta}$ for $i\in\{0,1,\ldots,2p^s\}$, and the Hamming distance $d(C)$ is completely determined by*

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

5. Cyclic codes of length p^s over $\mathcal{R}$

Cyclic codes of length p^s over $\mathcal{R}$ are ideals of the residue ring $\mathcal{R}_1 = \frac{\mathcal{R}[x]}{\langle x^{p^s}-1\rangle}$. The following fact is easy to verify, and will play an important role in our consideration later:

Lemma 5.1. *For any non-negative integer n, $(x-1)^{p^n} = x^{p^n}-1$ in $\mathcal{R}[x]$. In particular, $x-1$ is nilpotent in $\mathcal{R}_1$ with nilpotency index p^s.*

Lemma 5.2. *Let $f(x) \in \mathcal{R}_1$. Then $f(x)$ can be uniquely expressed as*

$$f(x) = \sum_{i=0}^{p^s-1} a_{0i}(x-1)^i + u\sum_{i=0}^{p^s-1} a_{1i}(x-1)^i = a_{00} + (x-1)\sum_{i=1}^{p^s-1} a_{0i}(x-1)^{i-1} + u\sum_{i=0}^{p^s-1} a_{1i}(x-1)^i,$$

where $a_{0i}, a_{1i} \in \mathbb{F}_{p^m}$. Furthermore, $f(x)$ is invertible if and only if $a_{00} \neq 0$.

Proof. The representation of $f(x)$ follows from the fact that it can be viewed as a polynomial of degree less than p^s over $\mathcal{R}$. Each coefficient a_i of $f(x)$ is an element of $\mathcal{R}$, that can be expressed uniquely by $a_{0i}, a_{1i} \in \mathbb{F}_{p^m}$ as $a_i = a_{0i} + ua_{1i}$. Expressing $f(x)$ in this representation, the last assertion follows from the fact that u and $x-1$ are both nilpotent in $\mathcal{R}_1$. □

Proposition 5.3. *The ring $\mathcal{R}_1$ is a local ring with the maximal ideal $\langle u, x-1\rangle$, but it is not a chain ring.*

Proof. By Lemma 5.2, the ideal $\langle u, x-1\rangle$ is the set of all non-invertible elements of $\mathcal{R}_1$. Hence, $\mathcal{R}_1$ is a local ring with maximal ideal $\langle u, x-1\rangle$. Suppose $u \in \langle x-1\rangle$. Then there are polynomials $f_1(x)$ and $f_2(x) \in \mathcal{R}[x]$ such that $u = (x-1)f_1(x) + (x^{p^s}-1)f_2(x)$. However, this is impossible because plugging in $x = 1$ yields $u = 0$. Hence, $u \notin \langle x-1\rangle$. Obviously, $x-1 \notin \langle u\rangle$, because, for example, $(x-1)^2 \neq 0$ in $\mathcal{R}_1$. Thus, $\langle u, x-1\rangle$ is not a principal ideal of $\mathcal{R}_1$, implying that $\mathcal{R}_1$ is not a chain ring according to Proposition 2.1. □

Theorem 5.4. *Cyclic codes of length p^s over $\mathcal{R}$, i.e., ideals of the ring $\mathcal{R}_1$, are*

- *Type* 1 (*trivial ideals*): $\langle 0\rangle$, $\langle 1\rangle$.
- *Type* 2 (*principal ideals with nonmonic polynomial generators*): $\langle u(x-1)^i\rangle$, *where* $0 \leqslant i \leqslant p^s - 1$.
- *Type* 3 (*principal ideals with monic polynomial generators*): $\langle (x-1)^i + u(x-1)^t h(x)\rangle$, *where* $1 \leqslant i \leqslant p^s - 1$, $0 \leqslant t < i$, *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 $h_0 \neq 0$.*
- *Type* 4 (*nonprincipal ideals*): $\langle (x-1)^i + u\sum_{j=0}^{\omega-1} c_j(x-1)^j, u(x-1)^\omega\rangle$, *where* $1 \leqslant i \leqslant p^s - 1$, $c_j \in \mathbb{F}_{p^m}$, *and $\omega < T$, where T is the smallest integer such that $u(x-1)^T \in \langle (x-1)^i + u\sum_{j=0}^{i-1} c_j(x-1)^j\rangle$; or equivalently, $\langle (x-1)^i + u(x-1)^t h(x), u(x-1)^\omega\rangle$, with $h(x)$ as in Type* 3, *and* $\deg(h) \leqslant \omega - t - 1$.

Proof. Ideals of Type 1 are the trivial ideals. Let I be an arbitrary nontrivial ideal of $\mathcal{R}_1$. We proceed by establishing all possible forms that the ideal I can have.

- Case 1. $I \subseteq \langle u\rangle$: Then any element of I must have the form $u\sum_{i=0}^{p^s-1} b_{1i}(x-1)^i$, where $b_{1i} \in \mathbb{F}_{p^m}$. Then there exists an element $b \in I$ that has the smallest k such that $b_{1k} \neq 0$. Hence, each element $c(x) \in I$ has the form $c(x) = u(x-1)^k\sum_{i=k}^{p^s-1} c_{1i}(x-1)^{i-k}$, which implies $I \subseteq \langle u(x-1)^k\rangle$. However, we have $b \in I$ with

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

  As $b_{1k} \neq 0$, $b_{1k} + \sum_{i=k+1}^{p^s-1} b_{1i}(x-1)^{i-k}$ is invertible, and thus, $u(x-1)^k \in I$. Therefore, $I = \langle u(x-1)^k\rangle$, which means that the nontrivial ideals of $\mathcal{R}_1$ contained in $\langle u\rangle$ are $\langle u(x-1)^k\rangle$, $0 \leqslant k \leqslant p^s - 1$, which are ideals of Type 2.
- Case 2. $I \nsubseteq \langle u\rangle$: Let I_u denote the set of elements in I reduced modulo u. Then I_u is a nonzero ideal of the ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$, which is a chain ring with ideals $\langle (x-1)^j\rangle$, where $0 \leqslant j \leqslant p^s$, according to [11, Propositions 3.2, 6.1, and Theorem 6.2]. Hence, there is an integer $i \in \{0, 1, \ldots, p^s - 1\}$

such that $I_u = \langle (x-1)^i \rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$. Therefore, there exists an element $c(x) = \sum_{j=0}^{p^s-1} c_{0j}(x-1)^j + u\sum_{j=0}^{p^s-1} c_{1j}(x-1)^j \in \mathcal{R}_1$, where $c_{0j}, c_{1j} \in \mathbb{F}_{p^m}$, such that $(x-1)^i + uc(x) \in I$. Because $(x-1)^i + uc(x) = (x-1)^i + u\sum_{j=0}^{p^s-1} c_{0j}(x-1)^j \in I$, and for all l with $i \leqslant l \leqslant p^s-1$, $u(x-1)^l = u[(x-1)^i + uc(x)](x-1)^{l-i} \in I$, it follows that $(x-1)^i + u\sum_{j=0}^{i-1} c_{0j}(x-1)^j \in I$. We now have two subcases.

- Case 2a. $I = \langle (x-1)^i + u\sum_{j=0}^{i-1} c_{0j}(x-1)^j \rangle$, then I can be expressed as $I = \langle (x-1)^i + u(x-1)^t h(x) \rangle$, such that either $h(x)$ is 0 or $h(x)$ is a unit that can be represented as $h(x) = break\sum_j h_j(x-1)^j$, with $h_j \in \mathbb{F}_{p^m}$, and $h_0 \neq 0$, which means that I is of Type 3.
- Case 2b. $\langle (x-1)^i + u\sum_{j=0}^{i-1} c_{0j}(x-1)^j \rangle \subsetneq I$. Then there exists $f(x) \in I \setminus \langle (x-1)^i + u\sum_{j=0}^{i-1} \times c_{0j}(x-1)^j \rangle$, and therefore, there is a polynomial $g(x) \in \mathcal{R}_1$ such that

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

and $h(x)$ can be expressed as $h(x) = \sum_{j=0}^{i-1} h_{0j}(x-1)^j + u\sum_{j=0}^{i-1} h_{1j}(x-1)^j$, where $h_{0j}, h_{1j} \in \mathbb{F}_{p^m}$. Now, $h(x)$ reduced modulo u is in $I_u = \langle (x-1)^i \rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$, and thus, $h_{0j} = 0$ for all $0 \leqslant j \leqslant i-1$, i.e., $h(x) = u\sum_{j=0}^{i-1} h_{1j}(x-1)^j$. Because $h(x) \neq 0$, there is a smallest integer k_f, $0 \leqslant k_f \leqslant i-1$, such that $h_{1k_f} \neq 0$. Then

$$h(x) = u\sum_{j=k_f}^{i-1} h_{1j}(x-1)^j = u(x-1)^{k_f}\left(h_{1k_f} + \sum_{j=k_f+1}^{i-1} h_{1j}(x-1)^{j-k_f}\right).$$

As $h_{1k_f} \neq 0$, $h_{1k_f} + \sum_{j=k_f+1}^{i-1} h_{1j}(x-1)^{j-k_f}$ is an invertible element in $\mathcal{R}_1$, and hence, $u(x-1)^{k_f} = (h_{1k_f} + \sum_{j=k_f+1}^{i-1} h_{1j}(x-1)^{j-k_f})^{-1} h(x) \in I$.

We have shown that for any $f(x) \in I \setminus \langle (x-1)^i + u\sum_{j=0}^{i-1} c_{0j}(x-1)^j \rangle$, there is an integer k_f, $0 \leqslant k_f \leqslant i-1$, such that $u(x-1)^{k_f} \in I$. Let $\omega = \min\{k_f \mid f(x) \in I \setminus \langle (x-1)^i + u\sum_{j=0}^{i-1} c_{0j} \times (x-1)^j \rangle\}$. Then, $\langle (x-1)^i + u\sum_{j=0}^{i-1} c_{0j}(x-1)^j, u(x-1)^\omega \rangle \subseteq I$. Moreover, by our above construction, for any $f(x) \in I$, there exists $g(x) \in I$ such that $f(x) - g(x)[(x-1)^i + u\sum_{j=0}^{i-1} c_{0j}(x-1)^j] \in \langle u(x-1)^\omega \rangle$, implying that, $f(x) \in \langle (x-1)^i + u\sum_{j=0}^{i-1} c_{0j}(x-1)^j, u(x-1)^\omega \rangle$. Thus,

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

Let T be the smallest integer such that $u(x-1)^T \in \langle (x-1)^i + u\sum_{j=0}^{i-1} c_j(x-1)^j \rangle$. If $\omega \geqslant T$, then, $I = \langle (x-1)^i + u\sum_{j=0}^{\omega-1} c_j(x-1)^j, u(x-1)^\omega \rangle = \langle (x-1)^i + u\sum_{j=0}^{i-1} c_j(x-1)^j \rangle$, which contradicts the assumption of this Case 2b. Hence, $\omega < T$, and therefore, I is of Type 4. □

For cyclic codes of Type 4 according to the classification in Theorem 5.4, the number T plays a very important role. We now determine T for each code $C = \langle (x-1)^i + u\sum_{j=0}^{\omega-1} c_j(x-1)^j, u(x-1)^\omega \rangle$. First, $T \leqslant i$ because $u(x-1)^i = u[(x-1)^i + u(x-1)^t h(x)] \in C$. In case $h(x) = 0$, then $C = \langle (x-1)^i \rangle$, implying $T = i$.

Consider the case $h(x) \neq 0$, and so $h(x)$ is a unit. Because $u(x-1)^T \in \langle (x-1)^i + u(x-1)^t h(x) \rangle$, there exists $f(x) \in \mathcal{R}_1$, such that $u(x-1)^T = f(x)[(x-1)^i + u(x-1)^t h(x)]$. Write $f(x)$ as $f(x) = \sum_{j=0}^{p^s-1} b_{0j}(x-1)^j + u\sum_{j=0}^{p^s-1} b_{1j}(x-1)^j$, where $b_{0j}, b_{1j} \in \mathbb{F}_{p^m}$. Then

$$
\begin{aligned}
u(x-1)^T &= \Bigg[\sum_{j=0}^{p^s-1} b_{0j}(x-1)^j + u\sum_{j=0}^{p^s-1} b_{1j}(x-1)^j\Bigg]\big[(x-1)^i + u(x-1)^t h(x)\big] \\
&= (x-1)^i \sum_{j=0}^{p^s-1} b_{0j}(x-1)^j + u(x-1)^i \sum_{j=0}^{p^s-1} b_{1j}(x-1)^j + u(x-1)^t h(x) \sum_{j=0}^{p^s-1} b_{0j}(x-1)^j \\
&= (x-1)^i \sum_{j=0}^{p^s-i-1} b_{0j}(x-1)^j + (x-1)^{p^s} \sum_{j=p^s-i}^{p^s-1} b_{0j}(x-1)^{j+i-p^s} \\
&\quad + u(x-1)^i \sum_{j=0}^{p^s-i-1} b_{1j}(x-1)^j + u(x-1)^{p^s} \sum_{j=p^s-i}^{p^s-1} b_{1j}(x-1)^{j+i-p^s} \\
&\quad + u(x-1)^t h(x) \sum_{j=0}^{p^s-i-1} b_{0j}(x-1)^j + u(x-1)^t h(x) \sum_{j=p^s-i}^{p^s-1} b_{0j}(x-1)^j \\
&= u(x-1)^i \sum_{j=0}^{p^s-i-1} b_{1j}(x-1)^j + u(x-1)^t h(x) \sum_{j=p^s-i}^{p^s-1} b_{0j}(x-1)^j \\
&= u(x-1)^i \sum_{j=0}^{p^s-i-1} b_{1j}(x-1)^j + u(x-1)^{p^s-i+t} h(x) \sum_{j=0}^{i-1} b_{0,p^s-i+j}(x-1)^j.
\end{aligned}
$$

So, $T \geqslant \min\{i, p^s - i + t\}$. Moreover, $[(x-1)^i + u(x-1)^t h(x)](x-1)^{p^s-i} = u(x-1)^{p^s-i+t} h(x)$. Hence, $u(x-1)^{p^s-i+t} = [h(x)]^{-1}[(x-1)^i + u(x-1)^t h(x)](x-1)^{p^s-i} \in C$. Thus, $T \leqslant p^s - i + t$, which means that $T = \min\{i, p^s - i + t\}$. Therefore, we have proven the following.

Proposition 5.5. *Let T be the smallest integer such that $u(x-1)^T \in C = \langle (x-1)^i + u(x-1)^t h(x)\rangle$. Then*

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

We now compute the number of codewords in each cyclic code C. According to Proposition 2.5, it can be done by establishing the sizes of the torsion and residue codes of C. By definition and our classification in Theorem 5.4, $\mathrm{Tor}(C)$ and $\mathrm{Res}(C)$ can be readily obtained.

Lemma 5.6. *Let C be a cyclic code of length p^s over $\mathcal{R}$, as classified in Theorem 5.4. Then the torsion and residue codes of C are determined as follows.*

(i) *Type 1 (trivial ideals):*
- *If $C = \langle 0\rangle$, then $\mathrm{Tor}(C) = \mathrm{Res}(C) = \langle 0\rangle$.*
- *If $C = \langle 1\rangle$, then $\mathrm{Tor}(C) = \mathrm{Res}(C) = \langle 1\rangle$.*

(ii) *Type 2 (principal ideals with nonmonic polynomial generators): $C = \langle u(x-1)^i\rangle$, where $0 \leqslant i \leqslant p^s - 1$; then $\mathrm{Tor}(C) = \langle (x-1)^i\rangle$, and $\mathrm{Res}(C) = \langle 0\rangle$.*

(iii) *Type 3 (principal ideals with monic polynomial generators): $C = \langle (x-1)^i + u(x-1)^t h(x)\rangle$, where $1 \leqslant i \leqslant p^s - 1$, $0 \leqslant t < i$, and either $h(x)$ is 0 or $h(x)$ is a unit. Then $\mathrm{Tor}(C) = \langle (x-1)^T\rangle$, and $\mathrm{Res}(C) = \langle (x-1)^i\rangle$, where T is the smallest integer such that $u(x-1)^T \in C$, which is given by*

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

(iv) *Type 4 (nonprincipal ideals)*: $C = \langle (x-1)^i + u(x-1)^t h(x), u(x-1)^\kappa \rangle$, *where* $1 \leqslant i \leqslant p^s - 1$, $0 \leqslant t < i$, *either* $h(x)$ *is 0 or* $h(x)$ *is a unit, and* $\kappa < T$; *then* $\mathrm{Tor}(C) = \langle (x-1)^\kappa \rangle$, *and* $\mathrm{Res}(C) = \langle (x-1)^i \rangle$.

Lemma 5.6 indicates that for any cyclic code C of length p^s over $\mathcal{R}$, the torsion code $\mathrm{Tor}(C)$ and residue code $\mathrm{Res}(C)$ are cyclic codes of length p^s over $\mathbb{F}_{p^m}$. In contrast, by [11, Theorem 6.2], each cyclic code of length p^s over $\mathbb{F}_{p^m}$ is an ideal of the form $\langle (x-1)^i \rangle$ of the chain ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1 \rangle}$, where $0 \leqslant i \leqslant p^s$, and this code $\langle (x-1)^i \rangle$ contains $p^{m(p^s-i)}$ codewords. Therefore, in light of Proposition 2.5, we can now determine the sizes of all cyclic codes of length p^s over $\mathcal{R}$ by multiplying the sizes of $\mathrm{Tor}(C)$ and $\mathrm{Res}(C)$ in each case.

Theorem 5.7. *Let C be a cyclic code of length p^s over $\mathcal{R}$, as classified in Theorem* 5.4. *Then the number of codewords n_C of C is determined as follows.*

- *If* $C = \langle 0 \rangle$, *then* $n_C = 1$.
- *If* $C = \langle 1 \rangle$, *then* $n_C = p^{2mp^s}$.
- *If* $C = \langle u(x-1)^i \rangle$, *where* $0 \leqslant i \leqslant p^s - 1$, *then* $n_C = p^{m(p^s-i)}$.
- *If* $C = \langle (x-1)^i \rangle$, *where* $1 \leqslant i \leqslant p^s - 1$, *then* $n_C = p^{2m(p^s-i)}$.
- *If* $C = \langle (x-1)^i + u(x-1)^t h(x) \rangle$, *where* $1 \leqslant i \leqslant p^s - 1$, $0 \leqslant t < i$, *and* $h(x)$ *is a unit, then*

$$n_C = \begin{cases} p^{2m(p^s-i)}, & \text{if } 1 \leqslant i \leqslant p^{s-1} + \frac{t}{2}, \\ p^{m(p^s-t)}, & \text{if } p^{s-1} + \frac{t}{2} < i \leqslant p^s - 1. \end{cases}$$

- *If* $C = \langle (x-1)^i + u(x-1)^t h(x), u(x-1)^\kappa \rangle$, *where* $1 \leqslant i \leqslant p^s - 1$, $0 \leqslant t < i$, *either* $h(x)$ *is 0 or* $h(x)$ *is a unit, and*

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

then $n_C = p^{m(2p^s-i-\kappa)}$.

6. γ-Constacyclic codes of length p^s over $\mathcal{R}$

As mentioned in Section 2, there are $p^m(p^m-1)$ constacyclic codes corresponding to the units γ and $\alpha + u\beta$ of $\mathcal{R}$, where α, β, γ are nonzero elements of $\mathbb{F}_{p^m}$. The $(\alpha + u\beta)$-constacyclic codes were studied in Section 4. In this section, we now address the γ-constacyclic codes by constructing a one-to-one correspondence between cyclic and γ-constacyclic codes to apply our results from Section 5 to γ-constacyclic codes.

Because γ is a nonzero element of the field $\mathbb{F}_{p^m}$, $\gamma^{-p^m} = \gamma^{-1}$. By the division algorithm, there exist nonnegative integers γ_q, γ_r such that $s = \gamma_q m + \gamma_r$, and $0 \leqslant \gamma_r \leqslant m-1$. Let $\gamma_0 = \gamma^{-p^{(\gamma_q+1)m-s}} = \gamma^{-p^{m-\gamma_r}}$. Then $\gamma_0^{p^s} = \gamma^{-p^{(\gamma_q+1)m}} = \gamma^{-1}$.

Consider the map $\Psi : \frac{\mathcal{R}[x]}{\langle x^{p^s}-1 \rangle} \longrightarrow \frac{\mathcal{R}[x]}{\langle x^{p^s}-\gamma \rangle}$ defined by $\Psi(f(x)) = f(\gamma_0 x)$. For polynomials $f(x)$ and $g(x) \in R[x]$, $f(x) \equiv g(x) \pmod{x^{p^s}-1}$ if and only if there exists a polynomial $h(x) \in R[x]$ such that $f(x) - g(x) = h(x)(x^{p^s}-1)$, if and only if $f(\gamma_0 x) - g(\gamma_0 x) = h(\gamma_0 x)[(\gamma_0 x)^{p^s} - 1] = \gamma^{-1} h(\gamma_0 x)[x^{p^s} - \gamma]$, if and only if $f(\gamma_0 x) \equiv g(\gamma_0 x) \pmod{x^{p^s} - \gamma}$. This means that for $f, g \in \frac{\mathcal{R}[x]}{\langle x^{p^s}-1 \rangle}$, $\Psi(f(x)) = \Psi(g(x))$ in $\frac{\mathcal{R}[x]}{\langle x^{p^s}-\gamma \rangle}$ if and only if $f(x) = g(x)$ in $\frac{\mathcal{R}[x]}{\langle x^{p^s}-1 \rangle}$. Therefore, Ψ is well defined and one-to-one. It is easy to verify that Ψ is onto and is a ring homomorphism. Thus, Ψ is a ring isomorphism. Therefore, we have the following proposition.

Proposition 6.1. *The map* $\Psi : \frac{\mathcal{R}[x]}{\langle x^{p^s}-1\rangle} \longrightarrow \frac{\mathcal{R}[x]}{\langle x^{p^s}-\gamma\rangle}$ *given by* $f(x) \mapsto f(\gamma_0 x)$ *is a ring isomorphism. In particular, for* $A \subseteq \frac{\mathcal{R}[x]}{\langle x^{p^s}-1\rangle}$, $B \subseteq \frac{\mathcal{R}[x]}{\langle x^{p^s}-\gamma\rangle}$ *with* $\Psi(A) = B$, *then* A *is an ideal of* $\frac{\mathcal{R}[x]}{\langle x^{p^s}-1\rangle}$ *if and only if* B *is an ideal of* $\frac{\mathcal{R}[x]}{\langle x^{p^s}-\gamma\rangle}$. *Equivalently,* A *is a cyclic code of length* p^s *over* $\mathcal{R}$ *if and only if* B *is a* γ*-constacyclic code of length* p^s *over* $\mathcal{R}$.

Now, using the isomorphism Ψ, the results about cyclic code of length p^s over $\mathcal{R}$ in Section 5 can be applied to corresponding γ-constacyclic codes of length p^s over $\mathcal{R}$. Indeed, results in Section 5 for cyclic codes hold true with γ-constacyclic codes by replacing x by $\gamma_0 x$ and writing $h(x)$ more explicitly.

Acknowledgments

The author is grateful to the referees for their very meticulous reading of this manuscript. Their suggestions were very helpful in creating the improved final version.

References

[1] T. Abualrub, R. Oehmke, On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e, IEEE Trans. Inform. Theory 49 (2003) 2126–2133.
[2] M.M. Al-Ashker, Simplex codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, Arab. J. Sci. Eng. Sect. A Sci. 30 (2005) 277–285.
[3] E. Bannai, M. Harada, T. Ibukiyama, A. Munemasa, M. Oura, Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and applications to Hermitian modular forms, Abh. Math. Sem. Univ. Hamburg 73 (2003) 13–42.
[4] S.D. Berman, Semisimple cyclic and Abelian codes. II, Kibernetika (Kiev) 3 (1967) 21–30 (in Russian); translated as Cybernetics 3 (1967) 17–23.
[5] T. Blackford, Negacyclic codes over $\mathbb{Z}_4$ of even length, IEEE Trans. Inform. Theory 49 (2003) 1417–1424.
[6] T. Blackford, Cyclic codes over $\mathbb{Z}_4$ of oddly even length, in: International Workshop on Coding and Cryptography, WCC 2001, Discrete Appl. Math. 128 (2003) 27–46.
[7] A. Bonnecaze, P. Udaya, Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory 45 (1999) 1250–1255.
[8] A.R. Calderbank, A.R. Hammons, P.V. Kumar, N.J.A. Sloane, P. Solé, A linear construction for certain Kerdock and Preparata codes, Bull. Amer. Math. Soc. 29 (1993) 218–222.
[9] G. Castagnoli, J.L. Massey, P.A. Schoeller, N. von Seemann, On repeated-root cyclic codes, IEEE Trans. Inform. Theory 37 (1991) 337–342.
[10] H.Q. Dinh, Negacyclic codes of length 2^s over Galois rings, IEEE Trans. Inform. Theory 51 (2005) 4252–4262.
[11] H.Q. Dinh, On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions, Finite Fields Appl. 14 (2008) 22–40.
[12] H.Q. Dinh, S.R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory 50 (2004) 1728–1744.
[13] G. Falkner, B. Kowol, W. Heise, E. Zehendner, On the existence of cyclic optimal codes, Atti Semin. Mat. Fis. Univ. Modena 28 (1979) 326–341.
[14] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Inform. Theory 40 (1994) 301–319.
[15] W.C. Huffman, On the decomposition of self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ with an automorphism of odd prime order, Finite Fields Appl. 13 (2007) 681–712.
[16] W.C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.
[17] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes 10th Impression, North-Holland, Amsterdam, 1998.
[18] J.L. Massey, D.J. Costello, J. Justesen, Polynomial weights and code constructions, IEEE Trans. Inform. Theory 19 (1973) 101–110.
[19] A.A. Nechaev, Kerdock code in a cyclic form, Diskr. Math. (USSR) 1 (1989) 123–139 (in Russian), English translation: Discrete Math. Appl. 1 (1991) 365–384.
[20] C.-S. Nedeloaia, Weight distributions of cyclic self-dual codes, IEEE Trans. Inform. Theory 49 (2003) 1582–1591.
[21] G. Norton, A. Sălăgean-Mandache, On the structure of linear cyclic codes over finite chain rings, Appl. Algebra Engrg. Comm. Comput. 10 (2000) 489–506.
[22] V. Pless, W.C. Huffman, Handbook of Coding Theory, Elsevier, Amsterdam, 1998.
[23] R.M. Roth, G. Seroussi, On cyclic MDS codes of length q over GF(q), IEEE Trans. Inform. Theory 32 (1986) 284–285.
[24] A. Sălăgean, Repeated-root cyclic and negacyclic codes over finite chain rings, Discrete Appl. Math. 154 (2006) 413–419.
[25] I. Siap, Linear codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and their complete weight enumerators, in: Codes and Designs, Columbus, OH, 2000, in: Ohio State Univ. Math. Res. Inst. Publ., vol. 10, de Gruyter, Berlin, 2002, pp. 259–271.
[26] L.-Z. Tang, C.B. Soh, E. Gunawan, A note on the q-ary image of a q^m-ary repeated-root cyclic code, IEEE Trans. Inform. Theory 43 (1997) 732–737.
[27] P. Udaya, A. Bonnecaze, Decoding of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory 45 (1999) 2148–2157.
[28] J.H. van Lint, Repeated-root cyclic codes, IEEE Trans. Inform. Theory 37 (1991) 343–345.
[29] K.-H. Zimmermann, On generalizations of repeated-root cyclic codes, IEEE Trans. Inform. Theory 42 (1996) 641–649.