axioms

MDPI

Article

Constacyclic Codes over Finite Chain Rings of Characteristic p

Sami Alabiad * and Yousef Alkhamees

Department of Mathematics, King Saud University, Riyadh 11451, Saudi Arabia; ykhamees@ksu.edu.sa
* Correspondence: ssaif1@ksu.edu.sa

Abstract: Let R be a finite commutative chain ring of characteristic p with invariants p, r, and k. In this paper, we study λ-constacyclic codes of an arbitrary length N over R, where λ is a unit of R. We first reduce this to investigate constacyclic codes of length p^s ($N = n_1 p^s$, $p \nmid n_1$) over a certain finite chain ring $CR(u^k, r_b)$ of characteristic p, which is an extension of R. Then we use discrete Fourier transform (DFT) to construct an isomorphism γ between $R[x]/ < x^N - \lambda >$ and a direct sum $\oplus_{b \in I} S(r_b)$ of certain local rings, where I is the complete set of representatives of p-cyclotomic cosets modulo n_1. By this isomorphism, all codes over R and their dual codes are obtained from the ideals of $S(r_b)$. In addition, we determine explicitly the inverse of γ so that the unique polynomial representations of λ-constacyclic codes may be calculated. Finally, for $k = 2$ the exact number of such codes is provided.

Keywords: finite ring; linear code; polynomials; coding theory

check for updates

Citation: Alabiad, S.; Alkhamees, Y. Constacyclic Codes over Finite Chain Rings of Characteristic p. *Axioms* **2021**, *10*, 303. https://doi.org/10.3390/axioms10040303

Academic Editor: Hari Mohan Srivastava

Received: 15 October 2021
Accepted: 10 November 2021
Published: 12 November 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The class of constacyclic codes plays an important role in coding theory and has been a primary area of study (see [1–9]). In the literature, most research has been focused on the situation where the alphabet of these codes is a field. However, many important non-linear codes over finite fields are actually related via the Gray map to linear codes over finite rings and, particularly, over finite chain rings. Constacyclic codes of arbitrary length N over a finite ring R are identified with ideals of the polynomials ring $R[x]/ < x^N - \lambda >$. Let p be the characterstic of the residue field of a finite commutative chain ring R. When the length N is prime relative to p, constacyclic codes are easily determined by the unique factorization of $X^N - \lambda$ using Hensel's Lemma. On the other hand, case $p \mid N$ yields what is called repeated-root codes, which were studied for the first time by Berman [10] in 1967 (for more details, see [2,7,11,12]).

The class of finite chain rings has been extensively used as the alphabet of constacyclic codes [8,13–24]. This class was introduced in [23] to construct new sequences posessing optimal Hamming correlation properties, and these sequences were found to be useful in frequency hopping multiple-access (FHMA) spreading spectrum communication systems. The chain ring $\mathbb{Z}_4$ has been widely considered as alphabet of cyclic codes (special types of constacyclic codes) [17–19,25]. Doughtry et al. [16] generalized the results to cyclic codes of length N over $\mathbb{Z}_{p^n}$. Moreover, Kiah et al. [8] studied cyclic codes of length p^s over $GR(p^2, r)$, while Zhu et al. [26] examined a special class of constacyclic codes over $\mathbb{Z}_{p^n}$. Now, let R be a finite commutative chain ring of characteristic p with invariants p, r, and k. Cyclic codes and their dual codes were initially considered over R with $p = 2$ and $k = 2$ by Bonnecaze et al. [20]. Qian et al. [21] used discrete Fourier transform (DFT) to study cyclic codes over R. Moreover, Dinh [27] studied consatcyclic codes of length p^s over R when $k = 2$. Ozger et al. [22] discussed constacyclic codes over R under the condition $p = 2, k = 4$. Recently, in [15], Mu Han et al. classified cyclic codes of length np^s over R in case of $r = 1$ via DFT. Motivated by the above cited studies, the main objective of this paper is to extend the approach of Han et al. [15] and to obtain unique polynomial representations of constacyclic codes of any finite length N over R with arbitrary invariants

p, r, and k. This paper is organized as follows. Section 2 gives some basic definitions of linear codes. In Section 3, we construct unique representations of constacyclic codes of length p^s over R. Section 4 is devoted to establishing unique polynomial representations of constayclic codes of length $N = n_1 p^s$ over R using DFT, where $p \nmid n_1$. This representation enables us to compute Hamming distance and dual codes of any such constacyclic code. We also obtain the exact number of constacyclic codes when $k = 2$.

2. Preliminaries

All rings considered in this paper are finite commutative and possess an identity. In this section, we mention some definitions and introduce notations that will be used in the subsequent discussions.

2.1. Constacyclic Codes

A code of length N over a ring R is a nonempty subset of R^N, and R is referred to be the alphabet of the code. A code C is said to be linear if it is also a R-submodule of R^N. For a given unit λ of R, a linear code C is said to be constacyclic or more precisely λ-constacyclic if $(\lambda x_{N-1}, x_0, x_1, \ldots, x_{N-2}) \in C$, whenever $(x_0, x_1, \ldots, x_{N-2}, x_{N-1}) \in C$, i.e., C is closed under λ-constacyclic shifts. The cyclic and negacyclic codes are obtained when $\lambda = 1$ and -1, respectively.

Proposition 1 ([28,29]). *A linear code C of length N is a λ-constacyclic code over R if and only if C is an ideal of $R[x]/ < x^N - \lambda >$.*

2.2. Finite Chain Rings of Characteristic p

A ring R is a chain ring if it is local and its Jacobson radical $J(R)$ is principal. Every finite chain ring R is associated with five invariants p, n, r, k, and m. From now on, R is a finite chain ring of characteristic p, i.e., $n = 1$ and $m = k$. In this case, R is associated with p, r, and k. We denote $J(R) =< u >$, k the index of nilpotency of u, and p^r is the order of the residue field $R/J(R)$. Such chain rings are uniquely determined by their invariants p, r, and k [30].

Proposition 2 ([31,32]). *Let R be a finite chain ring of characteristic p with invariants p, r, k. Then, the following is the case:*
(i) R has a subfield F of order p^r;
(ii) $R = F \oplus uF \oplus \ldots \oplus u^{k-1}F$;
(iii) $R \cong F[u]/ < u^k >$;
(iv) If $U(R)$ is the group of units of R, then $U(R) \cong F^* \times (1 \oplus uF \oplus u^2F \oplus \ldots \oplus u^{k-1}F)$.

By Proposition 2, every unit λ of R can be uniquely written as $\lambda = \alpha + u\beta_1 + u^2\beta_2 + \ldots + u^{k-1}\beta_{k-1}$, where $\alpha \in F^*$ and $\beta_i \in F$ for $1 \leq i \leq k-1$. If l is the smallest positive integer such that $\beta_l \neq 0$, then the following is the case:

$$\lambda = \alpha + u^l\left(\beta_l + \ldots + u^{k-l-1}\beta_{k-l-l}\right) = \alpha + u^l\beta, \tag{1}$$

where $\beta = \beta_l + \ldots + u^{k-l-1}\beta_{k-l-l}$. Thus, every unit λ of R is of the form $\lambda = \alpha + u^l\beta$, where β is either 0 or a unit of R. Let the following be the case:

$$\alpha_0 = \alpha^{-p^{(q+1)r-s}}, \tag{2}$$

where $s = rq + t$ and $0 \leq t \leq r-1$. Then, $\alpha_0^{p^s} = \alpha^{-p^{(q+1)r}} = \alpha^{-1}$.

Remark 1. *If F is a finite field. The ring $F[x]/ < x^{p^s} - \alpha >$ is a chain ring with maximal ideal $< \alpha_0 x - 1 >$. Thus, α-constacyclic codes of length p^s over F are precisely the ideals $< (\alpha_0 x - 1)^i >$, where $0 \leq i \leq p^s$. Each α-constacyclic code $< (\alpha_0 x - 1)^i >$ has $p^{r(p^s - i)}$ codewords.*

Definition 1. *For any λ-constacyclic code C of length p^s over R and for $0 \leq i \leq k-1$, we define the following codes over F:*

$$Tor_i(C) = \mu\Big(\Big\{a \mid u^i a \in C\Big\}\Big), \tag{3}$$

where μ is the canonical homomorphism (modulo u). Moreover, $Tor_i(C)$ is called the ith torsion code of C, $\mu(C) = Tor_0(C) = Res(C)$ is the residue code of C, and $T_i(C) = T_i$ is called the ith-torsional degree of C.

Proposition 3 ([16])**.** *Let C be a λ-constacyclic code over R and i be an integer such that $0 \leq i \leq k-1$. Then, $T_i(C)$ is α-constacyclic codes of length p^s over F and $Tor_i(C) =< (\alpha_0 x - 1)^{T_i} >$ for some $0 \leq T_i \leq p^s$. Moreover, we have the following:*
(i) $|Tor_i(C)| = (p^r)^{p^s - T_i}$;
(ii) If $u^i\big((\lambda_0 x - 1)^{t_i} + ug(x)\big)$ in C, then $t_i \geq T_i$;
(iii) $p^s \geq T_0 \geq T_1 \geq \ldots \geq T_{k-1} \geq 0$;
(iv) $|C| = (p^r)^{kp^s - (T_0 + T_1 + \ldots + T_{k-1})}$.

Remark 2. *Obviously, T_i is the smallest degree amongst all the degrees of non-zero polynomials in $Tor_i(C)$.*

All symbols stated above shall retain their meanings throughout the article, in addition, $N = n_1 p^s$, $(n_1, p) = 1$.

3. Constacyclic Codes of Length p^s

In this section, we provide a unique representation for any constacyclic code of length p^s over R. This representation allows us to compute Hamming distances and dual codes as well as enumerates all constacyclic codes of length p^s over R, i.e., ideals of the quotient ring $R_{\alpha,\beta} = R[x]/ < x^{p^s} - (\alpha + u^l\beta) >$. Assume $k_1 = \lceil \frac{k}{l} \rceil$, i.e., k_1 is the smallest positive integer greater than $\frac{k}{l}$.

Lemma 1. *In $R_{\alpha,\beta}$, $< (\alpha_0 x - 1)^{p^s} >=< u^l >$. In particular, $(\alpha_0 x - 1)$ is nilpotent with nilpotency index $k_1 p^s$.*

Proof. Note that the following is the case.

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

Thus, $< (\alpha_0 x - 1)^{p^s} >=< u^l >$. The last statement follows immediately, since u^l has nilpotency index k_1. □

Proposition 4. *The ring $R_{\alpha,\beta}$ is a local ring with maximal ideal $< (\alpha_0 x - 1), u >$.*

Proof. Due to the fact that $R = F \oplus uF \oplus \ldots \oplus u^{k-1}F$, each element a of R has unique presentation as $a = \sum_{i=0}^{k-1} u^i a_i$, where $a_0, a_1, \ldots, a_{k-1}$ are elements of F. This implies that for any polynomial $f(x) \in R_{\alpha,\beta}$, $f(x)$ can be expressed uniquely as follows:

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

where a_{ij}s are elements of F. Due to the fact that $\alpha_0 x - 1$ and u are nilpotent, $f(x)$ is a unit if and only if $a_{00} \neq 0$. Moreover, if $f(x)$ is a zero divisor, i.e., $a_{00} = 0$, then

$f(x) \in < (\alpha_0 x - 1), u >$ by Lemma 1. Thus, the ideal $< (\alpha_0 x - 1), u >$ consists of all zero divisors of $R_{\alpha,\beta}$. Therefore, $R_{\alpha,\beta}$ is a local ring with maximal ideal $< (\alpha_0 x - 1), u >$. □

Remark 3. *If $k = 1$, $R_{\alpha,\beta} = R_\alpha$ is a chain ring with maximal ideal $< \alpha_0 x - 1 >$.*

Theorem 1. *If C is a $(\alpha + u^l\beta)$-constacyclic code of length p^s over R, then the following is the case:*

$$C =< g_0(x), g_1(x), \ldots, g_{k-1}(x) >, \tag{4}$$

where $g_i(x) = u^i(\alpha_0 x - 1)^{T_i} + u^{i+1}h_i(x)$, if $T_i < p^s$, where $h_i(x) \in R_{\alpha,\beta}$ such that deg $h_i < T_{i+1}$ or $g_i(x) = 0$ otherwise. Moreover, the k-tuple $(g_0(x), g_1(x), \ldots, g_{k-1}(x))$ is unique.

Proof. The proof will be carried out by induction. Let $R_i = F + uF + \ldots + u^iF$ and $R'_i = R_i[x]/ < x^{p^s} - (\alpha + u^l\beta) >$, where $0 \le i \le k-1$. First note that if $k = 1$, $R = F$, and the case is trivial. Now if $k = 2$, let μ_1 be the canonical homomorphism from R'_1 to R'_0. It is clear that *Ker* $\mu_1 =< u >$. Let C be a constacyclic code of length p^s over R_1 and μ_C be the restriction of μ_1 on C. Then,

$$Ker\ \mu_C = C \cap < u >=< u(\alpha_0 x - 1)^{T_1} >,$$

where $T_1 = T_1(C)$. Moreover, $Im\ \mu_C \cong C/Ker\ \mu_C$ is a constacyclic code of length p^s over R_0; thus,

$$Im\ \mu_C =< (\alpha_0 x - 1)^{T_0} >,$$

where $T_0 = T_0(C)$ and $0 \le T_0 \le p^s$. This implies that $(\alpha_0 x - 1)^{T_0} + ua(x) \in C$ for some $a(x)$ in R'_1, and $a(x)$ can be expressed as $a(x) = (\alpha_0 x - 1)^t h(x)$, where $h(x)$ is either zero or a unit. We can consider *deg* $a \le T_1$, and, therefore, $t +$ *deg* $h \le T_1$. Thus, C is generated by

$$g_0(x) = (\alpha_0 x - 1)^{T_0} + (\alpha_0 x - 1)^t h(x) \text{ and } g_1(x) = u(\alpha_0 x - 1)^{T_1}.$$

In cases when $T_0 = p^s$, then $C = ker\ \mu_C$; thus, $g_0(x) = 0$. Let us assume that the hypothesis is true for $k-2$ and we prove it for $k-1$. Let μ_{k-1} be the natural homomorphism (modulo u^{k-1}) from R'_{k-1} to R'_{k-2}. It is obvious that *Ker* $\mu_{k-1} =< u^{k-1} >$. Assume C is a constacyclic code of length p^s over R_{k-1}, and μ_C is the restriction of μ_{k-1} on C. Then,

$$Ker\ \mu_C =< u^{k-1} > \cap C =< u^{k-1}(\alpha_0 x - 1)^{T_{k-1}} > .$$

Now, since $Im\ \mu_C \cong C/Ker\ \mu_C$ is a constacyclic code of length p^s over R_{k-2}, and by the induction step,

$$Im\ \mu_C =< g'_0(x), g'_1(x), \ldots, g'_{k-2}(x) >,$$

where $g'_0(x), g'_1(x), \ldots, g'_{k-2}(x)$ satisfy the conditions of the theorem. This implies that there exist $a_i(x) \in R'_{k-1}$ such that $g_i(x) = g'_i(x) + u^{k-1}a_i(x) \in C$. Moreover, we have $T_i = T_i(\mu_I)$ for $i = 0, 1, 2, \ldots, k-2$. If we write $a_i(x) = (\alpha_0 x - 1)^{t_{k-i-1,i}} h_{k-i-1,i}(x)$ with *deg* $a_i \le T_{k-1}$, then $t_{k-i-1,i} +$ *deg* $h_{k-i-1,i} \le T_{k-1}$. Therefore, we can take $g_0(x), g_1(x), \ldots, g_{k-1}(x)$ as generators of C, where $g_{k-1}(x) = u^{k-1}(\alpha_0 x - 1)^{T_{k-1}}$. Now suppose

$$C =< e_0(x), e_1(x), \ldots, e_{k-1}(x) >,$$

where $e_0(x), e_1(x), \ldots, e_{k-1}(x)$ is another expression of C satisfying the conditions of the theorem. Then, the uniqueness follows from the induction step and the fact that $g_i(x) = e_i(x)$ *mod ker* μ_C for $i = 0, 1, 2, \ldots, k-2$. □

Corollary 1. *Suppose that $T_i < p^s$. Then, the smallest degree amongst the polynomials in C with leading coefficient u^i is T_i.*

Definition 2. *Let C be a constacyclic code over R. We call the unique k-tuple of polynomials described in Theorem 1 to be the representation of C.*

Next, we construct a one-to-one correspondence between cyclic and α-constacyclic codes, where α is a nonzero element of F. Consider the map $\Psi : R[x]/ < x^{p^s} - 1 > \longrightarrow R[x]/ < x^{p^s} - \alpha >$ defined by $\Psi(f(x)) = f(\alpha_0 x)$, where α_0 as in Equation (2). 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 $f(\alpha_0 x) - g(\alpha_0 x) = h(\alpha_0 x)[(\alpha_0 x)^{p^s} - 1] = \alpha^{-1} h(\alpha_0 x)[x^{p^s} - \alpha]$, if and only if $f(\alpha_0 x) \equiv g(\alpha_0 x) \pmod{x^{p^s} - \alpha}$. This means that Ψ is well defined and has one-to-one correspondence. It is easy to show that Ψ is a ring homomorphism. Thus, Ψ is a ring isomorphism.

Proposition 5. *The map $\Psi : R[x]/ < x^{p^s} - 1 > \longrightarrow R[x]/ < x^{p^s} - \alpha >$ defined by $\Psi(f(x)) = f(\alpha_0 x)$ is a ring isomorphism. In particular, C is a cyclic code of length p^s over R if and only if $\psi(C)$ is a α-constacyclic code of length p^s over R. Moreover, ψ is Hamming weight preserving.*

Hamming Distance and Dual Codes

Definition 3. *For a nonzero linear code C, the Hamming distances of C and $d(C)$ are defined by the following:*

$$d(C) = min\{wt(c) \mid c \neq 0, c \in C\}, \tag{5}$$

where $wt(c)$ is the number of nonzero components of $c = (c_0, c_1, \ldots, c_{N-1})$ in R^N. The zero code is conventionally said to have Hamming distance 0.

Theorem 2. *Let C be a constacyclic code of length p^s over R. Then,*

$$d(C) = d(Tor_{k-1}(C)).$$

Proof. For any nonzero codeword $c(x)$ of C, we have $wt(u^{k-1}c(x)) \leq wt(c(x))$. Then, it suffices to compute Hamming distance of $u^{k-1}c(x)$, where $c(x) \in C$. As $u^{k-1}c(x)$ and $\overline{c}(x)$ have the same number of nonzero coefficients, then $wt(u^{k-1}c(x)) = wt(\overline{c}(x))$. Thus, $d(C) = d(Tor_{k-1}(C))$. As $Tor_{k-1}(C)$ is a constacyclic code over F, its Hamming distance is completely determined (see [33], Theorem 4.11). □

Next, we consider the dual codes. Given N-tuples $x = (x_0, x_1, \ldots, x_{N-1})$ and $y = (y_0, y_1, \ldots, y_{N-1})$ in R^N, the inner product or dot products is defined as usual, with $x \cdot y = x_0 y_0 + x_1 y_1 + \ldots + x_{N-1} y_{N-1}$, which is evaluated in R. Two N-tuples x and y are called orthogonal if $x \cdot y = 0$.

Definition 4. *For a linear code C over R, its dual code $C^{\perp}$ is the set of N-tuples over R that is orthogonal to all codewords of C, i.e., $C^{\perp} = \{x \mid x \cdot y = 0, \forall y \in C\}$.*

The following propositions are well known [28,29,34,35].

Proposition 6. *Let λ be a unit of R. Then, the dual of a λ-constacyclic code over R is a λ^{-1}-constacyclic code over R.*

Proposition 7. *Let p be a prime and R be a finite chain ring of order p^z. The number of codewords in any linear code C of length N over R is p^e for some integer $e \in \{0, 1, \ldots, zN\}$. Moreover, the dual code $C^{\perp}$ has $p^{e'}$ codewords, where $e + e' = zN$, i.e., $|C| \cdot |C^{\perp}| = |R|^N$.*

Note that in $R_{\alpha,\beta}$, $(\alpha + u^l \beta)^{p^{k_1}} = \alpha^{p^{k_1}}$; thus, the following is the case.

$$(\alpha + u^l \beta)^{p^{k_1}} \alpha^{-p^{k_1}} = 1.$$

Therefore, the following is the case:

$$(\alpha + u^l\beta)^{-1} = (\alpha + u^l\beta)^{p^{k_1}-1}\alpha^{-p^{k_1}} \tag{6}$$

$$= [\alpha^{p^{k_1}-1} + \sum_{i=1}^{p^{k_1}-1} \binom{p^{k_1}-1}{i} \alpha^{p^{k_1}-1-i}(u^l\beta)^i]\alpha^{-p^{k_1}} \tag{7}$$

$$= \alpha^{-1} + (u^l\beta) \sum_{i=1}^{p^{k_1}-1} \binom{p^{k_1}-1}{i} \alpha^{-(1+i)}(u^l\beta)^{i-1} \tag{8}$$

$$= \alpha^{-1} + (u^l\beta)\alpha^{-1} \sum_{i=1}^{p^{k_1}-1} \binom{p^{k_1}-1}{i} \alpha^{-i}(u^l\beta)^{i-1} \tag{9}$$

$$= \alpha^{-1} + u^l\beta\alpha^{-1}\zeta, \tag{10}$$

where $\zeta = \sum_{i=1}^{p^{k_1}-1} \binom{p^{k_1}-1}{i} \alpha^{-i}(u^l\beta)^{i-1}$, which is a unit in $R_{\alpha,\beta}$.

Theorem 3. *Let C be a $(\alpha + u^l\beta)$-constacyclic code of length p^s over R as in Theorem 1. Then, $C^\perp$ is a $(\alpha^{-1} + u^l\beta\alpha^{-1}\zeta)$-constacyclic code of length p^s over R, and the following is the case:*

$$C^\perp = < f_0(x), f_1(x), \ldots, f_{k-1}(x) >, \tag{11}$$

where $f_i(x) = u^i(\alpha_0^{-1}x - 1)^{\overline{T}_i} + u^{i+1}a_i(x)$ for some $a_i(x) \in R_{\alpha^{-1},\beta\alpha^{-1}\zeta}$. Moreover, $\overline{T}_i = p^s - T_{k-1-i}$ for $0 \le i \le k-1$.

Proof. By Proposition 6, $C^\perp$ is a $(\alpha^{-1} + u^l\beta\alpha^{-1}\zeta)$-constacyclic code of length p^s over R; thus, by Theorem 1,

$$C^\perp = < f_0(x), f_1(x), \ldots, f_{k-1}(x) >,$$

where $f_i(x) = u^i(\alpha_0^{-1}x - 1)^{\overline{T}_i} + u^{i+1}h_i(x)$ for some $h_i(x) \in R'$ and $\overline{T}_i = T_i(C^\perp)$. By the definition of $C^\perp$, it is easy to deduce that $u^{k-1-i}(\alpha_0^{-1}x - 1)^{p^s - T_i} \in C^\perp$ and then $\overline{T}_{k-1-i} \le p^s - T_i$ for $0 \le i \le k-1$. As $|C| = (p^r)^{kp^s - (T_0+T_1+\ldots+T_{k-1})}$ and $|C| \cdot |C^\perp| = (p^r)^{kp^s}$ (Proposition 7), then $|C^\perp| = (p^r)^{T_0+T_1+\ldots+T_{k-1}}$. Thus, we must have $T_{k-1-i} + \overline{T}_i = p^s$ and so $\overline{T}_i = p^s - T_{k-1-i}$. □

Example 1. *Table 1 shows the representation of all proper cyclic codes of length 3 over the chain ring $R = \mathbb{Z}_3 + u\mathbb{Z}_3$ of characteristic 3.*

Table 1. Proper cyclic codes of length 3 over R.

$C \subseteq < u >$	$C \nsubseteq < u >$
$< 0 >$	$< (x-1), u(x-1) >$
$< u >$	$< (x-1), u >$
$< u(x-1) >$	$< (x-1)^2 >$
$< u(x-1)^2 >$	$< (x-1)^2, u >$
	$< (x-1)^2, u(x-1) >$
	$< (x-1) + u >$
	$< (x-1) + 2u >$
	$< (x-1)^2 + u >$
	$< (x-1)^2 + 2u >$
	$< (x-1)^2 + u >$
	$< (x-1)^2 + 2u >$

Example 2. *Table 2 shows the representation of all proper* $(1+u^2)$*-constacyclic codes of length* 2 *over the chain ring* $R = \mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$ *of characteristic* 2*. We have the following case.*

$$l = 2, \alpha = \alpha_0 = \beta = 1, u^2 = (x-1)^2 \text{ and } s = 1.$$

Table 2. Proper $(1+u^2)$-consacyclic codes of length 2 over R.

$C \subseteq < u >$	$C \nsubseteq < u >$
$< 0 >$	$< (x-1) >$
$< u >$	$< (x-1), u >$
$< u^2 >$	$< (x-1)+u, u^2 >$
$< u(x-1) >$	$< (x-1)+u >$
$< u(x-1)+u^2 >$	$< (x-1)+u, u(x-1) >$
$< u^2(x-1) >$	$< (x-1)+u+u^2 >$
$< u(x-1), u^2 >$	$< (x-1)+u(x-1)+u >$

Example 3. *Consider the constacyclic codes in Example 2. As* $(1+u^2)^{-1} = 1+u^2$ *by Equation (10),* $C^{\perp} = C$ *for any* $(1+u^2)$*-constacyclic code* C*. This means all* $(1+u^2)$*-constacyclic codes in Example 2 are self dual codes.*

4. Constacyclic Codes of Length N

4.1. Exension Rings

Let r' be a positive integer and let $CR(u^k, r') = R[x]/ < f(x) >$, where $f(x)$ is a monic basic irreducible of degree r' over R. Note that $f(x)$ can be chosen so that $CR(u^k, r')$ contains $(p^{r'}-1)$th root of unity. Moreover, $CR(u^k, r')$ is a chain ring of characteristic p with maximal ideal $< u >$ and residue field $K = F_{p^{rr'}}$. By Theorem 2,

$$CR(u^k, r') = K \oplus uK \oplus \ldots \oplus u^{k-1}K. \tag{12}$$

Let a be the order of p modulo n_1, then F_{p^a} contains a primitive n_1th root ξ of unity. Assume that K is the splitting field of $x^{n_1} - \alpha$ over F_{p^a}, where α is a nonzero element of F and $r' = aa'$ for some positive integer a' the degree of the extension. If θ is a root of $x^n - \alpha$ in F_{p^r}, then $\theta\xi^i$, for $0 \le i \le n_1 - 1$ are all distinct roots of $x^{n_1} - \alpha$ in F_{p^r}; hence, by Hensel's Lemma ([29], Theorem XIII.4), $CR(u^k, r)$ also contains all those roots. Now $x^{n_1} - \alpha$ factors uniquely into monic irreducible polynomials over F, and then again by Hensel's Lemma, $x^{n_1} - \alpha$ factors into monic basic irreducible polynomials over R as follows.

$$x^{n_1} - \alpha = f_1(x) f_2(x) \ldots f_m(x). \tag{13}$$

For each $0 \le j \le n_1 - 1$, there exists a unique i, $1 \le i \le m$ such that $f_i(\theta\xi^j) = 0$, and $f_i(x)$ is called the minimal polynomial of $\theta\xi^j$ over R.

Next, we introduce another extension:

$$S(r') = CR(u^k, r')[x]/ < x^{p^s} - (\alpha + u^l\beta) > \tag{14}$$

of $CR(u^k, r')$. Note that, for a suitable positive number r', S will be the alphabet of codes of length p^s over R that contains nth root of unity. The results of Lemma 1 and Proposition 4 hold for the ring S. Moreover, we define the following extension of R.

$$R_N = R[x]/ < x^N - (\alpha + u^l\beta) > . \tag{15}$$

Let r' be the order of p modulo n_1. Let $\sim$ be a relation on the set $\{1, 2, \ldots, n_1\}$ defined as $i \sim j$ if and only if $\theta\xi^i$ and $\theta\xi^j$ are roots of the same minimal polynomial, i.e., there is a unique b such that $f_b(\theta\xi^i) = f_b(\theta\xi^j) = 0$. It is easy to show this relation is equivalence.

Now, let I be the set of all classes of $\sim$, I_b be a class containing b, and r_b is the size of this class, i.e., $\mid I_b \mid = deg\ f_b(x) = r_b$.

4.2. Discrete Fourier Transform (DFT)

DFT has been used to study repeated-root codes over finite chain rings in [3,5,6]. We employ DFT as a tool to establish the structure of $(\alpha + u^l\beta)$-constacyclic codes over R for a given length N.

Remark 4. *In $S(r_b)$, we have $(\alpha + u^l\beta)^{p^{d-1}} = \alpha$, where $d = \lceil \frac{k}{l} \rceil$; hence, $x^{p^{s+d-1}} = \alpha$ and then $(\alpha_0 x)^{p^{s+d-1}} = 1$.*

Definition 5 (DFT)**.** *Let $\boldsymbol{c}$ be a vector in R^N with $c(x) = \Sigma_{i=0}^{n_1-1}\Sigma_{j=0}^{p^s-1} c_{i,j}x^{i+jn_1}$ the corresponding polynomial. The DFT of $c(x)$ is the following vector:*

$$(\hat{c}_0, \hat{c}_1, \ldots, \hat{c}_{n_1-1}) \in S(r')^{n_1}, \tag{16}$$

where $\hat{c}_b = c((\alpha_0 w)^{n'}\theta\xi^b) = \Sigma_{i=0}^{n_1-1}\Sigma_{j=0}^{p^s-1} c_{i,j}w^{n'i+j}(\alpha_0^{n'}\theta\xi^b)^i, b \in I$ and $n_1 n' \equiv 1\ (mod\ \ p^{s+d-1})$. Define the Mattson–Solomon polynomial of $\boldsymbol{c}$ to be the following.

$$\hat{c}(z) = \Sigma_{b=0}^{n_1-1}\hat{c}_{n_1-b}z^b. \tag{17}$$

Note that $\hat{c}_{n_1} = \hat{c}_0$.

The following lemma shows that if the Mattson–Solomon polynomial of **c** is given, then **c** can be recovered. Set $S = R_{\alpha,\beta} = R[w]/ < w^{p^s} - (\alpha + u^l\beta) >$. Let ϕ be the natural R-module isomorphism $\phi : S^{n_1} \longrightarrow R^N$ defined by the following case.

$$\phi(\sum_{i=0}^{p^s-1} c_{0,i}w^i, \ldots, \sum_{i=0}^{p^s-1} c_{n-1,i}w^i) = (c_{0,0}, c_{1,0}, \ldots, c_{n-1,0}, c_{0,1}, \ldots, c_{0,p^s-1}, c_{1,p^s-1} \ldots, c_{n-1,p^s-1}).$$

Lemma 2. *Let $\boldsymbol{c} \in R^N$ with $\hat{c}(z)$ its Mattson–Solomon polynomial. Then, the following is the case:*

$$\boldsymbol{c} = \phi[(1, u^{-n'}, u^{-2n'}, \ldots, u^{-(n_1-1)n'}) * \frac{1}{n_1}(\hat{c}(1), \hat{c}(\alpha^1), \ldots, \hat{c}(\alpha^{n_1-1}))], \tag{18}$$

where $*$ denotes component-wise multiplication.

Proof. Let $0 \leqslant t' \leqslant n_1 - 1$. Then, the following is the case.

$$\begin{aligned}
\hat{c}(\xi^t) = \sum_{b=0}^{n-1} \hat{c}_b\xi^{-bt} &= \sum_{b=0}^{n_1-1}(\sum_{i=0}^{n-1}\sum_{j=0}^{p^s-1} c_{i,j}w^{n'i+j}(\alpha_0^{n'}\theta\xi^b)^i)\xi^{-bt} \\
&= \sum_{i=0}^{n_1-1}\sum_{j=0}^{p^s-1} c_{i,j}w^{n'i+j}(\alpha_0^{n'}\theta)^i \sum_{b=0}^{n_1-1}\xi^{b(i-t)} \\
&= n_1((\alpha_0 w)^{n'}\theta)^t \sum_{j=0}^{p^s-1} c_{t,j}w^j.
\end{aligned}$$

Note that $\Sigma_{i=0}^{n_1-1}\xi^{ij} = 0$, when $j \neq 0\ \ (\text{mod}\ \ n_1)$. Then, by the definition of ϕ, we have

$$\mathbf{c} = \phi[(1, w^{-n'}, w^{-2n'}, \ldots, w^{-(n_1-1)n'}) * \frac{1}{n_1}(\hat{c}(1), \hat{c}(\alpha^1), \ldots, \hat{c}(\alpha^{n_1-1}))].$$

□

Remark 5. *Since $\theta\xi^b \in S(r_b)$, it is easy to verify that $\hat{c}_b \in S(r_b)$. Now let the following be the case.*

$$A = \{(\hat{c}_0, \hat{c}_2, \ldots, \hat{c}_{n_1-1}) \in S(r)^{n_1} | \hat{c}_i \in S(r_b), i \in I_b\}. \tag{19}$$

Note that A with component-wise addition and multiplication is a ring. Moreover, it is clear that $A \cong \oplus_{b\in I} S(r_b)$.

Theorem 4. *Let γ be the map $\gamma : R_N \longrightarrow \oplus_{b\in I} S(r_b)$, given by $\gamma(c(x)) = (\hat{c}_b)_{b\in I}$. Then, γ is a ring isomorphism. In particular, if C is a constacyclic code of length N over R, then the following is the case:*

$$C \cong \oplus_{b\in I} C_b, \tag{20}$$

where C_b is the constacyclic code $\{c((\alpha_0 w)^{n'}\theta\xi^b) \mid c(x) \in C\}$ of length p^s over $CR(u^k, r_b)$.

Proof. Define the map $\gamma : R_N \longrightarrow A$, where $\gamma(c(x)) = (\hat{c}_0, \hat{c}_2, \ldots, \hat{c}_{n_1-1})$. Let $a(x), b(x)$ be polynomials over R of degree less than N. Then, clearly $\gamma(a(x) + b(x)) = \gamma(a(x)) + \gamma(b(x))$ and also $\gamma(a(x)b(x)) = \gamma(a(x)) * \gamma(b(x))$, where $*$ denotes the componentwise product. Suppose $\gamma(c(x)) = \mathbf{0}$, then by Lemma 2, $\Sigma_{j=0}^{p^s-1} c_{t',j} u^j = 0$ for any t', where $0 \leqslant t' \leqslant n_1 - 1$. It follows that $c(x) = 0$, and this implies γ is an injection. Moreover, $|A| = \prod_{b\in I} p^{rr_b n_1 p^s} = p^{n_1 rN}$, which means that γ is a bijection. Therefore, γ is an isomorphism. The second statement follows directly because γ is a ring isomorphism. □

Before we obtain the structure of all constacyclic codes of length $n_1 p^s$ over R in terms of their generator polynomials, we provide the following lemma.

Lemma 3. *Let $f_b(x)$ be the minimal polynomial of $\theta\xi^b$ over R for each $b \in I$ and n' a positive integer such that $n_1 n' \equiv 1 \ (mod \ \ p^{s+d-1})$. Then, the following is the case:*
(i) $f_b((\alpha_0 w)^{n'}\theta\xi^i)$ is a unit if i is not in I_b;
(ii) $f_b((\alpha_0 w)^{n'}\theta\xi^b) \in < \alpha_0 w - 1 >$ but $f_b((\alpha_0 w)^{n'}\theta\xi^b)$ is not in $< (\alpha_0 w - 1)^2 >$.

Proof.
(i) Since $f_b(x) = \prod_{t\in I_b} (x - \theta\xi^t)$. Then, the following is the case.

$$\begin{aligned} f_b((\alpha_0 w)^{n'}\theta\xi^i) &= \prod_{t\in I_b} ((\alpha_0 w)^{n'}\theta\xi^i - \theta\xi^t) \\ &= \prod_{t\in I_b} [((\alpha_0 w)^{n'} - 1)\theta\xi^i + (\theta\xi^i - \theta\xi^t)]. \end{aligned}$$

Since i is not in I_b, then $\theta\xi^i - \theta\xi^e \neq 0$. Therefore, $f_b((\alpha_0 w)^{n'}\theta\xi^i)$ is a unit if i is not in I_b.
(ii) We know that $x_1^n - \alpha = \prod_{i\in I} f_i(x)$ and then $\prod_{i\in I} f_i((\alpha_0 w)^{n'}\theta\xi^b) = ((\alpha_0 w)^{n'}\theta\xi^b)^{n_1} - 1 = \alpha_0 w - 1$. However, from (i) we have $f_i((\alpha_0 w)^{n'}\theta\xi^b)$, which is a unit for $i \neq b$. Hence, $f_b((\alpha_0 w)^{n'}\theta\xi^b) = a(w)(\alpha_0 w - 1)$, where $a(w)$ is a unit in $S(r_b)$. It follows that $f_b((\alpha_0 w)^{n'}\theta\xi^b) \in (\alpha_0 w - 1)$. Now, suppose that $f_b((\alpha_0 w)^{n'}\theta\xi^b) \in < (\alpha_0 w - 1)^2 >$, which implies that $< \alpha_0 w - 1 > \subseteq < (\alpha_0 w - 1)^2 >$. However, this is a contradiction, and this completes the proof. □

Next, we introduce the polynomial representations of constacyclic codes over R. If C is a constacyclic code of length N over R. By Theorem 4, $C \cong \oplus_{b\in I} C_b$, where C_b is a constacyclic code of length p^s over $CR(u^k, r_b)$, and by Theorem 1:

$$C_b = < e_{0,b}(w), ue_{1,b}(w), \ldots, u^{k-1}e_{k-1,b}(w) >,$$

where $e_{i,b}(w) = (\alpha_0 w - 1)^{T_{i,b}} + uh_{i,b}(w)$. Now, fix i and for each $0 \leqslant j \leqslant p^s$. We define $F_j(x)$ to be the product of all minimal polynomials of α^b such that $Tor_i(C_b) = < (\alpha_0 w - 1)^j >$. By Lemma 3, the following is the case:

$$\prod_{j=0}^{p^s}[F_j((\alpha_0 w)^{n'}\theta\xi^b)]^j = a_b(w)(\alpha_0 w-1)^j, \tag{21}$$

where $a_b(\alpha_0 w)$ is a unit in $S(r_b)$. Define the following:

$$g_i(x) = \prod_{j=0}^{p^s}[F_j(x)]^j + pb_i(x), \tag{22}$$

where $b_i(x) = \gamma^{-1}((a_b(\alpha_0 w)h_{i,b}(\alpha_0 w))_{b\in I})$.

Theorem 5. *Let C be a constacyclic code of length N over R . Then, the following is the case.*

$$C =< g_0(x), ug_1(x), \ldots, u^{k-1}g_{k-1}(x) > . \tag{23}$$

Moreover, this representation is unique.

Proof. For every $b \in I$, $g_i((\alpha_0 w)^{n'}\alpha^b) \in < e_{i,b}(\alpha_0 w) >$ and then $p^i g_i((\alpha_0 w)^{n'}\theta\xi^b) \in C_b$. It follows that $u^i g_i(x) \in C$ for each i, $0 \le i \le k-1$. Furthermore, by Equations (21) and (22), $< g_i((\alpha_0 w)^{n'}\theta\xi^b) >=< e_{i,b}(\alpha_0 w) >$ for all b. Therefore, $g_0(x), ug_1(x), \ldots, u^{k-1}g_{k-1}(x)$ generate C (Theorem 4). The uniqueness of $g_i(x)$ follows from the uniqueness of $h_{i,b}(\alpha_0 w)$. □

Corollary 2. *If $C =< g_0(x), ug_1(x), \ldots, u^{k-1}g_{k-1}(x) >$ is a constacyclic code of length N over R, then $|C| = p^{rt'}$, where $t' = kN - \Sigma_{j=0}^{p^s} j deg\ F_j$.*

Proof. By Theorem 4, $|C| = \prod_{b\in I}|C_b|$ and $|C_b| = p^{rr_b(n_1 p^s - (T_{0,b}+T_{1,b}+\ldots+T_{k-1,b}))}$, and then by computing the product, we obtain the result. □

Remark 6. *If we choose $g_e(x)$ to have a minimal degree in the representation given by (23), we will obtain a minimal strong Gröbner basis $< g_0(x), \ldots, u^e g_e(x) >$ for C. For more details about minimal strong Gröbner basis, refer to [7].*

Next, we provide the enumeration of constacyclic codes of length N in terms of the length of p^s. In other words, the problem of enumeration of constacyclic codes of length N over R is reduced to that of constacyclic codes of length of power of p. The proof of the following result is direct by Theorem 5.

Corollary 3. *The number of distinct $(\alpha + u^l\beta)$-constacyclic codes of length N over R is the following:*

$$\prod_{b\in I} N_b, \tag{24}$$

where N_b is the number of $(\alpha + u^l\beta)$-constacyclic codes of length p^s over $CR(u^k, r_b)$.

Theorem 6. *If $k = 2$, then the number of distinct $(\alpha + u^l\beta)$-constacyclic codes of length N over R is the following:*

$$\prod_{b\in I}\left(\frac{p^{rr_b(z_b+1)}-1}{p^{rr_b}-1}\right), \tag{25}$$

where $z_b = min\{[\frac{d_b}{2}], p^{s-1}\}$ and $T_0(C_b) + T_1(C_b) = d_b \le p^s$.

Proof. By Corollary 3, it suffices to compute N_b, $b \in I$. First fix T_1; thus, $T_0 = d_b - T_1$. Let $d_p < p^s$. By Theorem 1, $< (\alpha_0 w-1)^{T_0} + ue(w), (\alpha_0 w-1)^{T_1} >$ is a representation. Moreover, we have $(p^{rr_b})^{T_1}$ choices for $e(w) = \sum_{i=0}^{T_1-1} a_i(\alpha_0 w-1)^i$. Theorem 1 implies that $T_1 < \min\{p^{s-1}, T_0\}$; hence, $T_1 < \min\{p^{s-1}, \lfloor\frac{d_p}{2}\rfloor\} = z_b$ because $T_1 + T_0 = d_p$. If

we vary T_1 from 0 to z_b, then there are $1 + p^{rr_b} + \ldots + (p^{rr_b})^{z_b} = \frac{p^{rr_b(z_b+1)}-1}{p^{rr_b}-1}$ of $(\alpha + u^l\beta)$-constacyclic codes of length p^s over $CR(u^k, r_b)$. In the case when $d_p = p^s$, we have two options. If $T_0 = p^s$, the only $(\alpha + u^l\beta)$-constacyclic code is $< 0, u >$ with $T_0 + T_1 = d_p$. If $T_0 < p^s$, we use a similar discussion as before. □

Remark 7. *When $k > 2$, the enumeration of all constacyclic codes of length N over R is a tedious computation.*

4.3. Torsion Codes and Hamming Distance

In this subsection, we first obtain the torsion codes of a constacyclic code C of length N over R in terms of the generators of C given in Theorem 5. Then, we reduce the Hamming distance of C to that of its $(k-1)$th torsion code.

Lemma 4. *Let $C =< g_0(x), ug_1(x), \ldots, u^{k-1}g_{k-1}(x) >$. If $u^i(h(x)) \in C$ such that $h(x) \in Tor_i(C)$, then deg $h \geq$ deg g_i.*

Proof. Assume that $u^i(h(x)) \in C$, then $u^i(h((\alpha_0 w)^{n'}\theta\xi^b)) \in C_b$, $b \in I$, $n_1 n' \equiv 1 \pmod{p^{s+d-1}}$. As $h(x) \in Tor_i(C)$, then $h((\alpha_0 w)^{n'}\alpha^b) \in Tor_i(C_p)$. This means, $h((\alpha_0 w)^{n'}\theta\xi^b) = c(w)(\alpha_0 w - 1)^{T_i}$ for some unit $c(w)$ in $S(r_b)$. Now, let $g(x) = p(x)\prod_{j=0}^{p^s}[F_j(x)]^j$, where $F_j(x)$ as defined in the proof of Theorem 5 and $p(x) = \gamma^{-1}((c_b(w)a_b^{-1}(w))_{b\in I})$. By (21), for each $b \in I$, $g((\alpha_0 w)^{n'}\theta\xi^b) = c(w)(\alpha_0 w - 1)^{T_i}$. Thus, $\gamma(h(x)) = \gamma(g(x))$; hence, $h(x) = g(x)$, i.e., deg $h =$ deg g. Therefore, deg $g \geq$ deg $\prod_{j=0}^{p^s}[F_j]^j =$ deg g_i by (22). □

Theorem 7. *If $C =< g_0(x), ug_1(x), \ldots, u^{k-1}g_{k-1}(x) >$, then $Tor_i(C) =< \overline{g_i}(x) >$.*

Proof. First, note that $u^i g_i(x) \in C$; thus, $< \overline{g_i}(x) > \subseteq Tor_i(C)$. Conversely, let $h(x) \in Tor_i(C)$, then by the definition of torsion codes, $u^i h(x) \in C$. We make use of Lemma 4, deg $h \geq$ deg g_i. By the division algorithm, there are $r(x)$ and $q(x)$ in R_N such that $h(x) - g_i(x)q(x) = r(x)$, where $r(x) = 0$ or deg $r <$ deg g_i. As $u^i r(x) \in C$, then by the minimality of deg g_i, we must have $r(x) = 0$. In other words, $h(x) \in < g_i(x) >$; thus, $\overline{h}(x) \in < \overline{g_i}(x) >$. Therefore, $Tor_i(C) \subseteq < \overline{g_i}(x) >$, and this ends the proof. □

Next, we obtain the Hamming distance of any cyclic code of length N over R.

Theorem 8. *Let C be a cyclic code of length N over R. Then, $d(C) = d(Tor_{k-1}(C))$.*

Proof. By the same argument as in Theorem 2, we obtain $d(C) = d(Tor_{k-1}(C))$, where $Tor_{k-1}(C) =< \overline{g}_{k-1}(x) >=< \prod_{j=0}^{p^s-1}\overline{F_j}(x) >$ from Theorem 7. □

4.4. Dual Codes

Define $F_j(x)$ as in the proof of Theorem 5. Let a_j be the constant of $F_j(x)$, $0 \leqslant j \leqslant p^s$. Since $\prod_{j=0}^{p^s}F_j(x) = x^{n_1} - \alpha$, then $\prod_{j=0}^{p^s}a_j = -\alpha$. Thus, a_js are units in R and a_js are the leading coefficient of $F_j^*(x) = x^{deg\ F_j}F_j(x^{-1})$. Let the following is the case.

$$m_j(x) = a_j^{-1}F_j^*(x). \tag{26}$$

Note that $m_j(x)$s are monic polynomials and $\prod_{j=0}^{p^s} a_j^{-1} = -\alpha^{-1}$. Hence, the following is the case.

$$\begin{aligned}\prod_{j=0}^{p^s} m_j(x) &= \left(\prod_{j=0}^{p^s} a_j^{-1}\right)\prod_{j=0}^{p^s} F_j^*(x)\\ &= -\alpha^{-1}x^{\Sigma_{j=0}^{p^s} deg\ F_j}\prod_{j=0}^{p^s} F_j(x^{-1})\\ &= -\alpha^{-1}x^{n_1}(x^{-n_1}-1)\\ &= x^{n_1}-\alpha^{-1}.\end{aligned}$$

Therefore, $m_j(x)$s are monic coprime divisors of $x^{n_1}-\alpha^{-1}$ in $R[x]$. Since $Tor_i(C_b) =< (\alpha_0 w-1)^j >$, then $F_j(\theta\xi^b)=0$, which implies that $F_j^*(\theta\xi^{n_1-b})=0$; hence, $m_j(\theta\xi^{n_1-b})=0$. It follows that $m_j(x)$ is the product of all minimal polynomials of α^{n_1-b} such that $Tor_i(C_b^\perp) =< (\alpha_0 w-1)^{p^s-j} >$. By Lemma 3, the following is the case:

$$\prod_{j=0}^{p^s}[F_j^*(\alpha_0 w^{n'}\theta\xi^{n_1-b})]^{p^s-j} = a_b(w)(\alpha_0 w-1)^{p^s-j}, \tag{27}$$

where $a_b(w)$ is a unit in $S(r_b)$. Define the following case:

$$G_i(x) = \prod_{j=0}^{p^s}[F_j^*(x)]^{p^s-j} + uc_i(x), \tag{28}$$

where $c_i(x) = \gamma^{-1}((a_b(w)h'_{i,b}(w))_{b\in I})$ and $h'_{i,b}(w)$ as in Theorem 3.

Theorem 9. *Let C be a constacyclic code of length N over R. Then, the following is the case.*

$$C^\perp =< G_0(x), uG_1(x), \ldots, u^{k-1}G_{k-1}(x) > .$$

Furthermore, $|C^\perp| = p^{rt'}$, where $t' = \Sigma_{j=0}^{p^s} jdeg\ F_j^*$.

Proof. By Theorem 4, $C = \oplus_{b\in I} C_b$, where C_b is a constcyclic code of length p^s over $CR(p^n, rr_b)$. Assume that $D = \oplus_{b\in I} C_b^\perp$. By the definition of dual code, $D \subseteq C^\perp$. On the other hand, we have $|C_b|\cdot|C_b^\perp| = p^{rr_b k p^s}$. Then, $|C|\cdot|D| = p^{rkN}$; thus,

$$C^\perp = D = \oplus_{b\in I} C_b^\perp.$$

Therefore, by a similar argument to that of the proof of Theorem 5, we obtain

$$C^\perp =< G_0(x), uG_1(x), \ldots, u^{k-1}G_{k-1}(x) >,$$

where $G_i(x)$ is defined in (28) and $0 \le i \le k-1$. By Corollary 2 and the fact that $|C^\perp|\cdot|C| = p^{rkN}$, we obtain $|C^\perp| = p^{rt'}$, where $t' = \Sigma_{j=0}^{p^s} jdeg\ \ F_j^*$. □

To summarize, the results of this section provide an algorithm for constructing the representation of constacyclic codes of length $N = n_1 p^s$ from those of length p^s. This algorithm consists of the following steps:

Step 1: Find θ, ξ, I and all r_b, $b \in I$;
Step 2: Compute $F_j(x)$ for each $0 \le j \le p^s$ when i is fixed;
Step 3: Find $a_b(x)$, $b \in I$ from the relation (21);
Step 4: Extract $b_i(x)$ by using $b_i(x) = \gamma^{-1}((a_b(w)h_{i,b}(w))_{b\in I})$, $0 \le i \le k-1$;
Step 5: Compute the polynomials $g_i(x)$ via Equation (22).

Next, we present an example illustrating the algorithm described above.

Example 4. *Consider* $R = \mathbb{Z}_2 + u\mathbb{Z}_2$ *and* $N = 6$. *First,* $n_1 = 3$, $I = \{0, 1\}$, $r_0 = 1$, *and* $r_1 = 2$. *Let* $C_0 =< (w-1), u(w-1) >$, *and* $C_1 =< (w-1), u >$ *be cyclic codes of length* 2 *over* R *and* $CR(u^2, 2)$, *respectively. Next, compute* $F_j(x)$ *for* $i = 0$. *As* $T_0(C_0) = 1 = T_0(C_1)$ *and by the definition of* $F_j(x)$,

$$F_0(x) = 1, F_2(x) = 1 \text{ and } F_1(x) = f_0(x)f_1(x) = (x-1)(x-\alpha)(x-\alpha^2) = x^3 - 1,$$

where α *is a third primitive root of unity satisfying* $\alpha^2 + \alpha + 1 = 0$. *Since* $h_{0,0}(x) = h_{0,1}(x) = 0$, *then* $b_0(x) = 0$; *thus,* $g_0(x) = \prod_{j=0}^{2} F_j(x)^j = x^3 - 1$. *Now, find* $F_j(x)$ *when* $i = 1$, *note that* $T_1(C_0) = 1$ *and* $T_1(C_1) = 0$. *It follows that* $F_2(x) = 1$, $F_0(x) = (x-\alpha)(x-\alpha^2)$ *and* $F_1(x) = (f_0(x)) = (x-1)$. *As* $b_1(x) = 0$ *since* $h_{1,0}(x) = 0 = h_{1,1}(x)$, $g_1(x) = \prod_{j=0}^{2} F_j(x)^j = x - 1$. *Therefore, by Theorem 5, the following is the case.*

$$C =< x^3 - 1, u(x-1) > .$$

Remark 8. *The same algorithm described above can be applied to compute the generators of dual codes. The main key for performing this is to consider* $C_b^{\perp}$ *instead of* C_b, *where* $b \in I$.

5. Conclusions

In this article, we have determined a unique representation of any constacyclic code of arbitrary length N over a finite chain ring of characteristic p via discrete Fourier transform (DFT). Such representations allowed us to compute Hamming distance and dual codes easily. Moreover, we managed to provide the number of constacyclic codes of length N over R in terms of that of length p^s, where $v_p(N) = s$ and v_p is the p-adic valuation. In particular, we provided the exact number of such codes when $k = 2$.

Author Contributions: Conceptualization, S.A. and Y.A.; methodology, S.A. and Y.A.; investigation, S.A. and Y.A.; writing—original draft preparation, S.A.; supervision, Y.A.; funding acquisition, Y.A. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to thank the Deanship of scientific research in King Saud University for funding and supporting this research through the initiative of DSR Graduate Students Research Support (GSR).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Falkner, G.; Kowol, B.; Heise, W.; Zehendner, E. On the existence of cyclic optimal codes. *Atti Semin. Mat. Fis. Univ. Modena* **1979**, *28*, 326–341.
2. Van Lint, J. Repeated-root cyclic codes. *IEEE Trans. Inform. Theory* **1991**, *37*, 343–345. [CrossRef]
3. Blackford, T. Negacyclic codes over $\mathbb{Z}_4$ of even length. *IEEE Trans. Inform. Theory* **2003**, *49*, 1417–1424. [CrossRef]
4. Norton, G.; Sălăgean, A. On the structure of linear cyclic codes over finite chain rings. *Appl. Algebra Engrg. Commun. Comput.* **2000**, *10*, 489–506. [CrossRef]
5. Blackford, T. Cyclic codes over $\mathbb{Z}_4$ of oddly even length. *Discret. Appl. Math.* **2003**, 128, 27–46. [CrossRef]
6. Dougherty, S.; Ling, S. Cyclic codes over $\mathbb{Z}_4$ of even length. *Des. Codes Cryptogr.* **2006**, *39*, 127–153. [CrossRef]
7. Sălăgean, A. Repeated-root cyclic and negacyclic codes over finite chain rings. *Discret. Appl. Math.* **2006**, *154*, 413–419. [CrossRef]
8. Kiah, H.; Leung, K.; Ling, S. Cyclic codes over GR(p^2, m) of length p^k. *Finite Fields Appl.* **2008**, *14*, 834–846. [CrossRef]
9. Zhu, S.; Kai, X. Dual and self-dual negacyclic codes of even length over $\mathbb{Z}_{2^a}$. *Discret. Math.* **2009**, 309, 2382–2391. [CrossRef]
10. Berman, S. Semisimple cyclic and abelian codes. *II Kibern.* **1967**, *3*, 21–30. [CrossRef]
11. Castagnoli, G.; Massey, J.; Schoeller, P.; Von Seemann, N. On repeated-root cyclic codes. *IEEE Trans. Inform. Theory* **1991**, *37*, 337–342. [CrossRef]

12. Massey, J.; Costello, D.; Justesen, J. Polynomial weights and code constructions. *IEEE Trans. Inform. Theory* **1973**, *19*, 101–110. [CrossRef]
13. Lui, X.; Lui, H. LCD codes over finite chain rings. *Finite Fields Appl.* **2015**, *43*, 1–19.
14. Dinh, H.; López-Permouth, S. Cyclic and negacyclic codes over finite chain rings. *IEEE Trans. Inform. Theory* **2004**, *50*, 1728–1744. [CrossRef]
15. Han, M.; Ye, Y.; Zhu, S.; Xu, C.; Dou, B. Cyclic codes over $F_p + uF_p + \ldots + u^{k-1}F_p$ with length $p^s n$. *Inf. Sci.* **2011**, *181*, 926–934. [CrossRef]
16. Dougherty, S.; Park, Y. On modular cyclic codes. *Finite Fields Appl.* **2007**, *13*, 31–57. [CrossRef]
17. Abualrub, T.; Oehmke, R. On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e. *IEEE Trans. Inform. Theory* **2003**, *49*, 2126–2133. [CrossRef]
18. Wolfmann, J. Negacyclic and cyclic codes over $\mathbb{Z}_4$. *IEEE Trans. Inform. Theory* **1999**, *45*, 2527–2532. [CrossRef]
19. Hammons, A., Jr.; Kumar, P.; Calderbank, A.; Sloane, N.; Sole, P. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inform. Theory* **1994**, *40*, 301–319. [CrossRef]
20. Bonnecaze, A.; Udaya, P. Cyclic codes and self-dual codes over $F_2 + uF_2$. *IEEE Trans. Inform. Theory* **1999**, *45*, 1250–1255. [CrossRef]
21. Qian, J.; Zhang, L.; Zhu, S. DFT for cyclic codes over $F + uF + \ldots + u^{k-1}F$. *Jem J. Appl. Math. Comput.* **2006**, *22*, 159–167. [CrossRef]
22. Ozger, Z.; Karaa, U.; Yıldıza, B. Linear, Cyclic and Constacyclic Codes over $S_4 = F_2 + uF_2 + u^2F_2 + u^3F_2$. *Fac. Sci. Math. Univ. Nis Serbia* **2014**, *28*, 897–906.
23. Udaya, P.; Siddiqi, M. Optimal large linear complexity frequency hopping patterns derived from polynomials residue class ring. *IEEE Trans. Inform. Theory* **1998**, *44*, 1492–1503. [CrossRef]
24. Jasbir, K.; Sucheta, D.; Ranjeet, S. On cyclic codes over Galois rings. *Discret. Appl. Math.* **2020**, *280*, 156–161.
25. Wolfmann, J. Binary images of cyclic codes over $\mathbb{Z}_4$. *IEEE Trans. Inform. Theory* **2001**, *47*, 1773–1779. [CrossRef]
26. Zhu, S.; Kai, X. A class of constacyclic codes over $\mathbb{Z}_{p^m}$. *Finite Fields Appl.* **2010**, *16*, 243–254. [CrossRef]
27. Dinh, H. Constacyclic codes of length p^s over $F_{p^m} + F_{p^m}$. *J. Algebra* **2010**, *324*, 940–950. [CrossRef]
28. Huffman, W.; Pless, V. *Fundamental of Error-Correcting Codes*; Cambridge University Press: Cambridge, UK, 2003.
29. Mac Williams, F.; Sloane, N. *The Theory of Error-Correcting Codes*; 10th Impression: Amsterdam, The Netherlands, 1998.
30. Alkhamees, Y. The determination of the group of automorphisms of a finite chain ring of characteristic p. *Quart. J. Math. Oxford* **1991**, *42*, 387–391. [CrossRef]
31. Clark, W. A coefficient ring of finite commutative chain rings. *Proc. Am. Math. Soc.* **1972**, *33*, 25–27.
32. Wirt, B. Finite Non-Commutative Local Rings. Ph.D. Thesis, University of Oklahoma, Norman, OK, USA, 1972.
33. Dinh, H. On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions. *Finite Fields Appl.* **2008**, *14*, 22–40. [CrossRef]
34. Dinh, H. Negacyclic codes of length 2^s over Galois rings. *IEEE Trans. Inform. Theory* **2005**, *51*, 4252–4262. [CrossRef]
35. Pless, V.; Huffman, W. *Handbook of Coding Theory*; Elsevier: Amsterdam, The Netherlands, 1998.