International Journal of Pure and Applied Mathematics
Volume 59 No. 2 2010, 213-224

ON THE GENERATOR POLYNOMIALS OF CONSTACYCLIC CODES OVER FINITE CHAIN RINGS

Somphong Jitman[1] §, Patanee Udomkavanich[2]

[1]Department of Mathematics
Faculty of Science
Chulalongkorn University
Bangkok, 10330, THAILAND
e-mail: somphong.c@student.chula.ac.th

[2]Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
Singapore, 637371, REPUBLIC OF SINGAPORE
e-mail: pattanee.u@chula.ac.th

Abstract: The structure of constacyclic codes over finite chain rings is determined in terms of generator polynomials. Moreover, some special forms of generator polynomials of cyclic, $(1-\gamma^{m-1})$-constacyclic and $(1+\gamma^{m-1})$-constacycic codes are given. Finally, generator polynomials of the Gray images of $(1-u)$-constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$ are rewarded.

AMS Subject Classification: 94B15, 94B60
Key Words: constacyclic code, finite chain ring, cyclic code, generator polynomial

1. Introduction

Cyclic and negacyclic codes over rings are of great interest because they form an important class of linear codes due to their rich algebraic structure. The structure of cyclic codes over $\mathbb{Z}_{p^m}$ was obtained by Calderbank and Sloane in

Received: January 22, 2010

§Correspondence author

[3] and later on, with a different proof by Kanwar in [6]. Using the techniques presented in [6], Wan [10] extended Kanwar's results to cyclic codes over Galois rings. In 2004, Dinh and López-Permouth extended the structure theorem given in [10] to cyclic and negacyclic codes over finite chain rings [4].

In this paper, we use techniques presented in [4] to characterize the structure of constacyclic codes, generalizations of both cyclic and negacyclic codes, over finite chain rings in the case where the code length and the characteristic of rings are relatively prime. Results concerning finite chain rings and some basic properties of constacyclic codes are recalled in Section 2. The structural characterization of constacyclic codes comes in Section 3. Finally, in Section 4, generator polynomials of Gray images of $(1-u)$-constacyclic codes over $\mathbb{F}_p+u\mathbb{F}_p$ are given as an application of the previous section.

2. Preliminaries

A finite commutative ring $\mathcal{R}$ with identity $1 \neq 0$ is called a *finite chain ring* if its ideals are linearly ordered by inclusion. It is easily seen that the ideals of $\mathcal{R}$ are principal and $\mathcal{R}$ has a unique maximal ideal. Let γ be a generator of its maximal ideal. The nilpotency index of $\mathcal{R}$ is defined to be the smallest positive integer m such that $\gamma^m = 0$. The residue field of $\mathcal{R}$ is $\mathcal{R}/\langle\gamma\rangle \cong \mathbb{F}_q$, for some prime power integer q. Note that both the characteristic and the cardinality of $\mathcal{R}$ were shown, in [2, Theorem 6.1.2], to be powers of p, the characteristic of its residue field. All ideals of $\mathcal{R}$ form a chain as follows:

$$\mathcal{R} = \langle 1 = \gamma^0\rangle \supsetneq \langle\gamma\rangle \supsetneq \langle\gamma^2\rangle \supsetneq \cdots \supsetneq \langle\gamma^{m-1}\rangle \supsetneq \langle\gamma^m\rangle = \{0\}.$$

Throughout this paper, let $\mathcal{R}$ denote a finite chain ring with maximal ideal $\langle\gamma\rangle$, nilpotency index m, and residue field $\mathbb{F}_q$. An element in $\mathcal{R}$ can be represented in terms of generators of its ideals as follows:

Lemma 1. (see [9, Lemma 2.4]) *Let $V \subseteq \mathcal{R}$ be a set of representatives for the equivalence classes of $\mathcal{R}$ under congruence modulo γ. Then the followings hold:*

(i) For each $a \in \mathcal{R}$, there are unique $a_0, a_1, \ldots a_{m-1} \in V$ such that

$$a = a_0 + a_1\gamma + \cdots + a_{m-1}\gamma^{m-1}.$$

(ii) $|V| = q$.

(iii) $|\langle\gamma^j\rangle| = q^{(m-j)}$ for $0 \leq j \leq m-1$.

Consequently, every unit $\lambda \in \mathcal{R}^*$ can be uniquely viewed as

$$\lambda = \lambda_0 + \lambda_1\gamma + \cdots + \lambda_{m-1}\gamma^{m-1},$$

where $\lambda_i \in V$ and $\lambda_0 \not\equiv 0 \pmod{\gamma}$.

A *code of length n over $\mathcal{R}$* is a nonempty subset of $\mathcal{R}^n$. A code $\mathcal{C}$ is said to be *linear* if it is a submodule of the $\mathcal{R}$-module $\mathcal{R}^n$. In this paper, any codes are assumed to be linear unless otherwise stated.

For a given unit $\lambda \in \mathcal{R}^*$, a code $\mathcal{C}$ is said to be constacyclic, or specifically, λ-constacyclic if

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

Especially, cyclic and negacyclic codes when λ are 1 and -1, respectively. It is well-known that λ-constacyclic codes over $\mathcal{R}$ are in correspondence with ideals in $\mathcal{R}[x]/\langle x^n - \lambda\rangle$.

Throughout this article, we assume that the code length n and the characteristic of $\mathcal{R}$ are relatively prime, or equivalently, the characteristic p of $\mathbb{F}_q$ and n are relatively prime.

Two polynomials $f(x), g(x) \in \mathcal{R}[x]$ are said to be *coprime* if $\mathcal{R}[x] = \langle f(x)\rangle + \langle g(x)\rangle$. In other words, $f(x), g(x)$ are coprime if and only if there exist $a(x), b(x) \in \mathcal{R}[x]$ such that $1 = a(x)f(x) + b(x)g(x)$. A polynomial $f(x)$ is called *square-free* if $f(x)$ has no square factor. A monic polynomial $f(x)$ in $\mathcal{R}[x]$ is said to be a basic irreducible polynomial if its componentwise reduction modulo γ is irreducible in $\mathbb{F}_q[x]$.

3. The Structure of Constacyclic Codes over Finite Chain Rings

In this section, we account for a structural description of a λ-constacyclic codes of length n over $\mathcal{R}$ in terms of the ideals in $\mathcal{R}[x]/\langle x^n - \lambda\rangle$, where λ is a unit in $\mathcal{R}$.

First, we note that the Hensel's Lemma (see [8, Theorem XIII.4]) guarantees that a basic monic irreducible polynomial in $\mathcal{R}[x]$ can be lifted from a monic irreducible polynomial in $\mathbb{F}_q[x]$. Moreover, the uniqueness of a lifted polynomial is guaranteed by the following proposition.

Proposition 2. (see [4, Proposition 2.7]) *If $p(x)$ is a monic polynomial in $\mathcal{R}[x]$ such that its componentwise reduction modulo γ is square free, then $p(x)$ has a uniquely factorization as a product of pairwise coprime monic basic irreducible polynomials.*

Since n and p are relatively prime, the componentwise reduction modulo γ of $x^n - \lambda$ is square free in $\mathbb{F}_q[x]$. It follows from Proposition 2 that $x^n - \lambda$ has a unique decomposition as a product of pairwise coprime monic basic irreducible polynomials in $\mathcal{R}[x]$.

For each factor $f(x)$ of $x^n - \lambda$, let $\widehat{f}(x)$ denote $\frac{x^n-\lambda}{f(x)}$. The notation $\widehat{f}(x)$ plays an important role in characterizing the structure of λ-constacyclic codes.

The next theorem follows immediately from an application of the proof of Theorem 3.2 in [4].

Theorem 3. *Let $x^n - \lambda = f_1(x)f_2(x)\dots f_r(x)$ be factored as a product of pairwise coprime monic basic irreducible polynomials in $\mathcal{R}[x]$. Then every ideal in $\mathcal{R}[x]/\langle x^n - \lambda\rangle$ is a sum of ideals of the form $\langle \gamma^j \widehat{f}_i(x) + \langle x^n - \lambda\rangle\rangle$, where $0 \le j \le m$ and $1 \le i \le r$.*

Corollary 4. *The numbers of λ-constacyclic codes of length n over $\mathcal{R}$ is $(m+1)^r$, where r is the number of factors in the unique factorization of $x^n - \lambda$ into a product of pairwise coprime monic basic irreducible polynomials.*

For a coset $f(x)+\langle x^n-\lambda\rangle$, if the degree of $f(x)$ is less than n, then $f(x)$ is its unique representative. For a convenience, we write $f(x)$ for the corresponding coset $f(x) + \langle x^n - \lambda\rangle$. However, the computation is reduced modulo $x^n - \lambda$.

According to Theorem 3, a λ-constacyclic code $\mathcal{C}$ can be viewed as

$$\begin{aligned}\mathcal{C} = \langle \widehat{f}_{k_1+1}(x)\rangle \oplus \cdots \oplus \widehat{f}_{k_1+k_2}(x)\rangle \oplus \langle \gamma\widehat{f}_{k_1+k_2+1}(x)\rangle \oplus \cdots \oplus \langle \gamma\widehat{f}_{k_1+k_2+k_3}(x)\rangle \\ \oplus \cdots \oplus \langle \gamma^{m-1}\widehat{f}_{k_1+\cdots+k_t+1}(x)\rangle \oplus \cdots \oplus \langle \gamma^{m-1}\widehat{f}_r(x)\rangle,\end{aligned}$$

where $k_1, k_2, \dots, k_t \ge 0$ and $k_1 + k_2 + \cdots + k_m + 1 \le r$. Let $k_0 = 0$ and k_{m+1} a nonnegative integer such that $k_1 + \cdots + k_m + k_{m+1} = r$. For each $i \in \{0, 1, \dots, m\}$, let $F_i(x)$ be a polynomial defined by

$$F_i(x) = \begin{cases} 1 & \text{if } k_{i+1} = 0, \\ f_{k_0+\cdots+k_i+1}(x)\dots f_{k_0+\cdots+k_{i+1}}(x) & \text{if } k_{i+1} \neq 0. \end{cases}$$

Then the next two theorems are consequences of Theorem 3.4 in [4] and Theorem 3.6 in [4], respectively.

Theorem 5. *Let $\mathcal{C}$ be a λ-constacyclic code of length n over $\mathcal{R}$. Then there exists a unique family of pairwise coprime monic polynomials $F_0(x), F_1(x), \dots, F_m(x)$ in $\mathcal{R}[x]$ such that $F_0(x)F_1(x)\dots F_m(x) = x^n - \lambda$ and*

$$\mathcal{C} = \langle \widehat{F}_1(x), \gamma\widehat{F}_2(x), \dots, \gamma^{m-1}\widehat{F}_m(x)\rangle.$$

Moreover, $|\mathcal{C}| = q^{\sum_{i=0}^{m-1}(m-i)\deg(F_{i+1}(x))}$

Theorem 6. *Let $\mathcal{C}$ be a λ-constacyclic code of length n over $\mathcal{R}$ with*

notations as in Theorem 5. Then $\mathcal{C} = \langle \widehat{F}_1(x) + \gamma\widehat{F}_2(x) + \cdots + \gamma^{m-1}\widehat{F}_m(x)\rangle$.

The next corollary follows directly from Theorem 6.

Corollary 7. *The ring* $\mathcal{R}[x]/\langle x^n - \lambda\rangle$ *is a principal ideal ring.*

For $0 \le i \le m-1$, define

$$g_i(x) = \begin{cases} F_0(x)F_{i+2}(x)\dots F_m(x) & \text{if } 0 \le i \le m-2, \\ F_0(x) & \text{if } i = m-1. \end{cases}$$

Then, by an application of the proof of Theorem 3.5 in [4], a λ-constacyclic code $\mathcal{C}$ of length n over $\mathcal{R}$ is shown to have a generator polynomial in the form of $g_i(x)$'s.

Theorem 8. *Let* $\mathcal{C}$ *be a* λ*-constacyclic code of length* n *over* $\mathcal{R}$. *Then there exist polynomials* $g_0(x), g_1(x), \dots, g_{m-1}(x)$ *in* $\mathcal{R}[x]$ *such that*

$$\mathcal{C} = \langle g_0(x), \gamma g_1(x), \dots, \gamma^{m-1}g_{m-1}(x)\rangle$$

and

$$g_0(x) \mid g_1(x) \mid \cdots \mid g_{m-1}(x) \mid (x^n - \lambda).$$

For the rest of this section, we generalized some results of [7] to work for arbitrary finite chain rings. We determine generator polynomials of some cyclic, $(1-\gamma^{m-1})$-constacyclic and $(1+\gamma^{m-1})$-constacyclic codes in other forms.

First, we recall some results concerning the structures of quotient rings $\mathcal{R}[x]/\langle x^n-1\rangle$, $\mathcal{R}[x]/\langle x^n-(1-\gamma^{m-1})\rangle$ and $\mathcal{R}[x]/\langle x^n-(1+\gamma^{m-1})\rangle$. Since the code length n and the characteristic of $\mathcal{R}$ are relatively prime, we have $\gcd(n,p) = 1$ and hence there exists $n' \in \{0, 1, \dots, p-1\}$ such that $nn' \equiv 1 (\mathrm{mod}\ p)$. Let $\beta = 1 + n'\gamma^{m-1}$. Then $\beta^j = (1+n'\gamma^{m-1})^j = 1 + jn'\gamma^{m-1} \in \mathcal{R}$, for all $j \in \mathbb{Z}$. In particular, $\beta^n = 1 + \gamma^{m-1}$ and $\beta^{-n} = 1 - \gamma^{m-1}$. It is easily seen that the following maps are ring isomorphisms:

$$\begin{aligned} \mu : \mathcal{R}[x]/\langle x^n - 1\rangle &\to \mathcal{R}[x]/\langle x^n - (1-\gamma^{m-1})\rangle \\ p(x) &\mapsto p(\beta x) \end{aligned}$$

and

$$\begin{aligned} \nu : \mathcal{R}[x]/\langle x^n - 1\rangle &\to \mathcal{R}[x]/\langle x^n - (1+\gamma^{m-1})\rangle \\ p(x) &\mapsto p(\beta^{-1} x). \end{aligned}$$

These isomorphisms induce one-to-one correspondences between the ideals of these rings.

Generator polynomials of cyclic, $(1-\gamma^{m-1})$-constacyclic and $(1+\gamma^{m-1})$-constacyclic codes are given as follows:

Theorem 9. *Let $A(x), B(x), C(x)$ be pairwise coprime monic polynomials in $\mathcal{R}[x]$ such that $x^n - 1 = A(x)B(x)C(x)$ and $\mathcal{C} = \langle A(x)B(x), \gamma^{m-1}A(x)C(x)\rangle$. Then $\mathcal{C} = \langle A(x)\left(B(x) + \gamma^{m-1}\right)\rangle$.*

Proof. Since $B(x)$ and $C(x)$ are coprime, there exist $S(x), T(x) \in \mathcal{R}[x]$ such that $1 = S(x)B(x) + T(x)C(x)$. Then

$$\gamma^{m-1}A(x) = S(x)\gamma^{m-1}A(x)B(x) + T(x)\gamma^{m-1}A(x)C(x) \in \mathcal{C}$$

because $\gamma^{m-1}A(x)B(x), \gamma^{m-1}A(x)C(x) \in \mathcal{C}$. Thus

$$A(x)(B(x) + \gamma^{m-1}) = A(x)B(x) + \gamma^{m-1}A(x) \in \mathcal{C}.$$

Therefore, $\langle A(x)(B(x) + \gamma^{m-1})\rangle \subseteq \mathcal{C}$.

On the other hand, in $\mathcal{R}[x]/\langle x^n - 1\rangle$, we have

$$\gamma^{m-1}A(x)C(x) = A(x)(B(x) + \gamma^{m-1})C(x) \in \langle A(x)(B(x) + \gamma^{m-1})\rangle$$

and

$$\gamma^{m-1}A(x)B(x) = A(x)(B(x) + \gamma^{m-1})\gamma^{m-1} \in \langle A(x)(B(x) + \gamma^{m-1})\rangle.$$

Since $B(x)$ and $C(x)$ are coprime, we have $\gamma^{m-1}A(x) \in \langle A(x)(B(x) + \gamma^{m-1})\rangle$. Consequently,

$$A(x)B(x) = A(x)(B(x) + \gamma^{m-1}) - \gamma^{m-1}A(x) \in \langle A(x)(B(x) + \gamma^{m-1})\rangle.$$

As desired, $\mathcal{C} \subseteq \langle A(x)(B(x) + \gamma^{m-1})\rangle$. □

Corollary 10. *If $m = 2$, then a cyclic code $\mathcal{C}$ of length n over $\mathcal{R}$ is generated by a polynomial of the form $A(x)\left(B(x) + \gamma^{m-1}\right)$ or a constant polynomial, where $A(x), B(x), C(x)$ are pairwise coprime monic polynomials in $\mathcal{R}[x]$ such that $x^n - 1 = A(x)B(x)C(x)$.*

Proof. Putting $m = 2$ in Theorem 5, we have $\mathcal{C} = \langle A(x)B(x), \gamma A(x)C(x)\rangle$. Then the result follows immediately from Theorem 9. □

Theorem 11. *Let $A(x), B(x), C(x)$ be pairwise coprime monic polynomials in $\mathcal{R}[x]$ such that $x^n - 1 = A(x)B(x)C(x)$. Then the followings hold:*

(i) $x^n - (1 - \gamma^{m-1}) = A'(x)B'(x)C'(x)$, where $A'(x) = \beta^{-\deg(A(x))}A(\beta x)$, $B'(\beta x) = \beta^{-\deg(B(x))}B(\beta x)$ and $C'(x) = \beta^{-\deg(C(x))}C(\beta x)$.

(ii) If $\mathcal{C}'$ is a $(1 - \gamma^{m-1})$-constacyclic code such that

$$\mathcal{C}' = \langle A'(x)B'(x), \gamma^{m-1}A'(x)C'(x)\rangle,$$

then $\mathcal{C}' = \langle A'(x)\left(B'(x) + \gamma^{m-1}\right)\rangle$.

Proof. Part i) follows immediately from the definitions of β, $A'(x)$, $B'(x)$ and $C'(x)$.

Part ii) is obtained via applying an argument similar to Theorem 9. □

Corollary 12. *If $m = 2$, then a $(1-\gamma)$-cyclic code $\mathcal{C}$ of length n over $\mathcal{R}$ is generated by a polynomial of the form $A'(x)\,(B'(x)+\gamma)$ or a constant polynomial, where $A'(x), B'(x), C'(x)$ are pairwise coprime monic polynomials in $\mathcal{R}[x]$ such that $x^n-(1-\gamma) = A'(x)B'(x)C'(x)$.*

Proof. Since μ is a ring isomorphism, $\mathcal{C}' = \mu(\mathcal{C})$ for some cyclic code $\mathcal{C}$ in $\mathcal{R}[x]/\langle x^n-1\rangle$. It follows from Theorem 9 that $\mathcal{C} = \langle A(x)B(x), \gamma A(x)C(x)\rangle$, where $x^n-1 = A(x)B(x)C(x)$ and $A(x), B(x), C(x)$ are pairwise coprime monic polynomials. Thus

$$\mathcal{C}' = \langle A(\beta x)B(\beta x), \gamma A(\beta x)C(\beta x)\rangle,$$

where $\beta = 1+n'\gamma$. Let $A'(x) = \beta^{-\deg(A(x))}A(\beta x), B'(x) = \beta^{-\deg(B(x))}B(\beta x)$ and $C'(x) = \beta^{-\deg(C(x))}C(\beta x)$. It is easily seen that $A'(x), B'(x), C'(x)$ are pairwise coprime monic polynomials satisfying $x^n-(1-\gamma) = A'(x)B'(x)C'(x)$ and

$$\mathcal{C}' = \langle \beta^{\deg(A(x))+\deg(B(x))}A'(x)B'(x), \gamma\beta^{\deg(A(x))+\deg(C(x))}A'(x)C'(x)\rangle.$$

As β is a unit,

$$\mathcal{C}' = \langle A'(x)B'(x), \gamma A'(x)C'(x)\rangle.$$

A desired result follows from Part ii) of Theorem 11. □

Theorem 13. *Let $A(x), B(x), C(x)$ be pairwise coprime monic polynomials in $\mathcal{R}[x]$ such that $x^n-1 = A(x)B(x)C(x)$. Then the followings hold:*

(i) $x^n-(1+\gamma^{m-1}) = A''(x)B''(x)C''(x)$, where $A''(x) = \beta^{\deg(A(x))}A(\beta^{-1}x)$, $B''(x) = \beta^{\deg(B(x))}B(\beta^{-1}x)$ and $C''(x) = \beta^{\deg(C(x))}C(\beta^{-1}x)$.

(ii) If C'' is a $(1+\gamma^{m-1})$-constacyclic code such that

$$\mathcal{C}'' = \langle A''(x)B''(x), \gamma^{m-1}A''(x)C''(x)\rangle,$$

then $\mathcal{C}'' = \langle A''(x)\left(B''(x)+\gamma^{m-1}\right)\rangle$.

Proof. Part i) follows directly from the definitions of β, $A''(x)$, $B''(x)$ and $C''(x)$.

Part ii) is obtained via applying an argument similar to Theorem 9. □

Using ν and Theorem 13, the next corollary is concluded by applying an argument similar to Corollary 12.

Corollary 14. *If $m = 2$, then a $(1+\gamma)$-constacyclic code $\mathcal{C}$ of length n over $\mathcal{R}$ is generated by a polynomial of the form $A''(x)\,(B''(x)+\gamma)$ or a constant polynomial, where $A''(x), B''(x), C''(x)$ are pairwise coprime monic polynomials in $\mathcal{R}[x]$ such that $x^n-(1+\gamma) = A''(x)B''(x)C''(x)$.*

Theorem 15. *Let notations be defined as above. Then the followings*

hold:

(i) In $\mathcal{R}[x]/\langle x^n-1\rangle$, *we have* $\langle A(x)\left(B(x)+\gamma^{m-1}\right)\rangle\cap\langle\gamma^{m-1}\rangle=\langle\gamma^{m-1}A(x)\rangle$.

(ii) In $\mathcal{R}[x]/\langle x^n-(1-\gamma^{m-1})\rangle$, *we have*

$$\langle A'(x)\left(B'(x)+\gamma^{m-1}\right)\rangle\cap\langle\gamma^{m-1}\rangle=\langle\gamma^{m-1}A'(x)\rangle.$$

(iii) In $\mathcal{R}[x]/\langle x^n-(1+\gamma^{m-1})\rangle$, *we have*

$$\langle A''(x)\left(B''(x)+\gamma^{m-1}\right)\rangle\cap\langle\gamma^{m-1}\rangle=\langle\gamma^{m-1}A''(x)\rangle.$$

Proof. Part *i*), if $C(x)=1$, then $A(x)B(x)=0\in\mathcal{R}[x]/\langle x^n-1\rangle$. It is clear that $\gamma^{m-1}A(x)\in\langle\gamma^{m-1}\rangle$. Hence

$$\langle A(x)(B(x)+\gamma^{m-1})\rangle\cap\langle\gamma^{m-1}\rangle=\langle\gamma^{m-1}A(x)\rangle\cap\langle\gamma^{m-1}\rangle=\langle\gamma^{m-1}A(x)\rangle.$$

Next, we assume that $C(x)\neq 1$. In the proof of Theorem 9, it has been shown that $\gamma^{m-1}A(x)\in\langle A(x)(B(x)+\gamma^{m-1})\rangle$. Clearly, $\gamma^{m-1}A(x)\in\langle\gamma^{m-1}\rangle$. Consequently,

$$\langle\gamma^{m-1}A(x)\rangle\subseteq\langle A(x)(B(x)+\gamma^{m-1})\rangle\cap\langle\gamma^{m-1}\rangle.$$

On the other hand, let $F(x)\in\langle A(x)(B(x)+\gamma^{m-1})\rangle\cap\langle\gamma^{m-1}\rangle$. Then

$$\gamma^{m-1}S(x)=F(x)=A(x)(B(x)+\gamma^{m-1})T(x)\in\mathcal{R}[x]/\langle x^n-1\rangle,$$

for some $S(x),T(x)$ in $\mathcal{R}[x]$. Since $C(x)\neq 0$, applying the division algorithm, we have

$$T(x)=C(x)Q(x)+R(x)$$

for some unique $Q(x),R(x)$ such that $\deg(R(x))<\deg(C(x))$ or $R(x)=0$. Thus,

$$\begin{aligned}\gamma^{m-1}S(x)=F(x)&=A(x)(B(x)+\gamma^{m-1})T(x)\\&=A(x)(B(x)+\gamma^{m-1})(C(x)Q(x)+R(x))\\&=A(x)B(x)R(x)+\gamma^{m-1}A(x)T(x)\\&\in\mathcal{R}[x]/\langle x^n-1\rangle.\end{aligned}\tag{1}$$

If $R(x)=0$, then $F(x)=\gamma^{m-1}A(x)T(x)\in\langle\gamma^{m-1}A(x)\rangle$.

Finally, we assume that $R(x)\neq 0$. Computing (1) modulo γ^{m-1}, we have $\widetilde{A(x)}\widetilde{B(x)}\widetilde{R(x)}=0\in(R/\gamma^{m-1})[x]/\langle x^n-1\rangle$, where $\widetilde{A(x)},\widetilde{B(x)},\widetilde{R(x)}$ denote the reductions modulo γ^{m-1} of $A(x),B(x),R(x)$, respectively. Since $\deg(R(x))<\deg(C(x))$, we have $\deg(\widetilde{A(x)}\widetilde{B(x)}\widetilde{R(x)})<n$. The hypothesis $C(x)\neq 1$ implies that $\widetilde{A(x)}\widetilde{B(x)}\neq 0$ is monic. Then $\widetilde{R(x)}=0$, and hence $R(x)=\gamma^{m-1}R_1(x)$ for some $R_1(x)$ in $R[x]$. Thus

$$F(x)=\gamma^{m-1}A(x)(B(x)R_1(x)+T(x))\in\langle\gamma^{m-1}A(x)\rangle.$$

As a result $\langle A(x)(B(x)+\gamma^{m-1})\rangle \cap \langle \gamma^{m-1}\rangle \subseteq \langle \gamma^{m-1}A(x)\rangle$.

Part ii) and Part iii) follows from applications of μ and ν, respectively. □

4. Generator Polynomials of the Gray Images of $(1-u)$-Constacyclic Codes over $\mathbb{F}_p + u\mathbb{F}_p$

In this section, we focus on $(1-u)$-consatcyclic codes of length n over $\mathbb{F}_p+u\mathbb{F}_p$, a finite chain ring with nilpotecy index $m=2$, characteristic p, maximal ideal $u\mathbb{F}_p$ and residue field $\mathbb{F}_p$. Generator polynomials of the Gray images of $(1-u)$-constacyclic codes will be given.

Following [5] the homogeneous weight of $r \in \mathbb{F}_p + u\mathbb{F}_p$ is defined in the form of

$$w_{hom}(r) = \begin{cases} p-1 & \text{if } r \in \mathbb{F}_p + u\mathbb{F}_p \setminus u\mathbb{F}_p, \\ p & \text{if } r \in u\mathbb{F}_p + u\mathbb{F}_p \setminus \{0\}, \\ 0 & \text{otherwise.} \end{cases}$$

The homogeneous weight w_{hom} on $\mathbb{F}_p + u\mathbb{F}_p$ is extended to a *weight function* in $(\mathbb{F}_p + u\mathbb{F}_p)^n$ by

$$w_{hom}(\mathbf{r}) = \sum_{i=0}^{n-1} w_{hom}(r_i),$$

where $\mathbf{r} = (r_0, r_1, \ldots, r_{n-1}) \in (\mathbb{F}_p + u\mathbb{F}_p)^n$. The *homogeneous distance* $d_{hom}(\mathbf{r}, \mathbf{s})$ between $\mathbf{r}, \mathbf{s} \in (\mathbb{F}_p + u\mathbb{F}_p)^n$ is defined to be $w_{hom}(\mathbf{r} - \mathbf{s})$.

The Gray map ϕ on $(\mathbb{F}_p + u\mathbb{F}_p)^n$, which is a light version of the Gray map defined in [1], is given by

$$\begin{aligned} \phi :& (\mathbb{F}_p + u\mathbb{F}_p)^n \to \mathbb{F}_p^{np} \\ & \mathbf{a} + u\mathbf{b} \mapsto (\mathbf{b}, \mathbf{b}+\mathbf{a}, \mathbf{b}+2\mathbf{a} \ldots, \mathbf{b}+(p-1)\mathbf{a}). \end{aligned}$$

This Gray map ϕ is an isometry from $((\mathbb{F}_p + u\mathbb{F}_p)^n, d_{hom})$ to $\mathbb{F}_p^{np}$ under the Hamming distance. It is also clear that ϕ preserves linearity of codes. The Gray map ϕ can be extend to polynomials. For a polynomial $H(x) = \sum_{i=0}^{n-1} H_i x^i$ of degree less than n in $(\mathbb{F}_p + u\mathbb{F}_p)[x]$, we define $\phi(H(x))$ to be the polynomial in $\mathbb{F}_p[x]$ of degree less than np that corresponds to $\phi(H_0, H_1, \ldots, H_{n-1})$.

The following lemma is a direct consequence of the above definition.

Lemma 16. *Let $H(x) \in (\mathbb{F}_p + u\mathbb{F}_p)[x]$ be such that $\deg(H(x)) < n$ and let $h(x) \in \mathbb{F}_p[x]$ be its reduction modulo u. Then the followings hold:*

(i) $\phi(uH(x)) \equiv h(x)(x^n-1)^{p-1} \bmod (x^{np}-1)$.

(ii) $\phi(h(x)) \equiv -x^n(x^n-1)^{p-2}h(x) \bmod (x^{pn}-1)$ *whenever* $h(x)$ *is regarded as a polynomial in* $(\mathbb{F}_p + u\mathbb{F}_p)[x]$.

In [1], the Gray images of $(1-u)$-constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$ have been show to be cyclic codes over $\mathbb{F}_p$.

Theorem 17. (see [1, Light Version of Theorem 2.2]) *A code* $\mathcal{C}$ *of length* n *over* $\mathbb{F}_p + u\mathbb{F}_p$ *is* $(1-u)$*-cyclic if and only if* $\phi(\mathcal{C})$ *is a cyclic code of length* np *over* $\mathbb{F}_p$.

Generator polynomials of the Gray images of $(1-u)$-constacyclic codes are given as follows:

Theorem 18. *Let* $\mathcal{C}'$ *be a* $(1-u)$*-constacyclic code of length* n *over* $\mathbb{F}_p + u\mathbb{F}_p$ *generated by* $A'(x)(B'(x)+u)$ *where* $x^n-(1-u) = A'(x)B'(x)C'(x)$ *and* $A'(x), B'(x), C'(x)$ *are monic pairwise coprime. Then* $\phi(\mathcal{C}')$ *is a cyclic code of length* np *over* $\mathbb{F}_p$ *generated by* $a(x)^p b(x)^{p-1}c(x)^{p-2}$ *where* $a(x), b(x), c(x)$ *are the reductions modulo* u *of* $A'(x), B'(x), C'(x)$*, respectively.*

Proof. Let $P(x)A'(x)(B'(x)+u)$ be in $\mathcal{C}'$, where $P(x)$ is a polynomial of degree less than n in $(\mathbb{F}_p + u\mathbb{F}_p)[x]$. Then, by the division algorithm, we have

$$P(x) = C'(x)Q(x) + R(x),$$

for some unique polynomials $Q(x), R(x)$ such that $\deg(R(x)) < \deg(C'(x))$ or $R(x) = 0$. Thus

$$\begin{aligned} P(x)A'(x)(B'(x)+u) &= A'(x)(B'(x)R(x) + uA'(x)P(x) \\ &= a(x)b(x)r(x) + us(x), \end{aligned}$$

where $r(x)$ is the reduction modulo u of $R(x)$ and for some $s(x) \in \mathbb{F}_p[x]$. Hence, by linearity of ϕ and Lemma 16, it follows that

$$\begin{aligned} \phi(P(x)A'(x)(B'(x)+u)) &= \phi(a(x)b(x)r(x)) + \phi(us(x)) \\ &= -x^n(x^n-1)^{p-2}a(x)b(x)r(x) + s(x)(x^n-1)^{p-1} \\ &= a(x)^{p-1}b(x)^{p-1}c(x)^{p-2}(-x^n r(x) + s(x)c(x)) \\ &\in \langle a(x)^{p-1}b(x)^{p-1}c(x)^{p-2} \rangle. \end{aligned}$$

Therefore, each element in $\phi(\mathcal{C}')$ can be viewed as $p(x)a(x)^{p-1}b(x)^{p-1}c(x)^{p-2}$ for some $p(x) \in \mathbb{F}_p[x]$. Note that, in $\mathbb{F}_p[x]/\langle x^{pn}-1 \rangle$,

$$c(x)p(x)a(x)^{p-1}b(x)^{p-1}c(x)^{p-2} = p(x)(x^n-1)^{p-1} = \phi(uP(x)),$$

where $P(x)$ is a polynomial in $(\mathbb{F}_p + u\mathbb{F}_p)[x]$ whose reduction modulo u is $p(x)$. Since $c(x)p(x)a(x)^{p-1}b(x)^{p-1}c(x)^{p-2} \in \phi(\mathcal{C}')$, we have $uP(x) \in \mathcal{C}'$. It follows

from Theorem 15 that $uP(x) \in \langle uA'(x)\rangle$, and hence $p(x) = t(x)a(x)$ for some $t(x) \in \mathbb{F}_p[x]$. Thus $p(x)a(x)^{p-1}b(x)^{p-1}c(x)^{p-2} = t(x)a(x)^p b(x)^{p-1}c(x)^{p-2} \in \langle a(x)^p b(x)^{p-1}c(x)^{p-2}\rangle$, i.e., $\phi(\mathcal{C}') \subseteq \langle a(x)^p b(x)^{p-1}c(x)^{p-2}\rangle$. Therefore, $\phi(\mathcal{C}') = \langle a(x)^p b(x)^{p-1}c(x)^{p-2}\rangle$ since they have the same cardinality. □

5. Conclusion

In this paper, we use techniques presented in [4] to characterize the structure of constacyclic codes which are generalization of both cyclic and negacyclic codes over finite chain rings in the case where the code length and the characteristic of rings are relatively prime. Some special forms of generator polynomials of some cyclic, $(1-\gamma^{m-1})$-constacyclic and $(1+\gamma^{m-1})$-constacycic codes are given. Moreover, generator polynomials of Gray images of some constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$ are rewarded.

Acknowledgments

The first author gratefully acknowledges the support from the Institute for the Promotion of Teaching Science and Technology of Thailand.

References

[1] M.C.V. Amarra, F.R. Nemenzo, On $(1-u)$-cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$, *Appl. Math. Lett.*, **21** (2008), 1129-1133.

[2] G. Bini, F. Flamini, *Finite Commutative Rings and their Applications*, Kluwer Academic Publishers, Massachusetts (2002).

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

[4] H.Q. Dinh, S.R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Trans Inform. Theory*, **50** (2004), 1728-1744.

[5] M. Greferath, S.E. Schmidt, Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code, *IEEE Transa. Inform. Theory*, **45** (1999), 2522-2624.

[6] P. Kanwar, Cyclic codes over the integers modulo p^m, *Finite Fields Appl.*, **3** (1997), 334-352.

[7] S. Ling, J. Blackford, $\mathbb{Z}_{p^{k+1}}$-linear codes, *IEEE Trans. Inform. Theory*, **48** (2002), 2592-2605.

[8] B.R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York (1974)

[9] G.H. Norton, A. Sălăgean, On the structure of linear and cyclic codes over a finite chain ring, *AAECC*, **10** (2000), 489-506.

[10] Z.X. Wan, Cyclic codes over Galois ring, *Algebr. Colloq.*, **6** (1999), 291-304.