Int. J. Communications, Network and System Sciences, **2012, 5, 222-227**
http://dx.doi.org/10.4236/ijcns.2012.54029 Published Online April 2012 (http://www.SciRP.org/journal/ijcns)

A Class of Constacyclic Codes over *R* + *vR* and Its Gray Image[*]

Dajian Liao, Yuansheng Tang
College of Science, Huaihai Institute of Technology, Lianyungang, China
Email: 1006268675@qq.com

Received January 30, 2012; revised February 13, 2012; accepted March 21, 2012

ABSTRACT

We study $(1 + 2v)$-constacyclic codes over $R + vR$ and their Gray images, where $v^2 + v = 0$ and R is a finite chain ring with maximal ideal $\langle \lambda \rangle$ and nilpotency index e. It is proved that the Gray map images of a $(1 + 2v)$-constacyclic codes of length n over $R + vR$ are distance-invariant linear cyclic codes of length $2n$ over R. The generator polynomials of this kind of codes for length n are determined, where n is relatively prime to p, p is the character of the field $R/\langle \lambda \rangle$. Their dual codes are also discussed.

Keywords: Frobenius Ring; Constacyclic Codes; Generator Polynomial; Dual Codes

1. Introduction

Cyclic codes are a very important class of codes, they were studied for over fifty years. After the discovery that certain good nonlinear binary codes can be constructed from cyclic codes over Z_4 via the Gray map, codes over finite rings have received much more attention. In particular, constacyclic codes over finite rings have been a topic of study. For example, Wolfmann [1] studied negacyclic codes over Z_4 of odd length and gave some important results about such negacyclic codes. Tapia-recillas and Vega generalized these results to the setting of codes over Z_{2^k} in [2]. More generally, the structure of negacyclic codes of length n over a finite chain ring R such that the length n is not divisible by the character p of the residue field $R/\langle \lambda \rangle$ was obtained by Dinh and López-Permouth in [3]. The situation when the code length n is divisible by the characteristic p of residue field of R yields the so-called repeated root codes. Dinh studied the structure of λ-constacyclic codes of length 2^s over Z_{2^k} [4] where λ is any unit of Z_{2^k} with form $4k - 1$, and established the Hamming, homogenous, Lee and Euclidean distances of all such constacyclic codes. Recently, linear codes over the ring $F_2 + uF_2 + vF_2 + uvF_2$ have been considered by Yildiz and Karadeniz in [5], where some good binary codes have been obtained as the images under two Gray maps. Some results about cyclic codes over $F_2 + vF_2$ and $F_p + vF_p$ were given by Zhu *et al.* in [6] and [7] respectively, where it is shown that cyclic codes over the ring are principally generated. As these two rings are not finite chain rings, some techniques used in the mentioned papers are different from those in the previous papers. It seems to be more difficult to deal with codes over these rings. In this paper, we investigate $(1 + 2v)$-constacyclic codes over $R + vR$ of length n (n is relatively prime to p, p is the character of the field $R/\langle \lambda \rangle$, where R is a finite chain ring with maximal ideal $\langle \lambda \rangle$ and nilpotency index e, and $v^2 = -v$. We define a Gray map from $R + vR$ to R^2 and prove that the Gray map image of $(1 + 2v)$-constacyclic codes over $R + vR$ of length n is a distance invariant linear cyclic codes of length $2n$ over R. The generator polynomials of this kind of codes of length n are determined and their dual codes are also discussed. We also prove that this class of constacyclic codes over the ring is principally generated.

2. Basic Concepts

In this section, we will review some fundamental backgrounds used in this paper. We assume the reader is familiar with standard terms from ring theory, as found in [8]. Let R be a finite commutative ring with identity. A code over R of length N is a nonempty subset of R^N, and a code is linear over R of length N if it is an R-submoodule of R^N. For some fixed unit μ of R, the μ-constacyclic shift τ_μ on R^N is the shift $\tau_\mu(c_0, c_1, \cdots, c_{N-1}) = (c_{N-1}, c_0, \cdots, c_{N-2})$ and a linear code C of length N over R is μ-constacyclic if the code is invariant under the

[*] Supported by the NSF of China (60473018); University graduate students' research and innovation plan of Jiangsu Province (CXLX11-0992).

μ-constacyclic shift τ_μ. Note that the R-module R^N is isomorphic to the R-module $R[x]/\langle x^N-\mu\rangle$. We identify a codeword $(c_0,c_1,\cdots,c_{N-1})$ with its polynomial representation $c(x)=c_0+c_1x+\cdots c_{N-1}x^{N-1}$. Then $xc(x)$ corresponds to the μ-constacyclic shift of $c(x)$ in the ring $R[x]/\langle x^N-\mu\rangle$. Thus μ-constacyclic codes of length N over R can be identified as ideals in the ring $R[x]/\langle x^N-\mu\rangle$. A code C is said to be cyclic if $\tau_1(C)=C$, negacyclic if $\tau_{-1}(C)=C$, μ-constacyclic if $\tau_\mu(C)=C$ respectively. Let R be a finite chain ring with maximal ideal $\langle\lambda\rangle$, e be the nilpotency index of λ, where p is the characteristic of the residue field $R/\langle\lambda\rangle$. In this section, we assume n to be a positive integer which is not divisible by p; that implies n is not divisible by the characteristic of the residue field $R/\langle\lambda\rangle$, so that x^n-1 is square free in $R[x]$. Therefore, x^n-1 has a unique decomposition as a product of basic irreducible pairwise coprime polynomials in $R[x]$. Customarily, for a polynomial f of degree k, it's reciprocal polynomial $x^kf(x^{-1})$ will be denoted by $f^*(x)$. Thus, for example, if $f(x)=a_0+a_1x+\cdots a_kx^k$, then $f^*(x)=a_k+a_{k-1}x+\cdots a_0x^k$. Moreover, if $f(x)$ is a factor of x^n-1, we denote $\hat{f}(x)=\dfrac{x^n-1}{f(x)}$, if $f(x)$ is a factor of x^n+1, we denote $\tilde{f}(x)=\dfrac{x^n+1}{f(x)}$, if $f(x)$ is a factor of $x^{2n}-1$, we denote $\overset{\frown}{f}(x)=\dfrac{x^{2n}-1}{f(x)}$. Obviously, we have $(x^n+1)\hat{f}(x)=\overset{\frown}{f}(x)$, $(x^n-1)\tilde{f}(x)=\overset{\frown}{f}(x)$.

The next six lemmas are well known, proof of them can be found in [4].

Lemma 2.1. Let C be a cyclic code of length n over a finite chain ring R (R has maximal ideal $\langle\lambda\rangle$ and e is the nilpotency of $\langle\lambda\rangle$). Then there exists a unique family of pairwise coprime monic polynomials $F_0(x),F_1(x)$, $\cdots$, $F_e(x)$ in $R[x]$ such that

$$F_0(x)F_1(x)\cdots F_e(x)=x^n-1$$

and $C=\left\langle\hat{F}_1(x),\hat{F}_2(x)\lambda,\cdots\hat{F}_e(x)\lambda^{e-1}\right\rangle$.

Moreover $|C|=|R/\langle\lambda\rangle|^{\sum_{i=1}^{e}(e-i)\cdot\deg(F_{i+1})}$.

Lemma 2.2. Let C be a cyclic code of length n with notation as in Lemma 2.1, and $F=\hat{F}_1(x)+\hat{F}_2(x)\lambda+\cdots+\hat{F}_e(x)\lambda^{e-1}$. Then F is a generating polynomial of C, *i.e.*, $C=\langle F\rangle$.

Lemma 2.3. Let C be a cyclic code over R with

$$C=\left\langle\hat{F}_1(x),\hat{F}_2(x)\lambda,\cdots\hat{F}_e(x)\lambda^{e-1}\right\rangle,$$

where $F_0(x)F_1(x)\cdots F_e(x)=x^n-1$ as in Lemma 2.1, and $F_{e+1}(x)=F_0(x)$, then

$$C^\perp=\left\langle\hat{F}_0^*(x),\hat{F}_e^*(x)\lambda,\cdots\hat{F}_2^*(x)\lambda^{e-1}\right\rangle$$

and $|C^\perp|=|R/\langle\lambda\rangle|^{\sum_{i=1}^{e}i\cdot\deg(F_{i+1})}$.

Lemma 2.4. Let C be a negacyclic code of length over a finite chain ring R (R has maximal ideal $\langle\lambda\rangle$ and e is the nilpotency of λ). Then there exists a unique family of pairwise coprime monic polynomials $G_0(x),G_1(x)$, $\cdots,G_e(x)$ in $R[x]$ such that

$$G_0(x)G_1(x)\cdots G_e(x)=x^n+1$$

and $C=\left\langle\tilde{G}_1(x),\tilde{G}_2(x)\lambda,\cdots,\tilde{G}_e(x)\lambda^{e-1}\right\rangle$.

Moreover $|C|=|R/\langle\lambda\rangle|^{\sum_{i=1}^{e}(e-i)\cdot\deg(G_{i+1})}$.

Lemma 2.5. Let C be a negacyclic code of length n with notations as in Lemma 2.6, and

$$G(x)=\tilde{G}_1(x)+\tilde{G}_2(x)\lambda+\cdots+\tilde{G}_e(x)\lambda^{e-1},$$

Then $G(x)$ is a generating polynomial of C, *i.e.*, $C=\langle G\rangle$.

Lemma 2.6. Let C be a negacyclic code over R with

$$C=\left\langle\tilde{G}_1(x),\tilde{G}_2(x)\lambda,\cdots,\tilde{G}_e(x)\lambda^{e-1}\right\rangle$$

where $G_0(x)G_1(x)\cdots G_e(x)=x^n+1$ as in Lemma 2.6 and $G_{e+1}=G_0$, then

$$C^\perp=\left\langle\tilde{G}_0^*(x),\tilde{G}_e^*(x)\lambda,\cdots,\tilde{G}_2^*(x)\lambda^{e-1}\right\rangle$$

and $|C^\perp|=|R/\langle\lambda\rangle|^{\sum_{i=1}^{e}i\cdot\deg(G_{i+1})}$.

3. Graymap

Let $\Re$ be the commutative ring $R+vR=\{a+bv|a,b\in R\}$ with $v^2=-v$. This ring is a kind of commutative Frobenius ring with two coprime ideals $\langle v\rangle=\{av|a\in R\}$ and $\langle 1+v\rangle=\{a+av|a\in R\}$. Obviously, both $R/\langle v\rangle$ and $R/\langle 1+v\rangle$ is isomorphic to R. By the Chinese Remainder Theorem, we have $R\cong\langle v\rangle\oplus\langle 1+v\rangle$.

In the rest of this paper, we denote $R+vR$ by $\Re$, where R is a finite chain ring with maximal ideal $\langle\lambda\rangle$, the nilpotency index of λ is e, the character of the residue field $R/\langle\lambda\rangle$ is p, a prime odd.

We first give the definition of the Gray map on R. Let $c=a+bv$ be an element in R, where $a,b\in R$. The Gray map $\varphi_{s,t}:\Re\to R^2$ is given by $\varphi_{s,t}(c)=(ta+sb,(t+2s)a-sb)$ where $s,t\in R$.

Lemma 3.1. The Gray map is bijection. If $s(t+s)$ is a unit in R.

Proof. Since $s(t+s)$ is a unit in R, we can define a map $\phi_{s,t}:R^2\to\Re$ by

$$\phi_{s,t}(x,y)=(2s(t+s))^{-1}(sx+sy+((t+2s)x-ty)v),$$

then for any $c = a + bv \in \Re$, we have

$$\begin{aligned}
&\phi_{s,t}\left(\varphi_{s,t}(c)\right)\\
&=\phi_{s,t}\left(ta+sb,(t+2s)a-sb\right)\\
&=\left(2s(t+s)\right)^{-1}\left(s(ta+sb)+s\left((t+2s)a-sb\right)\right)\\
&\quad+\left((t+2s)(ta+sb)-t\left((t+2s)a+tsb\right)v\right)\\
&=a+bv=c
\end{aligned}$$

This means that the c can be recovered from $\varphi_{s,t}(c)$ by the map $\phi_{s,t}$, hence the Gray map $\varphi_{s,t}$ is bijection.

The Gray map can be extended to $\Re^n$ in a natural way: $\varphi_{s,t}:\Re^n \to R^{2n}$

$$\begin{aligned}
&\left(c_0,c_1,\cdots,c_{n-1}\right)\to\left(ta_0+sb_0,\cdots,ta_{n-1}+sb_{n-1},\right.\\
&\left.(t+2s)a_0-sb_0,\cdots,(t+2s)a_{n-1}-sb_{n-1}\right)
\end{aligned}$$

It is obvious that for any $k_1,k_2 \in R, x,y \in \Re^n$, we have $\varphi_{s,t}(k_1x+k_2y)=k_1\varphi_{s,t}(x)+k_2\varphi_{s,t}(y)$ which means the Gray map $\varphi_{s,t}$ is *R*-linear.

Lemma 3.2. Let τ denote the $(1+2v)$-constacyclic shift of $\Re^n$ and σ denote the cyclic shift of R^{2n}. Let $\varphi_{s,t}$ be the Gray map of $\Re^n \to R^{2n}$, then $\varphi_{s,t}\tau=\sigma\varphi_{s,t}$.

Proof. Let $c=(c_0,c_1,\cdots c_{n-1})\in\Re^n$, where $c_i=a_i+b_i$ with $a_i,b_i\in R$ for $0\le i\le n-1$. From the definition of the Gray map, we have

$$\begin{aligned}
&\varphi_{s,t}(c)=\left(ta_0+sb_0,\cdots,ta_{n-1}+sb_{n-1},\right.\\
&\left.(t+2s)a_0-sb_0,\cdots,(t+2s)a_{n-1}-sb_{n-1}\right)
\end{aligned}$$

hence,

$$\begin{aligned}
&\sigma\left(\varphi_{s,t}(c)\right)=\left((t+2s)a_{n-1}-sb_{n-1},ta_0\right.\\
&\left.+sb_0,\cdots,ta_{n-1}+sb_{n-1},\cdots,(t+2s)a_{n-2}-sb_{n-2}\right).
\end{aligned}$$

On the other hand,

$$\begin{aligned}
\tau(c)&=\left((1+2v)c_{n-1},c_0,\cdots,c_{n-2}\right)\\
&=\left(a_{n-1}+\left(2a_{n-1}-b_{n-1}\right)v,a_0+b_0v,\cdots,a_{n-2}+b_{n-2}v\right)
\end{aligned}$$

We can deduce that

$$\begin{aligned}
\varphi_{s,t}\left(\tau(c)\right)&=\left((t+2s)a_{n-1}-sb_{n-1},ta_0+sb_0,\cdots,\right.\\
&\quad\left.ta_{n-1}+sb_{n-1},\cdots,(t+2s)a_{n-2}-sb_{n-2}\right)
\end{aligned}$$

Therefore, $\varphi_{s,t}\tau=\sigma\varphi_{s,t}$.

Theorem 3.1. A linear code C of length *n* over $\Re$ is a $(1+2v)$-constacyclic code if and only if $\varphi_{s,t}(C)$ is a cyclic code of length 2*n* over *R*.

Proof. It is an immediately consequence of Lemma 3.2.

Now we define a Gray weight for codes over R as follows.

Definition 3.1. The gray weight on $\Re$ is a weight function on R defined as

$$W_{s,t}:\Re\to N$$

$$W_{s,t}(a+bv)=\begin{cases}0: & \text{if}\quad a=0,b=0\\ 1: & \text{if}\quad ta+sb=0,(t+2s)a-sb\ne0\\ 1 & \text{if}\quad ta+sb\ne0,(t+2s)a-sb=0\\ 2 & \text{if}\quad ta+sb\ne0,(t+2s)a-sb\ne0\end{cases}$$

Define the gray weight of a codeword $c=(c_0,\ c_1,\cdots\ c_{n-1})\in\Re^n$ to be the rational sum of the Gray weights of its components, *i.e.* $W_{s,t}(c)=\sum_{i=0}^{n-1}W_{s,t}(c_i)$. The Gray distance $d_{s,t}$ is given by $d_{s,t}(c_1,c_2)=W_{s,t}(c_1-c_2)$. The minimum Gray distance of C is the smallest nonzero Gray distance between all pairs of distinct codeword of C. The minimum Gray weight of C is the smallest nonzero Gray weight among all codeword of C. If C is linear, the minimum Gray distance of C is the same as the minimum Gray weight of C. The Hamming weight $W(c)$ of a codeword c is the number of nonzero components in c. The Hamming distance $d_{s,t}(c_1,c_2)$ between two codeword (c_1 and c_2) is the Hamming weight of the codeword (c_1-c_2). The minimum Hamming distance d of C is define as min $\left\{d(c_1,c_2)\middle|c_1,c_2\in C,c_1\ne c_2\right\}$ (cf.[7]). It is obviously that for any codeword c of C, we have $W_{s,t}(c)=W\left(\varphi_{s,t}(c)\right)$.

Lemma 3.3. The gray map $\varphi_{s,t}$ is a distance-preserving map from ($\Re^n$, Gray distance) to (R^{2n}, Hamming distance).

Proof. Let $x=a_x+b_xv; y=a_y+b_yv$. From the definition of $\varphi_{s,t}$, we have

$$\begin{aligned}
&\varphi_{s,t}(x-y)\\
&=\varphi_{s,t}\left(a_x-a_y+\left(b_x-b_y\right)v\right)\\
&=\left(t\left(a_x-a_y\right)+s\left(b_x-b_y\right),(t+2s)\left(a_x-a_y\right)-s\left(b_x-b_y\right)\right)\\
&\left(ta_x+sb_x,(t+2s)a_x-sb_x\right)-\left(ta_y+sb_y,(t+2s)a_y-sb_y\right)\\
&=\varphi_{s,t}(x)-\varphi_{s,t}(y).
\end{aligned}$$

for any $x,y\in\Re^n$. Then

$$\begin{aligned}
d_{s,t}(x,y)&=W_{s,t}(x-y)=W\left(\varphi_{s,t}(x-y)\right)\\
&=W\left(\varphi_{s,t}(x)-\varphi_{s,t}(y)\right)=d\left(\varphi_{s,t}(x),\varphi_{s,t}(y)\right).
\end{aligned}$$

Corollary 3.1. The Gray image of a $(1+2v)$-constacyclic code of length *n* over $\Re$ under the Gray map is a distance invariant linear cyclic code of length 2*n* over *R*.

4. (1 + 2*v*)-Constacyclic Codes of Length *n* over $\Re$ and Their Gray Images

In this section, we study (1 + 2*v*)-constacyclic codes of length *n* over $\Re$ and their Gray images, where *n* is a positive integer which is not divisible by *p*, the characteristic of the residue field $R/\langle\lambda\rangle$. Two ideals m_1, m_2 of a ring *R* is called relatively prime if $m_1 + m_2 = R$.

Lemma 4.1. ([8], Theorem 1.3). Let $m_1, m_2, \cdots, m_n$ be ideals of a ring *R*, The following are equivalent:

1) For $i \neq j$ m_i and m_j are relatively prime;

2) The canonical homomorphism $R \to \oplus_{i=1}^{n} R/m_i$ is surjective.

Let $m = \bigcap_{i=1}^{n} m_i$, then the canonical homomorphism $R/m \to \oplus_{i=1}^{n} R/m_i$ is bijective.

A finite family $(a_i)_{i=1}^{k}$ of ideals of a commutative *R*, such that the canonical homomorphism of *R* to $\oplus_{i=1}^{k} R/a_i$ is an isomorphism is called a direct decomposition of *R*. The next lemma is well-known.

Lemma 4.2. let R be a commutative ring, $(a_i)_{i=1}^{k}$ a direct decomposition of *R* and *M* an *R*-module. With the notation we have:

1) There exists a family $(e_i)_{i=1}^{k}$ of idempotents of *R* such that $e_i e_j = 0$ for $i \neq j$. $\sum_{i=1}^{k} e_i = 1$ and $a_i = R(1 - e_i)$ for $i = 1,\ 2, \cdots,\ k$.

2) For $i = 1, 2, \cdots, k$, the submodule $M_i = e_i M$ is a complement in M of the submodule $a_i M = (1 - e_i) M$ so the R/a_i—modules M_i and $M/a_i M$ are isomorphic via the map

$$\psi_i : M_i \to M/a_i M\,,\ x \to x + a_i M$$

3) Every submodule *N* of *M* is an internal direct sum of submodules of $N_i = e_i N \in M_i$, which are isomorphic via ψ_i with the submodules $N_i' = (a_i M + e_i N)/a_i M$ of $M/a_i M$ ($i = 1, 2, \cdots, k$). Each N' is isomorphic to $N/a_i N$. Conversely, if for every $i = 1, 2, \cdots, k$, N_i' is a submodule of $M/a_i M$, then there is a unique submodule N of M, such that N is isomorphic with $\oplus_{i=1}^{k} N_i'$. Let $c = (c_0, c_1, \cdots c_n) \in \Re^n$, where $c_i = r_i v + g_i(1 + v)$, $0 \leq i \leq n - 1$. Denote $c_v = (r_1, r_2, \cdots r_{n-1})$, $c_{1+v} = (g_1, g_2, \cdots, g_{n-1})$. Let C be a (1 + 2*v*)-constacyclic codes of length *n* over $\Re$. Since $1 + v + (-v) = 1$, and $(1+v)^2 = 1 + v$, $(-v)^2 = -v$ then by Lemma 4.2, as a $\Re$-submodule of $\Re^n$, $C \cong vC \oplus (1+v)C$, where $vC = \{vc \mid c \in C\}, (1+v)C = \{(1+v)c \mid c \in C\}$. If we denote $C_v = \{c_v \mid c \in C\}, C_{1+v} = \{c_{1+v} \mid c \in C\}$, then it is obviously that $C_v \cong vC, C_{1+v} \cong (1+v)C$, hence $C \cong C_v \oplus C_{1+v}$.

Theorem 4.1. Let C be a linear codes of length *n* over $\Re$. Then C is a (1 + 2*v*)-constacyclic code of length *n* over $\Re$ if and only if C_v and C_{1+v} are negacyclic and cyclic codes of length *n* over *R* respectively.

Proof. Let $c = (c_0, c_1, \cdots, c_{n-1}) \in C \subseteq \Re^n$, where $c_i = r_i v + g_i(1+v)$, $r_i, g_i \in R$, $0 \leq i \leq n-1$. Then $c_v = (r_1, r_2, \cdots r_{n-1})$, $c_{1+v} = (g_1, g_2, \cdots, g_{n-1})$. By the definition of the μ-constacyclic shift τ_μ, we have $\tau_{(1+2v)}(c) = (-r_{n-1}v + g_{n-1}(1+v), c_0, \cdots, c_{n-2})$, then

$$\left(\tau_{(1+2v)}(c)\right)_v = (-r_{n-1}, r_0, \cdots, r_{n-2})$$

and $\left(\tau_{(1+2v)}(c)\right)_{1+v} = (g_{n-1}, g_0, \cdots, g_{n-2})$.

That means, if C is a (1 + 2*v*)-constacyclic codes of length *n* over $\Re$, then C_v and C_{1+v} are negacyclic and cyclic codes of length *n* over *R* respectively. On the other hand, if $\tau_\mu(c_v) = \tau_{-1}(c_v), \tau_\mu(c_{1+v}) = \tau_1(c_{1+v})$, then

$$\tau_\mu(c) = (-r_{n-1}v + g_{n-1}(1+v), c_0, \cdots, c_{n-2})$$
$$= ((1 = 2v)c_{n-1}, c_0, \cdots, c_{n-2}) = \tau_{(1+2v)}(c),$$

that means, if C_v and C_{1+v} are negacyclic and cyclic codes of length *n* over *R* respectively, then C is a (1 + 2*v*)-constacyclic codes of length *n* over $\Re$.

Theorem 4.2. Let C be a (1 + 2*v*)-constacyclic code of length *n* over $\Re$, then there are polynomials $F = F_1 + \lambda F_2 + \cdots \lambda^{e-1} F_e$ and $G = G_1 + \lambda G_2 + \cdots \lambda^{e-1} G_e$ over *R* such that $C = \langle vG, (1+v)F \rangle$, where $F_0, F_1, \cdots, F_e, G_0, G_1, \cdots, G_e$ are pairwise coprime monic polynomials over *R*, such that $F_0 F_1 \cdots F_e = x^n - 1$, $G_0 G_1 \cdots G_e = x^n + 1$.

Proof. Since C is a (1 + 2*v*)-constacyclic code of length *n* over $\Re$, then by Theorem 4.1, C_v and C_{1+v} are negacyclic and cyclic codes of length *n* over *R* respectively, then by Lemma 2.2 and Lemma 2.5, there are polynomials $F = F_1 + \lambda F_2 + \cdots \lambda^{e-1} F_e$ and

$$G = G_1 + \lambda G_2 + \cdots \lambda^{e-1} G_e$$

over *R* such that

$$C_v = \langle G \rangle \subseteq R[x]/(x^n + 1), C_{1+v} = \langle F \rangle \subseteq R[x]/(x^n - 1)$$

where $F_0, F_1, \cdots, F_e, G_0, G_1, \cdots, G_e$ are pairwise coprime monic polynomials over *R*, such that $F_0 F_1 \cdots F_e = x^n - 1$, $G_0 G_1 \cdots G_e = x^n + 1$. For any $c \in C$, then $c_v, c_{1+v} \in C_{1+v}$, there are $k_1(x), k_2(x) \in R[x]$ such that $c_v(x) = k_1(x) G(x) \mod (x^n + 1)$, $c_{1+v}(x) = k_2(x) F(x) \mod (x^n - 1)$, that means, there are $r_1(x), r_2(x) \in R[x]$ such that

$$c_v(x) = k_1(x) G(x) + r_1(x)(x^n + 1)$$
$$c_{1+v}(x) = k_2(x) F(x) + r_2(x)(x^n - 1)$$

Since $v(x^n - (1+2v)) = v(x^n + 1)$,

$$(1+v)(x^n - (1+2v)) = (1+v)(x^n - 1),$$

then

$$\begin{aligned} c(x) &= v c_v(x) + (1+v) c_{(1+v)}(x) \\ &= v k_1(x) G(x) + v r_1(x)(x^n + 1) \\ &\quad + (1+v)\left(k_2(x) F(x) + r_2(x)(x^n - 1)\right) \\ &= v k_1(x) G(x) + (1+v) k_2 F(x) \\ &\quad + \left(v r_1(x) + (1+v) r_2(x)\right)\left(x^n - (1+2v)\right) \end{aligned}$$

hence $c(x)=vk_1(x)G(x)+(1+v)k_2F(x)$ mod $\left(x^n-(1+2v)\right)$. So

$$c(x)\in\left\langle vG,(1+v)F\right\rangle\subseteq\Re[x]/\left(x^n-(1+2v)\right).$$

On the other hand, For any

$$d(x)\in\left\langle vG,(1+v)F\right\rangle\subseteq\Re[x]/\left(x^n-(1+2v)\right),$$

then there are polynomials $k_1(x),k_2(x)\in\Re[x]$ such that $d(x)\equiv k_1(x)G(x)v+k_2(x)F(x)(1+v)$ mod $\left(x^n-(1+2v)\right)$ then there are $r_1(x),r_2(x)\in R[x]$ such that $vk_1(x)=vr_1(x)$, $(1+v)k_2(x)=(1+v)r_2(x)$, and there is $r(x)=vr_v(x)+(1+v)r_{1+v}(x)$ such that

$$\begin{aligned}d(x)&=vd_v(x)+(1+v)d_{1+v}(x)\\&=G(x)r_1(x)+(1+v)F(x)r_2(x)\\&\quad+r(x)\left(x^n-(1+2v)\right),\end{aligned}$$

then

$$vd_v(x)=v\left(G(x)r_1(x)+r_v(x)\left(x^n+1\right)\right),$$

$$(1+v)d_{1+v}(x)=(1+v)\left(F(x)r_2(x)+r_{1+v}(x)\left(x^n-1\right)\right)$$

this means $d_v(x)\in\langle G\rangle\subseteq R[x]/\left(x^n+1\right)$, and $d_{(1+v)}(x)\in\langle F\rangle\subseteq R[x]/\left(x^n-1\right)$, hence $d_v\in C_v,d_{1+v}\in C_{1+v}$ then $d\in C$, so $\left\langle vG,(1+v)F\right\rangle\subseteq C$. This gives that $C=\left\langle vG,(1+v)F\right\rangle$.

From Lemma 2.1, 2.4, and the proof of Theorem 4.2, we immediately obtain the following result.

Corollary 4.1. Let $C=\left\langle vG,(1+v)F\right\rangle$ be a (1 + 2*v*)-constacyclic codes of length n over $\Re$, then

$$|C|=\left|R/\langle\lambda\rangle\right|^{\sum_{i=0}^{e-1}(e-i)\left(\deg G_{i+1}+\deg F_{i+1}\right)}.$$

Theorem 4.3. Let C be a (1 + 2*v*)-constacyclic code of length *n* over $\Re$, then there is a polynomial $f(x)$ over $\Re$ such that $C=\left\langle f(x)\right\rangle$.

Proof. By Theorem 4.2, there are polynomials

$$F=F_1+\lambda F_2+\cdots+\lambda^{e-1}F_e$$

and $G=G_1+\lambda G_2+\cdots+\lambda^{e-1}G_e$ over *R* such that

$$C=\left\langle vG,(1+v)F\right\rangle,$$

where $F_0,F_1,\cdots,F_e,G_0,G_1,\cdots,G_e$ are pairwise coprime monic polynomials over *R*, such that $F_0F_1\cdots F_e=x^n-1$, $G_0G_1\cdots G_e=x^n+1$.

Let $f(x)=vG(x)+(1+v)F(x)$, obviously,

$$\left\langle f(x)\right\rangle\subseteq C.$$

Note that $vf(x)=-vG(x)$, $(1+v)f(x)=(1+v)F(x)$, then hence $C=\left\langle f(x)\right\rangle$.

We now give the definition of polynomial Gray map over $\Re$. For any polynomial $c(x)\in\Re[x]$ with degree less then *n* can be represented as $c(x)+vb(x)$, where $a(x),b(x)\in R[x]$ and their degrees are less than *n*. Define the polynomial Gray map as follows:

$$\varphi_{F,s,t}:\Re[x]/\left(x^n-(1+2v)\right)\to R[x]/\left(x^{2n}-1\right)$$

$$\varphi_{F,s,t}\left(c(x)\right)=ta(x)+sb(x)+x^n\left((t+2s)a(x)-sb(x)\right)$$

It is obviously that $\varphi_{F,s,t}\left(c(x)\right)$ is the polynomial representation of $\varphi_{s,t}(c)$.

Theorem 4.4. Let $C=\left\langle vG,(1+v)F\right\rangle$ be a (1 + 2*v*)-constacyclic code of length *n* over $\Re$, where

$$F=F_1+\lambda F_2+\cdots+\lambda^{e-1}F_e$$

and

$$G=G_1+\lambda G_2+\cdots+\lambda^{e-1}G_e$$

are polynomials over *R*, $F_0,F_1,\cdots,F_e,G_0,G_1,\cdots,G_e$ are pairwise coprime monic polynomials over *R*, such that $F_0F_1\cdots F_e=x^n-1$, $G_0G_1\cdots G_e=x^n+1$.

If $s(t+s)\neq 0$, then $\varphi_{F,s,t}\left(C(x)\right)=\left\langle g(x)\right\rangle$, where

$$g(x)=\widehat{F_1G_1}+\lambda\widehat{F_2G_2}+\cdots+\lambda^{e-1}\widehat{F_eG_e}.$$

Proof. By Lemma 4.3, we know that $C=\left\langle f(x)\right\rangle$, where $f(x)=vG(x)+(1+v)F(x)$. Let $c(x)=f(x)r(x)$ be any element in C, where $r(x)$ can be written as $r(x)=vr_1(x)+(1+v)r_2(x)$, $r_1(x),r_2(x)\in R[x]$, it is obviously that $c(x)=vG(x)r_1(x)+(1+v)F(x)r_2(x)$. Then we have

$$\begin{aligned}&\varphi_{F,s,t}\left(c(x)\right)\\&=tF(x)r_2(x)+s\left(G(x)r_1(x)+F(x)r_2(x)\right)\\&\quad+x^n(t+2s)\left(F(x)r_2(x)-s\left(G(x)r_1(x)+F(x)r_2(x)\right)\right)\\&=(t+s)r_2(x)\left(\hat{F}_1+\lambda\hat{F}_2+\cdots+\lambda^{e-1}\hat{F}_e\right)\left(x^n+1\right)\\&\quad-sr_1(x)\left(\tilde{G}_1(x)+\lambda\tilde{G}_2(x)+\cdots+\lambda^{e-1}\tilde{G}_e(x)\right)\left(x^n-1\right)\\&=(t+s)r_2(x)\left(\widehat{F_1}+\lambda\widehat{F_2}+\cdots+\lambda^{e-1}\widehat{F_e}\right)\\&\quad-sr_1(x)\left(\widehat{G_1}(x)+\lambda\widehat{G_2}(x)+\cdots+\lambda^{e-1}\widehat{G_e}(x)\right)\\&=(t+s)r_2(x)\left(\widehat{F_1G_1}G_1+\lambda\widehat{F_2G_2}G_2+\cdots+\lambda^{e-1}\widehat{F_eG_e}G_e\right)\\&\quad-sr_1(x)\left(\widehat{F_1G_1}(x)F_1+\lambda\widehat{F_2G_2}F_2(x)+\cdots\right.\\&\quad\left.+\lambda^{e-1}\widehat{F_eG_e}F_e(x)\right)\\&\in\left\langle\widehat{F_1G_1},\lambda\widehat{F_2G_2},\cdots,\lambda^{e-1}\widehat{F_eG_e}\right\rangle=\left\langle g(x)\right\rangle.\end{aligned}$$

On the other hand, by Lemma 2.1, Lemma 2.5, Lemma 3.1 and Corollary 4.1, we know that

$$\left|\varphi_{F,s,t}(C)\right|=|C|=\left|R/\langle\lambda\rangle\right|^{\sum_{i=0}^{e-1}(e-i)\left(\deg G_{i+1}+\deg F_{i+1}\right)},$$

$$\left|\left\langle g(x)\right\rangle\right| = \left|R/\langle\lambda\rangle\right|^{\sum_{i=0}^{e-1}(e-i)\left(\deg G_{i+1}+\deg F_{i+1}\right)}$$

Hence,

$$\varphi_{F,s,t}(C) = \left\langle g(x)\right\rangle$$

We now study the dual codes of a (1 + 2v)-constacyclic code of length n over $\mathfrak{R}$.

Since $(1 + 2v)^2 = 1$, then the dual of a (1 + 2v)-constacyclic code is also a (1 + 2v)-constacyclic code. We have following result similar to Theorem 3.2 in [7].

Theorem 4.5. Assume the notation as Theorem 4.1. Let C be a (1 + 2v)-constacyclic code of length n over $\mathfrak{R}$, Then $C^{\perp} = vC_v^{\perp} + (1+v)C_{1+v}^{\perp}$.

By Theorem 4.5, Lemma 2.3 and Lemma 2.6, It is obviously that the above results of (1 + 2v)-constacyclic code can be carried over respectively to their dual codes. We list them here for the sake of completeness.

Corollary 4.2. Let $C = \left\langle vG(x),(1+v)F(x)\right\rangle$ be a (1 + 2v)-constacyclic codes of length n over $\mathfrak{R}$, and $F(x), G(x)$ are generator polynomials of C_v and C_{1+v} respectively. Where $F = F_1 + \lambda F_2 + \cdots + \lambda^{e-1}F_e$ and $G = G_1 + \lambda G_2 + \cdots + \lambda^{e-1}G_e$ are polynomials over R, $F_0, F_1, \cdots, F_e, G_0, G_1, \cdots, G$ are pairwise coprime monic polynomials over R, such that $F_0F_1\cdots F_e = x^n - 1_e$, $G_0G_1\cdots G_e = x^n + 1$.

Let

$$h_2^* = \widehat{F_0^*} + \lambda\widehat{F_e^*} + \cdots + \lambda^{e-1}\widehat{F_2^*},$$

$$h_1^* = \widehat{G_0^*} + \lambda\widehat{G_e^*} + \cdots + \lambda^{e-1}\widehat{G_2^*},$$

$$g^* = \overline{F_0^*G_0^*} + \lambda\overline{F_e^*G_e^*} + \cdots + \lambda^{e-1}\overline{F_2^*G_2^*}.$$

Then

1) $C^{\perp} = \left\langle vh_1^*(x),(1+v)h_2^*(x)\right\rangle$.

2) $C^{\perp} = \left\langle h(x)\right\rangle$ where $h(x) = vh_1^*(x) + (1+v)h_2^*(x)$.

3) $\varphi\left(C^{\perp}\right) = \left\langle g^*(x)\right\rangle$.

4) $\varphi\left(C^{\perp}\right) = \left(\varphi(C)\right)^{\perp}$.

5. Conclusion

In this paper, we establish the structure of (1 + 2v)-constacyclic codes of length n over $\mathfrak{R}$ and classified Gray maps from (1 + 2v)-constacyclic codes of length n over $\mathfrak{R}$ to R^{2n}, prove that the image of a (1 + 2v)-constacyclic codes of length n over $R + vR$ under the Gray map is a distance-invariant linear cyclic code of length 2n over R, where R is a finite chain ring. The generator polynomial of this kind of codes of length n are determined and their dual codes are also discussed.

REFERENCES

[1] J. Wolfmann, "Negacyclic and Cyclic Codes over Z_4," *IEEE Transactions on Information Theory*, Vol. 45, No. 7, 1999, pp. 2527-2532. doi:10.1109/18.296397

[2] H. Tapia-Recillas and G. Vega, "Some Constacyclic Codes over Z2k and Binary Quasi-Cyclic Codes," *Discrete Applied Mathematics*, Vol. 128, No. 1, 2002, pp. 305-316. doi:10.1016/S0166-218X(02)00453-5

[3] H. Q. Dinh and S. R. López-Permouth, "Cyclic and Negacyclic Codes over Finite Chain Rings," *I IEEE Transactions on Information Theory*, Vol. 50, No. 8, 2004, pp. 1728-1744. d oi:10.1109/TIT.2004.831789

[4] H. Q. Dinh, "Negacyclic Codes of Length 2^s over Galois Rings," *IEEE Transactions on Information Theory*, Vol. 51, No. 12, 2005, pp. 4252-4262. doi:10.1109/TIT.2005.859284

[5] B. Yildiz and S. Karadenniz, "Linear Codes over $F_2 + uF_2 + vF_2 + uvF_2$," *Designs, Codes and Cryptography*, Vol. 54, No. 1, 2010, pp. 61-81.

[6] S. X. Zhu, Y. Wang and M. Shi, "Some Results on Cyclic Codes over $F_2 + vF_2$," *IEEE Transactions on Information Theory*, Vol. 56, No. 4, 2010, pp. 1680-1684. doi:10.1109/TIT.2010.2040896

[7] S. X. Zhu and L. Wang, "A Class of Constacyclic Codes over $F_p + vF_p$ and Its Gray Image," *Discrete Mathematics*, Vol. 311, No. 9, 2011, pp. 2677-2682. doi:10.1016/j.disc.2011.08.015

[8] H. Matsumura, "Commutative Ring with Identity," Cambridge University Press, Cambridge, 1989.