Self-dual cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$

Leilei Gao
Department of Mathematics , School of Mathematics and Statistics,
Shandong University of Technology, Zibo , China.
E-mail address: gaoleileixzc@163.com

ABSTRACT

In this work, we describe the algebraic structure of self-dual cyclic codes over the ring $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, where $u^2=0$, $v^2=0$ and $uv=vu$. We provide a necessary and sufficient condition for the existence of self-dual cyclic codes of odd length n over the ring $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$. Further, by the Gray map, we construct self-dual codes over the ring $\mathbb{F}_2+u\mathbb{F}_2$.

Keywords: *Self-dual cyclic codes Gray map self-dual codes.*

1. Introduction

Codes over finite rings have been studied since the early 1970s. There are a lot of works on codes over finite rings after the discovery that certain the hidden linear structures behind well-known nonlinear codes such as Kerdock and Preparata codes as the Gray images of linear codes over $\mathbb{Z}_4$ [2].

Rings of order 16 are of importance in many areas. For example, the smallest local finite Frobenius commutative non-chain ring is of order 16 [8]. Recently, there are some works on linear codes over the ring $\mathbb{Z}_4+u\mathbb{Z}_4$, one of 16 elements rings, such as [9, 13, 6, 7]. In [6], the MacWilliams identities of linear codes and constructing formally self-dual codes over $\mathbb{Z}_4+u\mathbb{Z}_4$ are discussed. Later, some structural properties of cyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$ and constructing new $\mathbb{Z}_4$-linear codes are considered in [7]. Recently, Luo and Parampalli introduce algebraic structures of self-dual cyclic codes of odd length n over $\mathbb{Z}_4+u\mathbb{Z}_4$ and provide a necessary and sufficient condition for the existence of self-dual cyclic codes of odd length [9].

The ring $\Delta=\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, where $u^2=0$, $v^2=0$ and $uv=vu$, is another 16 elements ring. Recently, there are also some works on linear codes over this ring, such as [10, 3, 4, 5]. To the best of our knowledge, there have no any research on self-dual cyclic codes over Δ. We will do this issue in this paper.

The paper is organized as follows. In Section 2, we recall some results on the ring Δ. In Section 3, we consider some structural properties of cyclic codes over Δ. Then we describe the structures of self-dual cyclic codes and provide a necessary and sufficient condition for the existence of self-dual cyclic codes of odd length over Δ. In Section 4, by the Gray map, some examples of constructing self-dual codes over the ring $\Lambda=\mathbb{F}_2+u\mathbb{F}_2$ are given.

2. Preliminaries

Let $\Delta=\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, where $u^2=v^2=0$ and $uv=vu$. Then Δ is a commutative ring with 16 elements and characteristic 2. Any element of Δ can be expressed uniquely as $a+bu+cv+duv$, where $a,b,c,d\in\mathbb{F}_2$. There are 5 different nontrivial ideals of Δ (see [4]), which are described as follows

$$I_{uv}=\langle uv\rangle=\{0,uv\},$$

$$I_u=\langle u\rangle=\{0,u,uv,u+uv\},$$

$$I_v=\langle v\rangle=\{0,v,uv,v+uv\},$$

$$I_{u+v}=\langle u+v\rangle=\{0,u+v,uv,u+v+uv\},$$

$$I_{u,v}=\langle u,v\rangle=\{0,u,v,u+v,uv,u+uv,v+uv,u+v+uv\}.$$

Obviously, the ring Δ is not a finite chain ring. Observe that $I_{u,v}$ is the unique maximal ideal of Δ. Therefore, the local ring Δ is not principle either. Further, Δ is a local Frobenius ring [8].

Let $\Lambda=\mathbb{F}_2+u\mathbb{F}_2$, where $u^2=0$. Now we define the Gray map θ from Δ to Λ as follows

$$\begin{aligned}\theta:\Delta &\longrightarrow \Lambda\\ p+qv &\longmapsto (q,p+q),\end{aligned}$$

where $p,q\in\Lambda$. It is well known that the Lee weights of elements in Λ are defined as $w_L(0)=0$, $w_L(1)=1$, $w_L(u)=2$, $w_L(1+u)=1$. For any $\alpha=p+qv\in\Delta$, its Gray weight is defined as

$$w_G(\alpha)=w_L(q)+w_L(p+q),$$

where $p,q\in\Lambda$.

Define a Gray weight of a vector $c=(c_0,c_1,\dots,c_{n-1})\in\Delta^n$ to be the rational sum of the Gray weight of its component, i.e.

$$w_G(c)=w_G(c_0)+w_G(c_1)+\cdots+w_G(c_{n-1}).$$

For any elements $c_1,c_2\in\Delta^n$, the Gray distance is given by $d_G(c_1,c_2)=w_G(c_1-c_2)$. A code C of length n over Δ is a subset of Δ^n. C is a linear code if and only if C is an Δ-submodule of Δ^n. The minimum Gray distance of C is the smallest nonzero Gray distance between all pairs of distinct codewords. The minimum Gray weight of C is the smallest nonzero Gray weight among all codewords. If C is a linear code, then the minimum Gray distance is the same as the minimum Gray weight.

Now we extend the Gray map Θ to Δ^n as follows

$$\begin{aligned}\Theta:\Delta^n &\longrightarrow \Lambda^{2n}\\ (c_0,c_1,\dots,c_{n-1}) &\longmapsto (q_0,p_0+q_0,\dots,q_{n-1},p_{n-1}+q_{n-1}),\end{aligned}$$

where $c_i=p_i+q_iv, i=0,1,\dots,n-1$. The Gray map Θ is a distance-preserving map from Δ^n (Gray distance)to Λ^{2n} (Lee distance) and it is also Λ-linear.

Proof. For any $c_1,c_2\in\Delta^n$ and $k_1,k_2\in\Lambda$, we have $\Theta(k_1c_1+k_2c_2)=k_1\Theta(c_1)+k_2\Theta(c_2)$, which implies that Θ is Λ-linear. Let $c_1=(c_{1,0},c_{1,1},\dots,c_{1,n-1})$ and $c_2=(c_{2,0},c_{2,1},\dots,c_{2,n-1})$ be elements of Δ^n, where $c_{i,j}=p_{i,j}+q_{i,j}v, i=1,2, j=0,1,\dots,n-1$. Then $c_1-c_2=(c_{1,0}-c_{2,0},\dots,c_{1,n-1}-c_{2,n-1})$ and $\Theta(c_1-c_2)=\Theta(c_1)-\Theta(c_2)$. Therefore, $d_G(c_1,c_2)=w_G(c_1-c_2)=w_L(\Theta(c_1)-\Theta(c_2))=d_L(\Theta(c_1),\Theta(c_2))$. The second equality holds because of the definition is the Gray weight of the element in Λ.

Let C be a (n,M,d) linear code over Δ, where n,M,d are respectively the length, the number of the codewords and the minimum Gray distance of C. Then $\Theta(C)$ is a $(2n,M,d)$ linear code over Δ.

Proof. According to Proposition 1, we know that Θ is Λ-linear, which implies that $\Theta(C)$ is a Λ-linear code. From the definition of the Gray map Θ, $\Theta(C)$ is with length $2n$. Moreover, Θ is a bijective map from Δ^n to Λ^{2n} implying that $\Theta(C)$ has M codewords. At last, the preserving distance of Θ leads to $\Theta(C)$ has the minimum Lee distance d.

3. Structure of self-dual cyclic codes

Cyclic codes over the ring Δ are defined in a natural way. Let C be a linear code of length n over the ring Δ. If for any codeword $c=(c_0,c_1,\dots,c_{n-1})\in C$, the vector $(c_{n-1},c_0,c_1,\dots,c_{n-2})$ is also in C, then the code C is called a cyclic code over the ring Δ.

Let $R=\frac{\Delta[x]}{\langle x^n-1\rangle}$. We present any vector $(c_0,c_1,\dots,c_{n-1})\in\Delta^n$ by the residue class of the polynomial $c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ of R. Then we have a Δ-module isomorphism φ as follows

$$\begin{aligned}\varphi:\Delta^n &\longrightarrow R\\ (a_0,a_1,\dots,a_{n-1}) &\longmapsto a_0+a_1x+\cdots+a_{n-1}x^{n-1}+\langle x^n-1\rangle.\end{aligned}$$

It is easy to see that a linear code C of length n is a cyclic code over Δ if and only if $\varphi(C)$ is an ideal of R. In this paper, we identity cyclic codes over Δ with ideals of R.

Let $f(x)$ be a basic irreducible polynomial in $\Lambda[x]$ and $R_f=\frac{\Lambda[x]}{\langle f(x)\rangle}$. Then R_f is a chain ring. Further, its ideals can be given similarly to that of $\mathbb{Z}_4$ as follows. [1] $f(x)$ is a basic irreducible polynomial in $\Lambda[x]$, then the only ideals of R_f are 0, R_f and uR_f. Let $f(x)$ be a basic irreducible polynomial in $\Lambda[x]$ and $g(x)$ be a non-zero polynomial in R_f, then $g(x)$ is either a unit in the ring R_f or an element of uR_f.

Proof. Let ϕ be a map from $\Lambda[x]$ to $\mathbb{F}_2[x]$ which sends 0, u to 0; 1, $1+u$ to 1 and x to x. Since $f(x)$ is a basic irreducible polynomial in $\Lambda[x]$, then we can obtain $\gcd(\phi(g(x)),\phi(f(x)))=1 or \phi(f(x))$.

Case 1. $\gcd(\phi(g(x)),\phi(f(x)))=1$. This means that $\phi(g(x))$ and $\phi(f(x))$ are coprime in $\mathbb{F}_2[x]$. Then there exist polynomial $\lambda_1(x)$ and $\lambda_2(x)$ in $\Lambda[x]$ such that

$$\phi(\lambda_1(x))\phi(g(x))+\phi(\lambda_2(x))\phi(f(x))=1.$$

Thus

$$\lambda_1(x)g(x)+\lambda_2(x)f(x)=1+uk(x),$$

where $k(x)\in\Lambda[x]$. Multiplying the above equation by $uk(x)$, we have

$$uk(x)\lambda_1(x)g(x)+uk(x)\lambda_2(x)f(x)=uk(x).$$

Then we obtain

$$(1-uk(x))\lambda_1(x)g(x)+(1-uk(x))\lambda_2(x)f(x)=1.$$

Therefore, $g(x)$ and $f(x)$ are comprime in $\Lambda[x]$. Hence, it is easy to see that $g(x)$ is a unit in the ring R_f.

Case 2. $\gcd(\phi(g(x)),\phi(f(x)))=\phi(f(x))$. Since $g(x)$ is a non-zero polynomial in R_f, then $deg(g(x))<deg(f(x))$. Since $f(x)$ is a basic irreducible polynomial, then $deg(\phi(g(x)))<deg\phi((f(x)))$. This means that $\phi(g(x))=0$. So we can attain that $g(x)$ is an element of uR_f.

If $f(x)$ is a basic irreducible polynomial in $\Lambda[x]$, then the only ideals of R are the elements in $S=\{0,vR_f,uvR_f,R_f+vR_f,uR_f+vR_f,uR_f+uvR_f,(u+v\sum_{i\in A}x^i)R_f\}$, where A is a subset of $\{0,1,\dots,n-1\}$.

Proof. Let I be an arbitrary nontrivial ideal of $\frac{\Delta[x]}{\langle f(x)\rangle}$. If $I\subseteq vR_f$, by Lemma 1, it is easy to see that I is one of vR_f and uvR_f.

Assume that $I\nsubseteq vR_f$. Let $I_n=\{a(x)\in R_f|\exists b(x)\in R_f such that a(x)+vb(x)\in I\}$. Obviously, I_n is an ideal of the ring R_f. By Lemma 1, we have

(i) $I_n=R_f$, then there exists a polynomial $b(x)\in R_f$ such that $1+vb(x)\in I$. Therefore, $(1+vb(x))^2=1$ is in I. It follows that $I=R_f+vR_f$.

(ii) $I_n=uR_f$, then there exists an element $b(x)\in R_f$ such that $u+vb(x)\in I$, which implies that $uv=(u+vb(x))v$ is in I. So, we get $uvR_f\subseteq I$.

(ii-1) $b(x)=0$, then u is in I. Hence, $uR_f\subseteq I$. Therefore, $uR_f+uvR_f\subseteq I$. Moreover, we have

(ii-1-1) $I=uR_f+uvR_f$.

(ii-1-2) $uR_f+uvR_f\nsubseteq I$. Then there exists $\alpha(x)\in I\backslash(uR_f+uvR_f)$. Hence, there are polynomials $g(x),a(x),b(x)\in R_f$ such that $\alpha(x)=ua(x)+uvb(x)+vg(x)\in I$, which implies that $vg(x)\in I$. Observe that $\alpha(x)$ is not in uR_f+uvR_f, we get that $g(x)$ is not in uR_f. By Lemma 2, we know $g(x)$ is a unit in R_f. So there exists polynomial $h(x)$ in R_f such that $v=vg(x)h(x)\in I$. This means that $I=uR_f+vR_f$.

(ii-2) $b(x)\neq 0$, then $b(x)=\sum_{i\in A}x^i+u\sum_{j\in B}x^j$, where A,B are two subsets of $\{0,1,\dots,n-1\}$. Since $u+vb(x)=u+v(\sum_{i\in A}x^i)+uv(\sum_{j\in B}x^j)\in I$, then we can gain $u+v\sum_{i\in A}x^i\in I$. Hence, $\langle u+v\sum_{i\in A}x^i\rangle\subseteq I$.

(ii-2-1) $I=\langle u+v\sum_{i\in A}x^i\rangle=(u+v\sum_{i\in A}x^i)R_f+uvR_f$. Since $\sum_{i\in A}x^i$ is a unit in R_f and $uv=u(u+v\sum_{i\in A}x^i)(\sum_{i\in A}x^i)^{-1}$, then $I=(u+v\sum_{i\in A}x^i)R_f$.

(ii-2-2) $\langle u+v\sum_{i\in A}x^i\rangle\subsetneq I$. Then there exists $c(x)\in I\backslash\langle u+v\sum_{i\in A}x^i\rangle$. Therefore, there exist polynomials $a(x),h(x)\in R_f$ such that $vh(x)=c(x)-(u+v\sum_{i\in A}x^i)a(x)\in I$. Since $c(x)\notin\langle u+v\sum_{i\in A}x^i\rangle$, it follows that $h(x)\notin uR_f$. By Lemma 2, we have $h(x)$ is a unit in R_f, then v is in I. Let $a(x)=ua_1(x)+va_2(x)=(u+v\sum_{i\in A}x^i)a_1(x)+v(a_2(x)-a_1(x)\sum_{i\in A}x^i)\in\langle u+v\sum_{i\in A}x^i\rangle+vR_f=uR_f+vR_f$.

Let $x^n-1=f_1f_2\cdots f_m$ be a representation of as a product of basic irreducible pairwise-coprime polynomials in $\Lambda[x]$ and S_i be the set of ideals of $\frac{\Delta[x]}{\langle f_i(x)\rangle}$. Then $S_i=\{0,vR_{f_i},uvR_{f_i},R_{f_i}+vR_{f_i},uR_{f_i}+vR_{f_i},uR_f+uvR_{f_i},(u+v\sum_{i\in A}x^i)R_{f_i}\}=\{\sum(\langle u^{j_i}v^{k_i}+\langle f_i(x)\rangle\rangle)\}\cup\{\langle(u+v\sum_{j\in A}x^j)+\langle f_i(x)\rangle\rangle\}$, where $0\le j_i,k_i\le 2$, $1\le i\le m$. Let $f_1,f_2,\dots,f_m$ be a product of basic irreducible pairwise-coprime polynomials of x^n-1 in $\Lambda[x]$. Let $\hat{f}_i$ denote the polynomial $\frac{x^n-1}{f_i(x)}$. Then any ideal in R is a sum of ideals of the form $\langle u^{j_i}v^{k_i}\hat{f}_i+\langle x^n-1\rangle\rangle$ and $\langle(u+v\sum_{j\in A}x^j)\hat{f}_i+\langle x^n-1\rangle\rangle$, where $0\le j_i,k_i\le 2$, $1\le i\le m$ and A is a subset of $\{0,1,\dots,n-1\}$.

Proof. Observe that $f_i(x)$ and $\hat{f}_i(x)$ are coprime for $i=1,2,\dots,n-1$. Then there exist polynomials $b_i(x)$ and $c_i(x)$ in $\Delta[x]$ such that

$$b_i(x)\hat{f}_i(x)+c_i(x)f_i(x)=1.$$

Let $e_i(x)=b_i(x)\hat{f}_i(x)+\langle x^n-1\rangle$. By the Chinese Remainder Theorem, we have

$$R=\bigoplus_{i=1}^{m}Re_i(x)$$

and

$$Re_i(x)\cong\frac{\Delta[x]}{\langle f_i(x)\rangle},$$

for $i=1,2,\dots,n-1$. By Proposition 3, an ideal of R_{f_i} is one of the elements of S_i. Then I_i corresponds to the form $\langle u^{j_i}v^{k_i}\hat{f}_i+\langle x^n-1\rangle\rangle$ or $\langle(u+v\sum_{j\in A}x^j)\hat{f}_i+\langle x^n-1\rangle\rangle$ in $Re_i(x)$, where $0\le j_i,k_i\le 2$ and $1\le i\le m$. Therefore, I is a direct sum of ideals of the form $\langle u^{j_i}v^{k_i}\hat{f}_i+\langle x^n-1\rangle\rangle$ or $\langle(u+v\sum_{j\in A}x^j)\hat{f}_i+\langle x^n-1\rangle\rangle$ in R, where $0\le j_i,k_i\le 2$ and $1\le i\le m$.

By Proposition 4, we certify that any ideal in R is a sum of ideals of the form $\langle u^{j_i}v^{k_i}\hat{f}_i+\langle x^n-1\rangle\rangle$ and

$\langle (u+v\sum_{j\in A} x^j)\hat{f}_i + \langle x^n-1\rangle\rangle)$, where $0\le j_i,k_i\le 2$, $1\le i\le m$ and A is a subset of $\{0,1,\dots,n-1\}$. Through the analysis of the front, we know that a linear code C of length n is a cyclic code over Δ if and only if $\varphi(C)$ is an ideal of R. Therefore, we can gain the algebraic structure of cyclic codes over Δ. In order to simply the algebraic structure of cyclic codes, we need the following lemma first. Let $g_1(x),g_2(x),\dots,g_m(x)$ be monic polynomials in $\Lambda[x]$. Then we have

$$\langle g_1(x)\rangle + \langle g_2(x)\rangle + \cdots + \langle g_m(x)\rangle = \langle \mathcal{K}(x)\rangle,$$

where $\mathcal{K}(x) = \mathrm{g}cd(g_1(x),g_2(x),\dots,g_m(x))$.

Proof. Since $\mathcal{K}(x) = \mathrm{g}cd(g_1(x),g_2(x),\dots,g_m(x))$, then $\mathcal{K}(x)|g_i(x)$, for $i=1,2,\dots,m$. Hence, $\langle g_i(x)\rangle \subseteq \langle \mathcal{K}(x)\rangle$. Therefore, $\langle g_1(x)\rangle + \langle g_2(x)\rangle + \cdots + \langle g_m(x)\rangle \subseteq \langle \mathcal{K}(x)\rangle$.

Since $\mathcal{K}(x) = \mathrm{g}cd(g_1(x),g_2(x),\dots,g_m(x))$, then there have polynomials $a_1(x),\dots,a_m(x)$ in $\Lambda[x]$ such that

$$a_1(x)g_1(x) + a_2(x)g_2(x) + \cdots + a_m(x)g_m(x) = \mathcal{K}(x).$$

Therefore, $\langle \mathcal{K}(x)\rangle = \langle a_1(x)g_1(x) + a_2(x)g_2(x) + \cdots + a_m(x)g_m(x)\rangle \subseteq \langle g_1(x)\rangle + \langle g_2(x)\rangle + \cdots + \langle g_m(x)\rangle$. Hence, $\langle g_1(x)\rangle + \langle g_2(x)\rangle + \cdots + \langle g_m(x)\rangle = \langle \mathcal{K}(x)\rangle$.

Let C be a cyclic code of odd length n over Δ. Then

$$C = \langle \hat{F}_1\rangle \oplus \langle u\hat{F}_2\rangle \oplus \langle v\hat{F}_3\rangle \oplus \langle uv\hat{F}_4\rangle \oplus \langle (u+v\textstyle\sum_{j\in A} x^j)\hat{F}_5\rangle \oplus (\langle u\hat{F}_6\rangle + \langle v\hat{F}_6\rangle).$$

where A is a subset of $\{0,1,\dots,n-1\}$, $F_0,F_1,\dots,F_6$ in $\Lambda[x]$ are pairwise coprime monic polynomials and $F_0F_1\cdots F_6 = x^n-1$.

Proof. Let $f_1f_2\cdots f_m$ be a product of basic irreducible pairwise-coprime polynomials of x^n-1 in $\Lambda[x]$. By Proposition 4, C is a direct sum of ideals of the form $\langle u^{j_i}v^{k_i}\hat{f}_i\rangle$ and $\langle (u+v\sum_{j\in A} x^j)\hat{f}_i\rangle)$, where $0\le j_i,k_i\le 2$ and $1\le i\le m$. After arranging if necessary, we assume that

$$\begin{aligned} C = \ & \langle \hat{f}_{k_1+1}\rangle \oplus \cdots \oplus \langle \hat{f}_{k_1+k_2}\rangle \\ & \oplus \langle u\hat{f}_{k_1+k_2+1}\rangle \oplus \cdots \oplus \langle u\hat{f}_{k_1+k_2+k_3}\rangle \\ & \oplus \langle v\hat{f}_{k_1+k_2+k_3+1}\rangle \oplus \cdots \oplus \langle v\hat{f}_{k_1+k_2+k_3+k_4}\rangle \\ & \oplus \langle uv\hat{f}_{k_1+k_2+k_3+k_4+1}\rangle \oplus \cdots \oplus \langle uv\hat{f}_{k_1+k_2+k_3+k_4+k_5}\rangle \\ & \oplus \langle (u+v\textstyle\sum_{j\in A} x^j)\hat{f}_{k_1+k_2+k_3+k_4+k_5+1}\rangle \\ & \oplus \cdots \oplus \langle (u+v\textstyle\sum_{j\in A} x^j)\hat{f}_{k_1+k_2+k_3+k_4+k_5+k_6}\rangle \\ & \oplus \langle u\hat{f}_{k_1+k_2+k_3+k_4+k_5+k_6+1}\rangle + \langle v\hat{f}_{k_1+k_2+k_3+k_4+k_5+k_6+1}\rangle \\ & \oplus \cdots \oplus \langle u\hat{f}_m\rangle + \langle v\hat{f}_m\rangle, \end{aligned}$$

where $k_1,\dots,k_6\ge 0$ and $k_1+\cdots+k_6+1\le m$.

Then we define that

$$\begin{aligned} & F_0 = f_1\cdots f_{k_1}, F_1 = f_{k_1+1}\cdots f_{k_1+k_2}, \\ & F_2 = f_{k_1+k_2+1}\cdots f_{k_1+k_2+k_3}, F_3 = f_{k_1+k_2+k_3+1}\cdots f_{k_1+k_2+k_3+k_4}, \\ & F_4 = f_{k_1+k_2+k_3+k_4+1}\cdots f_{k_1+k_2+k_3+k_4+k_5}, \\ & F_5 = f_{k_1+k_2+k_3+k_4+k_5+1}\cdots f_{k_1+k_2+k_3+k_4+k_5+k_6}, \\ & F_6 = f_{k_1+k_2+k_3+k_4+k_5+k_6+1}\cdots f_m. \end{aligned}$$

Obviously, F_0, F_1,...,F_6 are pairwise coprime, $F_0F_1\cdots F_6 = x^n-1$.

By lemma 3, It is clear that

$$\begin{aligned} & \langle \hat{F}_1\rangle = \langle \hat{f}_{k_1+1}\rangle \oplus \cdots \oplus \langle \hat{f}_{k_1+k_2}\rangle, \langle u\hat{F}_2\rangle = \langle u\hat{f}_{k_1+k_2+1}\rangle \oplus \cdots \oplus \langle u\hat{f}_{k_1+k_2+k_3}\rangle, \\ & \langle v\hat{F}_3\rangle = \langle v\hat{f}_{k_1+k_2+k_3+1}\rangle \oplus \cdots \oplus \langle v\hat{f}_{k_1+k_2+k_3+k_4}\rangle, \\ & \langle uv\hat{F}_4\rangle = \langle uv\hat{f}_{k_1+k_2+k_3+k_4+1}\rangle \oplus \cdots \oplus \langle uv\hat{f}_{k_1+k_2+k_3+k_4+k_5}\rangle, \\ & \langle (u+v\textstyle\sum_{j\in A} x^j)\hat{F}_5\rangle = \langle (u+v\textstyle\sum_{j\in A} x^j)\hat{f}_{k_1+k_2+k_3+k_4+k_5+1}\rangle \\ & \oplus \cdots \oplus \langle (u+v\textstyle\sum_{j\in A} x^j)\hat{f}_{k_1+k_2+k_3+k_4+k_5+k_6}\rangle, \\ & \langle u\hat{F}_6\rangle + \langle v\hat{F}_6\rangle = (\langle u\hat{f}_{k_1+k_2+k_3+k_4+k_5+k_6+1}\rangle + \langle v\hat{f}_{k_1+k_2+k_3+k_4+k_5+k_6+1}\rangle) \\ & \oplus \cdots \oplus (\langle u\hat{f}_m\rangle + \langle v\hat{f}_m\rangle). \end{aligned}$$

Hence, we obtain

$$C = \langle \hat{F}_1\rangle \oplus \langle u\hat{F}_2\rangle \oplus \langle v\hat{F}_3\rangle \oplus \langle uv\hat{F}_4\rangle \oplus \langle (u+v\textstyle\sum_{j\in A} x^j)\hat{F}_5\rangle \oplus (\langle u\hat{F}_6\rangle + \langle v\hat{F}_6\rangle).$$

In the following content, we study the algebraic structure of self-dual cyclic codes of odd length n over Δ. Let $a = (a_0, a_1, \dots, a_{n-1})$, $b = (b_0, b_1, \dots, b_{n-1})$ be two vectors in Δ^n. The vectors a and b are called orthogonal if $a \cdot b = a_0 b_0 + a_1 b_1 + \cdots + a_{n-1} b_{n-1} = 0$. For a linear code C over Δ, its dual code $C^\perp = \{a \in \Delta^n | a \cdot b = 0, \forall b \in C\}$. If $C = C^\perp$, then C is called a self-dual code. If the number of codewords in any linear code C over Δ is 2^k, for some integer $k \in \{0,1, \dots, 4n\}$, then its dual code $C^\perp$ has 2^ℓ codewords, where $k + \ell = 4n$.

Let C be a cyclic code of odd length n with notation as in Theorem 1. Then $C^\perp = \langle \hat{F}_0^* \rangle \oplus \langle u\hat{F}_2^* \rangle \oplus \langle v\hat{F}_3^* \rangle \oplus (\langle u\hat{F}_4^* \rangle + \langle v\hat{F}_4^* \rangle) \oplus \langle (u + v\sum_{j \in A} x^j)\hat{F}_5^* \rangle \oplus \langle uv\hat{F}_6^* \rangle$, where F_i^* denotes the reciprocal polynomial of F_i, $i = 0,1, \dots, 6$.

Proof. Let $C^* = \langle \hat{F}_0^* \rangle \oplus \langle u\hat{F}_2^* \rangle \oplus \langle v\hat{F}_3^* \rangle \oplus (\langle u\hat{F}_4^* \rangle + \langle v\hat{F}_4^* \rangle) \oplus \langle (u + v\sum_{j \in A} x^j)\hat{F}_5^* \rangle \oplus \langle uv\hat{F}_6^* \rangle$. For $i, j \in \{0,1, \dots, 6\}$, if $i \neq j$, then $x^n - 1 | \hat{F}_i (\hat{F}_j^*)^*$. Therefore, $\hat{F}_i (\hat{F}_j^*)^* = 0$. Hence, $C^* \subseteq C^\perp$.

Since $|uv\Delta| = 2$, $|u\Delta| = |v\Delta| = |(u+v)\Delta| = 2^2$, $|u\Delta| + |v\Delta| = 2^3$ and $|\Delta| = 2^4$, let $k = 4\mathrm{d}egF_1 + 2\mathrm{d}egF_2 + 2\mathrm{d}egF_3 + \mathrm{d}egF_4 + 2\mathrm{d}egF_5 + 3\mathrm{d}egF_6$ and $\ell = 4\mathrm{d}egF_0 + 2\mathrm{d}egF_2 + 2\mathrm{d}egF_3 + 3\mathrm{d}egF_4 + 2\mathrm{d}egF_5 + \mathrm{d}egF_6$, then $|C| = 2^k$ and $|C^\perp| = 2^\ell$. Observe that $\ell + k = 4n$. Therefore, $|C^\perp| = |C^*|$. Hence, $C^\perp = C^*$.

In Theorem 1 and Theorem 2, we describe the algebraic structure of cyclic codes and their dual codes over the ring Δ. In the following, we provide a necessary and sufficient condition for the existence of self-dual cyclic codes as the main result of this paper. Let C be a cyclic code of odd length n with notation as in Theorem 2. Then C is self-dual if and only if $\langle F_0^* \rangle = \langle F_1 \rangle$, $\langle F_2^* \rangle = \langle F_2 \rangle$, $\langle F_3^* \rangle = \langle F_3 \rangle$, $\langle F_4^* \rangle = \langle F_6 \rangle$ and $\langle F_5^* \rangle = \langle F_5 \rangle$.

Proof. By checking generators of C and $C^\perp$, it is easy to see that if C is a self-dual code, then it need to meet $\langle F_0^* \rangle = \langle F_1 \rangle$, $\langle F_2^* \rangle = \langle F_2 \rangle$, $\langle F_3^* \rangle = \langle F_3 \rangle$, $\langle F_4^* \rangle = \langle F_6 \rangle$ and $\langle F_5^* \rangle = \langle F_5 \rangle$.

At the end of the paper, we will show that the Gray map images of self-dual codes over the ring Δ is also self-dual over the ring Λ. Let C be a linear code of length n over Δ. Then $\Theta(C)^\perp = \Theta(C^\perp)$. Moreover, if C is self-dual over Δ, then $\Theta(C)$ is also self-dual over Λ.

Proof. For all $c_1 = (c_{1,0}, c_{1,1}, \dots, c_{1,n-1}) \in C$ and $c_2 = (c_{2,0}, c_{2,1}, \dots, c_{2,n-1}) \in C^\perp$, where $c_{i,j} = p_{i,j} + q_{i,j}v$, $p_{i,j}, q_{i,j} \in \Lambda$, $i = 1,2$ and $j = 0,1, \dots, n-1$. Since $c_1 \cdot c_2 = 0$, then we have $\sum_{j=0}^{n-1} c_{1,j}c_{2,j} = \sum_{j=0}^{n-1} p_{1,j}p_{2,j} + \sum_{j=0}^{n-1} (p_{1,j}q_{2,j} + p_{2,j}q_{1,j})v = 0$ implying $\sum_{j=0}^{n-1} p_{1,j}p_{2,j} = 0$ and $\sum_{j=0}^{n-1} (p_{1,j}q_{2,j} + p_{2,j}q_{1,j}) = 0$. Therefore, $\Theta(c_1) \cdot \Theta(c_2) = \sum_{j=0}^{n-1} (p_{1,j}p_{2,j} + p_{1,j}q_{2,j} + p_{2,j}q_{1,j}) = 0$. Thus, $\Theta(C)^\perp \subseteq \Theta(C)^\perp$. From Proposition 2, we have $|\Theta(C)^\perp| = |\Theta(C)^\perp|$, which implies that $\Theta(C)^\perp = \Theta(C^\perp)$. Clearly, $\Theta(C)$ is self-orthogonal if C is self-dual. Since $|\Theta(C)| = |C|$, then $\Theta(C)$ is self-dual.

4. Example

In this section, we show some examples of self-dual cyclic codes of odd length n over Δ applying Theorem 3. Moreover, by Proposition 5, we can construct some self-dual codes of length $2n$ over Λ. We compute the minimum distance of the codes below by the computational algebra system Magma [12]. Let $n = 5$. Then

$$x^5 - 1 = (1 + x)(1 + x + x^2 + x^3 + x^4)$$

over Λ. Suppose that $F_2 = 1 + x$ and $F_3 = 1 + x + x^2 + x^3 + x^4$, where $\langle F_2^* \rangle = \langle F_2 \rangle$ and $\langle F_3 \rangle = \langle F_3^* \rangle$. Let $C = \langle u(1 + x + x^2 + x^3 + x^4), v(1 + x) \rangle$. By Theorem 3, C is a self-dual cyclic code of length 5 over Δ with parameter $(5, 4^4 2^2, 4)$. By and Proposition 2 and Proposition 5, we know $\Theta(C)$ is a self-dual code over Λ with parameter $(10, 2^{10}, 4)$. This code is optimal [11]. Let $n = 7$. Then $x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3) = f_1 f_2 f_3$ over Λ and $\langle f_1^* \rangle = \langle f_1 \rangle$, $\langle f_2^* \rangle = \langle f_3 \rangle$, $\langle f_3^* \rangle = \langle f_2 \rangle$. By Theorem 3, some self-dual cyclic codes of length 14 over Λ are obtained in Table 1.

Table 1: Self-dual cyclic codes of length 14 over Λ.

Generators	d_C	$\Theta(C)$
$\langle f_1f_2, uf_2f_3\rangle$	4	$(14, 4^7, 4)$
$\langle f_1f_2, vf_2f_3\rangle$	4	$(14, 4^7, 4)$
$\langle f_1f_2, (u+v)f_2f_3\rangle$	4	$(14, 4^7, 4)$
$\langle f_1f_3, uf_1f_3\rangle$	4	$(14, 4^7, 4)$
$\langle f_1f_3, vf_1f_3\rangle$	4	$(14, 4^7, 4)$
$\langle f_1f_3, (u+v)f_1f_3\rangle$	4	$(14, 4^7, 4)$
$\langle uvf_1f_3, uf_1f_2, vf_1$	4	$(14, 4^7, 4)$
$\langle uvf_1f_3, uf_1f_2, vf_1$	4	$(14, 4^7, 4)$
$\langle uvf_1f_3, uf_1f_2, vf_1$ $v)f_2f_3\rangle$	4	$(14, 4^7, 4)$
$\langle uvf_1f_2, uf_1f_3, vf_1$	4	$(14, 4^7, 4)$
$\langle uvf_1f_2, uf_1f_3, vf_1$	4	$(14, 4^7, 4)$
$\langle uvf_1f_2, uf_1f_3, vf_1$ $v)f_2f_3\rangle$	4	$(14, 4^7, 4)$

Let $n = 15$. Then $x^{15} - 1 = (1+x)(1+x+x^2)(1+x+x^4)(1+x^3+x^4)(1+x+x^2+x^3+x^4) = f_1f_2f_3f_4f_5$ over Λ. Observe that $\langle f_1^*\rangle = \langle f_1\rangle$, $\langle f_2^*\rangle = \langle f_2\rangle$, $\langle f_5^*\rangle = \langle f_5\rangle$, $\langle f_3^*\rangle = \langle f_4\rangle$. By Theorem 3, some self-dual cyclic codes of length 30 over Λ are shown in Table 2.

Table 2: Self-dual cyclic codes of length 30 over Λ.

Generators	d_C	$\Theta(C)$
$\langle f_1f_2f_4f_5, uf_3f_4f_5,$	8	$(30, 4^{15}, 8)$
$\langle f_1f_2f_4f_5, uf_3f_4f_5,$ $v)f_1f_2f_3f_4\rangle$	8	$(30, 4^{15}, 8)$
$\langle f_1f_2f_4f_5, uf_3f_4\rangle$	6	$(30, 4^{15}, 6)$
$\langle f_1f_2f_4f_5, vf_3f_4\rangle$	6	$(30, 4^{15}, 6)$
$\langle f_1f_2f_4f_5, (u+v)f_3f_4\rangle$	6	$(30, 4^{15}, 6)$
$\langle f_1f_2f_4f_5, (u+v)f_3f_4f_5, vf_1f_2f_3f$	6	$(30, 4^{15}, 6)$
$\langle uvf_1f_2f_4f_5, uf_3, v$	4	$(30, 4^{15}, 4)$
$\langle uvf_1f_2f_4f_5, vf_3, u$	4	$(30, 4^{15}, 4)$
$\langle uvf_1f_2f_4f_5, uf_3f_5$	4	$(30, 4^{15}, 4)$

References

[1]. A. Bonnecaze, P. Udaya, *Cyclic code and self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory, **45**, (1999), 1250-1255

[2]. A.R.J. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory, **44**, (1998), 1369-1387

[3]. B. Yildiz, S. Karadeniz, *Self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, J. Franklin Inst. **347**, (2010), 1888-1894

[4]. B. Yildiz, S. Karadeniz, *Linear codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes Cryptogr., **54**, (2010), 61-81

[5]. B. Yildiz, S. Karadeniz, *Cyclic codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes Cryptogr., **58**, (2011), 221-234

[6]. B. Yildiz, S. Karadeniz, *Linear codes over* $\mathbb{Z}_4 + u\mathbb{Z}_4$*: MacWilliams identities projections, and formally self-dual codes*, Finite Fields Appl., **27**, (2014), 24-40

[7]. B. Yildiz, N. Aydin, *On cyclic codes over* $\mathbb{Z}_4 + u\mathbb{Z}_4$ *and their* $\mathbb{Z}_4$*-images*, Int. J. Inform. Coding Theory, **2**, (2014), 226-237

[8]. E. Mart$1\breve{3}053'$fnez-Moro, S. Szabo, *On codes over local Frobenius non-chain rings of order* 16, Contemporary Math., **634**, (2015), 227-240

[9]. R. Luo, U. Parampalli, *Self-Dual Cyclic Codes over* $\mathbb{Z}_4 + u\mathbb{Z}_4$, IEICE Trans. Fundamentals, **4**, (2017), 969-974

[10]. S. Karadeniz, B. Yildiz, $(1+v)$*-Constacyclic codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, J. Franklin Inst. **348**, (2011), 2625-2632

[11]. S.T. Dougherty, P. Gaborit, M. Harada, P. Sole, *Type II codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory, **45**, (1999), 32-45

[12]. W. Bosma, J. Cannon, C. Playoust, *The MAGMA algebra system I: the user language*, J. Symb. Comput., **24**, (1997), 235-265

[13]. X.S. Kai, S.X. Zhu, L.Q. Wang, *A Family of constacyclic codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, J. Syst. Sci. Complex., **25**, (2012), 1032-1040