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 linear structures behind well-known nonlinear codes such as Kerdock and Preparata codes are 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 $n$. 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 $\Delta$. We will do this issue in this paper.

The paper is organized as follows. In Section 2, we recall some results on the ring $\Delta$. In Section 3, we consider some structural properties of cyclic codes over $\Delta$. 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 $\Delta$. 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 $\Delta$ is a commutative ring with 16 elements and characteristic 2. Any element of $\Delta$ 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 $\Delta$ (see [4]), which are described as follows

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

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

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

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

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

Obviously, the ring $\Delta$ is not a finite chain ring. Observe that $I_{u,v}$ is the unique maximal ideal of $\Delta$. Therefore, the local ring $\Delta$ is not principle either. Further, $\Delta$ 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 $\theta$ from $\Delta$ to $\Lambda$ as follows

$\theta: \Delta \rightarrow \Lambda$\n
$p + qv \rightarrow (q, p + q),$

where $p, q \in \Lambda$. It is well known that the Lee weights of elements in $\Lambda$ 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
Define a Gray weight of a vector \( c = (c_0, c_1, ..., c_{n-1}) \in \Delta^n \) to be the rational sum of the Gray weight of its component, i.e.,

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

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 \( \Delta \) is a subset of \( \Delta^n \). \( C \) is a linear code if and only if \( C \) is an \( \Delta \)-submodule of \( \Delta^n \). 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 \( \theta \) to \( \Delta^n \) as follows

\[
\begin{align*}
\theta &: \Delta^n \\
&\quad \rightarrow \Lambda^{2n} \\
(\ell_0, \ell_1, ..., \ell_{n-1}) &\mapsto (q_{0,0} + q_{0,1} + \cdots + q_{0,n-1}, \ell_0 + \ell_1, ..., \ell_{n-1}),
\end{align*}
\]

where \( \ell_i = p_i + q_i \), \( i = 0, ..., n-1 \). The Gray map \( \theta \) is a distance-preserving map from \( \Delta^n \) (Gray distance) to \( \Lambda^{2n} \) (Lee distance) and it is also \( \Lambda \)-linear.

**Proof.** For any \( c_1, c_2 \in \Delta^n \) and \( k_1, k_2 \in \Lambda \), we have \( \theta(k_1 \ell_1 + k_2 \ell_2) = k_1 \theta(\ell_1) + k_2 \theta(\ell_2) \), which implies that \( \theta \) is \( \Lambda \)-linear. Let \( c_1 = (c_{1,0}, c_{1,1}, ..., c_{1,n-1}) \) and \( c_2 = (c_{2,0}, c_{2,1}, ..., c_{2,n-1}) \) be elements of \( \Delta^n \), where \( c_{i,j} = p_{i,j} + q_{i,j}, i, j = 0, 1, ..., n-1 \). Then \( c_1 - c_2 = (c_{1,0} - c_{2,0}, ..., c_{1,n-1} - c_{2,n-1}) \) 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 \( \Lambda \).

Let \( C \) be a \((n, M, d)\) linear code over \( \Delta \), 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 \( \Lambda \).

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

3. **Structure of self-dual cyclic codes**

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

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

\[
\begin{align*}
\varphi &: \Delta^n \\
&\quad \rightarrow R \\
(a_0, a_1, ..., a_{n-1}) &\mapsto a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + (x^n - 1).
\end{align*}
\]

It is easy to see that a linear code \( C \) of length \( n \) is a cyclic code over \( \Delta \) if and only if \( \varphi(C) \) is an ideal of \( R \). In this paper, we identity cyclic codes over \( \Delta \) via 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 \( u R_f \). \( f(x) \) 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 \( u R_f \).

**Proof.** Let \( \phi \) 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 \( \text{gcd}(\phi(g(x)), \phi(f(x))) = 1 \), or \( \phi(f(x)) \).

Case 1. \( \text{gcd}(\phi(g(x)), \phi(f(x))) = 1 \). 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 coprime in \( \Lambda[x] \). Hence, it is easy to see that \( g(x) \) is a unit in the ring \( R_f \).

Case 2. \( \gcd(g(x),\phi(f(x))) = \phi(f(x)) \). 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 \( \deg(\phi(g(x))) < \deg(g((f(x)))) \). This means that \( \phi(g(x)) = 0 \). So we can say 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 \( S = \{ 0, vR_f, uvR_f, R_f, uR_f, vR_f, uR_f + uvR_f, uR_f + uvR_f \} \), where \( A \) is a subset of \( \{ 0, 1, \ldots, n-1 \} \).

**Proof.** Let \( I \) be an arbitrary nontrivial ideal of \( \frac{\Lambda[x]}{\langle f(x) \rangle} \). If \( I \not\subseteq vR_f \), by Lemma 1, it is easy to see that \( I \) is one of \( vR_f \) and \( uvR_f \).

Assume that \( I \not\subseteq vR_f \). Let \( I_n = \{ a(x) \in R_f | \exists b(x) \in R_f \text{such that } a(x) + vb(x) \in I \} \). 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 \( uvR_f \subseteq I \).

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

(iii-1-1) \( I = uR_f + uvR_f \).

(iii-1-2) \( uR_f + uvR_f \not\subseteq I \). Then there exists \( a(x) \in I \setminus (uR_f + uvR_f) \). Hence, there are polynomials \( g(x), a(x), b(x) \in R_f \) such that \( a(x) = u(x) + wb(x) + v\phi(x) \in I \), which implies that \( v\phi(x) \in I \). Observe that \( a(x) \) 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 \( v = \phi(x)h(x) \in I \). This means that \( I = uR_f + vR_f \).

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

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

(ii-2-2) \( (u + v\sum_{k \in A} x^k) \not\subseteq I \). Then there exists \( c(x) \in I \setminus (u + v\sum_{k \in A} x^k) \). Therefore, there exist polynomials \( a(x), h(x) \in R_f \) such that \( vh(x) = c(x) - (u + v\sum_{k \in A} x^k)a(x) \in I \). Since \( c(x) \not\in (u + v\sum_{k \in A} x^k) \), it follows that \( h(x) \not\in uR_f \). By Lemma 2, we have \( h(x) \) is a unit in \( R_f \), then \( v \) is in \( I \). Let \( a(x) = uA_1(x) + \lambda_2(x) = (u + v\sum_{k \in A} x^k)A_1(x) + (vA_2(x) - A_1(x)\sum_{k \in A} x^k) \in (u + v\sum_{k \in A} x^k) + vR_f = uR_f + vR_f \).

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

By Proposition 4, we certify that any ideal in \( R \) is a sum of ideals of the form \( \langle u^{j_i}v^{k_i} \tilde{f}_i + (x^n - 1) \rangle \) and
\((u + v \sum_{j \in A} x^j) F_i + (x^n - 1)\), where \(0 \leq j_i, k_i \leq 2, 1 \leq i \leq m\) and \(A\) is a subset of \(\{0,1,\ldots,n-1\}\). Through the analysis of the front, we know that a linear code \(C\) of length \(n\) is a cyclic code over \(\mathbb{D}\) if and only if \(\varphi(C)\) is an ideal of \(R\). Therefore, we can gain the algebraic structure of cyclic codes over \(\mathbb{D}\). In order to simply the algebraic structure of cyclic codes, we need the following lemma first. Let \(g_1(x), g_2(x), \ldots, g_m(x)\) be monic polynomials in \(\Lambda[x]\). Then we have

\[
\langle g_1(x) \rangle + \langle g_2(x) \rangle + \cdots + \langle g_m(x) \rangle = \langle K(x) \rangle,
\]

where \(K(x) = \gcd(g_1(x), g_2(x), \ldots, g_m(x))\).

**Proof.** Since \(K(x) = \gcd(g_1(x), g_2(x), \ldots, g_m(x))\), then \(K(x)g_i(x)\), for \(i = 1, 2, \ldots, m\). Hence, \(\langle g_i(x) \rangle \subseteq \langle K(x) \rangle\). Therefore, \(\langle g_1(x) \rangle + \langle g_2(x) \rangle + \cdots + \langle g_m(x) \rangle \subseteq \langle K(x) \rangle\).

Let \(K\) be a cyclic code of odd length \(n\) over \(\mathbb{D}\). Then

\[
C = \langle \tilde{F}_1 \rangle \oplus \langle \tilde{F}_2 \rangle \oplus \langle \tilde{F}_3 \rangle \oplus \langle \tilde{F}_4 \rangle \oplus \langle (u + v \sum_{j \in A} x^j) \tilde{F}_5 \rangle \oplus \langle (u \tilde{F}_6) + (v \tilde{F}_6) \rangle,
\]

where \(A\) is a subset of \(\{0,1,\ldots,n-1\}\), \(F_0, F_1, \ldots, F_6\) 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 \(\langle u^{1/v_j} f_j \rangle\) and \(\langle (u + v \sum_{j \in A} x^j) f_j' \rangle\), where \(0 \leq j, k_i \leq 2\) and \(1 \leq i \leq m\). After arranging if necessary, we assume that

\[
C = \langle \tilde{f}_{k_1+1} \rangle \oplus \cdots \oplus \langle \tilde{f}_{k_1+k_2} \rangle \oplus \langle u \tilde{f}_{k_1+k_2+k_3} \rangle \oplus \cdots \oplus \langle u \tilde{f}_{k_1+k_2+k_3+k_4} \rangle \oplus \langle uv \tilde{f}_{k_1+k_2+k_3+k_4+k_5} \rangle \oplus \cdots \oplus \langle uv \tilde{f}_{k_1+k_2+k_3+k_4+k_5+k_6} \rangle \oplus \langle (u + v \sum_{j \in A} x^j) \tilde{f}_{k_1+k_2+k_3+k_4+k_5+k_6+1} \rangle \oplus \cdots \oplus \langle (u \tilde{f}_m) \rangle + \langle (v \tilde{f}_m) \rangle,
\]

where \(k_1, \ldots, k_6 \geq 0\) and \(k_1 + \cdots + k_6 + 1 \leq m\).

Then we define that

\[
F_0 = f_1 \cdots f_{k_1}, F_1 = f_{k_1+1} \cdots f_{k_1+k_2},
\]

\[
F_2 = f_{k_1+k_2+1} \cdots f_{k_1+k_2+k_3}, F_3 = f_{k_1+k_2+k_3+1} \cdots f_{k_1+k_2+k_3+k_4},
\]

\[
F_4 = f_{k_1+k_2+k_3+k_4+1} \cdots f_{k_1+k_2+k_3+k_4+k_5},
\]

\[
F_5 = f_{k_1+k_2+k_3+k_4+k_5+1} \cdots f_{k_1+k_2+k_3+k_4+k_5+k_6},
\]

\[
F_6 = f_{k_1+k_2+k_3+k_4+k_5+k_6+1} \cdots f_m.
\]

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

By Lemma 3, It is clear that

\[
\langle \tilde{F}_1 \rangle = \langle \tilde{f}_{k_1+1} \rangle \oplus \cdots \oplus \langle \tilde{f}_{k_1+k_2} \rangle, \langle \tilde{F}_2 \rangle = \langle u \tilde{f}_{k_1+k_2+k_3} \rangle \oplus \cdots \oplus \langle u \tilde{f}_{k_1+k_2+k_3+k_4} \rangle,
\]

\[
\langle \tilde{F}_3 \rangle = \langle uv \tilde{f}_{k_1+k_2+k_3+k_4+k_5} \rangle \oplus \cdots \oplus \langle uv \tilde{f}_{k_1+k_2+k_3+k_4+k_5+k_6} \rangle,
\]

\[
\langle u + v \sum_{j \in A} x^j \rangle \tilde{F}_5 = \langle (u + v \sum_{j \in A} x^j) \tilde{f}_{k_1+k_2+k_3+k_4+k_5+k_6+1} \rangle \oplus \cdots \oplus \langle (u \tilde{f}_m) \rangle + \langle (v \tilde{f}_m) \rangle,
\]

Hence, we obtain

\[
C = \langle \tilde{F}_1 \rangle \oplus \langle \tilde{F}_2 \rangle \oplus \langle \tilde{F}_3 \rangle \oplus \langle \tilde{F}_4 \rangle \oplus \langle (u + v \sum_{j \in A} x^j) \tilde{F}_5 \rangle \oplus \langle (u \tilde{F}_6) + (v \tilde{F}_6) \rangle.
\]
In the following content, we study the algebraic structure of self-dual cyclic codes of odd length \( n \) over \( \Delta \). Let \( a = (a_0, a_1, \ldots, a_{n-1}) \), \( b = (b_0, b_1, \ldots, b_{n-1}) \) be two vectors in \( \Delta^n \). The vectors \( a \) and \( b \) are called orthogonal if \( a \cdot b = a_0b_0 + a_1b_1 + \cdots + a_{n-1}b_{n-1} = 0 \). For a linear code \( C \) over \( \Delta \), 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 \( \Delta \) is \( 2^k \), for some integer \( k \in \{ 0,1,\ldots,n \} \), then its dual code \( C^\perp \) has \( 2^k \) codewords, where \( k + \ell = 4n \).

Let \( C \) be a cyclic code of odd length \( n \) with notation as in Theorem 1. Then \( C^\perp = \langle F_0^\perp \rangle \oplus \langle uF_2^\perp \rangle \oplus \langle vF_3^\perp \rangle \oplus \langle (u+v\sum_{j\in\Lambda}x^j)F_2^\perp \rangle \oplus \langle uvF_6^\perp \rangle \), where \( F_i^\perp \) denotes the reciprocal polynomial of \( F_i \), \( i = 0,1,\ldots,6 \).

**Proof.** Let \( C^\perp = \langle F_0^\perp \rangle \oplus \langle uF_2^\perp \rangle \oplus \langle vF_3^\perp \rangle \oplus \langle (u+v\sum_{j\in\Lambda}x^j)F_2^\perp \rangle \oplus \langle uvF_6^\perp \rangle \). For \( i,j \in \{0,1,\ldots,6\} \), if \( i \neq j \), then \( x^n - 1 \mid F_i^\perp F_j^\perp \). Therefore, \( F_i^\perp F_j^\perp \) is a code of length \( n \). Hence, \( C^\perp \subseteq C^\perp \).

Since \( |\nu\Delta| = 2 \), \( |\nu\Delta| = |\nu| \Delta = 1 \), \( |\nu\Delta| = 2 \), \( |\nu\Delta| = 3 \) and \( |\Delta| = 4 \), let \( k = 4 \deg F_1 + 2 \deg F_2 + 2 \deg F_3 + 2 \deg F_4 + 3 \deg F_6 \) and \( \ell = 4 \deg F_0 + 2 \deg F_2 + 2 \deg F_3 + 3 \deg F_4 + 2 \deg F_5 + 2 \deg F_6 \), then \( |\Delta| = 2^k \) and \( |\Delta| = 2^\ell \). Observe that \( k + \ell = 4n \). Therefore, \( |\Delta| = |\Delta| \). Hence, \( C^\perp = C^\perp \).

In Theorem 1 and Theorem 2, we describe the algebraic structure of cyclic codes and their dual codes over the ring \( \Delta \). 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 \( \langle F_0^\perp \rangle = \langle F_1 \rangle = \langle F_2 \rangle = \langle F_3 \rangle = \langle F_4 \rangle = \langle F_5 \rangle = \langle F_6 \rangle \).

**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 \( \langle F_0 \rangle = \langle F_1 \rangle = \langle F_2 \rangle = \langle F_3 \rangle = \langle F_4 \rangle = \langle F_5 \rangle = \langle F_6 \rangle \).

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

**Proof.** For all \( c_1 = (c_{1,0}, c_{1,1} \ldots, c_{1,n-1}) \in C \) and \( c_2 = (c_{2,0}, c_{2,1} \ldots, c_{2,n-1}) \in C^\perp \), where \( c_{i,j} = p_{i,j} + q_{i,j} \nu \), \( p_{i,j}, q_{i,j} \in \Lambda \), \( i, j = 0,1,\ldots,n-1 \). Since \( c_1 \cdot c_2 = 0 \), then we have \( \sum_{j=0}^{n-1} p_{1,j} p_{2,j} + \sum_{j=0}^{n-1} p_{1,j} q_{2,j} + p_{2,j} q_{1,j} = 0 \). Therefore, \( \Theta(C_1 \cdot C_2) = \sum_{j=0}^{n-1} (p_{1,j} p_{2,j} + p_{1,j} q_{2,j} + p_{2,j} q_{1,j}) + 0 \). Thus, \( \Theta(C^\perp) \subseteq \Theta(C)^\perp \). From Proposition 2, we have \( |\Theta(C)^\perp| = |\Theta(C)| \), 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 \( \Delta \) applying Theorem 3. Moreover, by Proposition 5, we can construct some self-dual codes of length \( 2n \) over \( \Lambda \). We compute the minimum distance of the codes below by the computational algebra system Magma [12]. Let \( n = 5 \). Then \( x^5 - 1 = (1 + \nu)(1 + x + x^2 + x^3 + x^4) \) over \( \Lambda \). Suppose that \( F_2 = 1 + x \) and \( F_3 = 1 + x + x^2 + x^3 + x^4 \), where \( \langle F_0 \rangle = \langle F_2 \rangle \) and \( \langle F_3 \rangle = \langle F_4 \rangle \). Let \( C = \langle x(1 + x + x^2 + x^3 + x^4), (1 + x + x^3) \rangle \). By Theorem 3, \( C \) is a self-dual cyclic code of length 5 over \( \Delta \) with parameter \( (5,4^2)^2 \), 4. By and Proposition 2 and Proposition 5, we know \( \Theta(C) \) is a self-dual code over \( \Lambda \) with parameter \( (10,2^{10},4) \). This code is optimal [11]. Let \( n = 7 \). Then \( x^7 - 1 = (1 + x)(1 + x + x^2)(1 + x + x^3 + x^4) \) over \( \Lambda \). By Theorem 3, some self-dual cyclic codes of length 14 over \( \Lambda \) are obtained in Table 1.
Table 1: Self-dual cyclic codes of length 14 over Λ.

<table>
<thead>
<tr>
<th>Generators</th>
<th>$d_C$</th>
<th>$\Theta(C)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(f_1f_2, uf_3f_5)$</td>
<td>4</td>
<td>(14, 4', 4)</td>
</tr>
<tr>
<td>$(f_1f_2, v_3f_5)$</td>
<td>4</td>
<td>(14, 4', 4)</td>
</tr>
<tr>
<td>$(f_1f_2, (u + v)f_3f_5)$</td>
<td>4</td>
<td>(14, 4', 4)</td>
</tr>
<tr>
<td>$(f_1f_3, uf_3f_5)$</td>
<td>4</td>
<td>(14, 4', 4)</td>
</tr>
<tr>
<td>$(f_1f_3, v_3f_5)$</td>
<td>4</td>
<td>(14, 4', 4)</td>
</tr>
<tr>
<td>$(f_1f_3, (u + v)f_3f_5)$</td>
<td>4</td>
<td>(14, 4', 4)</td>
</tr>
<tr>
<td>$(uw_1f_3, uf_3f_5, v_3f_5)$</td>
<td>4</td>
<td>(14, 4', 4)</td>
</tr>
</tbody>
</table>

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 $(f_1^*) = (f_1)$, $(f_2^*) = (f_2)$, $(f_3^*) = (f_3)$, $(f_4^*) = (f_4)$. 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.

<table>
<thead>
<tr>
<th>Generators</th>
<th>$d_C$</th>
<th>$\Theta(C)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(f_1f_2f_3f_5, uf_3f_5f_5)$</td>
<td>8</td>
<td>(30, 4^{15}, 8)</td>
</tr>
<tr>
<td>$(f_1f_2f_3f_5, uf_5f_5f_3f_5, v)f_1f_2f_3f_5)$</td>
<td>8</td>
<td>(30, 4^{15}, 8)</td>
</tr>
<tr>
<td>$(f_1f_2f_3f_5, uf_3f_5f_5)$</td>
<td>6</td>
<td>(30, 4^{15}, 6)</td>
</tr>
<tr>
<td>$(f_1f_2f_3f_5, v_3f_5f_5)$</td>
<td>6</td>
<td>(30, 4^{15}, 6)</td>
</tr>
<tr>
<td>$(f_1f_2f_3f_5, (u + v)f_3f_5f_5)$</td>
<td>6</td>
<td>(30, 4^{15}, 6)</td>
</tr>
<tr>
<td>$(f_1f_2f_3f_5, (u + v)f_3f_5f_5, v_3f_5f_5f_5)$</td>
<td>6</td>
<td>(30, 4^{15}, 6)</td>
</tr>
<tr>
<td>$(uw_1f_3f_5, uf_3f_5, v_3f_5)$</td>
<td>4</td>
<td>(30, 4^{15}, 4)</td>
</tr>
<tr>
<td>$(uw_1f_3f_5, v_3f_5, u)$</td>
<td>4</td>
<td>(30, 4^{15}, 4)</td>
</tr>
<tr>
<td>$(uw_1f_3f_5, uf_3f_5f_5)$</td>
<td>4</td>
<td>(30, 4^{15}, 4)</td>
</tr>
</tbody>
</table>
References


[4]. B. Yildiz, S. Karadeniz, Linear codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$, 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


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

