Cyclic Code and Self-Dual Code over $F_2 + uF_2 + u^2F_2$

FENG Qian Qian$^1$, ZHOU Wei Gang$^2$
(1. Department of Mathematics, Xiangfan University, Hubei 441053, China; 2. School of Mathematics and Statistics, Wuhan University, Hubei 430072, China)
(E-mail: qiyu4094@sina.com)

Abstract We give the structures of a cyclic code over ring

$$R = F_2 + uF_2 + u^2F_2 = \{0, 1, u, u^2, v, v^2, uv, v^3\},$$

where $u^3 = 0$, of odd length and its dual code. For the cyclic code, necessary and sufficient conditions for the existence of self-dual code are provided.

Keywords ring $F_2 + uF_2 + u^2F_2$; cyclic code; residue code; torsion code; self-dual code.

1. Introduction

From the 1990s, the theory of codes over finite rings has gained prominence since the significant discovery of Nechaev$^{[1]}$. Nechaev showed that several well-known prominent families of good nonlinear binary codes can be identified as images of linear codes over $Z_4$ under the Gray map. Since then, codes over finite rings have received much attention$^{[2-4]}$. Many results in codes over finite rings especially over ring $Z_4$ have been obtained. Recently, a new ring $F_2 + uF_2 + u^2F_2 = \{0, 1, u, 1+u\}$, where $u^2 = 0$, has been studied in $^{[5-7]}$.

In this paper, we obtain the structures of a cyclic code over $R = F_2 + uF_2 + u^2F_2$ of odd length and its cyclic dual code. We also provide necessary and sufficient conditions for the existence of self-dual code for the cyclic code.

2. Notations and definitions

$R$ is a commutative chain ring of 8 elements which are $\{0, 1, u, u^2, v, v^2, uv, v^3\}$, where $u^3 = 0$, $v = 1 + u$, $v^2 = 1 + u^2$, $v^3 = 1 + u + u^2$ and $uv = u + u^2$. The elements of $R$ are the polynomials over $F_2$ modulo the ideal $(u^3)$ of $F_2[u]$, where $F_2$ is the binary field $\{0, 1\}$. Addition and multiplication operations over $R$ are given in the Tables 1 and 2. The ring $R$ has maximal ideal $uR = \{0, u, u^2, uv\}$.

Received date: 2007-05-11; Accepted date: 2008-05-07
Table 1 Addition operator

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>u</th>
<th>v</th>
<th>u²</th>
<th>uv</th>
<th>v²</th>
<th>v³</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>u</td>
<td>v</td>
<td>u²</td>
<td>uv</td>
<td>v²</td>
<td>v³</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>v</td>
<td>u</td>
<td>v²</td>
<td>u²</td>
<td>uv</td>
<td>v²</td>
</tr>
<tr>
<td>u</td>
<td>u</td>
<td>v</td>
<td>0</td>
<td>1</td>
<td>uv</td>
<td>u²</td>
<td>v³</td>
<td>v²</td>
</tr>
<tr>
<td>v</td>
<td>v</td>
<td>u</td>
<td>1</td>
<td>0</td>
<td>v³</td>
<td>v²</td>
<td>uv</td>
<td>u²</td>
</tr>
<tr>
<td>u²</td>
<td>u²</td>
<td>v²</td>
<td>uv</td>
<td>v³</td>
<td>0</td>
<td>u</td>
<td>1</td>
<td>v</td>
</tr>
<tr>
<td>uv</td>
<td>uv</td>
<td>v³</td>
<td>u²</td>
<td>v²</td>
<td>u</td>
<td>0</td>
<td>v</td>
<td>1</td>
</tr>
<tr>
<td>v²</td>
<td>v²</td>
<td>u²</td>
<td>v³</td>
<td>uv</td>
<td>1</td>
<td>v</td>
<td>0</td>
<td>u</td>
</tr>
<tr>
<td>v³</td>
<td>v³</td>
<td>uv</td>
<td>v²</td>
<td>u²</td>
<td>v</td>
<td>1</td>
<td>u</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 2 Multiplication operator

<table>
<thead>
<tr>
<th>·</th>
<th>0</th>
<th>1</th>
<th>u</th>
<th>v</th>
<th>u²</th>
<th>uv</th>
<th>v²</th>
<th>v³</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>u</td>
<td>v</td>
<td>u²</td>
<td>uv</td>
<td>v²</td>
<td>v³</td>
</tr>
<tr>
<td>u</td>
<td>0</td>
<td>u</td>
<td>u²</td>
<td>uv</td>
<td>0</td>
<td>u²</td>
<td>u</td>
<td>uv</td>
</tr>
<tr>
<td>v</td>
<td>0</td>
<td>v</td>
<td>uv</td>
<td>v²</td>
<td>u²</td>
<td>u</td>
<td>v³</td>
<td>1</td>
</tr>
<tr>
<td>u²</td>
<td>0</td>
<td>u²</td>
<td>0</td>
<td>u²</td>
<td>0</td>
<td>0</td>
<td>u²</td>
<td>u²</td>
</tr>
<tr>
<td>uv</td>
<td>0</td>
<td>uv</td>
<td>u²</td>
<td>u</td>
<td>0</td>
<td>u²</td>
<td>uv</td>
<td>u</td>
</tr>
<tr>
<td>v²</td>
<td>0</td>
<td>v²</td>
<td>u</td>
<td>v³</td>
<td>u²</td>
<td>uv</td>
<td>1</td>
<td>v</td>
</tr>
<tr>
<td>v³</td>
<td>0</td>
<td>v³</td>
<td>uv</td>
<td>1</td>
<td>u²</td>
<td>u</td>
<td>v</td>
<td>v²</td>
</tr>
</tbody>
</table>

For a finite ring $R$, consider the set $R^n$ of $n$-tuples of elements from $R$ as a module over $R$ in the usual way. A subset $C \subseteq R^n$ is called a linear codes of length $n$ over $R$ if $C$ is an $R$-submodule of $R^n$. A code $C$ is called cyclic if for every codeword $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in C$, its cyclic shift $(x_{n-1}, x_0, \ldots, x_{n-2})$ is also in $C$.

Given $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$ and $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1}) \in R^n$, their scalar product (or dot product) is $\langle \mathbf{x}, \mathbf{y} \rangle = x_0y_0 + \cdots + x_{n-1}y_{n-1} \in R$. Two words $x, y$ are called orthogonal if $\langle x, y \rangle = 0$. For a linear code $C$ over $R$, its dual code $C^\perp$ is the set of words over $R$ that are orthogonal to all codewords of $C$, i.e., $C^\perp = \{ \mathbf{c} \in R^n | \langle \mathbf{c}, \mathbf{e} \rangle = 0, \forall \mathbf{e} \in C \}$.

A code $C$ is called self-dual if $C = C^\perp$. An $n$-tuple $c = (c_0, c_1, \ldots, c_{n-1}) \in R^n$ is identified with the polynomial $c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ in $R[x]/(x^n - 1)$, which is called the polynomial representation of $c = (c_0, c_1, \ldots, c_{n-1})$. For any $\lambda = r(\lambda) + uq(\lambda) + u²p(\lambda) \in R$, $r(\lambda), q(\lambda), p(\lambda) \in F_2$. Let $\bar{\lambda} = r(\lambda)$ denote the reduction of $\lambda$.

Define a polynomial reduction mapping

$$u : R[x] \rightarrow F_2[x], \ f(x) = \sum_{i=0}^{r} a_i x^i \rightarrow \sum_{i=0}^{r} \bar{a}_i x^i.$$

A monic polynomial $f(x)$ over $R[x]$ is said to be a basic irreducible polynomial if its projection $uf(x)$ is irreducible over $F_2[x]$. 


Let $C$ be a linear code over $R$. We define the reduction code $C_{(1)}$ and the torsion code $C_{(2)}$ of $C$ as follows. $C_{(1)} = \{ x \in F_2^n \mid \exists y, z \in F_2^n \text{ s.t. } x + yu + zu^2 \in C \}$ and $C_{(2)} = \{ x \in F_2^n \mid u^2x \in C \}$.

Let $f_1(x), f_2(x) \in R[x]$. $f_1(x)$ is called an associate of $f_2(x)$ if there is an invertible element $r \in R$ such that $f_1(x) = rf_2(x)$.

3. Main results and proof

It is well known that a linear code $C$ of odd length, denoted $n$, over $R$ is cyclic code if and only if the set of polynomial representation of its codewords is an ideal of $R[x]/(x^n - 1)$.

Lemma 3.1 If $f$ is a basic irreducible polynomial of the ring $R[x]$, then $R[x]/(f(x))$ has the following ideals: (0), $1 + (f(x)), (u + (f(x)), (u^2 + (f(x)))$.

Proof (1) First we show that for distinct values of $i, j \in \{0, 1, 2\}$, $(u^i + (f(x))) \neq (u^j + (f(x)))$. Suppose $(u^i + (f(x))) = (u^j + (f(x)))$. There exists $g(x) \in R[x]$ with $\deg(g) < \deg(f)$ such that $u^i + (f) = u^jg(x) + (f)$. That means $u^jg(x) = u^i$. As $\deg(u^i) \leq \deg(g(x)) < \deg(f)$, it follows that $u^i = 0$. Multiplying by $u^{3-j}$ gives $u^{3-j+i} = 0$, which is a contradiction to our hypothesis that $u$ has nilpotency 3 and $0 < 3 - j + i < 3$.

(2) Let $I$ be a nonzero ideal of $R[x]/(f)$ and $h + (f)$ a nonzero element of $I$. By assumption, $f$ is a basic irreducible polynomial in $R[x]$. Hence, $f$ is irreducible in $R[x]$. Therefore, $\gcd(h, f) = 1$ or $\bar{f}$. If $\gcd(h, \bar{f}) = 1$, i.e., $h$ and $f$ are coprime in $R[x]$, then $h$ and $f$ are coprime in $R[x]$. So there exist $a, b \in R[x]$ such that $ah + bf = 1$. That implies $(a + (f))(h + (f)) = 1 + (f)$, whence $h + (f)$ is invertible in $R[x]/(f)$. Therefore, $I = (1 + (f))$. For the case $\gcd(h, \bar{f}) = \bar{f}$, for all $h + (f) \in I$, which means $\bar{f} | h$ and $f | h$. Hence, there exist $p, v \in R[x]$ such that $h = fp + uv$, whence $h + (f) \in (u + (f))$ for all $h + (f) \in I$, implying $I \subseteq (u + (f))$. Let $k$ be the greatest integer < 3 such that $I \subseteq (u^k + (f))$. Then, as $I \nsubseteq (u^{k+1} + (f))$, there is a nonzero element $h_0 + (f) \in I$ such that $h_0 + (f) \notin (u^{k+1} + (f))$. Since $h_0 + (f) \in I \subseteq (u^k + (f))$, there exist $p_0, v_0 \in R[x]$ such that $h_0 = p_0f + v_0u^k$. Now $\gcd(v_0, \bar{f}) = 1$ or $\bar{f}$. Suppose $\gcd(v_0, \bar{f}) = \bar{f}$. Then $\bar{f} | v_0$ and $f | v_0$. So there exist $p_1, v_1 \in R[x]$ such that $v_0 = p_1f + v_1u$. Hence, $h_0 = p_0f + v_0u^k = p_0f + (p_1f + v_1u)u^k = (p_0 + p_1u) + u^k + v_1u$. It follows that $h_0 + (f) \in (u^{k+1} + (f))$, a contradiction. Thus, $\gcd(v_0, \bar{f}) = 1$. The same argument as above yields that $v_0 + (f)$ is invertible in $R[x]/(f)$, which means that there exists $w_0 + (f) \in R[x]/(f)$ such that $(w_0 + (f))(v_0 + (f)) = 1 + (f)$. Therefore, $u^k + (f) = (w_0 + (f))(u^kv_0 + (f)) = (w_0 + (f))h_0 + (f) \in I$. Consequently, $I = (u^k + (f)) \ (k = 0, 1, 2)$. □

Theorem 3.2 Let $x^n - 1 = f_1, f_2, \ldots, f_r$ be a representation of $x^n - 1$ as a product of basic
irreducible pairwise-coprime polynomials in \( R[x] \). Then any ideal in \( R[x]/(x^n - 1) \) is a sum of
\[
(\hat{f}_i + (x^n - 1)), \quad (uf_\hat{i} + (x^n - 1)), \quad (u^2 \hat{f}_i + (x^n - 1)),
\]
where \( 0 \leq i \leq r \) and \( \hat{f}_i = (x^n - 1)/f_i = \Pi_{j \neq i} f_j \).

**Proof** By the Chinese Remainder theorem, we have
\[
R_n = R[x]/(x^n - 1) = R[x]/(f_1) \cap (f_2) \cap \cdots \cap (f_r)
\quad \cong R[x]/(f_1) \oplus R[x]/(f_2) \oplus \cdots \oplus R[x]/(f_r).
\]
Thus, any ideal \( I \) of \( R[x]/(x^n - 1) \) is of the form \( \oplus \sum_{i=1}^{r} I_i \), where \( I_i \) is an ideal of \( R[x]/(f_i) \).
By Lemma 3.1, \( I_i = (0) \) or \( (u^n + (f_i)) \) for \( 0 \leq m \leq 2 \). Then \( I_i \) corresponds to \( (u^n f_i + (x^n - 1)) \) \( (0 \leq m \leq 2) \in R[x]/(x^n - 1) \).

**Theorem 3.3** Let \( C \) be a cyclic code of odd length \( n \). Then there exists a unique family of pairwise coprime monic polynomials \( F_0, F_1, F_2, F_3 \in R[x] \) such that \( x^n - 1 = F_0 F_1 F_2 F_3 \) and
\[
C = (\hat{F}_1, u\hat{F}_2, u^2\hat{F}_3).
\]
Moreover
\[
| C | = 2^l, \quad l = \sum_{i=0}^{2} (3 - i) \text{deg} F_{i+1}.
\]

**Proof** Let \( x^n - 1 = f_1, f_2, \ldots, f_r \) be the unique factorization of \( x^n - 1 \) into a product of monic basic irreducible pairwise coprime polynomials. By Theorem 3.2, \( C \) is a direct sum of ideals of the form \( (u^j f_i) \) \( (0 \leq i \leq r) \). After reordering if necessary, we can assume that \( C \) is a direct sum of the form
\[
(\hat{f}_{k_1+1}), (\hat{f}_{k_1+2}), \ldots, (\hat{f}_{k_1+k_2}); (uf_{k_1+k_2+1}), \ldots, (uf_{k_1+k_2+k_3}); (u^2 \hat{f}_{k_1+k_2+k_3+1}), \ldots, (u^2 \hat{f}_r),
\]
i.e.,
\[
C = (f_1 f_2 f_3 \cdots f_{k_1+k_2+1} \cdots f_r, uf_{k_1+k_2+1} \cdots f_r, u^2 f_{k_1+k_2+k_3+1} \cdots f_r),
\]
Let
\[
\hat{F}_1 = f_1 f_2 f_3 \cdots f_{k_1+k_2+1} \cdots f_r,
\]
\[
\hat{F}_2 = f_1 f_2 f_3 \cdots f_{k_1+k_2} f_{k_1+k_2+k_3+1} \cdots f_r,
\]
\[
\hat{F}_3 = f_1 f_2 f_3 \cdots f_{k_1+k_2+k_3}.
\]
Then
\[
F_i = \begin{cases} 
1, & k_{i+1} = 0; \\
\frac{1}{f_{k_0+k_1+\cdots+k_{i+1}} \cdots f_{k_0+k_1+\cdots+k_{i+1}}}, & k_{i+1} \neq 0, \quad (k_0 = 0, 0 \leq i \leq 3).
\end{cases}
\]
Thus, by our construction, it is clear that \( C = (\hat{F}_1, u\hat{F}_2, u^2\hat{F}_3) \) and \( x^n - 1 = F_0 F_1 F_2 F_3 = f_1 f_2 \cdots f_r \).
To prove the uniqueness, assume \( G_0, G_1, G_2, G_3 \) are pairwise coprime monic polynomials in \( R[x] \) such that \( G_0 G_1 G_2 G_3 = x^n - 1 \) and \( C = (G_1, uG_2, u^2G_3) \). Thus, \( C = (G_1) + (uG_2) + (u^2G_3) \).
Now there exist nonnegative integers \( l_0 = 0, l_1, \ldots, l_{t+1} \), with \( l_0 + l_1 + \cdots + l_{t+1} = r \), and a permutation \( \{f'_1, \ldots, f'_r\}\) of \( \{f_1, f_2, \ldots, f_r\}\) such that \( G_i = f'_{l_0+i+1} \cdots f'_{l_0+i+l_{t+1}} \) for \( i = 0, 1, 2, 3 \). Hence,

\[
C = (\hat{f}'_{l_1+1}) \oplus \cdots \oplus (\hat{f}'_{l_2}) \oplus (u \hat{f}'_{l_1+l_2+1}) \oplus (u^2 \hat{f}'_{l_1+l_2+l_3+1}) \oplus \cdots \oplus (u^2 \hat{f}'_r).
\]

It follows that \( l_i = k_i \) for \( i = 0, 1, 2, 3 \). Furthermore, \( \{f'_{l_0+\cdots+l_{t+1}}, \ldots, f'_{l_0+\cdots+l_{t+1}}\}\) is a permutation of \( \{f_{k_0+\cdots+k_{t+1}}, \ldots, f_{k_0+\cdots+k_{t+1}}\}\). Therefore, \( F_i = G_i \) for \( i = 0, 1, 2, 3 \). To calculate the order \( |C| \), note that

\[
C = (\hat{F}_1, u \hat{F}_2, u^2 \hat{F}_3), \quad C = (\hat{F}_1) \oplus (u \hat{F}_2) \oplus (u^3 \hat{F}_3).
\]

Hence, \( |C| = 2^3 \deg \hat{F}_1 2^2 \deg \hat{F}_2 2 \deg \hat{F}_3 = 2^4 \). \( \square \)

**Theorem 3.4** Let \( C \) be a cyclic code of odd length \( n \) over \( R \). Then there exist polynomials \( g_0, g_1, g_2 \) in \( R[x] \) such that \( C = (g_0, u g_1, u^2 g_2) \) and \( g_2 | g_1 | g_0 | x^n - 1 \).

**Proof**

By Theorem 3.3, there exists a family of pairwise coprime monic polynomials \( F_0, F_1, F_2, F_3 \) in \( R[x] \) such that \( x^n - 1 = F_0 F_1 F_2 F_3 \) and \( C = (\hat{F}_1, u \hat{F}_2, u^2 \hat{F}_3) \). Define

\[
g_0 = F_0 F_2 F_3, \quad g_1 = F_0 F_3, \quad g_2 = F_0.
\]

Clearly, \( g_2 | g_1 | g_0 | x^n - 1 \). Moreover, for \( 0 \leq i \leq 2 \), we have

\[
u^i \hat{F}_{i+1} = u^i F_0 F_1 \cdots F_i F_{i+2} \cdots F_3 = u^i g_1 F_1 F_2 \cdots F_i.
\]

Therefore, \( C \subseteq (g_0, u g_1, u^2 g_2) \). On the other hand, \( g_0 = F_0 F_2 F_3 \in C \). Since \( F_1 \) and \( F_2 \) are coprime polynomials in \( R[x] \), there exist polynomials \( u_1, v_1 \in R[x] \) such that \( u_1 F_1 + v_1 F_2 = 1 \). It follows that

\[
g_1 = F_0 F_3 = (u_1 F_1 + v_1 F_2) F_0 F_3 = u_1 F_0 F_1 F_3 + v_1 F_0 F_2 F_3 = u_1 \hat{F}_2 + v_1 g_0,
\]

whence \( u_1 g_1 = u u_1 \hat{F}_2 + u v_1 g_0 \in C \). Continuing this process, we obtain \( u^2 g_2 \in C \), which implies \( C \supseteq (g_0, u g_1, u^2 g_2) \). Consequently, \( C = (g_0, u g_1, u^2 g_2) \). \( \square \)

**Theorem 3.5** Let \( C \) be a cyclic code of odd length \( n \) over \( R \). With notations as in Theorem 3.4, denote \( G = \hat{F}_1 + u \hat{F}_2 + u^2 \hat{F}_3 \). Then \( G \) is a generating polynomial of \( C \), i.e., \( C = (G) \).

**Proof**

For any distinct \( i, j \in \{0, 1, 2, 3\} \), we have \( (x^n - 1) | \hat{F}_i \hat{F}_j \). Therefore, \( \hat{F}_i \hat{F}_j = 0 \) in \( R[x] / (x^n - 1) \). Moreover, for any \( 1 \leq i \leq 3 \), \( F_i \) and \( \hat{F}_i \) are coprime. Hence, there exist \( b_i, c_i \in R[x] \) such that \( b_i \hat{F}_i + c_i F_i = 1 \). Thus, for any integer \( 1 \leq m \leq 3 \), we have \( \prod_{i=1}^{m} (b_i \hat{F}_i + c_i F_i) = 1 \). Multiplying the left-hand side of this equation out, we get that there exist polynomials \( a_{m0}, a_{m1}, \ldots, a_{mm} \) such that

\[
a_{m0} F_1 F_2 \cdots F_m + a_{m1} \hat{F}_1 F_2 \cdots F_m + a_{m2} F_1 \hat{F}_2 \cdots F_m + \cdots + a_{mm} F_1 F_2 \cdots F_{m-1} \hat{F}_m = 1.
\]

In particular, when \( m = 3 \), multiplying both sides of the above equation by \( u^2 \hat{F}_3 \) yields

\[
u^2 \hat{F}_3 = u^2 a_{m0} F_1 F_2 \hat{F}_3.
\]
Since
\[ F_1 F_2 G = u^2 F_1 F_2 \hat{F}_3, \]
\[ G F_1 F_2 a_{m0} = u^2 \hat{F}_3, \]
\[ u^2 \hat{F}_3 \in (G). \] Continuing this process, we obtain that \( u \hat{F}_2 \in (G) \) and \( \hat{F}_1 \in (G) \), i.e., \( C \subset (G) \). It is clear that \( C \supset (G) \). Consequently, \( C = (G) \). \qed

Next, we discuss the structure of the dual code of the cyclic code.

**Lemma 3.6** [9] Let \( C \) be a linear code of length \( n \) over \( R \). \(|R| = p^α \). Then \(|C|\) is a power of \( p \).
Assume \(|C| = p^d \) and \(|C^⊥| = p^j \). Then \( d + l = nα \).

**Theorem 3.7** Let \( C \) be a cyclic code of odd length \( n \) over \( R \) with \( C = (\hat{F}_1, u \hat{F}_2, u^2 \hat{F}_3) \), \(|C| = 2^l \) and \( l = \sum_{i=0}^{2} (3 - i) \deg F_{i+1} \), where \( x^n - 1 = F_0 F_1 F_2 F_3 \) and \( F_4 = F_0 \), as in Theorem 3.4. Then
\[ |C^⊥| = 2^{\sum_{i=1}^{3} i \deg F_{i+1}} \]
and \( C^⊥ = (\hat{F}_0^*, u \hat{F}_3^*, u^2 \hat{F}_2^*) \), where \( F^* = x^\deg(F) F(1/x) \).

**Proof** Denote \( C_1 = (\hat{F}_0^*, u \hat{F}_3^*, u^2 \hat{F}_2^*) \). Next we show that \( C_1 = C^⊥ \). For any \( 0 \leq i, j \leq 3 \), we have
\[ (u^i \hat{F}_{i+1})(u^j \hat{F}_{3-j+1})^* \equiv 0 \pmod{x^n - 1}. \]
Therefore, \( C_1 \subset C^⊥ \). Let \(|C^⊥| = 2^{l'} \) and \(|C| = 2^l \). By Lemma 3.6, \( h' + l = 3n \). Hence \( h' = \sum_{i=1}^{3} i \deg F_{i+1} \). Note that \(|C| = 2^{\sum_{i=1}^{3} i \deg F_{i+1}} \). Consequently, \( C_1 = C^⊥ \). \qed

Next, we discuss the residue and torsion codes of the cyclic code over \( R \).

**Theorem 3.8** Let \( C \) be a cyclic code of odd length \( n \) over \( R \) with \( C = (\hat{F}_1, u \hat{F}_2, u^2 \hat{F}_3) \), where \( x^n - 1 = F_0 F_1 F_2 F_3 \) and \( F_0, F_1, F_2, F_3 \) are pairwise coprime monic polynomials. We have the residue code \( C_{(1)} = u(F_0 F_2 F_3) \) of dimension \( \deg(F_1) \) and the torsion code \( C_{(2)} = u(F_0) \) of dimension \( \deg(F_1) + \deg(F_2) + \deg(F_3) \).

**Theorem 3.9** Let \( C = (\hat{F}_1, u \hat{F}_2, u^2 \hat{F}_3) \) and \( x^n - 1 = F_0 F_1 F_2 F_3 \). Then \( C \) is self-dual if and only if \( F_i \) is an associate of \( F_j^* \) for all \( i, j \in \{0, 1, 2, 3\} \) such that \( i + j \equiv 1 \pmod{4} \).

**Proof** By Theorem 3.7, \( C^⊥ = (\hat{F}_0^*, u \hat{F}_3^*, u^2 \hat{F}_2^*) \). Hence, if \( F_i \) is an associate of \( F_j^* \) for \( i, j \in \{0, 1, 2, 3\} \) such that \( i + j \equiv 1 \pmod{4} \), then
\[ C = (\hat{F}_1, u \hat{F}_2, u^2 \hat{F}_3) = (\hat{F}_0^*, u \hat{F}_3^*, u^2 \hat{F}_2^*) = C^⊥, \]
i.e., \( C \) is self-dual.

On the other hand, assume \( C = C^⊥ \). Let \( c_i \) denote the constants of \( F_i \) (\( 0 \leq i \leq 3 \)). Since \( x^n - 1 = F_0 F_1 F_2 F_3 \), we have \( c_0 c_1 c_2 c_3 = -1 \). Therefore, \( c_i \)s are invertible elements of \( R \) and \( c_i \)s are leading coefficients of \( F_i \)s. For all \( i, j \in \{0, 1, 2, 3\} \) such that \( i + j \equiv 1 \pmod{4} \), denote \( G_i = u_i F_j^* \), where \( u_i \)s are monic polynomials. Note that \( u_i = c_j^{-1} \), and \( u_0 u_1 u_2 u_3 = c_0^{-1} c_1^{-1} c_2^{-1} c_3^{-1} = -1 \). Now
\[ C = (\hat{F}_1, u \hat{F}_2, u^2 \hat{F}_3) = C^⊥ = (\hat{F}_0^*, u \hat{F}_3^*, u^2 \hat{F}_2^*) = (G_1, uG_2, u^2G_3). \]
Also,

\[ G_0G_1G_2G_3 = (u_0u_1u_2u_3)F_1^*F_0^*F_3^*F_2^* = -F_0^*F_1^*F_2^*F_3^* \]
\[ = -x^{\deg F_0 + \deg F_1 + \deg F_2 + \deg F_3}F_0(x^{-1})F_1(x^{-1})F_2(x^{-1})F_3(x^{-1}) \]
\[ = -x^n(x^{-n} - 1) = x^n - 1. \]

From the uniqueness in Theorem 3.3, \( G_i = F_i \) and \( F_i = u_iF_j^* \). The proof is completed. \( \square \)

References

[8] AL-ASHKER M M. Simplex codes over the ring \( \sum_{i=0}^{n} u^i F_2 \) [J]. Turkish J. Math., 2005, 29(3): 221–233.