**Cyclic Codes of Length \( n \) Over \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \)**

Hualu Liu*

*School of Mathematics and Physics, Hubei Polytechnic University, Huangshi Hubei, 435003, China*

**Abstract:** We study the structure of cyclic codes of an arbitrary length \( n \) over the ring \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \), which is not a finite chain ring. We prove that the Gray image of a cyclic code over \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \) is a 3-quasi-cyclic code over \( \mathbb{F}_p \).

**Keywords:** Linear codes, cyclic codes, Gray map.

1. INTRODUCTION

Cyclic codes over finite rings are important class of codes from a theoretical and practical viewpoint. It has been shown that certain good nonlinear binary codes such as binary Kerdock codes are the Gray images of some \( \mathbb{Z}_4 \)-linear codes [1]. Using the Gray map a new set of linear or nonlinear binary codes has been constructed as the Gray images of some codes over rings [2-5]. Recently, cyclic codes over ring \( \mathbb{F}_p \) have been considered by Yildiz and Konadeniz in [6], where some good binary codes have been obtained as the images under two Gray maps. Some results related to cyclic codes over \( \mathbb{F}_p + \mathbb{F}_p \) were given by Zhu et al. in [2], where cyclic codes over the ring are principally generated.

In this work, we focus on codes over the ring \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \), where \( u^2 = uv = vu = 0 \) and \( v^2 = v \). First, we define the Gray map from \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \) to \( \mathbb{F}_p \) and prove that the image of a linear code of length \( n \) over \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \) under the Gray map is a distance-invariant linear code of length \( 3n \) over \( \mathbb{F}_p \). Next, we determine the generator polynomials of such cyclic codes over \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \) and prove that the images under Gray maps of cyclic codes over \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \) are 3-quasi-cyclic codes over \( \mathbb{F}_p \).

2. LINEAR CODES OVER THE RING \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \)

The ring \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \) is defined as a characteristic \( p \) ring subject to the restrictions \( u^2 = uv = vu = 0 \) and \( v^2 = v \).

Let \( W_L \) be the Lee weight of the element over \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \) and \( W_H \) be the ordinary Hamming weight for the binary codes. So

\[
W_L(a + ub + vc) = W_H(c, b + c, a + b + c)
\]

(2.1)

\( \forall a, b, c \in \mathbb{F}_p \). The definition of the weight immediately leads to a Gray map from \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \) to \( \mathbb{F}_p^3 \) which can naturally be extended to \( (\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p)^n \):

\[
\varphi(a + ub + vc) = (c, b + c, a + b + c)
\]

(2.2)

Note that \( \varphi \) extends to a distance-preserving isometry:

\[ (\mathbb{F}_p^3, \text{Lee weight}) \rightarrow (\mathbb{F}_p^n, \text{Hamming weight}) \].

**Theorem 2.1.** If \( C \) is a linear code over \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \) of length \( n \), size \( p^k \) and minimum Lee weight \( d \), then \( \varphi(C) \) is a linear code with parameters [3\( n \), \( k \), \( d \)] over \( \mathbb{F}_p \).

3. CHARACTERIZATION OF CYCLIC CODES OVER \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \)

The notions of cyclic shift and cyclic codes are standard for codes over all rings. Briefly, for any ring \( R \), a cyclic shift on \( R^n \) is a permutation \( T \) such that

\[ T(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, \ldots, c_{n-2}) \].

A linear code over ring \( R \) of length \( n \) is cyclic if it is invariant under cyclic shift. It is known that a linear code over ring \( R \) is cyclic if and only if its polynomial representation is an ideal in \( \mathbb{R}[x] < x^n - 1 > \).

[7] Let \( C \) be a cyclic code over \( \mathbb{F}_p + u\mathbb{F}_p \) of length \( n \). Then
Cyclic Codes of Length $n$ Over $F_p + uF_p + vF_p$

$$C = \langle g(x) + up(x), ua(x) \rangle,$$
with $a(x) \mid g(x) \mid (x^n - 1), a(x) \mid p(x) \frac{x^n - 1}{g(x)}, \deg a > \deg p.$

**Lemma 3.2 ([7])** With the same notations as the Lemma 3.1. If $(n, p) = 1$, then

$$C = \langle g(x) + ua(x) \rangle.$$

In the following, we will introduce a homomorphism from $F_p + uF_p + vF_p$ to $F_p + uF_p$ and use it to characterize cyclic codes over $F_p + uF_p + vF_p$ by using the results obtained from cyclic codes over $F_p + uF_p$.

Start with the homomorphism $\psi : F_p + uF_p + vF_p \mapsto F_p + uF_p$, with $\psi(a + ub + vd) = a + ub$. This homomorphism then can be extended to a homomorphism of rings of polynomials $\psi : \frac{(F_p + uF_p + vF_p)[x]}{x^n - 1} \mapsto \frac{(F_p + uF_p)[x]}{x^n - 1}$, by letting $\psi(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}) = \psi(c_0) + \psi(c_1)x + \cdots + \psi(c_{n-1})x^{n-1}$.

**Theorem 3.3** Let $C$ be a cyclic code over $F_p + uF_p + vF_p$ of length $n$. Then

$$C = \langle g(x) + up_1(x) + vp_2(x), ua_1(x) + va_2(x) \rangle$$
with $a_1 \mid g(x) \mid (x^n - 1)$ and $a_2 \mid p_1(x) \frac{x^n - 1}{g(x)}$.

**Proof.** Restrict $\psi$ onto $C$. Since $C$ is invariant under the cyclic shift, so is $\psi(C)$. This means $\text{Im}(\psi)$ is a cyclic code over $F_p + uF_p$. By Lemma 3.1, we have

$$\text{Im}(\psi) = \langle g(x) + up_1(x), ua_1(x) \rangle,$$
where $g, p_1, a_1$ are polynomials in $\frac{F_p[x]}{x^n - 1}$ satisfying the conditions $a_1 \mid g(x) \mid (x^n - 1), a_1 \mid p_1(x) \frac{x^n - 1}{g(x)}$.

On the other hand, $\text{Ker}(\psi)$ is also a cyclic code over $vF_p$. We can consider it to be $v$ times a cyclic code over $F_p$. By using the characterization [8], we have

$$\text{Ker}(\psi) = v \langle a_2(x) \rangle,$$

where $a_2$ is a polynomial in $\frac{F_p[x]}{x^n - 1}$ satisfying the condition $a_2 \mid (x^n - 1)$. Since $va_1(x) \in \text{Ker}(\psi) = v \langle a_2(x) \rangle$, $a_1 \mid a_2$.

For any $f(x) \in C$, we can write $f(x) = f_1(x) + uf_2(x) + vf_3(x)$, where $f_1, f_2, f_3$ are polynomials in $F_p[x]$. Suppose that

$$C_1 = \{ f_1(x) + uf_2(x) \mid \text{There exists } f_3(x) \in \frac{F_p[x]}{x^n - 1},$$

such that $f_1(x) + uf_2(x) + vf_3(x) \in C$.

Then, $C_1 = \text{Im}(\psi) = \langle g(x) + up_1(x), ua_1(x) \rangle$. Therefore, we have

$$\langle g(x) + up_1(x) + vp_2(x), ua_1(x) + va_2(x) \rangle \subseteq C.$$

Conversely, for any $f(x) \in C_1$, we have $f(x) = f_1(x) + uf_2(x) + vf_3(x)$, where $f_1(x) + uf_2(x)$ is in $C_1 = \langle g(x) + up_1(x), ua_1(x) \rangle$. Hence there exist $c(x), d(x)$ in $F_p[x]$ such that

$$f(x) = c(x)[g(x) + up_1(x)] + ud(x)a_1(x) + vf_3(x)$$

$$= c(x)[g(x) + up_1(x) + vp_2(x)] + d(x)[ua_1(x) + va_2(x)] + v[f_3(x) - c(x)p_2(x) - d(x)q_2(x)].$$

It is easy to see that $v[f_3(x) - c(x)p_2(x) - d(x)q_2(x)] \in \text{Ker}(\psi) = \langle va_2(x) \rangle$. Therefore

$$f(x) \in \langle g(x) + up_1(x) + vp_2(x), ua_1(x) + va_2(x) \rangle$$
i.e., $C \subseteq \langle g(x) + up_1(x) + vp_2(x), ua_1(x) + va_2(x) \rangle$ which completes the proof.

**Theorem 3.4** Let $C$ be a cyclic code over $F_p + uF_p + vF_p$ of length $n$. When $(n, p) = 1$, then $C$ is an ideal in $R_n$ which can be generated by

$$C = \langle g_1(x) + up_1(x), vb_1(x), vg_2(x) \rangle,$$

where $g_1, g_2, p_1, b_1$ are polynomials in $\frac{F_p[x]}{x^n - 1}$ satisfying the conditions $p_1 \mid g_1(x) \mid (x^n - 1), g_2(x) \mid (x^n - 1)$.
Proof. Suppose \( C \) is a cyclic code over \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \) of length \( n \). Then \( \psi(C) \) is a cyclic code over \( \mathbb{F}_p + u\mathbb{F}_p \) and \( \text{Ker}(\psi) \) is \( \nu \) times a cyclic code of order \( \mathbb{F}_p \) of odd length \( n \).

By Lemma 3.2, we have
\[
\text{Im}(\psi) = \left\{ g_1(x) + up_1(x) \right\}
\]
where \( g_1 \) and \( p_1 \) are binary polynomials with \( p_1 | g_1 | x^n - 1 \) and
\[
\text{Ker}(\psi) = \nu \left\{ g_2(x) \right\}
\]

Where, \( g_1 \) is a binary polynomial with \( g_1(x) | x^n - 1 \).

Now combining (3.1) with (3.2) we see that we can write
\[
C = \left\{ g_1(x) + up_1(x) + vb(x), v g_2(x) \right\},
\]

With the same conditions on \( g_1, g_2 \) and \( p_1 \). Now \( b(x) \) is a polynomial in \( \mathbb{F}_p[x] / (x^n - 1) \). Hence we can write
\[
b(x) = b_1(x) + ub_2(x), b_1(x), b_2(x) \in \mathbb{F}_p[x] / (x^n - 1).
\]

Therefore,
\[
C = \left\{ g_1(x) + up_1(x) + vb_1(x), v g_2(x) \right\}.
\]

4. GRAY IMAGES OF CYCLIC CODES OVER \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \)

Before characterizing the binary images of cyclic codes, we recall the definition of quasi-cyclic codes.

**Definition 4.1** Let \( T \) be the cyclic shift on \( (\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p)^n \). We say that a linear code \( C \) is \( s \)-quasi-cyclic if it is invariant under \( T^s \), i.e., \( T^s(C) = C \).

Quasi-cyclic codes have been studied extensively in the literature (see [9]) and good parameters have been obtained.

**Theorem 4.2** Let \( C \) be a cyclic code of length \( n \) over the ring \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \). Then \( \varphi(C) \) is a \( 3 \)-quasi-cyclic linear code of length \( 3n \) over \( \mathbb{F}_p \).

**Proof.** Note that if \( c = (c_0, c_1, \ldots, c_{n-1}) \in C \) with \( c_i = c_{i0} + uc_{i1} + vc_{i2} \) for \( i = 0, 1, \ldots, n-1 \), then
\[
\varphi(c) = \varphi(c_0, c_1, \ldots, c_{n-1}) = (\varphi(c_0), \varphi(c_1), \ldots, \varphi(c_{n-1}))
\]
\[
= (c_{02}, c_{01} + c_{01}, c_{02} + c_{01} + c_{00}, \ldots, c_{n-1,2} + c_{n-1,1} + c_{n-1,0}).
\]

Hence,
\[
T^3 \varphi(c) = (c_{n-1,2} + c_{n-1,1}, c_{n-1,0}, c_{n-1,1}, c_{n-1,2} + c_{n-1,0}, c_{02},
\]
\[
c_{01} + c_{01}, c_{00}, \ldots, c_{n-2,2}, c_{n-2,1} + c_{n-2,0}.
\]

(4.1)

We know that \( C \) is a cyclic code over \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \) if and only if \( T(C) = C \). By \( c = (c_0, c_1, \ldots, c_{n-1}) \in C \), we know
\[
T(c) = (c_{n-1,1}, c_{n-1,0}, \ldots, c_{n-2,0}) \equiv C \in C.
\]

Therefore,
\[
\varphi(T(c)) = \varphi(T(c)) = (\varphi(c_{n-1,1}), \varphi(c_{n-1,0}), \varphi(c_{n-1,1}), \varphi(c_{n-1,2})\]
\[
= (c_{n-1,2} + c_{n-1,1}, c_{n-1,0}, c_{n-1,1}, c_{n-1,2} + c_{n-1,0}, c_{02},
\]
\[
c_{01} + c_{01}, c_{00}, \ldots, c_{n-2,2}, c_{n-2,1} + c_{n-2,0}.
\]
\[
(4.2)
\]

Combining (4.1) with (4.2), we obtain
\[
\varphi(T(c)) = \varphi(T(c)) = T^3(\varphi(C)).
\]

Which implies that \( \varphi(C) \) is invariant under \( T^3 \). This proves that \( \varphi(C) \) is a \( 3 \)-quasi-cyclic code linear code of length \( 3n \) over \( \mathbb{F}_p \).

**CONCLUSION**

We have characterized cyclic codes over \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \) and proved that the Gray images of cyclic codes over \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \) are \( 3 \)-quasi-cyclic binary linear codes over \( \mathbb{F}_p \). We believe that some better codes can be obtained as the images of cyclic codes over the ring \( \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p \).

Another direction for research in this topic is of the generalization \( F_q + uF_q + vF_q \) of \( F_p + uF_p + vF_p \), where \( q \) is a prime power.

**CONFLICT OF INTEREST**

The author confirms that this article content has no conflict of interest.

**ACKNOWLEDGEMENTS**

The author is supported by the Natural Science Foundation of Hubei Polytechnic University (11yjz377B) and the Teaching Research Foundation of Hubei Polytechnic University (2013A04). The authors are grateful to the referees.
Cyclic Codes of Length $n$ Over $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p$

Their suggestions were valuable to create an improved final version.

REFERENCES


