(1 + u^2) - CYCLIC AND CYCLIC CODES OVER 
\[ \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 \]

HUA LIANG and YUAN-SHENG TANG

Department of Mathematics
Huaiyin Teachers College
Huaian 223300, Jiangsu
P. R. China
e-mail: lianghuawq@163.com

School of Mathematical Science
Yangzhou University
Yangzhou 225002, Jiangsu
P. R. China

Abstract

By constructing a Gray map \( \Phi \), (1 + u^2) - cyclic and cyclic codes over the ring 
\[ R = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 \] are studied. We prove that \( C \) is a (1 + u^2) - cyclic code of length \( n \) over \( R \), if and only if \( \Phi(C) \) is a quasi-cyclic code over \( \mathbb{F}_2 \) of index 2 and of length \( 4n \). We also prove that, if \( n \) is odd, then every binary code which is the Gray image of a linear cyclic code of length \( n \) over \( R \) is equivalent to a linear quasi-cyclic code over \( \mathbb{F}_2 \) of index 2 and length \( 4n \).

1. Introduction

There has been tremendous interest and research in codes over finite rings, especially the ring \( \mathbb{Z}_4 \), in recent years. Codes over \( \mathbb{Z}_4 \) are linked
to binary code via the Gray map. In [7], Wolfmann showed that the Gray image of a linear negacyclic code over $\mathbb{Z}_4$ of length $n$ is a distance-invariant (not necessary linear) cyclic code. He also showed that, for odd $n$, the Gray image of a linear cyclic code over $\mathbb{Z}_4$ of length $n$ is equivalent to a binary cyclic code. Codes over $\mathbb{F}_2 + u\mathbb{F}_2$ also have been discussed by a number of authors. In [3], Bonnecaze and Udaya studied cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. Qian and et al. [5] have studied cyclic code of odd length over $\mathbb{F}_2 + u\mathbb{F}_2$. Recently, Abualrub and Siap [1] studied $(1 + u)$-cyclic code of arbitrary length over $\mathbb{F}_2 + u\mathbb{F}_2$.

In this paper, by constructing a Gray map $\Phi$, we prove that, if $n$ is odd, the Gray image of a linear cyclic code of length $n$ over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ is equivalent to a cyclic code of length $4n$ over $\mathbb{F}_2$.

2. Preliminaries

Let $R$ be the commutative ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 := \mathbb{F}_2[u]/(u^3)$, where $u^3 = 0$. The binary field $\mathbb{F}_2$ is a subring of $R$. The element of $R$ may be written as $0, 1, u, 1 + u, u^2, 1 + u^2, u + u^2$, and $1 + u + u^2$.

We emphasize that, throughout this paper, $R$ denotes the commutative ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$.

**Definition 2.1.** For any $\lambda \in R \setminus \{0\}$, let $\nu_\lambda$ be the map from $R^n$ to $R^n$, given by

$$
\nu_\lambda(r_0, r_1, \ldots, r_{n-1}) = (\lambda r_{n-1}, r_0, r_1, \ldots, r_{n-2}).
$$

**Definition 2.2.** Let $\overline{R}$ be a commutative ring, and $m$ be a positive integer. Then the shift $\sigma$ of $\overline{R}^m$ is the permutation defined by

$$
\sigma(q_0, q_1, \ldots, q_{m-1}) = (q_{m-1}, q_0, q_1, \ldots, q_{m-2}),
$$

and for any positive integer $s$, let

$$
\sigma^{\otimes s} : \overline{R}^{ms} \rightarrow \overline{R}^{ms},
$$
A linear code of length $n$ over $R$ is a $R$-submodule of $R^n$. A cyclic code of length $n$ over $R$ is a subset $C$ of $R^n$ such that $\sigma(C) = C$. A code $C$ over $R$ satisfying $\nu_x(C) = C$ is called a constacyclic code, or a $\lambda$-cyclic code, while a code $C'$ over $\tilde{R}$ satisfying $\sigma^{s}(C') = C'$ is called a quasi-cyclic code of index $s$ and of length $ms$. A 1-cyclic code is a cyclic code. A quasi-cyclic code of index 1 is a cyclic code.

In this paper, a cyclic, constacyclic, quasi-cyclic code need not be linear.

Let $C$ be a code of length $n$ over $R$, and $P(C)$ be its polynomial representation, i.e.,

$$P(C) = \left\{ \sum_{i=0}^{n-1} r_i x^i \middle| (r_0, r_1, \ldots, r_{n-1}) \in C \right\}.$$  

It is easy to prove that:

**Proposition 2.3.** (1) A subset $C$ of $R^n$ is a linear cyclic code of length $n$, if and only if $P(C)$ is an ideal of $R[x]/(x^n - 1)$.

(2) A subset $C$ of $R^n$ is a linear $\lambda$-cyclic code of length $n$, if and only if $P(C)$ is an ideal of $R[x]/(x^n - \lambda)$.

The following proposition is analogy of Proposition 2.3 [7], the proof is also similar, so we omit it here.

**Proposition 2.4.** Let $\mu$ be the map of $R[x]/(x^n - 1)$ into $R[x]/(x^n - (1 + u^2))$ defined by $\mu(a(x)) = a((1 + u^2)x)$. 

If \( n \) is odd, then \( \mu \) is a ring isomorphism. Hence, a subset \( I \) of \( R[x]/(x^n - 1) \) is an ideal, if and only if \( \mu(I) \) is an ideal of \( R[x]/(x^n - (1 + u^2)) \).

Let \( \tilde{\mu} \) be the map:

\[
\tilde{\mu} : R^n \to R^n, \quad (r_0, r_1, \ldots, r_{n-1}) \mapsto (r_0, (1 + u^2)r_1, (1 + u^2)^2r_2, \ldots, (1 + u^2)^{n-1}r_{n-1}).
\]

The following corollary is now an immediate consequence of Propositions 2.3 and 2.4.

**Corollary 2.5.** Let \( n \) be odd, then \( C \subseteq R^n \) is a linear cyclic code, if and only if \( \tilde{\mu}(C) \) is a linear \((1 + u^2)\)-cyclic code.

### 3. Gray Map

Every element \( c \in R^n \) can be expressed uniquely as \( c = x + uy + u^2z \), where \( x, y, \) and \( z \) are in \( F_2^n \).

**Definition 3.1.** The Gray map \( \Phi \) from \( R \) to \( F_2^3 \) is given by

\[
\Phi(r) = (a_3, a_3 + a_1, a_3 + a_2, a_3 + a_2 + a_1),
\]

where \( r = a_1 + u a_2 + u^2 a_3 \) is in \( R \), and \( a_1, a_2, a_3 \) are in \( F_2 \).

The Gray map can be extended to \( R^n \) in a natural way, for \( c = x + uy + u^2z \in R^n \), let

\[
\Phi(c) = (z, z + x, z + y, z + y + x),
\]

where \( x = (x_0, x_1, \ldots, x_{n-1}), y = (y_0, y_1, \ldots, y_{n-1}), z = (z_0, z_1, \ldots, z_{n-1}) \in F_2^n \).

It is easy to see that \( \Phi \) is injective and linear.

**Proposition 3.2.** Let \( \lambda = 1 + u^2 \). Then \( \Phi \nu_{\lambda} = \sigma^{\otimes 2} \Phi \).
(1 + u^2). CYCLIC AND CYCLIC CODES OVER $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$

**Proof.** Let $r = (r_0, r_1, \ldots, r_{n-1}) = x + uy + u^2z$ be in $R^n$, where $x = (x_0, x_1, \ldots, x_{n-1}), y = (y_0, y_1, \ldots, y_{n-1}), z = (z_0, z_1, \ldots, z_{n-1}) \in \mathbb{F}_2^n$. From definitions, we obtain

$$\Phi(r) = (z, z + x, z + y, z + y + x)$$

$$= (z_0, \ldots, z_{n-1}, z_0 + x_0, \ldots, z_{n-1} + x_{n-1}, z_0 + y_0, \ldots, z_{n-1} + y_{n-1}, z_0 + y_0 + x_0, \ldots, z_{n-1} + y_{n-1} + x_{n-1}),$$

and

$$\sigma^{u^2}(\Phi(r)) = (z_{n-1} + x_{n-1}, z_0, \ldots, z_{n-1}, z_0 + x_0, \ldots, z_{n-2} + x_{n-2}, z_{n-1} + y_{n-1} + x_{n-1}, z_0 + y_0 + x_0, \ldots, z_{n-1} + y_{n-1} + x_{n-1}).$$

Let $\lambda = 1 + u^2$. Then

$$\nu_{\lambda}(r) = ((1 + u^2)r_{n-1}, r_0, r_1, \ldots, r_{n-2})$$

$$= (x_{n-1} + uy_{n-1} + u^2(z_{n-1} + x_{n-1}), x_0 + uy_0 + u^2z_0, \ldots, x_{n-2} + uy_{n-2} + u^2z_{n-2}).$$

From Definition 3.1, we have

$$\Phi(\nu_{\lambda}(r)) = (z_{n-1} + x_{n-1}, z_0, \ldots, z_{n-1}, z_0 + x_0, \ldots, z_{n-2} + x_{n-2}, z_{n-1} + y_{n-1} + x_{n-1}, z_0 + y_0 + x_0, \ldots, z_{n-2} + y_{n-2} + y_{n-2}, z_{n-1} + y_{n-1}, z_0 + y_0 + x_0, \ldots, z_{n-1} + y_{n-1} + x_{n-1}).$$

So, $\Phi(\nu_{\lambda}(r)) = \sigma^{u^2}(\Phi(r))$. \qed

4. Binary Images of (1 + u^2)-Cyclic and Cyclic Codes Over R

**Theorem 4.1.** A code $C$ of length $n$ over $R$ is a $(1 + u^2)$-cyclic code, if and only if $\Phi(C)$ is a quasi-cyclic code over $\mathbb{F}_2$ of index 2 and of length $4n$. 
Proof. Let \( \lambda = 1 + u^2 \). If \( C \) is a \((1 + u^2)\)-cyclic code of length \( n \) over \( R \), then \( \nu_{\lambda}(C) = C \). It follows from Proposition 3.2 that \( \sigma^{\otimes 2}(\Phi(C)) = \Phi(\nu_{\lambda}(C)) = \Phi(C) \), so \( \Phi(C) \) is a quasi-cyclic code over \( F_2 \) of index 2 and of length \( 4n \). Conversely, if \( \Phi(C) \) is a quasi-cyclic code over \( F_2 \) of index 2 and of length \( 4n \), then it follows from Proposition 3.2 that \( \Phi(\nu_{\lambda}(C)) = \sigma^{\otimes 2}(\Phi(C)) = \Phi(C) \), so \( \nu_{\lambda}(C) = C \), since \( \Phi \) is injective.

Using Corollary 2.5 and Theorem 4.1, we obtain the following result.

**Corollary 4.2.** Let \( n \) be odd. If \( C \subseteq R^n \) is a linear cyclic code, then \( \Phi(\tilde{\mu}(C)) \) is a linear quasi-cyclic code over \( F_2 \) of index 2 and of length \( 4n \).

**Definition 4.3.** Let \( \tau \) be the following permutation of \( \{0, 1, \ldots, 4n - 1\} \) with \( n \) odd:

\[
\tau = (1, n + 1)(3, n + 3) \cdots (2i + 1, n + 2i + 1) \cdots (n - 2, 2n - 2)(2n + 1, 3n + 1) \cdots (2n + 3, 3n + 3) \cdots (2n + 2i + 1, 3n + 2i + 1) \cdots (3n - 2, 4n - 2).
\]

Let \( \pi \) be the permutations on \( F_2^{4n} \), given by

\[
\pi(a_0, a_1, \ldots, a_{4n-1}) = (a_{\tau(0)}, a_{\tau(1)}, \ldots, a_{\tau(4n-1)}).
\]

**Proposition 4.4.** Assume \( n \) is odd. Then \( \Phi\tilde{\mu} = \pi\Phi \).

Proof. Let \( r = (r_0, r_1, \ldots, r_{n-1}) = x + uy + u^2z \) be in \( R^n \), where

\[
x = (x_0, x_1, \ldots, x_{n-1}), \quad y = (y_0, y_1, \ldots, y_{n-1}), \quad z = (z_0, z_1, \ldots, z_{n-1}) \in F_2^n.
\]

Then,

\[
\pi(\Phi(r)) = \pi(z_0, \ldots, z_{n-1}, z_0 + x_0, \ldots, z_{n-1} + x_{n-1}, z_0 + y_0, \ldots, z_{n-1} + y_{n-1}, z_0 + x_0, \ldots, z_{n-1} + y_{n-1} + x_{n-1})
\]

\[
= (z_0, z_1 + x_1, z_2, z_3 + x_3, z_4, \ldots, z_{n-2} + x_{n-2}, z_{n-1}, z_0 + x_0, z_1, z_2 + x_2, z_3, z_4 + x_4, \ldots, z_{n-2}, z_{n-1} + x_{n-1}, z_0 + y_0, z_1 + y_1 + x_1, z_2 + y_2, z_3 + y_3 + x_3, \ldots, z_{n-2} + y_{n-2} + x_{n-2}, z_{n-1} + y_{n-1}, z_0 + y_0 + x_0, z_1 + y_1, z_2 + y_2 + x_2, z_3 + y_3, \ldots, z_{n-2} + y_{n-2}, z_{n-1} + y_{n-1} + x_{n-1}).
\]
(1 + u^2). CYCLIC AND CYCLIC CODES OVER \( \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 \)

From
\[
\tilde{\mu}(r) = (r_0, (1 + u^2)r_1, (1 + u^2)^2r_2, \ldots, (1 + u^2)^{n-1}r_{n-1})
\]
\[
= (r_0, (1 + u^2)r_1, (1 + u^2)r_2, \ldots, (1 + u^2)r_{n-2}, r_{n-1})
\]
\[
= (x_0 + u\gamma_0 + u^2z_0, x_1 + u\gamma_1 + u^2(z_1 + x_1), x_2 + u\gamma_2 + u^2z_2, \\
x_3 + u\gamma_3 + u^2(z_3 + x_3), \ldots, x_{n-2} + u\gamma_{n-2} + u^2(z_{n-2} + x_{n-2}),
\]
\[
x_{n-1} + u\gamma_{n-1} + u^2z_{n-1}).
\]
It follows that, if \( \Phi(\tilde{\mu}(r)) = (q_0, q_1, \ldots, q_{4n-1}) \), then for \( 0 \leq j \leq n-1 \):

if \( j \) even: \( q_j = z_j, q_{n+j} = z_j + x_j, q_{2n+j} = z_j + y_j, q_{3n+j} = z_j + y_j + x_j, \)

if \( j \) odd: \( q_j = z_j + x_j, q_{n+j} = z_j, q_{2n+j} = z_j + y_j + x_j, q_{3n+j} = z_j + y_j. \)

We see that \( \Phi(\tilde{\mu}(r)) = \pi(\Phi(r)) \) and, therefore, \( \Phi\tilde{\mu} = \pi \Phi. \)

**Corollary 4.5.** If \( n \) is odd and, if \( \Gamma \) is the Gray image of a linear cyclic code over \( R \) of length \( n \), then \( \pi(\Gamma) \) is a linear cyclic code over \( \mathbb{F}_2 \) of index 2 and length \( 4n. \)

**Proof.** Let \( \Gamma \) be such that \( \Gamma = \Phi(C) \), where \( C \) is a linear cyclic code over \( R \). From Proposition 4.4, \( (\Phi\tilde{\mu})(C) = (\pi \Phi)(C) = \pi(\Gamma) \). It follows from Corollary 4.2, that \( \pi(\Gamma) \) is a linear quasi-cyclic code over \( \mathbb{F}_2 \) of index 2 and length \( 4n. \)

Recall that two codes \( \Gamma \) and \( \Delta \) of length \( m \) over \( \mathbb{F}_2 \) are said to be equivalent, if there exists a permutation \( \omega \) of \( \{0, 1, 2, \ldots, m-1\} \) such that \( \Delta = \omega(\Gamma) \), where \( \omega \) is the permutation of \( \mathbb{F}_2^m \), such that
\[
\omega(a_0, a_1, \ldots, a_{m-1}) = (a_{\omega(0)}, a_{\omega(1)}, \ldots, a_{\omega(m-1)}).
\]
Obviously, a consequence of the previous result now is
Theorem 4.6. If \( n \) is odd, then the Gray image of a linear cyclic code over \( R \) of length \( n \) is equivalent to a linear cyclic code over \( \mathbb{F}_2 \) of index 2 and length \( 4n \).

5. Conclusion

In this paper, we studied \((1 + u^2)\)-cyclic and cyclic codes over \( \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 \) and characterized codes over \( \mathbb{F}_2 \), which are the Gray images of \((1 + u^2)\)-cyclic and cyclic codes over \( \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 \). An interesting question is to study constacyclic and cyclic codes over \( \mathbb{F}_p + u\mathbb{F}_p + \cdots + u^k\mathbb{F}_p \), where \( k \) is a position integer and \( p \) is a prime number.

References


