Journal of Mathematical Sciences: Advances and Applications
Volume 4, Number 1, 2010, Pages 153-160

$(1 + u^2)$- 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 Φ, $(1 + u^2)$- 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 4_n.

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

2010 Mathematics Subject Classification: 94B05, 94B15.

Keywords and phrases: cyclic code, constacyclic code, quasi-cyclic codes, Gray map, permutation.

Received August 9, 2009

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 Φ, 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 ν_λ be the map from R^n to R^n, given by

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

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

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

and for any positive integer s, let

$$\sigma^{\otimes s} : \overline{R}^{ms} \to \overline{R}^{ms},$$

$$(a^{(1)}|a^{(2)}|\cdots|a^{(s)}) \to (\sigma(a^{(1)})|\sigma(a^{(2)})|\cdots|\sigma(a^{(s)})),$$

where $a^{(1)}, a^{(2)}, \cdots, a^{(s)} \in \overline{R}^m$. In particular, $\sigma^{\otimes 1} = \sigma$.

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 $\nu_\lambda(C) = C$ is called a constacyclic code, or a λ-cyclic code, while a code C' over $\overline{R}$ satisfying $\sigma^{\otimes s}(C') = C'$ 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.,

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

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 λ-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 μ 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 μ 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:

$$\tilde{\mu} : R^n \to R^n,$$

$$(r_0, r_1, \cdots, r_{n-1}) \to (r_0, (1+u^2)r_1, (1+u^2)^2 r_2, \cdots, (1+u^2)^i r_i, \cdots, (1+u^2)^{n-1} r_{n-1}).$$

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 $c = x + uy + u^2 z$, where x, y, and z are in $\mathbb{F}_2^n$.

Definition 3.1. The Gray map Φ from R to $\mathbb{F}_2^4$ is given by

$$\Phi(r) = (a_3, a_3 + a_1, a_3 + a_2, a_3 + a_2 + a_1),$$

where $r = a_1 + ua_2 + u^2 a_3$ is in R, and a_1, a_2, a_3 are in $\mathbb{F}_2$.

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

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

where $x = (x_0, x_1, \cdots, x_{n-1})$, $y = (y_0, y_1, \cdots, y_{n-1})$, $z = (z_0, z_1, \cdots, z_{n-1}) \in \mathbb{F}_2^n$.

It is easy to see that Φ is injective and linear.

Proposition 3.2. *Let $\lambda = 1 + u^2$. Then $\Phi\nu_\lambda = \sigma^{\otimes 2}\Phi$.*

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

$$\begin{aligned}\Phi(r) &= (z, z + x, z + y, z + y + x)\\ &= (z_0, \cdots, z_{n-1}, z_0 + x_0, \cdots, z_{n-1} + x_{n-1}, z_0 + y_0, \cdots,\\ &\quad z_{n-1} + y_{n-1}, z_0 + y_0 + x_0, \cdots, z_{n-1} + y_{n-1} + x_{n-1}),\end{aligned}$$

and

$$\begin{aligned}\sigma^{\otimes 2}(\Phi(r)) &= (z_{n-1} + x_{n-1}, z_0, \cdots, z_{n-1}, z_0 + x_0, \cdots,\\ &\quad z_{n-2} + x_{n-2}, z_{n-1} + y_{n-1} + x_{n-1}, z_0 + y_0, \cdots, z_{n-1} + y_{n-1},\\ &\quad z_0 + y_0 + x_0, \cdots, z_{n-2} + y_{n-2} + x_{n-2}).\end{aligned}$$

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

$$\begin{aligned}\nu_\lambda(r) &= ((1 + u^2)r_{n-1}, r_0, r_1, \cdots, r_{n-2})\\ &= (x_{n-1} + uy_{n-1} + u^2(z_{n-1} + x_{n-1}), x_0 + uy_0 + u^2 z_0, \cdots,\\ &\quad x_{n-2} + uy_{n-2} + u^2 z_{n-2}).\end{aligned}$$

From Definition 3.1, we have

$$\begin{aligned}\Phi(\nu_\lambda(r)) &= (z_{n-1} + x_{n-1}, z_0, \cdots, z_{n-2}, z_{n-1}, z_0 + x_0, \cdots, z_{n-2} + x_{n-2},\\ &\quad z_{n-1} + y_{n-1} + x_{n-1}, \; z_0 + y_0, \cdots, z_{n-2} + y_{n-2}, z_{n-1} + y_{n-1},\\ &\quad z_0 + y_0 + x_0, \cdots, z_{n-2} + y_{n-2} + x_{n-2}).\end{aligned}$$

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

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 $\mathbb{F}_2$ of index 2 and of length $4n$. Conversely, if $\Phi(C)$ is a quasi-cyclic code over $\mathbb{F}_2$ 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 Φ 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 $\mathbb{F}_2$ of index 2 and of length $4n$.*

Definition 4.3. Let τ be the following permutation of $\{0, 1, \cdots, 4n - 1\}$ with n odd:

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

Let π be the permutations on $\mathbb{F}_2^{4n}$, given by

$$\pi(a_0, a_1, \cdots, a_{4n-1}) = (a_{\tau(0)}, a_{\tau(1)}, \cdots, a_{\tau(4n-1)}).$$

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

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

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

$= (z_0, z_1 + x_1, z_2, z_3 + x_3, z_4, \cdots, z_{n-2} + x_{n-2}, z_{n-1}, z_0 + x_0, z_1, z_2 + x_2, z_3, z_4 + x_4, \cdots, z_{n-2}, z_{n-1} + x_{n-1}, z_0 + y_0, z_1 + y_1 + x_1, z_2 + y_2, z_3 + y_3 + x_3, \cdots, z_{n-2} + y_{n-2} + x_{n-2}, z_{n-1} + y_{n-1}, z_0 + y_0 + x_0, z_1 + y_1, z_2 + y_2 + x_2, z_3 + y_3, \cdots, z_{n-2} + y_{n-2}, z_{n-1} + y_{n-1} + x_{n-1})$.

From

$$\widetilde{\mu}(r) = (r_0, (1+u^2)r_1, (1+u^2)^2 r_2, \cdots, (1+u^2)^i r_i, \cdots, (1+u^2)^{n-1} r_{n-1})$$

$$= (r_0, (1+u^2)r_1, r_2, (1+u^2)r_3, \cdots, (1+u^2)r_{n-2}, r_{n-1})$$

$$= (x_0 + uy_0 + u^2 z_0, x_1 + uy_1 + u^2(z_1 + x_1), x_2 + uy_2 + u^2 z_2,$$

$$x_3 + uy_3 + u^2(z_3 + x_3), \cdots, x_{n-2} + uy_{n-2} + u^2(z_{n-2} + x_{n-2}),$$

$$x_{n-1} + uy_{n-1} + u^2 z_{n-1}).$$

It follows that, if $\Phi(\widetilde{\mu}(r)) = (q_0, q_1, \cdots, q_{4n-1})$, then for $0 \le j \le n-1$:

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 $\Phi(\widetilde{\mu}(r)) = \pi(\Phi(r))$ and, therefore, $\Phi\widetilde{\mu} = \pi\Phi$. □

Corollary 4.5. *If n is odd and, if Γ 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 4_n.*

Proof. Let Γ be such that $\Gamma = \Phi(C)$, where C is a linear cyclic code over R. From Proposition 4.4, $(\Phi\widetilde{\mu})(C) = (\pi\Phi)(C) = \pi(\Gamma)$. 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 Γ and Δ of length m over $\mathbb{F}_2$ are said to be equivalent, if there exists a permutation ω of $\{0, 1, 2, \cdots, m-1\}$ such that $\Delta = \omega(\Gamma)$, where ω is the permutation of $\mathbb{F}_2^m$, such that

$$\omega(a_0, a_1, \cdots, a_{m-1}) = (a_{\omega(0)}, a_{\omega(1)}, \cdots, a_{\omega(m-1)}).$$

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* 4_n.

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

[1] T. Abualrub and I. Siap, Constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, J. Franklin. Inst. 346(5) (2009), 520-529.

[2] M. C. V. Amarra and F. R. Nemenzo, On $(1-u)$-cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$, Appl. Math. Lett. 21 (2008), 1129-1133.

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

[4] S. Ling and J. Blackford, $\mathbb{Z}_{p^{k+1}}$-linear codes, IEEE Trans. Inform. Theory 45 (2002), 2592-2605.

[5] J. F. Qian, L. N. Zhang and S. X. Zhu, $(1+u)$ constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, Appl. Math. Lett. 19 (2006), 820-823.

[6] J. Wolfmann, Binary images of cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 47 (1996), 1773-1779.

[7] J. Wolfmann, Negacyclic and cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 45 (1999), 2527-2532.

■