TWMS J. App. Eng. Math. V.9, N.4, 2019, pp. 876-881

ON GRAY IMAGES OF CONSTACYCLIC CODES OVER THE FINITE RING $\mathbb{F}_2 + u_1\mathbb{F}_2 + u_2\mathbb{F}_2$

MUSTAFA ÖZKAN[1], ABDULLAH DERTLI[2], YASEMIN CENGELLENMIS[1], §

Abstract. We introduce the finite ring $\mathbb{F}_2 + u_1\mathbb{F}_2 + u_2\mathbb{F}_2$, ${u_1}^2 = u_1$, ${u_2}^2 = 0\,, u_1.u_2 = u_2.u_1 = 0$ which is not a finite chain ring. We focus on $(1 + u_2)$-constacyclic codes over $\mathbb{F}_2 + u_1\mathbb{F}_2 + u_2\mathbb{F}_2$ of odd length. We prove that the Gray image of a linear $(1 + u_2)$ -constacyclic code over $\mathbb{F}_2 + u_1\mathbb{F}_2 + u_2\mathbb{F}_2$ of odd length n is a quasi-cyclic code of index 4 and length $4n$ over $\mathbb{F}_2$.

Keywords: Constacylic code, Gray image.

AMS Subject Classification: 94B15

1. Introduction

In [6], Wolfman showed that the Gray image of a linear negacyclic code over Z_4 of length n is distance invariant (not necessarily linear) cyclic code. It was shown that, for odd n, the Gray image of a linear cyclic code over Z_4 of length n is equivalent to a binary cyclic code. In 2006, J.F. Qian et al. introduced linear $(1 + u)$-constacyclic codes and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and characterized codes over $\mathbb{F}_2$ which are the Gray images of $(1 + u)$-constacyclic codes or cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ in [4]. In [1] , they extended the result of [4] to codes over the commutative ring $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ where p is a prime,$k \in \mathrm{N}$ and $u^2 = 0$, In [5], it was introduced $(1 + u^2)$-constacyclic codes or cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, $u^3 = 0$ and characterized codes over $\mathbb{F}_2$ which are the Gray images of $(1 + u^2)$ -constacyclic or cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. In [2], it was introduced $(1-u^m)$-constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + \ldots + u^m\mathbb{F}_2$, $u^{m+1} = 0$ and characterized codes over $\mathbb{F}_2$. In 2011, $(1+v)$-constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ were studied. $(1+v)$ -constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, $u^2 = v^2 = 0\,, u.v - v.u = 0$ of odd length were characterized with the help of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. A new Gray map was defined. It was shown that the image under the Gray map of $(1+v)$-constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ are cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ in [3]. In 2013, X. Xiaofang

[1] Department of Mathematics, Trakya University, Edirne, Turkey.
e-mail: mustafaozkan22@icloud.com, mustafaozkan@trakya.edu.tr.
ORCID: https://orcid.org/0000-0001-7398-8564.
[2] Department of Mathematics, Ondokuz Mayis University, Samsun, Turkey.
e-mail: abdullah.dertli@gmail.com; ORCID: https://orcid.org/0000-0001-8687-032X.
[1] Department of Mathematics, Trakya University, Edirne, Turkey.
e-mail: ycengellenmis@yahoo.com; ORCID: https://orcid.org/0000-0002-8133-9836.
§ Manuscript received: August 30, 2017; accepted: May 10, 2018.
TWMS Journal of Applied and Engineering Mathematics, Vol.9, No.4

studied $(1+v)$-constacyclic codes over the ring $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2$, $u^2 = v^2 = 0\,, u.v = v.u = 0$, $(1+v)$-constacyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2$ of odd length are characterized with the help of cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2$ in [7].

This paper is organized as follows. In section 2, we give some knowledge about the ring $R = \mathbb{F}_2+u_1\mathbb{F}_2+u_2\mathbb{F}_2$, ${u_1}^2 = u_1$, ${u_2}^2 = 0\,, u_1.u_2 = u_2.u_1 = 0$ and the codes over R . In section 3, we have the relationship between cyclic code over and $(1+u_2)$-constacyclic code over R . In section 4, the Gray image of $(1+u_2)$-constacyclic code over R of odd length is obtained.

2. Preliminaries

The ring $R = \mathbb{F}_2+u_1\mathbb{F}_2+u_2\mathbb{F}_2$ is defined as a chacteristic 2 ring subject to the restrictions ${u_1}^2 = u_1$, ${u_2}^2 = 0\,, u_1.u_2 = u_2.u_1 = 0$. The isomorphism $\mathbb{F}_2+u_1\mathbb{F}_2+u_2\mathbb{F}_2 \cong \mathbb{F}_2[u_1,u_2]/ < u_1^2 = u_1, u_2^2 = 0, u_1u_2 = u_2u_1 = 0 >$ is obvious to see. The elements of R may be written as $0, 1, u_1, u_2, 1+u_1, 1+u_2, u_1+u_2, 1+u_1+u_2$. Addition and multiplication operations over R are given in the following tables :

Table 1

$\oplus$	0	1	u_1	u_2	$1+u_1$	$1+u_2$	u_1+u_2	$1+u_1+u_2$
0	0	1	u_1	u_2	$1+u_1$	$1+u_2$	u_1+u_2	$1+u_1+u_2$
1	1	0	$1+u_1$	$1+u_2$	u_1	u_2	$1+u_1+u_2$	u_1+u_2
u_1	u_1	$1+u_1$	0	u_1+u_2	1	$1+u_1+u_2$	u_2	$1+u_2$
u_2	u_2	$1+u_2$	u_1+u_2	0	$1+u_1+u_2$	1	u_1	$1+u_1$
$1+u_1$	$1+u_1$	u_1	1	$1+u_1+u_2$	0	u_1+u_2	$1+u_2$	u_2
$1+u_2$	$1+u_2$	u_2	$1+u_1+u_2$	1	u_1+u_2	0	$1+u_1$	u_1
u_1+u_2	u_1+u_2	$1+u_1+u_2$	u_2	u_1	$1+u_2$	$1+u_1$	0	1
$1+u_1+u_2$	$1+u_1+u_2$	u_1+u_2	$1+u_2$	$1+u_1$	u_2	u_1	1	0

Table 2

$\otimes$	0	1	u_1	u_2	$1+u_1$	$1+u_2$	u_1+u_2	$1+u_1+u_2$
0	0	0	0	0	0	0	0	0
1	0	1	u_1	u_2	$1+u_1$	$1+u_2$	u_1+u_2	$1+u_1+u_2$
u_1	0	u_1	u_1	0	0	u_1	u_1	0
u_2	0	u_2	0	0	u_2	u_2	0	u_2
$1+u_1$	0	$1+u_1$	0	u_2	$1+u_1$	$1+u_1+u_2$	u_2	$1+u_1+u_2$
$1+u_2$	0	$1+u_2$	u_1	u_2	$1+u_1+u_2$	1	u_1+u_2	$1+u_1$
u_1+u_2	0	u_1+u_2	u_1	0	u_2	u_1+u_2	u_1	u_2
$1+u_1+u_2$	0	$1+u_1+u_2$	0	u_2	$1+u_1+u_2$	$1+u_1$	u_2	$1+u_1$

The units of R can be found to be following $R^* = \{1, 1+u_2\}$. It can be easily find all the ideals of R to be listed as,

$$\{0\} = I_0 \subset I_{u_1} \subset I_{u_1+u_2} \subset R = I_{1+u_2}$$
$$\{0\} = I_0 \subset I_{u_2} \subset I_{1+u_1} = I_{1+u_1+u_2} \subset R = I_{1+u_2}$$

R is not a finite chain ring. It has got two maximal ideals, $I_{u_1+u_2}$ and I_{u_1} . It is semi local ring. Morever, R is principal ring. We take R to be a natural extension of the ring

$R_2 = \mathbb{F}_2 + u_2\mathbb{F}_2$, ${u_2}^2 = 0$. The elements of R_2 may be written as $0, 1, u_2, 1+u_2$ where 1 and $1+u_2$ are only units in R_2. R_2 has three ideals $(0), (1)$ and (u_2).

A linear code C over R(or R_2) of length n is a R (or R_2) submodule of R^n (or ${R_2}^n$). A linear code C over $\mathbb{F}_2$ of length n is a $\mathbb{F}_2$ subvector space ${\mathbb{F}_2}^n$. An element of C is called a codeword . Each codeword c in such a code C is an n-tuple of the form $c = (c_o, c_1, ..., c_{n-1}) \in R^n$ (or ${R_2}^n$, $\mathbb{F}_2^n$) and can be represented by

$$c = (c_0, c_1, ..., c_{n-1}) \longleftrightarrow c(x) = \sum_{i=0}^{n-1} c_i x^i \in R[x] \text{ (or } R_2[x] \text{ , } \mathbb{F}_2[x] \text{).}$$

The Gray map Φ_1 on R is given by

$$\Phi_1 : R \longrightarrow R_2^2$$

$$a + u_1 b + u_2\, c \mapsto \Phi_1(a + u_1 b + u_2 c) = \Phi_1(r + u_1 q) = (u_2.r, q)$$

where $r = a + u_2 c$ and $q = b + u_2 c$. We will extend Φ_1 to R^n naturally as follows $\Phi_1(c_0, c_1, ..., c_{n-1}) = (u_2.r_0, u_2.r_1, ..., u_2.r_{n-1}, q_0, q_1, ..., q_{n-1})$ where $c_i = r_i + u_2.q_i$ for all $i = 0, 1, ..., n-1$.

The Gray map Φ_2 on R_2 is given by

$$\Phi_2 : R_2 \longrightarrow \mathbb{F}_2^2$$

$$s + u_2 t \mapsto (s, t)$$

where $s, t \in \mathbb{F}_2$. We will extend Φ_2 to R_2^n naturally as follows

$$\Phi_2 : R_2^n \longrightarrow \mathbb{F}_2^{2n}$$

$$(c_0, ..., c_{n-1}) \mapsto (s_0, ..., s_{n-1}, t_0, ..., t_{n-1})$$

where $c_i = s_i + u_2.t_i$, $s_i, t_i \in \mathbb{F}_2$ for all $i = 0, 1, ..., n-1$.

The weight $w_1(r)$ of $r \in R$ is given by

$$w_1(r) = \begin{cases} 0 \ ; \ r = 0 \\ 1 \ ; \ r = 1, u_1, u_2 \\ 2 \ ; \ r = 1 + u_1, 1 + u_2, u_1 + u_2 \\ 3 \ ; \ r = 1 + u_1 + u_2 \end{cases}$$

This extends to a weight function in R^n. If $r = (r_0, r_1, ..., r_{n-1}) \in R^n$ then $w_1(r)$ $= \sum_{i=0}^{n-1} w_1(r_i)$. The distance $d_1(x, y)$ between any distinct vectors $x, y \in R^n$ is defined to be $w_1(x - y)$. The d_1 minimum distance of C is defined as $d_1(C) = \min\{d_1(x, y)\}$ for any $x, y \in C$, $x \neq y$.

The weight $w_2(t)$ of $t \in R_2$ is given by

$$w_2(t) = \begin{cases} 0 \ ; \ t = 0 \\ 1 \ ; \ t = 1, u_2 \\ 2 \ ; \ t = 1 + u_2 \end{cases}$$

This extends to a weight function in R_2^n . If $t = (t_o, t_1, ..., t_{n-1}) \in R_2^n$ then $w_2(t)$= $\sum_{i=0}^{n-1} w_2(t_i)$. The distance $d_2(x, y)$ between any distinct vectors $x, y \in R_2^n$ is defined to be $w_2(x - y)$. The d_2 minimum distance of C is defined as $d_2(C) = \min\{d_2(x, y)\}$ for any $x, y \in C$, $x \neq y$.

Let C be a code over $\mathbb{F}_2$ of length n and let $c = (c_0, c_1, ..., c_{n-1})$ be a codeword of C. The Hamming weight of C is defined as

$$w_H(c) = \sum_{i=0}^{n-1} w_H(c_i)$$

where $w_H(c_i) = 1$ if $c_i = 1$ and $w_H(c_i) = 0$ if $c_i = 0$. The minimum Hamming distance of C is defined as $d_H = \min\{d_H(c, c')\}$ for any $c, c' \in C, c \neq c'$.

Φ_1 and Φ_2 are distance preserving map from (R^n, d_1) to (R_2^{2n}, d_2) and (R_2^{2n}, d_2) to $(\mathbb{F}_2^{4n}, d_H)$, respectively.

Expressing elements of R as $a + u_1 b + u_2 c = r + u_1 q$ where $r = a + u_2 c$ and $q = b + u_2 c$ are both in R_2, we see that

$$w_1(a + u_1 b + u_2 c) = w_1(r + u_1 q) = w_2(u_2 r, q) = w_H(0, b, a, c)$$

A cyclic shift on R^n is a permutation σ such that

$$\sigma(c_0, c_1, ..., c_{n-1}) = (c_{n-1}, c_0, ..., c_{n-2})$$

A linear code C over R of length n is said to be cyclic code if it is invariant under the cyclic shift $\sigma(C) = C$.

A $(1 + u_2)$-constacyclic shift γ act on R^n as

$$\gamma(c_0, c_1, ..., c_{n-1}) = ((1 + u_2)c_{n-1}, c_0, ..., c_{n-2})$$

A linear code C over R of length n is said to be $(1 + u_2)$-constacyclic code if it is invariant under the $(1 + u_2)$-constacyclic shift $\gamma(C) = C$.

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

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

A code C of length n over R is cyclic if and only if $P(C)$ is an ideal of $R[x]/\langle x^n - 1\rangle$.

A code C of length n over R is $(1 + u_2)$-constacyclic if and only if $P(C)$ is an ideal of $R[x]/\langle x^n - (1 + u_2)\rangle$

Let $a \in R_2^{2n}$ with $a = (a_0, a_1, ..., a_{2n-1}) = (a^{(0)}|a^{(1)})$, $a^{(i)} \in R_2^n$ for all $i = 0, 1$. Let $\sigma^{\otimes 2}$ be the map from R_2^{2n} to R_2^{2n} given by

$$\sigma^{\otimes 2}(a) = \left(\sigma(a^{(0)})|\sigma(a^{(1)})\right)$$

where σ is the usual cyclic shift. A code $\hat{C}$ of length $2n$ over R_2 is said to be quasi-cyclic code of index 2 of $\sigma^{\otimes 2}(\hat{C}) = \hat{C}$.

Let $a \in \mathbb{F}_2^{4n}$ with $a = (a_0, a_1, ..., a_{4n-1}) = (a^{(0)}|a^{(1)}|a^{(2)}|a^{(3)})$, $a^{(i)} \in \mathbb{F}_2^n$ for all $i = 0, 1, 2, 3$. Let $\sigma^{\otimes 4}$ be the map from $\mathbb{F}_2^{4n}$ to $\mathbb{F}_2^{4n}$ given by

$$\sigma^{\otimes 4}(a) = \left(\sigma(a^{(0)})|\sigma(a^{(1)})|\sigma(a^{(2)})|\sigma(a^{(3)})\right)$$

where σ is the usual cyclic shift. A code $\hat{C}$ of length $4n$ over $\mathbb{F}_2$ is said to be quasi-cyclic code of index 4 of $\sigma^{\otimes 4}(\hat{C}) = \hat{C}$.

3. The relationship between Cyclic Codes Over R and $(1 + u_2)$-Constacyclic Codes Over R

Suppose n is odd. Let

$$\begin{array}{rcl} \mu & : & R[x]/\langle x^n - 1\rangle \longrightarrow R[x]/\langle x^n - (1 + u_2)\rangle \\ r(x) & \longmapsto & r((1 + u_2)x) \end{array}$$

The μ is a ring isomorphism. So I is an ideal of $R[x]/\langle x^n - 1\rangle$ if and only if $\mu(I)$ is an ideal of $R[x]/\langle x^n - (1 + u_2)\rangle$.

If $\overline{\mu}$ is given as follows,

$$\begin{aligned} \overline{\mu} &: R^n \longrightarrow R^n \\ r &= (r_0, ..., r_{n-1}) = (r_0, (1+u_2)r_1 ..., (1+u_2)^{n-1} r_{n-1}) \end{aligned}$$

then we have,

Proposition 3.1. *A code C of length n over R is cyclic code if and only if $\overline{\mu}(C)$ is linear $(1+u_2)$-constacyclic code.*

4. $(1+u_2)$-Constacyclic Codes Over R of Odd Length and Their Images

Firstly, we obtained even length quasi-cyclic codes of index 2 over R_2 as the Φ_1 Gray images of $(1+u_2)$-constacyclic codes over R, later we obtained the Φ_2 Gray image of quasi-cyclic code of index 2 over R_2 with length even.

Proposition 4.1. $\sigma^{\otimes 2}\Phi_1 = \Phi_1\gamma$

Proof. Let $c = (c_0, c_1, ..., c_{n-1}) \in R^n$ where $c_i = r_i + u_1 q_i$ for $i = 0, 1, ..., n-1$. If $\Phi_1(c_0, c_1, ..., c_{n-1}) = \Phi_1(r_0+u_1q_0, r_1+u_1q_1, ..., r_{n-1}+u_1q_{n-1}) = (u_2r_0, u_2r_1, ..., u_2r_{n-1}, q_0, ..., q_{n-1})$ then $\sigma^{\otimes 2}\Phi_1(c) = (u_2r_{n-1}, u_2r_0, ..., u_2r_{n-2}, q_{n-1}, q_0, ..., q_{n-2})$.

On the other hand $\gamma(c_0, ..., c_{n-1}) = ((1+u_2)c_{n-1}, c_0, ..., c_{n-2})$ where $(1+u_2)c_{n-1} = r_{n-1}+u_2r_{n-1}+u_1q_{n-1}$. Then $\Phi_1(\gamma(c)) = \Phi_1((r_{n-1}+u_2r_{n-1})+u_1q_{n-1}, r_0+u_1q_0, ..., r_{n-2}+u_1q_{n-2}) = (u_2r_{n-1}, u_2r_0, ..., u_2r_{n-2}, q_{n-1}, q_0, ..., q_{n-2})$. □

Theorem 4.1. *A code C of length n over R is $(1+u_2)$-constacyclic code if and only if $\Phi_1(C)$ is quasi-cyclic code of index 2 and length $2n$ over R_2.*

Proof. Suppose C is $(1+u_2)$-constacyclic code, then $\gamma(C) = C$. By applying Φ_1, we have $\Phi_1(\gamma(C)) = \Phi_1(C)$. By using the Proposition 4.1 , we have $\sigma^{\otimes 2}(\Phi_1(C)) = \Phi_1(\gamma(C)) = \Phi_1(C)$. So $\Phi_1(C)$ is quasi-cyclic code of index 2. Conversely, if $\Phi_1(C)$ is quasi-cyclic code of index 2, then $\sigma^{\otimes 2}(\Phi_1(C)) = \Phi_1(C)$. By using the Proposition 4.1, we have $\sigma^{\otimes 2}(\Phi_1(C)) = \Phi_1(\gamma(C)) = \Phi_1(C)$. Since Φ_1 is injective it follows that $\gamma(C) = C$. □

Now, we will obtain the Φ_2 Gray image of even length quasi-cyclic code of index 2 over R_2.

Proposition 4.2. $\sigma^{\otimes 4}\Phi_2 = \Phi_2\sigma^{\otimes 2}$

Proof. It is proved as in the proof of the Proposition 4.1. □

Theorem 4.2. *A code B length $2n$ over R_2 is quasi-cyclic code of index 2 if and only if $\Phi_2(B)$ is quasi-cyclic code of index 4 over $\mathbb{F}_2$ with length $4n$.*

Proof. It is proved as in the proof of the Theorem 4.1. . □

Corollary

A code C odd length n over R is $(1+u_2)$-constacyclic if and only if $\Phi_2(\Phi_1(C))$ is quasi-cyclic code of index 4 and length $4n$ over $\mathbb{F}_2$.

5. conclusion

It is introduced that the finite ring $\mathbb{F}_2 + u_1\mathbb{F}_2 + u_2\mathbb{F}_2, u_1^2 = u_1, u_2^2 = 0, u_1u_2 = u_2u_1 = 0$. Also, it is obtained that the Gray image of linear $(1+u_2)$-constacyclic code over R of odd length n.

References

[1] M. C. Amarra, F. R. Nemenzo, (2008), On $(1-u)$-cyclic codes over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$, Applied Mathematics Letters, 21, pp. 1129-1133.

[2] Y. Cengellenmis, (2009), On $(1+u^m)$-cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+ ... +u^m\mathbb{F}_2$, Int J.Contemp. Math Sciences, 20 (4), pp. 987-992.

[3] S. Karadeniz, B. Yldz, (2011), On $(1-v)$-constacyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, Journal of the Franklin Institute , 348, pp. 2625-2632.

[4] J.F. Qian, L. N. Zhang, S. X. Zhu, (2006), ($(1+u)$-constacyclic and cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$, Applied Mathematics Letters 19, pp. 820-823.

[5] J. F. Qian, L. N. Zhang, S. X. Zhu, (2006), Constacyclic and cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$, IEICE Trans.Fundamentals, 89-a (6), pp. 1863-1865.

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

[7] Xu Xioafang, (2013), (1+v)-constacyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2$, Computer Engineering and Applications, 49 (12), pp. 77-79.

Mustafa Özkan is a doctor in the Department of Mathematics at Trakya University in Turkey. He received his PhD degree in 2016 from mathematics at Trakya University. He has given talks at international conferences. His research interest is algebraic coding theory.

Abdullah Dertli is a research assistant doctor in the Department of Mathematics, Ondokuz Mays University, Samsun, Turkey. He received his B.Sc. and M.Sc. in Mathematics from Trakya University of Turkey. He received his Ph.D. in mathematics from Ondokuz Mays University of Turkey. His research interests include algebra and coding theory.

Yasemin Cengellenmis got Msci degree in mathematics from Trakya University, Turkey. She received her PhD degree in mathematics from Trakya University. Currently, she is associate professor in the Department of Matematics at Trakya University. Her research area is coding theory.