GRAY IMAGES OF (1+v)-CONSTACYCLIC CODES OVER A PARTICULAR RING

Mustafa Özkan and Figen Öke

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 94B05, 94B15; Secondary 94B60.

Keywords and phrases: Cylic Codes, Gray Map, Codes Over Rings.

Abstract. In this paper the ring $\mathbb{F}_2[u,v]/\langle u^3,v^2,u.v\rangle$ where $u^3=0,v^2=0$, u.v=v.u=0 is defined and (1+v)- constacyclic codes over this ring are studied. It is shown that the Gray image of (1+v)- constacyclic codes with odd order over the ring $\mathbb{F}_2[u,v]/\langle u^3,v^2,u.v\rangle$ is a cyclic code over the ring $\mathbb{F}_2[u]/\langle u^3\rangle$ where $u^3=0$. Also there is a quasicyclic code of index 2 over the binary field.

1 Introduction

Certain Linear codes for example cyclic, constacyclic and quasicyclic codes over the ring \mathbb{Z}_{p^k} and over the all types of finite chain rings were studied before. Gray maps which preserve minimum distance of codes have been defined between these rings and finite fields. Then using this kind map the new codes have been written. Especially; codes over the field \mathbb{F}_2 which are the Gray images of cyclic and constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ where $u^3 = 0$ were studied in [5]. Also (1+v)- constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ where $u^2 = v^2 = 0$, u.v-v.u = 0 were studied in [7]. (1+v)-constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ of odd length were characterized by using cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. X. Xiaofang studied (1+v)-constacyclic codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ where $u^2 = v^2 = 0$, u.v = v.u = 0 in [8].

In this paper the ring $R=\mathbb{F}_2+v\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ where $u^3=0, \ v^2=0, \ u.v=v.u=0$ is defined and the weight function on this ring is given at first. Then the Gray map is defined from the ring R to the ring $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ where $u^3=0$ and using this map the relation between cyclic and constacyclic codes is obtained. Using a Gray map defined from the ring $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ where $u^3=0$ to \mathbb{F}_2 , the relation between (1+v)-constacyclic codes over R and quasicyclic codes over \mathbb{F}_2 is described.

2 Preliminaries

It is known that $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ is a ring with the usual addition and multiplication. Also it is known that this ring is isomorphic to the ring $\mathbb{F}_2[u]/_{<u}^3>$ where $u^3=0$. Writing $R_1=\mathbb{F}_2+v\mathbb{F}_2$ where $v^2=0$ instead of \mathbb{F}_2 the set $R_1+uR_1+u^2R_1$ where $u^3=0$ is obtained. Then we have $R_1+uR_1+u^2R_1=(\mathbb{F}_2+v\mathbb{F}_2)+u.(\mathbb{F}_2+v\mathbb{F}_2)+u^2.(\mathbb{F}_2+v\mathbb{F}_2)=\mathbb{F}_2+v\mathbb{F}_2+u\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$

Let C be a (n, M, d)_code. It means that C has the length n, it has M elements and its minimum distance is d.

Definition 2.1. Let R be a ring. Each submodule C of \mathbb{R}^n is called a linear code with length n over the ring R. If C is a linear code with length n over the field \mathbb{F}_2 , it is a subspace of \mathbb{F}_2^n . Each codeword c in such a code C is a n-tuple of the form $c = (c_0, c_1, ..., c_{n-1}) \in \mathbb{R}^n$ and can be represented by

$$c = (c_o, c_1, ..., c_{n-1}) \leftrightarrow c(x) = \sum_{i=0}^{n-1} c_i . x^i \in R[x]$$

This notation can be written for the elements of the ring R_1^n and \mathbb{F}_2^n similarly. The Gray map from the ring R to R_1^2 is defined as;

$$\Phi: R \to R_1^2 \Phi(a + bv + cu + du^2) = \Phi(r + qv) = (q, q + r)$$

where $r = a + cu + du^2$ and $q = b + au + (a + c)u^2$.

The map Φ can be generalized to \mathbb{R}^n as;

 $\Phi(t_o,t_1,...,t_{n-1})=(q_0,q_1,...,q_{n-1},q_0+r_0,q_1+r_1,...,q_{n-1}+r_{n-1}) \text{ where } t_i=r_i+q_iv \text{ such that } r_i=a_i+c_iu+d_iu^2, \ q_i=b_i+a_iu+(a_i+c_i)u^2 \text{ , for all } i=0,1,...,n-1 \text{ . Note that } t=1,...,n-1$ the Gray map from R_1 to \mathbb{F}_2^4 is defined as ;

$$\Phi_1: R_1 \to \mathbb{F}_2^4 \Phi_1(x + yu + zu^2) = (z, x + z, y + z, x + y + z)$$

The map Φ_1 can be generalized to R_1^n as;

$$\Phi_1: R_1^n \to \mathbb{F}_2^{4n}$$

 $\Phi_1(b_o,b_1,...,b_{n-1}) = (z_o,z_1,...,z_{n-1},x_0+z_o,x_1+z_1,...,x_{n-1}+z_{n-1},y_0+z_o,y_1+z_1,...,y_{n-1}+z_{n-1},x_o+y_0+z_o,x_1+y_1+z_1,...,x_{n-1}+y_{n-1}+z_{n-1})$ where $x_i, y_i, z_i \in \mathbb{F}_2$, for i = 0, 1, ..., n - 1.

The weight function w_R for each element s of $R=\mathbb{F}_2+v\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ is defined as ;

$$w_R(s) = \begin{cases} 0 & ; s = 0 \\ 2 & ; s = 1 + v + u \\ 4 & ; s = u, u + u^2, 1 + v + u + u^2 \\ 6 & ; \text{otherwise} \end{cases}$$

Then $w_R(s) = \sum_{i=0}^{n-1} w_R(s_i)$ is satisfied for each element $s = (s_o, s_1, ..., s_{n-1}) \in \mathbb{R}^n$.

It is known that the Lee weight of each $t \in R_1$ is defined as;

$$w_L(t) = \begin{cases} 0 & ; \ t = 0 \\ 4 & ; \ t = u^2 \\ 2 & ; \ \text{otherwise} \end{cases}$$

Then $w_L(t)=\sum\limits_{i=0}^{n-1}w_L(t_i)$ is satisfied for each element $t=(t_o,t_1,...,t_{n-1})\in R_1^n$. The Hamming weight on \mathbb{F}_2 is defined as $w_H(0)=0$, $w_H(1)=1$. Hence $w_H(c)=1$

 $\sum\limits_{i=0}^{n-1} w_H(c_i)$ is hold for each $c=(c_o,c_1,...,c_{n-1})\in \mathbb{F}_2^n$.

The minimum distance of a code C is defined as;

 $d_R(C) = \min\{d_R(x,y)\}\$, here $x,y \in C$, $x \neq y$ if C is a code over R,

 $d_L(C)=\min\{d_L(x,y)\}$, here $x,y\in C$, $x\neq y$ if C is a code over R_1 and $d_H(C)=\min\{d_H(x,y)\}$, here $x,y\in C$, $x\neq y$ if C is a code over \mathbb{F}_2 . Each element of Ris written as $a+bv+cu+du^2=r+qv$ where $r=a+cu+du^2\in R_1, q=b+au+(a+c)u^2\in R_1$

Thus $w_R(a+bv+cu+du^2) = w_R(r+vq) = w_L(q,q+r) = w_H(a+c,a+c+d,a+b+c,b+c+d,c,d,b+c,a+b+d)$

It is clearly seen that the equalities $w_R(s)=w_L(\Phi(s))=w_H(\Phi_1(\Phi(s)))$ for each $s\in R^n$ are satisfied. Therefore it means that Φ is an isometry from (R^n,d_R) to (R^{2n}_1,d_L) and Φ_1 is an isometry from (R^{2n}_1,d_L) to (\mathbb{F}_2^{8n},d_H) .

A cyclic shift on \mathbb{R}^n is a permutation σ such that

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

A linear code C over R of length n is said to be cyclic code if it is satisfied the equality $\sigma(C)=C$. A (1+v)- constacyclic shift γ acts on R^n as

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

A linear code C over R of length n is said to be (1+v)—constacyclic code if it is satisfied the equality $\gamma(C) = C$.

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

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

Let D be a code of length 2n over R_1 and P(D) be its polynomial representation,

$$P_1(D) = \left\{ \sum_{i=0}^{2n-1} s_i.x^i \mid (s_0, s_1, ..., s_{2n-1}) \in D \right\}.$$

Using these notations we have;

Proposition 2.2. (a) A code C of length n over R is cyclic if and only if P(C) is an ideal of $R[x]/\langle x^n-1\rangle$.

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

A cyclic shift on R_1^{2n} is a permutation τ such that

$$\tau(d_o, d_1, ..., d_{2n-1}) = (d_{2n-1}, d_0, ..., d_{2n-2})$$

Let $D \subseteq R_1^{2n}$ be a linear code. If $\tau(D) = D$ then D is called a cyclic code over R_1 . A $(1+u^2)$ -constacyclic shift on R_1^{2n} is a permutation ν such that

$$\nu(d_0, d_1, ..., d_{2n-1}) = ((1 + u^2).d_{2n-1}, d_0, ..., d_{2n-2})$$

Let $D\subseteq R_1^{2n}$ be a linear code. If $\nu(D)=D$ then D is called a $(1+u^2)$ -constacyclic code over R_1 . Let $C'\subseteq \mathbb{F}_2^{8n}$ be a linear code,

$$\sigma^{\otimes 2} : \mathbb{F}_2^{8n} \to \mathbb{F}_2^{8n}$$

$$\sigma^{\otimes 2}(d_o, d_1, ..., d_{8n-1}) = (d_{4n-1}, d_0, ..., d_{4n-2}, d_{8n-1}, d_{4n}, ..., d_{8n-2}).$$

If $\sigma^{\otimes 2}(C') = C'$ then C' is called a quasicyclic code of index 2 over \mathbb{F}_2 .

Proposition 2.3. (a) A code D of length 2n over R_1 is cyclic if and only if $P_1(D)$ is an ideal of $R_1[x]/\langle x^n-1\rangle$.

(b) A code D of length 2n over R_1 is $(1+u^2)$ -constacyclic if and only if $P_1(D)$ is an ideal of $R_1[x]/\langle x^n-(1+v)\rangle$.

3 Cyclic codes and (1+v)—constacyclic codes over the ring R

The equality $(1+v)^n = (1+v)$ is satisfied when n is an odd and the equality $(1+v)^n = 1$ is satisfied when n is even number. Through this section n is an odd number.

Proposition 3.1. Define
$$\mu: R[x]/\langle x^n-1\rangle \to R[x]/\langle x^n-(1+v)\rangle$$

$$r(x) \mapsto r((1+v)x)$$

 μ is a ring isomorphism when n is an odd number.

Proof. Remember that $(1+v)^n = (1+v)$ when n is an odd number.

Let $a(x) \equiv b(x) \pmod{x^n-1}$. It is clear that $a(x)-b(x)=(x^n-1).q(x)$, $q(x) \in R[x]$ and writing (1+v).x instead of x it is obtained that

$$a((1+v).x) - b((1+v).x) = ((1+v)^n.x^n - 1).q((1+v).x), q((1+v).x) \in R[x]$$

$$=((1+v).x^n-1).q((1+v).x)$$

$$=((1+v).x^n-(1+v)^2).q((1+v).x)=(1+v).(x^n-(1+v)).q((1+v).x)=(x^n-(1+v)).q((1+v).x).(1+v)=(x^n-(1+v)).p(x)\;,\;p(x)\in R[x].$$
 Then $a((1+v).x)\equiv b((1+v).x)\pmod{(x^n-(1+v))}$.

Therefore we have;

Corollary 3.2. I is an ideal of $R[x]/\langle x^n-1\rangle$ if and only if $\mu(I)$ is an ideal of $R[x]/\langle x^n-(1+v)\rangle$.

Proposition 3.3. Define the map $\overline{\mu}: R^n \to R^n$

$$(r_o, r_1, ..., r_{n-1}) \mapsto (r_o, (1+v).r_1, ..., (1+v)^i.r_i, (1+v)^{n-1}r_{n-1})$$

A code C of length n over R is a cyclic code if and only if $\bar{\mu}$ is a linear (1+v)-constacyclic code.

4 Gray images of the codes over the ring R

In this section firstly it will be shown that the Gray image of a (1+v)-constacyclic code over R is a cyclic code with even lenght. Secondly it will be shown that the Gray image of a $(1+u^2)$ -constacyclic code over R_1 is a quasicyclic code with even length.

Proposition 4.1. Let γ be a (1+v)-constacyclic shift on R^n and τ be a cyclic shift on R_1^{2n} . If Φ is a Gray map from R^n to R_1^{2n} which is defined before, then $\Phi \cdot \gamma = \tau \cdot \Phi$ is satisfied.

Proof. Let
$$c = (c_0, c_1, ..., c_{n-1}) \in R^n$$
 where $c_i = r_i + q_i v$ for $0 \le i \le n-1$.
 If $\Phi(c) = \Phi(c_0, c_1, ..., c_{n-1}) = \Phi(r_0 + q_0 v, r_1 + q_1 v, ..., r_{n-1} + q_{n-1} v)$

$$= (q_0, q_1, ..., q_{n-1}, q_0 + r_0, q_1 + r_1, ..., q_{n-1} + r_{n-1})$$

then
$$tau(\Phi(c)) = \tau(q_0, q_1, ..., q_{n-1}, q_0 + r_0, q_1 + r_1, ..., q_{n-1} + r_{n-1})$$

= $(q_{n-1} + r_{n-1}, q_0, q_1, ..., q_{n-1}, q_0 + r_0, ..., q_{n-2} + r_{n-2})$

On the other hand, $\gamma(c)=\gamma(c_0,c_1,...,c_{n-1})=((1+v).c_{n-1},c_0,...,c_{n-2})$ where $(1+v).c_{n-1}=r_{n-1}+(q_{n-1}+r_{n-1})v$. Then $\Phi\left(\gamma(c)\right)=\Phi\left(r_{n-1}+(q_{n-1}+r_{n-1})v,r_0+q_0v,q_1,...,r_{n-2}+q_{n-2}v\right)=(q_{n-1}+r_{n-1},q_0,q_1,...,q_{n-1},q_0+r_0,...,q_{n-2}+r_{n-2})$

Theorem 4.2. A code C with length n over R is (1+v)-constacyclic code if and only if $\Phi(C)$ is a cyclic code with length 2n over R_1 .

Proof. Suppose that C is (1+v)—constacyclic code. Then $\gamma(C)=C$. By applying Φ , we have $\Phi(\gamma(C))=\Phi(C)$. By using the Proposition 4.1, we have $\tau(\Phi(C))=\Phi(\gamma(C))=\Phi(C)$. So $\Phi(C)$ is a cyclic code. Conversely, if $\Phi(C)$ is a cyclic code, then $\tau(\Phi(C))=\Phi(C)$. By using the Proposition 4.1, we have $\tau(\Phi(C))=\Phi(\gamma(C))=\Phi(C)$. Since Φ is injective then $\gamma(C)=C$.

Proposition 4.3. Let ν be the $(1+u^2)$ -constacyclic shift on R_1^{2n} and $\sigma^{\otimes 2}$ be the quasicyclic shift on \mathbb{F}_2^{8n} . If Φ_1 is a Gray map from R_1^{2n} to \mathbb{F}_2^{8n} which is defined before, then $\sigma^{\otimes 2}.\Phi_1=\Phi_1.\nu$ is satisfied.

Proof. Let $t=(t_0,t_1,...,t_{n-1})\in R_1^{2n}$ where $t_i=x_i+y_iu+z_iu^2$ for $0\leqslant i\leqslant n-1$. If $\nu(t)=\nu(t_0,t_1,...,t_{2n-1})=((1+u^2).t_{2n-1},t_0,...,t_{2n-2})$ where $(1+u^2).t_{2n-1}=(1+u^2).(x_{2n-1}+y_{2n-1}u+z_{2n-1}u^2)=x_{2n-1}+y_{2n-1}u+(x_{2n-1}+z_{2n-1})u^2$, then $\Phi_1.\nu(t)=\Phi_1((1+u^2).t_{2n-1},t_0,...,t_{2n-2})=\Phi_1(x_{2n-1}+y_{2n-1}u+(x_{2n-1}+z_{2n-1})u^2,x_0+y_0u+z_0u^2,...,x_{2n-2}+y_{2n-2}u+z_{2n-2}u^2)=(x_{2n-1}+z_{2n-1},z_0,z_1,...,z_{2n-1},x_0+z_0,...,x_{2n-2}+z_{2n-2},x_{2n-1}+y_{2n-1}+z_{2n-1},y_0+z_0,...,y_{2n-1}+z_{2n-1},x_0+y_0+z_0,...,x_{2n-2}+y_{2n-2}+z_{2n-2})$ On the other hand, if $\Phi_1(t)=\Phi_1(t_0,t_1,...,t_{2n-1})=(z_0,z_1,...,z_{2n-1},x_0+z_0,...,x_{2n-1}+z_{2n-1},y_0+z_0,...,y_{2n-1}+z_{2n-1},x_0+y_0+z_0,...,x_{2n-1}+z_{2n-1})$ then we have $\sigma^{\otimes 2}.\Phi_1(t)=\sigma^{\otimes 2}(t_0,t_1,...,t_{2n-1})=(z_0,z_1,...,z_{2n-1},x_0+z_0,...,y_{2n-1}+z_{2n-1},x_0+z_0,...,y_{2n-1}+z_{2n-1},x_0+z_0,...,y_{2n-1}+z_{2n-1},x_0+z_0,...,y_{2n-1}+z_{2n-1},x_0+z_0,...,x_{2n-1}+z_{2n-1},x_0+z_0,...,x_{2n-1}+z_{2n-1},x_0+z_0,...,x_{2n-1}+z_{2n-1},x_0+z_0,...,x_{2n-1}+z_{2n-1},x_0+z_0,...,x_{2n-1}+z_{2n-1},x_0+z_0,...,x_{2n-1}+z_{2n-1},x_0+z_0,...,x_{2n-1}+z_{2n-1},x_0+z_0,...,x_{2n-1}+z_{2n-1},x_0+z_0,...,x_{2n-2}+z_{2n-2})$

Theorem 4.4. A code C with length 2n over R_1 is a $(1 + u^2)$ -constacyclic code if and only if $\Phi_1(C)$ is quasicyclic code of index 2, with length 8n over \mathbb{F}_2 .

Proof. If C is $(1+u^2)$ —constacyclic code, $\nu(C)=C$. Then have $\Phi_1(\nu(C))=\Phi_1(C)$ and $\sigma^{\otimes 2}(\Phi_1(C))=\Phi_1(\nu(C))=\Phi_1(C)$ from Proposition 4.3. So $\Phi_1(C)$ is quasicyclic code of index 2. Conversely, if $\Phi_1(C)$ is quasicyclic code of index 2, then $\sigma^{\otimes 2}(\Phi_1(C))=\Phi_1(C)$. By using the Proposition 4.3, we have $\sigma^{\otimes 2}(\Phi_1(C))=\Phi_1(\nu(C))=\Phi_1(C)$. Since Φ_1 is injective then $\nu(C)=C$.

Using the above theories the main conclusion is given below:

Corollary 4.5. A code C with odd length n over R is (1+v)-constacyclic code if and only if $\Phi_1(\Phi(C))$ is quasicyclic code of index 2 and with length 8n over \mathbb{F}_2 .

Conclusion. It is presented the finite ring $R = \mathbb{F}_2 + v\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ where $u^3 = 0$, $v^2 = 0$ and u.v = v.u = 0. It is acquired that the Gray image of linear (1 + v)-constacyclic code over R with length n.

References

- [1] S. Roman, Coding and Information Theory, Graduate Texts in Mathematics, Springer Verlag (1992).
- [2] J.Wolfmann, Negacyclic and cyclic codes over Z4, IEEE Trans. Inf. Theory 45, 2527–2532, (1999).
- [3] S. Ling and J. T. Blackford, $Z_{p^{k+1}}$ _Linear codes, *IEEE Trans. On Inform. Theory* **45**,No **9**, 2592–2605, (2006).
- [4] Q. Jian-Fa, L. N. Zhang and S. X. Zhu, (1+u)- cyclic and cyclic codes over the ring F_2+uF_2 , Applied Mathematics Letters 19, 820–823, (2006).
- [5] Q. Jian-Fa, L. N. Zhang and S. X. Zhu, Constacyclic and cyclic codes over $F_2 + uF_2 + u^2F_2$, *IEICE Trans. Fundamentals* **E89-A**, No19, 1863–1865, (2006).
- [6] P. Udomkavanich and S. Jitman, On the Gray Image of $(1-u^m)$ —Cyclic Codes $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}+\ldots+u^m\mathbb{F}_{p^k}$, Int.J. Contemp. Math. Sciences **4**, No**26**, 1265–1272, (2009).
- [7] S.Karadeniz and B.Yildiz, 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 Institude 348, 2625–2632, (2011).
- [8] X. Xioafang, (1+v)—constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$, Computer Engineering and Applications **49**, No**12**, 77–79, (2013).
- [9] M.Özkan and F. Öke, A relation between Hadamard codes and some special codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *App. Mathematics and Inf. Sci.* 10, No2, 701–704, (2016).
- [10] M.Özkan and F. Öke, Some Special Codes Over $\mathbb{F}_3 + v\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$, Mathematical Sciences and Applications E-Notes 4, No1, 40–44, (2016).

Author information

Mustafa Özkan and Figen Öke, Department of Mathematics, Faculty of Science, Trakya University, 22030-Edirne, TURKEY.

E-mail: mustafaozkan@trakya.edu

Received: February 22, 2016.

Accepted: September 8, 2016.