The Open Automation and Control Systems Journal, 2014, *6*, 788-791

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 $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ 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 $\mathbb{F}_2 + v\mathbb{F}_2$ 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-quasic-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

$$W_L(a+ub+vc) = W_H(c, b+c, a+b+c) \tag{2.1}$$

$\forall a,b,c \in \mathbb{F}_p$. 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 $(\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p)^n$:

$$\varphi(a+ub+vc) = (c, b+c, a+b+c) \tag{2.2}$$

Note that φ extends to a distance-preserving isometry:

$$\varphi:\ ((\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p)^n, \textit{Lee weight}) \to$$

$$(\mathbb{F}^{3n}, \textit{Hamming weight}).$$

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 $[3n,k,d]$ 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 $\dfrac{R[x]}{< x^n - 1 >}$.

Lemma 3.1 ([7]) Let C be a cyclic code over $\mathbb{F}_p + u\mathbb{F}_p$ of length n. Then

*Address correspondence to this author at the 16 Guilin Road(N), Huangshi, Hubei, China. Postcard: 435003; Tel: 15871201946;
E-mail: hwlulu@aliyun.com

1874-4443/14

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

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

$$\psi:\ \frac{(F_p+uF_p+vF_p)[x]}{\langle x^n-1\rangle}\mapsto\frac{(F_p+uF_p)[x]}{\langle x^n-1\rangle},$$

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

$C=\langle g(x)+up_1(x)+vp_2(x), ua_1(x)+vq_1(x), va_2(x)\rangle$ with $a_2\big|a_1\big|g\big|(x^n-1)$ and $a_1(x)\Big|p_1(x)\dfrac{x^n-1}{g(x)}$.

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

$\mathrm{Im}(\psi)=\langle g(x)+up_1(x), ua_1(x)\rangle$,

where g,p_1,a_1 are polynomials in $\dfrac{F_p[x]}{\langle x^n-1\rangle}$ satisfying the conditions $a_1\big|g\big|(x^n-1)$, $a_1(x)\Big|p_1(x)\dfrac{x^n-1}{g(x)}$.

On the other hand, $Ker(\psi)$ 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

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

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

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

$$C_1=\{f_1(x)+uf_2(x)\,\Big|\,\textit{There exists } f_3(x)\in\frac{F_p[x]}{\langle x^n-1\rangle},$$

$\textit{such that } f_1(x)+uf_2(x)+vf_3(x)\in C\}$

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

$\langle g(x)+up_1(x)+vp_2(x), ua_1(x)+vq_1(x), va_2(x)\rangle\subseteq C.$

Conversely, for any $f(x)\in C$, 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

$$f(x)=c(x)[g(x)+up_1(x)]+ud(x)a_1(x)+vf_3(x)$$
$$=c(x)[g(x)+up_1(x)+up_2(x)]+d(x)[ua_1(x)+vq_1(x)]$$
$$+v[f_3(x)-c(x)p_2(x)-d(x)q_1(x)].$$

It is easy to see that $v[f_3(x)-c(x)p_2(x)-d(x)q_1(x)]$ $\in Ker(\psi)=\langle va_2(x)\rangle$. Therefore

$f(x)\in\langle g(x)+up_1(x)+vp_2(x), ua_1(x)+vq_1(x), va_2(x)\rangle$ i.e., $C\subseteq\langle g(x)+up_1(x)+vp_2(x), ua_1(x)+vq_1(x), va_2(x)\rangle$ 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 $\dfrac{F_p[x]}{\langle x^n-1\rangle}$ satisfying the conditions $p_1\big|g_1\big|(x^n-1)$, $g_2(x)\big|(x^n-1)$.

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 $Ker(\psi)$ is v times a cyclic code of over $\mathbb{F}_p$ of odd length n.

By Lemma 3.2, we have

$$\mathrm{Im}(\psi)=\langle g_1(x)+up_1(x)\rangle \tag{3.1}$$

where g_1 and p_1 are binary polynomials with $p_1|g_1|(x^n-1)$ and

$$Ker(\psi)=v\langle g_2(x)\rangle \tag{3.2}$$

Where, g_1 is a binary polynomial with $g_2(x)|(x^n-1)$. Now combining (3.1) with (3.2) we see that we can write

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

With the same conditions on g_1, g_2 and p_1. Now $b(x)$ is a polynomial in $\frac{(\mathbb{F}_p+u\mathbb{F}_p)[x]}{\langle x^n-1\rangle}$. Hence we can write

$$b(x)=b_1(x)+ub_2(x),\ b_1(x),b_2(x)\in\frac{\mathbb{F}_p[x]}{\langle x^n-1\rangle}.$$

Therefore,

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

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 a s-quasi-cyclic if it is invariable 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-quasic-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

$$\varphi(c)=\varphi(c_0,c_1,\ldots,c_{n-1})=(\varphi(c_0),\varphi(c_1),\ldots,\varphi(c_{n-1}))$$
$$=(c_{02},c_{02}+c_{01},c_{02}+c_{01}+c_{00},\ldots,$$
$$c_{n-1,2},c_{n-1,2}+c_{n-1,1},c_{n-1,2}+c_{n-1,1}+c_{n-1,0}).$$

Hence,

$$T^3\varphi(c)=(c_{n-1,2},c_{n-1,2}+c_{n-1,1},c_{n-1,2}+c_{n-1,1}+c_{n-1,0},c_{02},$$
$$c_{02}+c_{01},c_{02}+c_{01}+c_{00},\ldots,c_{n-2,2},c_{n-2,2}+c_{n-2,1},$$
$$c_{n-2,2}+c_{n-2,1}+c_{n-2,0}) \tag{4.1}$$

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

$$T(c)=(c_{n-1},c_0,c_1,\ldots,c_{n-2})\in C.$$

Therefore,

$$\varphi T(c)=\varphi(T(c))=(\varphi(c_{n-1}),\varphi(c_0),\varphi(c_1),\ldots,\varphi(c_{n-2}))$$
$$=(c_{n-1,2},c_{n-1,2}+c_{n-1,1},c_{n-1,2}+c_{n-1,1}+c_{n-1,0},c_{02},$$
$$c_{02}+c_{01},c_{02}+c_{01}+c_{00},\ldots,c_{n-2,2},c_{n-2,2}+c_{n-2,1},$$
$$c_{n-2,2}+c_{n-2,1}+c_{n-2,0}) \tag{4.2}$$

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 $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q$ of $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p$, 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 (11yjz37B) and the Teaching Research Foundation of Hubei Polytechnic University (2013A04). The authors are grateful to the referees.

Their suggestions were valuable to create an improved final version.

REFERENCES

[1] R. Hammans, P. V. Kumar, and A. R. Calderbank, "The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 301-319, 1994.

[2] Z. Shixin, W. Yang, and S. Minjia, "Some results on cyclic codes over $\mathbb{F}_2+v\mathbb{F}_2$," *IEEE Trans. Inform. Theory*, vol. 56, pp. 1680-1684, 2010.

[3] J. Wolfmann, "Nagacylic and cyclic codes over $\mathbb{Z}_4$," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2527-2532, 1999.

[4] J. Wolfmann, "Binary image of cyclic codes over $\mathbb{Z}_4$," *IEEE Trans. Inform. Theory*, vol. 47, pp. 1773-1779, 2001.

[5] T. Abualrub, and I. Siap, "Cyclic codes over the rings $\mathbb{Z}_2+u\mathbb{Z}_2$ and $\mathbb{Z}_2+u\mathbb{Z}_2+u^2\mathbb{Z}_2$," *Des. Codes Crypt.* , vol. 42, pp. 273-287, 2007.

[6] Yildiz, and S. Karadenniz, "Cyclic code over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$," *Des. Codes. Crypt.* , vol. 58, pp. 273-287, 2010.

[7] L. Ping, and Z. Shixin, "Cyclic codes of arbitrary lengths over the ring $\mathbb{F}_q+u\mathbb{F}_q$," *J. China Univ. Sci. Tech.*, vol. 38, pp. 1392-1396, 2008.

[8] W. C. Huffman, V. S. Pless, *Fundameutals of Error-correcting Codes*, Cambridge: Cambrige University Press, 2003.

[9] H. Tapia-recillas, and G. Vega, "Some constacylic codes over $\mathbb{Z}_4$ and binary quasi-cyclic codes," *Discrete Appl. Math*, vol. 128, pp. 305-316, 2003.

Received: November 26, 2014 Revised: January 08, 2015 Accepted: January 21, 2015