第47卷第11期
2017年11月

中国科学技术大学学报
JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA

Vol.47,No.11
Nov. 2017

文章编号:0253-2778(2017)7-0899-07

Linear codes and their weight enumerators over the ring $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p$

CHEN Yanna[1,2], WU Huazhang[1,2], SHI Minjia[2]

(1. *Key Laboratory of Intelligent Computing and Signal Processing, Ministry of Education, Anhui University, Hefei* 230039, *China*;
2. *School of Mathematical Sciences, Anhui University, Hefei* 230601, *China*)

Abstract: The linear codes over the ring $R=\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p$ were studied, where p is a prime and $u^2=u$, $v^2=v$, $uv=vu$. A kind of Gray map and some weight enumerators and their relationships of linear codes over R were discussed. Moreover, an example was given to show the validity of the above weight enumerators formulas.

Key words: linear codes; Gray map; weight enumerators

CLC number: O157.4 **Document code**: A doi:10.3969/j.issn.0253-2778.2017.07.003

2010 Mathematics Subject Classification: 94B15

Citation: CHEN Yanna, WU Huazhang, SHI Minjia. Linear codes and their weight enumerators over the ring $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p$ [J]. Journal of University of Science and Technology of China, 2017,47(11): 899-905.
陈燕娜,吴化璋,施敏加. 环 $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p$ 上的线性码和它们的重量计数器[J]. 中国科学技术大学学报,2017,47(11):899-905.

环 $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p$ 上的线性码和它们的重量计数器

陈燕娜[1,2],吴化璋[1,2],施敏加[2]

(1.安徽大学计算智能与信号处理教育部重点实验室,安徽合肥 230039;2.安徽大学数学科学学院,安徽合肥 230601)

摘要:研究了环 $R=\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p$ 上的线性码,其中,p 是一个素数,$u^2=u$,$v^2=v$,$uv=vu$.讨论了该环上线性码的一类Gary映射和一些重量计数器并获得了这些重量计数器之间的关系.此外,给出一个实例验证了这些重量计数器的正确性.

关键词:线性码;Gary映射;重量计数器

0 Introduction

In 1948, Shannon published a landmark paper *A mathematical theory of communication* that signified the beginning of both information theory and encoding. Among all types of codes, linear codes are widely studied, because of their algebraic structures, they are easy to be described, encoded, and decoded than nonlinear codes.

The aim of this paper is to introduce and study

Received: 2017-04-25; **Revised**: 2017-09-19

Foundation item: Supported by National Natural Science Foundation of China (61672036), the Open Research Fund of Key Laboratory of Intelligent Computing and Signal Processing, Ministry of Education, Anhui University.

Biography: CHEN Yanna, female, born in 1992, master. Research field: Algebraic coding theory. E-mail:chenyanna881@163.com.

Corresponding author: WU Huazhang, PhD/Prof. E-mail: wuhz@ahu.edu.cn.

linear codes, and their Gray map over the ring $R=\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p$, where $u^2=u$, $v^2=v$, $uv=vu$ and p is a prime. The ring R has been used as an alphabet to study linear codes and skew-cyclic codes[11]. Recently linear codes and their extensions are considered over various kinds of rings. For example, LCD codes have attracted the attention of more and more researchers, e.g., LCD codes over finite field were first studied by Massey in 1992[5]. Esmaeili and Yari studied complementary dual quasi-cyclic codes[2] and Sendrier showed the Gilbert-Varshamov bound of such codes[6]. Also weight enumerators are an important direction of research. Gao gave some results on linear codes over $\mathbb{F}_p+u\mathbb{F}_p+u^2\mathbb{F}_p$[3]. Since the ring R can be seen as the direct product $\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p$, in the present paper we can combine the results and methods of the above papers to discuss the linear codes over R.

The remainder of this paper is organized as follows. In Section 1, we introduce some preliminary results about the ring R and linear codes over the finite field $\mathbb{F}_p$. Section 2 considers the weight of the element of R and introduces a Gray map, which leads to some useful results on linear codes over R. Section 3 is devoted to the investigation of some kinds of weight enumerators of linear codes over R together with their relationships. Section 4 is the conclusion of the paper.

1 Preliminary results

Let C be a linear code of length n and dimension k over $\mathbb{F}_p$ and $P(C)$ be its polynomial representation, i.e.,

$$P(C)=\left\{\sum_{i=0}^{n-1}c_ix^i \mid (c_0,c_1,\cdots,c_{n-1})\in C\right\}.$$

Let σ and τ_l be maps from $\mathbb{F}_p{}^n$ to $\mathbb{F}_p{}^n$ given by $\sigma(a_0,a_1,\cdots,a_{n-1})=(a_{n-1},a_0,\cdots,a_{n-2})$, and $\tau_l(c_0,c_1,\cdots,c_{n-1})=\tau_l(c^0\mid c^1\mid\cdots\mid c^{l-1})=(\sigma(c^0)\mid\sigma(c^1)\mid\cdots\mid\sigma(c^{l-1}))$, where $c^i=(c_{im},c_{im+1},\cdots,c_{(i+1)m-1})$, $i=0,1,\cdots,l-1$, and $n=ml$. Then C is said to be cyclic if $\sigma(C)=C$, and C is called a quasi-cyclic code of index l if $\tau_l(C)=C$.

It is easy to see that $R=\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p$ is a ring of characteristic p, containing four maximal ideals:

$$m_1=\langle u,v\rangle,\ m_2=\langle u-1,v-1\rangle,$$
$$m_3=\langle u-1,v\rangle,\ m_4=\langle u,v-1\rangle.$$

Let

$$\Psi: R\rightarrow R/m_1\times R/m_2\times R/m_3\times R/m_4$$

be the canonical homomorphism defined by $x\mapsto(x+m_1,x+m_2,x+m_3,x+m_4)$. By the Chinese Remainder Theorem, the map is an isomorphism, from this we can see that R is a principal ideal ring. It is convenient to write the decomposition given in the following formula using orthogonal idempotents in R,

$$\begin{aligned}R&=\alpha_1R\oplus\alpha_2R\oplus\alpha_3R\oplus\alpha_4R=\\&\alpha_1\mathbb{F}_{\mathrm{p}}\oplus\alpha_2\mathbb{F}_{\mathrm{p}}\oplus\alpha_3\mathbb{F}_{\mathrm{p}}\oplus\alpha_4\mathbb{F}_{\mathrm{p}}\end{aligned}\qquad(1)$$

where $\alpha_1=1-u-v+uv$, $\alpha_2=uv$, $\alpha_3=u-uv$, $\alpha_4=v-uv$. It is easy to verify that $\alpha_i{}^2=\alpha_i$, $\alpha_i\alpha_j=0$ and $\sum_{k=1}^4\alpha_k=1$, with $i,j=1,2,3,4$, $i\neq j$ and $\alpha_iR\cong\mathbb{F}_{\mathrm{p}}$. Any element of R can be expressed uniquely as: $r=a+ub+vc+uvd=\alpha_1a+\alpha_2(a+b+c+d)+\alpha_3(a+b)+\alpha_4(a+c)$, with $a,b,c,d\in\mathbb{F}_p$.

The dual code $C^\perp$ of C with respect to the Euclidean inner product is defined as

$$C^\perp=\left\{x\in R^n\mid x\cdot y=\sum_{i=0}^{n-1}x_iy_i=0,\forall y\in C\right\},$$

where $x=(x_0,x_1,\cdots,x_{n-1})$, $y=(y_0,y_1,\cdots,y_{n-1})$.

A code C is self-orthogonal if $C\subseteq C^\perp$, and C is self-dual if $C=C^\perp$.

If A_i $(i=1,2,3,4)$ are codes over R, we denote their direct sum by

$$A_1\oplus A_2\oplus A_3\oplus A_4=$$
$$\{a_1+a_2+a_3+a_4\mid a_i\in A_i,i=1,2,3,4\}.$$

For a linear code C of length n over R, define as

$$C_1=\{a\in\mathbb{F}_p^n\mid\exists b,c,d\in\mathbb{F}_p^n,$$
$$\alpha_1a+\alpha_2b+\alpha_3c+\alpha_4d\in C\},$$
$$C_2=\{b\in\mathbb{F}_p^n\mid\exists a,c,d\in\mathbb{F}_p^n,$$
$$\alpha_1a+\alpha_2b+\alpha_3c+\alpha_4d\in C\},$$
$$C_3=\{c\in\mathbb{F}_p^n\mid\exists a,b,d\in\mathbb{F}_p^n,$$

$$\alpha_1 a+\alpha_2 b+\alpha_3 c+\alpha_4 d\in C\},$$
$$C_4=\{d\in\mathbb{F}_p^n\mid \exists a,b,c\in\mathbb{F}_p^n,$$
$$\alpha_1 a+\alpha_2 b+\alpha_3 c+\alpha_4 d\in C\}.$$

It is easy to check that C_1, C_2, C_3 and C_4 are linear codes of length n over $\mathbb{F}_p$. By the ring decomposition of R in (1) a linear code C over R can be uniquely expressed as

$$C=\alpha_1C_1\oplus\alpha_2C_2\oplus\alpha_3C_3\oplus\alpha_4C_4 \qquad (2)$$

Furthermore, a linear code C is self-dual over R if and only if C_1,C_2,C_3 and C_4 are self-dual over $\mathbb{F}_p$.

2 Linear codes over R and their Gray map

Definition 2.1 The Gray map Φ from R^n to $\mathbb{F}_p{}^{4n}$ is defined by

$$\Phi: R^n\rightarrow\mathbb{F}_p{}^{4n},$$
$$(r_0,r_1,\cdots,r_{n-1})\mapsto$$
$$(a_0,a_0+b_0+c_0+d_0,a_0+b_0,a_0+c_0,\cdots,$$
$$a_{n-1},a_{n-1}+b_{n-1}+c_{n-1}+d_{n-1},$$
$$a_{n-1}+b_{n-1},a_{n-1}+c_{n-1}),$$

where $r_i=a_i+ub_i+vc_i+uvd_i\in R$ and $i=0,1,\cdots,n-1$.

For any element $r=a+ub+vc+uvd\in R$, we define the Lee weight, denoted by w_L, as

$$w_L(a+ub+vc+uvd)=$$
$$w_H(a,a+b+c+d,a+b,a+c),$$

where w_H denotes the ordinary Hamming weight for p-ary codes. The Lee weight of a codeword $r=(r_0,r_1,\cdots,r_{n-1})\in R^n$ is defined to be the rational sum as $w_L(r)=\sum_{i=0}^{n-1}w_L(r_i)$ and for $r,r'\in R^n$, the Lee distance is defined as $d_L(r,r')=w_L(r-r')$. The minimum Lee distance of a linear code over R is defined as $\min\{d_L(r,r')\mid r,r'\in C, r\neq r'\}$. We denote the Hamming distance of a p-ary code C by $d_H(C)$.

Now, we give some results which can be found in Ref.[12].

Theorem 2.1[12] The Gray map Φ is also $\mathbb{F}_p$-linear. The map Φ is a weight-preserving map from (R^n, Lee weight) to ($\mathbb{F}_p^{4n}$, Hamming weight), i.e.,

$$w_L(x)=w_H(\Phi(x)),\text{ for all } x\in R^n,$$

and Φ is also a distance-preserving map from (R^n, Lee distance) to ($\mathbb{F}_p^{4n}$, Hamming distance), i.e., $d_L(x,y)=d_H(\Phi(x),\Phi(y))$, for all $x,y\in R^n$.

Theorem 2.2[12] Let C be an (n,M,d) linear code over R, then $\Phi(C)$ is an $[4n,\log_pM,d]$ linear code over $\mathbb{F}_p$.

Lemma 2.1[11] If G_i are generator matrices of p-ary linear codes C_i ($i=1,2,3,4$) in Eq.(2), respectively, then the generator matrix of C is

$$G=\begin{bmatrix}\alpha_1G_1\\ \alpha_2G_2\\ \alpha_3G_3\\ \alpha_4G_4\end{bmatrix} \qquad (3)$$

From Lemma 2.1 we can easily derive the following results.

Theorem 2.3 If C is a linear code of length n over R with generator matrice G, then

$$\Phi(G)=\begin{bmatrix}\Phi(\alpha_1G_1)\\ \Phi(\alpha_2G_2)\\ \Phi(\alpha_3G_3)\\ \Phi(\alpha_4G_4)\end{bmatrix}=\begin{bmatrix}G_1&0&0&0\\0&G_2&0&0\\0&0&G_3&0\\0&0&0&G_4\end{bmatrix} \quad (4)$$

Proof Keep the above notations. Let $a\in C_1$, $b\in C_2$, $c\in C_3$, $d\in C_4$. Since

$$\Phi(\alpha_1a)=\Phi(a-ua-va+uva)=(a,0,0,0),$$
$$\Phi(\alpha_2b)=\Phi(ub+uvb)=(0,b,0,0),$$
$$\Phi(\alpha_3c)=\Phi(uc-uvc)=(0,0,c,0),$$
$$\Phi(\alpha_4d)=\Phi(vd-uvd)=(0,0,0,d),$$

then the proof is completed.

An important connection that we want to investigate is the relation between the dual and the Gray image of a code. We have the following theorem.

Theorem 2.4 Let C be a linear code over R. Then $\Phi(C)^\perp=\Phi(C^\perp)$. Moreover, if C is self-dual, so is $\Phi(C)$ over $\mathbb{F}_p$.

Proof Without loss of generality, for arbitrary $r_1=(r_{10},r_{11},\cdots,r_{1,n-1})\in C$ and $r_2=(r_{20},r_{21},\cdots,r_{2,n-1\}})\in C^\perp$, where $r_{ji}=a_{ji}+ub_{ji}+vc_{ji}+uvd_{ji}\in R$, $a_{ji},b_{ji},c_{ji},d_{ji}\in\mathbb{F}_{\mathrm{p}}$, $j=1,2$ and $i=0,1,\cdots,n-1$. Then $r_1\cdot r_2=0$, which implies $\sum_{i=0}^{n-1}a_{1i}a_{2i}=0$, $\sum_{i=0}^{n-1}(a_{1i}b_{2i}+a_{2i}b_{1i}+b_{1i}b_{2i})=0$, $\sum_{i=0}^{n-1}(a_{1i}c_{2i}+a_{2i}c_{1i}+c_{1i}c_{2i})=0$ and

$$\sum_{i=0}^{n-1}(a_{1i}d_{2i}+b_{1i}c_{2i}+b_{1i}d_{2i}+b_{2i}c_{1i}+c_{1i}d_{2i}+ a_{2i}d_{1i}+b_{2i}d_{1i}+c_{2i}d_{1i}+d_{1i}d_{2i})=0.$$

Therefore,

$\Phi(r_1)\cdot\Phi(r_2)=\sum_{i=0}^{n-1}a_{1i}a_{2i}+\sum_{i=0}^{n-1}(a_{1i}+b_{1i}+c_{1i}+d_{1i})(a_{2i}+b_{2i}+c_{2i}+d_{2i})+\sum_{i=0}^{n-1}(a_{1i}+b_{1i})(a_{2i}+b_{2i})+\sum_{i=0}^{n-1}(a_{1i}+c_{1i})(a_{2i}+c_{2i})=4\sum_{i=0}^{n-1}a_{1i}a_{2i}+2\sum_{i=0}^{n-1}(a_{1i}b_{2i}+a_{2i}b_{1i}+b_{1i}b_{2i})+2\sum_{i=0}^{n-1}(a_{1i}c_{2i}+a_{2i}c_{1i}+c_{1i}c_{2i})+\sum_{i=0}^{n-1}(a_{1i}d_{2i}+b_{1i}c_{2i}+b_{1i}d_{2i}+b_{2i}c_{1i}+c_{1i}d_{2i}+a_{2i}d_{1i}+b_{2i}d_{1i}+c_{2i}d_{1i}+d_{1i}d_{2i})=0.$

Thus $\Phi(C^{\perp})\subseteq\Phi(C)^{\perp}$.

From Theorem 2.2, we can verify that $|\Phi(C)^{\perp}|=|\Phi(C^{\perp})|$, which implies that $\Phi(C)^{\perp}=\Phi(C^{\perp})$. If $C=C^{\perp}$, then $\Phi(C)=\Phi(C^{\perp})=\Phi(C)^{\perp}$, which implies $\Phi(C)$ is self-dual.

Next, we give an example to illustrate the above results.

Example 2.1 (i) Let C be a linear code of length 4 generated by the matrix G over $R=\mathbb{F}_5+u\mathbb{F}_5+v\mathbb{F}_5+uv\mathbb{F}_5$, where

$$G=\begin{bmatrix}\alpha_1G_1\\ \alpha_2G_2\\ \alpha_3G_3\\ \alpha_4G_4\end{bmatrix},$$

and

$$G_1=\begin{bmatrix}1&0&2&0\\0&1&0&3\end{bmatrix},\ G_2=\begin{bmatrix}1&0&0&2\\0&1&2&0\end{bmatrix},$$

$$G_3=\begin{bmatrix}1&0&3&0\\0&1&0&2\end{bmatrix},\ G_4=\begin{bmatrix}1&0&0&3\\0&1&3&0\end{bmatrix}.$$

Then C is a self-dual code over R. Moreover, by Theorem 2.2, $\Phi(C)$ is a self-dual code of length 16 over $\mathbb{F}_5$. It is a $[16,8,2]$ self-dual code. And after some row elementary operations on the matrix $\Phi(C)$, the self-dual code $\Phi(C)$ has the following generator matrix

$$\begin{bmatrix}G_1&0&0&0\\0&G_2&0&0\\0&0&G_3&0\\0&0&0&G_4\end{bmatrix}\rightarrow\begin{bmatrix}1&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0&0&0&0&0&0&2&0&0\\0&0&1&0&0&0&0&0&0&0&3&0&0&0&0&0\\0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&3\\0&0&0&0&1&0&0&0&0&0&0&0&3&0&0&0\\0&0&0&0&0&1&0&0&0&2&0&0&0&0&0&0\\0&0&0&0&0&0&1&0&0&0&0&0&0&0&2&0\\0&0&0&0&0&0&0&1&0&0&0&3&0&0&0&0\end{bmatrix}.$$

(ii) If we let C be a linear code of length 2 generated by the matrix G over $R=\mathbb{F}_7+u\mathbb{F}_7+v\mathbb{F}_7+uv\mathbb{F}_7$, where

$$G_1=\begin{bmatrix}1&2\\3&4\end{bmatrix},\ G_2=\begin{bmatrix}4&1\\1&1\end{bmatrix},$$

$$G_3=\begin{bmatrix}2&3\\1&2\end{bmatrix},G_4=\begin{bmatrix}1&2\\3&4\end{bmatrix}.$$

It is easy to deduce that the generator matrix of $\Phi(C)$ is as follows

$$\begin{bmatrix}1&2&0&0&0&0&0&0\\3&4&0&0&0&0&0&0\\0&0&4&1&0&0&0&0\\0&0&1&1&0&0&0&0\\0&0&0&0&2&3&0&0\\0&0&0&0&1&2&0&0\\0&0&0&0&0&0&1&2\\0&0&0&0&0&0&3&4\end{bmatrix}.$$

$\Phi(C)$ is an $[8,8,1]$ cyclic linear code over $\mathbb{F}_7$, and it is universe code of length 8 and MDS code at the same time.

(iii) Similarily, if we take $n=2$ and let C be a cyclic code of length 3 generated by $g(x)=(v-uv)x+1$ over $R=\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$. Then $\Phi(C)$ is a suboptimal $[8,7,1]$ linear code over $\mathbb{F}_2$.

Lemma 2.2[4] There exists at least one self-dual cyclic code of length n over $\mathbb{F}_p$ if and only if p is a power of 2 and n is even.

Theorem 2.5 There exists a self-dual cyclic code of length n over R if and only if p is power of 2 and n is even.

Proof We know that $C=\alpha_1C_1\oplus\alpha_2C_2\oplus\alpha_3C_3\oplus\alpha_4C_4$. From Lemma 2.2, we have that C_1, C_2, C_3 and C_4 are self-dual cyclic codes over $\mathbb{F}_p$ if and only if p is power of 2 and n is even.

Lemma 2.3[11] Let $C=\alpha_1C_1\oplus\alpha_2C_2\oplus\alpha_3C_3\oplus\alpha_4C_4$ be a cyclic code of length n over R. Then $C=\langle\alpha_1g_1(x),\alpha_2g_2(x),\alpha_3g_3(x),\alpha_4g_4(x)\rangle$, where $g_i(x)$ is a generator polynomial of cyclic code C_i, $1\leqslant i\leqslant 4$. Furthermore, $|C|=p^{4n-\sum_{i=1}^{4}\deg(g_i(x))}$.

Lemma 2.4[11] Let $C=\alpha_1C_1\oplus\alpha_2C_2\oplus\alpha_3C_3\oplus\alpha_4C_4$ be a cyclic code of length n over R, such that $C=\langle\alpha_1g_1(x),\alpha_2g_2(x),\alpha_3g_3(x),\alpha_4g_4(x)\rangle$ and $C^{\perp}$ is its dual. Let $h_i(x)\in\mathbb{F}_p[x]$ such that $g_i(x)h_i(x)=x^n-1$. Then $C^{\perp}=\alpha_1C_1{}^{\perp}\oplus\alpha_2C_2{}^{\perp}\oplus\alpha_3C_3{}^{\perp}\oplus\alpha_4C_4{}^{\perp}$, where $C_i{}^{\perp}$ is the dual of the cyclic code over $\mathbb{F}_p$. Furthermore, $C^{\perp}=\langle\alpha_1h_1^*(x),\alpha_2h_2^*(x),\alpha_3h_3^*(x),\alpha_4h_4^*(x)\rangle$, where $h_j^*(x)=x^{\deg h_j(x)}h_j(1/x)$.

Theorem 2.6[12] If C is a cyclic code of length n over R, then $\Phi(C)$ is a 4-quasi cyclic code of length $4n$ over $\mathbb{F}_p$.

Armed with Theorems 2.4～2.6, we can easily obtain the following results. Here we omit the proof.

Theorem 2.7 $C=\alpha_1C_1\oplus\alpha_2C_2\oplus\alpha_3C_3\oplus\alpha_4C_4$ be a self-dual cyclic code over $R_2=\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}+v\,\mathbb{F}_{2\mathrm{m}}+uv\mathbb{F}_{2^m}$. Then $\Phi(C)$ is a self-dual 4-quasi-cyclic code over $\mathbb{F}_{2^m}$.

3 Weight enumerators of linear codes over *R*

Let C be a linear code of length n over R. Suppose that e is an element of R, i.e., $e=a+ub+vc+uvd$ with a, b, c, $d\in\mathbb{F}_p$. For all $x=(x_0, x_1,\cdots,x_{n-1})\in R^n$, define the weight of x at e to be

$$w_e(x)=|\{i\mid x_i=e\}|.$$

Definition 3.1 The complete weight enumerator of R is defined to be the homogeneous polynomial of degree n in p^4 indeterminates $X_0, X_1, X_u, X_v, \cdots, X_{(p-1)+u(p-1)+v(p-1)+uv(p-1)}$, that is,

$$\mathrm{cwe}_C(X_0,X_1,X_u,X_v,\cdots,$$
$$X_{(p-1)+u(p-1)+v(p-1)+uv(p-1)})=$$
$$\sum_{c\in C}X_0^{w0(c)}X_1^{w1(c)}X_u^{wu(c)}X_v^{wv(c)}\cdots$$
$$X_{(p-1)+u(p-1)+v(p-1)+uv(p-1)}^{w_{(p-1)+u(p-1)+v(p-1)+uv(p-1)}(c)}.$$

Definition 3.2 Let A_i be the number of elements of the Lee weight i in C. Then the set $\{A_0, A_1, A_2, \cdots, A_{4n}\}$ is called the Lee weight distribution of C. Define the Lee weight enumerator of C as

$$\mathrm{Lee}_C(X,Y)=\sum_{i=0}^{4n}A_i\,X^{4n-i}Y^i \tag{5}$$

or

$$\mathrm{Lee}_C(X,Y)=\sum_{c\in C}X^{4n-w_L(c)}Y^{w_L(c)} \tag{6}$$

For any codeword c of C, define T_0, T_1, T_2, T_3, T_4 to be the numbers of components of c with Lee weight 0,1,2,3 and 4, respectively. Then the Lee weight of c is

$$w_L(c)=T_1+2T_2+3T_3+4T_4.$$

The Hamming weight $w_H(c)$ of $c\in C$ is defined to be

$$w_H(c)=T_1+T_2+T_3+T_4.$$

Define the symmetrized weight enumerator of C as

$$\mathrm{swe}_C(X_0,X_1,X_2,X_3,X_4)=$$
$$\mathrm{cwe}_C(X_0,X_1,X_u,\cdots,X_{(p-1)+u(p-1)+v(p-1)+uv(p-1)})=$$
$$\sum_{c\in C}X_0^{T_0}X_1^{T_1}X_2^{T_2}X_3^{T_3}X_4^{T_4} \tag{7}$$

Define the Hamming weight enumerator of C as

$$\mathrm{Ham}_C(X,Y)=\sum_{c\in C}X^{n-w_H(c)}Y^{w_H(c)} \qquad (8)$$

For the above weight enumerators we have the following results.

Theorem 3.1 Let C be a linear code of length n over R. Then

(ⅰ) $\mathrm{Lee}_C(X,Y)=\mathrm{swe}_C(X^4,X^3Y,X^2Y^2,XY^3,Y^4)$;

(ⅱ) $\mathrm{Ham}_C(X,Y)=\mathrm{swe}_C(X,Y,Y,Y,Y)$;

(ⅲ) $\mathrm{Lee}_C(X,Y)=\mathrm{Ham}_{\Phi(C)}(X,Y)$;

(ⅳ) $\mathrm{Lee}_{C^\perp}(X,Y)=\frac{1}{|C|}\mathrm{Lee}_C(X+(p-1)Y,X-Y)$.

Proof (ⅰ) From the definition of the symmetrized weight enumerator, we have

$$\mathrm{swe}_C(X^4,X^3Y,X^2Y^2,XY^3,Y^4)=$$
$$\sum_{c\in C}(X^4)^{T_0}(X^3Y)^{T_1}(X^2Y^2)^{T_2}(XY^3)^{T_3}(Y^4)^{T_4}=$$
$$\sum_{c\in C}X^{4T_0+3T_1+2T_2+T_3}Y^{T_1+2T_2+3T_3+4T_4}=$$
$$\sum_{c\in C}X^{4n-w_L(c)}Y^{w_L(c)}=\mathrm{Lee}_C(X,Y).$$

(ⅱ) From the definition of symmetrized weight enumerator, we have

$$\mathrm{swe}_C(X,Y,Y,Y,Y)=\sum_{c\in C}X^{T_0}Y^{T_1}Y^{T_2}Y^{T_3}Y^{T_4}=$$
$$\sum_{c\in C}X^{T_0}Y^{T_1+T_2+T_3+T_4}=$$
$$\sum_{c\in C}X^{n-w_H(c)}Y^{w_H(c)}=\mathrm{Ham}_C(X,Y).$$

(ⅲ) From the definition of weight enumerator, we obtain that

$$\mathrm{Lee}_C(X,Y)=\sum_{c\in C}X^{4n-w_L(c)}Y^{w_L(c)}=$$
$$\sum_{\Phi(c)\in\Phi(C)}X^{4n-w_H(\Phi(c))}Y^{w_H(\Phi(c))}=\mathrm{Ham}_{\Phi(C)}(X,Y)\ .$$

(ⅳ) From Theorem 2.4, $\Phi(C^\perp)=\Phi(C)^\perp$ and they are both $\mathbb{F}_p$-linear according to Theorem 2.1. By Proposition 2.6 in Ref.[9] and case (ⅲ), we have

$$\mathrm{Lee}_{C^\perp}(X,Y)=\mathrm{Ham}_{\Phi(C^\perp)}(X,Y)=$$
$$\mathrm{Ham}_{\Phi(C)^\perp}(X,Y)=$$
$$\frac{1}{|\Phi(C)|}\mathrm{Ham}_{\Phi(C)}(X+(p-1)Y,X-Y)=$$
$$\frac{1}{|C|}\mathrm{Ham}_{\Phi(C)}(X+(p-1)Y,X-Y)=$$
$$\frac{1}{|C|}\mathrm{Lee}_C(X+(p-1)Y,X-Y)\ .$$

Example 3.1 Let C be a linear code of length $n=2$ over $R_2=\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ with generator matrix

$$G=\begin{pmatrix}u+v & 0\\ 0 & 1+u+v\end{pmatrix}.$$

Then $|C|=16$ and C consists of the following sixteen codewords:

$$(0,0),\ (u+v,0),\ (u+uv,0),(v+uv,0),$$
$$(0,1+u+v),(u+v,1+u+v),$$
$$(u+uv,1+u+v),\ (v+uv,1+u+v),$$
$$(0,uv),\ (u+v,uv),\ (u+uv,uv),$$
$$(v+uv,uv),\ (0,1+u+v+uv),$$
$$(u+v,1+u+v+uv),$$
$$(u+uv,1+u+v+uv),$$
$$(v+uv,1+u+v+uv).$$

Therefore,

$$\Phi(C)=\{(0,0,0,0,0,0,0,0),(0,0,1,1,0,0,0,0),$$
$$(0,0,1,0,0,0,0,0),(0,0,0,1,0,0,0,0),$$
$$(0,0,0,0,1,1,0,0),(0,0,1,1,1,1,0,0),$$
$$(0,0,1,0,1,1,0,0),(0,0,0,1,1,1,0,0),$$
$$(0,0,0,0,0,1,0,0),(0,0,1,1,0,1,0,0),$$
$$(0,0,1,0,0,1,0,0),(0,0,0,1,0,1,0,0),$$
$$(0,0,0,0,1,0,0,0),(0,0,1,1,1,0,0,0),$$
$$(0,0,1,0,1,0,0,0),(0,0,0,1,1,0,0,0)\}.$$

It is easy to compute that $C^\perp$ has 16 codewords with generator matrix

$$H=\begin{pmatrix}0 & u+v\\ 1+u+v & 0\end{pmatrix}.$$

$$C^\perp=\{(0,0),\ (0,u+v),\ (0,u+uv),\ (0,v+uv),$$
$$(1+u+v,0),(1+u+v,u+v),$$
$$(1+u+v,u+uv),\ (1+u+v,v+uv),$$
$$(uv,0),\ (uv,u+v),\ (uv,u+uv),$$
$$(uv,v+uv),\ (1+u+v+uv,0),$$
$$(1+u+v+uv,u+v),$$
$$(1+u+v+uv,u+uv),$$
$$(1+u+v+uv,v+uv)\}.$$

From Definition 3.2, we have that

$$\mathrm{Lee}_C(X,Y)=A_0X^8Y^0+A_1X^7Y^1+$$
$$A_2X^6Y^2+A_3X^5Y^3+A_4X^4Y^4=$$
$$=X^8+4X^7Y+6X^6Y^2+4X^5Y^3+X^4Y^4 \qquad (9)$$

From Eq.(7), we have that

$$\mathrm{swe}_C(X_0,X_1,X_2,X_3,X_4)=X_0^2+4XX_{10}+$$
$$2X_0X_2+4X_1^2+X_2^2+4XX_{21}.$$

Hence

$$\begin{aligned}&\mathrm{swe}_C(X^4,X^3Y,X^2Y^2,XY^3,Y^4)=\\&(X^4)^2+4(X^4\cdot X^3Y)+2(X^4\cdot X^2Y^2)+\\&4(X^3Y)^2+(X^2Y^2)^2+4(X^3Y\cdot X^2Y^2)=\\&X^8+4X^7Y+6X^6Y^2+4X^5Y^3+X^4Y^4\end{aligned}\tag{10}$$

From (9) and (10), the part (i) of Theorem 3.1 is valid.

$$\begin{aligned}&\mathrm{swe}_C(X,Y,Y,Y,Y)=X^2+4(X\cdot Y)+\\&2(X\cdot Y)+4Y^2+Y^2+4(Y\cdot Y)=\\&X^2+6XY+9Y^2,\end{aligned}$$

and Eq.(8) implies $Ham_C(X,Y)=X^2+6XY+9Y^2$, which is in accordance with the part (ⅱ) of Theorem 3.1.

In terms of the elements of $\Phi(C)$, we calculate

$$\begin{aligned}&\mathrm{Ham}_{\Phi(C)}(X,Y)=X^8+4X^7Y+\\&6X^6Y^2+4X^5Y^3+X^4Y^4\end{aligned}\tag{11}$$

The part (ⅲ) of Theorem 3.1 is deduced by (9) and (11).

On account of

$$\begin{aligned}&\mathrm{Lee}_{C^\perp}(X,Y)=X^8+4X^7Y+\\&6X^6Y^2+4X^5Y^3+X^4Y^4,\end{aligned}$$

and

$$\begin{aligned}&\mathrm{Lee}_C((X+Y),(X-Y))=(X+Y)^8+\\&4(X+Y)^7(X-Y)+6(X+Y)^6(X-Y)^2+\\&4(X+Y)^5(X-Y)^3+(X+Y)^4(X-Y)^4=\\&16X^8+64X^7Y+96X^6Y^2+64X^5Y^3+16X^4Y^4.\end{aligned}$$

Thus $\mathrm{Lee}_{C^\perp}(X,Y)=\frac{1}{|C|}\mathrm{Lee}_C(X+(p-1)Y,X-Y)$, the part (ⅳ) is satisfied.

4 Conclusion

In this paper we study some properties of linear codes over the ring $R=\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\,\mathbb{F}_p$, where $u^2=u$, $v^2=v$, $uv=vu$, and p is a prime. A kind of Gray map is introduced, which is a weight-preserving map from R^n to $\mathbb{F}_p^{4n}$ and can be used to derive some useful results. Some weight enumerators and the relationships between them are discussed. We plan to discuss some other codes over the ring R in the future.

References

[1] ARASU K T, GULLIVER T A. Self-dual codes over $\mathbb{F}_p$ and weighing matrices[J]. IEEE Transactions on Information Theory, 2001, 47(5): 2051-2055.

[2] ESMAEILI M, YARI S. On complementary-dual quasi-cyclic codes [J]. Finite Fields and Their Applications, 2009, 15(3): 375-386.

[3] GAO J. Some results on linear codes over $\mathbb{F}_q+u\mathbb{F}_q+u^2\mathbb{F}_q$[J]. Journal of Applied Mathematics and Computing, 2015, 47(1): 473-485.

[4] JIA Y, LING S, XING C P. On self-dual cyclic codes over finite fields[J]. IEEE Transactions on Information Theory, 2011, 57(4): 2243-2251.

[5] MASSEY J L. Linear codes with complementary duals [J]. Discrete Mathematics, 1992,106(9): 337-342.

[6] SENDRIER N. Linear codes with complementary duals meet the Gilbert-Varshamov bound [J]. Discrete Mathematics, 2004, 285(1-3): 345-347.

[7] SHARMA A, RANI S. On constacyclic codes over finite fields[J]. Cryptography and Communications, 2016, 8(4): 1-20.

[8] SHI M J, LIU Y. The MacWilliams identity of the linear codes over the ring $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p$[J]. Research Journal of Applied Sciences Engineering and Technology,2012, 4(16): 2778-2782.

[9] WAN Z X. Series on Applied Mathematics: Quaternary Codes[M]. Singapore: World Scientific, 1997.

[10] YANG X, MASSEY J L. The condition for a cyclic code to have a complementary dual [J]. Discrete Mathematics, 1994, 126(1-3): 391-393.

[11] YAO T, SHI M J, SOLÉ P. Skew cyclic codes over $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q$[J]. Algebra Combinatorics Discrete Structures and Applications, 2015, 2(3): 163-168.

[12] ZHANG Y T. Research on constacyclic codes over some classes of finite non-chain rings[D]. Hefei: Hefei University of Technology, 2013.

[13] ZHU S X, WANG L Q. A class of constacyclic codes over $\mathbb{F}_p+v\mathbb{F}_p$ and its Gray image [J]. Discrete Mathematics, 2011, 311(23-24): 2677-2682.