Research Journal of Applied Sciences, Engineering and Technology 5(23): 5435-5437, 2013
DOI:10.19026/rjaset.5.4214
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: November 24, 2012 Accepted: January 17, 2013 Published: May 28, 2013

Research Article

Two MacWilliams Identities of the Linear Code over Ring F_2+ vF_2

[1]Peng Hu and [2]Wei Dai
[1]School of Mathematics and Physics, Hubei Polytechnic University, Huangshi 435003, China
[2]School of Economics and Management, Hubei Polytechnic University, Huangshi 435003, China

Abstract: This study defined the ring F_2+ vF_2, as well as its complete weight enumerator and symmetric weight enumerator. By introducing a special variable *t*, we deduced two Macwilliams identities for the two weight enumerators of the linear code and the dual code over the ring F_2+ vF_2.

Keywords: Complete weight enumerator, linear codes, mac williams identities, symmetric weight enumerato

INTRODUCTION

A great deal of attention has been paid to codes over finite rings from the 1990s since a landmark paper (Hammons, 1994), which showed that certain nonlinear binary codes can be constructed from Z_4-linear codes via the Gray map and that nonlinear binary codes (Preparata and Kerdock codes) satisfy with MacWilliams identity. The MacWilliams identity, describing the mutual relationship of the weight distribution between the linear codes and its dual codes, has a wide application. Reference (MacWilliams, 1963) presented the MacWilliams identity for Hamming weight of linear codes over finite field F_q. Wan (1997) made systematical description of the MacWilliams identity with all weight over ring Z_4. Zhu (2003) reported the MacWilliams identity of a symmetric form over ring Z_k. Yu and Zhu (2006) researched the MacWilliams identity over the ring $F_2 + uF_2$. Recently, Yildiz *et al*. (2004) made a research on the linear codes and the MacWilliams identity of the complete weight enumerator over the ring F_2+ uF_2+vF_2+uvF_2 (Karadeniz and Yildiz, 2010). In this study, firstly we give a ring $R = F_2$+vF_2, where $v^2 = v$. Secondly, by introducing a special variable t we obtain the MacWilliams identity for the complete weight enumerator and the symmetric weight enumerator in virtue of the method in Karadeniz and Yildiz (2010). Finally, we verify the two identities by some examples and explain their functions.

PRELIMINARIES

Let:

$$R=F_2+vF_2=\left\{a+bv\middle|v^2=0,a,b\in F_2\right\}=\left\{0,1,v,1+v\right\}$$

Its ideal is:

$$I_0=\{0\}\subseteq I_v=\{0,v\}\subseteq I_1=\{0,1,v,1+v\}$$

So, R belongs to be a finite chain ring.
Suppose $R^n = \{(x_1, x_2, \ldots, x_n)/x_i \in R, i = 1, 2, \ldots , n\}$

Every nonempty subset of Ring R^n is called to be R code. The linear code C with the length of n over R is defined as the R- submodule of R^n.

$$\forall x=(x_1,x_2,\cdots,x_n), y=(y_1,y_2,\cdots,y_n)\in R^n$$

Define their inner product by:

$$x\cdot y=x_1y_1+x_2y_2+\cdots+x_ny_n$$

If $x{\cdot}y$ = 0, then *x*, *y* can be called to be mutual orthogonal. Let:

$$C^{\perp}=\{x\in R^n \,|\, x\cdot y=0,\forall y\in C\}$$

It is easy to prove that $C^{\perp}$ is the linear code over R, referred as the dual code of *C*. Then *C* is called as a self-orthogonal code. If $C = C^{\perp}$, then C is self-orthogonal.

Firstly we introduce the concept of the complete weight enumerator.

Define 1: Suppose *C* is a linear code of length *n* over *R*, where *r* is one element of R. For $\forall x=(x_1,x_2,\cdots,x_n)\in R^n$, $w_r(x)=\sum_{i=1}^{n-1}\delta_{x_i,r}$ is called as the weight of x to *r*, where δ is the Kronecker function $\delta_{\alpha,\, b} = \{1\ \alpha = b\ /0\ \alpha \neq b$. So we define:

$$C_{we_C}(X_0,X_1,X_v,X_{1+v})=\sum_{c\in C}\prod_{r\in R}X_r^{w_r(c)}$$

Corresponding Author: Wei Dai, School of Economics and Management, Hubei Polytechnic University, Huangshi 435003, China

as the complete weight enumerator of the linear code C.

In the following, in order to introduce the concept of the symmetric weight enumerator, the elements of ring R should be classified.

The elements of ring R can be divided into the following three sets:

$$D_0 = \{0\}, D_1 = \{1, 1+v\}, D_2 = \{v\}$$

Define the map: $I: R \to \{0,1,2\}$

$$r \mapsto I(r) = I, \text{ if } r \in D_i$$

Define 2: Suppose C is a linear code over R. Then:

$$S_{we_C}(X_0, X_1, X_2) = C_{we_C}(X_{I(0)}, X_{I(1)}, X_{I(1+v)}, X_{I(v)})$$

can be called as the symmetric weight enumerator of code C.

MACWILLIAMS IDENTITY

In order to obtain two weight enumerators of MacWilliams identity, we introduce a special variable *t*. Let $t^v = -1$and $t^{a+b} = t^a \cdot t^b$, where *a, b*∈*R*. Obviously, $t^0 = t^2 = 1$.

Lemma 1: For any non-zero ideal J in R, there exists $\sum_{k \in J} t^k = 0$.

Proof: $\sum_{k \in I_v} t^k = t^0 + t^v = 0$

$$\sum_{k \in I_1} t^k = t^0 + t^1 + t^v + t^{1+v} = 1 + t - 1 - t = 0$$

Theorem 2: Suppose C is a linear code of length n over R and $C^{\perp}$ is the dual code of C. Then:

$$C_{we_{C^{\perp}}}(X_0, X_1, X_v, X_{1+v}) = \frac{1}{|C|} C_{we_C}(X_0 + X_1 + X_v + X_{1+v},$$

$$X_0 + tX_1 - X_v - tX_{1+v}, X_0 - X_1 + X_v - X_{1+v}, X_0 - tX_1 - X_v + tX_{1+v})$$

Proof: Define the function of C:

$$F(c) = \sum_{x \in R^n} t^{c \cdot x} \prod_{r \in R} X_r^{w_r(x)}$$

Then:

$$\sum_{c \in C} F(c) = \sum_{c \in C}\left(\sum_{x \in C^{\perp}} t^{c \cdot x} \prod_{r \in R} X_r^{w_r(x)}\right) + \sum_{c \in C}\left(\sum_{x \notin C^{\perp}} t^{c \cdot x} \prod_{r \in R} X_r^{w_r(x)}\right)$$
$$= \sum_{x \in C^{\perp}} \prod_{r \in R} X_r^{w_r(x)} \sum_{c \in C} t^{c \cdot x} + \sum_{x \notin C^{\perp}} \prod_{r \in R} X_r^{w_r(x)} \sum_{c \in C} t^{c \cdot x} \quad (1)$$

For every fixed x ∈ R^n, study the function:

$$f_x: \begin{array}{c} C \longrightarrow R \\ c \mapsto f_x(c) = c \cdot x \end{array}$$

Obviously, f_x is a module homomorphism. We observed that:

$$Ker(f_x) = C \Leftrightarrow c \cdot x = 0, \forall c \in C \Leftrightarrow x \in C^{\perp}$$

so the first part of formula (1) can be written as:

$$\sum_{x \in C^{\perp}} \prod_{r \in R} X_r^{w_r(x)} \sum_{c \in C} t^{c \cdot x} = |C| \sum_{x \in C^{\perp}} \prod_{r \in R} X_r^{w_r(x)}$$

If $x \notin C^{\perp}$, then Ker (f_x) ≠ C. So Im(f_x) is a non-zero ideal of R. Thus by virtue of the Lemma 1, we can obtain that, for every such x, there exists $\sum_{c \in C} t^{c \cdot x} = 0$. Therefore, the second part of the formula (1) equals to zero.

So the formula (1) can be written as:

$$\sum_{c \in C} F(c) = |C| \sum_{x \in C^{\perp}} \prod_{r \in R} X_r^{w_r(x)}$$

Then there exists the identity:

$$C_{we_{C^{\perp}}}(X_0, X_1, X_v, X_{1+v}) = \frac{1}{|C|} \sum_{c \in C} F(c) \quad (2)$$

Let's transform the expression of F(c) again. By means of Konecker function, we get:

$$F(c) = \sum_{(x_1, x_2, \cdots, x_n) \in R^n} t^{c \cdot x} \prod_{r \in R} X_r^{w_r(x)}$$

$$= \sum_{(x_1, x_2, \cdots, x_n) \in R^n} \left[\prod_{j=1} t^{c_j \cdot x_j} \left(\prod_{x \in R} X_r^{\delta(x_j, r)}\right)\right]$$

$$= \sum_{x_1 \in R} \cdots \sum_{x_n \in R} \left(t^{c_1 \cdot x_1} X_0^{\delta(x_1, 0)} X_1^{\delta(x_1, 1)} X_v^{\delta(x_1, v)} X_{1+v}^{\delta(x_1, 1+v)}\right) \cdots$$

$$\left(t^{c_n \cdot x_n} X_0^{\delta(x_n, 0)} X_1^{\delta(x_n, 1)} X_v^{\delta(x_n, v)} X_{1+v}^{\delta(x_n, 1+v)}\right)$$

$$= \sum_{x_1 \in R} \left(t^{c_1 \cdot x_1} X_0^{\delta(x_1, 0)} X_1^{\delta(x_1, 1)} X_v^{\delta(x_1, v)} X_{1+v}^{\delta(x_1, 1+v)}\right) \cdots$$

$$\sum_{x_n \in R} \left(t^{c_n \cdot x_n} X_0^{\delta(x_n, 0)} X_1^{\delta(x_n, 1)} X_v^{\delta(x_n, v)} X_{1+v}^{\delta(x_n, 1+v)}\right)$$

$$= \prod_{j=1}^{n} \left(\sum_{r \in R} t^{c_j \cdot r} X_r\right)$$

$$= \left(\sum_{r \in R} X_r\right)^{w_0(x)} \left(\sum_{r \in R} t^r X_r\right)^{w_1(x)} \left(\sum_{r \in R} t^{v \cdot r} X_r\right)^{w_v(x)} \left(\sum_{r \in R} t^{(1+v) \cdot r} X_r\right)^{w_{1+v}(x)}$$

Substituting the above expressions into the formula (2), we have:

$$C_{we_{C^{\perp}}}(X_0, X_1, X_v, X_{1+v})$$

$$= \frac{1}{|C|} C_{we_C}(\sum_{r\in R} X_r, \sum_{r\in R} t^r X_r, \sum_{r\in R} t^{v\cdot r} X_r, \sum_{r\in R} t^{(1+v)\cdot r} X_r)$$

$$= \frac{1}{|C|} C_{we_C}(X_0 + X_1 + X_v + X_{1+v}, X_0 + tX_1 - X_v - tX_{1+v},$$

$$X_0 - X_1 + X_v - X_{1+v}, X_0 - tX_1 - X_v + tX_{1+v})$$

Theorem 3: Suppose C is a linear code of length n over R, we can obtain

$$S_{we_{C^{\perp}}}(X_0, X_1, X_2) = \frac{1}{|C|} S_{we_C}(X_0 + 2X_1 + X_2, X_0 - X_2, X_0 - X_2)$$

Proof: According to the definition of the symmetric weight enumerator and Theorem 2, we know:

$$S_{we_{C^{\perp}}}(X_0, X_1, X_2) = C_{we_{C^{\perp}}}(X_{I(0)}, X_{I(1)}, X_{I(1+v)}, X_{I(v)})$$

$$= \frac{1}{|C|} C_{we_C}(\sum_{r\in R} X_{I(r)}, \sum_{r\in R} t^r X_{I(r)}, \sum_{r\in R} t^{(1+v)\cdot r} X_{I(r)}, \sum_{r\in R} t^{v\cdot r} X_{I(r)})$$

$$= \frac{1}{|C|} C_{we_C}\left(\sum_{s=0}^{2}\left(\sum_{r\in D_s} X_s\right), \sum_{s=0}^{2}\left(\sum_{r\in D_s} t^r X_s\right), \sum_{s=0}^{2}\left(\sum_{r\in D_s} t^{(1+v)\cdot r} X_s\right), \sum_{s=0}^{2}\left(\sum_{r\in D_s} t^{v\cdot r} X_s\right)\right)$$

$$= \frac{1}{|C|} C_{we_C}\left(X_0 + 2X_1 + X_2, X_0 - X_2, X_0 - X_2, X_0 - X_2\right)$$

$$= \frac{1}{|C|} S_{we_C}\left(X_0 + 2X_1 + X_2, X_0 - X_2, X_0 - X_2\right)$$

EXAMPLE

In the following, we will give some examples to illustrate the application of Theorem 2 and 3.

Proof: Obviously:

$$C = \{(0,0), (1,1), (v,v), (1+v, 1+v)\}$$

is the linear code over R, with its complete weight enumerator and symmetric weight enumerator being, respectively,

$$C_{we_C}(X_0, X_1, X_v, X_{1+v}) = X_0^2 + X_1^2 + X_v^2 + X_{1+v}^2$$

And:

$$S_{we_C}(X_0, X_1, X_2) = X_0^2 + 2X_1^2 + X_2^2$$

Then according to Theorem 2, the complete weight enumerator of the dual code $C^{\perp}$ is obtained to be:

$$C_{we_{C^{\perp}}}(X_0, X_1, X_v, X_{1+v}) = \frac{1}{4}[(X_0 + X_1 + X_v + X_{1+v})^2$$
$$+(X_0 + tX_1 - X_v - tX_{1+v})^2 + (X_0 - X_1 + X_v - X_{1+v})^2$$

$$+(X_0 - tX_1 - X_v + tX_{1+v})^2]$$
$$= X_0^2 + X_1^2 + X_v^2 + X_{1+v}^2$$

Therefore, we can get $C^{\perp} = C$, that is to say, C is a self-dual code.

Likewise, based on Theorem 3.3, we get the symmetric weight enumerator of the dual code $C^{\perp}$,

$$S_{we_{C^{\perp}}}(X_0, X_1, X_2) = \frac{1}{4} S_{we_C}(X_0 + 2X_1 + X_2, X_0 - X_2, X_0 - X_2)$$
$$= \frac{1}{4}[(X_0 + 2X_1 + X_2)^2 + 2(X_0 - X_2)^2 + (X_0 - X_2)^2]$$

$$= X_0^2 + 2X_1^2 + X_2^2 + X_0 X_1 + X_1 X_2$$

ACKNOWLEDGMENT

This study has been financially supported by School-level innovative talents project (grant no.12xjz20C).

REFERENCES

Hammons, A.R., 1994. The Z_4 linearty of Kerdock, Preparata, Goethals and related codes. IEEE T. Inform. Theory, 40: 301-319.

Karadeniz, B. and S. Yildiz, 2010. Linear codes over *F₂+ uF₂+vF₂+uvF₂*. Designs Codes Cryptog., 54: 61-81.

MacWilliams, F.J., 1963. A theorem on the distribution of weights in systematic code. Bell. Syst. Tech. J., 42: 79-84.

Wan, Z.X., 1997. Quaternary Code. World Scientific, Singapore.

Yildiz, N., Y. Aysan, F. Sahin and O. Cinar, 2004. Potential inocu- lum sources of tomato stem and pith necrosis caused by Pseudomonas viridiflava in the eastern Mediterranean re-gion of Turkey. J. Plant Diseas. Protect., 111: 380-387.

Yu, H.F. and S.X. Zhu, 2006. Identities of linear codes and their codes over. J. Univ., Sci. Technol. China, 36: 1285-1288.

Zhu, S.X., 2003. The macwilliams identities of symmetric form of linear codes. J. Elec. Inform., 25: 901-906.