环 $F_p + vF_p + v^2F_p$ 上线性码的各种重量计数器及其 MacWilliams 恒等式

施敏加，刘　艳
（安徽大学数学科学学院，安徽合肥 230601）

摘　要： 首先给出了环 $R = F_p + vF_p + v^2F_p$ 上线性码及其对偶码的结构及其 Gray 象的性质. 定义了环 R 上线性码的各种重量计数器并讨论了它们之间的关系，特别的，确定了该环上线性码与其对偶码之间关于完全重量计数器的 MacWilliams 恒等式，利用该恒等式，进一步建立了该环上线性码与其对偶码之间的一种对称形式的 MacWilliams 恒等式. 最后，利用该对称形式的 MacWilliams 恒等式得到了该环上的 Hamming 重量计数器和 Lee 重量计数器的 MacWilliams 恒等式，利用不同的方法推广了文献[7]中的结果.

关键词： 线性码；完全重量计数器；对称重量计数器；MacWilliams 恒等式
中图分类号： TN911.22　**文献标识码：** A　**文章编号：** 0372-2112 (2014)07-1387-05
电子学报 URL： http://www.ejournal.org.cn　**DOI：** 10.3969/j.issn.0372-2112.2014.07.022

Several Weight Enumerators of Linear Codes and Their MacWilliams Identities over Ring $F_p + vF_p + v^2F_p$

SHI Min-jia, LIU Yan
(*School of Mathematical Sciences of Anhui University, Hefei, Anhui 230601, China*)

Abstract: We first give the structures of linear codes and the proposition of their Gray images. A complete weight enumerator of linear codes over ring $R = F_p + vF_p + v^2F_p$ is defined; we define some weight enumerators of linear codes and their dual codes, and then discuss the relations between them. A MacWilliams identity between linear codes and their dual over R with respect to the complete weight enumerator is given. By using this identity, a symmetrized form MacWilliams identitiy between linear codes and their dual over the ring is also established, and MacWilliams identities with respect to Hamming and Lee enumerator can be as results of the symmetrized MacWilliams identitiy, we generalize the results in[7] using different method.

Key words: linear code; complete weight enumerator; symmetrized weight enumerator; MacWilliams identity

1　引言

近几年，很多编码学者将研究兴趣从有限域上转移到有限环上来，越来越多的性能优异的非线性码被人们所发现，从而使得环 Z_4 乃至更一般的有限环上的编码理论研究进入了一个全新的方向.

码的重量分布是计算各种译码错误概率的主要依据，也是探索码字结构的重要窗口，通过它能透彻的了解码的内部结构. 重量计数器则是研究码的重量分布的一种有力工具，对它的研究有很多，如文献[1]研究了环 Z_4 上线性码的各种重量计数器的 MacWilliams 恒等式；文献[2]研究了环 Z_4 上线性码关于 RT 重量的 MacWilliams 恒等式；文献[3]研究了环 $F_2 + uF_2$ 上关于 Lee 重量的 MacWilliams 恒等式. 文献[4]研究了环 Z_k 上线性码的对称形式的 MacWilliams 恒等式. 对于非链环上线性码及其对偶码之间各种重量计数器的 MacWilliams 恒等式，最近也引起了编码学者的兴趣. 文献[5]研究了环 $F_2 + vF_2 (v^2 = v)$ 上的线性码及其循环码的结构. 文献[6]研究了环 $F_p + vF_p (v^2 = 1)$ 上线性码及其对偶码之间的各种重量计数器的 MacWilliams 恒等式. 文献[7]研究了环 $F_2 + vF_2 + v^2F_2 (v^3 = v)$ 上线性码及其对偶码之间的各种重量计数器的 MacWilliams 恒等式并讨论了该环上循环码的结构.

本文继续研究非有限链环 R 上线性码及其对偶码之间各种重量计数器的 MacWilliams 恒等式，其结果推广了文献[7]中的结果，但所采用的方法不同.

2　环 R 上的线性码及其 Gray 象

文献[8]中给出环 $F_2 + vF_2 + v^2F_2 (v^3 = v)$ 的上任意一个非零线性码的生成矩阵，由此可得环 R 上任意一非零的线性码 C 都等价于由如下矩阵 $\boldsymbol{G}$ 所生成

收稿日期：2013-10-22；修回日期：2014-01-18；责任编辑：蓝红杰
基金项目：国家自然科学基金（No.61202068）；安徽省高校优秀青年人才基金重点项目（No.2012SQRL020ZD）

$$\begin{pmatrix} \boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B}_1+v\boldsymbol{B}_2 & \boldsymbol{C}_1+v\boldsymbol{C}_2 & \boldsymbol{D}_1+v\boldsymbol{D}_2 & \boldsymbol{E}_1+v\boldsymbol{E}_2 & \boldsymbol{F}_1+v\boldsymbol{F}_2 & \boldsymbol{G}_1 \\ \boldsymbol{0} & v\boldsymbol{I}_{k_2} & \boldsymbol{0} & \boldsymbol{0} & (v-1)\boldsymbol{D}_3+(v+1)\boldsymbol{D}_4 & v\boldsymbol{E}_3+(v-1)\boldsymbol{E}_4+(v+1)\boldsymbol{E}_5 & v\boldsymbol{F}_3+(v-1)\boldsymbol{F}_4+(v+1)\boldsymbol{F}_5 & \boldsymbol{G}_2 \\ \boldsymbol{0} & \boldsymbol{0} & (v-1)\boldsymbol{I}_{k_3} & \boldsymbol{0} & (v-1)\boldsymbol{D}_5+(v+1)\boldsymbol{D}_6 & (v-1)\boldsymbol{E}_6+(v+1)\boldsymbol{E}_7 & (v-1)\boldsymbol{F}_6+(v+1)\boldsymbol{F}_7 & \boldsymbol{G}_3 \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & (v+1)\boldsymbol{I}_{k_4} & (v+1)\boldsymbol{D}_7 & (v+1)\boldsymbol{E}_8 & (v+1)\boldsymbol{F}_8 & \boldsymbol{G}_4 \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & (v^2-1)\boldsymbol{I}_{k_5} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{G}_5 \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & (v^2+v)\boldsymbol{I}_{k_6} & \boldsymbol{0} & \boldsymbol{G}_6 \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & (v^2-v)\boldsymbol{I}_{k_7} & \boldsymbol{G}_7 \end{pmatrix}$$

其中 $\boldsymbol{G}_1=\boldsymbol{G}_{11}+v\boldsymbol{G}_{12}+v^2\boldsymbol{G}_{13}$, $\boldsymbol{G}_2=v\boldsymbol{G}_{21}+(v-1)\boldsymbol{G}_{22}+(v+1)\boldsymbol{G}_{23}+(v^2-1)\boldsymbol{G}_{24}+(v^2+v)\boldsymbol{G}_{25}+(v^2-v)\boldsymbol{G}_{26}$, $\boldsymbol{G}_3=(v-1)\boldsymbol{G}_{31}+(v+1)\boldsymbol{G}_{32}+(v^2-1)\boldsymbol{G}_{33}+(v^2+v)\boldsymbol{G}_{34}+(v^2-v)\boldsymbol{G}_{35}$, $\boldsymbol{G}_4=(v+1)\boldsymbol{G}_{41}+(v^2-1)\boldsymbol{G}_{42}+(v^2+v)\boldsymbol{G}_{43}+(v^2-v)\boldsymbol{G}_{44}$, $\boldsymbol{G}_5=(v^2-1)\boldsymbol{G}_{51}+(v^2+v)\boldsymbol{G}_{52}+(v^2-v)\boldsymbol{G}_{53}$, $\boldsymbol{G}_6=(v^2+v)\boldsymbol{G}_{61}+(v^2-v)\boldsymbol{G}_{62}$, $\boldsymbol{G}_7=(v^2-v)\boldsymbol{G}_{71}$, $\boldsymbol{A}$, $\boldsymbol{B}_1$, $\boldsymbol{B}_2$, $\boldsymbol{C}_1$, $\boldsymbol{C}_2$, $\boldsymbol{D}_1\sim\boldsymbol{D}_7$, $\boldsymbol{E}_1\sim\boldsymbol{E}_8$, $\boldsymbol{F}_1\sim\boldsymbol{F}_8$, $\boldsymbol{G}_{ij}(1\leqslant i\leqslant 7, 1\leqslant j\leqslant 6)$是 F_p 上的矩阵，$\boldsymbol{I}_{k_i}$是 $k_i\times k_i$ 阶的单位阵，并且线性码包含了 $p^{3k_1+2k_2+2k_3+2k_4+k_5+k_6+k_7}$个码字.设线性码 C 的对偶码 $C^{\perp}$的生成矩阵为 $\boldsymbol{H}$，则有 $\boldsymbol{G}^{\mathrm{T}}\boldsymbol{H}=\boldsymbol{0}$，其中 $\boldsymbol{G}^{\mathrm{T}}$ 为矩阵 $\boldsymbol{G}$ 的转置，由此可得 C 的对偶码 $C^{\perp}$的生成矩阵如下

$$\begin{pmatrix} \boldsymbol{H}_1 & \boldsymbol{H}_2 & \boldsymbol{H}_3 & \boldsymbol{H}_4 & \boldsymbol{H}_5 & \boldsymbol{H}_6 & \boldsymbol{H}_7 & \boldsymbol{I}_{n-(k_1+k_2+k_3+k_4+k_5+k_6+k_7)} \\ \boldsymbol{J}_1 & \boldsymbol{J}_2 & \boldsymbol{J}_3 & \boldsymbol{J}_4 & \boldsymbol{J}_5 & \boldsymbol{J}_6 & (v+1)\boldsymbol{I}_{k_7} & \boldsymbol{0} \\ \boldsymbol{K}_1 & \boldsymbol{K}_2 & \boldsymbol{K}_3 & \boldsymbol{K}_4 & \boldsymbol{K}_5 & (v-1)\boldsymbol{I}_{k_6} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{L}_1 & \boldsymbol{L}_2 & \boldsymbol{L}_3 & \boldsymbol{L}_4 & v\boldsymbol{I}_{k_5} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{M}_1 & \boldsymbol{M}_2 & \boldsymbol{M}_3 & (v^2-v)\boldsymbol{I}_{k_4} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{N}_1 & \boldsymbol{N}_2 & (v^2+v)\boldsymbol{I}_{k_3} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ (p-1)(v^2-1)\boldsymbol{A}^{\mathrm{T}} & (v^2-1)\boldsymbol{I}_{k_2} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \end{pmatrix}$$

其中 $\boldsymbol{H}_1\sim\boldsymbol{H}_7$, $\boldsymbol{J}_1\sim\boldsymbol{J}_6$, $\boldsymbol{K}_1\sim\boldsymbol{K}_5$, $\boldsymbol{L}_1\sim\boldsymbol{L}_4$, $\boldsymbol{M}_1\sim\boldsymbol{M}_3$, $\boldsymbol{N}_1$, $\boldsymbol{N}_2$ 是 R 上的矩阵，并且码字的个数为 $p^{3n-3k_1-2k_2-2k_3-2k_4-k_5-k_6-k_7}$.

定义 1　记 R 中元素的一个划分 $D_i,(i=0,1,2,3)$为：$D_0=\{0\}$, $D_1=\{bv\mid b\in F_p{}^*\}\cup\{cv^2\mid c\in F_p{}^*\}\cup\{c-cv^2\mid c\in F_p{}^*\}$, $D_2=\{bv+cv^2\mid b,c\in F_p{}^*\}\cup\{a\mid a\in F_p{}^*\}\cup\{a+cv^2\mid a,c\in F_p{}^*, a+c\neq 0(\mathrm{mod}\ p)\}\cup\{a+bv-av^2\mid a,b\in F_p{}^*\}$, $D_3=\{a+bv\mid a,b\in F_p{}^*\}\cup\{a+bv+cv^2\mid a,b,c\in F_p{}^*, a+c\neq 0(\mathrm{mod}\ p)\}$.

定义 2　$\forall r\in R$ 的 Lee 重量定义为 $W_L(r)=i$, $r\in D_i$，码字 $c=(c_0,c_1,\cdots c_{n-1})\in R^n$ 的 Lee 重量定义为 $W_L(c)=\sum_{i=0}^{n-1}W_L(c_i)$. 对 $\forall x=(x_0,x_1,\cdots,x_{n-1})\in R^n$，定义 $w_{D_j}(x)$为 x 中属于集合 D_j 的分量的个数，即有 $w_{D_j}(x)=\sum_{i=0}^{n-1}\delta_{D_j,x_i}$，其中 $\delta_{D_j,x_i}=\begin{cases}1, x_i\in D_j\\ 0, x_i\notin D_j\end{cases}$, $j=0,1,2,3$，则 $W_L(x)=W_{D_1}(x)+2W_{D_2}(x)+3W_{D_3}(x)$.

仿照文献[7]中的讨论，我们有如下引理.

引理 1　若 R^n 到 F_p^{3n} 的 Gray 映射为 $\varphi(a+bv+cv^2)=(a,a+c,b)$, $\forall a,b,c\in F_p^n$，则 φ 是从（R^n，Lee 距离）到（F_p^{3n}，Hamming 距离）的线性保距 Gray 映射.

利用引理 1，仿照文献[5]中引理 3.5 的方法可以证明如下结论.

定理 1　设 C 为 R 上长为 n 的线性码，$C^{\perp}$为其对偶码，则 $\varphi(C)$与 $\varphi(C^{\perp})$为域 F_p 上长为 $3n$ 的线性码，且也是互为对偶的.

3　环 R 上线性码的各种重量计数器及其 MacWilliams 恒等式

设 C 是 R 上长为 n 的线性码，若用 $B_i(i=0,1,2,\cdots,3n)$表示 C 中所有 Lee 重量为 i 的码字个数，则称 $\{B_0,B_1,\cdots,B_{3n}\}$为 C 的 Lee 重量分布，称 $\mathrm{Lee}_C(X,Y)=\sum_{i=0}^{3n}B_iX^{3n-i}Y^i$ 为 C 的 Lee 重量计数器，且 $\mathrm{Lee}_C(X,Y)=\sum_{c\in C}X^{3n-W_L(c)}Y^{W_L(c)}$.定义 R 上码 C 的对称重量计数器为 $swe_C(X_0,X_1,X_2,X_3)=\sum_{c\in C}X_0^{W_{D_0}(c)}X_1^{W_{D_1}(c)}X_2^{W_{D_2}(c)}X_3^{W_{D_3}(c)}$ 及码 C 的 Hamming 重量计数器 $Ham_C(X,Y)=\sum_{c\in C}X^{n-W_H(c)}Y^{W_H(c)}$，且 $W_H(c)=W_{D_1}(c)+W_{D_2}(c)+W_{D_3}(c)$，称为码字 C 的 Hamming 重量.

定理 2　关于以上这几种重量计数器的定义，有如下等式成立.

(1) $\mathrm{Lee}_C(X,Y)=swe_C(X^3,X^2Y,XY^2,Y^3)$, $\mathrm{Lee}_C(X,$

$Y)=W_{\varphi(C)}(X,Y)$;

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

证明　(1)由对称重量计数器的定义和引理 1 可得(1)和(2)中的第一个等式.由文献[6]中定理 2 的证明和定理 1 知,$W_{\Phi(C^{\perp})}(X,Y)=\frac{1}{|\Phi(C)|}W_{\Phi(C)}(X+(p-1)Y,X-Y)$,又因 $|C|=|\varphi(C)|$,利用本定理 1 中的第二个等式有 $\mathrm{Lee}_{C^{\perp}}(X,Y)=W_{\varphi(C^{\perp})}(X,Y)=\frac{1}{|\varphi(C)|}W_{\varphi(C)}(X+(p-1)Y,X-Y)=\frac{1}{|C|}\mathrm{Lee}_C(X+(p-1)Y,X-Y)$.

仿照文献[7]中定理 3,我们有如下定理.

定理 3　设 C 是 R 上长为 n 的线性码,则 R 上码 C 的 Lee 重量分布 $\{B_0,B_1,\cdots,B_{3n}\}$ 与其对偶码 $C^{\perp}$ 的 Lee 重量分布 $\{B_0',B_1',\cdots,B_{3n}'\}$ 的关系:$B_k'=\frac{1}{|C|}\sum_{i=0}^{3n}B_iP_k(i,3n)$,其中 $P_k(i,3n)$ 为 Krawtchouk 多项式,定义为 $P_k(i,n)=\sum_{j=0}^{k}(-1)^j(p-1)^{k-j}C_i^jC_{n-i}^{k-j}$.

设 C 是 R 上长为 n 的线性码,$a\in R$,对 $\forall\, x=(x_1,x_2,\cdots,x_n)\in R^n$,定义 x 在 a 的重量为 $w_a(x)=\sum_{i=1}^{n}\delta_{a,x_i}$,其中 $\delta_{a,x_i}=\begin{cases}1, x_i=a\\ 0, x_i\neq a.\end{cases}$

定义 3　定义码 C 的完全重量计数器为

$cwe_C(X_0,X_1,\cdots,X_{(p-1)+(p-1)v+(p-1)v^2})=\sum_{c\in C}\prod_{r\in R}X_r^{w_r(c)}=X_0^{w_0(c)}X_1^{w_1(c)}\cdots X_{(p-1)+(p-1)v+(p-1)v^2}^{w_{(p-1)+(p-1)v+(p-1)v^2}(c)}$.

定义 4　定义 χ 为从环 R 到复数域 $\mathbb{C}$ 的特征,对 $\forall\, x=a+bv+cv^2\in R$,有 $\chi(x)=\xi^c$,其中 $\xi=e^{2\pi i/p}$.

引理 2　设 C 是 R 上长为 n 的线性码,$C^{\perp}$ 为 C 的对偶码,对 $\forall\, x,y\in R^n$,$\sum_{x\in C^{\perp}}f(x)=\frac{1}{|C|}\sum_{x\in C}\hat{f}(x)$,其中 $\hat{f}(x)=\sum_{y\in R^n}\chi(x\cdot y)f(y)$,$\forall\, x\in R^n$,$f$ 为定义在 R^n 上取值于 $\mathbb{C}[X_0,X_1,\cdots,X_{(p-1)+(p-1)v+(p-1)v^2}]$ 的函数.

定理 4　设 C 是 R 上长为 n 的线性码,$C^{\perp}$ 为 C 的对偶码,则

$$cwe_{C^{\perp}}(X_0,X_1,\cdots,X_{(p-1)+(p-1)v+(p-1)v^2})=\frac{1}{|C|}cwe_C\Big(\sum_{r\in R}\chi(0r)X_r,\sum_{r\in R}\chi(1r)X_r,\cdots,\sum_{r\in R}\chi(((p-1)+(p-1)v+(p-1)v^2)r)X_r\Big).$$

证明　在引理 2 中令 $f(x)=\prod_{r\in R}X_r^{w_r(x)}=X_0^{w_0(x)}X_1^{w_1(x)}\cdots X_{(p-1)+(p-1)v+(p-1)v^2}^{w_{(p-1)+(p-1)v+(p-1)v^2}(x)}$,$\forall\, x\in R^n$,则 $\hat{f}(x)=\sum_{y\in R^n}\chi(x\cdot y)X_0^{w_0(y)}X_1^{w_1(y)}\cdots X_{(p-1)+(p-1)v+(p-1)v^2}^{w_{(p-1)+(p-1)v+(p-1)v^2}(y)}$. 又对 $\forall\, a\in R$,$w_a(y)=\delta_{a,y_1}+\delta_{a,y_2}+\cdots+\delta_{a,y_n}$,则有

$$\begin{aligned}\hat{f}(x)&=\sum_{y\in R^n}\big(\chi(x_1y_1)X_0^{\delta_{0,y_1}}X_1^{\delta_{1,y_1}}\cdots X_{(p-1)+(p-1)v+(p-1)v^2}^{\delta_{(p-1)+(p-1)v+(p-1)v^2,y_1}}\big)\\&\quad\cdots\big(\chi(x_ny_n)X_0^{\delta_{0,y_n}}\cdots X_{(p-1)+(p-1)v+(p-1)v^2}^{\delta_{(p-1)+(p-1)v+(p-1)v^2,y_n}}\big)\\&=\Big(\sum_{y_1\in R}\chi(x_1y_1)X_0^{\delta_{0,y_1}}X_1^{\delta_{1,y_1}}\cdots X_{(p-1)+(p-1)v+(p-1)v^2}^{\delta_{(p-1)+(p-1)v+(p-1)^2v,y_1}}\Big)\\&\quad\cdots\Big(\sum_{y_n\in R}\chi(x_ny_n)X_0^{\delta_{0,y_n}}\cdots X_{(p-1)+(p-1)v+(p-1)v^2}^{\delta_{(p-1)+(p-1)v+(p-1)v^2,y_n}}\Big)\\&=\Big(\sum_{r\in R}\chi(x_1r)X_r\Big)\cdots\Big(\sum_{r\in R}\chi(x_nr)X_r\Big)\end{aligned}$$

注意到 x 中等于 j 的分量恰好有 $w_j(x)$ 个,所以 $\hat{f}(x)=\prod_{j\in R}\Big(\sum_{r\in R}\chi(jr)X_r\Big)^{w_j(x)}$,由引理 2 知,

$$\begin{aligned}&cwe_{C^{\perp}}(X_0,X_1,\cdots,X_{(p-1)+(p-1)v+(p-1)v^2})\\&=\sum_{c\in C^{\perp}}\prod_{r\in R}X_r^{w_r(c)}=\sum_{c\in C^{\perp}}f(x)\\&=\frac{1}{|C|}\sum_{x\in C}\hat{f}(x)=\frac{1}{|C|}\sum_{x\in C}\prod_{j\in R}\Big(\sum_{r\in R}\chi(jr)X_r\Big)^{w_j(x)}\\&=\frac{1}{|C|}cwe_C\Big(\sum_{r\in R}\chi(0r)X_r,\sum_{r\in R}\chi(1r)X_r,\cdots,\\&\sum_{r\in R}\chi(((p-1)+(p-1)v+(p-1)v^2)r)X_r\Big).\end{aligned}$$

定义 5[8]　设 C_1,C_2 是 R 上两个长为 n 的线性码,如果存在一个 n 维单调变换 μ 使得 $\mu(C_1)=C_2$,其中 $\mu(C_1)=\{\mu(c)\mid c\in C_1\}$,则称 C_1 和 C_2 是数乘等价的.

数乘等价的 R 码的完全重量计数器可能是不同的,为此,我们给出对称重量计数器的概念,其意义在于数乘等价的码的对称重量计数器是相同的.

定义 6　码 C 的对称重量计数器又可定义为

$swe_C(X_0,X_1,X_2,X_3)=cwe_C(X_{I(0)},X_{I(1)},\cdots,X_{I((p-1)+(p-1)v+(p-1)v^2)})$,其中 $I(a)=i$,$\forall\, a\in D_i$,$i=0,1,2,3$.

引理 3　符号定义与前面同,则有

(1)若 $i\in D_0$,$\sum_{r\in D_0}\chi(ir)=1$,$\sum_{r\in D_1}\chi(ir)=3(p-1)$,$\sum_{r\in D_2}\chi(ir)=3(p-1)^2$,$\sum_{r\in D_3}\chi(ir)=(p-1)^3$;

(2)若 $i\in D_1$,$\sum_{r\in D_0}\chi(ir)=1$,$\sum_{r\in D_1}\chi(ir)=2p-3$,$\sum_{r\in D_2}\chi(ir)=(p-1)(p-3)$,$\sum_{r\in D_3}\chi(ir)=-(p-1)^2$;

(3)若 $i\in D_2$,则有 $\sum_{r\in D_0}\chi(ir)=1$,$\sum_{r\in D_1}\chi(ir)=p-3$,$\sum_{r\in D_2}\chi(ir)=3-2p$,$\sum_{r\in D_3}\chi(ir)=p-1$;

(4)若 $i\in D_3$,则有 $\sum_{r\in D_0}\chi(ir)=1$,$\sum_{r\in D_1}\chi(ir)=-3$,

$\sum_{r\in D_2}\chi(ir)=3,\sum_{r\in D_3}\chi(r)=-1.$

证明 由定义 1 和定义 4,我们有

(1)若 $i\in D_0$,则$\sum_{r\in D_0}\chi(ir)=1,\sum_{r\in D_1}\chi(ir)=|D_1|=3(p-1),\sum_{r\in D_2}\chi(ir)=|D_2|=3(p-1)^2,\sum_{r\in D_3}\chi(ir)=|D_3|=(p-1)^3$;

(2)若 $i\in D_1$,则有$\sum_{r\in D_0}\chi(ir)=\chi(0)=1$;当 $i=yv,y\in F_p^*$ 时,$\sum_{r\in D_1}\chi(ir)=\sum_{b\in F_p^*}\xi^{by}+\sum_{c\in F_p^*}\xi^0+\sum_{a\in F_p^*}\xi^o=2p-3,\sum_{r\in D_2}\chi(ir)=\sum_{a\in F_p^*}\xi^0+\sum_{b\in F_p^*}\sum_{c\in F_p^*}\xi^{by}+\sum_{a\in F_p^*}\sum_{c\in F_p^*,c\neq -a}\xi^0+\sum_{a\in F_p^*}\sum_{b\in F_p^*}\xi^{by}=(p-1)(p-3),\sum_{r\in D_3}\chi(ir)=\sum_{a\in F_p^*}\sum_{b\in F_p^*}\xi^{by}+\sum_{a\in F_p^*}\sum_{b\in F_p^*}\sum_{c\in F_p^*,c\neq -a}\xi^{by}=-(p-1)^2$;

类似地,可证当 $i=zv^2,z\in F_p^*$ 和 $i=x-xv^2,x\in F_p^*$ 时结论成立.(3)和(4)证明过程同(2).

引理 4 对$\forall\, i,j$属于同一个 $D_l,l=0,1,2,3$,总有$\sum_{r\in R}\Phi(ir)=\sum_{r\in R}\Phi(jr)$.

证明 由引理 3 可知,当 $i,j\in D_0$ 时,$\sum_{r\in R}\chi(ir)=\sum_{r\in R}\chi(jr)=p^3$;当 $i,j\in D_1$、D_2 和 D_3 时,$\sum_{r\in R}\chi(ir)=\sum_{r\in R}\chi(jr)=0$.

定理 5 设 C 是 R 上长为 n 的线性码,$C^\perp$为 C 的对偶码,则

$$swe_{C^\perp}(X_0,X_1,X_2,X_3)=\frac{1}{|C|}swe_C(X_0+3(p-1)X_1+3(p-1)^2X_2+(p-1)^3X_3,X_0+(2p-3)X_1+(p-1)(p-3)X_2-(p-1)^2X_3,X_0+(p-3)X_1+(3-2p)X_2+(p-1)X_3,X_0-3X_1+3X_2-X_3).$$

证明 由定理 4 可知

$$swe_{C^\perp}(X_0,X_1,X_2,X_3)=cwe_{C^\perp}(X_{I(0)},X_{I(1)},\cdots,X_{I((p-1)+(p-1)v+(p-1)v^2)})$$
$$=\frac{1}{|C|}cwe_C\Big(\sum_{r\in R}\Phi(0r)X_{I(r)},\sum_{r\in R}\Phi(1r)X_{I(r)},\cdots,\sum_{r\in R}\Phi(((p-1)+(p-1)v+(p-1)v^2)r)X_{I(r)}\Big)$$
$$=\frac{1}{|C|}cwe_C\Big(\sum_{s=0}^{3}\sum_{r\in D_s}\Phi(0r)X_s,\sum_{s=0}^{3}\sum_{r\in D_s}\Phi(1r)X_s,\cdots,\sum_{s=0}^{3}\sum_{r\in D_s}\Phi(((p-1)+(p-1)v+(p-1)v^2)r)X_s\Big)$$

由引理 4,若 i,j 属于同一集合 D_i,则$\sum_{s=0}^{3}\sum_{r\in D_s}\Phi(ir)X_s=\sum_{s=0}^{3}\sum_{r\in D_s}\Phi(jr)X_s$,故

$$swe_{C^\perp}(X_0,X_1,X_2,X_3)=\frac{1}{|C|}swe_C\Big(\sum_{s=0}^{3}\sum_{r\in D_s}\Phi(0r)X_s,\sum_{s=0}^{3}\sum_{r\in D_s}\Phi(vr)X_s,\sum_{s=0}^{3}\sum_{r\in D_s}\Phi(1r)X_s,\sum_{s=0}^{3}\sum_{r\in D_s}\Phi((1+v)r)X_s\Big),$$

其中 $0,v,1,1+v$ 依次取自 D_0,D_1,D_2,D_3,由引理 3 知

$$\sum_{s=0}^{3}\sum_{r\in D_s}\Phi(0r)X_s=X_0+3(p-1)X_1+3(p-1)^2X_2+(p-1)^3X_3,$$
$$\sum_{s=0}^{3}\sum_{r\in D_s}\Phi(vr)X_s=X_0+(2p-3)X_1+(p-1)(p-3)X_2-(p-1)^2X_3,$$
$$\sum_{s=0}^{3}\sum_{r\in D_s}\Phi(1r)X_s=X_0+(p-3)X_1+(3-2p)X_2+(p-1)X_3,$$
$$\sum_{s=0}^{3}\sum_{r\in D_s}\Phi((1+v)r)X_s=X_0-3X_1+3X_2-X_3,$$

因此有,$swe_{C^\perp}(X_0,X_1,X_2,X_3)=\frac{1}{|C|}swe_C(X_0+3(p-1)X_1+3(p-1)^2X_2+(p-1)^3X_3,X_0+(2p-3)X_1+(p-1)(p-3)X_2-(p-1)^2X_3,X_0+(p-3)X_1+(3-2p)X_2+(p-1)X_3,X_0-3X_1+3X_2-X_3)$.

推论 1 由定理 5 可以给出定理 2 中(2)的第二个等式的另外一种证明,即

$$Lee_{C^\perp}(X,Y)=swe_{C^\perp}(X^3,X^2Y,XY^2,Y^3)$$
$$=\frac{1}{|C|}swe_C(X^3+3(p-1)X^2Y+3(p-1)^2XY^2+(p-1)Y^3,X^3+(2p-3)X^2Y+(p-1)(p-3)XY^2-(p-1)^2Y^3,X^3+(p-3)X^2Y+(3-2p)XY^2+(p-1)Y^3,X^3-3X^2Y+3XY^2-Y^3)$$
$$=\frac{1}{|C|}swe_C((X+(p-1)Y)^3,(X+(p-1)Y)^2(X-Y),(X+(p-1)Y)(X-Y)^2,(X-Y)^3)$$
$$=\frac{1}{|C|}Lee_C(X+(p-1)Y,X-Y).$$

推论 2 设 C 与 $C^\perp$是 R 上的互为对偶的线性码,则 $Ham_{C^\perp}(X,Y)=\frac{1}{|C|}Ham_C(X+(p^3-1)Y,X-Y)$.

4 应用举例

下面通过一个例子来说明本文主要结果的应用.

设 C 是环 $F_3+vF_3+v^2F_3$ 上长为 2 的线性码,其生成矩阵为 $\boldsymbol{G}=\begin{pmatrix}v+1&0\\0&v\end{pmatrix}$,有 81 个码字.由 $C^\perp$的生成矩阵可知,$C^\perp$是由 $\boldsymbol{H}=\begin{pmatrix}v^2+2v&v^2-1\\v^2-v&0\end{pmatrix}$生成的线性

码,有 9 个码字,即 $C^{\perp}=\{(0,0),(2v^2+v,2v^2+1),(v^2+2v,v^2+2),(2v^2+v,v^2+2),(v^2+2v,2v^2+1),(2v^2+v,0),(0,v^2+2),(v^2+2v,0),(0,2v^2+1)\}$.

根据前面介绍的定义,有 $swe_{C^{\perp}}(X_0,X_1,X_2,X_3)=X_0^2+2X_0X_1+2X_0X_2+4X_1X_2$, $Ham_{C^{\perp}}(X,Y)=X^2+4Y^2+4XY$, $Lee_{C^{\perp}}(X,Y)=X^6+2X^5Y+2X^4Y^2+4X^3Y^3$.

因为 $|C^{\perp}|=9$ 较小, $|C|=81$ 较大,通过 $C^{\perp}$ 的各种重量分布,直接可得 C 的重量分布,而不需要去求出码 C 中的具体码字.根据定理 5,得码 $C^{\perp}$ 的对偶码 C 的对称重量计数器为 $swe_c(X_0,X_1,X_2,X_3)=\frac{1}{|C^{\perp}|}swe_{C^{\perp}}(X_0+6X_1+12X_2+8X_3,X_0+3X_1-4X_3,X_0-3X_2+2X_3,X_0-3X_1+3X_2-X_3)=X_0^2+8X_1^2+X_2^2+6X_0X_1+4X_0X_3+16X_1X_2+16X_1X_3+16X_2X_3$

根据推论 2,得码 $C^{\perp}$ 的对偶码 C 的 Hamming 重量计数器 $Ham_C(X,Y)=\frac{1}{|C^{\perp}|}Ham_{C^{\perp}}(X+26Y,X-Y)=X^2+64Y^2+16XY$.根据定理 2 和推论 1 可得码 $C^{\perp}$ 的对偶码 C 的 Lee 重量计数器为 $\mathrm{Lee}_C(X,Y)=X^6+6X^5Y+14X^4Y^2+20X^3Y^3+24X^2Y^4+16XY^5$.

另一方面,可以将码 C 中的 81 个码字全部列出来,直接验证可知所得的结论是完全正确的.

注:对于 C 的 Lee 重量分布,我们还可以通过定理 3 来计算.在本例中,因为 $B_0'=1$, $B_1'=B_2'=2$, $B_3'=4$,由定理 3 中 B_i 与 B_i' 的关系知, $B_0=1$, $B_1=6$, $B_2=14$, $B_3=20$, $B_4=24$, $B_5=16$ 与由定理 2 计算的结果一致.

5　结束语

建立了环 $F_p+vF_p+v^2F_p$ 上线性码及其对偶码之间各种重量计数器的 MacWilliams 恒等式.我们采用了不同的方法,(横向)推广了文献[7]中的结果($p=2$ 的情形);且建立了该环上线性码及其对偶码之间关于完全重量和对称重量计数器的 MacWilliams 恒等式,而这两个 MacWilliams 恒等式在文献[7]中没有被包含,这又从纵向推广了文献[7]中的结果.

参考文献

[1] Z X Wan. Quaternary Codes[M]. River Edge N J: World Scientific Pub, 1997.

[2] 朱士信,等.环 Z_4 上线性码关于 RT 的 MacWilliams 恒等式[J].电子学报,2009,37(5):1115–1118.
Zhu Shixin, et al. MacWilliams identities of Linear codes over ring Z_4 with respect to the RT Metric[J]. Acta Electronica Sinica, 2009, 37(5): 1115–1118. (in Chinese)

[3] Zhu Shixin, Tang yongsheng. A MacWilliams type identity on Lee weight for linear codes over F_2+uF_2[J]. Journal of System Sciences & Complexity, 2012, 25(1): 186–194.

[4] 朱士信. Z_k 上线性码的对称形式的 MacWilliams 恒等式[J].电子与信息学报,2003,25(7):901–906.
Zhu Shixin. A symmetrized MacWilliams identity of Z_k-linear code[J]. Journal of Electronics and Information Technology, 2003, 25(7): 901–906. (in Chinese)

[5] Shixin Zhu, Yu Wang, Minjia Shi. Some result on cyclic code over F_2+vF_2[J]. IEEE Transactions on Information Theory 2010, 56(4): 1680–1684.

[6] 施敏加,等.非主理想环 F_p+vF_p 上线性码的 MacWilliams 恒等式[J].电子学报,2011,39(10):2449–2453.
Shi Minjia, et al. MacWilliams identities of linear codes over non-principal ring F_p+vF_p[J]. Acta Electronica Sinica, 2011, 39(10): 2449–2453. (in Chinese)

[7] MinJia Shi, Patrick Solé, Bo Wu. Cyclic codes and the weight enumerator of linear codes over $F_2+vF_2+v^2F_2$[J]. Appl Comput Math, 2013, 12(2): 247–255.

[8] 李雨,陈鲁生.环 F_p+uF_p 上线性码的 MacWilliams 恒等式[J].南开大学学报,2010,4(2):78–84.
Li Yu, Chen Lusheng. MacWilliams identities of linear codes over ring F_p+uF_p[J]. Acta Scientiarum Naturalium Universitatis Nankaiensis, 2010, 4(2): 78–84. (in Chinese)

作者简介

施敏加　男,1980 年生于安徽安庆,博士,安徽大学数学科学学院副教授,硕士生导师,主要研究方向为代数编码与密码.
E-mail: smjwcl.good@163.com

刘　艳　女,1989 年生于安徽合肥,硕士研究生.研究方向为代数编码.