环 Z4 + uZ4 线性码关于李重量的一类 MacWilliams 恒等式

李 平[1],李珊珊[1],唐永生[2]
(1.合肥工业大学数学学院,安徽合肥 230009; 2.合肥师范学院数学与统计学院,安徽合肥 230601)

摘 要: MacWilliams 恒等式是研究线性码及其对偶码的码字重量分布的一个非常有用的工具,而码字的重量分布的研究是编码研究中一个非常重要的研究方向.本文定义了环 $Z4+uZ4$ 上长度为 n 的线性码的 m-层李重量计数器,给出了环 $Z4+uZ4$ 上长度为 n 的线性码关于李重量的一类 MacWilliams 恒等式.证明了该等式是生成矩阵在环 $Z4+uZ4$ 上的环 $GR(4,m)+uGR(4,m)$上线性码关于李重量的 MacWilliams 恒等式.进一步,利用 Krawtchouk 多项式,获得了环 $Z4+uZ4$ 上长度为 n 的线性码的等价形式 MacWilliams 恒等式.

关键词: 线性码; 李重量; m-层重量计数器; MacWilliams 恒等式
中图分类号: TN911.22 **文献标识码:** A **文章编号:** 0372-2112 (2015)12-2461-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.12.017

A Type of MacWilliams Identity for Linear Codes over $Z4+uZ4$ on Lee Weight

LI Ping[1], LI Shan-shan[1], TANG Yong-sheng[2]
(1. *School of Mathematics, Hefei University of Technology, Hefei, Anhui* 230009, *China*;
2. *School of Mathematics and Statistics, Hefei Normal University, Hefei, Anhui* 230601, *China*)

Abstract: MacWilliams identity is an useful tool in studying weight distributions of linear codes and their duals. Weight distribution is also an important topic of coding theory. This paper defines the m-ply Lee weight enumerators for linear codes of length n over $Z4+u\ Z4$. We give a type of Mac-Williams identity for linear codes of length n over $Z4+u\ Z4$ on Lee weight. We prove that this identity is the MacWilliams identity on Lee weight for linear codes over $GR(4,m)+uGR(4,m)$ having generator matrix over $Z4+u\ Z4$. Furthermore, by means of Krawtchouk polynomials the equivalent form of the type of MacWilliams identity for linear codes of length n over $Z4+u\ Z4$ is obtained.

Key words: linear codes; Lee weight; m-ply weight enumerator; MacWilliams identities

1 引言

二十世纪九十年代,Hammons[1]等人证明了非线性二元 Preparata 码和 Kerdock 码是环$\mathbb{Z}_4$上线性码并且满足 MacWilliams 恒等式,解决这一问题的关键是环$\mathbb{Z}_4$上码字的李重量,主要是通过 Gray 映射将环$\mathbb{Z}_4$上码字的李重量与其 Gray 像建立了联系.从此以后,有限环上的纠错码理论得到了编码研究者的广泛关注.近年来,编码研究者对剩余类多项式环$\mathbb{F}_{p^s}+u\ \mathbb{F}_{p^s}+\cdots+u^{k-1}\mathbb{F}_{p^s}$产生了极大的兴趣($p$ 为素数并且 $u^k=0$). Bachoc[2]利用了环$\mathbb{F}_p+u\ \mathbb{F}_p$上的线性码进行格的构造.施敏加等人[3,4]分别研究了环$\mathbb{F}_2+u\ \mathbb{F}_2$上长度为 2^s 的循环码距离和环$\mathbb{F}_p+v\ \mathbb{F}_p$上线性码的 Gray 像. Dinh 和 Nguyen[5]研究了环$\mathbb{F}_{2^m}+u\ \mathbb{F}_{2^m}+\cdots+u^{a-1}\mathbb{F}_{2^m}$上的常循环码. Zhu 和 Wang[6]讨论了环$\mathbb{F}_p+v\ \mathbb{F}_p$上一类常循环码并利用 Gray 映射获得了域$\mathbb{F}_p$上一批最优码. Kai 等人[7]研究了环$\mathbb{F}_2+u\ \mathbb{F}_2+v\ \mathbb{F}_2+uv\ \mathbb{F}_2$上一类常循环码的 Gray 像. Yildiz 和 Karadeniz[8]研究了环$\mathbb{Z}_4+u\ \mathbb{Z}_4$上的线性码和形式自对偶码.

收稿日期:2014-05-06;修回日期:2014-09-22;责任编辑:覃怀银
基金项目:国家自然科学基金(No.61370089);安徽省自然科学基金(No.1408085QF116);安徽省高校省级科学研究项目(No.KJ2013B221);合肥工业大学博士专项科研资助基金(No.JZ2014HGBZ0029);中央高校基本科研业务费专项资金资助项目(No.J2014HGXJ0073);东南大学移动通信国家重点实验室开放研究基金资助课题(2014D04);2014 年安徽省高校优秀青年人才支撑计划项目(No.皖教秘人[2014]181);合肥师范学院校级科研机构基金(No.2015JG09)

MacWilliams[9]恒等式是描述线性码的码字的各种重量分布与其对偶码的码字的相应的重量分布之间的相互关系,并且这一等式得到广泛应用.Wei[10]讨论了有限域上线性码的支重量及其广义汉明重量,并且介绍了线性码的广义汉明重量在第二型密切信道(the wire-tap channel of type Ⅱ)中的作用.后来,人们通过定义线性码的各种不同的广义重量计数器,得到了各种不同形式的广义 MacWilliams 恒等式.Shiromoto[11,12]分别讨论了有限环上线性码的关于李重量和欧几里得重量的 MacWilliams 恒等式和生成矩阵在 GF(q)上的 GF(q^m)线性码的重量计数器.Cui 和 Pei[13]给出了环$\mathbb{Z}_4$上线性码的广义 MacWilliams 恒等式.Dougherty[14]等人研究了环$\mathbb{Z}_4$上线性码的广义李重量并且给出了有限环上广义汉明重量的 MacWilliams 恒等式.唐永生[15]深入研究了有限环上线性码的 MacWilliams 恒等式.

本文利用了文献[15,16]的方法,定义了环$\mathbb{Z}_4+u\mathbb{Z}_4$上长度为 n 的线性码的 m-层李重量计数器,给出了环$\mathbb{Z}_4+u\mathbb{Z}_4$上长度为 n 的线性码的关于李重量的一类 MacWilliams 恒等式.证明了该等式是生成矩阵在环$\mathbb{Z}_4+u\mathbb{Z}_4$上的环 $\mathrm{GR}(4,m)+u\mathrm{GR}(4,m)$上线性码关于李重量的 MacWilliams 恒等式.进一步,利用 Krawtchouk 多项式,获得了环$\mathbb{Z}_4+u\mathbb{Z}_4$上长度为 n 的线性码的等价形式的 MacWilliams 恒等式.

2 预备知识

设$\mathbb{Z}_4+u\mathbb{Z}_4=\mathbb{Z}_4[u]/(u^2)$是一个特征为 4 的交换环并且 $u^2=0$.环$\mathbb{Z}_4+u\mathbb{Z}_4$上的任意元素 r 都可唯一表示为:$r=a+ub$,这里的 $a,b\in\mathbb{Z}_4$.设 n 是一个正整数,$(\mathbb{Z}_4+u\mathbb{Z}_4)^n$是由$\mathbb{Z}_4+u\mathbb{Z}_4$上的 n 维向量所组成的集合,即:$(\mathbb{Z}_4+u\mathbb{Z}_4)^n=\{(x_1,x_2,\cdots,x_n)\mid x_i\in\mathbb{Z}_4+u\mathbb{Z}_4,i=1,2,\cdots,n\}$.设 C 是$(\mathbb{Z}_4+u\mathbb{Z}_4)^n$中一个子加群,那么称 C 为环$\mathbb{Z}_4+u\mathbb{Z}_4$上一个长度为 n 的线性码.对于任意的 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n),\boldsymbol{y}=(y_1,y_2,\cdots,y_n)\in(\mathbb{Z}_4+u\mathbb{Z}_4)^n$,定义

$$\boldsymbol{x}\cdot\boldsymbol{y}=x_1y_1+x_2y_2+\cdots+x_ny_n \tag{1}$$

称为 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的内积.若 $\boldsymbol{x}\cdot\boldsymbol{y}=0$,则称 $\boldsymbol{x}$ 与 $\boldsymbol{y}$ 是正交的.

设 C 是环$\mathbb{Z}_4+u\mathbb{Z}_4$上一个长度为 n 的线性码,定义为:$C^{\perp}=\{\boldsymbol{x}\in(\mathbb{Z}_4+u\mathbb{Z}_4)^n\mid\boldsymbol{x}\cdot\boldsymbol{y}=0,\forall\,\boldsymbol{y}\in C\}$.易证 $C^{\perp}$也是一个线性码,称为 C 的对偶码.设 $N=\{1,2,\cdots,n\}$,对任意的 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in(\mathbb{Z}_4+u\mathbb{Z}_4)^n$ 的支集定义为:$\mathrm{Supp}(\boldsymbol{x})=\{i\in N\mid x_i\neq0\}$.对于$\mathbb{Z}_4$中的元素 0,1,2,3,其李重量分别定义为 0,1,2,1.对于向量 $\boldsymbol{c}\in\mathbb{Z}_4^n$,它的李重量定义为各个分量的李重量之和.定义李重量的支集形式:$\mathrm{Supp}_L(c)=\{i\mid c_i=1\text{ 或者 }c_i=3\}\cup\{j,j\mid c_j=2\}$,这里的 $\mathrm{Supp}_L(c)$视为多重集.很显然,$|\mathrm{Supp}_L(c)|=\mathrm{Lee}(c)$.

注 对任意正整数 b 和有限集 $M=\{i_1,i_2,\cdots,i_t\}\subseteq N$,多重集 bM 记为 $bM=\{\overbrace{i_1,\cdots,i_1}^{b},\overbrace{i_2,\cdots,i_2}^{b},\cdots,\overbrace{i_t,\cdots,i_t}^{b}\}$.

设 C 是环$\mathbb{Z}_4$上长度为 $2n$ 的线性码,C 的李重量计数器定义为:$\mathrm{Lee}_c(x,y)=\sum_{c\in C}x^{4n-\mathrm{Lee}(c)}y^{\mathrm{Lee}(c)}$.显然有 $\mathrm{Lee}_C(x,y)=\sum_{i=0}^{4n}A_ix^{4n-i}y^i$,这里的 A_i 表示 C 中所有李重量为 i 的码字个数.环$\mathbb{Z}_4+u\mathbb{Z}_4$上的 Gray 映射定义为[8]:

$$\begin{aligned}\Phi:\mathbb{Z}_4+u\mathbb{Z}_4&\longrightarrow\mathbb{Z}_4^2\\(a+ub)&\longmapsto(b,a+b)\end{aligned} \tag{2}$$

环$\mathbb{Z}_4+u\mathbb{Z}_4$中任一元素 $a+ub$ 的李重量 w_L 定义为:$w_L(a+ub)=w_L(b,a+b)$.这个映射可以自然地推广$(\mathbb{Z}_4+u\mathbb{Z}_4)^n\to\mathbb{Z}_4^{2n}$,并且是一个由$((\mathbb{Z}_4+u\mathbb{Z}_4)^n$,李重量)到$(\mathbb{Z}_4^{2n}$,李重量)的保重量和保线性的双射.从而,对任意的 $\boldsymbol{c}\in(\mathbb{Z}_4+u\mathbb{Z}_4)^n$,$w_L(c)=w_L(\Phi(c))$.

设 $C\subseteq V=(\mathbb{Z}_4+u\mathbb{Z}_4)^n$是$\mathbb{Z}_4+u\mathbb{Z}_4$上线性码,$S\subseteq N=\{1,2,\cdots,n\}$,定义:

$$V(S)=\{v\in V\mid\mathrm{Supp}(v)\subseteq S\} \tag{3}$$

$$C(S)=C\cap V(S)=\{c\in C\mid\mathrm{Supp}(c)\subseteq S\} \tag{4}$$

很显然 $V(S)$和 $C(S)$都是 V 的子模.设 $C^*=\mathrm{Hom}_R(C,R)$,定义一个 R 上映射:

$$\begin{aligned}f:V&\longrightarrow C^*\\y&\longmapsto(\hat{y}:x\longmapsto\langle x,y\rangle)\end{aligned} \tag{5}$$

则 f 是 R 上一个满射且易得 R 上一个同构:$C^*\cong V/C^{\perp}$.

因为环$\mathbb{Z}_4+u\mathbb{Z}_4$是一个拟弗罗贝尼斯环(quasi-Frobenius rings),所以$|C|\cdot|C^{\perp}|=16^n$并且下面的引理成立.

引理 1[17] 设 C 是环$\mathbb{Z}_4+u\mathbb{Z}_4$上长度为 n 的线性码,$S\subseteq N=\{1,2,\cdots,n\}$是任一子集,那么$\mathbb{Z}_4+u\mathbb{Z}_4$模有下面基本正合序列

$$0\to C^{\perp}(S)\xrightarrow{\text{inclusion}}V(S)\xrightarrow{f}C^*\xrightarrow{\text{restriction}}C(N-S)^*\to0 \tag{6}$$

这里的 inclusion,restriction 分别表示包含和限制映射.

Yildiz 和 Karadeniz 在文献[8]中环$\mathbb{Z}_4+u\mathbb{Z}_4$上长度为 n 的线性码 C 的李重量计数器定义为:$\mathrm{Lee}_C(x,y)=\sum_{c\in C}x^{4n-w_L(c)}y^{w_L(c)}$,得到了环$\mathbb{Z}_4+u\mathbb{Z}_4$上长度为 n 的线性码 C 关于李重量的 MacWilliams 恒等式为:$\mathrm{Lee}_{C^{\perp}}(x,y)=\frac{1}{|C|}\mathrm{Lee}_C(x+y,x-y)$.

3 环$\mathbb{Z}_4+u\mathbb{Z}_4$上线性码关于李重量的一类 MacWilliams 恒等式

定义 1 环$\mathbb{Z}_4+u\mathbb{Z}_4$上长度为 n 的线性码 C 关于李重量的 m-层重量计数器定义为:

$$\mathrm{Lee}_C^{(m)}(x,y)=\sum_{c^1,\cdots,c^m\in C}x^{4n-s(c^1,\cdots,c^m)}y^{s(c^1,\cdots,c^m)} \tag{7}$$

这里的 $s(c^1,\cdots,c^m)=|\mathrm{Sup}\,\mathrm{p}_L(c^1)\cup\cdots\cup\mathrm{Sup}\,\mathrm{p}_L(c^m)|$.

线性码 C 的另一种 m-层李重量计数器定义为:$\mathrm{Lee}_C^{'(m)}(x,y)=\sum_{S\subseteq N}|C(S)|^m x^{|4N-4S|}y^{|4S|}$.

定理 1　设 C 是环$\mathbb{Z}_4+u\mathbb{Z}_4$ 上长度为 n 的线性码,$C^{\perp}$是 C 的对偶码.那么

$$\mathrm{Lee}_{C^{\perp}}^{(m)}(x,y)=\frac{1}{|C|^m}\mathrm{Lee}_C^{(m)}(x+(2^m-1)y,x-y) \tag{8}$$

证明　根据 C 的另一种 m-层李重量计数器定义得:

$$\begin{aligned}
&\mathrm{Lee}_C^{'}(m)(x,y)\\
&=\sum_{S\subseteq N}|C(S)|^m x^{|4N-4S|}y^{|4S|}\\
&=\sum_{S\subseteq N}\Big(\sum_{T\subseteq 4S}\big|\{c^i\in C\mid \mathrm{Supp}_L(c^i)=T\}\big|\Big)^m\\
&\quad\cdot x^{|4N-4S|}y^{|4S|}\\
&=\sum_{S\subseteq N}\sum_{T_1,\cdots,T_m\subseteq 4S}\big|\{(c^1,\cdots,c^m)\mid c^i\in C,\mathrm{Supp}_L(c^i)=T_i\}\big|\\
&\quad\cdot x^{|4N-4S|}y^{|4S|}\\
&=\sum_{T_1,\cdots,T_m\subseteq 4N}\big|\{(c^1,\cdots,c^m)\mid c^i\in C,\mathrm{Supp}_L(c^i)=T_i\}\big|\\
&\quad\cdot\sum_{T_1\cup\cdots\cup T_m\subseteq 4S\subseteq 4N}x^{|4N-4S|}y^{|4S|}
\end{aligned}\tag{9}$$

记 $S'=T_1\cup\cdots\cup T_m$,$4S=S'\cup U$ 且 $S'\cap U=\varnothing$,则$|4S|=|S'|+|U|$.

根据二项等式得:

$$\begin{aligned}
&\mathrm{Lee}_C^{'(m)}(x,y)\\
&=\sum_{T_1,\cdots,T_m\subseteq 4S}\big|\{(c^1,\cdots,c^m)\mid c^i\in C,\mathrm{Supp}_L(c^i)=T_i\}\big|\\
&\quad\cdot\sum_{U\subseteq 4N-S'}x^{|4N|-|S'|-|U|}y^{|S'|+|U|}\\
&=\sum_{T_1,\cdots,T_m\subseteq 4N}\big|\{(c^1,\cdots,c^m)\mid c^i\in C,\mathrm{Supp}_L(c^i)=T_i\}\big|\\
&\quad\cdot(x+y)^{|4N|-|S'|}y^{|S'|}\\
&=\mathrm{Lee}_C^{(m)}(x+y,y)
\end{aligned}\tag{10}$$

这里的二项等式为:

$$\sum_{S'\subseteq 4S\subseteq 4N}x^{|4N|-|4S|}y^{|4S|}=\sum_{U\subseteq 4N-S'}x^{|4N|-|S'|-|U|}y^{|S'|+|U|}=(x+y)^{|4N|-|S'|}y^{|S'|}$$

同理根据 $C^{\perp}$的另一种 m-层李重量计数器的定义得:

$$\mathrm{Lee}_{C^{\perp}}^{'(m)}(x,y)=\mathrm{Lee}_{C^{\perp}}^{(m)}(x+y,y) \tag{11}$$

因此有:

$$\mathrm{Lee}_{C^{\perp}}^{(m)}(x,y)=\mathrm{Lee}_{C^{\perp}}^{'(m)}(x-y,y) \tag{12}$$

另一方面,根据引理 1 得:

$$|C|\cdot|C^{\perp}(S)|=|V(S)|\cdot|C(N-S)| \tag{13}$$

因为

$$\mathrm{Lee}_{C^{\perp}}^{'(m)}(x,y)=\sum_{S\subseteq N}|C^{\perp}(S)|^m x^{|4N|-|4S|}y^{|4S|} \tag{14}$$

所以根据等式(13)得:

$$\begin{aligned}
&\mathrm{Lee}_{C^{\perp}}^{'(m)}(x,y)\\
&=\sum_{S\subseteq N}\frac{1}{|C|^m}|V(S)|^m|C(N-S)|^m x^{|4N|-|4S|}y^{|4S|}\\
&=\frac{1}{|C|^m}\sum_{S\subseteq N}|C(N-S)|^m x^{|4N|-|4S|}(2^m y)^{|4S|}\\
&=\frac{1}{|C|^m}\sum_{S\subseteq N}|C(S)|^m x^{|4S|}(16^{\frac{m}{4}}y)^{|4N|-|4S|}\\
&=\frac{1}{|C|^m}\sum_{S\subseteq N}|C(S)|^m x^{|4S|}(2^m y)^{|4N|-|4S|}\\
&=\mathrm{Lee}_C^{'(m)}(2^m y,x)
\end{aligned}\tag{15}$$

因此

$$\begin{aligned}
\mathrm{Lee}_{C^{\perp}}^{(m)}(x,y)&=\mathrm{Lee}_{C^{\perp}}^{'(m)}(x-y,y)\\
&=\frac{1}{|C|^m}\mathrm{Lee}_C^{'(m)}(2^m y,x-y)\\
&=\frac{1}{|C|^m}\mathrm{Lee}_C^{(m)}(x+(2^m-1)y,x-y)
\end{aligned}\tag{16}$$

设 GR(4,m)是特征为 4,基数为 4^m,这里的 m 与定义 1 中的意义相同.可以认为 GR(4,m)是秩为 m 的$\mathbb{Z}_4$ 自由模.如果 $a_1,a_2,\cdots,a_m$ 是$\mathbb{Z}_4$ 自由的,并且生成$\mathbb{Z}_4$ 模 GR(4,m),那么$\{a_1,a_2,\cdots,a_m\}$称为$\mathbb{Z}_4$ 上 GR(4,m)一组基.设

$M=\mathbb{Z}_4+u\mathbb{Z}_4$,$\widetilde{M}=\mathrm{GR}(4,m)+u\mathrm{GR}(4,m)=\bigoplus_{l=1}^{m}Ma_l$

定义:

$$\widetilde{M}^n=\widetilde{M}\otimes_M M^n=\Big\{\sum_{l=1}^{m}a_l\otimes v^l\mid v^l\in M^n\Big\} \tag{17}$$

这里的$\otimes$表示 M 上的张量积,因此对 $v^l=(v_1^l,v_2^l,\cdots,v_n^l)$,

$$\sum_{l=1}^{m}a_l\otimes v^l=\Big(\sum_{l=1}^{m}a_l v_1^l,\sum_{l=1}^{m}a_l v_2^l,\cdots,\sum_{l=1}^{m}a_l v_n^l\Big) \tag{18}$$

类似定义:

$$C^{(m)}=\widetilde{M}\otimes_M C=\Big\{\sum_{l=1}^{m}a_l\otimes c^l\mid c^l\in C\Big\} \tag{19}$$

因此,对任意的 $\tilde{c}\in C^{(m)}$,$\mathrm{Lee}(\tilde{c})=\sum_{i=1}^{m}\mathrm{Lee}(c^l)$.

类似文献[11]中的定理 1,可以得到 $C^{(m)}$的李重量计数器与 C 的 m-层李重量计数器的关系.

定理 2　设 $\mathrm{Lee}_C(x,y)$是 $C^{(m)}$的李重量计数器,$\mathrm{Lee}_C^{(m)}(x,y)$表示 C 的 m-层李重量计数器;那么

$$\mathrm{Lee}_C(x,y)=\mathrm{Lee}_C^{(m)}(x,y) \tag{20}$$

设 C 是环$\mathbb{Z}_4+u\mathbb{Z}_4$ 上长度为 n 的线性码,$\{a_1,a_2,\cdots,a_m\}$是环$\mathbb{Z}_4+u\mathbb{Z}_4$ 一组自由基,C 的生成矩阵为 $\boldsymbol{G}$,那么 $C^{(m)}$是 GR(4,m)+uGR(4,m)上线性码,生成矩阵也为 $\boldsymbol{G}$.根据定理 1 和 2,得到下面的推论.

推论 1　设 $C^{(m)}$是环 GR(4,m)+uGR(4,m)上线性码,$(C^{(m)})^{\perp}$是 $C^{(m)}$的对偶码,$\mathrm{Lee}_C^{'}(x,y)$是$(C^{(m)})^{\perp}$

的李重量计数器,则有

$$\mathrm{Lee}'_C(x,y)=\frac{1}{|C|^m}\mathrm{Lee}_C(x+(2^m-1)y,x-y) \quad (21)$$

4 MacWilliams 恒等式的等价形式

下面我们将给出环$\mathbb{Z}_4+u\mathbb{Z}_4$上线性码的李重量的一类 MacWilliams 恒等式的等价形式.首先介绍一种多项式(Krawtchouk 多项式)的定义.

定义 2 设 n,m 是正整数,x 是不定元,多项式

$$\begin{aligned}\mathrm{K}_k(x)&=\mathrm{K}_k(x,2n)\\&=\sum_{j=0}^{k}(-1)^j(2^m-1)^{k-j}\binom{x}{j}\binom{2n-x}{k-j},\\&k=0,1,2,\cdots\end{aligned} \quad (22)$$

称为 Krawtchouk 多项式,这里的$\binom{x}{j}$表示二项式系数.

下面我们将给出环$\mathbb{Z}_4+u\mathbb{Z}_4$上任意一个线性码的 m-层李重量分布与其对偶码的 m-层李重量分布之间的关系.

引理 2[15] 设 C 是环$\mathbb{Z}_4$上长度为 $2n$ 的线性码,$\{A_0^{(m)},A_1^{(m)},\cdots,A_{4n}^{(m)}\}$是 C 的 m-层李重量分布,$\{A_0^{('m)},A_1^{('m)},\cdots,A_{4n}^{('m)}\}$是 $C^\perp$的 m-层李重量分布,那么

$$A_k^{('m)}=\frac{1}{|C|^m}\sum_{i=0}^{4n}A_i^{(m)}K_k(i),k=0,1,\cdots,4n \quad (23)$$

定理 3 设 C 是环$\mathbb{Z}_4+u\mathbb{Z}_4$上长度为 n 的线性码,对任一正整数 m,$\mathrm{Lee}_C^{(m)}(x,y)$记为 C 的 m-层李重量计数器,$\Phi(C)$记为 C 的 Gray 像并且 $\mathrm{Lee}_{\Phi(C)}^{(m)}(x,y)$记为 $\Phi(C)$的 m-层李重量计数器,那么

$$\mathrm{Lee}_C^{(m)}(x,y)=\mathrm{Lee}_{\Phi(C)}^{(m)}(x,y) \quad (24)$$

证明 因为

$$\mathrm{Lee}_C^{(m)}(x,y)=\sum_{i=0}^{4n}B_i^{(m)}x^{4n-i}y^i \quad (25)$$

$$\mathrm{Lee}_{\Phi(C)}^{(m)}(x,y)=\sum_{i=0}^{4n}A_i^{(m)}x^{4n-i}y^i \quad (26)$$

这里的 $B_i^{(m)},A_i^{(m)}$ 是分别是 C 的 m-层李重量分布和 $\Phi(C)$的 m-层李重量分布.

根据 Φ 的保重性,得 $B_i^{(m)}=A_i^{(m)},i=0,1,\cdots,4n$.

证毕.

定理 4 设 C 是环$\mathbb{Z}_4+u\mathbb{Z}_4$上长度为 n 的线性码,$\{B_0^{(m)},B_1^{(m)},\cdots,B_{4n}^{(m)}\}$是 C 的 m-层李重量分布,$\{B_0^{('m)},B_1^{('m)},\cdots,B_{4n}^{('m)}\}$是 $C^\perp$的 m-层李重量分布,那么

$$B_k^{('m)}=\frac{1}{|C|^m}\sum_{i=0}^{4n}B_i^{(m)}\mathrm{K}_k(i),k=0,1,\cdots,4n \quad (27)$$

证明 因为

$$\mathrm{Lee}_C^{(m)}(x,y)=\sum_{i=0}^{4n}B_i^{(m)}x^{4n-i}y^i \quad (28)$$

$$\mathrm{Lee}_{\Phi(C)}^{(m)}(x,y)=\sum_{i=0}^{4n}A_i^{(m)}x^{4n-i}y^i \quad (29)$$

这里的 $B_i^{(m)},A_i^{(m)}$ 分别是码 C 的 m-层李重量分布和 $\Phi(C)$的 m-层李重量分布.

根据引理 2,得 $A_i^{(m)}=B_i^{(m)},i=0,1,\cdots,4n$.

设 $A_i^{('m)}$ 是$\Phi(C^\perp)$的 m-层李重量分布,$B_i^{('m)}$ 是 $C^\perp$的 m-层李重量分布,则有 $A_i^{('m)}=B_i^{('m)},i=0,1,\cdots,4n$.

根据引理 2,有

$$A_k^{('m)}=\frac{1}{|\Phi(C)|^m}\sum_{i=0}^{4n}A_i^{(m)}\mathrm{K}_k(i),k=0,1,\cdots,4n \quad (30)$$

因为$|C|=|\Phi(C)|$,所以有

$$B_k^{('m)}=\frac{1}{|C|^m}\sum_{i=0}^{4n}B_i^{(m)}\mathrm{K}_k(i),k=0,1,\cdots,4n$$

证毕.

根据定理 3 和 4,可以直接得到推论 1 的另一种表达式.

推论 2 设$\{T_0,T_1,\cdots,T_{4n}\}$是环 $\mathrm{GR}(4,m)+u\cdot\mathrm{GR}(4,m)$上 $C^{(m)}$的李重量分布,并且$\{T'_0,T'_1,\cdots,T'_{4n}\}$是环 $\mathrm{GR}(4,m)+u\mathrm{GR}(4,m)$上$(C^{(m)})^\perp$的李重量分布,那么

$$T'_k=\frac{1}{|C|^m}\sum_{i=0}^{4n}T_i\mathrm{K}_k(i),k=0,1,\cdots,4n \quad (31)$$

最后,我们通过一个具体例子,说明本文主要结论的应用.

例 1 设 $C=\{(0,0),(2u,2u)\}$是环$\mathbb{Z}_4+u\mathbb{Z}_4$上长度为 2 的线性码,则 $C^\perp$的生成矩阵为 $\boldsymbol{G}=\begin{pmatrix}u&u\\0&2u\end{pmatrix}$,$\Phi(C)$的生成矩阵为 $\boldsymbol{G}'=\begin{pmatrix}0&0&0&0\\2&2&2&2\end{pmatrix}$.取 $m=2$ 时,设 Galois 环 GR(4,2)是剩余类环$\mathbb{Z}_4[x]/(h(x))$,这里的 $h(x)$是$\mathbb{Z}_4[x]$中次数为 2 的首一的基本不可约多项式,ξ是 $h(x)$的一个根,那么 $T=\{0,1,\xi,\xi^2\}$为 Galois 环 GR(4,2)的 Teichmüller 集,$\{1,\xi\}$是$\mathbb{Z}_4$一组自由基.因此 $C^{(2)}=\{(0,0),(2u,2u),\xi(2u,2u),(1+\xi)(2u,2u)\}$是 Galois 环 GR(4,2)上长度为 2 的线性码.下面利用两种方法分别计算环 $\mathrm{GR}(4,2)+u\mathrm{GR}(4,2)$上长度为 2 的线性码 $C^{(2)}$的李重量分布.

方法Ⅰ

根据推论 1,得到

$$\begin{aligned}\mathrm{Lee}_{C^\perp}^{(2)}(x,y)&=x^8+84x^6y^2+336x^5y^3+1470x^4y^4+3360x^3y^5\\&+5124x^2y^6+15288xy^7+y^8.\end{aligned}$$

即:$T'_0=1,T'_1=0,T'_2=84,T'_3=336,T'_4=1470,T'_5=3360,T'_6=5124,T'_7=15288,T'_8=1$.

方法Ⅱ

因为 $T_0=1,T_1=0,T_2=0,T_3=0,T_4=0,T_5=0,T_6=0,T_7=0,T_8=1$,所以根据推论 2,得

$T_0' = 1, T_1' = 0, T_2' = 84, T_3' = 336, T_4' = 1470,$

$T_5' = 3360, T_6' = 5124, T_7' = 15288, T_8' = 1.$

以上两种方法的结果完全一致.

5　结束语

本文定义了环$\mathbb{Z}_4 + u\mathbb{Z}_4$上长度为 n 的线性码的 m-层李重量计数器,给出了环$\mathbb{Z}_4 + u\mathbb{Z}_4$上长度为 n 的线性码的关于李重量的一类 MacWilliams 恒等式.证明了该等式是生成矩阵在环$\mathbb{Z}_4 + u\mathbb{Z}_4$上的环 GR(4, m) + uGR(4, m)上线性码关于李重量的 MacWilliams 恒等式.进一步,利用 Krawtchouk 多项式,获得了环$\mathbb{Z}_4 + u\mathbb{Z}_4$上长度为 n 的线性码的等价形式的 MacWilliams 恒等式.

参考文献

[1] Hammons A R, Kumar Jr P V, Calderbank A R, Solance N J A, Solé P. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes[J]. IEEE Transactions on Information Theory, 1994, 40(2): 301 – 319.

[2] Bachoc C. Application of coding theory to the construvtion of modular lattices[J]. Journal of Combinatorial Theory, Series A, 1997, 78(1): 92 – 119.

[3] 施敏加,杨善林,朱士信.环$\mathbb{F}_2 + u\mathbb{F}_2$上长度为 2^s 的循环码的距离[J].电子学报,2011,39(1):29 – 34.
Shi Min-jia , Yang Shan-lin , Zhu Shi-xin. On minimum distances of cyclic codes of length 2^sover $\mathbb{F}_2 + u\mathbb{F}_2$[J]. Acta Electronica Sinica, 2011, 39(1): 29 – 34. (in Chinese)

[4] Shi M J, Yang S L, Zhu S X. Good p-ary quasic-cyclic codes from cyclic codes over $F_p + vF_p$[J]. Journal of Systems Science and Complexity, 2012, 25(2): 375 – 384.

[5] Dinh H Q, Nguyen H D T. On some classes of constacyclic codes over polynomial residue rings[J]. Advances in Mathematics of Communications, 2012, 6(2): 175 – 191.

[6] 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.

[7] Kai X S, Zhu S X, Wang L Q. A family of constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$[J]. Journal of Systems Science and Complexity, 2012, 25(5): 1032 – 1040.

[8] Yildiz B, Karadeniz S. Linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$: MacWilliams identities, projections, and formally self-dual codes[J]. Finite Field and Their Applications, 2014, 27(1): 24 – 40.

[9] MacWilliams F J, Sloane N J A. The Theory of Error-Correcting Codes[M]. Amsterdam, the Netherlands: North-Holland, 1977. 125 – 154.

[10] Wei V K. Generalized Hamming weights for linear codes[J]. IEEE Transactions on Information Theory, 1991, 37(5): 1412 – 1418.

[11] Shiromoto K. The weight Enumerator of linear codes over GF(q^m) having generator matrix over GF(q)[J]. Design Codes and Cryptography, 1999, 16(1): 87 – 92.

[12] Shiromoto K. A basic exact sequence for the Lee and Euclidean weights of linear codes over $\mathbb{Z}_l$[J]. Linear Algebra and Its Applications, 1999, 295(1): 191 – 200.

[13] Cui J, Pei J Y. Generalized MacWilliams identities for $\mathbb{Z}_4$-linear codes[J]. IEEE Transactions on Information Theory, 2004, 50(12): 3302 – 3305.

[14] Dougherty S, Gupta M, Shiromoto K. Generalized weights for codes over finite rings[J]. Australasian Journal of Combinatorics, 2005, 31(1): 231 – 241.

[15] 唐永生.有限环上循环码的中国积和线性码的 MacWilliams 恒等式的研究[D].合肥:合肥工业大学硕士学位论文,2009.

[16] Zhu S X, Tang Y S. A MacWilliams type identity on Lee weight for linear codes over $\mathbb{F}_2 + u\mathbb{F}_2$[J]. Journal of Systems Science and Complexity, 2012, 25(1): 186 – 194.

[17] Shiromoto K. Singleton bounds for codes over finite rings[J]. Journal of Algebraic Combinatorics, 2000, 12(1): 95 – 99.

作者简介

李　平　男,1971 年 11 月出生于安徽省巢湖市,现为合肥工业大学副教授,博士,硕士研究生导师,主要从事代数编码及非线性移位寄存器序列的研究.
E-mail: lpmath@126.com

李珊珊　女,1988 年 12 月出生于河南省新乡市,硕士研究生,主要从事代数编码的研究.
E-mail: lssxkmath@126.com

唐永生(通信作者)　男,1981 年 9 月出生于安徽省庐江县,现为合肥师范学院讲师,博士,主要从事代数编码、量子信息以及线性和非线性移位寄存器序列的研究.
E-mail: ysh_tang@163.com