arXiv:2601.02608v1 [cs.IT] 5 Jan 2026

有限域上的权与麦克威廉姆斯恒等式的失效

JAY A. WOOD

谨以此文纪念：*William Browder，1934–2025*年；*Alan T. Huckleberry，1941–2025*年；*Catherine M. Murphy，1940–2025*年

Abstract. 在20世纪60年代，MacWilliams证明，有限域上线性码的汉明重量枚举器完全决定其对偶码的汉明重量枚举器，反之亦然。特别地，如果两个线性码具有相同的汉明重量枚举器，那么它们的对偶码也具有相同的汉明重量枚举器。

与此相反，有限域上的权有一大类，其重量枚举器表现出相反的性质：存在两个重量枚举器相同、但对偶码的重量枚举器不同的线性码。

1. Introduction

20世纪60年代初，Florence Jessie MacWilliams（1917–1990）证明，线性码的汉明重量枚举器 $C \subseteq \mathbb{F}_q^n$ 决定了其对偶码的汉明重量枚举器 $C^\perp$，反之亦然。这些重量枚举器之间的关系由麦克威廉姆斯恒等式 [12, 13]所概括：

$$\mathrm{hwe}_{C^\perp}(X,Y) = \frac{1}{|C|}\,\mathrm{hwe}_C(X+(q-1)Y, X-Y). \tag{1.1}$$

麦克威廉姆斯恒等式的一个直接推论是：若两个线性码 C，$D \subseteq \mathbb{F}_q^n$ 满足 $\mathsf{hwe}_C = \mathsf{hwe}_D$，则 $\mathsf{hwe}_{C^\perp} = \mathsf{hwe}_{D^\perp}$。我们称汉明重量*尊重*对偶性。

麦克威廉姆斯恒等式已通过多种方式得到推广：推广码的字母表，以及推广枚举器。对于汉明重量枚举器，麦克威廉姆斯

2020 数学主题分类。主分类：94B05。关键词和短语。麦克威廉姆斯恒等式、对偶码、反例。

恒等式适用于有限阿贝尔群上的加法码 [4] 以及有限弗罗贝尼乌斯环上的线性码 [16]。

汉明重量枚举器可以有两种解读方式。一种方式是统计码字中非零项的数量；另一种方式是相加码字中各项的权值。这些解读方式引出了汉明重量枚举器的两种推广：使用更一般的划分，或使用更一般的权。

设 A 为一个有限阿贝尔群，并设 $\mathcal{P}$ 是 A的一个划分。对于任意加性码 $C \subseteq A^n$，都可以定义一个划分枚举器，用于记录码字中属于该划分各个分块的项数。汉明重量枚举器是将 A划分为 $\{0\}$和 $A-\{0\}$所得划分的划分枚举器，而完全枚举器则使用将 $A = \cup_{a\in A}\{a\}$ 划分为单元组的完全划分。某些称为自反划分的划分能够导出性质良好的MacWilliams恒等式。有关此内容及更多信息，请参见 [8]。

另一种推广采用更一般的权，这正是本文的主题。设 A 是一个赋有整数值权 w的有限阿贝尔群。我们假设 $w\colon\ A \to \mathbb{Z}$，其中 $w(0) = 0$，且对于 $a \neq 0$，$w(a) > 0$ 。记 w 的最大值为 $w_{\max}$。将w 加性地扩展到 A^n，使得 $w(a_1,\ a_2,\ \ldots\ldots,\ a_n) = \sum_{i=1}^{n} w(a_i)$。对于任意加性码 $C \subseteq A^n$，定义其 w-权重量枚举器为

$$\mathrm{wwe}_C(X, Y) = \sum_{c\in C} X^{nw_{\max}-w(c)}Y^{w(c)}.$$

自然会产生这样的问题：*MacWilliams*恒等式是否适用于 w-权重量枚举器？

如上所述，MacWilliams恒等式适用于汉明重量。对于 $\mathbb{F}_q$上的齐次重量，它们同样成立（因为在该情形下，齐次重量是汉明重量的倍数）；对于 $\mathbb{Z}/4\mathbb{Z}$ [10]上的李重量，以及对于 $M_{2\times 2}(\mathbb{F}_2)$ [19]上的齐次重量，也同样成立。由于权未能保持对偶性，MacWilliams恒等式不成立：对于矩阵 [5]上的Rosenbloom-Tsfasman重量；对于$\mathbb{Z}/m\mathbb{Z}$上的李重量，$m \geq 5$ [1]；对于 $\mathbb{Z}/m\mathbb{Z}$、 $m \geq 6$上的齐次重量，其中 m不是素数 [18]；以及对于许多在有限链环或矩阵环 $M_{k\times k}(\mathbb{F}_q)$ [19]上具有最大对称性的权。后面的结果表明，一个权能够保持对偶性或许是很罕见的情况。

本文进一步凸显了尊重对偶性的权之罕见性。主要结果定理 2.8 可以解释为：对于满足某些限制的有限域上的权，一般的权并不尊重对偶性。

以下概述论证思路。考虑整数值权w 在 $\mathbb{F}_q$ 上，并要求 $w(a) = w(-a)$ 对 $a \in \mathbb{F}_q$ 成立，且w 不是汉明重量的倍数。另假设 w 是非退化的（定义见定义 2.3）。目标是通过构造线性码 w，证明 C、$D \subseteq \mathbb{F}_q^n$（对某个 n）不尊重对偶性，使得 $\mathsf{wwe}_C = \mathrm{wwe}_D$，但 $\mathsf{wwe}_{C^\perp} \neq \mathrm{wwe}_{D^\perp}$。

我们考虑定义在 $\mathbb{F}_q$上的维数为 2 的线性码，并且不失一般性地考虑大小为 $2\times n$ 的生成矩阵，其列具有一种特定的标准形（3.4），这种标准形体现了权 w的对称性。要表示一个线性码 C，只需指定一个重数函数 η_C，它记录了某一特定列在 C的生成矩阵中出现的次数。有序列出 ω_C中码字的权 C，便可得到重数函数的一个线性函数：$\omega_C = W\eta_C$，其中矩阵 W仅取决于权 w。

两个线性码 C，$D \subseteq \mathbb{F}_q^n$ 满足 $\mathsf{wwe}_C = \mathsf{wwe}_D$，当且仅当它们的码字权有序列表 ω_C 和 ω_D互为排列。此时，我们反向推导——从互为排列的有序列表 ω_C 和 ω_D 出发，反解线性方程 $\omega = W\eta$，求出 η_C 和 η_D。矩阵 W 具有丰富的结构，便于进行细致分析。让列表 ω_C 和 ω_D 非常简单，仅包含两种不同的权，就可以证明所得的重数函数 η_C 和 η_D的各项均为非负，因此可用于定义线性码。此外，还可以分析小权对偶码字的数量，并证明这些数量至少在一般情况下彼此不同。

致谢。2025年，三位对我影响深远的数学家相继离世。本科期间，Huckleberry 教授教我复分析；他的课程激励我在研究生院攻读复微分几何。Browder 教授建议我研究 $\mathbb{Z}/4\mathbb{Z}$值二元二次型，这让我进入了编码理论中美妙的 $\mathbb{Z}_4$世界。Cathy Murphy 曾与我共事，并担任系主任十年。她慷慨而周到的指导为我带来了许多机会。

2. Preliminaries

本节回顾代数编码理论中的一些定义，并确立本文将通篇使用的符号。由于我们将证明的大多数定理都针对定义在有限域 $\mathbb{F}_q$ 或整数剩余环 $\mathbb{Z}/m\mathbb{Z}$ 上的线性码，因此我们将

将定义范围限定为定义在含幺有限交换环上的线性码。有关更多细节，或非交换环所需的修改，请参见 [17]。

设 R 是一个带幺元的有限交换环。用 $\mathcal{U}(R)$ 表示 R 的单位群，即可逆元素。有限域 $\mathbb{F}_q$ 的单位群等于其非零元素的乘法群 $\mathbb{F}_q^\times$；$\mathbb{F}_q^\times$ 是一个循环群，由某个称为 $\mathbb{F}_q$ 的本原元 α生成。在 R^n 上定义点积 如下：

$$x \cdot y = \sum_{i=1}^{n} x_i y_i \in R,$$

对于 $x = (x_1, x_2, \ldots, x_n)$ $y = (y_1, y_2, \ldots, y_n) \in R^n$。

在 R 上长度为 n 的线性码 是一个 R-子模 $C \subseteq R^n$。给定一个线性码 $C \subseteq R^n$，定义其对偶码 $C^\perp \subseteq R^n$ 如下：

$$C^\perp = \{y \in R^n \colon x \cdot y = 0 \text{ for all } x \in C\}.$$

一般而言，对于线性码 $C \subseteq R^n$，有 $C \subseteq (C^\perp)^\perp$。当 R 是有限域 $\mathbb{F}_q$ 且 $C \subseteq \mathbb{F}_q^n$ 是线性码时，根据线性代数可知，$\dim_{\mathbb{F}_q} C^\perp = n - \dim_{\mathbb{F}_q} C$ 且 $C = (C^\perp)^\perp$。这些性质可推广到有限弗罗贝尼乌斯环 [17]: $|C| \cdot |C^\perp| = |R^n|$，且 $C = (C^\perp)^\perp$。有限域都是 Frobenius 环。

在 R 上的权 是一个复值函数 $w\colon R \to \mathbb{C}$，满足 $w(0) = 0$。本文中，权假定取整数值，且满足$w(0) = 0$ 以及 $w(r) > 0$，其中 $r \neq 0$。记 w 的最大值为$w_{\max}$，记 w 的最小正值为 $\mathring{w}$。权 w 确定了 $\mathcal{U}(R)$ 中的一个对称群 $\mathrm{Sym}(w)$：

$$\mathrm{Sym}(w) = \{u \in \mathcal{U}(R) \colon w(ur) = w(r) \text{ for all } r \in R\}. \tag{2.1}$$

对称群 $\mathrm{Sym}(w)$ 通过环乘法作用于 R，而 $\mathrm{Sym}(w)$ 通过对 $\lambda \in R^\sharp$ 的取值进行乘法，作用于 $\mathrm{Hom}_R(R, R)$；后者是 R-模同态 $\lambda\colon R \to R$ 所成的群。元素$\lambda \in R^\sharp$ 称为泛函；其输入写在左侧。记 $x \in R$ 和 $\lambda \in R^\sharp$ 的 $\mathrm{Sym}(w)$-轨道分别为 $[x]$ 和 $[\lambda]$。定义矩阵 $\mathcal{W}$，其行由 R 的非零 $\mathrm{Sym}(w)$-轨道索引，列由 $R^\sharp$ 的非零 $\mathrm{Sym}(w)$-轨道索引：

$$\mathcal{W}_{[x],[\lambda]} = w(x\lambda). \tag{2.2}$$

根据 $\mathrm{Sym}(w)$ 的定义，这些值是定义良好的。

定义 2.3. A 的权重 w 在 R 上是 非退化的，如果（$\mathcal{W}$ 2.2）的矩阵 在 $\mathbb{Q}$上可逆。

例 2.4. 汉明重量 定义在任意有限环 R上:

$$\mathrm{H}(r) = \begin{cases} 0, & r = 0, \\ 1, & r \neq 0. \end{cases}$$

汉明重量的对称群为 Sym(H) $= \mathcal{U}(R)$。当且仅当 R 是 Frobenius 时，汉明重量是非退化的： [16,定理 6.3、6.4]和 [17, 定理 7.2]。

例 2.5。 对于整数剩余环 $R = \mathbb{Z}/m\mathbb{Z}$，用满足 $-m/2 < r \leq m/2$ 的整数 r 唯一表示剩余类。在 $\mathbb{Z}/m\mathbb{Z}$ 上定义李重量 L 和欧几里得权重 E:

$$\mathrm{L}(r) = |r|, \quad \mathrm{E}(r) = |r|^2,$$

其中 $|r|$ 是 $\mathbb{Z}$ 上通常的（阿基米德）绝对值。汉明重量、李重量和欧几里得权重分别是，1、2 次幂权重的特例；这些幂权重定义在整数 $\ell \geq 0$ 上： $w^{(\ell)}$

$$w^{(\ell)}(r) = |r|^{\ell}, \quad r \in \mathbb{Z}/m\mathbb{Z}.$$

除汉明重量外，所有幂权重 $w^{(\ell)}$、 $\ell = 1$、2、..... 都有 Sym($w^{(\ell)}$) $= \{\pm 1\} \subseteq \mathcal{U}(\mathbb{Z}/m\mathbb{Z})$。已知李重量和欧几里得权重是非退化的 [6]。

尽管本文未对其进行研究，齐次重量是在任意含幺有限环上定义的另一种重要权；当且仅当该环为 Frobenius 环时，它才是非退化的 [9]。

w 上的权 R 可通过以下方式加性地扩展为 R^n 上的权:

$$w(r_1, r_2, \ldots, r_n) = \sum_{i=1}^{n} w(r_i).$$

还可以用其他方式在 R^n 上定义权，但这不是本文的研究主题。

线性码 $C \subseteq R^n$ 的 w-权重量枚举器是 $\mathbb{C}[X, Y]$ 中的一个关于 $nw_{\max}$ 次齐次多项式，定义为

$$\mathrm{wwe}_C(X, Y) = \sum_{c \in C} X^{nw_{\max} - w(c)} Y^{w(c)}.$$

为节省公式展示空间，我们通常令 $X = 1$ 和 $Y = y$。这样会失去关于码长 n 的直接信息。

有限域上的汉明重量 $\mathbb{F}_q$方面，MacWilliams [12, 13]证明了线性码的汉明重量枚举器 $C \subseteq \mathbb{F}_q^n$与其对偶码的汉明重量枚举器相关；参见（1.1）。后来，这一结果被推广到有限弗罗贝尼乌斯环上的汉明重量 [16]；这类环包括整数剩余环 $\mathbb{Z}/m\mathbb{Z}$。

定义 2.6。当一个权 w 在 R 对偶性下保持不变时，是指它具有以下性质：对于线性码 C，$D \subseteq R^n$，如果 $\mathrm{wwe}_C = \mathrm{wwe}_D$，那么 $\mathrm{wwe}_{C^\perp} = \mathrm{wwe}_{D^\perp}$。

麦克威廉姆斯恒等式（1.1）表明，$\mathbb{F}_q$ 上的汉明重量尊重对偶性。

备注2.7。另一种理解尊重对偶性的方式是考察一个码的重量分布。对于码 $C \subseteq R^n$ 和整数 j，定义

$$A_j(C) = |\{c \in C : w(c) = j\}|.$$

已知 A_j 即可确定 wwe_C：

$$\mathrm{wwe}_C(X, Y) = \sum_j A_j(C) X^{nw_{\max} - j} Y^j.$$

若对于相同长度的线性码 C、D，对所有 j 都有 $A_j(C) = A_j(D)$，则对所有 j都有 $A_j(C^\perp) = A_j(D^\perp)$，那么称权 w 尊重对偶性。

本文的主要结果是，大多数定义在 $\mathbb{F}_q$ 上的权都不尊重对偶性。为了准确陈述这一结果，我们还需要给出一些定义。

设 w 是有限域 $\mathbb{F}_q$上的一个权。假设 w 取整数值，且 $w(0) = 0$，对于非零的 $r \in \mathbb{F}_q$，有 $w(r) > 0$。记$\mathring{w} = \min\{w(r) : r \in \mathbb{F}_q, r \neq 0\}$。假设对称群 $\mathrm{Sym}(w)$ 满足 $-1 \in \mathrm{Sym}(w)$ 和 $\mathrm{Sym}(w) \neq \mathbb{F}_q^\times$。（最后一个条件意味着 w 不是汉明重量的倍数。）固定 $\mathbb{F}_q$的一个本原元 α；也就是说，α 生成循环群 $\mathbb{F}_q^\times$。令 t为使 α^t 生成 $\mathrm{Sym}(w)$ 的最小正整数。于是$t|\mathrm{Sym}(w)| = |\mathbb{F}_q^\times| = q - 1$。由于 $\mathrm{Sym}(w) \neq \mathbb{F}_q^\times$，我们有 $t \geq 2$。又因为$\alpha^t \in \mathrm{Sym}(w)$，可知对于所有 j，$w(\alpha^{t+j}) = w(\alpha^t \alpha^j) = w(\alpha^j)$。

定义 $\breve{w}$和 $c_m(w, w)$，对于 $m = 0, 1, \ldots, t-1$，定义如下

$$\breve{w} = \sum_{j=0}^{t-1} w(\alpha^j), \quad c_m(w, w) = \sum_{j=0}^{t-1} w(\alpha^j) w(\alpha^{m+j}).$$

下面给出主要结果的精确表述。

定理 2.8。设 w 是 $\mathbb{F}_q$上的整数值权，满足 $w(0) = 0$且 $w(r) > 0$，其中 $r \neq 0$。假设 w 满足：

- w 是非退化的，
- $-1 \in \mathrm{Sym}(w)$，
- $\mathrm{Sym}(w) \neq \mathbb{F}_q^\times$，
- 最小值 $\mathring{w}$ 恰好在一个 $\mathrm{Sym}(w)$-轨道上取得，

- 以下数值中至少有两个不同：

$$qc_1(w,w), qc_2(w,w), \ldots, qc_{\lfloor t/2 \rfloor}(w,w), ((q-1)/t)\breve{w}^2.$$

那么，对于某个 n，存在两个线性码 $C, D \subseteq \mathbb{F}_q^n$，满足 $\mathrm{wwe}_C = \mathrm{wwe}_D$，但 $\mathrm{wwe}_{C^\perp} \neq \mathrm{wwe}_{D^\perp}$。特别地， w 不保持对偶性。

3. Presenting linear codes via multiplicity functions

我们继续假设 R 是一个含幺有限交换环，且 w 是 R 上的权，其中 $w(0) = 0$，并且对于所有非零 $r \in R$， $w(r) > 0$。将 w 加性地扩展到 R^n，使得 $w(r_1, r_2, \ldots, r_n) = w(r_1) + w(r_2) + \cdots + w(r_n)$。 w 的对称群 $\mathrm{Sym}(w)$ 在 (2.1) 中定义。

一个 R-线性码 $C \subseteq R^n$ 可以表示为某个 $k \times n$ 矩阵 G 的行空间，该矩阵称为生成矩阵。 C 中的每个码字都具有 $c = vG$ 的形式，其中 $v \in R^k$。记 $v = (v_1, v_2, \ldots, v_k) \in R^k$，并且 $G = (g_{i,j})$，其中 $i = 1, 2, \ldots, k$ 且 $j = 1, 2, \ldots, n$，那么，对于 $c = vG$，

$$w(c) = w(vG) = \sum_{j=1}^{n} w(\sum_{i=1}^{k} v_i g_{i,j}). \tag{3.1}$$

$w(c)$ 的这个公式在以下情况下保持不变：

- 对 G 的列进行置换，或
- 对于任意 $j = 1, 2, \ldots, n$，将 G 的第 j 列乘以 $h_j \in \mathrm{Sym}(w)$。

因此，将 G <style id='4} 的列限制为来自 $\mathrm{Sym}(w)$ 作用于所有列组成的空间所得轨道的代表元集合，并不失一般性。此外， $w(c)$ 的值只取决于各个代表元作为 G 的列出现多少次，即这些代表元的重数。事实上，设代表元集合为 $\mathcal{O} = \{\lambda_1, \lambda_2, \ldots, \lambda_N\}$，且 λ_ι 作为 G 的列出现 η_ι 次。则（3.1）变为

$$w(c) = \sum_{\iota=1}^{N} w(v\lambda_\iota)\eta_\iota. \tag{3.2}$$

对称群还以第二种方式出现，这次它作用于输入 $c = vG$。如果 $u \in \mathrm{Sym}(w)$，那么 $w(uvG) = w(vG)$。因此，线性码 c 的重量分布完全由 w 在 R^k 中 $\mathrm{Sym}(w)$-轨道 $[v]$ 的代表元上的取值，以及 $\mathrm{Sym}(w)$-轨道的大小决定。给定一个代表元 v，其轨道对 $A_{w(vG)}(C)$ 的贡献为 $|[v]|$。

现在，我们来详细推导如下情形： $R = \mathbb{F}_q$ 是一个有限域， w 是定义在 $\mathbb{F}_q$上的任意整数值权，并满足若干

限制。与上文一样，假设 $w(0) = 0$ 且对所有非零$r \in \mathbb{F}_q$， $w(r) > 0$ 。此外，假设 $-1 \in \mathsf{Sym}(w)$ and $\mathsf{Sym}(w) \neq \mathbb{F}_q^\times$，因此 w 并不等于汉明重量的某个常数倍。

如第 2 节所述，令 α 为 $\mathbb{F}_q$的本原元，并令t 为满足 α^t 生成 $\mathsf{Sym}(w)$ 的最小正整数。那么$t|\mathrm{Sym}(w)| = |\mathbb{F}_q^\times| = q-1$。由于 $\mathsf{Sym}(w) \neq \mathbb{F}_q^\times$，因此 $t \geq 2$。

我们将构造定义在 $\mathbb{F}_q$ 上的维数为 2 的线性码，因此生成矩阵的大小为 $2 \times n$。特别地，生成矩阵的列属于 $\mathbb{F}_q^2$。对称群 $\mathsf{Sym}(w)$ 通过数乘作用于 $\mathbb{F}_q^2$ 。注意，非零向量 $v \in \mathbb{F}_q^2$ 的 $\mathsf{Sym}(w)$-轨道包含在由 v张成的一维向量子空间中。为列出非零 $\mathsf{Sym}(w)$-轨道代表元的集合 $\mathcal{O}$ ，我们先写出生成 $\mathbb{F}_q^2$的一维子空间的某些元素。在 $\mathbb{F}_q^2$中有 $q+1$ 个一维线性子空间。选取的生成元如下：

$$\ell_\infty = \langle 0, 1\rangle, \ell_0 = \langle 1, 0\rangle, \text{ and } \ell_j = \langle 1, \alpha^j\rangle \text{ for } j = 1, 2, \ldots, q-1. \tag{3.3}$$

注意 $\ell_{q-1} = \langle 1, \ 1\rangle$。每个生成元 ℓ_μ 都为 $\mathcal{O}$贡献一组代表元，如图3.1所示。 $\mathcal{O}$中的元素也代表输入上的 $\mathsf{Sym}(w)$-轨道。

线性码的生成矩阵 G 由指定 $\mathcal{O}$ 中的每个元素作为 G的一列出现多少次来确定。此信息将用一个重数函数 η： $\mathcal{O} \to \mathbb{N}$编码。也就是说， η（$\alpha^i \ell_\mu$）作为 G的一列出现 $\alpha^i \ell_\mu$ 次。

构造一个大小为 t（$q+1$） $\times t$（$q+1$）的矩阵 W，其行和列以 $\mathcal{O}$中的元素为索引：

$$W_{\alpha^i \ell_\mu, \alpha^j \ell_\nu} = w(\alpha^i \ell_\mu \cdot \alpha^j \ell_\nu), \quad \alpha^i \ell_\mu, \alpha^j \ell_\nu \in \mathcal{O}, \tag{3.5}$$

其中， $\cdot$ 是 $\mathbb{F}_q^2$上的标准点积。当 η 是确定生成矩阵 G的重数函数时，矩阵乘积

FIGURE 3.1. 在 $\mathbb{F}_q^2$中的 $\mathsf{Sym}(w)$-轨道的代表元

$$\begin{aligned}\mathcal{O} = \{&\ell_\infty, \alpha\ell_\infty, \alpha^2\ell_\infty, \ldots, \alpha^{t-1}\ell_\infty;\\ &\ell_0, \alpha\ell_0, \alpha^2\ell_0, \ldots, \alpha^{t-1}\ell_0;\\ &\ell_1, \alpha\ell_1, \alpha^2\ell_1, \ldots, \alpha^{t-1}\ell_1;\\ &\vdots\\ &\ell_{q-1}, \alpha\ell_{q-1}, \alpha^2\ell_{q-1}, \ldots, \alpha^{t-1}\ell_{q-1}\}.\end{aligned} \tag{3.4}$$

$\omega = W\eta$ 是一个列向量，其元素由 $\mathcal{O}$中的元素索引。由 $\alpha^i\ell_\mu$ 索引的元素为

$$\omega_{\alpha^i\ell_\mu} = (W\eta)_{\alpha^i\ell_\mu} = \sum_{\alpha^j\ell_\nu\in\mathcal{O}} w(\alpha^i\ell_\mu\cdot\alpha^j\ell_\nu)\eta(\alpha^j\ell_\nu).$$

根据（3.2），该表达式恰好是 w（$\alpha^i\ell_\mu G$）。总之，列向量 $\omega = W\eta$ 由 C的所有码字的权组成，并按 Sym-轨道组织。我们将 ω 称为轨道权重列表。注意到，对于所有 w（uvG）$= w$（vG），$u\in\mathrm{Sym}(w)$，ω的取值连同 Sym(w)-轨道的大小，决定了线性码 C的重量分布：

$$A_s(C) = \sum_{\substack{\alpha^i\ell_\mu\in\mathcal{O}:\\ \omega_{\alpha^i\ell_\mu}=s}} |[\alpha^i\ell_\mu]|, \tag{3.6}$$

其中 $[\alpha^i\ell_\mu]$是 $\alpha^i\ell_\mu$的 Sym(w)-轨道。

4. Dual codewords of small weight

继续假设 R 是一个含幺元的有限交换环。给定一个 R-线性码 $C\subseteq R^n$，记 λ_i，$i = 1, 2, \ldots, n$为i次坐标投影 λ_i：$C\to R$，其中 $\lambda_i(c_1, c_2, \ldots, c_n) = c_i$ 对于$c = (c_1, c_2, \ldots, c_n)\in C$。称 λ_i 为一个坐标泛函；λ_i 是 R-模的同态。

定义线性码的有效长度 C 为

$$\mathrm{efflen}(C) = |\{i\colon \lambda_i(c)\neq 0 \text{ for some } c\in C\}|.$$

若 C 由生成矩阵给出，则有效长度就是该生成矩阵中非零列的数量。有效长度会忽略所有码字在相应坐标位置上都为零的坐标。

实值权重 w 在 R 上称为 均衡 [11]，如果存在一个正的常数 ζ 使得 $\sum_{r\in I} w(r) = \zeta|I|$ 对每个非零理想$I\subseteq R$都成立。术语 预齐次 用于 [3]。

例 4.1。由于域中只有一个非零理想，因此有限域上取正值的任意权都是均衡的。$\mathbb{Z}/2^a\mathbb{Z}$ 上的李重量是均衡的，且 $\zeta = 2^{a-1}$。有限弗罗贝尼乌斯环上的齐次重量是均衡的，[9, 推论 1.6]。

命题 4.2. 设 w 是有限交换环 R上常数为 ζ 的均衡权。若 $C\subseteq R^n$ 是一个线性码，则

$$\sum_{c\in C} w(c) = \zeta|C|\,\mathrm{efflen}(C).$$

证明。考虑坐标泛函 $\lambda_i\colon C \to R$, $i = 1, 2, \ldots\ldots, n$。若 $\lambda_i = 0$, 则 i 不会计入有效长度。若 $\lambda_i \neq 0$, 则 i 会计入有效长度, 且像 $\lambda_i(C)$是 R的非零理想。

每个元素 $b \in \lambda_i(C)$ 都被 $|\ker \lambda_i| = |C|/|\lambda_i(C)|$ 次命中。于是

$$\begin{aligned}\sum_{c\in C} w(c) &= \sum_{c\in C}\sum_{i\colon \lambda_i\neq 0} w(\lambda_i(c)) = \sum_{i\colon \lambda_i\neq 0} |\ker \lambda_i| \sum_{b\in\lambda_i(C)} w(b)\\ &= \sum_{i\colon \lambda_i\neq 0} \frac{|C|}{|\lambda_i(C)|} \sum_{b\in\lambda_i(C)} w(b) = \operatorname{efflen}(C)|C|\zeta. \qquad \square\end{aligned}$$

注记 4.3。这一结果本质上与 [2,第 319], 页中的一个命题相同; 那些作者将其归功于 Slepian [14,命题 6]。

推论 4.4。设 w 为一个均衡权。若 $C_1, C_2 \subseteq R^n$ 是两个具有相同 w-重量分布的线性码, 则 C_1, C_2 具有相同的有效长度, $\operatorname{efflen}(C_1)$ =$\operatorname{efflen}(C_2)$。

证明。假设 $A_s(C_1) = A_s(C_2)$ 对所有 s 都成立。由于$\sum_s A_s(C) = |C|$, 因此有 $|C_1| = |C_2|$。因为 $\sum_s sA_s(C) = \sum_{c\in C} w(c)$, 我们还有 $\sum_{c\in C_1} w(c) = \sum_{c\in C_2} w(c)$。现在应用命题 4.2。 $\square$

现在考虑有限域上的线性码 $\mathbb{F}_q$。由例 4.1可知, $\mathbb{F}_q$ 上的每个权都是均衡的。下一个结果可由推论 4.4直接得出。

推论 4.5。设 w 是 $\mathbb{F}_q$ 上的任意权。若 C_1、$C_2 \subseteq \mathbb{F}_q^n$ 是具有相同 w-重量分布的线性码, 则 C_1、C_2 具有相同的有效长度, $\operatorname{efflen}(C_1)$ =$\operatorname{efflen}(C_2)$。

若向量 $x \in \mathbb{F}_q^n$ 恰有一个非零项, 则称其为单元组 。若向量 x 恰有两个非零项, 则称其为双元组 。定义

$$\begin{aligned}A_j^{\mathrm{sing}}(C) &= |\{x \in C\colon x \text{ is a singleton and } w(x) = j\}|,\\ A_j^{\mathrm{dble}}(C) &= |\{x \in C\colon x \text{ is a doubleton and } w(x) = j\}|.\end{aligned}$$

在 $\mathbb{F}_q$ 上, 对偶码字中的单重量码字仅由原生成矩阵中的零列产生。由此得到下一个结果。

命题 4.6。设 w 是 $\mathbb{F}_q$ 上的任意权。若 C_1、$C_2 \subseteq \mathbb{F}_q^n$ 是具有相同 w-重量分布的线性码, 则对于所有 s, $A_s^{\mathrm{sing}}(C_1^\perp) = A_s^{\mathrm{sing}}(C_2^\perp)$。

证明。任何非零元素 $r \in \mathbb{F}_q$ 都是可逆的。如果 r 消去坐标泛函 λ_i, 即 $\lambda_i r = 0$, 那么 $\lambda_i = 0$。因此, $A_s^{\mathrm{sing}}(C_1^\perp) =$

$A_s^{\mathrm{sing}}(\mathbb{F}_q)(n-\mathrm{efflen}(C_1))$，其中 $A_s^{\mathrm{sing}}(\mathbb{F}_q)$ 是$\mathbb{F}_q$ 中权为 s的元素个数。由推论 4.5 可得结论。□

对于双元素集，我们假设线性码通过一个重数函数给出 η，如第 3 节所示。我们还假设 w 具有以下性质：$-1 \in \mathrm{Sym}(w)$，且最小正值 $\mathring{w}$ 在 w 上仅由唯一的 $\mathrm{Sym}(w)$-轨道取得。

引理 4.7。设 w 是有限环 R 上的一个权，满足 $w(0)=0$ 且$w(r)>0$ 对非零 $r \in R$成立。设 $\mathring{w}$ 是w 在 R上取得的最小正值。若 $v \in R^n$ 满足 $\mathring{w} \le w(v) < 2\mathring{w}$，则 v 是一个单元组。若 $w(v) = 2\mathring{w}$，则 v 要么是一个单元组(其非零项的权为 $2\mathring{w}$)，要么是一个双元组(其两个非零项的权均为$\mathring{w}$)。特别地，对于任意线性码 $C \subseteq R^n$，

$$A_{2\mathring{w}}(C) = A_{2\mathring{w}}^{\mathrm{sing}}(C) + A_{2\mathring{w}}^{\mathrm{dble}}(C).$$

证明。如果向量 $v \in R^n$ 有 n' 个非零项，那么 $w(v) \ge n'\mathring{w}$。当且仅当每个非零项的权为 $\mathring{w}$时，等号成立。□

命题 4.8。设 w 是 $\mathbb{F}_q$ 上的一个权，满足 $-1 \in \mathrm{Sym}(w)$，且$\mathring{w}$ 在唯一一个 $\mathrm{Sym}(w)$-轨道上取到。设 C 是 $\mathbb{F}_q$上的一个线性码，其零位置由重数函数 η给出。那么

$$A_{2\mathring{w}}(C^\perp) = A_{2\mathring{w}}^{\mathrm{dble}}(C^\perp) = |\mathrm{Sym}(w)| \sum_{\iota} \binom{\eta_\iota}{2}.$$

证明。由于 C 中没有零位置，$A_s^{\mathrm{sing}}(C^\perp) = 0$ 对所有$s>0$都成立。因此，根据引理 4.7，$A_{2\mathring{w}}(C^\perp) = A_{2\mathring{w}}^{\mathrm{dble}}(C^\perp)$。

设 $x \in C^\perp$ 是一个双元组，满足 $w(x) = 2\mathring{w}$。由于是双元组，x 恰有两个非零项，记为 x_i，x_j。因为 $2\mathring{w} = w(x)$ =$w(x_i)$+$w(x_j)$，并且 $w(x_i)$ $w(x_j)$ 均至少为 $\mathring{w}$，可知 $w(x_i)$ =$w(x_j)$ = $\mathring{w}$。根据假设，x_i，x_j 必须属于使 w 取最小值的唯一 $\mathrm{Sym}(w)$-轨道。由假设 $-1 \in \mathrm{Sym}(w)$，可知$-x_i$ 与 x_i，x_j属于同一个 $\mathrm{Sym}(w)$-轨道。

设最小化轨道为 $[\mathring{r}]$。那么，对于某个 h_i，$h_j \in \mathrm{Sym}(w)$，有 $x_i = h_i\mathring{r}$ 和 $x_j = h_j\mathring{r}$ 。于是 $-x_ix_j^{-1} = -h_ih_j^{-1} \in \mathrm{Sym}(w)$。

由于 $x \in C^\perp$，我们有 $\lambda_i x_i + \lambda_j x_j = 0$。特别地，$\lambda_i$，$\lambda_j$ 线性相关，且 $\lambda_j = -\lambda_i x_i x_j^{-1} = \lambda_i(-h_ih_j^{-1})$。特别地，$\lambda_j$，$\lambda_i$ 属于同一个 $\mathrm{Sym}(w)$-轨道。根据 $\mathcal{O}$ 中代表元的唯一选取，我们有 $\lambda_j = \lambda_i$。这进而意味着 $x_j = -x_i$。

我们看到，通过从同一个 $\mathrm{Sym}(w)$-轨道中选取两个坐标泛函，并选取一个元素$h \in \mathrm{Sym}(w)$，即可得到对 $A_{2\mathring{w}}^{\mathrm{dble}}(C^\perp)$ 的贡献。然后令 $x_i = h\mathring{r}$ 和 $x_j = -h\mathring{r}$。□

注记 4.9。 如果有 $n_0 = n - \mathsf{efflen}(C)$ 个零位置，那么在 $C^\perp$ 中还会有额外的 $|\mathsf{Sym}(w)|^2\binom{n_0}{2}$ 个权为 $2\mathring{w}$ 的双元素集。 x_i 与 x_j之间不再有任何关系。

5. Some structured matrices

给定权 w 在 $\mathbb{F}_q$上，矩阵 W 在（3.5）中定义，结果发现它具有相当丰富的结构。本节将详细考察这一结构及一种相关结构。

取一个正整数 n。令 I_n 为单位矩阵， J_n为全一矩阵；也就是说， J_n 的每个元素都等于 1。对于一种结构，考虑所有具有如下形式的复矩阵：

$$M_{x,y} = (x-y)I_n + yJ_n = \begin{bmatrix} x & y & y & \cdots & y \\ y & x & y & \cdots & y \\ \vdots & & \ddots & & \vdots \\ y & y & \cdots & x & y \\ y & y & \cdots & y & x \end{bmatrix}. \tag{5.1}$$

引理 5.2。 若 $M_{x,\ y}$ 具有 (5.1)中的形式，则

$$\det M_{x,y} = (x + (n-1)y)(x-y)^{n-1}.$$

证明。 从每个其他行中减去第一行。然后将第 2 列至第 n 列加到第一列上。这些行变换和列变换不会改变行列式的值。经过这些行变换和列变换后，得到一个上三角矩阵，其行列式如所述。□

引理 5.3. 设 $M_{x,\ y}$ 如 (5.1)所示。若 $M_{x,\ y}$ 可逆，则$M^{-1}_{x,\ y}$ 也具有 (5.1) 中的形式。

证明。 将两个具有 (5.1) 所示形式的矩阵相乘：$M_{x,\ y}M_{z,\ w}$。 乘积具有如下形式$M_{\delta,\ \epsilon}$， 其中

$$\begin{aligned} \delta &= xz + (n-1)yw, \\ \epsilon &= xw + yz + (n-2)yw. \end{aligned}$$

令 $\delta = 1$， $\epsilon = 0$，并求解所得方程组，得到 z， w:

$$\begin{bmatrix} x & (n-1)y \\ y & x + (n-2)y \end{bmatrix} \begin{bmatrix} z \\ w \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

由于系数矩阵可逆，因此存在唯一的解。事实上，其行列式 $(x-y)(x + (n-1)y)$ 与 $\det M_{x,\ y}$ 具有相同的因子，而根据假设，该行列式非零。□

第二类结构来自形如(3.5)的矩阵。将讨论略作推广将会很有益。

固定一个子群 $H \subsetneq \mathbb{F}_q^\times$。（在（3.5）的语境中，对于有限域 $\mathbb{F}_q$上的权 w， $H = \mathrm{Sym}(w)$。）固定 $\mathbb{F}_q^\times$的一个本原元 α，令 t 为使 α^t 生成 H的最小正整数；于是 $t|H| = |\mathbb{F}_q^\times| = q-1$。由于 $H \neq \mathbb{F}_q^\times$，$t \geq 2$。若函数 $a\colon \mathbb{F}_q \to \mathbb{C}$ 满足对所有 $r \in \mathbb{F}_q$ 和所有 $h \in H$， $a(hr) = a(r)$，则称其为 H-不变函数。根据 H-不变性， a 的每个取值都是 $a(0)$ $a(1)$ $a(\alpha), \ldots, a(\alpha^{t-1})$ 之一。（在公式中，我们有时用 a_r 代替 $a(r)$。）

将（2.2）推广后，我们对每个 H-不变函数 $a\colon \mathbb{F}_q \to \mathbb{C}$ 关联一个 $t \times t$ 循环矩阵 $\mathcal{A}$，其行和列由以下元素索引$\{0, 1, \ldots, t-1\}$:

$$\mathcal{A}_{i,j} = a(\alpha^{i+j}), \quad i, j \in \{0, 1, \ldots, t-1\}. \tag{5.4}$$

回顾来自（ ℓ_μ， $\mu \in \{\infty, 0, 1, \ldots, q-1\}$，见（3.3），以及 $\mathcal{O}$，见（3.4），这里使用非零 H-轨道。将 x与 $y \in \mathbb{F}_q^2$ 的点积记为 $x \cdot y$。

引理 5.5。对于向量 ℓ_μ, $\mu \in \{\infty, 0, 1, \ldots, q-1\}$，定义 $f\colon \mathbb{F}_q^2 \to \mathbb{F}_q$，使其满足 $f(x) = x \cdot \ell_\mu$。那么存在唯一的 $\nu \in \{\infty, 0, 1, \ldots, q-1\}$，使得 $f(\ell_\nu) = 0$。

证明。 $\mathbb{F}_q^2$ 上的点积是非退化的，因此 f 非零。由于 f是线性的，它是满射，因此 $\dim \ker f = 1$。任意两个不同的ℓ_ν， ℓ_σ都线性无关，所以至多有一个 ℓ_ν包含在 $\ker f$中。若 $\mu = 0$ 或 ∞，则分别使用 $\nu = \infty$ 或 0。对于 $\mu \neq 0$， ∞，使用满足 $\alpha^\nu = -\alpha^{-\mu}$的$\nu$。□

当 $\ell_\nu \cdot \ell_\mu = 0$ 时，写作 $\ell_\mu^\perp \ell_\nu$。下一个引理描述在某些线性变换 $\mathbb{F}_q^2 \to \mathbb{F}_q^2$ 作用下， H-轨道会发生什么。

引理 5.6. 对于 $\alpha^i \ell_\mu$、 $\alpha^j \ell_\nu \in \mathcal{O}$，定义 $F\colon \mathbb{F}_q^2 \to \mathbb{F}_q^2$，使得 $F(x) = \langle x \cdot \alpha^i \ell_\mu, x \cdot \alpha^j \ell_\nu \rangle$。当 $x = \alpha^k \ell_\sigma$ 遍历 $\mathcal{O}$ 时，

- 当 $\mu = \nu$ 时： F 将包含在 $\ell_\mu^\perp$ 中的 t -轨道映射到 0，并且对包含在 $\langle 1$ 中的每个 t 轨道，恰好命中 $\alpha^{j-i}\rangle$ q 次；
- 当 $\mu \neq \nu$ 时： F 恰好命中 $\mathbb{F}_q^2$ 中每个非零 H-轨道一次。

证明。 当 $\mu \neq \nu$ 时，向量 $\alpha^i \ell_\mu, \alpha^j \ell_\nu$ 线性无关，因此 F 是一个同构。 $\mathcal{O}$ 中的元素是（非零） H-轨道的代表元，而 H-轨道划分了 $\mathbb{F}_q^2$。同构将轨道划分映回自身。因此，每个 H-轨道都必定恰好被命中一次。

当 $\mu = \nu$ 时，向量 $\alpha^i \ell_\mu$， $\alpha^j \ell_\nu$ 线性相关，因此 F 的秩为 1，其像等于由 $\mathbb{F}_q^2$ 张成的一维子空间

由 $\langle \alpha^i, \alpha^j \rangle$ 张成。事实上， $F(x) = (x \cdot \ell_\mu)\langle \alpha^i, \alpha^j \rangle = (x \cdot \ell_\mu)\alpha^i \langle 1, \alpha^{j-i} \rangle$。正如我们在引理 5.5 中看到的， t 非零 H-轨道映射为零（那些包含在 $\ell_\mu^\perp$ 中的轨道）。其余 qt 非零 H-轨道覆盖了包含在 $\langle \alpha^i$ 中的 t 轨道，每个轨道覆盖 q 次。$\alpha^j \rangle$ □

下面给出第二类结构的定义，它是（3.5）的一个轻微推广，因为 $a(0)$ 不受必须等于 0 的限制。对于每个 H-不变函数 $a\colon \mathbb{F}_q \to \mathbb{C}$，定义一个 $t(q+1) \times t(q+1)$ 矩阵 A，其行和列由 $\mathcal{O}$ 的元素作为索引：

$$A_{\alpha^i \ell_\mu, \alpha^j \ell_\nu} = a(\alpha^i \ell_\mu \cdot \alpha^j \ell_\nu). \tag{5.7}$$

这些索引满足 $i, j = 0, 1, \ldots, t-1$ 以及 $\mu, \nu \in \{\infty, 0, 1, \ldots, q-1\}$。注意， A 是一个对称矩阵。矩阵 A 具有继承自 $\mathcal{O}$的分块的分块形式。

例 5.8。 在 $\mathbb{F}_5$ 中，令 $H = \{\pm 1\} \subseteq \mathbb{F}_5^\times$。取 $\alpha = 2$。则 $t = 2$且

$$\begin{aligned}\mathcal{O} = \{&\langle 0,1\rangle, \langle 0,2\rangle, \langle 1,0\rangle, \langle 2,0\rangle, \langle 1,2\rangle, \langle 2,4\rangle,\\ &\langle 1,4\rangle, \langle 2,3\rangle, \langle 1,3\rangle, \langle 2,1\rangle, \langle 1,1\rangle, \langle 2,2\rangle\}.\end{aligned}$$

设 $a\colon \mathbb{F}_5 \to \mathbb{C}$ 是 H-不变的。则 $a_4 = a_1$、 $a_3 = a_2$，以及

$$A = \left[\begin{array}{cccccccccccc}
a_1 & a_2 & a_0 & a_0 & a_2 & a_1 & a_1 & a_2 & a_2 & a_1 & a_1 & a_2 \\
a_2 & a_1 & a_0 & a_0 & a_1 & a_2 & a_2 & a_1 & a_1 & a_2 & a_2 & a_1 \\ \hline
a_0 & a_0 & a_1 & a_2 & a_1 & a_2 & a_1 & a_2 & a_1 & a_2 & a_1 & a_2 \\
a_0 & a_0 & a_2 & a_1 & a_2 & a_1 & a_2 & a_1 & a_2 & a_1 & a_2 & a_1 \\ \hline
a_2 & a_1 & a_1 & a_2 & a_0 & a_0 & a_1 & a_2 & a_2 & a_1 & a_2 & a_1 \\
a_1 & a_2 & a_2 & a_1 & a_0 & a_0 & a_2 & a_1 & a_1 & a_2 & a_1 & a_2 \\ \hline
a_1 & a_2 & a_1 & a_2 & a_1 & a_2 & a_2 & a_1 & a_2 & a_1 & a_0 & a_0 \\
a_2 & a_1 & a_2 & a_1 & a_2 & a_1 & a_1 & a_2 & a_1 & a_2 & a_0 & a_0 \\ \hline
a_2 & a_1 & a_1 & a_2 & a_2 & a_1 & a_2 & a_1 & a_0 & a_0 & a_1 & a_2 \\
a_1 & a_2 & a_2 & a_1 & a_1 & a_2 & a_1 & a_2 & a_0 & a_0 & a_2 & a_1 \\ \hline
a_1 & a_2 & a_1 & a_2 & a_2 & a_1 & a_0 & a_0 & a_1 & a_2 & a_2 & a_1 \\
a_2 & a_1 & a_2 & a_1 & a_1 & a_2 & a_0 & a_0 & a_2 & a_1 & a_1 & a_2
\end{array}\right].$$

例子5.8 说明了以下一般结果。

引理 5.9. 对于任意 H-不变函数 $a\colon \mathbb{F}_q \to \mathbb{C}$，矩阵 A的分块有以下两种类型：

- 该分块是全 *1* 矩阵的 $a(0)$ 倍；或者
- 该分块是循环矩阵： $a(1)$ $a(\alpha) \ldots, a(\alpha^{t-1})$，或其循环移位。

对于给定的块行，第一类有一个分块，第二类有 q 个分块。对于 A的每一行，有 t 个条目等于 $a(0)$

以及 q 个条目分别等于 $a(1)$ $a(\alpha)\ldots,a(\alpha^{t-1})$。每一行各条目的和为 $ta(0)+q\sum_{j=0}^{t-1}a(\alpha^j)$。

证明。由 ℓ_μ 和 ℓ_ν 确定的分块，其 i,j 项等于 $a(\alpha^i\ell_\mu\cdot\alpha^j\ell_\nu)=a(\alpha^{i+j}(\ell_\mu\cdot\ell_\nu))$。如果 $\ell_\mu\cdot\ell_\nu=0$，那么该分块中的所有项都等于 $a(0)$。也就是说，该分块是 $a(0)$ 乘以一个 $t\times t$ 阶全 1 矩阵。

如果 $\ell_\mu\cdot\ell_\nu\neq 0$，那么对于某个 $k\in\{0,1,\ldots,q-2\}$，有 $\ell_\mu\cdot\ell_\nu=\alpha^k$。于是，$i,j$ 项等于 $a(\alpha^{i+j+k})$。由 a 的 H 不变性，这得到一个以 $a(\alpha^k)$ 开头的循环矩阵。

对于每个 ℓ_μ，存在唯一的 ℓ_ν 满足 $\ell_\mu\cdot\ell_\nu=0$，由引理 5.5。 □

推论 5.10。 设 $a(0)=0$。则 A 的任意一行或一列中各项之和为 $q\sum_{j=0}^{t-1}a(\alpha^j)$。若 A 可逆，则 A^{-1} 的任意一行或一列中各项之和为 $1/(q\sum_{j=0}^{t-1}a(\alpha^j))$。

证明。行和由引理 5.9 和 $a(0)=0$得出。这意味着全一向量 $\mathbf{1}$ 是 A 的特征向量，其特征值为 $q\sum_{j=0}^{t-1}a(\alpha^j)$。若 A 可逆，将特征向量方程两边乘以 A^{-1} 可得 $\mathbf{1}$是 A^{-1} 的特征向量，其特征值为$1/(q\sum_{j=0}^{t-1}w(\alpha^j))$。列和可由 A 是对称矩阵这一点得出。 □

现在考虑第二个 H-不变函数 $b\colon\ \mathbb{F}_q\to\mathbb{C}$，其关联矩阵为 B，大小为 $t(q+1)\times t(q+1)$。与上文一样，H-不变性意味着 b的每个取值都等于以下某个值：$b(0)$ $b(1)$ $b(\alpha)$ $b(\alpha^2)\ldots$，$b(\alpha^{t-1})$。

对于 H-不变函数 a，$b\colon\ \mathbb{F}_q\to\mathbb{C}$，定义 $\breve{a}$ 以及移位为 m、$m=0,1,\ldots,t-1$时的相关$c_m(a,b)$，

$$\breve{a}=\sum_{j=0}^{t-1}a(\alpha^j),\quad c_m(a,b)=\sum_{j=0}^{t-1}a(\alpha^j)b(\alpha^m\alpha^j). \tag{5.11}$$

引理 5.12。 $c_m(a,b)$ H不变函数的相关满足两个性质：

- $c_{m+t}(a,b)=c_m(a,b)$，因此指标 m 在模 t意义下是有定义的；
- $c_{t-m}(a,b)=c_m(b,a)$；特别地，$c_{t-m}(a,a)=c_m(a,a)$。

证明。第一个性质是 H 不变性的推论。第二个性质可通过对求和重新编号得到。□

现在我们从分块的角度讨论乘积 AB。

引理 5.13。 乘积 AB 具有以下特征：

- 对角分块是如下形式的相关矩阵

$$\begin{bmatrix} ta_0b_0+qc_0 & ta_0b_0+qc_1 & \cdots & ta_0b_0+qc_{t-1} \\ ta_0b_0+qc_{t-1} & ta_0b_0+qc_0 & \cdots & ta_0b_0+qc_{t-2} \\ \vdots & \vdots & \ddots & \vdots \\ ta_0b_0+qc_1 & ta_0b_0+qc_2 & \cdots & ta_0b_0+qc_0 \end{bmatrix},$$

  其中 $c_m = c_m(a,b)$ 始终成立。
- 所有非对角线分块都相同，即全由1 构成的矩阵
  ˘ ˘乘以 $a_0b + \breve{a}b_0 + ((q-1)/t)\breve{a}b$。

证明。 </*style*}先考虑非对角线分块的情形，其位置由, $\alpha^j\ell_\nu$索引，其中 $\mu \neq \nu$。 AB 在 E_o处对应的元素为

$$E_o = \sum_{\alpha^k\ell_\sigma \in \mathcal{O}} a(\alpha^{i+k}\ell_\mu \cdot \ell_\sigma)\, b(\alpha^{k+j}\ell_\sigma \cdot \ell_\nu).$$

如引理 5.6所示，每个 H-轨道恰好命中一次。利用 H-不变性 a以及 b，可得

$$\begin{aligned} E_o &= \sum_{k=0}^{t-1} a(0)b(\alpha^k) + \sum_{k=0}^{t-1}\sum_{r\in\mathbb{F}_q} a(\alpha^k)b(\alpha^k r) \\ &= \sum_{k=0}^{t-1} a(0)b(\alpha^k) + \sum_{k=0}^{t-1} a(\alpha^k)b(0) + \sum_{k=0}^{t-1}\sum_{m=0}^{q-2} a(\alpha^k)b(\alpha^{k+m}) \\ &= \sum_{k=0}^{t-1} a(0)b(\alpha^k) + \sum_{k=0}^{t-1} a(\alpha^k)b(0) + \frac{q-1}{t}\sum_{k=0}^{t-1}\sum_{m=0}^{t-1} a(\alpha^k)b(\alpha^{k+m}) \\ &= \sum_{k=0}^{t-1} a(0)b(\alpha^k) + \sum_{k=0}^{t-1} a(\alpha^k)b(0) + \frac{q-1}{t}\sum_{k=0}^{t-1} a(\alpha^k)\sum_{m'=0}^{t-1} b(\alpha^{m'}). \end{aligned}$$

最后一步中，我们通过 $m' = k+m$重新进行索引。

现在来看一个对角线块，使得 $\mu = \nu$。位置索引为 $\alpha^i\ell_\mu$， $\alpha^j\ell_\mu$ 处的元素 E_d 为

$$E_d = \sum_{\alpha^k\ell_\sigma \in \mathcal{O}} a(\alpha^{i+k}\ell_\mu \cdot \ell_\sigma)\, b(\alpha^{k+j}\ell_\sigma \cdot \ell_\mu).$$

根据引理 5.5，存在一个 ℓ_τ使得 $\ell_\mu \cdot \ell_\tau = 0$。对于其余的$q$向量 ℓ_σ, $\ell_\mu \cdot \ell_\sigma \neq 0$，因此 $\ell_\mu \cdot \ell_\sigma = \alpha^{m_\sigma}$，对于某个 $m_\sigma = 0$，1，...， $q-2$。

分离出包含在一个 ℓ_σ 中的轨道对 E_d 的贡献：

$$\begin{aligned}
&\sum_{k=0}^{t-1} a(\alpha^{i+k}\ell_\mu \cdot \ell_\sigma)\, b(\alpha^{k+j}\ell_\sigma \cdot \ell_\mu) \\
&\qquad = \begin{cases} ta(0)b(0), & \ell_\mu \cdot \ell_\sigma = 0, \\ \sum_{k=0}^{t-1} a(\alpha^{i+k}\alpha^{m_\sigma})\, b(\alpha^{k+j}\alpha^{m_\sigma}), & \ell_\mu \cdot \ell_\sigma \neq 0, \end{cases} \\
&\qquad = \begin{cases} ta(0)b(0), & \ell_\mu \cdot \ell_\sigma = 0, \\ \sum_{k=0}^{t-1} a(\alpha^{i+k})\, b(\alpha^{k+j}), & \ell_\mu \cdot \ell_\sigma \neq 0, \end{cases}
\end{aligned}$$

利用 H-不变性并对求和重新编号。将所有 ℓ_σ 的贡献相加，得到

$$\begin{aligned}
E_d &= ta(0)b(0) + q\sum_{k=0}^{t-1} a(\alpha^{i+k})\, b(\alpha^{k+j}) \\
&= ta(0)b(0) + qc_{j-i}(a,b).
\end{aligned}$$

□

推论 5.14。 设 $a\colon \mathbb{F}_q \to \mathbb{C}$ 是 H-不变的，且 $a(0) = 0$。假设 $\mathcal{A}$ 的 (5.4)矩阵可逆。那么， A 的 (5.7)矩阵也可逆，且逆矩阵 A^{-1} 具有 (5.7)的形式。

证明。 下面给出关于未知的 H-不变函数 b 的线性方程组：

$$\begin{aligned}
c_0(b,a) &= 1/q, \\
c_1(b,a) &= 0, \\
&\vdots \\
c_{t-1}(b,a) &= 0, \\
b(0) &= -((q-1)/t)\left(b(1) + \cdots + b(\alpha^{t-1})\right).
\end{aligned}$$

前 t 个方程的系数矩阵恰好是矩阵 $\mathcal{A}$，根据假设该矩阵可逆。因此，前 t个方程有唯一解 $b(1)$ $b(\alpha)\ldots, b(\alpha^{t-1})$，而最后一个方程给出 $b(0)$。根据引理 5.13， $BA = I_{t(q+1)}$，因此 $B = A^{-1}$。 □

注记 5.15。 结构化矩阵的定义可以扩展到（5.7）之外，其中使用了 H-轨道来定义 $\mathbb{F}_q^2$ （3.4）。使用 H-轨道也可以得到类似的结果，其中 $\mathbb{F}_q^k$ 可取任意整数 $k \geq 2$。

6. Constructing two-weight codes

本节将介绍几种双重量码的构造方法，它们都具有相同的重量分布。具体而言，我们通过对 ω 采用不同的选择来求解矩阵方程 $W\eta = \omega$。

假设 w 是定义在 $\mathbb{F}_q$ 上的非退化权，且 $w(0) = 0$。这意味着式 (5.4) 中的矩阵 $\mathcal{W}$ 可逆。通常，我们假设 w 取正整数值，但 $w(0) = 0$ 除外。记 $H = \mathrm{Sym}(w) \subseteq \mathbb{F}_q^\times$，并令 t 为满足 α^t 生成 H 的最小正整数，其中 α 是 $\mathbb{F}_q$ 的本原元。假设 $H \neq \mathbb{F}_q^\times$，于是 $t|H| = (q-1)$，其中 $t \geq 2$。由 H-不变性， $w(1)$ $w(\alpha)$ $w(\alpha^2)$.....、 $w(\alpha^{t-1})$ 的取值完全确定了 w。

要构造的线性码将具有维数 2。非零 H-轨道在 $\mathbb{F}_q^2$ 中的代表元为 $\mathcal{O}$ ，见式 (3.4)。将这类轨道的数量记为 $\tau = |\mathcal{O}| = t(q+1$。由推论 W （3.5）中的矩阵可逆，推论编号为 5.14。对于向量 η 和 $\omega \in \mathbb{Q}^\tau$，我们将仔细考察方程 $W\eta = \omega$ 在 ω 仅取两个正值时的解。我们希望了解在什么情况下，存在满足 $W\eta = \omega$ 且 η 所有取值均为非负的解。

将 $\mathbb{Q}^\tau$ 视为从 $\mathcal{O}$ 到 $\mathbb{Q}$的函数空间，并将 $\lambda \in \mathcal{O}$记作 $\mathcal{O}$中的一个典型元素。令 $\varrho \in \mathbb{Q}$ 为正数， $\varrho \neq 1$，并选取两个大小相同的子集 S， $S' \subseteq \mathcal{O}$： $s = |S| = |S'|$。定义元素ω， $\omega' \in \mathbb{Q}^{\mathcal{O}}$ 如下：

$$\omega(\lambda) = \begin{cases} \varrho, & \lambda \in S, \\ 1, & \text{otherwise;} \end{cases} \qquad \omega'(\lambda) = \begin{cases} \varrho, & \lambda \in S', \\ 1, & \text{otherwise.} \end{cases} \tag{6.1}$$

引理 6.2。 设 ω， ω' 如 (6.1)所示，且 $s = |S| = |S'|$。方程 $W\eta = \omega$， $W\eta' = \omega'$ 的解 η， η' 满足 $\sum_{\lambda\in\mathcal{O}} \eta(\lambda) = \sum_{\lambda\in\mathcal{O}} \eta'(\lambda)$。

证明。 在左侧乘以 $\omega = W\eta$ 和全 1 行向量 $\mathbf{1}$。根据推论 5.10， $\mathbf{1}$ 是 W的左特征向量，因此

$$\mathbf{1}\omega = \mathbf{1}W\eta,$$
$$s\varrho + \tau - s = q(\sum_{j=0}^{t-1} w(\alpha^j))\mathbf{1}\eta = q(\sum_{j=0}^{t-1} w(\alpha^j)) \sum_{\lambda\in\mathcal{O}} \eta(\lambda).$$

对 $\omega' = W\eta'$ 进行相同操作即可得到该结果。 □

以下是本文的主要技术成果。阅读证明时，读者或许会发现参阅例9.1很有帮助。

引理 6.3. 设 w 是$\mathbb{F}_q$上的非退化有理值权，其中 $w(0) = 0$, $w(r) > 0$，对于 $r \neq 0$，且 $H = \mathrm{Sym}(w) \neq \mathbb{F}_q^\times$。

固定一个满足 $0 < s < \tau = |\mathcal{O}|$ 的整数 s。那么存在有理数 $\delta^{(s)}$ $\boldsymbol{min}\delta_{\max}^{(s)}$，其中 $0 < \delta^{(s)}$ $\boldsymbol{min} < 1 < \delta_{\max}^{(s)}$，使得：对于任意子集$S \subset \mathcal{O}$，满足 $|S| = s$，以及任意满足 $\delta^{(s)}$ $\boldsymbol{min} \leq \varrho \leq \delta_{\max}^{(s)}$ 的 ϱ，方程 $W\eta = \omega$ 的解 η（其中 ω 如 *(6.1)* 中所示）满足 $\eta(\lambda) \geq 0$ 对所有 $\lambda \in \mathcal{O}$ 均成立。特别地，数 $\delta^{(s)}$ $\boldsymbol{min}\delta_{\max}^{(s)}$ 不依赖于大小为 s的子集 S 的选择。

证明。取任意满足 $|S| = s$ 的子集 $S \subset \mathcal{O}$，并考虑 (6.1) 中将 ϱ 作为未知值的 ω。由于 w 非退化，W 可逆。因此存在 $\eta = W^{-1}\omega$。这意味着 $\eta(\lambda) = P(\lambda) + Q(\lambda)\varrho$，其中 $Q(\lambda)$ 是 W^{-1} 在第 λ 行、由 S 中元素索引的各列上的项之和，而 $P(\lambda)$ 是第 λ 行其余各项之和。根据推论 5.10，$P(\lambda) + Q(\lambda) > 0$，对所有 $\lambda \in \mathcal{O}$ 均成立。这意味着，对于每个 λ，$P(\lambda)$ $Q(\lambda)$ 中至多一个可以为负。

如果 $P(\lambda) < 0$，那么 $Q(\lambda) > |P(\lambda)| > 0$，且 $\eta(\lambda) \geq 0$ 当且仅当 $\varrho \geq |P(\lambda)|/Q(\lambda)$。注意，$0 < |P(\lambda)|/Q(\lambda) < 1$。类似地，如果 $Q(\lambda) < 0$，那么 $P(\lambda) > |Q(\lambda)| > 0$，且 $\eta(\lambda) \geq 0$ 当且仅当$\varrho \leq P(\lambda)/|Q(\lambda)|$。注意，$P(\lambda)/|Q(\lambda)| > 1$。当 $P(\lambda)$ 和 $Q(\lambda)$ 均为非负时，对 ϱ 没有额外限制。

定义 $\delta_{\min}^S, \delta_{\max}^S$ 如下：

$$\delta_{\min}^S = \max\{|P(\lambda)|/Q(\lambda) \colon P(\lambda) < 0\},$$
$$\delta_{\max}^S = \min\{P(\lambda)/|Q(\lambda)| \colon Q(\lambda) < 0\}.$$

由于我们要找的是有限集正有理数中的最大值和最小值，因此可知 $0 < \delta_{\min}^S < 1 < \delta_{\max}^S$。如果 ϱ 满足$\delta_{\min}^S \leq \varrho \leq \delta_{\max}^S$，那么 ϱ 满足上一段中的所有不等式，并且每个 $\eta(\lambda)$ 都是非负的。

现在对满足 $|S| = s$ 的子集 $S \subset \mathcal{O}$ 进行优化。定义：

$$\delta_{\min}^{(s)} = \max\{\delta_{\min}^S \colon S \subset \mathcal{O}, |S| = s\},$$
$$\delta_{\max}^{(s)} = \min\{\delta_{\max}^S \colon S \subset \mathcal{O}, |S| = s\}.$$

由于大小为 s 的 $\mathcal{O}$ 子集只有有限多个，我们仍有 $0 <^{\delta^{(s)}\text{最小值}} < 1 < \delta_{\max}^{(s)}$。如果 ϱ 满足 $\delta^{(s)}{}_{\text{最小值}} \leq \varrho \leq \delta_{\max}^{(s)}$，那么对于所有满足 $|S| = s$ 的 S，都有 $\delta_{\min}^S \leq \varrho \leq \delta_{\max}^S$，因此对于任意满足$|S| = s$ 的 S，$\eta(\lambda) \geq 0, \lambda \in \mathcal{O}$。□

Define $\mathfrak{q}(\eta) = \sum_{\lambda \in \mathcal{O}} \eta(\lambda)(\eta(\lambda) - 1)$, $\eta \in \mathbb{Q}^{\mathcal{O}}$.

定理 6.4. 设 w 是 $\mathbb{F}_q$上的非退化有理值权，且 $w(0) = 0$, $w(r) > 0$ 对于 $r \neq 0$成立，并且 $H = \mathrm{Sym}(w) \neq \mathbb{F}_q^\times$。

假设（5.11）中的值$((q-1)/t)\,\breve{w}^2, qc_m(w,w),\ m=1,2,\dots,\lfloor t/2\rfloor$并非全都相等。那么存在两个子集 $S,S'\subseteq\mathcal{O}$，满足$|S|=|S'|=2$，使得对于满足$\delta^{(2)}\ \min\le\varrho\le\delta^{(2)}_{\max}$的 ϱ 值（至多有两个例外），以及如（6.1）中的 ω,ω'，方程 $W\eta=\omega, W\eta'=\omega'$的解 η,η'满足 $\eta(\lambda)\ge 0$, $\eta'(\lambda)\ge 0$对所有 $\lambda\in\mathcal{O}$均成立，且 $\mathfrak{q}(\eta)\ne\mathfrak{q}(\eta')$。

证明。我们已经看到，假设 w 非退化，意味着矩阵 $\mathcal{W}$（5.4）可逆。推论 5.14 于是推出矩阵 W（5.7）可逆，且其逆矩阵W^{-1}也具有（5.7）的形式。令 $b\colon \mathbb{F}_q\to\mathbb{Q}$为推论 给出的 H5.14 中的 $B=W^{-1}$不变函数。

假设 $((q-1)/t)\,\breve{w}^2, qc_m(w,w),\ m=1,2,\dots,\lfloor t/2\rfloor$并非全都相等，再结合引理 5.13，可知 W^2 不具有形式 (5.1)。接着，由引理 5.3 可知 $B^2=W^{-2}$ 也不具有形式 (5.1)。因此，将引理 5.13 应用于 $B^2=W^{-2}$，可知 $((q-1)/t)\breve{b}^2, tb_0^2+qc_m(b,b),\ m=1,2,\dots,\lfloor t/2\rfloor$并非全都相等。

有两种情况：

- $((q-1)/t)\breve{b}^2\ne tb_0^2+qc_m(b,\ b)$，其中某个 m，或者
- $tb_0^2+qc_{m_1}(b,\ b)\ne tb_0^2+qc_{m_2}(b,\ b)$，其中某个 $m_1\ne m_2$。

若 $((q-1)/t)\breve{b}^2\ne tb_0^2+qc_m(b,\ b)$，令 $S=\{\ell_0,\alpha^m\ell_0\}$ 和 $S'=\{\ell_0,\ell_\infty\}$。若 $tb_0^2+qc_{m_1}(b,\ b)\ne tb_0^2+qc_{m_2}(b,\ b)$，令 $S=\{\ell_0,\alpha^{m_1}\ell_0\}$和 $S'=\{\ell_0,\alpha^{m_2}\ell_0\}$。两种情况下，$|S|=|S'|=2$。

将引理 6.3 与 $s=2$ 应用于 S 和 S'，可得$\eta(\lambda)\ge 0$ 且 $\eta'(\lambda)\ge 0$，前提是 $\delta^{(2)}$ 最小$\le\varrho\le\delta^{(2)}_{\max}$。

设 $f(\varrho)=\mathfrak{q}(\eta)-\mathfrak{q}(\eta')$，并回忆引理 6.3 的证明，其中$\eta(\lambda)=P(\lambda)+Q(\lambda)\varrho$以及 $\eta'(\lambda)=P'(\lambda)+Q'(\lambda)\varrho$。为节省篇幅，记 η_λ为 $\eta(\lambda)$，等等。展开 $f(\varrho)$，并应用引理 6.2：

$$\begin{aligned} f(\varrho)&=\sum_{\lambda\in\mathcal{O}}(\eta_\lambda^2-\eta_\lambda'^2)\\ &=\sum_{\lambda\in\mathcal{O}}(P_\lambda^2-P_\lambda'^2)+2\sum_{\lambda\in\mathcal{O}}(P_\lambda Q_\lambda-P'_\lambda Q'_\lambda)\varrho+\sum_{\lambda\in\mathcal{O}}(Q_\lambda^2-Q_\lambda'^2)\varrho^2. \end{aligned}$$

仔细考察 $\sum_{\lambda\in\mathcal{O}}(Q_\lambda^2-Q_\lambda'^2)$。若 $((q-1)/t)\breve{b}^2\ne tb_0^2+qc_m(b,b)$，则由 (6.1) 可得 $Q_\lambda=g_{\lambda,\ell_0}+g_{\lambda,\alpha^m\ell_0}$ 以及 $Q'_\lambda=g_{\lambda,\ell_0}+g_{\lambda,\ell_\infty}$，其中 $g_{\lambda,\lambda'}$是 W^{-1} 的 λ,λ'项。将引理 5.9 应用于 b，可知 $B=W^{-1}$ 的每一行或每一列都包含相同的元素，只是位置不同。这意味着 $\sum_{\lambda\in\mathcal{O}}g^2_{\lambda,\lambda'}$ 的值与 λ'无关。因此$\sum_{\lambda\in\mathcal{O}}(Q_\lambda^2-Q_\lambda'^2)=2\sum_{\lambda\in\mathcal{O}}(g_{\lambda,\ell_0}g_{\lambda,\alpha^m\ell_0}-g_{\lambda,\ell_0}g_{\lambda,\ell_\infty})$。

由于 W 和 W^{-1} 是对称矩阵，我们可将和式$\sum_{\lambda\in\mathcal{O}}(Q_\lambda^2-Q_\lambda'^2)$识别为 W^{-2}的 ℓ_0，$\alpha^m\ell_0$项与

减去 ℓ_0, ℓ_∞项 W^{-2}。根据引理 5.13，这些项分别为$tb_0^2+qc_m(b,\ b)$ 和 $((q-1)/t)\breve{b}^2$。因此 $\sum_{\lambda\in\mathcal{O}}(Q_\lambda^2-Q_\lambda'^2)\neq 0$。

使用相同的论证，若 $tb_0^2+qc_{m_1}(b,b)\neq tb_0^2+qc_{m_2}(b,b)$，我们可将和式 $\sum_{\lambda\in\mathcal{O}}(Q_\lambda^2-Q_\lambda'^2)$ 识别为 $\ell_0,\alpha^{m_1}\ell_0$ 项与 W^{-2} 中的 $\ell_0,\alpha^{m_2}\ell_0$ 项之差的两倍。再次根据引理 5.13，这两项分别为 $tb_0^2+qc_{m_1}(b,b)$ 和 $tb_0^2+qc_{m_2}(b,b)$。因此$\sum_{\lambda\in\mathcal{O}}(Q_\lambda^2-Q_\lambda'^2)\neq 0$。

无论哪种情况，我们都可以得出结论：$f(\varrho)$ 是一个非平凡二次函数，至多有两个有理零点。令 ϱ 满足 $\delta^{(2)}{}_{\text{最小}}\leq\varrho\leq\delta^{(2)}_{\max}$，并避开 f 的零点，便可看出 $\mathfrak{q}(\eta)\neq\mathfrak{q}(\eta')$。□

注记 6.5. 可以证明，在定理 6.4 的假设下，$\varrho=1$ 是 f 的二重零点。

让我们考察在6.4 定理的假设下，$t=2$的情形。由于 $t\mid(q-1)$，q 在 $t=2$时必须为奇数。权 w 只有两个非零值，即 $w_1=w(\alpha)$ 和 $w_2=w(\alpha^2)$。事实上，$w_1\neq w_2$；否则，$\mathsf{Sym}(w)=\mathbb{F}_q^\times$，那么我们得到的将是 $t=1$，而不是 $t=2$。由此可知，w 是非退化的。事实上，由 (5.4)，

$$\mathcal{W}=\begin{bmatrix}w_2 & w_1\\ w_1 & w_2\end{bmatrix}.$$

那么 $\det\mathcal{W}=w_2^2-w_1^2=(w_1+w_2)(w_1-w_2)\neq 0$。

由于 $1\leq m\leq\lfloor t/2\rfloor$，当$t=2$时，$m$ 唯一可能的取值是 $m=1$。现在考虑 $((q-1)/t)\ \breve{w}^2=qc_1(w,\ w)$，其中 $t=2$。

展开 $((q-1)/2)\ \breve{w}^2=qc_1(w,\ w)$，得到 $(q-1)(w_1^2+2w_1w_2+w_2^2)=4qw_1w_2$，它关于 w_1 和 w_2对称。令 $x=w_2/w_1$，并整理得

$$w_1\left((q-1)-2(q+1)x+(q-1)x^2\right)=0.$$

方程关于 w_1，w_2 的对称性意味着 x 中的解互为倒数。解出 x得

$$x=\frac{q+1\pm 2\sqrt{q}}{q-1}.$$

当 q 不是平方数时，x 的这些值（因此 w_1，w_2中至少有一个）是无理数。但当 q 是平方数时，这些值是有理数。

下面列出一些较小的值，记住 q 必须是奇数（且是素数幂）。

(6.6)

q	9	25	49	81
$x,1/x$	$2,1/2$	$3/2,2/3$	$4/3,3/4$	$5/4,4/5$

总结：

命题 6.7. 假设 q 是一个奇素数的奇次幂。令 w 为定义在 $\mathbb{F}_q$上的任意整数值权，满足 $w(0) = 0$, $w(r) > 0$，其中 $r \neq 0$。若 $t = (q-1)/|\mathrm{Sym}(w)| = 2$，则 w 是非退化的，并且满足 $((q-1)/2)\,\check{w}^2 \neq qc_1(w, w)$。

7. Final arguments

本节中，我们完成主定理——定理 2.8的证明。

定理 2.8 的证明。应用定理 6.4：选取一个满足 $\delta^{(2)}\ \min \leq \varrho \leq \delta^{(2)}_{\max}$ 且使得 $\mathfrak{q}(\eta) \neq \mathfrak{q}(\eta')$ 的 ϱ 有理值，其中η、η'是由 (6.1) 得到的、分别对应于 $W\eta = \omega$ 和 $W\eta' = \omega'$ 的解。由于 ω 和ω' 是有理向量，且 W 是一个整数项可逆矩阵（在 $\mathbb{Q}$ 上可逆），因此向量 η 和 η' 的项都是（非负）有理数。

选取一个足够大的整数 N，使得 $N\eta$和 $N\eta'$的项都是（非负）整数。利用 $N\eta$和 $N\eta'$分别作为其重数函数，定义线性码 C 和 D 。它们的轨道权列表分别为 $N\omega = W(N\eta)$ 和 $N\omega' = W(N\eta')$。由于 W 是一个正项整数矩阵，且 $N\eta$, $N\eta'$ 是非负整数向量，因此 $N\omega$、$N\omega'$的项都是非负整数。根据 (6.1) 的形式，我们有

$$\mathrm{wwe}_C = \mathrm{wwe}_D = 1 + 2|\mathrm{Sym}(w)|t^{N\varrho} + (t(q+1) - 2)|\mathrm{Sym}(w)|t^N.$$

也就是说，有两个具有权 $N\varrho$ 的 $\mathrm{Sym}(w)$-轨道，其余轨道的权为 N。

现在考虑对偶码。我们断言 $A_{2\mathring{w}}(C^\perp) \neq A_{2\mathring{w}}(D^\perp)$。根据引理 4.7，

$$\begin{aligned} &A_{2\mathring{w}}(C^\perp) - A_{2\mathring{w}}(D^\perp) \\ &\quad = A^{\mathrm{sing}}_{2\mathring{w}}(C^\perp) - A^{\mathrm{sing}}_{2\mathring{w}}(D^\perp) + A^{\mathrm{dble}}_{2\mathring{w}}(C^\perp) - A^{\mathrm{dble}}_{2\mathring{w}}(D^\perp). \end{aligned}$$

由于 $\mathrm{wwe}_C = \mathrm{wwe}_D$，命题 4.6 表明，对于所有 s，$A^{\mathrm{sing}}_s(C^\perp) = A^{\mathrm{sing}}_s(D^\perp)$。记住，选择 ϱ 时使得 $\mathfrak{q}(\eta) \neq \mathfrak{q}\eta'$。然后，利用引理 6.2，我们看到 $\mathfrak{q}(N\eta) - \mathfrak{q}N\eta' = N^2(\mathfrak{q}(\eta) - \mathfrak{q}(\eta')) \neq 0$。根据命题 4.8，有 $A^{\mathrm{dble}}_{2\mathring{w}}(C^\perp) - A^{\mathrm{dble}}_{2\mathring{w}}D^\perp \neq 0$。因此 $A_{2\mathring{w}}(C^\perp) \neq A_{2\mathring{w}}D^\perp$。□

8. 对称化枚举器

在本节中，我们将简要概述由群作用给出的对称化枚举式。这将使我们能够在许多例子中计算 w-重量枚举器。证明及更多细节见 [8], [16], [17], 或 [19]。

我们将重点讨论有限域 $\mathbb{F}_q$上的线性码。域 $\mathbb{F}_q$ 的大小为 $q = p^l$ ，其中 p 是素数， l是正整数。绝对迹tr: $\mathbb{F}_q \to \mathbb{F}_p$ 定义为

$$\mathrm{tr}(r) = r + r^p + r^{p^2} + \ldots + r^{p^{l-1}}, \quad r \in \mathbb{F}_q.$$

绝对迹是 $\mathbb{F}_p$-向量空间的一个非零同态。固定一个本原 p 次单位根 $\zeta \in \mathbb{C}$。定义 χ: $\mathbb{F}_q \to \mathbb{C}^\times$ by$\chi(r) = \zeta^{\mathrm{tr}(r)}$; χ 是 $\mathbb{F}_q$的一个生成特征。

固定一个子群 $H \subseteq \mathbb{F}_q^\times$。固定 $\mathbb{F}_q$中的一个本原元 α ，并令 t 为使 α^t 生成 H的最小正整数。子群H 通过乘法作用于 $\mathbb{F}_q$ 。 H 的轨道为: $P_0 = \{0\}$ 以及 $\mathbb{F}_q^\times$中的陪集 $P_i = \alpha^i H$、 $i = 1, 2, \ldots\ldots, t$。注意 $P_t = H$。这些轨道构成 $\mathbb{F}_q$的一个划分 $\mathcal{P}_H = (P_i)_{i=0}^t$ 。对于 $r \in \mathbb{F}_q$, 当 $r \in P_i$时，记 $\nu(r) = i$。

与 $\mathcal{P}_H$ 相关联的克拉夫丘克矩阵 K 是 $(t+1) \times (t+1)$ 矩阵，对 i, $j = 0, 1, \ldots\ldots, t$ 定义如下

$$\begin{aligned} K_{0,j} &= |P_j|, \\ K_{i,j} &= \sum_{s \in P_j} \chi(\alpha^i s), \quad i = 1, 2, \ldots, t. \end{aligned} \tag{8.1}$$

线性码的对称化枚举式 se_C 是划分 $\mathcal{P}_H$的划分枚举器。它是多项式环 $\mathbb{C}[Z_0, Z_1, \ldots, Z_t]$ 中的一个元素，其定义为

$$\mathrm{se}_C(Z_0, Z_1, \ldots, Z_t) = \sum_{c \in C} \prod_{k=1}^{n} Z_{\nu(c_k)}, \tag{8.2}$$

其中 $c = (c_1, c_2, \ldots, c_n) \in C$。(8.2)中的乘积记录了 c 中属于各个 H-轨道的元素个数。

对称化枚举式满足麦克威廉姆斯恒等式:

$$\mathrm{se}_{C^\perp}(Z_0, \ldots, Z_t) = \frac{1}{|C|} \mathrm{se}_C(\mathcal{Z}_0, \mathcal{Z}_1, \ldots, \mathcal{Z}_t)|_{\mathcal{Z}_i \leftarrow \sum_{j=0}^t K_{i,j} Z_j}. \tag{8.3}$$

设 w 是 $\mathbb{F}_q$上的一个整数值权，满足 $w(0) = 0$ 且$w(r) > 0$ 对非零 r成立。令 $H = \mathsf{Sym}(w)$，并如上构造划分$\mathcal{P}_H$。那么，线性码 $C \subseteq \mathbb{F}_q^n$ 的 w-重量枚举器 wwe_C 可通过将变量 $Z_0 \rightsquigarrow 1$ 和 $Z_i \rightsquigarrow y^{w(\alpha^i)}$ 取特定值来从对称化枚举式 se_C 中恢复，其中 $i = 1, 2, \ldots, t$。即,

$$\mathrm{wwe}_C(y) = \mathrm{se}_C(Z_0, Z_1, \ldots, Z_t)|_{Z_0 \leftarrow 1, Z_i \leftarrow y^{w(\alpha^i)}}. \tag{8.4}$$

注意，轨道 $P_i = \alpha^i H$ 中的任意元素都可写成 $r = \alpha^i h$ ，其中 $h \in H$。于是 $w(r) = w(\alpha^i)$，因为 $h \in H = \mathsf{Sym}(w)$。

9. Examples

本节给出几个示例，以说明定理2.8及其假设。所有复杂计算均使用 SageMath 完成 [15]。第一个示例进行了显式计算，与定理2.8的证明相呼应。

例 9.1. 考虑 E on $\mathbb{F}_5$ 上的欧几里得权重：

r	0	1	2	3	4
$\mathrm{E}(r)$	0	1	4	4	1

注意，$\mathrm{Sym}(\mathrm{E}) = \{\pm 1\} = \{1, 4\}$。我们选择 $\alpha = 2$，使得 $t = 2$。那么矩阵 $\mathcal{W}$ (5.4) 为

$$\mathcal{W} = \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}.$$

于是 $\det \mathcal{W} = -15 \neq 0$，因此权重 E 是非退化的。（一般而言，欧几里得权重在任意 $\mathbb{Z}/m\mathbb{Z}$ 阶 [6]上都是非退化的。）如例 5.8所示，我们看到

$$W = \begin{bmatrix} 1 & 4 & 0 & 0 & 4 & 1 & 1 & 4 & 4 & 1 & 1 & 4 \\ 4 & 1 & 0 & 0 & 1 & 4 & 4 & 1 & 1 & 4 & 4 & 1 \\ 0 & 0 & 1 & 4 & 1 & 4 & 1 & 4 & 1 & 4 & 1 & 4 \\ 0 & 0 & 4 & 1 & 4 & 1 & 4 & 1 & 4 & 1 & 4 & 1 \\ 4 & 1 & 1 & 4 & 0 & 0 & 1 & 4 & 4 & 1 & 4 & 1 \\ 1 & 4 & 4 & 1 & 0 & 0 & 4 & 1 & 1 & 4 & 1 & 4 \\ 1 & 4 & 1 & 4 & 1 & 4 & 4 & 1 & 4 & 1 & 0 & 0 \\ 4 & 1 & 4 & 1 & 4 & 1 & 1 & 4 & 1 & 4 & 0 & 0 \\ 4 & 1 & 1 & 4 & 4 & 1 & 4 & 1 & 0 & 0 & 1 & 4 \\ 1 & 4 & 4 & 1 & 1 & 4 & 1 & 4 & 0 & 0 & 4 & 1 \\ 1 & 4 & 1 & 4 & 4 & 1 & 0 & 0 & 1 & 4 & 4 & 1 \\ 4 & 1 & 4 & 1 & 1 & 4 & 0 & 0 & 4 & 1 & 1 & 4 \end{bmatrix}.$$

于是 $-75W^{-1}$ 等于

$$\begin{bmatrix}
1 & -4 & 6 & 6 & -4 & 1 & 1 & -4 & -4 & 1 & 1 & -4 \\
-4 & 1 & 6 & 6 & 1 & -4 & -4 & 1 & 1 & -4 & -4 & 1 \\
6 & 6 & 1 & -4 & 1 & -4 & 1 & -4 & 1 & -4 & 1 & -4 \\
6 & 6 & -4 & 1 & -4 & 1 & -4 & 1 & -4 & 1 & -4 & 1 \\
-4 & 1 & 1 & -4 & 6 & 6 & 1 & -4 & -4 & 1 & -4 & 1 \\
1 & -4 & -4 & 1 & 6 & 6 & -4 & 1 & 1 & -4 & 1 & -4 \\
1 & -4 & 1 & -4 & 1 & -4 & -4 & 1 & -4 & 1 & 6 & 6 \\
-4 & 1 & -4 & 1 & -4 & 1 & 1 & -4 & 1 & -4 & 6 & 6 \\
-4 & 1 & 1 & -4 & -4 & 1 & -4 & 1 & 6 & 6 & 1 & -4 \\
1 & -4 & -4 & 1 & 1 & -4 & 1 & -4 & 6 & 6 & -4 & 1 \\
1 & -4 & 1 & -4 & -4 & 1 & 6 & 6 & 1 & -4 & -4 & 1 \\
-4 & 1 & -4 & 1 & 1 & -4 & 6 & 6 & -4 & 1 & 1 & -4
\end{bmatrix}.$$

注意到 W 的行和与列和均等于 25，而 W^{-1} 的行和与列和均等于 $1/25$，这正如推论 5.10 所预期的那样。矩阵 W^2 沿对角线有 2×2 个分块 $\left[\begin{smallmatrix}85 & 40\\ 40 & 85\end{smallmatrix}\right]$，其余所有元素均等于 50。类似地，矩阵 $5625W^{-2}$ 沿对角线有 2×2 个分块 $\left[\begin{smallmatrix}157 & 32\\ 32 & 157\end{smallmatrix}\right]$，其余所有元素均等于 -18。由于 $c_0(w,w)=17$，$c_1(w,w)=8$，以及 $\breve{w}=5$，我们看到 W^2 符合引理 5.13 的形式。对于满足 $B=-75W^{-1}$ 的 $\mathrm{Sym}(w)$-不变函数 b，情况类似：$b(0)=6$，$b(1)=1$，$b(2)=-4$。于是 $\breve{b}=-3$，$c_0(b,b)=17$，且 $c_1(b,b)=-8$。

如定理6.4的证明中一样，令

$$\omega=\langle 1,1,\varrho,\varrho,1,1,1,1,1,1,1,1\rangle,$$
$$\omega'=\langle \varrho,1,\varrho,1,1,1,1,1,1,1,1,1\rangle.$$

求解 $W\eta=\omega$ 和 $W\eta'=\omega'$；然后使用 $N=75$ 清除分母：

$$\begin{aligned}
75\eta =&\langle -12\varrho+15,-12\varrho+15,3\varrho,3\varrho,3\varrho,3\varrho,3\varrho,3\varrho,3\varrho,3\varrho,3\varrho,3\varrho\rangle,\\
75\eta' =&\langle -7\varrho+10,-2\varrho+5,-7\varrho+10,-2\varrho+5,3\varrho,3\varrho,\\
&\quad -2\varrho+5,8\varrho-5,3\varrho,3\varrho,-2\varrho+5,8\varrho-5\rangle.
\end{aligned}$$

如果 $5/8\le\varrho\le 5/4$，所有元素都将是非负的。计算可得 $f(\varrho)=\mathfrak{q}(\eta)-\mathfrak{q}(\eta')=100(\varrho-1)^2$。首项系数与 W^{-2} 的元素有关：$100=2(32-(-18))$。

依次使用 ϱ 的两个极点，并进行适当归一化：

$$\begin{aligned}
\eta_{C_-} &= \langle 4,4,1,1,1,1,1,1,1,1,1,1\rangle,\\
\omega_{C_-} &= \langle 40,40,25,25,40,40,40,40,40,40,40,40\rangle,\\
\eta_{D_-} &= \langle 3,2,3,2,1,1,2,0,1,1,2,0\rangle,\\
\omega_{D_-} &= \langle 25,40,25,40,40,40,40,40,40,40,40,40\rangle;\\
\eta_{C_+} &= \langle 0,0,3,3,3,3,3,3,3,3,3,3\rangle,\\
\omega_{C_+} &= \langle 60,60,75,75,60,60,60,60,60,60,60,60\rangle,\\
\eta_{D_+} &= \langle 1,2,1,2,3,3,2,4,3,3,2,4\rangle,\\
\omega_{D_+} &= \langle 75,60,75,60,60,60,60,60,60,60,60,60\rangle.
\end{aligned}$$

线性码 C_- 和 D_- 的长度为 18，而 C_+ 和 D_+ 的长度为 30；参见引理6.2。所有非零轨道的大小均为 2，因此

$$\begin{aligned}
\mathrm{ewe}_{C_-} &= \mathrm{ewe}_{D_-} = 1 + 4y^{25} + 20y^{40},\\
\mathrm{ewe}_{C_+} &= \mathrm{ewe}_{D_+} = 1 + 20y^{60} + 4y^{75}.
\end{aligned}$$

权的比值按设计为 $25/40 = 5/8$ 和 $75/60 = 5/4$。由引理6.2、引理4.7和命题4.8，可得

$$\begin{aligned}
A_2(C_-^\perp) - A_2(D_-^\perp) &= 24 - 20 = 4,\\
A_2(C_+^\perp) - A_2(D_+^\perp) &= 60 - 56 = 4.
\end{aligned}$$

这些线性码的对称化枚举式（8.2）为：

$$\begin{aligned}
\mathrm{se}_{C_-} &= Z_0^{18} + 4Z_0^8Z_1^5Z_2^5 + 20Z_0^2Z_1^8Z_2^8,\\
\mathrm{se}_{D_-} &= Z_0^{18} + 4Z_0^5Z_1^9Z_2^4 + 16Z_0^2Z_1^8Z_2^8 + 4Z_0^5Z_1^4Z_2^9;\\
\mathrm{se}_{C_+} &= Z_0^{30} + 20Z_0^6Z_1^{12}Z_2^{12} + 4Z_1^{15}Z_2^{15},\\
\mathrm{se}_{D_+} &= Z_0^{30} + 4Z_0^3Z_1^{16}Z_2^{11} + 16Z_0^6Z_1^{12}Z_2^{12} + 4Z_0^3Z_1^{11}Z_2^{16}.
\end{aligned}$$

通过代入 $Z_0 \rightsquigarrow 1$，$Z_1 \rightsquigarrow y^4$和 $Z_2 \rightsquigarrow y$，根据（8.4），对称化枚举式可得欧几里得重量枚举式。

用于 se 的麦克威廉姆斯恒等式的克拉夫丘克矩阵（8.1）为

$$K = \begin{bmatrix} 1 & 2 & 2 \\ 1 & (\sqrt{5}-1)/2 & -(\sqrt{5}+1)/2 \\ 1 & -(\sqrt{5}+1)/2 & (\sqrt{5}-1)/2 \end{bmatrix}.$$

那么，（8.3），再进行特化（8.4），得到

$$\begin{aligned}
\mathrm{wwe}_{C_-^\perp} &= 1 + 24y^2 + 296y^3 + 1900y^4 + 10760y^5 + \cdots, \\
\mathrm{wwe}_{D_-^\perp} &= 1 + 20y^2 + 296y^3 + 1956y^4 + 10760y^5 + \cdots; \\
\mathrm{wwe}_{C_+^\perp} &= 1 + 60y^2 + 1260y^3 + 17880y^4 + 182772y^5 + \cdots, \\
\mathrm{wwe}_{D_+^\perp} &= 1 + 56y^2 + 1304y^3 + 17720y^4 + 182816y^5 + \cdots.
\end{aligned}$$

接下来的两个例子讨论了（6.6）中出现的一些权和有限域。在一种情形下，在 $\mathbb{F}_9$ 上，我们发现麦克威廉姆斯恒等式成立。在另一种情形下，在 $\mathbb{F}_{25}$ 上，我们发现，尽管定理 2.8 不适用，引理 6.3 给出的线性码仍表明对偶性并不成立。

例 9.2。令 $q = 9$。多项式 $x^2 - x - 1$ 在 $\mathbb{F}_3$上不可约。设 $\mathbb{F}_9 = \mathbb{F}_3[\alpha]/(\alpha^2 - \alpha - 1)$。乘法群 $\mathbb{F}_9^\times$是一个阶为 8 的循环群，由 α 生成。也就是说，α 是一个本原元：

i	0	1	2	3	4	5	6	7
α^i	1	α	$1+\alpha$	$1+2\alpha$	2	2α	$2+2\alpha$	$2+\alpha$

存在唯一的子群 $H \subset \mathbb{F}_9^\times$ 满足 $|H| = 4$：$H = \{1, 1+\alpha, 2, 2+2\alpha\}$；$H$ 由 α^2生成，因此 $t = 2$。在 $\mathbb{F}_9$上的一个权 w，若 Sym$(w) = H$，则有两个非零正值，分别记作 w_2（对应 H）和 w_1（对应陪集 $\alpha H = \{\alpha, 1+2\alpha, 2\alpha, 2+\alpha\}$）。注意 $w_1 \neq w_2$。事实上，若 $w_1 = w_2$，则 Sym(w)= $\mathbb{F}_9^\times$严格大于 H。

权 w 是非退化的。矩阵 $\mathcal{W}$（5.4）为

$$\mathcal{W} = \begin{bmatrix} w_2 & w_1 \\ w_1 & w_2 \end{bmatrix},$$

其行列式非零：$\det \mathcal{W} = w_2^2 - w_1^2 \neq 0$。

（6.6）中尤其值得关注的是 $w_1 = 1$，$w_2 = 2$（或反过来：$w_1 = 2$，$w_2 = 1$）。正如预期，$((q-1)/t)\,\breve{w}^2 = 36 = qc_1$（$w$，$w$），因此定理 2.8不适用。

定义两个 $\mathbb{F}_3$-线性同构 f，g: $\mathbb{F}_9 \to \mathbb{F}_3^2$，以 $\{1, \alpha\}$ 作为 $\mathbb{F}_9$ 的 $\mathbb{F}_3$-基：

$$f(x + y\alpha) = (x + y, x), \qquad g(x + y\alpha) = (y, x - y).$$

以下是它们的取值，其中 $(a,\ b) \in \mathbb{F}_3^2$ 写作 ab：

$x+y\alpha$	0	1	α	$1+\alpha$	$1+2\alpha$	2	2α	$2+2\alpha$	$2+\alpha$
$f(x+y\alpha)$	00	11	10	21	01	22	20	12	02
$g(x+y\alpha)$	00	01	12	10	22	02	21	20	11

当 w 具有 $w_1 = 1$，$w_2 = 2$时，f 是从 $\mathbb{F}_9$（赋予权 w）到 $\mathbb{F}_3^2$（赋予来自 $\mathbb{F}_3$ 的汉明重量）的等距映射。若取值顺序相反，即 $w_1 = 2$，$w_2 = 1$，则与汉明重量等距映射的是 g。

假设两个向量 $v, v' \in \mathbb{F}_9^n$ 满足 $v \cdot v' = 0$，其中使用 $\mathbb{F}_9$ 上的标准点积。记 $v = (x_1 + y_1\alpha, \ldots, x_n + y_n\alpha)$，$v'$ 也类似。注意，$r \in \mathbb{F}_9$ 的绝对迹为 $\mathrm{tr}(r) = r + r^3$，因此 $\mathrm{tr}(1) = 2$，$\mathrm{tr}(\alpha) = 1$，且 $\mathrm{tr}(\alpha^2) = 0$。于是

$$
\begin{aligned}
0 = \mathrm{tr}(v \cdot v') &= \sum_{i=1}^{n} \left(x_i x_i' + (x_i y_i' + y_i x_i')\alpha + y_i y_i' \alpha^2 \right) \\
&= \sum_{i=1}^{n} \left(x_i x_i' \,\mathrm{tr}(1) + (x_i y_i' + y_i x_i')\,\mathrm{tr}(\alpha) + y_i y_i' \,\mathrm{tr}(\alpha^2) \right) \\
&= \sum_{i=1}^{n} \left(2x_i x_i' + x_i y_i' + y_i x_i' \right) \\
&= \begin{cases} \sum_{i=1}^{n} \left((x_i + y_i)x_i' + x_i(x_i' + y_i') \right) \\ \sum_{i=1}^{n} \left(y_i y_i' - (x_i - y_i)(x_i' - y_i') \right). \end{cases}
\end{aligned}
$$

虽然最后这些表达式并非 $\mathbb{F}_3^{2n}$ 上的标准点积，但可以证明，汉明重量的麦克威廉姆斯恒等式对这些内积仍然成立。因此，这里讨论的 $\mathbb{F}_9$ 上的两种权继承了麦克威廉姆斯恒等式，因而满足对偶性。

例 9.3。设 $q = 25$ 和 $t = 2$。多项式 $x^2 - x - 3$ 在 $\mathbb{F}_5$ 上不可约。用这个多项式表示 $\mathbb{F}_{25} = \mathbb{F}_5[\beta]/(\beta^2 - \beta - 3)$。乘法群 $\mathbb{F}_{25}^{\times}$ 是一个阶为 24 的循环群，而 β 是一个生成元（本原元）。存在唯一的一个阶为 12 的子群 H；H 由 $\beta^2 = \beta + 3$ 生成。若权 w 满足 $\mathrm{Sym}(w) = H$，则它有两个非零正值，记为 w_2，在 H 上取值；另一个值 w_1 则在另一个陪集 βH 上取值。正如例 9.2 中所述，$w_1 \neq w_2$。

特别值得关注的是（6.6）中 $w_1 = 2$、$w_2 = 3$（或反之：$w_1 = 3$、$w_2 = 2$）的情形。借助 SageMath 的计算得到 $\delta^{(2)}_{\text{最小}} = 5/6$ 以及 $\delta^{(2)}_{\max} = 25/24$。进一步地，在 $\varrho \in \{5/6, 25/24\}$（6.1）中进行计算，得到两对线性码：长度为 62 的 C、D，以及长度为 C'、D' 的

250，具有如下 w-重量枚举器：

$$\begin{aligned}
\mathrm{wwe}_C &= 1 + 24t^{125} + 600t^{150},\\
\mathrm{wwe}_D &= 1 + 24t^{125} + 600t^{150},\\
\mathrm{wwe}_{C^\perp} &= 1 + 360t^4 + 1464t^5 + 114120t^6 + \cdots,\\
\mathrm{wwe}_{D^\perp} &= 1 + 360t^4 + \ 864t^5 + 115920t^6 + \cdots;\\
\mathrm{wwe}_{C'} &= 1 + 600t^{600} + 24t^{625},\\
\mathrm{wwe}_{D'} &= 1 + 600t^{600} + 24t^{625},\\
\mathrm{wwe}_{C'^\perp} &= 1 + 6000t^4 + 15000t^5 + 7116000t^6 + \cdots,\\
\mathrm{wwe}_{D'^\perp} &= 1 + 6000t^4 + 14400t^5 + 7117800t^6 + \cdots.
\end{aligned}$$

对于 ϱ 的两个取值，我们看到对偶码在 A_5处不同。因此，权 w 不具有对偶性。

对偶码的 A_5 值可以直接由原码的重数函数 η 计算得出 C。权为 5 的向量必定是一个双元组，其中一个非零项位于 H，另一个非零项位于 βH。当 $x\beta^{i_1}\ell_{\mu_1} + y\beta^{i_2}\ell_{\mu_2} = 0$ 时，双元组将是一个对偶码字，其中 x、y 是该双元组的非零项，分别出现在位置 $\beta^{i_1}\ell_{\mu_1}$、$\beta^{i_2}\ell_{\mu_2}$。由于这些直线 ℓ_μ 线性无关，我们必须有 $\mu_1 = \mu_2$。于是 $x\beta^{i_1} + y\beta^{i_2} = 0$，或 $x = -y\beta^{i_2-i_1}$。

由于 $t = 2$，i_1、$i_2 \in \{0, 1\}$。为了使 x、y 属于不同的陪集，$i_2 - i_1$ 必须为奇数。因此，对于每个等于 ℓ_μ 的列和每个等于 $\beta\ell_\mu$的列，任取一个 $y \in \mathbb{F}_{25}^\times$ 并令 $x = -y\beta$。于是$x\ell_\mu + y\beta\ell_\mu = 0$。这给出了计数

$$A_5(C^\perp) = \sum_\mu 24\eta(\ell_\mu)\eta(\beta\ell_\mu).$$

我们的最后一个例子讨论幂重量 $w^{(\ell)}$。

例 9.4。考虑例 $w^{(\ell)}$ 中的幂重量2.5 在$\mathbb{Z}/m\mathbb{Z}$上。由于 $w^{(0)}$ 是汉明重量，因此麦克威廉姆斯恒等式对 $w^{(0)}$ 上的任意 $\mathbb{Z}/m\mathbb{Z}$，$m \geq 2$，[16]都成立。幂权重 $w^{(1)}$等于李重量 L。我们知道，L 的麦克威廉姆斯恒等式在 $\mathbb{Z}/m\mathbb{Z}$ 上对 $m = 2$、3、4 和 L 在$\mathbb{Z}/m\mathbb{Z}$ 上对 $m \geq 5$、[1]不满足对偶性。

假设 $\ell \geq 1$。那么，对称群 $H = \mathrm{Sym}(w^{(\ell)}) = \{\pm 1\}$。首先考虑 $m = p$ 为素数的情形。如果 $p = 2$ 或 $p = 3$，所有幂重量 $w^{(\ell)}$ 都等于汉明重量。再次，我们知道麦克威廉姆斯恒等式成立。因此现在假设 $p \geq 5$。

对于 $p \geq 5$，每个幂权重 $w^{(\ell)}$，$\ell \geq 1$满足定理 2.8 的五个假设中的三个，即 $-1 \in \mathrm{Sym}(w^{(\ell)})$、$\mathrm{Sym}(w^{(\ell)}) \neq \mathbb{F}_p^\times$（这里需要 $p \geq 5$），以及最小值 $\mathring{w}^{(\ell)} = 1$在 $H = \{\pm 1\}$上取得。剩下的是关于非退化性以及关于 $qc_1(w, w)$ 等具有不同取值的假设。

李重量 $\mathrm{L} = w^{(1)}$ 和欧几里得权重 $\mathrm{E} = w^{(2)}$ 已知在 $\mathbb{F}_p$ [7]上是非退化的；事实上，它们在所有 $\mathbb{Z}/m\mathbb{Z}$ [6]上都是非退化的。对于 $\ell \geq 3$，目前只有数值证据。例如，SageMath 计算表明，矩阵 $\mathcal{W}^{(\ell)}$（5.4）在 $\ell = 3$、4、……、10 时，对于前 100 个素数均具有最大秩。

现在来看关于 $qc_1(w, w)$ 等取不同值的假设。由于 $|H| = 2$, $t = (p-1)/2$。如果 $p = 5$，那么 $t = 2$，并且只有$5c_1(w^{(\ell)}, w^{(\ell)})$ 和 $2(\breve{w}^{(\ell)})^2$ 可用。这些表达式为：

$$\begin{aligned} 5c_1(w^{(\ell)}, w^{(\ell)}) &= 5 \cdot 2^{\ell+1}, \\ 2(\breve{w}^{(\ell)})^2 &= 2(1 + 2^\ell)^2. \end{aligned}$$

由于 $\ell \geq 1$，这些值不同：第一个能被 4 整除，而第二个模 4 同余于 2。

对于 $p = 7$，其中 $t = 3$：同样，只有 $7c_1(w^{(\ell)}, w^{(\ell)})$ 和 $2(\breve{w}^{(\ell)})^2$ 可用。现在的表达式为：

$$\begin{aligned} 7c_1(w^{(\ell)}, w^{(\ell)}) &= 7(2^\ell + 3^\ell + 6^\ell), \\ 2(\breve{w}^{(\ell)})^2 &= 2(1 + 2^\ell + 3^\ell)^2. \end{aligned}$$

同样，这些值并不相同：第一个是奇数，第二个是偶数。

对于 $p \geq 11$，我们有 $t \geq 5$，因此 $pc_2(w^{(\ell)}, w^{(\ell)})$ 也可用（也可能还有其他 $pc_j(w^{(\ell)}, w^{(\ell)})$）。同样，有数值证据。SageMath 计算表明，对于 $\ell = 1$, 2，……，10，在大于 7 的前 1000 个素数中，$c_1(w^{(\ell)}, w^{(\ell)}) \neq c_2(w^{(\ell)}, w^{(\ell)})$。

一旦知道某个 $w^{(\ell)}$ 满足定理 2.8对于所有素数 $p \geq 5$的假设，就可以通过遵循 [1]中证明的相应部分，将结果推广到所有$\mathbb{Z}/m\mathbb{Z}$, $m \geq 4$ ($m \geq 5$ 仅对 $\ell = 1$ 而言）。这需要找到在 $m = 4$，6，9（$m = 6$，8，9 对于 $\ell = 1$）时不满足对偶性的线性码示例。

最后，我们以一个猜想作结。

猜想 9.5。幂权重 $w^{(\ell)}$, $\ell \geq 2$ 在任何 $\mathbb{Z}/m\mathbb{Z}$, $m \geq 4$ 上都不保持对偶性。

References

[1] N. Abdelghany 和 J. A. WOOD, 《整数剩余类环》上的李重量枚举式的麦克威廉姆斯恒等式失效, 《离散数学》343（2020）, 第 11 期, 112036, 12 页。MR 4119402[2] E. F. Assmus, Jr. 和 H. F. Mattson, Jr., 《纠错码：公理化方法》, 《信息与控制》6（1963）, 315–330。MR 0178997（31 #3251）[3] I. Constantinescu、W. Heise 和 T. Honold, 《有限环》上码之间等距映射的单项式扩张, 《第五届代数与组合编码理论国际研讨会》（ACCT '96）（保加利亚索佐波尔）, Unicorn, 舒门, 1996, 第 98–104 页。[4] P. Delsarte, 《编码理论关联方案的代数方法》, 《飞利浦研究报告增刊》（1973）, 第 10 期, vi+97。MR 384310[5]S. T. Dougherty 和 M. M. Skriganov, 麦克威廉斯对偶与 Rosenbloom-Tsfasman度量, 《莫斯科数学杂志》2（2002）, 第 1 期, 81–97, 199。MR 1900585[6] S. Dyshko, 《整数剩余类环上李重量码与欧几里得重量码的扩张定理》, 《设计、码与密码学》87（2019）, 第 6 期, 1253–1269。MR 3947347[7] S. Dyshko、Ph. Langevin 和 J. A. WOOD, 《Maillet 行列式的两个类比》, 《巴黎科学院数学报告》354（2016）, 第 7 期, 649–652。[8]H. Gluesing-Luerssen, 《加法码的傅里叶自反划分与麦克威廉姆斯恒等式》, 《设计、码与密码学》75（2015）, 第 3 期, 543–563。MR 3336966[9] M. Greferath 和 S. E. Schmidt, 《有限环组合学与麦克威廉斯等价定理》, 《组合理论杂志》A辑92（2000）, 第 1 期, 17–28。MR 1783936（2001j:94045）[10] A. R. Hammons, Jr.、P. V. Kumar、A. R. Calderbank、N. J. A. Sloane 和 P. Sol´e, Kerdock、Preparata、Goethals 及相关码的 $\mathbb{Z}_4$-线性, 《IEEE信息论汇刊》40（1994）, 第 2 期, 301–319。MR 1294046（95k:94030）[11] W. Heise 和 T. Honold, 《有限环上的齐次权与均衡权》, 《第七届代数与组合编码理论国际研讨会》（ACCT-2000）（保加利亚班斯科）, 2000, 第 183–188 页。[12]F. J. MacWilliams, 《初等阿贝尔群的组合问题》, ProQuest LLC, 密歇根州安娜堡, 1962, 博士学位论文——拉德克利夫学院。MR 2939359[13] , 《系统码中权的分布定理》, 《贝尔系统技术杂志》42（1963）, 79–94。MR 0149978（26 #7462）[14] D. Slepian, 《一类二元信号字母表》, 《贝尔系统技术杂志》35（1956）, 203–234。[15] Sage开发团队, SageMath, Sage数学软件系统（版本 9.5）, 2022, https://www.sagemath.org。[16] J. A. WOOD, 《有限环上模的对偶性及其在编码理论中的应用》, 《美国数学杂志》121（1999）, 第 3 期, 555–575。MR 1738408[17] , 《有限模上线性码的基础：扩张定理与麦克威廉姆斯恒等式》, 《环上的码》（安卡拉, 2008）（P. Sol´e 编）, 编码理论与密码学丛书, 第 6 卷, 世界科学出版社, 新泽西州哈肯萨克, 2009, 第 124–190 页。MR 2850303

[18] ———,整数剩余类环上的齐次重量枚举式与麦克威廉姆斯恒等式失效，《阿根廷数学联合会杂志》**64 (2023)**，第 2 期，333–353 页。[19] ，具有最大对称性的重量与麦克威廉姆斯恒等式失效，《代数结构与应用》，《当代数学》，第 826 卷，美国数学会，[普罗维登斯], 罗得岛州，[2025] ©2025年，361–430 页。MR 4963840

Western Michigan University电子
邮件地址：jay.wood@wmich.edu