

## VI-2 类 5 维 $q$ 元线性码的汉明重量谱的确定

胡国香<sup>1,2</sup>, 张焕国<sup>1</sup>

(1. 武汉大学计算机学院, 湖北 武汉 430072; 2. 中南民族大学数学与统计学学院, 湖北 武汉 430074)

**摘要:**  $\text{GF}(q)$  上  $[n, k; q]$  线性码  $c$  的汉明重量谱为序列  $(d_1, d_2, \dots, d_k)$ , 其中  $d_r$  是  $c$  的  $r$  维子码的最小支撑重量。第 VI 类 5 维  $q$  元线性码的汉明重量谱, 按照新的必要条件可以分成 6 个子类。运用有限射影几何方法研究 VI-2 类的 5 维  $q$  元线性码的汉明重量谱, 确定 VI-2 类 5 维  $q$  元线性码的几乎所有汉明重量谱。

**关键词:** 汉明重量; 线性码; 差序列; 射影几何

中图分类号: TN 911.2

文献标识码: A

## VI-2 class of Hamming weight of $q$ -ary linear codes with dimension 5

HU Guo-xiang<sup>1,2</sup>, ZHANG Huan-guo<sup>1</sup>

(1. School of Computer, Wuhan University, Wuhan 430072, China;

2. School of Mathematics and Statistics, South-Central University for Nationalities, Wuhan 430074, China)

**Abstract:** The Hamming weight hierarchy of a linear  $[n, k; q]$  code  $c$  over  $\text{GF}(q)$  is the sequence  $(d_1, d_2, \dots, d_k)$ , where  $d_r$  is the smallest support weight of an  $r$ -dimensional subcode of  $c$ . According to some new necessary conditions, the VI class Hamming weight hierarchies of  $q$ -ary linear codes of dimension 5 can be divided into six subclasses. By using the finite projective geometry method, VI-2 subclass and determine were researched almost all weight hierarchies of the VI-2 subclass of weight hierarchies of  $q$ -ary linear codes with dimension 5.

**Key words:** Hamming weight, linear codes, difference sequence, projective geometry

### 1 引言

通信系统中信息的传递离不开编码, 而汉明重量是编码理论中非常重要的基本概念, 与编码中码的检错以及纠错能力息息相关。编码理论的创始人之一汉明 (Hamming) 提出了汉明重量。广义汉明重量最初是由用于第 2 类窃密信道的线性编码方案所触动而提出的。假设发送者有  $k$  bit 信息被编成  $n$  bit 码后通过此信道传送给接收者。入侵者能够从信道码中随意窃取到其中的  $s$  bit 数据。传送的信道假设是无噪的, 因而正确

译码没有问题。问题的焦点是如何阻止入侵者获太多的信息, 也就是设计出一种编码方案, 使入侵者截取  $s$  bit 数据时, 对于数据的可疑度(不确定度)尽可能得大。事实上, 当一种线性码用于上述信道时, 广义汉明重量可以完全表现出该码的特性。线性码的广义汉明重量谱是 Wei<sup>[1]</sup>首次正式提出的, 广义汉明重量是码的最小距离的推广。线性码是编码理论中一类非常重要的码, 很多其他形式的码都可以和线性码找到一定的联系。汉明重量的另一种形式被 Forney 称作长度/维数轮廓, 在线性码的格子复杂度分析<sup>[2~6]</sup>、译

收稿日期: 2015-02-02; 修回日期: 2015-04-20

基金项目: 国家自然科学基金资助项目 (No.61303212, No.61170080, No.61332019, No.U1135004); 湖北省自然科学基金资助项目 (No.2014CBF440)

**Foundation Items:** The National Natural Science Foundation of China (No.61303212, No.61170080, No.61332019, No.U1135004), The Natural Science Foundation of Hubei Province (No.2014CBF440)

码分析<sup>[7~9]</sup>、检错分析<sup>[10]</sup>等方面都有非常重要的应用,文献[11]也详细讨论了其应用。重量谱的概念由 Wei 提出以后,立即成为编码理论的一个前沿研究热点。

### 1.1 基础知识

对于一个码  $D$ ,  $D$  中的所有码字的非零位置的全体所构成的集合称为  $D$  的支撑集,记为  $c(D)$ ,即  $c(D) = \bigcup_{c \in D} \{i | c_i \neq 0, c = (c_1, c_2, \dots, c_n)\}$ ,支撑集的大小记为  $w_s(D) = |c(D)|$ 。

对于一个参数为  $[n, k; q]$  的码  $C$  (即  $GF(q)$  上码长为  $n$  的  $k$  维码),当  $1 \leq r \leq k$  时,  $r$  阶广义汉明重量 (或最小支撑重量) 定义为  $d_r(C) = \min\{w_s(D) | D \text{ 是 } C \text{ 的 } r \text{ 维子码}\}$ ,特别  $d_1(C)$  即为通常意义下码  $C$  的最小距离,序列  $(d_1, d_2, d_3, d_4, d_5)$  称为广义汉明重量,也简称为汉明重量谱。

“如何确定线性码的汉明重量谱”一直是编码理论研究的核心问题。关于汉明重量谱的研究,第 1 个研究方向是关于具体的各类线性纠错码的。由于确定  $d_1$  是编码理论中尚未完全解决的难题,因此  $d_r$  的确定更加困难,目前仅有少数的几类码确定了重量谱。文献[12]确定了 RM 码、汉明码及其补码、扩展汉明码、极大距离可分码等的重量谱;文献[13~15]对广义汉明重量的上下限进行了研究;文献[16,17]中,重量谱的类别被扩展到线性等重码。第 2 个方向是关于一般线性码的。对于一般线性码的重量谱,传统的研究方法有组合方法与计算机搜索。但是随着线性码维数的增加,重量谱的类别也呈指数增加,对于高维数线性码重量谱的研究更加困难,这 2 种方法均不太适用。目前来看,有限射影几何方法对于高维数线性码重量谱的研究较为适用。

### 1.2 相关工作

1992 年,密码学家 Helleseth<sup>[18]</sup>提出了确定一般线性码的所有可能的汉明重量谱,这也是编码理论中一个非常有意义的理论问题。1996 年,陈文德等<sup>[19]</sup>提出了有限射影几何方法,并第一次有效地用于确定 4 维  $q$  元线性码的汉明重量谱。他们还把 4 维  $q$  元线性码及其汉明重量谱分成了 9 类,用有限射影几何方法取得了丰富的分类研究成果,参见文献[20,21]等。文献[22]对 4 维  $q$  元线性码的汉明重量谱进行研究,确定 4 维  $q$  元线性码的几乎所有的汉明重量谱。文献[23]中把 5 维  $q$  元线性码及其汉明重量谱分成 6 类,

并对 6 类码中的 II-1 类进行了研究,文献[24]对 II-2 类进行了研究。文献[25]确定了 5 维  $q$  元线性码 V-1 类的几乎所有的汉明重量谱。文献[26]确定了 5 维  $q$  元线性码 V-2 类的几乎所有的汉明重量谱。在文献[27]中第 VI 类 5 维  $q$  元线性码的汉明重量谱又被分成了 6 个子类,并对其中的 VI-1 类进行研究,确定该类的几乎所有的汉明重量谱。本文将对文献[27]中的 VI-2 子类进行研究,并确定其几乎所有的汉明重量谱。

本文主要研究了文献[27]中 5 维  $q$  元线性码的第 VI-2 类的汉明重量谱。利用有限射影几何方法,通过往 4 维空间进行投影,把重量谱的确定转化为 4 维空间中的点、线、面、体的赋值函数的确定问题,使确定重量谱这一抽象的理论问题变得更为形象化。

## 2 预备知识

在本文中,  $C$  表示  $[n, 5; q]$  线性码,即  $GF(q)$  上的码长为  $n$  的 5 维  $q$  元线性码,差序列  $(d_1, d_2, d_3, d_4, d_5)$  称为码  $C$  的汉明重量谱。

一个码  $C$  对应于一个差序列  $(d_1, d_2, d_3, d_4, d_5)$ ,所有的线性码  $C$  确定了一个序列集,本文的目标是确定这类序列集中几乎所有的序列。

如果对参数为  $[n, 5; q]$  的码  $C$  添加一个零列,得到参数为  $[n+1, 5; q]$  的码  $C' = \{(c | 0) | c \in C\}$ 。码  $C$  与  $C'$  具有相同的汉明重量谱,因此不失一般性,可假设  $n = d_5$ 。

令  $i_0 = d_5 - d_4, i_1 = d_4 - d_3, i_2 = d_3 - d_2, i_3 = d_2 - d_1, i_4 = d_1$ , 则序列  $(i_0, i_1, i_2, i_3, i_4)$  称为  $[d_4, 5; q]$  码的差序列 (简称 DS)。显然,DS 和汉明重量谱之间可以相互转化。因此“确定汉明重量谱”可归结为“确定差序列”。由文献[1]可知,对所有的  $r$ , 均有  $i_r \geq 1$ 。

令  $G$  为码  $C$  的生成矩阵,对  $\forall x \in GF(q)^5$ , 用  $m(x)$  表示  $x$  在矩阵  $G$  的列中所出现的次数。如果  $x = ay$  (其中  $y$  为  $G$  中的列,  $a \in GF(q)$  且  $a \neq 0$ ), 则可用  $x$  代替  $y$  且不改任一子码的支撑重量,因此可以用射影空间  $PG(4, q)$  中的点来描述  $G$  中的列。用  $V_4$  来表示射影空间  $PG(4, q)$ , 赋值函数为  $m: V_4 \rightarrow N, N = \{0, 1, 2, \dots\}$ 。对  $\forall p \in V_4$ , 称  $m(p)$  为  $p$  的值 (或者重量)。对  $\forall S \in V_4$ , 定义  $S$  的值为  $m(S) = \sum_{p \in S} m(p)$ 。文献[4]中证明了汉明重量谱为

$(d_1, d_2, d_3, d_4, d_5)$  码的存在性等价于满足下面条件式 (1) 的赋值函数  $m$  的存在性

$$\begin{aligned} & \max\{m(U_r) | U_r \text{ 是 } V_4 \text{ 中的 } r \text{ 维子空间}\} \\ & = \sum_{j=0}^r i_j, 0 \leq r \leq 4 \end{aligned} \quad (1)$$

用  $p^*, l^*, P^*, V^*$  分别表示  $r = 0, 1, 2, 3$  时, 赋值函数取式(1)右侧最大值的最重点、最重线、最重面、最重体。确定码的几乎所有可能的汉明重量谱的有限射影几何方法的核心是: 先用几何方法得到差序列的最紧并且最好的必要条件, 再对满足这一必要条件的几乎所有的  $i_j$  构造出满足式(1)并且尽量均匀的赋值函数  $m$ 。

定义 1 以符号  $N(i)$  表示  $i_0 = i$  时某一类差序列的数目, 以符号  $M(i)$  表示  $i_0 = i$  时这类差序列的必要条件中所含序列的数目, 若  $\lim_{i \rightarrow \infty} \frac{N(i)}{M(i)} = 1$ , 则称此必要条件是几乎充分的。

### 3 主要结果

文献[27]中把 5 维  $q$  元线性码的第 VI 类的差序列的必要条件分成 6 个子类, 并对其中的 VI-1 类进行了研究, 其他 5 个子类的重量谱均未确定。相比 VI-1 类来说, VI-2 重量谱的确定更为困难, 因为当  $i_1$  取得上界时, 赋值函数的取值不完全为  $i_0$  的整数倍, 需要考虑将  $i_0$  进行分数化处理。

本文研究这 6 类中的 VI-2 个子类。由文献[27]可得 VI-2 类差序列的必要条件如下。

定理 1 对于 5 维  $q$  元线性码,  $(i_0, i_1, i_2, i_3, i_4)$  是满足 VI-2 类差序列的必要条件

$$\begin{cases} \frac{i_0}{q} < i_1 < i_0 \\ qi_1 < i_2 < qi_0 \\ qi_2 < i_3 < \frac{q^2}{q+1}(i_0 + i_2) \\ i_0 < i_4 < (q^3 + q^2 + q)i_1 - i_2 - i_3 \end{cases}$$

下面将构造出 VI-2 类的几乎所有可能的汉明重量谱, 即证明上述必要条件是几乎充分的, 以下的引理 1 ~ 引理 4 将给出各种条件下的详细证明与赋值函数的构造。

引理 1 设

$$i_1 = i_0 - 2 \quad (2)$$

$$i_2 = qi_1 + q - 1 \quad (3)$$

$$i_3 = qi_2 + q \quad (4)$$

$$i_4 = (q^3 + q^2 + q)i_1 - i_2 - i_3 - (q^3 + q^2 + q) \quad (5)$$

这里  $i_1, i_4$  取的上界,  $i_2, i_3$  取的下界, 则满足条件式(2)~(5)的序列  $(i_0, i_1, i_2, i_3, i_4)$  是差序列。

证明 把式(2)~(5)代入后, 得

$$m(l^*) = i_0 + i_1 = 2i_0 - 2$$

$$\begin{aligned} m(P^*) &= i_0 + i_1 + i_2 \\ &= i_0 - 2 + (q+1)(i_1 + 1) \end{aligned}$$

$$\begin{aligned} m(V^*) &= i_0 + i_1 + i_2 + i_3 \\ &= i_0 - 2 + (q^2 + q + 1)(i_1 + 1) \end{aligned}$$

$$m(V_4) = i_0 + i_1 + (q^3 + q^2 + q)i_1$$

设  $PG(4, q)$  表示以不在一个体内的 5 个点  $e_1, e_2, e_3, e_4, e_5$  做顶点的 4 维多面体, 如图 1 所示。用符号  $\langle x_1, x_2, \dots, x_t \rangle$  表示由点  $x_1, x_2, \dots, x_t$  生成的  $t-1$  维子空间。

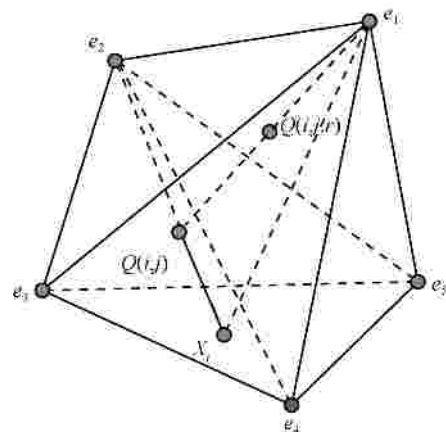


图 1 边界结构

定义下面这些符号为

$$\langle e_3, e_4, e_5 \rangle = \{X_i | 0 < i < q^2 + q + 1\}$$

$$\frac{\langle e_2, X_i \rangle}{\{e_2\}} = \{Q(i, j) | 0 < j < q\} \text{ (自 } e_2 \text{ 开始的点)}$$

$$\frac{\langle e_1, Q(i, j) \rangle}{\{e_1\}} = \{Q(i, j, r) | 0 < r < q\} \text{ (自 } e_1 \text{ 开始的点)}$$

构造赋值函数  $m(\cdot)$  如下

$$m(x) = \begin{cases} i_0, & x = e_1 \\ i_0 - 2, & x = e_2 \\ 0, & x \in \frac{\langle e_1, e_2 \rangle}{\{e_1, e_2\}} \\ x = Q(i, j, r) (0 < i < q^2 + q + 1) \\ \left[ \frac{i_0 - 3}{q} \right] + 1, & \begin{cases} 0 < j < i_0 - 1 - q \left[ \frac{i_0 - 3}{q} \right], \\ q - (i_0 - 3 - q \left[ \frac{i_0 - 3}{q} \right]) < r < q \\ i_0 - 1 - q \left[ \frac{i_0 - 3}{q} \right] < j < q, \\ 0 < r < i_0 - 3 - q \left[ \frac{i_0 - 3}{q} \right] \end{cases} \\ \left[ \frac{i_0 - 3}{q} \right], & \begin{cases} x = Q(i, j, r) \\ \begin{cases} i_0 - 1 - q \left[ \frac{i_0 - 3}{q} \right] < j < q, \\ i_0 - 3 - q \left[ \frac{i_0 - 3}{q} \right] < r < q \\ 0 < j < i_0 - 1 - q \left[ \frac{i_0 - 3}{q} \right], \\ 0 < r < q - (i_0 - 3 - q \left[ \frac{i_0 - 3}{q} \right]) \end{cases} \end{cases} \end{cases}$$

点、线、面、体之间的关系说明如下。

1) 由上述赋值函数的构造可得， $e_1$  为最重点， $\langle e_1, e_2 \rangle$  为最重线， $\langle e_3, e_4, e_5 \rangle$  为最重面， $\langle e_2, e_3, e_4, e_5 \rangle$  为最重体。

可以证明过  $e_1$  点的线除  $\langle e_1, e_2 \rangle$  外，其余每一条线  $l$  的值均为  $i_0 + i_1 - 1$ 。

体  $\langle e_2, e_3, e_4, e_5 \rangle$  内过  $e_2$  点的线的值均为  $i_0 + i_1 - 1 = i_0 - 2 + (i_1 + 1)$ 。

体  $\langle e_2, e_3, e_4, e_5 \rangle$  内赋值最大的线即为过点  $e_2$  的线，最大的面即为过  $e_2$  的面，且体  $\langle e_2, e_3, e_4, e_5 \rangle$  内过  $e_2$  点的每一个面均为最重面。过  $e_1$  点的面当中值最大的为过线  $\langle e_1, e_2 \rangle$  的面  $P$ ，且

$$\begin{aligned} m(P) &= i_0 + i_1 + q(i_1 - 1) \\ &= i_0 + i_1 + i_2 - 2q + 1 < m(P^*) \end{aligned}$$

所以， $P^* \notin P^*$ 。

过线  $\langle e_1, e_2 \rangle$  的体  $V$  的值为

$$\begin{aligned} m(V) &= i_0 + i_1 + (q^2 + q)(i_1 - 1) \\ &= i_0 + i_1 + i_2 + i_3 - (2q^2 + 2q - 1) < m(V^*) \end{aligned}$$

所以  $V^* \notin V^*$ 。因此上述构造的边界结构满足式

(1) 并且符合 VI 类的必要条件，即  $P^* \notin P^*$ ， $V^* \notin V^*$  且  $P^* \notin V^*$ 。

为了从上述边界结构得到一般结构，首先用体集降  $i_1$  到下界附近，而保持其他  $i_j$  仍为边界值（引理 2）；然后将  $i_2$  上升到上界附近，而保持  $i_3, i_4$  仍为边界值（引理 3）；再将  $i_3$  上升到上界附近，而保持  $i_4$  仍为边界值（引理 4）；最后将  $i_4$  下降到下界附近。

引理 2 对任意满足条件式(3)~式(5)的序列  $(i_0, i_1, i_2, i_3, i_4)$ ，如果

$$\frac{i_0}{q} + h_1(q) \leq i_1 \leq i_0 - 2 \quad (6)$$

其中， $h_1(q) = q^6(q^2 - 1)$ ，则  $(i_0, i_1, i_2, i_3, i_4)$  是差序列。

证明 定义以下一些符号（如图 2 所示）。

记  $l_m$  ( $0 < m < q + 1$ ) 为  $\langle e_2, e_3, e_4 \rangle$  内过  $e_2$  点的线

$$\begin{aligned} \frac{\langle e_2, e_3, e_4 \rangle}{\{e_2\}} &= \{C_k \mid 0 < k < q^2 + q\} \\ \frac{\langle e_2, e_3, e_4, e_5 \rangle}{\langle e_2, e_3, e_4 \rangle} &= \{B_j \mid 0 < j < q^3\} \\ \frac{V_4}{\langle e_1, e_2 \rangle, \langle e_2, e_3, e_4, e_5 \rangle} &= \{A_i \mid 0 < i < q^4 - q\} \end{aligned}$$

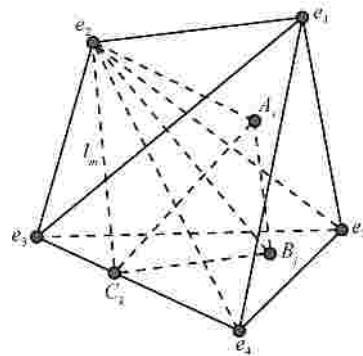


图 2  $i_1$  下降结构

构造赋值函数  $m'(\cdot)$  如下

$$m'(x) = \begin{cases} i_0, & x = e_1 \\ m(x) - 1, & x \in \langle l_m, B_j, A_i \rangle \text{ 且} \\ & A_i \notin \langle e_1, B_j, l_m \rangle \\ m(x), & \text{其他} \end{cases}$$

当取遍满足条件的所有的体  $\langle l_m, B_j, A_i \rangle$  时，称  $i_1$  下降一圈或  $i_1$  循环一次。 $i_1$  每循环一次， $i_1$  的值下降  $(q+1)q^3(q^4 - q^3) = q^6(q^2 - 1)$ 。

$\frac{\langle e_2, e_3, e_4 \rangle}{\{e_2\}}$  中每个点的值均下降  $q^6(q - 1)$ ，每个

点  $B_j$  的值下降  $q^5(q^2-1)$ ,  $\frac{\langle e_1, e_2, e_3, e_4 \rangle}{\{\langle e_1, e_2 \rangle, \langle e_2, e_3, e_4 \rangle\}}$  中每个

点  $A_i$  的值下降  $q^7$ ,  $\frac{\langle e_1, B_j \rangle}{\{e_1, B_j\}}$  中每个点的值下降

$q^5(q^2-1)$ 。

假设最多循环  $w_1$  次, 因为点的值下降但始终非

负, 所以  $\left\lfloor \frac{i_0-3}{q} \right\rfloor - w_1 q^7 \geq 0$ , 即  $w_1 \leq \frac{\left\lfloor \frac{i_0-3}{q} \right\rfloor}{q^7}$ , 而

此时  $i_1 = i_0 - 2 - w_1 q^6(q^2-1) > \frac{i_0}{q}$ 。

所以可令

$i_1 - w_1 q^6(q^2-1) = i_0 - 2 - w_1 q^6(q^2-1) - \frac{i_0}{q}$ , 故

$$w_1 = \frac{(q-1)i_0 - 2q}{q^7(q^2-1)}$$

取  $w_1 = \left\lfloor \frac{(q-1)i_0 - 2q}{q^7(q^2-1)} \right\rfloor$ , 则  $i_1$  可下降至

$$\begin{aligned} i_1 &= i_0 - 2 - w_1 q^6(q^2-1) \\ &< i_0 - 2 - q^6(q^2-1) \left( \frac{(q-1)i_0 - 2q}{q^7(q^2-1)} - 1 \right) \\ &= \frac{i_0}{q} + h_1(q) \end{aligned}$$

所以取  $w_1 = \left\lfloor \frac{(q-1)i_0 - 2q}{q^7(q^2-1)} \right\rfloor$ ,  $i_1$  可下降至下界附近, 而每个点的值均大于 0, 为后面  $i_2$  及  $i_3$  的上升做准备。

引理 3 对任意满足条件式(4)~式(6)的序列  $(i_0, i_1, i_2, i_3, i_4)$ , 如果

$$qi_1 + q - 1 = i_2 = qi_0 - h_2(q) \quad (7)$$

其中,  $h_2(q) = q^4(q^2-1) + q + 1$ , 则  $(i_0, i_1, i_2, i_3, i_4)$  是差序列。

证明 先定义以下一些符号(如图 3 所示)。

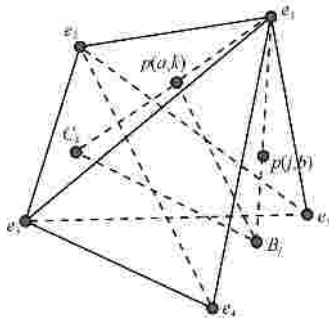


图 3  $i_2$  上升结构

$$\frac{\langle e_1, C_k \rangle}{\{e_1, C_k\}} = \{p(k, a) \mid 0 < a < q-1\}$$

$$\frac{\langle e_1, B_j \rangle}{\{e_1, B_j\}} = \{p(j, b) \mid 0 < b < q-1\}$$

构造赋值函数  $m''(\cdot)$  如下

$$m''(x) = \begin{cases} i_0, x = e_1 \\ m'(x) + 1, x \in \langle C_k, B_j \rangle \\ m'(x) - 1, x \in \langle B_j, p(a, k) \rangle, x = p(j, b) \\ m'(x), \text{其他} \end{cases}$$

取遍满足条件的所有的线与点时, 称  $i_2$  上升一圈,  $i_2$  每上升 1 圈,  $i_2$  的值上升  $q^4(q^2-1)$ ;

$\langle e_2, e_3, e_4 \rangle$  中每个点  $C_k$  的值上升  $q^3(q-1)$ ; 每个点  $\{e_2\}$

$B_j$  的值上升  $q^2(q^2-1)$ ; 线  $\langle e_1, e_2 \rangle$  上每个点的值

不变;  $\langle e_1, e_2, e_3, e_4 \rangle$  中的每个点的值均下降  $q^3$ , 其余  $q^4 - q^3$  个点的值均下降  $q^2(q+1)$ 。

假设最多循环  $w_2$  次。

1) 由点的非负性, 可得

$$\left\lfloor \frac{i_0-3}{q} \right\rfloor - w_1 q^7 - w_2 q^3 \geq 0$$

$$\text{所以, } w_2 \leq \frac{\left\lfloor \frac{i_0-3}{q} \right\rfloor - w_1 q^4}{q^3}$$

又由

$$\left\lfloor \frac{i_0-3}{q} \right\rfloor - w_1 q^5(q^2-1) - w_2 q^2(q+1) \geq 0$$

$$\text{所以, } w_2 \leq \frac{\left\lfloor \frac{i_0-3}{q} \right\rfloor - w_1 q^3(q-1)}{q^2(q+1)}$$

2) 由  $t^* \notin V^*$  可得

$$\begin{aligned} 2i_0 - 3 - w_1 q^6(q^2-1) - qq^6(q-1)w_1 + w_2 qq^3(q-1) \\ > 2i_0 - 3 - w_1 q^6(q^2-1) \end{aligned}$$

所以,  $w_2 > q^3 w_1$ 。

又由

$$\begin{aligned} 2i_0 - 3 - w_1 q^6(q^2-1) - qq^5(q^2-1)w_1 + w_2 qq^2(q^2-1) \\ > 2i_0 - 3 - w_1 q^6(q^2-1) \end{aligned}$$

所以,  $w_2 > q^3 w_1$ 。

又由

$$\frac{i_0 - 2}{q}(q + 1) - (q + 1)w_1q^6(q - 1) + (q + 1)w_2q^3(q - 1) = 2i_0 - 3 - w_1q^6(q^2 - 1)$$

所以,  $w_2 = \frac{i_0 - 2}{q^4(q + 1)}$ 。

又由

$$\frac{i_0 - 2}{q}(q + 1) - w_1q^6(q - 1) - qw_1q^5(q^2 - 1) + w_2q^3(q - 1) + qw_2q^2(q^2 - 1) = 2i_0 - 3 - w_1q^6(q^2 - 1)$$

所以,  $w_2 = \frac{i_0 - 2}{q^4(q + 2)} + \frac{q^3}{q + 2}w_1$ 。

3) 由面之间的关系可得

$$i_0 + i_1 + i_2 - w_1q^6(q^2 - 1) - qq^6(q - 1)w_1 - q^2q^5(q^2 - 1)w_1 + w_2qq^3(q - 1) + w_2q^2q^2(q^2 - 1)$$

$$= i_0 + i_1 + i_2 - w_1q^6(q^2 - 1) + q^4(q^2 - 1)w_2$$

所以,  $w_2 = q^3(q + 2)w_1$ 。

又由

$$\frac{i_0 - 2}{q}(q^2 + q + 1) - (q + 1)q^6(q - 1)w_1 - q^2q^5(q^2 - 1)w_1 + (q + 1)q^3(q - 1)w_2 + q^2q^2(q^2 - 1)w_2$$

$$= i_0 + (q + 1)[i_0 - 2 - q^6(q^2 - 1)w_1] + q^4(q^2 - 1)w_2$$

所以,  $w_2 = \frac{i_0}{q^4(q + 1)}$ 。

由  $w_1$  的范围可知,  $q^3w_1$  最小。

由  $i_1 = i_0 - 2 - q^6(q^2 - 1)w_1$  可得,  $w_1 = \frac{i_0 - 2 - i_1}{q^6(q^2 - 1)}$ , 所以,  $q^3w_1 = \frac{i_0 - 2 - i_1}{q^3(q^2 - 1)}$ 。

取  $w_2 = \left\lfloor \frac{i_0 - 2 - i_1}{q^3(q^2 - 1)} \right\rfloor$ 。

下面证明  $i_2$  可上升至上界

$$\begin{aligned} i_2 &= qi_1 + q - 1 + w_2q^4(q^2 - 1) \\ &= qi_1 + q - 1 + q^4(q^2 - 1) \left\lfloor \frac{i_0 - 2 - i_1}{q^3(q^2 - 1)} \right\rfloor \\ &> qi_1 + q - 1 + q^4(q^2 - 1) \left( \frac{i_0 - 2 - i_1}{q^3(q^2 - 1)} - 1 \right) \\ &= qi_0 - h_2(q) \end{aligned}$$

所以, 当  $w_2 = \left\lfloor \frac{i_0 - 2 - i_1}{q^3(q^2 - 1)} \right\rfloor$  时,  $i_2$  可上升到上界

附近。

引理 4 对任意满足条件式(5) ~ 式(7)的序列  $(i_0, i_1, i_2, i_3, i_4)$ , 如果

$$qi_2 + q - i_3 = \frac{q^3}{q^2 + q + 1}(i_0 + i_1 + i_2) - h_3(q) \quad (8)$$

其中,  $h_3(q) = q^3(q - 1)$ , 则  $(i_0, i_1, i_2, i_3, i_4)$  是差序列。

证明 如图 4 所示, 构造赋值函数  $m''(\cdot)$  如下

$$m''(x) = \begin{cases} i_0, & x = e_1 \\ m''(x) + 1, & x = B_j \\ m''(x) - 1, & x = p(j, b) \\ m''(x), & \text{其他} \end{cases}$$

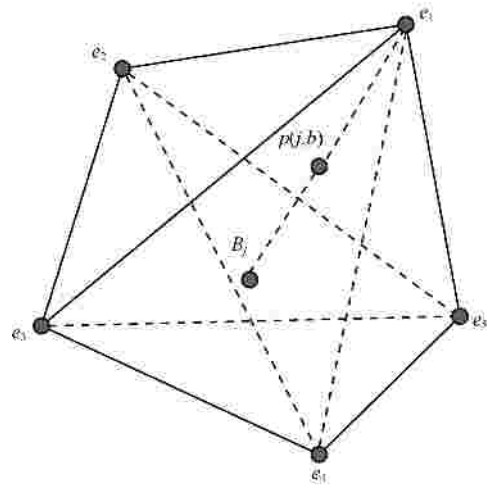


图 4  $i_3$  上升结构

当取遍满足条件的所有的点  $B_j$  与  $p(j, b)$  时, 称  $i_3$  上升 1 圈,  $i_3$  每上升 1 圈,  $i_3$  的值上升  $q^3(q - 1)$ ; 每个点  $B_j$  的值上升  $q - 1$ ;  $\frac{\langle e_1, B_j \rangle}{\{e_1, B_j\}}$  中每个点的值下降 1。假设最多循环  $w_3$  次。

1) 由点的非负性, 可得

$$\left\lfloor \frac{i_0 - 3}{q} \right\rfloor - w_1q^5(q^2 - 1) - w_2q^2(q + 1) - w_3 = 0$$

所以,  $w_3 = \left\lfloor \frac{i_0 - 3}{q} \right\rfloor - q^5(q^2 - 1)w_1 - q^2(q + 1)w_2$ 。

2) 由  $l^* \in V^*$  可得

$$\begin{aligned} 2i_0 - 3 - w_1q^6(q^2 - 1) - qq^5(q^2 - 1)w_1 + qq^2(q^2 - 1)w_2 + q(q - 1)w_3 \\ = 2i_0 - 3 - w_1q^6(q^2 - 1) \end{aligned}$$

所以,  $w_3 = q^5(q + 1)w_1 - q^2(q + 1)w_2$ 。

又由

$$\frac{i_0 - 3}{q}(q + 1) - w_1 q^6 (q - 1) - q q^5 (q^2 - 1) w_1 + q^3 (q - 1) w_2 + q q^2 (q^2 - 1) w_2 + q (q - 1) w_3$$

$$2i_0 - 3 - w_1 q^6 (q^2 - 1)$$

所以,  $w_3 = \frac{i_0 - 3}{q^2} + q^5 w_1 - q^2 (q + 2) w_2$ 。

3) 由面之间的关系, 可得

$$i_0 + i_1 + i_2 - q w_1 q^6 (q - 1) - w_1 q^6 (q^2 - 1) - q^2 w_1 q^5 (q^2 - 1) + q w_2 q^3 (q - 1) + q^2 w_2 q^2 (q^2 - 1) + q^2 (q - 1) w_3$$

$$i_0 + i_1 + i_2 - (q + 1) w_1 q^6 (q^2 - 1) + q^4 (q^2 - 1) w_2$$

所以,  $w_3 = q^5 w_1 - q^2 w_2$ 。

又由

$$(q^2 + q + 1) \frac{i_0 - 3}{q} - (q + 1) w_1 q^6 (q - 1) - q^2 w_1 q^5 (q^2 - 1) +$$

$$(q + 1) w_2 q^3 (q - 1) + q^2 w_2 q^2 (q^2 - 1) + q^2 (q - 1) w_3$$

$$i_0 + i_1 + i_2$$

所以,  $w_3 = \frac{i_0 - 2}{q^3} - q (q + 1) w_2$ 。

由  $w_1, w_2$  的范围, 易知  $q^5 w_1 - q^2 w_2$  最小。所以, 取  $w_3 = q^5 w_1 - q^2 w_2$ , 此时  $p^* \notin P^*, l^* \notin V^*$ 。

由  $i_1 = i_0 - 2 - q^6 (q^2 - 1) w_1$  可得:  $w_1 = \frac{i_0 - 2 - i_1}{q^6 (q^2 - 1)}$ ;

由  $i_2 = q i_1 + q - 1 + q^4 (q^2 - 1) w_2$  可得:  $w_2 = \frac{i_2 - q i_1 - q + 1}{q^4 (q^2 - 1)}$ 。

所以,

$$q^5 w_1 - q^2 w_2 = q^5 \frac{i_0 - 2 - i_1}{q^6 (q^2 - 1)} - q^2 \frac{i_2 - q i_1 - q + 1}{q^4 (q^2 - 1)}$$

$$= \frac{q i_0 - i_2 - q - 1}{q^2 (q^2 - 1)}$$

取  $w_3 = \left\lfloor \frac{q i_0 - i_2 - q - 1}{q^2 (q^2 - 1)} \right\rfloor$ 。

下面证明  $i_3$  可上升至上界

$$i_3 = q i_2 + q + w_3 q^3 (q - 1)$$

$$= q i_2 + q + q^3 (q - 1) \left\lfloor \frac{q i_0 - i_2 - q - 1}{q^2 (q^2 - 1)} \right\rfloor$$

$$> q i_2 + q + q^3 (q - 1) \left( \frac{q i_0 - i_2 - q - 1}{q^2 (q^2 - 1)} - 1 \right)$$

$$= \frac{q^2}{q + 1} (i_0 + i_2) - h_3 (q)$$

所以, 当  $w_3 = \left\lfloor \frac{q i_0 - i_2 - q - 1}{q^2 (q^2 - 1)} \right\rfloor$  时,  $i_3$  可上升到

上界附近。

$i_4$  从上界可以一直往下降, 直到  $\frac{V_4}{\{l^*, V^*\}}$  所有点

的值均降为 0, 这时  $i_4$  的下界为  $i_0$ 。

因为  $q i_1 + q - 1 \leq i_2 \leq q i_0 - h_2 (q)$ , 所以,

$$i_1 \leq i_0 - \frac{h_2 (q)}{q} - \frac{q - 1}{q} = i_0 - 2 - q^3 (q^2 - 1);$$

又由  $\frac{i_0}{q} + h_1 (q) \leq i_1 \leq i_0 - 2$ , 所以,  $\frac{i_0}{q} + h_1 (q) \leq i_1 \leq i_0 - 2 -$

$$q^3 (q^2 - 1),$$
 可得  $i_0 \leq \frac{q h_1 (q) + 2 q + q^4 (q^2 - 1)}{q - 1} = h_0 (q)$ 。

由上述引理 1 ~ 引理 4, 可得如下的定理。

定理 2 对于 5 维  $q$  元线性码,  $(i_0, i_1, i_2, i_3, i_4)$  是

满足 VI-2 类差序列的充分条件:

- 1)  $h_0 (q) \leq i_0$ ;
- 2)  $\frac{i_0}{q} + h_1 (q) \leq i_1 \leq i_0 - 2$ ;
- 3)  $q i_1 + q - 1 \leq i_2 \leq q i_0 - h_2 (q)$ ;
- 4)  $q i_2 + q \leq i_3 \leq \frac{q^2}{q + 1} (i_0 + i_2) - h_3 (q)$ ;
- 5)  $i_0 \leq i_4 \leq (q^3 + q^2 + q) i_1 - i_2 - i_3$ 。

其中,  $h_0 (q) = q^4 (q + 1) (q^3 + 1) + 2 + \frac{2}{q - 1}$ ,  $h_1 (q) =$

$q^6 (q^2 - 1)$ ,  $h_2 (q) = q^4 (q^2 - 1) + q + 1$ ,  $h_3 (q) = q^3 (q - 1)$ 。

所以, 由引理 1 ~ 引理 4, 该定理的充分性得证, 也就得到了 VI-2 类的几乎所有的差序列。

以符号  $N(i)$  表示  $i_0 \leq i$  时, VI-2 类差序列的数目, 以符号  $M(i)$  表示  $i_0 \leq i$  时, 上述定理必要条件

所含序列的数目, 经计算可得  $\lim_{i \rightarrow \infty} \frac{N(i)}{M(i)} = 1$ 。

#### 4 结束语

本文对 5 维  $q$  元线性码中的第 VI-2 类进行研究, 运用有限射影几何方法通过对射影空间中的点进行赋值, 得到不同条件下赋值函数的构造, 从而得到第 VI-2 类 5 维  $q$  元线性码的几乎所有的汉明重量谱。

#### 参考文献:

[1] WEI V K. Generalized Hamming weight for liner codes[J]. IEEE Transactions Information Theory, 1991,37(5):1412-1418.  
 [2] FORNEY G D. Dimension/length profiles and trellis complexity f

- linear block codes[J]. IEEE Transactions Information Theory, 1994, 40(6):1741-1752.
- [3] KASAMI T, TAKATA T, FUJIWARA T, et al. On the optimum bit orders with respect to the state complexity of trellis diagrams for binary linear codes[J]. IEEE Transactions Information Theory, 1993, 39(1): 242-245.
- [4] MORELOS-ZARAGOZA R, FUJIWARA T, KASAMI T, et al. Constructions of generalized concatenated codes and their trellis-based decoding complexity[J]. IEEE Transactions Information Theory, 1999, 45(2): 725-731.
- [5] SHANY V, BE'ERY Y. The preparata and goethals codes: trellis complexity and twisted squaring constructions[J]. IEEE Transactions Information Theory, 1999, 45(5): 1667-1673.
- [6] VARDY A, BE'ERY Y. Maximum-likelihood soft decision decoding of BCH codes[J]. IEEE Transactions Information Theory, 1994, 40(2): 546-554.
- [7] FOSSORIER M P C, LIN S. A unified method for evaluating the error-correction radius of reliability-based soft-decision algorithms for linear block codes[J]. IEEE Transactions Information Theory, 1998, 44(2): 691-700.
- [8] FOSSORIER M P C, LIN S, SNYDERS J. Reliability-based syndrome decoding of linear block codes[J]. IEEE Transactions Information Theory, 1998, 44(1): 388-398.
- [9] GAZELLE D, SNYDERS J. Reliability-based code-search algorithms for maximum-likelihood decoding of block codes[J]. IEEE Transactions Information Theory, 1997, 43(1):239-249.
- [10] KLØVE T. The worst-case probability of undetected error for linear codes on the local binomial channel[J]. IEEE Transactions Information Theory, 1996, 42(1): 172-179.
- [11] 岳殿武, 鄞广增. 广义 Hamming 重量, 维数/长度轮廓及其应用[J]. 电子学报, 1999, 27(4):111-115.  
YUE D W, FENG G Z. Generalized Hamming weight, dimension/length profile and their applications[J]. Chinese Journal of Electronics, 1999, 27(4):111-115.
- [12] 罗守山, 陈萍, 杨义先. 广义汉明重量下限函数  $L_i(j, d)$  的新证明[J]. 北京邮电大学学报, 1996, 19(4):67-70.  
LUO S S, CHEN P, YANG Y X. A new proof of lower bound  $L_i(j, d)$  of generalized Hamming weights[J]. Beijing University of Posts and Telecommunications, 1996, 19(4):67-70.
- [13] 罗守山, 杨义先, 吴伟陵. 线性码广义汉明重量的上限函数[J]. 通信学报, 1999, 20(11):86-90.  
LUO S S, YANG Y X, WU W L. The upper bound of generalized Hamming weight of linear codes[J]. Journal on Communications, 1999, 20(11):86-90.
- [14] 岳殿武, 胡正名. 广义 Hamming 重量上/下界的对偶定理[J]. 通信学报, 1997, 18(7):76-78.  
YUE D W, HU Z M. A dual theorem of upper and lower bound of generalized Hamming weights[J]. Journal on Communications, 1997, 18(7):76-78.
- [15] 岳殿武, 胡正名. 关于 BCH 码的广义 Hamming 重量上下限[J]. 通信学报, 1997, 18(4):75-79.  
YUE D W, HU Z M. Upper bounds and lower bounds on generalized Hamming weight for BCH codes[J]. Journal of Communications, 1997, 18(4):75-79.
- [16] 岳殿武, 胡正名. 广义 Hamming 重量和等重码[J]. 电子科学学刊, 1997, 19(4):553-557.  
YUE D W, HU Z M. Generalized Hamming weights and equal weight codes[J]. Journal of Electronics, 1997, 19(4):553-557.
- [17] 岳殿武, 江凌云, 段冰娟. 线性等重码格子复杂度的确定[J]. 应用科学学报, 2000, 18(1):68-71.  
YUE D W, JIANG L Y, DUAN B J. The determination of trellis complexity of linear constant weight codes[J]. Journal of Applied Sciences, 2000, 18(1):68-71.
- [18] HELLESETH T, KLØVE T, YTREHUS Ø. Generalized Hamming weights of linear codes[J]. IEEE Transactions Information Theory, 1992, 38(3): 1133-1140.
- [19] CHEN W D, KLØVE T. The weight hierarchies of  $q$ -ary codes of dimension 4[J]. IEEE Transactions Information Theory, 1996, 42(7): 2265-2272.
- [20] CHEN W D, KLØVE T. Bounds on the weight hierarchies of linear codes of dimension 4[J]. IEEE Trans Inform Theory, 1997, 43(6): 2047-2054.
- [21] CHEN W D, KLØVE T. The weight hierarchies of  $q$ -ary codes of dimension 4[J]. IEEE Transactions Information Theory, 1996, 42(7):2265-2272.
- [22] HU G X, CHEN W D. The weight hierarchies of  $q$ -ary linear codes of dimension 4[J]. Discrete Mathematics, 2010, 310(24):3528-3536.
- [23] 王丽君, 陈文德. 5 维  $q$  元线性码重量谱的分类与确定[J]. 系统科学与数学, 2011, 31(4): 402-413.  
WANG L J, CHEN W D. The classification and determination on weight hierarchies of  $q$ -ary linear codes of dimension 5[J]. Journal of Systems Science and Complexity, 2011, 31(4): 402-413.
- [24] 王丽君, 陈文德. II<sub>2</sub> 类 5 维  $q$  元线性码的重量谱[J]. 数学的实践与认识, 2011, 41(21): 244-252.  
WANG L J, CHEN W D. The weight hierarchies of  $q$ -ary linear codes of dimension 5 in class II<sub>2</sub>[J]. Mathematics in Practice and Theory, 2011, 41(21):244-252.
- [25] 王丽君, 陈文德. 一类 5 维  $q$  元线性码重量谱的确定[J]. 科学通报, 2011, 56(25):2150-2155.  
WANG L J, CHEN W D. Determination on a class of weight hierarchies of  $q$ -ary linear codes of dimension 5[J]. Chinese Science and Bulletin, 2011, 56(25):2150-2155.
- [26] 王丽君, 陈文德. V<sub>2</sub> 类 5 维  $q$  元线性码的重量谱[J]. 数学的实践与认识, 2012, 42(5): 237-245.  
WANG L J, CHEN W D. The weight hierarchies of  $q$ -ary linear codes of dimension 5 in class V<sub>2</sub>[J]. Mathematics in Practice and Theory, 2012, 42(5):237-245.
- [27] HU G X, ZHANG H G, WANG L J, et al. A class of the Hamming weight hierarchy of linear codes with dimension 5[J]. Tsinghua Science and Technology, 2014, 19(5):442-451.

## 作者简介:



胡国香 (1978-), 女, 山东烟台人, 武汉大学博士生, 中南民族大学副教授, 主要研究方向为密码学与信息安全。



张焕国 (1945-), 男, 河北元氏人, 武汉大学教授、博士生导师, 主要研究方向为信息安全、可信计算、容错计算与计算机应用等。