

一类5维 q 元线性码重量谱的确定

王丽君^①, 陈文德^②

① 中南民族大学数学与统计学学院, 武汉 430074;

② 中国科学院数学与系统科学研究院, 系统控制实验室与信息安全中心, 北京 100190

E-mail: wanglj_9@sina.com

2011-05-23 收稿, 2011-07-06 接受

中南民族大学中央高校基本科研业务费专项资金资助项目(CZQ10007)

摘要 “确定一般线性码的所有可能的重量谱”是通信系统中提出的一个有重要科学意义的基本理论问题. 但当 k 或 q 稍大时, 对于 k 维 q 元码, 这是不可能的, 问题的合理提法修改成: “确定 k 维 q 元一般线性码几乎所有的重量谱”. 基于有限射影几何方法, 本文研究V类5维 q 元线性码, 文中找出了V类5维码的重量谱的新必要条件, 把V类5维码的重量谱分为两个子类, 并发展改进了“子空间集法”, 从而确定了V类5维 q 元线性码几乎所有的重量谱. 这为确定5维中剩下的3类重量谱开辟了道路, 突破了难点. 同时, 新必要条件说明原来 k 维码重量谱的必要条件是不够的, 需要研究出进一步的新必要条件, 才能攻击与解决 k 维难题.

关键词

重量谱

5维 q 元线性码

差序列

有限射影几何

子空间集

信息科学是一门新兴的跨学科的科学, 它以信息为主要研究对象. 1948年Shannon发表了著名的论文《通信中的数学理论》, 创立了信息论. 纠错码是信息论的一个分支, 它为避免数据传输过程中发生错误提供了一种能检错和纠错的数学方法. 纠错码理论至今已有丰富的研究成果和广泛的应用, 近年来仍有很多问题成为研究热点, 如LDPC码^[1]、级联码^[2]、量子码^[3]等. 本文所研究的问题始于编码理论创始人之一, Hamming提出的Hamming重量这一概念. k 维线性码的重量谱, 也称为广义Hamming重量, 是一个序列 $(d_1, d_2, \dots, d_k)$, 其中 d_1 即为Hamming重量, 它由Wei^[4]提出, 提出的背景是 d_r 可应用于第二类窃密信道. 重量谱在线性码格子复杂度, 码的检错性能等多方面也都具有重要的应用价值. 总之, 码的重量谱是一组基本的重要参数, 并与通信系统的设计及其安全性有密切的关系. Kløve等人在文献[5]提出了“确定一般线性码的所有可能的重量谱”问题, 这是通信系统中提出的一个有重要科学意义的基本理论问题. 在 $k \leq 4$ 时, 文献[5,6]确定了2元一般线性码的所有重量谱.

纠错码的研究, 需要各种数学方法, 见文献[7~9]等. 1996年陈文德和Kløve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 元码的重量谱^[10]. 他们还把4维码及其重量谱分成了9类^[11], 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[11~13]等. 按这种分类法, 也可对更高维数的线性码分类, 但随着维数的增加这种分类法所得到的类数会迅速膨胀, 5维码就有114类, 难以一一确定. 在文献[6]必要条件的基础上文献[14]把5维码及其重量谱分成6类, 大大缩小了类数; 从而可能把4维码的研究成果, 对应提高到5维码.

从文献[15]看出, 当 k 或 q 增大时, 不能确定为重量谱的未知序列的数目急剧增加, 呈组合爆炸之势, 因此当 k 或 q 稍大时确定 k 维 q 元码所有重量谱是不可能的, 问题的合理提法修改成: “确定 k 维 q 元一般线性码几乎所有的重量谱”, 这个问题与方向是由陈文德和Kløve在2003年首次提出的^[16]. 这是一个难题. 至今这个问题仅对 k 维某些小类(例如I类)^[16], 3维码^[15], 4维码^[17]有所解决. “确定5维 q 元一般线性码几乎所有重量谱”是一个挑战性的新题目,

英文引用格式: Wang L J, Chen W D. Determination on a class of weight hierarchies of q -ary linear codes of dimension 5 (in Chinese). Chinese Sci Bull (Chinese Ver), 2011, 56: 2150–2155, doi: 10.1360/972010-2009

比 4 维码的对应问题困难复杂得多, 这方面成果极少. 文献[14]发展了文献[16]中提出的“子空间集”方法, 拓展了文献[17]的“落差法”, 用有限射影几何方法确定了 5 维码几乎所有的 II 类重量谱. 5 维中的 I, II 类与 4 维中的 I, II 类对应; 但 5 维其他 4 类在 4 维中没有对应类, 这是新的困难. 若按 II 类中的分类方法, 5 维码的 V 类重量谱分成 4 个子类, 其中 2 个子类中很难找出重量谱, 因此 V 类比 II 类要困难复杂得多. 为了解决这一困难, 本文用有限射影几何方法找出了 V 类 5 维码重量谱的新必要条件, 使得 5 维码的 V 类重量谱可以仅分为两个子类, 并改进了“落差法”, 从而确定了 V 类 5 维码的几乎所有的重量谱. 这为确定 5 维中剩下的 3 类重量谱开辟了道路, 突破了难点. 同时, 新必要条件说明文献[3]的 k 维码重量谱的必要条件是不够的, 需要研究出进一步的新必要条件, 才能攻击与解决 k 维难题.

1 有限射影几何方法

本文中 C 均表示有限域 $GF(q)$ 上 $[n, k; q]$ 线性码, 即 q 元、 n 长、 k 维线性码. 设 C 的任一子码记为 D , D 中所有码字的非零位置全体构成的集合称为 D 的支持集, 记为 $\chi(D)$. 即 $= \cup_{c \in D} \{i | c_i \neq 0, \text{ 这里 } c = (c_1, c_2, \dots, c_n)\}$, 支持集的大小记为 $\omega_s(D) = |\chi(D)|$.

令 $d_r = d_r(C) = \min\{\omega_s(D) | D \text{ 是 } C \text{ 的 } r \text{ 维子码}\}$, $1 \leq r \leq k$, 称为 C 的第 r 个最小支持重量或广义 Hamming 重量, 序列 $(d_1, d_2, \dots, d_k)$ 称为 C 的重量谱^[14](Weight hierarchy).

不失一般性, 假设 $n = d_k$. 令 $i_r = d_{k-r} - d_{k-r-1}$, $0 \leq r \leq k-1$, ($d_0 = 0$), 则序列 $(i_0, i_1, \dots, i_k)$ 称为 $[d_k, k; q]$ 码的差序列(简称 DS). 显然, DS 可由重量谱得到, 反之亦然. 于是确定重量谱归结为确定差序列.

令 G 为 C 的生成矩阵, 对 $\forall x \in GF(q)^n$, 用 $m(x)$ 表示 x 在 G 的列中出现的次数. 若 $x = \alpha y$, 其中 y 为 G 中的列, $\alpha \in GF(q)$ 且 $\alpha \neq 0$, 则可用 x 代替 y 而不改变任一子码的支持重, 因此可用射影空间 $PG(4, q)$ 中的点来描述 G 中的列. 令 V_4 为 $PG(4, q)$, 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(或重). 对 $\forall S \subset V_4$, 定义 S 的值为 $m(S) = \sum_{p \in S} m(p)$. 文献[10]证明了: 重量谱为 $(d_1, d_2, d_3, d_4, d_5)$ 的码的存在性等价于满足如下条件的赋值函数 m 的存在性:

$$\max\{m(U_r) | U_r \text{ 是 } V_4 \text{ 中的 } r \text{ 维子空间}\}$$

$$= \sum_{j=0}^r i_j, 0 \leq r \leq 4. \quad (1)$$

用 p^*, l^*, P^*, V^* , 分别表示 $r=0, 1, 2, 3$ 时赋值取(1)式右侧最大值的最重点, 线, 面, 体. 确定码的几乎所有重量谱的有限射影几何方法的核心就是: 先用几何法得到差序列最紧最好的必要条件, 再对满足这条件的几乎所有 i_j 构造出满足(1)式的尽量均匀的赋值函数 m .

2 主要结果

定义 2.1 以符号 $N(i)$ 表示 $i_0 \leq i$ 时某一类差序列 $(i_0, i_1, i_2, i_3, i_4)$ 的充分条件所含序列的数目, 符号 $M(i)$ 表示 $i_0 \leq i$ 时此类差序列的必要条件所含序列的数目.

如果 $\lim_{i \rightarrow \infty} \frac{N(i)}{M(i)} = 1$, 则称此必要条件是几乎充分的.

在文献[14]中, 把 5 维码的差序列的必要条件分成 6 类, 任两类中没有公共序列, 据此也就把差序列(重量谱)分成 6 类. 本文研究 V 类差序列. 文献[14]中其

必要条件为: $i_1 \leq qi_0, qi_1 < i_2 \leq \frac{q^2}{q+1}(i_0 + i_1), \frac{q^2}{q+1}(i_1 + i_2)$

$< i_3 \leq qi_2, i_0 \leq i_4 \leq (q^3 + q^2 + q)i_1 - i_2 - i_3$. 文献[14]中 V 类的必要条件不是最紧的, 最好的; 据此分出的 4 个子类中, 有 2 个子类没有差序列, 另一个子类中只有部分差序列. 下面的定理 2.1, 给 V 类差序列增加两个新必要条件, 且说明 V 类差序列的这个新必要条件是几乎充分的.

定理 2.1 V 类差序列 $(i_0, i_1, i_2, i_3, i_4)$ 的以下必要条件是几乎充分的:

- (i) $\frac{i_0}{q^2} < i_1 \leq qi_0$,
- (ii) $qi_1 < i_2 \leq \min\left\{\frac{q^2}{q+1}(i_0 + i_1), (q^2 + q)i_1 - i_0\right\}$,
- (iii) $\frac{q^2}{q+1}(i_1 + i_2) < i_3 \leq qi_2$,
- (iv) $i_0 \leq i_4 \leq (q^3 + q^2 + q)i_1 - i_2 - i_3$.

好的充分条件能够确定 V 类 5 维码几乎所有的重量谱.

3 新必要条件与分类

首先来推导出关键的新必要条件: $i_2 \leq (q^2 + q)i_1 - i_0$ 与 $i_1 > i_0/q^2$.

事实上, 如果 P^* 过 p^* , 则 $m(P^*) = i_0 + i_1 + i_2 = i_0 + \sum_{p^* \in l \subset P^*} (m(l) - i_0) \leq i_0 + (q+1)i_1$, 得 $i_2 \leq qi_1$, 这与 $i_2 > qi_1$ 矛盾, 故 P^* 必不过 p^* .

当 P^* 不过 p^* , 则 p^* 与 P^* 形成体 V , 有 $m(P^*) \leq m(V) - i_0 = \sum_{p^* \in l \subset V} (m(l) - i_0) \leq (q^2 + q + 1)i_1$, 即 $i_0 + i_1 + i_2 \leq (q^2 + q + 1)i_1$, 从而得: $i_2 \leq (q^2 + q)i_1 - i_0$. 又 $qi_1 < i_2 \leq (q^2 + q)i_1 - i_0$, 可得 $i_1 > i_0/q^2$. 2 个新的必要条件得到了.

$$\text{因 } (q^2 + q)i_1 - i_0 - \frac{q^2}{q+1}(i_0 + i_1) = (q^2 + q + 1)(qi_1 - i_0)/$$

$(q+1)$, 故当 $i_1 > i_0/q$ 时, 取 i_2 的上界为 $\frac{q^2}{q+1}(i_0 + i_1)$;

当 $i_1 \leq i_0/q$ 时, 取 i_2 的上界为 $(q^2 + q)i_1 - i_0$.

因此可将 V 类差序列的必要条件分为两个没有公共序列的子类: V1 和 V2.

$$\text{V1 类: } \frac{i_0}{q} < i_1 \leq qi_0, \quad qi_1 < i_2 \leq \frac{q^2}{q+1}(i_0 + i_1),$$

$$\frac{q^2}{q+1}(i_1 + i_2) < i_3 \leq qi_2, \quad i_0 \leq i_4 \leq (q^3 + q^2 + q)i_1 - i_2 - i_3.$$

$$\text{V2 类: } \frac{i_0}{q^2} < i_1 \leq \frac{i_0}{q}, \quad qi_1 < i_2 \leq (q^2 + q)i_1 - i_0,$$

$$\frac{q^2}{q+1}(i_1 + i_2) < i_3 \leq qi_2, \quad i_0 \leq i_4 \leq (q^3 + q^2 + q)i_1 - i_2 - i_3.$$

因 V 类差序列的必要条件满足 $V1 \cup V2 = V$, 定理 2.1 的证明转化为证 V1 类差序列的必要条件几乎充分和 V2 类差序列的必要条件几乎充分, 亦即找到 V1 和 V2 类差序列的充分条件. 它与必要条件十分接近.

4 V1 类的充分条件

为找到 V1 类差序列的充分条件(定理 4.1), 第一步是在 i_j 取边界值时, 构造出满足(1)式的赋值函数 m , 称它为边界结构.

引理 4.1 设

$$i_1 = qi_0 - (q+1), \quad (2)$$

$$i_2 = qi_1 + q, \quad (3)$$

$$i_3 = qi_2, \quad (4)$$

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

这里 i_1, i_2, i_3, i_4 为上界. i_2 为下界(i_1 取(2)式时 i_2 的上下界相等). 则边界序列 $(i_0, i_1, i_2, i_3, i_4)$ 为差序列.

证明: 把边界各式代入后, 得:

$$m(l^*) = i_0 + i_1 = (q+1)i_0 - (q+1),$$

$$m(P^*) = i_0 + i_1 + i_2 = (q^2 + q + 1)i_0 - (q^2 + q + 1),$$

$$\begin{aligned} m(V^*) &= i_0 + i_1 + i_2 + i_3 \\ &= (q^3 + q^2 + q + 1)i_0 - (q^3 + q^2 + q + 1). \end{aligned}$$

设 $PG(4, q)$ 为不在一个体内的 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 $\langle x_1, x_2, \dots, x_t \rangle$ 表示 $x_1, x_2, \dots, x_t$ 生成的 $t-1$ 维子空间.

定义 $X_i \in \langle e_1, e_3, e_4, e_5 \rangle$, $0 \leq i < q^3 + q^2 + q + 1$. 记 $\langle e_2, X_i \rangle$ 上自 e_2 后第一个点为 p_i , $0 \leq i < q^3 + q^2 + q + 1$.

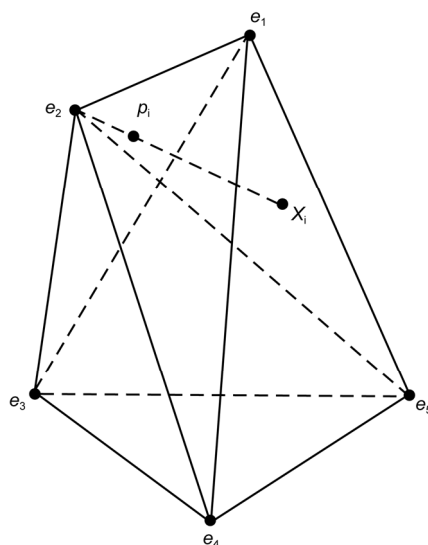


图 1 $PG(4, q)$ 中构造边界结构的简图

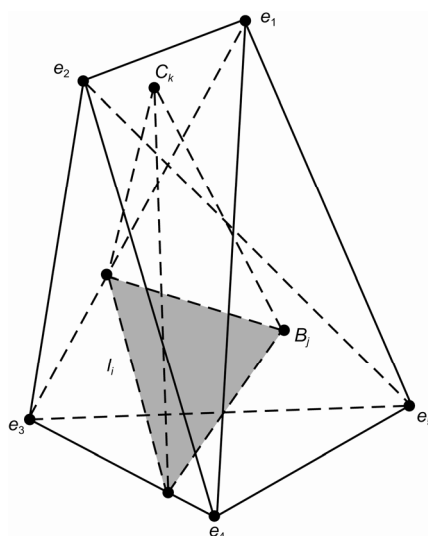


图 2 使 i_1 下降所用的简图

其中 $\langle I_1, B_1, C_k \rangle$ 为 $PG(4, q)$ 中的体

构造赋值函数如下:

$$m(x) = \begin{cases} i_0, & x = e_2; \\ i_0 - 2, & x = p_i (0 \leq i < q^3 + q^2 + q + 1); \\ i_0 - 1, & \text{其他.} \end{cases}$$

即 e_2 取值为 i_0 , e_2 与 $\langle e_1, e_3, e_4, e_5 \rangle$ 上每点的连线上有一点取值为 $i_0 - 2$ (这个点不在 $\langle e_1, e_3, e_4, e_5 \rangle$ 上), 其余各点均为 $i_0 - 1$.

这样, 取 e_2 为 p^* . $\langle e_1, e_3 \rangle$ 为 l^* . $\langle e_1, e_3, e_4 \rangle$ 为 $P^*(\langle e_1, e_3, e_4, e_5 \rangle)$ 内所有的面都为 P^* . $\langle e_1, e_3, e_4, e_5 \rangle$ 为 V^* . 易验(1)式成立.

为了从上述边界结构得到一般结构, 我们先用体集降 i_1 到下界附近, 而保持其它 i_j 仍为边界值(引理 4.2), 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 4.3), 最后将 i_3, i_4 降到下界附近(定理 4.1).

引理 4.2 对任意满足(3)~(5)的序列 $(i_0, i_1, i_2, i_3, i_4)$, 如果

$$\frac{i_0}{q} + f_1(q) \leq i_1 \leq qi_0 - f_2(q), \quad (6)$$

其中 $f_1(q) = q^9 - q^7 + q - 1$, $f_2(q) = q^{11} + 3q^{10} + 2q^9 - 2q^8 - 5q^7 - q^6 + q^5 + q^4 - q^3 + 2q^2 - 3q + 13$, 则 $(i_0, i_1, i_2, i_3, i_4)$ 是差序列.

证明: 定义 l_i 为 $\langle e_1, e_3, e_4 \rangle$ 上除 $\langle e_1, e_3 \rangle$ 外的线, $0 \leq i < q^2 + q$; $B_j \in \langle e_1, e_3, e_4, e_5 \rangle \setminus \langle e_1, e_3, e_4 \rangle$, $0 \leq j < q^3$; $C_k \in V_4 \setminus (\langle e_1, e_3, e_4, e_5 \rangle \cup \langle l_i, B_j, e_2 \rangle)$, $0 \leq k < q^4 - q^3$. $\langle l_i, B_j, C_k \rangle$ 形成体集.

在 $m(x)$ 的基础上, 略作变形, 构造函数 $m'(x)$ 如下:

$$m'(x) = \begin{cases} m(x) - 1, & x \in \langle l_i, B_j, C_k \rangle; \\ m(x), & \text{其他.} \end{cases}$$

体集中每个体与 V_4 中每条线至少交于一点, 故变形一次, 每根线至少下降值 1 (简记为 $\downarrow 1$); $\langle e_1, e_2 \rangle \downarrow 1$, 仍为 l^* , i_0 不变, $i_1 \downarrow 1$. 类似地, 体与面至少交于一线, 面至少 $\downarrow (q+1)$; $\langle e_1, e_3, e_4 \rangle \downarrow (q+1)$, 仍为 P^* , 体与体至少交于一面, 体至少 $\downarrow (q^2 + q + 1)$, $\langle e_1, e_3, e_4, e_5 \rangle \downarrow (q^2 + q + 1)$, 仍为 V^* . i_2, i_3, i_4 分别 $\downarrow q, q^2, q^3$, (1)式仍成立, 下降后的序列仍为差序列, (3)~(5)边界式仍满足. 这就是用体集这种“子空间集”方法的好处.

体 $\langle l_i, B_j, C_k \rangle$ 共 $q^7(q^2 - 1)$ 个. 逐一用 $q^7(q^2 - 1)$ 个体及 $m'(x)$ 式迭代变形 $q^7(q^2 - 1)$ 次后 (称为下降一圈), $i_1 \downarrow q^7(q^2 - 1)$, $B_j \downarrow q^6(q^2 - 1)$, $\langle e_1, e_3, e_4 \rangle \setminus \langle e_1, e_3 \rangle$ 上每点 $\downarrow q^6(q^2 - 1)$, 还有 $\langle e_1, e_2, e_3, e_4 \rangle \setminus (\langle e_1, e_2, e_3 \rangle \cup \langle e_1, e_3, e_4 \rangle)$ 上每点 (共 $q^3 - q^2$ 个点) $\downarrow (q^2 - 1)q^3q^3 = q^6(q^2 - 1)$ (为使该点不在体 $\langle l_i, B_j, e_2 \rangle$ 内, 面 $\langle e_1, e_3, e_4 \rangle$ 上只有 $q^2 - 1$ 条线可以选, B_j 点有

q^3 个可以选, 又在 $\langle l_i, B_j, C_k \rangle \setminus \langle l_i, B_j \rangle$ 中, 有 q^3 个点可以够成体 $\langle l_i, B_j, C_k \rangle$, $\langle e_1, e_3, e_4, e_5 \rangle \cup \langle e_1, e_2, e_3, e_4 \rangle$ 外 (共 $q^4 - q^3$ 个点) 的每个点 $\downarrow (q^2 + q)(q^3 - q^2)q^3 = q^6(q^2 - 1)$. $\langle e_1, e_3 \rangle$ 上每点 $\downarrow q^7(q - 1)$, $\langle e_1, e_2, e_3 \rangle \setminus (e_2 \cup \langle e_1, e_3 \rangle)$ 上 (共 $q^2 - 1$ 个点) 每点 $\downarrow q^2q^3q^3 = q^8$.

为保证最小值点一直 ≥ 0 , 可算出最大下降圈数

$$\omega_1: (i_0 - 2) - \omega_1 q^8 \geq 0, \text{ 得 } \omega_1 \leq \frac{i_0 - 2}{q^8}. \text{ 取 } \omega_1 = \left\lfloor \frac{i_0 - 2}{q^8} \right\rfloor,$$

$$\text{则 } i_1 \text{ 可降至 } qi_0 - (q + 1) - \omega_1 q^7(q^2 - 1) < qi_0 - (q + 1) - \left(\frac{i_0 - 2}{q^8} - 1 \right) q^7(q^2 - 1) < \frac{i_0}{q} + q^9 - q^7 + q - 1 = \frac{i_0}{q} + f_1(q).$$

注意到引理 4.2 中的体集很特殊, 当 i_1 下降时, $\langle e_1, e_3 \rangle$ 中的点比 $\langle e_1, e_3, e_4, e_5 \rangle$ 中其余点减得少, 经过一圈后, $\langle e_1, e_3, e_4, e_5 \rangle$ 中只有 $\langle e_1, e_3 \rangle$ 仍是最重线, $\langle e_1, e_3, e_4, e_5 \rangle$ 内只有过 $\langle e_1, e_3 \rangle$ 的面仍是最重面. 这样在 $\langle e_1, e_3, e_4, e_5 \rangle$ 内部形成“落差”, 为 i_2 上升及 i_3 下降做好了准备.

引理 4.3 对任意满足(4)(5)(6)的序列 $(i_0, i_1, i_2, i_3, i_4)$, 如果

$$qi_1 + f_3(q) \leq i_2 \leq \frac{q^2}{q+1}(i_0 + i_1) - f_4(q), \quad (7)$$

其中 $f_3(q) = q^{10} - q^9 - q^5 + 2q^4 - 3q^3 + 5q^2 - 8q + 14$, $f_4(q) = q^6(q - 1)(q^4 + 2q^3 + 3q^2 + q - 2)$, 则 $(i_0, i_1, i_2, i_3, i_4)$ 是差序列.

证明: 定义 $A_i \in \langle e_1, e_3, e_4 \rangle \setminus \langle e_1, e_3 \rangle$, $0 \leq i < q^2$; B_j 同引理 4.2; $E_k \in \langle e_2, A_i, B_j \rangle \setminus (\langle e_2, A_i \rangle \cup \langle A_i, B_j \rangle)$, $0 \leq k < q^2 - q$; $F_l \in \langle e_2, A_i \rangle \setminus \{e_2, A_i\}$, $0 \leq l < q - 1$, 如图 3 所示.

构造函数 $m''(x)$ 如下:

$$m''(x) = \begin{cases} m'(x) + 1, & x \in \langle A_i, B_j \rangle; \\ m'(x) - 1, & x \in \langle A_i, E_k \rangle \setminus \{A_i\}; \\ m'(x) - 1, & x = F_l \\ m'(x), & \text{其他.} \end{cases}$$

这里的 $m'(x)$ 是指(6)式中 i_1 取定某值后对应的 (迭代多次后所得的) 赋值函数. 可以验证: 用结构 $m''(x)$ 可将 i_2 上升到上界附近, 而保持 i_3, i_4 仍为边界值, 序列仍为差序列.

定理 4.1 对于 5 维 q 元线性码, $(i_0, i_1, i_2, i_3, i_4)$ 为 V1 类差序列的充分条件是:

- (i) $f_0(q) \leq i_0$;
- (ii) $\frac{i_0}{q} + f_1(q) \leq i_1 \leq qi_0 - f_2(q)$;
- (iii) $qi_1 + f_3(q) \leq i_2 \leq \frac{q^2}{q+1}(i_0 + i_1) - f_4(q)$;

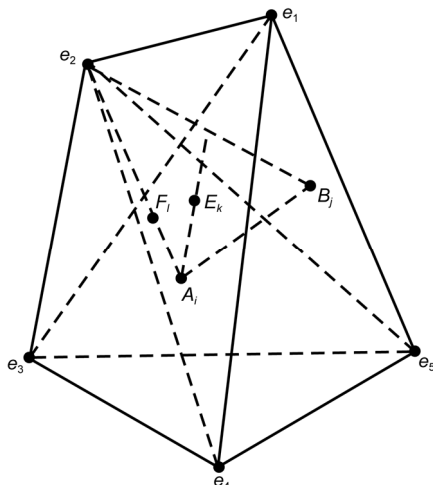


图3 使 i_2 上升所用的简图

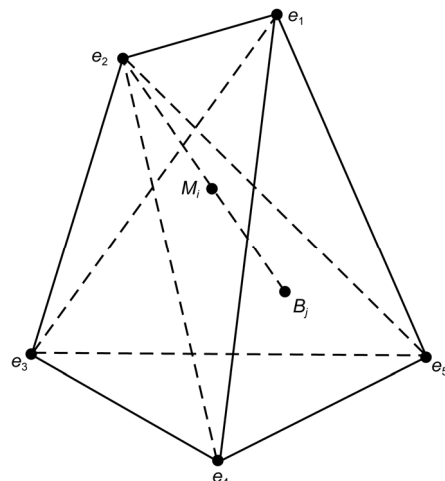


图4 使 i_3 下降所用的简图

$$(iv) \frac{q^2}{q+1}(i_1 + i_2) + f_5(q) \leq i_3 \leq qi_2;$$

$$(v) i_0 \leq i_4 \leq (q^3 + q^2 + q)i_1 - i_2 - i_3.$$

其中 $f_0(q) = q^{10} + 3q^9 + 4q^8 + q^7 - 2q^6 - q^4 + q^3 - 2q^2 + 3q + 5$, $f_1(q) = q^9 - q^7 + q - 1$, $f_2(q) = q^{11} + 3q^{10} + 2q^9 - 2q^8 - 5q^7 - q^6 + q^5 + q^4 - q^3 + 2q^2 - 3q + 13$, $f_3(q) = q^{10} - q^9 - q^5 + 2q^4 - 3q^3 + 5q^2 - 8q + 14$, $f_4(q) = q^6(q-1)(q^4 + 2q^3 + 3q^2 + q - 2)$, $f_5(q) = 2q^3(q-1)$.

证明: 定义 B_j 同引理 4.2; $M_i \in \langle e_2, B_j \rangle \setminus \{e_2, B_j\}$ $0 \leq i < (q-1)$, 如图 4 所示.

构造函数 $m'''(x)$ 如下:

$$m'''(x) = \begin{cases} m''(x) - 1, & x = B_j; \\ m''(x) + 1, & x = M_i; \\ m''(x), & \text{其他.} \end{cases}$$

其中 $m''(x)$ 是指 (7) 式中 i_2 取定某值后对应的 (迭代多次后所得的) 赋值函数. 可以验证: 用结构 $m'''(x)$ 可将 i_3 下降到下界附近, 而保持 i_4 仍为边界值, 序列仍为差序列. i_4 可直接往下降, 一直降到 i_0 , 降到 $\langle e_1, e_3, e_4, e_5 \rangle \cup \{e_2\}$ 之外所有点取值为 0.

以 $N_1(i)$ 表示 $i_0 \leq i$ 时满足 V1 类差序列的充分条件所含序列的数目, 以 $M_1(i)$ 表示 $i_0 \leq i$ 时满足 V1 类的必要条件中所含序列的数目, 用定理 4.1 经计算可得

$$\lim_{i \rightarrow \infty} \frac{N_1(i)}{M_1(i)} = 1. \text{ 从而有}$$

定理 4.2 V1 类差序列 $(i_0, i_1, i_2, i_3, i_4)$ 的必要条件是几乎充分的.

5 V2 类

定理 5.1 V2 类差序列 $(i_0, i_1, i_2, i_3, i_4)$ 的以下必要条件是几乎充分的:

- (i) $\frac{i_0}{q^2} < i_1 \leq \frac{i_0}{q}$;
- (ii) $qi_1 < i_2 \leq (q^2 + q)i_1 - i_0$;
- (iii) $\frac{q^2}{q+1}(i_1 + i_2) < i_3 \leq qi_2$;
- (iv) $i_0 \leq i_4 \leq (q^3 + q^2 + q)i_1 - i_2 - i_3$.

证明类似于 V1 类 (定理 4.2), 详略. 由定理 4.2 与定理 5.1, 我们证得了本文主要结果定理 2.1.

参考文献

- Zhang G H, Wang J H, Li X Y, et al. Tight lower bound of consecutive lengths for QC-LDPC codes with girth at least ten. Chinese Sci Bull, 2011, 56: 1272-1277
- Liu X J, Zhao C M, Sun X J. Low complexity Chase-2 decoding of concatenated codes. Chinese Sci Bull, 2010, 55: 3066-3070
- Wang W Y, Feng R Q, Feng K Q. Inhomogenous quantum codes (I): Additive case. Sci China Math, 2010, 53: 2501-2510
- Wei V K. Generalized Hamming weight for linear codes. IEEE Trans Inform Theory, 1991, 37: 1412-1418

- 5 Helleseeth T, Kløve T, Ytrehus ø. Generalized Hamming weights of linear codes. *IEEE Trans Inform Theory*, 1992, 38: 1133–1140
- 6 Kløve T. Minimum support weights of binary codes. *IEEE Trans Inform Theory*, 1993, 39: 648–654
- 7 万哲先. 代数和编码. 北京: 科学出版社, 1985
- 8 王新梅, 肖国镇. 纠错码——原理与方法. 西安: 西安电子科技大学出版社, 1991
- 9 冯克勤. 纠错码的代数理论. 北京: 清华大学出版社, 2003
- 10 Chen W D, Kløve T. The weight hierarchies of q -ary codes of dimension 4. *IEEE Trans Inform Theory*, 1996, 42: 2265–2272
- 11 Chen W D, Kløve T. Bounds on the weight hierarchies of linear codes of dimension 4. *IEEE Trans Inform Theory*, 1997, 43: 2047–2054
- 12 Chen W D, Kløve T. Weight hierarchies of extremal non-chain binary codes of dimension 4. *IEEE Trans Inform Theory*, 1999, 45: 276–281
- 13 王丽君, 夏永波, 陈文德. 4 维 3 元断链码的重量谱. *系统科学与数学*, 2009, 29: 742–749
- 14 王丽君, 陈文德. 5 维 q 元线性码重量谱的分类与确定. *系统科学与数学*, 2011, 31: 402–413
- 15 Chen W D, Kløve T. The weight hierarchies of linear codes of dimension 3. *J Stat Plan Inf*, 2001, 94: 167–179
- 16 Chen W D, Kløve T. Weight hierarchies of linear codes satisfying the almost chain condition. *Sci China Ser F: Inf Sci*, 2003, 46: 175–186
- 17 Hu G X, Chen W D. The weight hierarchies of q -ary linear codes of dimension 4. *Discrete Math*, 2010, 310: 3528–3536

Determination on a class of weight hierarchies of q -ary linear codes of dimension 5

WANG LiJun¹ & CHEN WenDe²

¹ College of Mathematics and Statistics, South-Central University for Nationalities, Wuhan 430074, China;

² Laboratory of Systems and Control and Information Security Center, Institute of Systems Science, Chinese Academy of Sciences, Beijing 100190, China

To determine all possible weight hierarchies of general linear codes is a basic theory having important scientific significance raised in the communication system. But when k or q is larger, it is impossible for q -ary linear codes of dimension k . Reasonable formulation of the problem is modified: to determine almost all the weight hierarchies of q -ary general linear codes of dimension k . Based on the finite projective geometry method, q -ary linear codes of dimension 5 in class V are studied in this paper, in which we find new necessary conditions of weight hierarchies of 5-dimensional codes in class V, and classify the weight hierarchies of 5-dimensional codes in class V into two subclass, and advance subspace set method, and determine almost all the weight hierarchies of q -ary linear codes of dimension 5 in class V. It open the way for the remaining three class of weight hierarchies of 5-dimensional codes, and break through the difficulty. Furthermore, new necessary conditions show that original necessary conditions of weight hierarchies are not enough. We need to develop further new necessary conditions, in order to attack and solve problems of dimension k .

q -ary linear codes of dimension 5, deference sequence, finite projective geometry, subspace set method

doi: 10.1360/972010-2009