

Hermitian 码的完全权分布^{*}

谭晓青, 李艳会, 朱思铭

(中山大学数学与计算机科学学院, 广东 广州, 510275)

摘 要: Hermitian 码的完全权分布对其自身编码和解码算法的设计、改进及性能分析都具有关键的作用。讨论了 Hermitian 码完全权分布的计算问题, 结合计算机应用得出了几个具体 Hermitian 码的完全权分布, 同时, 提出了在 Hermitian 码及其对偶码的最小距离确定下时, 一种计算 Hermitian 码完全权分布的简化算法。

关键词: Hermitian 码; 线性码; 对偶码; 权分布 (重量分布)

中图分类号: O157.4 **文献标识码:** A **文章编号:** 0529-6579 (2003) 01-0009-03

作为几何 Goppa 码的特例 Hermitian 码一直都是被研究得最为透彻的一类代数几何码^[1], 其最小 Hamming 权^[2], 自同构群^[3]等已被彻底了解, 但是其权分布到目前为止还未得到很好的解决。无论是从理论上还是未来可能的商业应用上来讲, Hermitian 码完全权分布都是目前代数几何码研究中最为重要的问题之一。

1 Hermitian 码

有限域 F_{q^2} 上的一条 Hermitian 曲线 χ 如下:

$$y^q \oplus y = x^{q+1}$$

其上除无穷远点外还另有 q^3 个有理点, 令其函数域为 $E = F_{q^2}(x, y)$, 考虑 E 中的 2 个除子:

$$D = \prod_{\alpha \in F_{q^2}} \prod_{Q \in \mathcal{Q}(\alpha)} Q, \\ G_m = Q_\infty^m$$

其中, Q_∞^m 表示 E 中无穷除子。当

$$2g - 2 < m < n = q^3 = \deg D$$

时, 其中 $g = \frac{q(q-1)}{2}$,

码:

$$C(D, G_m) = \{ \{ f(Q) \}_{Q \in \text{supp}(D)} \mid \forall f \in L(G_m) \} \triangleq C_m^{(q^2)}$$

其中, $\text{supp}(D)$ 是 D 的支座, $L(G_m)$ 是由一组单项式 $x^i y^j$ 生成, $B(m) = \{ x^i y^j \mid 0 \leq i, 0 \leq j \leq q-1, iq + j(q+1) \leq m \}$ 是 $L(G_m)$ 的一组基。

$C_m^{(q^2)}$ 是 F_{q^2} 上一个 $[n = q^3, k_m = m + 1 - g, d_{\min} \geq n - m]$ 线性码, 该线性码即为 Hermitian 码, $d_{\min}$ 指该线性码的最小 Hamming 距离。

2 一般线性码及 Hermitian 码权分布

若 C 是一个 $[n, k, d]$ 线性码 (以下用 d 代替 $d_{\min}$), $\{A_i\}$ 是 C 的重量分布, 即 A_i 等于 C 中 Hamming 重量为 i 的码字个数。如何计算线性码的重量分布? 最直接的方法是列出 C 中所有的码字, 然后计算 C 的重量分布, 当 n 很大时, 这种方法显然是不现实的, 而且事实上也证明了, 线性码的重量分布, 最小距离, 覆盖半径和译码等问题, 除少数几类码是已知的以外, 一般要解决它们是很困难的, 是一个 NP 完全问题, 因此设计行之有效的计算码的重量分布的方法, 是编码理论的一个重要任务, 通过 C 与 $C^\perp$ 的重量分布之间的联系, 是解决这个问题的一种途径。文[4], 就有如下结论:

设 C 是 $GF(q)$ 上的 $[n, k, d]$ 线性码, $C^\perp$ 是其对偶码, 且 $C^\perp$ 的最小距离为 d' , 并设 $\{A_i\}$ 和 $\{A_i'\}$ 分别是 C 和 $C^\perp$ 的重量分布, 当 $A_d, A_{d+1}, \dots, A_{n-d}$ 已知时, 有:

$$\sum_{j=1}^t (-1)^{t-j} \begin{bmatrix} d'-j \\ t-j \end{bmatrix} \begin{bmatrix} n \\ d'-j \end{bmatrix} (q^{k-d'+j} - 1) + \sum_{j=1}^t \sum_{i=d}^{n-d'} (-1)^{t-j+1} \begin{bmatrix} d'-j \\ t-j \end{bmatrix} \begin{bmatrix} n-i \\ d'-j \end{bmatrix} A_i = A_{n-d'+t} \quad (1)$$

上述结论实际上也是由线性码及其对偶码的重量分布关系的经典结论 MacWilliams 定理推导而来。在这里要知道线性码及其对偶码的最小距离, 而对于 Hermitian 码来说, 其最小距离也是难以确定的, 但在一定条件下, Hermitian 码的最小距离是可以确定的。由文[5], 对于 Hermitian 码, 当 $q \mid m$ 时, $d = n - m$, 因此, 关于 Hermitian 码的权分布, 有

* 收稿日期: 2002-05-20

作者简介: 谭晓青 (1976 年生), 女, 博士研究生; E-mail: txqdoudou@163.com

这样一个结论:

定理 设 $C_m^{(q^2)}$ 是 $GF(q^2)$ 上的 Hermitian 码, 当 $q \mid m$ 且 $q \mid m+2$ 时, $C_m^{(q^2)}$ 为线性码

$$\left[q^3, m+1-\frac{q^2-q}{2}, d=q^3-m \right]$$

该 Hermitian 码 $C_m^{(q^2)}$ 的对偶码则为线性码

$$\left[q^3, m+1-\frac{q^2-q}{2}, d=q+m+2-q^2 \right]$$

只要 $A_d, A_{d+1}, \cdots, A_{q^3-d}$ 已知时, 该 Hermitian 码及其对偶码的重量分布可以完全确定。

3 两个实例

3.1 F_{2^2} 上 Hermitian 码 $C_4^{(2^2)}[8, 4, 4]$ 的权分布计算

F_{2^2} 上的 Hermitian 码 $C_4^{(2^2)}[8, 4, 4]$ 是一个自对偶码。由文[3], $C_m^{(q^2)}$ 的完全权分布满足:

$$\omega(x, y) = \sum A_r x^{n-r} y^r = \sum_{i=0}^m B_i y^i (x-y)^{m-i} + x^n, n=q^3$$

其中, $B_i = \binom{n}{m-i} (q^{2(i-g+1)} - 1)$ 对 $i \geq 2g-1$ 成立。由该结论, 知 $C_4^{(2^2)}[8, 4, 4]$ 完全权分布可如下确定:

$$\omega(x, y) = x^8 + 255y^8 + 504y^7(x-y) + 420y^6(x-y)^2 + 168y^5(x-y)^3 + B_0y^4(x-y)^4$$

其中, 码 $C_4^{(2^2)}[8, 4, 4]$ 中, $q=2, m=4, q \mid m$ 且 $q \mid m+2$, 由前面的结论, 若知道 A_4 , 则

$$\begin{aligned} A_5 &= 168 - 4A_4 \\ A_6 &= -84 + 6A_4 \\ A_7 &= 168 - 4A_4 \\ A_8 &= 3 + A_4 \end{aligned}$$

用计算机搜索很容易得出 $A_4=18$, 另外, 我们知道 F_{2^2} 上的 Hermitian 曲线是一条椭圆曲线, 利用文[2] 可以从理论上证明 A_4 的值为 18。于是可得出 $C_4^{(2^2)}$ 的完全权分布为: $A_8=21, A_7=96, A_6=24, A_5=96, A_4=18, A_3=0, A_2=0, A_1=0, A_0=1$ 。

3.2 F_{3^2} 上 Hermitian 码 $C_9^{(3^2)}[27, 7, 18]$ 权分布的计算

考虑 F_{3^2} 上的一个 Hermitian 码, 由文[4], 当 $2g-2 < m \leq n-q^2$ 时, $d=n-m$, 若取 $m=9$, 则 F_{3^2} 上有 Hermitian 码 $C_9^{(3^2)}[27, 7, 18]$, 设

$$F_{3^2} = \frac{Z_3[x]}{x^2+1} =$$

$$\{0, 1, 2, x, x+1, x+2, 2x+1, 2x+2\}$$

则 $C_9^{(3^2)}$ 是下述矩阵的列向量在有限域上张成的 F_9^{27} 的 7 维线性子空间:

1	0	0	0	0	0	0
1	0	0	0	0	x	2
1	0	0	0	0	2x	2
1	1	1	1	2	2	1
1	1	1	1	x+2	x+2	x
1	1	1	1	2x+2	2x+2	2x
1	2	1	2	1	2	1
1	2	1	2	2x+1	x+2	x
1	2	1	2	x+1	2x+2	2x
1	x	2	2x	2x	2	1
1	x	2	2x	2x+2	x+2	x
1	x	2	2x	2x+1	2x+2	2x
1	x+1	2x	2x+1	x+1	1	1
1	x+1	2x	2x+1	2x	x+1	2x
1	x+1	2x	2x+1	2	2x+1	x
1	x+2	x	2x+2	x+2	1	1
1	x+2	x	2x+2	1	x+1	2x
1	x+2	x	2x+2	2x	2x+1	x
1	2x	2	2	x	2	1
1	2x	2	2	x+1	x+2	x
1	2x	2	2	x+2	2x+2	2x
1	2x+1	x	x+1	2x+1	1	1
1	2x+1	x	x+1	2	x+1	2x
1	2x+1	x	x+1	x	2x+1	x
1	2x+2	2x	x+2	2x+2	1	1
1	2x+2	2x	x+2	x	x+1	2x
1	2x+2	2x	x+2	1	2x+1	x

其对偶码的维数为 $n-k=27-7=20 \Rightarrow$ 对应的 $m=22$, 设其最小距离为 d' , 所以其对偶码为 $[27, 20, d']$, 由文[2], 当 $q^3-q^2 \leq m \leq q^3; m=q^3-q^2+aq+b; 0 \leq b \leq a \leq q-1$ 时, $d=n-m+b$ 。对其对偶码 $[27, 20, d']$, $m=22=3^3-3^2+3-1, a=1, b=1$ 则有 $d'=6$ 。

这里 $d'=6$, 只要知道 $A_{18}, A_{19}, A_{20}, A_{21}$, 则:

$$\begin{aligned} A_{22} &= 6\,458\,400 - 126A_{18} - 56A_{19} - 21A_{20} - 6A_{21} \\ A_{23} &= -19\,515\,600 + 504A_{18} + 210A_{19} + 70A_{20} + 15A_{21} \\ A_{24} &= 32\,666\,400 - 840A_{18} - 336A_{19} - 105A_{20} - 20A_{21} \\ A_{25} &= -24\,763\,752 + 720A_{18} + 280A_{19} + 84A_{20} + 15A_{21} \\ A_{26} &= 11\,647\,584 - 315A_{18} - 120A_{19} - 35A_{20} - 6A_{21} \\ A_{27} &= -1\,710\,064 + 56A_{18} + 21A_{19} + 6A_{20} + A_{21} \end{aligned}$$

利用计算机编程搜索生成的 7 维线性子空间上非零个数为 18, 19, 20, 21 的向量, 并分别统计这样的向量个数, 得到 $A_{18}=8\,448, A_{19}=3\,996, A_{20}=63$

504, $A_{21} = 216\ 864$, 再利用上面的等式计算出 $A_{22} \cdots A_{27}$, 得到了 $C_9^{(3^2)} = [27, 7, 18]$ 的完全权分布: $A_0 = 1, A_1 = 0, \cdots, A_{17} = 0, A_{18} = 8\ 448, A_{19} = 3\ 996, A_{20} = 63\ 504, A_{21} = 216\ 864, A_{22} = 521\ 424, A_{23} = 832\ 032, A_{24} = 1\ 138\ 320, A_{25} = 1\ 094\ 904, A_{26} = 667\ 440, A_{27} = 200\ 072$

4 求 Hermitian 码权分布的一个简化算法

对于 Hermitian 码及其对偶码的最小距离已知的这类码, 要求其权分布可用以下算法思想用计算机程序实现。算法思想:

步骤 1, 用 2 个函数分别定义有限域 F_{q^2} 上的加法 $\oplus$ 与乘法 $\otimes$ (在这里可用整数 $0 \cdots q^2 - 1$ 来表示 F_{q^2} 上的元素);

步骤 2, 定义 $L(G_m)$ 中的基函数组 $f_1, f_2, \cdots, f_k (f_i (i=1, \cdots, k) \in B(m)$ 是关于 x 和 y 的幂函数);

步骤 3, 计算满足等式: $y^q \oplus y = x^{q+1}$ (其中加法和乘幂由步骤 1 定义) 的所有有理点 (x, y) 共 q^3 个;

步骤 4, 将这 q^3 个点分别代入步骤 2 定义的 k 个函数中, 得到该 Hermitian 码的生成矩阵, 把它放在一个二维数组(维数为 $k \times q^3$) 里;

步骤 5, 用一个一维数组来存放生成线性子空间的任一向量(为基向量在有限域上的线性组合), 搜索所生成的非零分量个数为 $d, d+1, \cdots, n-d'$

的向量, 并分别统计这样向量的个数, 得到 $A_d, A_{d+1}, \cdots, A_{q^3-d'}$;

步骤 6, 利用计算机根据公式 (1) 计算 $A_{q^3-d+t} (t=1, \cdots, d')$ 得到完全权分布。

算法分析: 由前面第 2 部分的分析, 可以证明该算法的可行性。这个算法的一个主要优点就是它没有去穷举所有的码字, 而只是去搜索满足预先设定条件的码字, 这在时间上就提高了很多。所以对于那类自身及其对偶码的最小距离确定情况下的 Hermitian 码, 利用这种算法思想编写程序计算, 很快就能得到它的完全权分布。该算法的不足之处在于, Hermitian 码的最小距离并不是容易确定的, 即使它自身的最小距离能够被确定, 其对偶码的最小距离也是不容易确定的。

参考文献:

[1] 冯贵良, 吴新文. 代数几何码[M] . 北京: 科学出版社, 1998.

[2] YANG K, KUMAR P V. On the true minimum distance of Hermitian codes[J] . Coding Theory and Algebraic Geometry, Proceeding, Luminy 1991, INM, 1518: 99- 107.

[3] KATSMAN G L, TSFASMAN M. Spectra of algebraic geometry codes[J] . Probl Inform Trans, 1987, 23: 262- 275.

[4] 邢朝平, 冯克勤. 线性码的重量分布[J] . 数学的实践与认识, 1990(2) : 20- 23.

[5] 邢朝平, 冯克勤. Hermitian 码的最小距离[J] . 科学通报, 1990(23) : 1768- 1771.

The Complete Weight Distribution of Hermitian Code

TAN Xiao qing, LI Yan hui, ZHU Si ming

(Department of Mathematics, Sun Yat sen University, Guangzhou 510275, China)

Abstract: The complete weight distribution of Hermitian code is of pivotal effect on algorithm designing, improving and capability analysis about its encoding or decoding. The computation problem of Hermitian code's weight distribution is discussed, some complete weight distributions of specific Hermitian codes are gotten. Also, a simplified algorithm of computing the complete weight distribution of Hermitian code is given when the least Hamming distance of it and its dual code are made certain.

Key words: Hermitian code; linear code; dual code; weight distribution