

Hermitian 码的权分布*

许楚芬

(中山大学数学系, 广东 广州 510275)

摘 要: 从理论上讲, Hermitian 码的完全权分布是目前代数几何码研究中最重要的问题之一, 文章结合理论分析及计算机应用对 4 元域及 16 元域上两类 Hermitian 码给出了完全的权分布。

关键词: Hermitian 码; Hamming 权; 完全权分布

中图分类号: O157.4 **文献标识码:** A **文章编号:** 0529-6579 (2003) S1-0250-04

自从代数几何码出现以来, Hermitian 码一直是最典型并被研究得最透彻的一类代数几何码, 其最小 Hamming 权^[1], 自同构群^[2]等已被彻底了解。最近由于 R. Pellikaan 等^[3]对广义 Hamming 权的推广 Feng-Rao 界的工作, Munuera 在文^[4]中完全确定了 Hermitian 码的所有广义 Hamming 权。为了 Hermitian 码最后可能的商业应用, 目前人们对一些具体的 Hermitian 码正在研究, 改进已有的解码算法及对解码算法进行性能分析^[5]。从理论上讲, Hermitian 码的完全权分布是目前代数几何码研究中最重要的问题之一, 从以后的可能商业应用而言, 其权分布对编码及解码算法的设计, 改进及性能分析也具关键作用。

目前对代数几何码的权分布, 较为重要的两个工作是文^[6]及^[7], 其重点是希望通过理论分析得到权分布尽可能多的知识, 但是两者应用到具体码上均不是很成功, 由文^[6]只可以得到部分知识, 其最好的应用是对椭圆曲线码, 由文^[7]对 Hermitian 码应用只可做到 9 元域上 Hermitian 码。本文结合理论分析及计算机应用对 4 元域及 16 元域上两类 Hermitian 码给出了完全的权分布。

1 预备知识

设 F_q 是 q 元有限域, $C \subset F_q^n$ 是一个 k 维线性子空间。对任意向量 $w \in C$ 定义其支集

$$\text{supp}(w) = \{i \mid w = (w_1, w_2, \dots, w_n), w_i \neq 0\}$$

定义此向量(或码字)的 Hamming 权

$$\text{wt}(w) = \#(\text{supp}(w))$$

其中 $\#$ 表示一个集合中元素个数。而码 C 的最小 Hamming 权(或最小距离)

$$d(C) = \min_{\substack{x \in C \\ w \neq 0}} \text{wt}(w)$$

称 C 是一个线性 $[n, k, d]$ 码, 一般而言, 它可用于纠 $\lfloor (d-1)/2 \rfloor$ 个错。记 A_i 是码 C 中权为 i 的码字个数, 那么 $\{A_0, A_1, \dots, A_n\}$ 称为码 C 的(完全)权分布, 显然这是码 C 的最重要的(理论上及应用上)一组参数。

F_{q^2} 上 Hermitian 曲线是由下述曲线 X

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

易知此对应一条光滑的代数曲线。众所周知它是达到 Hasse-Weil 界的所谓最大曲线。其亏格 $g = q(q-1)/2$ 。除无穷远点 Q 外, X 上另 q^3 个有理点 (x, y) (要求 $x, y \in F_{q^2}$)是由下述方法得到: 任取 $y \in F_{q^2}$, 由有限域知识 y^{q+1} 必在 $F_q \subset F_{q^2}$ 中, 而 $x^q + x$ 是 F_{q^2}/F_q 的迹算子, 故对每个这样的 $y^{q+1} \in F_q$, 共有 q 个 $x \in F_{q^2}$ 满足方程, y 有 q^2 个选择, 对每个固定 y , x 有 q 个选择, 故有 $qq^2 = q^3$ 个点 $P_1, P_2, \dots, P_{q^3}$ 。众所周知这是 X 上所有 (F_{q^2}) 有理点全体(包括 Q 共 $q^3 + 1$ 个)。

对任一个 X 上 F_{q^2} 有理函数 f , 考虑 f 在 $P = \{P_1, P_2, \dots, P_{q^3}\}$ 上的赋值向量 $ev(f) \in F_{q^2}^n$, $n = q^3$, $ev(f) = (f(P_1), \dots, f(P_{q^3}))$ 。取 $1, y, x, y^2, xy, x^2, \dots, y^a, \dots, y^u x^{a-u}$, 为上述函数, 由其赋值向量生成的 $F_{q^2}^n$ 的子空间即 Hermitian 码 C_m , 其中 $m = qu + (q+1)(a-u) = (q+1)a - u$ 是函数在无穷远点 Q 的最大可能阶数, 由代数几何码知识, C_m 是一个 $[n, k, d]$ 码, 其中

$$n = q^3$$

$$k = m - g + 1$$

$$d \geq q^3 - m$$

* 收稿日期: 2003-01-04

作者简介: 许楚芬(1977年生), 女, 助理讲师; E-mail: snake_chu@hotmail.com

此文中研究的第一个 Hermitian 码是 F_4 (即 $q = 2$, 曲线方程是 $x^2 + x = y^3$) 上的, 其中 $a = 2 = u$, 即 $C_4^{(4)}$ (over F_4), 这是一个 $[8, 4, 4]$ 自对偶码。另一个是 F_{16} (即 $q = 4$, 曲线方程是 $x^4 + x = y^5$) 上的 $C_{12}^{(16)}$, 即, $a = 2 = u, m = 12$, 这是一个 $[64, 7, 52]$ 码。由 MacWilliams 定理^[8], 由此也可求出 F_{16} 上 $C_{62}^{(16)}$ 这个对偶 $[64, 57, 2]$ 码的完全权分布。

2 理论分析

首先对码 C_m 的完全权分布有

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

其中 $B_i = \binom{n}{m-i} (q^{2(i-g+1)} - 1)$ 对 $i \geq 2g-1$ 成立^[6]。由于 B_i 不可以完全确定, 故由^[6]的这一主要结果无法知道 $A_n, A_{n-1}, \dots, A_d$ 。

在 $[8, 4, 4]$ Hermitian 码 $C_4^{(4)}$ 情形, 除 B_0 外其余 B_i 可完全确定如下:

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

由^[6]对椭圆曲线 (F_4 上 Hermitian 曲线 $g = 0$, 即是椭圆曲线) 分析知 $B_0 = 3H$, H 是除子 $4Q$ 线性等价于 $P_1 + P_2 + P_3 + P_4$ 的 $\{i_1, i_2, i_3, i_4\} \subset \{1, 2, 3, 4, 5, 6, 7, 8\}$ 的 $\{i_1, i_2, i_3, i_4\}$ 的个数, 由于 $P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8$ 按第 1 节的分析, 其中两两成对与 Q 共线, 故在这 4 条线 (每条线上有 Q 及两个 P 中点) 中任取两条, 由于线上两个 P 中点之和线性等价于 $2Q$ (注意 Q 处与 X 交点只有 Q), 故此两条线上 4 个点与 $4Q$ 线性等价, 即 $H \geq \binom{4}{2} = 6$ 。

定理 $H = 6$

证明 由于 Q 为椭圆曲线之零点, 则由^[6]中定理 6 知 X 的共 9 个 F_4 有理点之群同构于 $(Z/3Z) \oplus (Z/3Z)$, Q 对应 0 元素, $P_1, P_2, \dots, P_8$ 对应其它 8 个点, 为了证明定理, 由上述分析及椭圆曲线上群结构定义, 只需证对 $\forall a, b, c, d \in (Z/3Z) \oplus (Z/3Z)$, a, b, c, d 均非零且不同, 但 $a + b + c + d = 0$, 则 $\{a, b, c, d\} = \{a, -a, b, -b\}$ 即可。不妨设 4 个点为 $(i_1, j_1), (i_2, j_2), (i_3, j_3), (i_4, j_4)$, 则

$$i_1 + i_2 + i_3 + i_4 \equiv 0 \pmod{3}$$

$$j_1 + j_2 + j_3 + j_4 \equiv 0 \pmod{3}$$

若 $i_1, i_2, i_3, i_4, j_1, j_2, j_3, j_4$ 全不为 0, 则易知结论成立, 这种点只有 $(1, 1), (2, 2), (3, 3), (4, 4)$ 满足结论, 若有一个, 不妨设为 $i_1 = 0$, 且 i_2, i_3, i_4 全不为 0, 则由 $i_2 + i_3 + i_4 \equiv 0 \pmod{3}$, 知道 $i_2 = i_3 = i_4$, 故 $i_2,$

$i_3, i_4 \in (Z/3Z)$, 且全不同, 故 $j_2 + j_3 + j_4 \equiv 0 \pmod{3}$, 即 $j_1 = 0$, 则 $(i_1, j_1) = (0, 0)$, 矛盾。故 j_2, j_3, j_4 中必有另一个, 不妨设为 $j_2 = 0$, 故 j_1, j_2 不全为 0, 且不同, 故 $\{j_1, j_2\} = \{1, 2\}$ 即 $j_1 + j_2 \equiv 0 \pmod{3}$, 即

$$(i_1, j_1) + (i_2, j_2) = 0$$

$$(i_3, j_3) + (i_4, j_4) = 0$$

在 $(Z/3Z) \oplus (Z/3Z)$ 中成立, 结论成立。证毕。

我们注意到 $C_4^{(4)}$ 是自对偶码, 故很自然想用 $w(x, y)$ 满足 MacWilliams 恒等式^[8] 来确定惟一个不知道的 B_0 , 但经计算知, 对任何 B_0 , MacWilliams 恒等式均成立。即自对偶性无法提供 B_0 信息, 故只有用上述椭圆曲线知识确定 $B_0 = 18$ 。最后知 $C_4^{(4)}$ 的完全权分布是

$$A_8 = 21 \quad A_7 = 96 \quad A_6 = 24 \quad A_5 = 96$$

$$A_4 = 18 \quad A_3 = 0 \quad A_2 = 0 \quad A_1 = 0 \quad A_0 = 1$$

下面 F_{16} 对上 $[64, 7, 52]$ 码 $C_{12}^{(16)}$ 进行理论分析, 由 A_i 及 B_i 的关系我们有:

$$A_{64} = B_{12} - B_{11} + B_{10} - B_9 + B_8 - B_7 +$$

$$B_6 - B_5 - B_4 - B_3 + B_2 - B_1 = \sum_{i=0}^{12} (-1)^i B_i$$

$$A_{63} = \sum_{i=0}^{11} (12-i)(-1)^i B_i$$

$$A_{62} = 66B_0 - 55B_1 + 45B_2 - 36B_3 + 28B_4 - 21B_5 + 15B_6 - 10B_7 + 6B_8 - 3B_9 + B_{10}$$

$$A_{61} = -220B_0 + 165B_1 - 120B_2 + 84B_3 - 56B_4 + 35B_5 - 20B_6 + 10B_7 - 4B_8 + B_9$$

$$A_{60} = 495B_0 - 330B_1 + 210B_2 - 126B_3 + 70B_4 - 35B_5 + 15B_6 - 5B_7 + B_8$$

$$A_{59} = -792B_0 + 462B_1 - 252B_2 + 126B_3 - 56B_4 + 21B_5 - 6B_6 + B_7$$

$$A_{58} = 924B_0 - 462B_1 + 210B_2 - 84B_3 + 28B_4 - 7B_5 + B_6$$

$$A_{57} = -792B_0 + 330B_1 - 120B_2 + 36B_3 - 8B_4 + B_5$$

$$A_{56} = 495B_0 - 165B_1 + 45B_2 - 9B_3$$

$$A_{54} = 66B_0 - 11B_2 + b^2$$

$$A_{53} = -12B_0 + B_1$$

$$A_{52} = B_0$$

利用计算机的结果 (见以下第 3 节), 从 $A_{64}, A_{63}, \dots, A_{52}$ 的值可以求出 $B_0, B_1, \dots, B_{12}$ 的值, 如下:

$$A_{52} = 150000 \quad B_0 = 150000$$

$$A_{53} = 547200 \quad B_1 = 2347200$$

$$A_{54} = 846240 \quad B_2 = 16765440$$

$$A_{55} = 3175680 \quad B_3 = 74734080$$

$$A_{56} = 756400 \quad B_4 = 238765320$$

$$\begin{aligned}
A_{57} &= 15513600 & B_5 &= 591286080 \\
A_{58} &= 28595520 & B_6 &= 1184895840 \\
A_{59} &= 42658560 & B_7 &= 1948674240 \\
A_{60} &= 55296080 & B_8 &= 2602847760 \\
A_{61} &= 52137600 & B_9 &= 2730450240 \\
A_{62} &= 39601440 & B_{10} &= 2113927200 \\
A_{63} &= 17694720 & B_{11} &= 1073741760 \\
A_{64} &= 4553415 & B_{12} &= 268435455
\end{aligned}$$

由文[6]的基本定理,

$$B_{12} = 16^7, B_{11} = \binom{64}{1}(16^6 - 1),$$

$$B_{10} = \binom{64}{2}(16^5 - 1)$$

且

$$\max\{0, (12^{64} - i)(16^{i-5} - 1)\} \leq B_i \leq \binom{64}{i}(16^{(i/2)} - 1)$$

我们可验证上述 $B_0, B_1, \dots, B_{12}$ 满足这些结果, 这说明计算机的结果是完全可信的。

3 计算机计算

设 $F_4 = \{0, 1, w, w^2\}$, 我们知 $C_4^{(4)}$ 是由下述矩阵的行向量张成的 F_4^4 的 4 维线性子空间

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & w & w & w & w^2 & w^2 & w^2 \\
0 & 0 & 1 & w & w^2 & 1 & w & w^2 \\
0 & 0 & 1 & w^2 & w & 1 & w^2 & w
\end{pmatrix}$$

设 $F_{16} = \{0, 1, w, w^2, \dots, w^{14}\}$, 已知 $C_{12}^{(16)}$ 是由下述矩阵的行向量张成的 F_{16}^{64} 的 7 维线性子空间,

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & w & 1 & w & w^2 & 1 & 0 \\
1 & w^3 & w & w^6 & w^4 & w^2 & w^9 & 0 \\
1 & w^6 & w & w^{12} & w^7 & w^2 & w^3 & 0 \\
1 & w^9 & w & w^3 & w^{10} & w^2 & w^{12} & 0 \\
1 & w^{12} & w & w^9 & w^{13} & w^2 & w^6 & 0 \\
1 & 1 & w^2 & 1 & w^2 & w^4 & 1 & 0 \\
1 & w^3 & w^2 & w^6 & w^4 & w^4 & w^9 & 0 \\
1 & w^6 & w^2 & w^{12} & w^8 & w^4 & w^3 & 0 \\
1 & w^9 & w^2 & w^3 & w^{11} & w^4 & w^{12} & 0 \\
1 & w^{12} & w^2 & w^9 & w^{14} & w^4 & w^6 & 0 \\
1 & w^2 & w^3 & w^4 & w^5 & w^6 & w^6 & 0 \\
1 & w^5 & w^3 & w^{10} & w^8 & w^6 & 1 & 0 \\
1 & w^8 & w^3 & w & w^{11} & w^6 & w^9 & 0 \\
1 & w^{10} & w^3 & w^7 & w^{14} & w^6 & w^3 & 0
\end{pmatrix}^T$$

$$\begin{pmatrix}
1 & w^{14} & w^3 & w^{13} & w^2 & w^6 & w^{12} \\
1 & 1 & w^4 & 1 & w^4 & w^8 & 1 \\
1 & w^3 & w^4 & w^6 & w^7 & w^8 & w^9 \\
1 & w^6 & w^4 & w^{12} & w^{10} & w^8 & w^3 \\
1 & w^9 & w^4 & w^3 & w^{13} & w^8 & w^{12} \\
1 & w^{12} & w^4 & w^9 & w & w^8 & w^6 \\
1 & 0 & w^5 & 0 & 0 & w^{10} & 0 \\
1 & w & w^6 & w^2 & w^7 & w^{12} & w^3 \\
1 & w^4 & w^6 & w^8 & w^{10} & w^{12} & w^{12} \\
1 & w^7 & w^6 & w^{14} & w^{13} & w^{12} & w^6 \\
1 & w^{10} & w^6 & w^5 & w & w^{12} & 1 \\
1 & w^{13} & w^6 & w^{11} & w^4 & w^{12} & w^9 \\
1 & w & w^7 & w^2 & w^8 & w^{14} & w^3 \\
1 & w^4 & w^7 & w^8 & w^{11} & w^{14} & w^{12} \\
1 & w^7 & w^7 & w^{14} & w^{14} & w^{14} & w^6 \\
1 & w^{10} & w^7 & w^5 & w^2 & w^{14} & 1 \\
1 & w^{13} & w^7 & w^{11} & w^5 & w^{14} & w^9 \\
1 & 1 & w^8 & 1 & w^8 & w & 1 \\
1 & w^3 & w^8 & w^6 & w^{11} & w & w^9 \\
1 & w^6 & w^8 & w^{12} & w^{14} & w & w^3 \\
1 & w^9 & w^8 & w^3 & w^2 & w & w^{12} \\
1 & w^{12} & w^8 & w^9 & w^5 & w & w^6 \\
1 & w & w^9 & w^2 & w^{10} & w^3 & w^3 \\
1 & w^4 & w^9 & w^8 & w^{13} & w^3 & w^{12} \\
1 & w^7 & w^9 & w^{14} & w & w^3 & w^6 \\
1 & w^{10} & w^9 & w^5 & w^4 & w^3 & 1 \\
1 & w^{13} & w^9 & w^{11} & w^7 & w^3 & w^9 \\
1 & 0 & w^{10} & 0 & 0 & w^5 & 0 \\
1 & w^2 & w^{11} & w^4 & w^{13} & w^7 & w^6 \\
1 & w^5 & w^{11} & w^{10} & w & w^7 & 1 \\
1 & w^8 & w^{11} & w & w^4 & w^7 & w^9 \\
1 & w^{10} & w^{11} & w^7 & w^7 & w^7 & w^3 \\
1 & w^{14} & w^{11} & w^{13} & w^{10} & w^7 & w^{12} \\
1 & w^2 & w^{12} & w^4 & w^{14} & w^9 & w^6 \\
1 & w^5 & w^{12} & w^{10} & w^2 & w^9 & 1 \\
1 & w^8 & w^{12} & w & w^5 & w^9 & w^9 \\
1 & w^{10} & w^{12} & w^7 & w^8 & w^9 & w^3 \\
1 & w^{14} & w^{12} & w^{13} & w^{11} & w^9 & w^{12} \\
1 & w & w^{13} & w^2 & w^{14} & w^{11} & w^3 \\
1 & w^4 & w^{13} & w^8 & w^2 & w^{11} & w^{12} \\
1 & w^7 & w^{13} & w^{14} & w^5 & w^{11} & w^6 \\
1 & w^{10} & w^{13} & w^5 & w^8 & w^{11} & 1 \\
1 & w^{13} & w^{13} & w^{11} & w^{11} & w^{11} & w^9 \\
1 & w^2 & w^{14} & w^4 & w & w^{13} & w^6 \\
1 & w^5 & w^{14} & w^{10} & w^4 & w^{13} & 1 \\
1 & w^8 & w^{14} & w & w^7 & w^{13} & w^9 \\
1 & w^{10} & w^{14} & w^7 & w^{10} & w^{13} & w^3 \\
1 & w^{14} & w^{14} & w^{13} & w^{13} & w^{13} & w^{12}
\end{pmatrix}$$

算法 (仅列出 $[64, 7, 52]$ 码的权分布的算法, $[8, 4, 4]$ 码的权分布的算法类似可得)

(1) 编制一个 F_{16} 的加法表。

(2) 定义 7 个一维数组 $x_i[64]$, ($i = 0, \dots, 6$), 分别储存 $1, y, xy^2, yx, x^2, y^3$ 共 7 个向量。

(3) 令 $c_i = j, j = 0, 1, \dots, 15$; 计算 $c_i * x_i$, 并储存在二维数组 $a_i[16][64]$ 中。

(4) 用穷举法列出所有 $\sum_{i=0}^6 [16][64]$, 共有 16^7 个向量, 这个向量组成 $1, y, x, y^2, yx, x^2, y^3$, 7 个向量在 F_{16}^{64} 中张成的子空间 C 。

(5) 数出 C 中每个向量含“0”元素的个数。

(6) 求出 C 在 i 个位置为零的向量个数, 即 A_{64-i} , 全部求出即得上述 $[64, 7, 52]$ 码的权分布。

算法改进

(1) 由于计算 16^7 个含 64 个元素的向量并不是一件容易的事情, 即使是比较好的 PC 机, 也要花上好几天的时间, 因此算法必须改进。考虑到 1 与 c_0 的乘积, 实际上是 1 中每个元素与 c_0 的乘积, 而 1 中每个元素均为 1, 乘以 c_0 后每个元素仍相同, 所以可以利用该性质对算法进行改进。只计算 16^6 个含 64 个元素的向量, 即先不考虑 $c_0 1$, 再利用 16^6 的结果, 推算出全部 16^7 个向量的含零元素的个数。

(2) 由于有些计算机因硬件因素的限制, 不能定义 16^7 个二维数组, 甚至连 16^6 个数组也办不到, 因此只利用一个一维数组存储向量, 计算出一个向量后, 马上对其进行数“数零”, 数完后再计算下一个向量, 这样大大节省了内存空间。

结果

(1) $[8, 4, 4]$ 码的权分布:

$$A_0 = 1 \quad A_1 = 0 \quad A_2 = 0 \quad A_3 = 0 \quad A_4 = 18$$

$$A_5 = 96 \quad A_6 = 24 \quad A_7 = 96 \quad A_8 = 21$$

(2) $[64, 7, 52]$ 码的权分布:

$$A_0 = 0 \quad A_1 = 0 \quad A_2 = 0 \cdots$$

$$A_{51} = 0 \quad A_{52} = 150000 \quad A_{53} = 547200$$

$$A_{54} = 846240 \quad A_{55} = 3175680 \quad A_{56} = 7565400$$

$$A_{57} = 15513600 \quad A_{58} = 28595520 \quad A_{59} = 42658560$$

$$A_{60} = 55396080 \quad A_{61} = 52137600$$

$$A_{62} = 39601440 \quad A_{63} = 17694720 \quad A_{64} = 4553415$$

参考文献:

- [1] YANG K, KUMARA P V. On the true minimum distances of Hermitian codes[J]. Lect Notes in Math, 1992, 1518: 99 - 107.
- [2] XING C. On automorphism groups of the Hermitian codes [J]. IEEE Trans Inform Theory, 1995, 41: 1629 - 1635.
- [3] HEIJNEN P, PELLIKAN R. Generalized Hamming weights of q -ary Reed-Muller codes[J]. IEEE Trans Inform Theory, 1998, 44: 181 - 197.
- [4] MUNUERA C. The weight hierarchy of Hermitian codes[J]. J Discrete Math, 2000, 139(1): 79 - 104.
- [5] JENSEN H E, NELSON R R, HOLDT T. Performance analysis of a decoding for algebraic geometric codes[J]. DTU Mat-Report No. 1998 - 09.
- [6] KATSMAN G L, TSFASMAN M. Spectra of algebraic geometry codes[J]. Probl Inform Trans, 1987, 23: 262 - 275.
- [7] DUURSMA I M. Weight distribution of geometric Goppa codes[J]. Trans AMS, 1999.
- [8] van LINT J H. Introduction to coding theory[M]. Springer-Verlag, 1982: GTM 86.

The Weight Distribution of Hermitian Code

XU Chu-fen

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

Abstract: The complete weight distribution of Hermitian code is one of the most important problems in algebraic code research. Here, based on theoretical analysis and computer applications, the complete weight distributions of 4-variable and 16-variable domain are both obtained.

Key words: Hermitian code; Hermitian weight; distribution of complete distribution