关于 Goppa 码、 BCH 码的广义 Hamming 重量 [1]

岳殿武 胡正名 *

(南京邮电学院通信工程系 186 信箱 南京 210003)
*(北京邮电大学信息工程系 145 信箱 北京 100876)

摘 要 本文研究了 Goppa 码、 BCH 码的广义 Hamming 重量，给出了 Goppa 码的广义 Hamming 重量的一个下界以及求该下界的一个算法；对于本原、狭义 BCH 码，给出了后面一些广义 Hamming 重量的确切值。

关键词 广义 Hamming 重量， Goppa 码， BCH 码

中图号 TN911.2

1 引 言

1991 年， V.K.Wei 提出了广义 Hamming 重量这一新的概念 [1] ，引起了国内外不少学者对广义 Hamming 重量的研究兴趣 [2−6] 。广义 Hamming 重量是线性码的一个基本描述参数，它在编码、密码研究中均有应用 [1,2] 。下面先简述一下广义 Hamming 重量的定义及其基本性质。

令 Ψ 表示码长为 n 、 F_q 上的分组码，定义 Ψ 的支集为

$$X(\Psi)=\{i|\exists c=(c_1,c_2,\cdots,c_n)\in\Psi,\quad c_i\neq 0\}.$$

令 C 表示 F_q 上的一个 $[n,k]$ 线性码。对于 $1\leq r\leq k$ ，我们定义 C 的第 r 广义 Hamming 重量为

$$d_r(C)=\min\{|X(\Psi)|:\Psi是C的任意一个r维子码\}.$$

我们称集合 $\{d_r(C)|1\leq r\leq k\}$ 为码 C 的重量谱系。

关于码 C 的广义 Hamming 重量有如下几个重要的基本性质：

(1) 单调性 $1\leq d_1(C)<d_2(C)<\cdots<d_k(C)\leq n$ 。

(2) 对偶性 令 $C^{\perp}$ 表示 C 的对偶码，则

$$\{d_u(C^{\perp})|1\leq u\leq n-k\}=\{1,2,\cdots,n\}-\{n+1-d_r(C)|1\leq r\leq k\}.$$

(3) 广义 Singleton 界 $d_r(C)\leq n-k+r,\ r=1,2,\cdots,k$ 。

下面一个基本结果在第 2 节中很有用途。

定理 1[2,3] 令 H 表示码 C 的一致校验矩阵， d^* 表示某一正整数，则第 r 广义 Hamming 重量 $d_r(C)=d^*$ ，当且仅当如下两个条件成立：

(1) 对于 H 的任意 d^*-1 列，其秩不少于 d^*-r 。

(2) 在 H 中有 d^* 列，其秩为 d^*-r 。

本文研究了 Goppa 码、 BCH 码的广义 Hamming 重量问题。由于求出 Goppa 码的真正最小距离——第一广义 Hamming 重量是十分困难的问题 [4] ，因此我们的研究策略是给

[1] 1997-08-01 收到， 1998-03-09 定稿
国家自然科学基金资助课题

出比较好的 Goppa 码广义 Hamming 重量的界. 在第 2 节中, 我们给出了 Goppa 码的广义 Hamming 重量的一个下界以及求该下界的算法. 文献 [3,5,6] 研究了纠两个错、纠三个错的本原、狭义 BCH 码的广义 Hamming 重量, 给出了第二、第三广义 Hamming 重量的确切值. 在第 3 节中, 我们考虑了 Goppa 码的特例——一般本原、狭义 BCH 码, 给出了后面一些广义 Hamming 重量的确切值.

2 Goppa 码的广义 Hamming 重量下界

令 F_{q^m} 表示一个有限域, 其中 q 为一个素数幂, m 为一个非负的整数.

定义 1 令 $L=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}\subset F_{q^m}$ 表示位置集, $g(z)=\Pi_{l=1}^{s}(z-\beta_l)^{r_l}$ 表示生成多项式, 它是 F_{q^m} 上的多项式, 满足 $g(\alpha_i)\neq 0, i=1,2,\cdots,n$, 则 Goppa 码 $\Gamma(L,g)$ 就是满足下式的 F_q 上的 n 元向量 $a=(a_1,a_2,\cdots,a_n)$ 的全体:

$$\sum_{i=1}^{n}\frac{a_i}{z-\alpha_i}\equiv 0 \mod(g(z)).$$

对于上述 Goppa 码 $\Gamma(L,g)$, 记 $r=\deg(g(z))$, 则其一致校验矩阵通常为 [4]

$$B=\begin{bmatrix}1 & 1 & \cdots & 1\\ \alpha_1 & \alpha_2 & \cdots & \alpha_n\\ \vdots & \vdots & \cdots & \vdots\\ \alpha_1^{r-1} & \alpha_2^{r-1} & \cdots & \alpha_n^{r-1}\end{bmatrix}\begin{bmatrix}g(\alpha_1)^{-1} & & & \\ & g(\alpha_2)^{-1} & & \\ & & \ddots & \\ & & & g(\alpha_n)^{-1}\end{bmatrix}.$$

由文献 [7] 知, Goppa 码 $\Gamma(L,g)$ 的一致校验矩阵等价于

$$H=[B_1,B_2,\cdots,B_s]^T=(h_{ij}),$$

其中 $B_i, i=1,2,\cdots,s$ 表示矩阵:

$$B_i=\begin{bmatrix}(\alpha_1-\beta_i)^{-1} & (\alpha_2-\beta_i)^{-1} & \cdots & (\alpha_n-\beta_i)^{-1}\\ (\alpha_1-\beta_i)^{-2} & (\alpha_2-\beta_i)^{-2} & \cdots & (\alpha_n-\beta_i)^{-2}\\ \vdots & \vdots & \vdots & \vdots\\ (\alpha_1-\beta_i)^{-r_i} & (\alpha_2-\beta_i)^{-r_i} & \cdots & (\alpha_n-\beta_i)^{-r_i}\end{bmatrix}.$$

记 $H^*=[H,H^{(1)},H^{(2)},\cdots,H^{(m-1)}]^T$, 这里 $H^{(b)}=(h_{ij}^{q^b})$, $b=1,2,\cdots,m-1$.

引理 1[8] H^* 与 H 等价, 即 H^* 也可作为 $\Gamma(L,g)$ 的一致校验矩阵.

引理 2[8] 若 $x_1,x_2,\cdots,x_s$ 互不相同, $a_1,a_2,\cdots,a_u$ 互不相同, 且

$$(x_i+a_j)\neq 0,\qquad 1\leq i\leq s,\quad 1\leq j\leq u,$$

则下面矩阵 E 的秩为 u.

$$E=[E_1,E_2,\cdots,E_s]^T,$$

这里 E_i, $i=1,2,\cdots,s$ 表示成矩阵为

$$E_i=\begin{bmatrix}(x_1+a_i)^{-1} & (x_2+a_i)^{-1} & \cdots & (x_n+a_i)^{-1}\\ (x_1+a_i)^{-2} & (x_2+a_i)^{-2} & \cdots & (x_n+a_i)^{-2}\\ \vdots & \vdots & \vdots & \vdots\\ (x_1+a_i)^{-\lambda_i} & (x_2+a_i)^{-\lambda_i} & \cdots & (x_n+a_i)^{-\lambda_i}\end{bmatrix},$$

其中 λ_i 满足 $\sum_{i=l}^{s}\lambda_i=u$ 。

将 H^* 中重复行删除，并对剩下的所有行进行重排，所得矩阵记为 Q ， Q 可表示为 $Q=[Q_1,Q_2,\cdots,Q_s]^T$ 。这里 Q_i ， $i=1,2,\cdots,s$ 表示为

$$Q_i=\begin{bmatrix}(\alpha_1-\beta_i)^{-p(1,i)} & (\alpha_2-\beta_i)^{-p(1,i)} & \cdots & (\alpha_n-\beta_i)^{-p(1,i)}\\ (\alpha_1-\beta_i)^{-p(2,i)} & (\alpha_2-\beta_i)^{-p(2,i)} & \cdots & (\alpha_n-\beta_i)^{-p(2,i)}\\ \vdots & \vdots & \vdots & \vdots\\ (\alpha_1-\beta_i)^{-p(b_i,i)} & (\alpha_2-\beta_i)^{-p(b_i,i)} & \cdots & (\alpha_n-\beta_i)^{-p(b_i,i)}\end{bmatrix},$$

其中 $1=p(1,i)<p(2,i)<\cdots<p(b_i,i)$ 。选取 Q_i ， $i=1,2,\cdots,s$ 的一部分组成一个新矩阵 R ， $R=[R_1,R_2,\cdots,R_s]^T$ 。这里 R_i ， $i=1,2,\cdots,s$ 表示为

$$R_i=\begin{bmatrix}(\alpha_1-\beta_i)^{-p(1,i)} & (\alpha_2-\beta_i)^{-p(1,i)} & \cdots & (\alpha_n-\beta_i)^{-p(1,i)}\\ (\alpha_1-\beta_i)^{-p(2,i)} & (\alpha_2-\beta_i)^{-p(2,i)} & \cdots & (\alpha_n-\beta_i)^{-p(2,i)}\\ \vdots & \vdots & \vdots & \vdots\\ (\alpha_1-\beta_i)^{-p(n_i,i)} & (\alpha_2-\beta_i)^{-p(n_i,i)} & \cdots & (\alpha_n-\beta_i)^{-p(n_i,i)}\end{bmatrix},$$

其中 $1\le n_i\le b_i$ ， $1\le i\le s$ 。

定理 2 给定正整数 $\nu\le n$ ，如果 $\sum_{i=1}^{s}p(n_i,i)\le\nu-1$ ，那么 Q 的任何 $\nu-1$ 列，其秩至少为 $\sum_{i=1}^{s}n_i$ 。

证明 任取 Q 的 $\nu-1$ 列—— $i_1,i_2,\cdots,i_{\nu-1}$ 列，这些列所组成的矩阵记为 J 。显然，在 J 中存在 $N\times N^*$ 阶子矩阵 $U=[U_1,U_2,\cdots,U_s]^T$ ，其中 $N=\sum_{i=1}^{s}n_i$ ， $N^*=\sum_{i=1}^{s}p(n_i,i)$ ，而 $U_i,i=1,2,\cdots,s$, 表示为

$$U_i=\begin{bmatrix}(\alpha_{i_1}-\beta_i)^{-p(1,i)} & (\alpha_{i_2}-\beta_i)^{-p(1,i)} & \cdots & (\alpha_{i_{N^*}}-\beta_i)^{-p(1,i)}\\ (\alpha_{i_1}-\beta_i)^{-p(2,i)} & (\alpha_{i_2}-\beta_i)^{-p(2,i)} & \cdots & (\alpha_{i_{N^*}}-\beta_i)^{-p(2,i)}\\ \vdots & \vdots & \vdots & \vdots\\ (\alpha_{i_1}-\beta_i)^{-p(n_i,i)} & (\alpha_{i_2}-\beta_i)^{-p(n_i,i)} & \cdots & (\alpha_{i_{N^*}}-\beta_i)^{-p(n_i,i)}\end{bmatrix},$$

因为矩阵 U 又是 $N^*\times N^*$ 阶矩阵 $V=[V_1,V_2,\cdots,V_s]^Y$ 的子矩阵，这里 V_i ， $i=1,2,\cdots,s$ 为

$$V_i=\begin{bmatrix}(\alpha_{i_1}-\beta_i)^{-1} & (\alpha_{i_2}-\beta_i)^{-1} & \cdots & (\alpha_{i_{N^*}}-\beta_i)^{-1}\\ (\alpha_{i_1}-\beta_i)^{-2} & (\alpha_{i_2}-\beta_i)^{-2} & \cdots & (\alpha_{i_{N^*}}-\beta_i)^{-2}\\ \vdots & \vdots & \vdots & \vdots\\ (\alpha_{i_1}-\beta_i)^{-p(n_i,i)} & (\alpha_{i_2}-\beta_i)^{-p(n_i,i)} & \cdots & (\alpha_{i_{N^*}}-\beta_i)^{-p(n_i,i)}\end{bmatrix},$$

由于 $g(\alpha_j)\ne 0$ ，知 $\alpha_j-\beta_i\ne 0$ ，且 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 互不相同， $-\beta_1,-\beta_2,\cdots,-\beta_s$ 互不相同，所以矩阵 V 满足引理 2 的条件， V 的秩为 N^* 。而 U 的所有行均在 V 中，故 U 的行

秩为 N， U 的列秩亦为 N，则 J 的列秩至少为 N。这样 Q 的任何 $\nu-1$ 列，其秩应至少为 $N=\sum_{i=1}^{s}n_i$。 证毕

定理 3 给出一个正整数 $\nu\le n$。记 $N=\max\{\sum_{i=1}^{s}n_i|\sum_{i=1}^{s}p(n_i,i)\le\nu-1\}$，$r=\nu-N$，则 $d_r(\Gamma(L,g))\ge\nu$。

证明 因为 Q 与 H^* 等价，所以 Q 也是 Goppa 码 $\Gamma(L,g)$ 的一致校验矩阵。再由定理 1 和定理 2 即得证。 证毕

下面我们给出求 N 的一个算法。

求 N 的算法：先给定一个正整数 $\nu\ge n$。

第 1 步 令 N=0, $p(n_i,i)=0$, $i=1,2,\cdots,s$。 $J_i=\{p(1,i),p(2,i),\cdots,p(b_i,i)\}$。

第 2 步 取 $p=\min\{x|x\in\bigcup_{i=1}^{s}J_i\}$。不妨设 $p\in J_{i_0}$。令

$$p(n_i,i)=\begin{cases}p, & i=i_0;\\ p(n_i,i), & i\ne i_0.\end{cases}$$

第 3 步 首先判定 $\sum_{i=1}^{s}p(n_i,i)\le\nu-1$ 是否成立。如果成立，则进行第 4 步；否则，结束运算，现在的 N 即为所求。

第 4 步 令 $N=N+1$， $J_{i_0}=J_{i_0}-\{p\}$ 转到第 2 步。

命题 1 记 Goppa 码 $\Gamma(L,g)$ 的维数为 k，则 $d_r(\Gamma(L,g))=n$。

证明 假设 $d_r(\Gamma(L,g))<n$，则存在某个 $i\in\{1,2,\cdots,n\}$ 使得对任意的 $\Gamma(L,g)$ 的码字 $a=(a_1,a_2,\cdots,a_n)$，均有 $a_i=0$。不妨设 $i=1$，则存在一个 $r\times r$ 阶的可逆矩阵 p 使得 $H'=PH$，这里 $r=\deg(g(z))$，而 H' 的第一列为全零列。设 H' 的前 r 列所组成的矩阵记为 W'， H 的前 r 列所组成的矩阵记为 W，则 $W'=PW$，且行列式

$$|W'|=|PW|=|P||W|=0,$$

这样 $|W|=0$。这是不可能的。故假设不成立， $d_r(\Gamma(L,g))=n$。 证毕

3 本原 BCH 码的一些广义 Hamming 重量的确定

设正整数 $s\le q^m-2$，记 C_s 为关于 s 的以 q^m-1 为模的分圆陪集 [4]。设 α 表示 F_{q^m} 的本原元，记

$$M^{(s)}(x)=\prod_{i\in C_s}(x-\alpha^i).$$

定义 2 设 C 为码长 $n\le q^m-1$、 F_q 上的循环码，给定正整数 δ，整数 h，若 C 生成多项式表示为

$$g(x)=\text{l.c.m}\{M^{(h)}(x),M^{(h+1)}(x),\cdots,M^{(h+\delta-2)}(x)\},$$

(其中 l.c.m. 表示最小公倍)，则称 C 为码长为 n 设计距离为 δ 的关于 h 的一个 q 元 BCH 码。若 $h=1$，则称 C 为狭义 BCH 码；若 $n=q^m-1$，则称 C 为本原 BCH 码。对于本原狭义 BCH 码简记为 $B(\delta)$。

对于本原狭义 BCH 码 $B(\delta)$，令 α 表示 F_{q^m} 的本原元。其一致校验矩阵为 [4]

$$H=\begin{bmatrix}1 & \alpha & \cdots & \alpha^{n-1}\\ 1 & \alpha^2 & \cdots & \alpha^{2(n-1)}\\ \vdots & \vdots & \vdots & \vdots\\ 1 & \alpha^{\delta-1} & \cdots & \alpha^{(\delta-1)(n-1)}\end{bmatrix}=(h_{ij}).$$

记 $H^*=[H,H^{(1)},H^{(2)},\cdots,H^{(m-1)}]^T$ ，这里 $H^{(b)}=(h_{ij}^{q^b})$ ， $b=1,2,\cdots,m-1$ 。将 H^* 的重复的行删去，并对行进行重排，所得的矩阵为

$$Q=\begin{bmatrix}1 & \alpha^{p_1} & \cdots & \alpha^{(n-1)p_1}\\ 1 & \alpha^{p_2} & \cdots & \alpha^{(n-1)p_2}\\ \vdots & \vdots & \vdots & \vdots\\ 1 & \alpha^{p_l} & \cdots & \alpha^{(n-1)p_l}\end{bmatrix}.$$

这里 $p_1,p_2,\cdots,p_l$ 满足 $1=p_1<p_2<\cdots<p_l$ 。

由于本原狭义 BCH 码是 Goppa 码子类 [4] ，故由第 2 节讨论，易得出如下结果。

推论 1 给定整数 ν ， $1\le\nu\le n$ ，若有 j 使 $p_j\le\nu-1$ ，则

$$d_r(B(\delta))\ge\nu,\qquad r=\nu-j.$$

推论 2 令 k 表示码 $B(\delta))$ 的维数，则

$$d_{k-u}(B(\delta))=n-u,\quad u=0,1,2,\cdots,n-N(\delta)-1.$$

证明 因为 $p_l=N(\delta)$ ，故由推论 1 得

$$d_{N(\delta)-l+1}(B(\delta))\ge N(\delta)+1.$$

既然 $n-k=|\bigcup_{i=1}^{\delta-1}C_i|$ ，那么 $l=n-k$ ，则 $d_{N(\delta)-n+k+1}(B(\delta))\ge N(\delta)+1$ 。由广义 Hamming 重量的广义 Singleton 界知

$$d_{N(\delta)-n+k+1}(B(\delta))\le n-k+N(\delta)-n+k+1=N(\delta)+1.$$

这样 $d_{N(\delta)-n+k+1}(B(\delta))=N(\delta)+1$ ，即 $d_{k-u}(B(\delta))=n-u$ ， $u=n-(N(\delta)+1)$ 。再由广义 Hamming 重量的单调性和广义 Singleton 界我们不难证得

$$d_{k-u}(B(\delta))=n-u,\quad u=1,2,\cdots,n-N(\delta)-1.$$

因此此推论成立。　　证毕

参 考 文 献

[1] Wei V K. Generalized Hamming weights for linear codes. IEEE Trans. on IT, 1991, IT-37(5): 1412–1418.

[2] Wei V K, Yang K. On the generalized Hamming weights of product codes. IEEE Trans. on IT, 1993, IT-39(5): 1709–1713.

[3] Feng G L, *et al.* On the generalized Hamming weights for several classes of cyclic codes. IEEE Trans. on IT, 1992, IT-38(3): 1125–1130.

[4] Mac Williams F J, Sloane N J A. The Theory of Error-Corrorecting Codes. Amsterdam: North-Holland Publishing Company, 1997, Chapter 9 and Chapter 12.

[5] Van der Geer G, van der Vlugt M. On the generalized Hamming weights of BCH codes. IEEE Trans. on IT, 1994, IT-40(2): 543–546.

[6] Chung H. The 2-nd Generalized Hamming Weights of Double-Error-Correcting Binary BCH Codes and Their Dual Codes. In: Lecture Note in Computer Scicence, Vol.539, AAECC-9, New York: Springer-Verlag, 1991, 118–129.

[7] Tzeng K K, Zimmermann K. On extending Goppa codes to cyclic codes. IEEE Trans. on IT, 1975, IT-21(6): 712–716.

[8] 冯贵良. Goppa 码最小距离下限和维数上限的扩张. 电子学报, 1983, 11(2): 66–72.

GENERALIZED HAMMING WEIGHTS FOR Goppa CODES AND BCH CODES

Yue Dianwu Hu Zhengming*

(*Dept. of Comm. Eng., Nanjing Institute of Posts and Telecomm., Nanjing* 210003)

*(*Dept. of Infor. Eng., Beijing University of Posts and Telecomm., Beijing*100088)

Abstract In this paper, generalized Hamming weights for Goppa codes and BCH codes are studied. Lower bounds of generalized Hamming weights for Goppa codes are obtained and an algorithm to find the lower bounds is given. Moreover, the last few generalized Hamming weights for narrow and primitive BCH codes are determined.

Key words Generalized Hamming weight, Goppa code, BCH code

岳殿武: 男, 1965 年生, 博士, 副教授, 从事纠错编码与信息安全方面的教学和科研工作.
胡正名: 男, 1931 年生, 教授, 博士生导师, 从事应用数学和信息科学方面的教学和科研工作.