关于 q 元 BCH 码的维数和最小距离 [1]

岳殿武 胡正名

(北京邮电大学信息工程系 181 信箱 北京 100088)

摘 要 本文讨论的是 q 元狭义本原 BCH 码，以下简称 BCH 码。首先给出了一定条件下求 BCH 码维数的一般公式，该结果改进了 MacWilliams 等人 (1977) 的结果。然后给出了求 BCH 码维数的一般迭代方法。此外，本文还指出了 BCH 码的最小距离的 BCH 界是分圆陪集首，我们猜测 BCH 码的最小距离也是分圆陪集首。

关键词 BCH 码，分圆陪集，维数，最小距离

中图号 TN911.22

1 引 言

BCH 码是一类很重要的纠错码。自从它产生以来，人们就对它进行了广泛的讨论。

本文对 q 元狭义本原 BCH 码进行了讨论。首先给出了 BCH 码的维数表示定理，然后推出了在一定条件下求 BCH 码维数的通用公式。该结果改进了文献 [1] 第 263 页中推论 8 。(注：那里的二元 BCH 码是指二元狭义本原 BCH 码，不是一般的二元 BCH 码。参见文献 [1] 第 258 页中注记。) 并且，我们还给出了求 BCH 码维数的一般迭代方法。最后，通过对近年来关于 BCH 码最小距离结果分析，我们给出了关于 BCH 码最小距离的两个猜测。

2 求 q 元 BCH 码的维数

定义 1 设正整数 $s \le q^m - 2$, $s \cdot q^{m_s} = s \bmod (q^m - 1)$，称集合 $\{s, sq, \cdots, sq^{m_s-1}\}$ 为以 $q^m - 1$ 为模关于 s 的分圆陪集 (或循环陪集)，记它为 C_s 。记 $a_s = \min_{p \in C_s} p$，称 a_s 为分圆陪集 C_s 首元，简称为分圆陪集首。称集合 $\{a_s | \ 0 < s \le q^m - 2\}$ 为以 $q^m - 1$ 为模的分圆陪集首集，记为 A_m 。

定义 2[1] 设 α 表示 GF(q^m) 的本原元，记

$$M^{(s)}(x) = \prod_{i \in C_s} (x - \alpha^i). \tag{1}$$

[1] 1994-11-01 收到，1995-02-27 定稿
国家自然科学基金资助课题

设 C 为码长 $n \le q^m - 1$ 的 GF(q) 上循环码，如果对某 $\delta > 0$，其生成多项式表示为

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

其中 $b \ge 0$，则称 C 为设计距离为 δ 的一个 q 元 BCH 码。若 $b = 1$，则称为狭义 BCH 码；若 $n = q^m - 1$，则称为本原 BCH 码。我们要讨论的就是 $b = 1$， $n = q^m - 1$ 情况下的 BCH 码——狭义本原 BCH 码，以下简称 BCH 码。

定义关于 A_m 的一个符号函数如下

$$u_i = \begin{cases} 1, & i \in A_m; \\ 0, & i \notin A_m. \end{cases} \tag{3}$$

定理 1 q 元 BCH 码的维数可表示为

$$\dim C = n - \sum_{i=1}^{\delta-1} |C_i| \cdot u_i. \tag{4}$$

证明 因为 $\dim C = n - \deg(g(x))$，而 $g(x)$ 的次数就是集合 $\bigcup_{i=1}^{\delta-1} C_i$ 的元素个数，所以 $\dim C = n - \left|\bigcup_{i=1}^{\delta-1} C_i\right|$。($X$ 为一集合，用 $|X|$ 表示 X 的元素个数，以下同) 对于每个 C_i，显然有 $a_i \le i$；又若 $a, b \in A_m$，则 $C_a \cap C_b = \phi$，所以由 u_i 这一符号定义可知 (4) 式成立。

引理 1[1] $0 < s \le q^m - 2$, $|C_s| | m$。

引理 2[2] 设 $s \in A_m$, $m = p \cdot v$，则 $|C_s| | p$ 充要条件是存在正整数 r，使 s 可表示为

$$s = r \cdot [q^{(v-1)p} + q^{(v-2)p} + \cdots + q^p + 1]. \tag{5}$$

引理 3 如果 m 为素数，则

$$|C_s| = \begin{cases} 1, & s = q^{m-1} + q^{m-2} + \cdots + 1; \\ m, & \text{其它}. \end{cases} \tag{6}$$

证明 由引理 1 和引理 2 知，如 m 为素数，则应有 $v = m, p = 1$ 或 $v = 1, p = m$。如果 $v = m, p = 1$，则有 $s = q^{m-1} + q^{m-2} + \cdots + 1$, $|C_s| = 1$；如果 $v = 1, p = m$，则 $|C_s| = m$, $s \ne q^{m-1} + q^{m-2} + \cdots + 1$。

因此由定理 1 和引理 3 不难得定理 2。

定理 2 若 m 为素数，则 BCH 码维数为

$$\dim C = \begin{cases} n - m \cdot \sum_{i=1}^{\delta-1} \delta_i, & \delta - 2 < q^{m-1} + q^{m-2} + \cdots + 1; \\ n - m \cdot \sum_{i=1}^{\delta-1} \delta_i + m - 1, & \text{否则}. \end{cases} \tag{7}$$

定义 3 设 t 为一个正整数，如果有集合 $\{s|s \le t, s \ne k \cdot q, k$ 为任意正整数 $\} \subset A_m$，则称 t 为 A_m 的一个非重复界，所有这些 t 中的最大者，则称为 A_m 的最大非重复界，记它为 T。

引理 4[2,3]

$$T = \begin{cases} q^{(m+1)/2} - 1, & m \text{ 为奇数;} \\ 2 \cdot q^{m/2} - 1, & m \text{为偶数.} \end{cases} \tag{8}$$

引理 5[2] (1) 当 m 为奇数时，$0 < s \le T$，则 $|C_s| = m$。(2) 当 m 为偶数，如果 $0 < s \le T$，则有 $|C_s| = m$，若 $s \ne q^{m/2} + 1$；$|C_s| = m/2$，若 $s = q^{m/2} + 1$。

定理 3 设 C 为设计距离为 δ 的 q 元 BCH 码，则

(1) 若 $\delta - 1 < q^{\lceil m/2 \rceil} + 1$ ($\lceil x \rceil$ 表示不小于 x 的最小整数，以下同)，则该 BCH 码维数为

$$\dim C = n - m \cdot [\delta^{(q)} \cdot (q-1) + \delta^{(0)}]. \tag{9}$$

(2) 若 m 为偶数，且 $q^{m/2} + 1 \le \delta - 1 < T + 2$，则该 BCH 码维数为

$$\dim C = n - m \cdot [\delta^{(q)} \cdot (q-1) + \delta^{(0)}] + m/2. \tag{10}$$

这里 $\delta^{(q)}, \delta^{(0)}$ 满足 $\delta - 1 = \delta^{(q)} \cdot q + \delta^{(0)}, 0 \le \delta^{(0)} < q$。

证明 (1) 由引理 4 和引理 5 知，当 $\delta - 1 < q^{\lceil m/2 \rceil} + 1$ 时，$|C_s| = m, i \le \delta - 1$。对于 $i = k \cdot q$，由定义 1 知，$C_i = C_k$，因此由引理 4 知，此时

$$u_i = \begin{cases} 1, & i \ne k \cdot q; \\ 0, & i = k \cdot q. \end{cases} \tag{11}$$

故由定理 1 知，此时 BCH 码维数为

$$\dim C = n - m \cdot \sum_{i=1}^{\delta-1} u_i = n - m \cdot [\delta^{(q)} \cdot (q-1) + \delta^{(0)}]. \tag{12}$$

(2) 对于 m 为偶数，且 $q^{m/2} + 1 \le \delta - 1 < T + 2 = 2q^{m/2} + 1$ 时，由引理 5 知 $|C_i| = m, i \ne q^{m/2} + 1; |C_i| = m/2, i = q^{m/2} + 1, i \le \delta - 1$。故再由引理 4 和定理 1 知

$$\dim C = n - m \sum_{i=1}^{\delta-1} u_i + m/2 = n - m[\delta^{(q)} \cdot (q-1) + \delta^{(0)}] + m/2. \tag{13}$$

推论 1 设 C 为码长为 $n = 2^m - 1$ 的二元 BCH 码，其设计距离 $\delta = 2t + 1$，则当 $2t - 1 < 2^{\lceil m/2 \rceil} + 1$ 时，该 BCH 码的维数为

$$\dim C = 2^m - 1 - m \cdot t. \tag{14}$$

证明 因为 $2t - 1 < 2^{\lceil m/2 \rceil} + 1$，$2t < 2^{\lceil m/2 \rceil} + 2$，所以 $\delta - 1 = 2t \le 2^{\lceil m/2 \rceil} < 2^{\lceil m/2 \rceil} + 1$，由定理 3(1) 易知 (14) 式成立。

推论 1 为文献 [1] 的结果，因此定理 3 是它的推广改进的结果。

令

$$A(m,\delta)=\{a|\ a\in A_m, a<\delta\}, \tag{15}$$

$$B(m,\delta,d)=\{a|\ a\in A(m,\delta), |C_a||d\}, \tag{16}$$

$$N(m,\delta,d)=|B(m,\delta,d)|, \tag{17}$$

$$C(m,\delta,d)=\{a|\ a\in A(m,\delta), |C_a|=d\}, \tag{18}$$

$$I(m,\delta,d)=|C(m,\delta,d)|. \tag{19}$$

定理 4 设 C 为 q 元 BCH 码，则其维数为

$$\dim C=n-\sum_{d|m} d\cdot I(m,\delta,d); \tag{20}$$

而 $I(m,\delta,d)$ 迭代公式为

$$I(m,\delta,d)=N(m,\delta,d)-\sum_{i=1}^{k}N(m,\delta,\frac{d}{p_i})+\sum_{1\le i<j<k}N\left(m,\delta,\frac{d}{p_ip_j}\right)$$
$$+\cdots+(-1)^kN(m,\delta,d/(p_1p_2\cdots p_k)), \tag{21}$$

其中 $p_1,p_2,\cdots,p_k$ 为 d 素因子分解 $d=p_1^{e_1}\cdot p_2^{e_2}\cdots p_k^{e_k}$ 的素数。

证明 由引理 1 、定理 1 以及上述符号定义易知 (20) 式成立。(21) 式可由组合数学中的容斥原理得证。

定理 5 设 $d|m$ ，则 $N(m,\delta,d)=|A(d,\delta')|$ 。其中 $\delta'=\lceil\delta/[(q^m-1)/(q^d-1)]\rceil$ 。

证明 若 $s\in B(m,\delta,d)$ ，则 $s\in A_m$ ， $|C_s||d$ ， $d|m$, 设 $m=v\cdot d$ ，由引理 2 知有正整数 r 使

$$s=r\cdot[q^{(v-1)d}+q^{(v-2)d}+\cdots+q^d+1]=r\cdot(q^m-1)/(q^d-1). \tag{22}$$

由于 $s\in A_m$ ， $0<s<q^m-1$ 使 $r=s/[(q^m-1)/(q^d-1)]<q^d-1$ ，又因为 $s\in B(m,\delta,d)$ ，$s<\delta$ ，则有

$$r=s/[(q^m-1)/(q^d-1)]<\delta/[(q^m-1)/(q^d-1)]\le\lceil\delta/[(q^m-1)/(q^d-1)]\rceil. \tag{23}$$

因为 $s\in A_m$，则若 $k\le|C_s|-1$ 均有 $sq^k\ge s$，即 $r\cdot[(q^m-1)/(q^d-1)]\cdot q^k\ge r\cdot(q^m-1)/(q^d-1)$，故有 $r\cdot q^k\ge r$ 成立，由此可知 $r\in A_d$，再由 (23) 式知 $r\in A(d,\delta')$，这里 $\delta'=\lceil\delta/[(q^m-1)/(q^d-1)]\rceil$. 故 $N(m,\delta,d)\le|A(d,\delta')|$ 。反过来容易推出，若 $r\in A(d,\delta')$, $s=r\cdot(q^m-1)/(q^d-1)$ ，则有 $s\in B(m,\delta,d)$ ，从而 $N(m,\delta,d)\ge|A(d,\delta')|$ ，故可得 $N(m,\delta,d)=|A(d,\delta')|$ 。

由定理 4 知，求 BCH 码维数问题可转化为求 $I(m,\delta,d)$ 问题；而由定理 5 可知，求 $I(m,\delta,d)$ 问题可转化为求 $|A(m,\delta)|$ 问题。

定理 6 (1) 若 $\delta-1<T+1$，则 $|A(m,\delta)|=\delta^{(q)}(q-1)+\delta^{(0)}$ ；(2) 若 $\delta-1\ge(q-1)q^{m-1}-1$，则 $|A(m,\delta)|=|A_m|$ 。

证明 (1) 由 T 定义和定理 3 证明过程易得证。(2) $(q-1)\cdot q^{m-1}-1$ 是 A_m 的最大元素[2]，故得证。

推论 2 若 $m=p^\lambda$，$\lambda\geq 1$，则

$$\dim C = n - p^\lambda |A(p^\lambda,\delta)| + \sum_{k=0}^{\lambda-1}(p-1)p^k|A(p^k,\delta_k)|, \tag{24}$$

其中 $\delta_k=\lceil \delta/[(q^{p^\lambda}-1)/(q^{p^k}-1)]\rceil$, $k=0,1,2,\ldots,\lambda-1$。

证明 由定理 4 知 $\dim C = n-\sum_{k=0}^{\lambda} p^k\cdot I(m,\delta,p^k)$。当 $k=1,2,\cdots,\lambda$ 时，有

$$I(m,\delta,p^k)=N(m,\delta,p^k)-N(m,\delta,p^{k-1}). \tag{25}$$

又 $I(m,\delta,1)=N(m,\delta,1)$，再由定理 5 可得

$$N(m,\delta,p^k)=|A(p^k,\delta_k)|. \tag{26}$$

由 (25)、(26) 式可推得

$$\begin{aligned}\dim C &= n-\sum_{k=1}^{\lambda}p^k[|A(p^k,\delta_k)|-|A(p^{k-1},\delta_{k-1})|]-A(1,\delta_0)\\ &= n-\sum_{k=1}^{\lambda}p^k|A(p^k,\delta_k)|+\sum_{k=1}^{\lambda}p^k(p^{k-1},\delta_{k-1})-A(1,\delta_0)\\ &= n-p^\lambda|A(p^\lambda,\delta)|-\sum_{k=1}^{\lambda-1}p^\lambda|A(p^k,\delta_k)|\\ &\quad +p\sum_{k=2}^{\lambda}p^{k-1}|A(p^{k-1},\delta_{k-1})|+(p-1)A(1,\delta_0)\\ &= n-p^\lambda|A(p^\lambda,\delta)|+\sum_{k=0}^{\lambda-1}(p-1)p^k|A(p^k,\delta_k)|.\end{aligned} \tag{27}$$

推论 3 若 m 为素数，则

$$\dim C = n-m\cdot|A(m,\delta)|+(m-1)\cdot e_\delta. \tag{28}$$

这里 e_δ 表示

$$e_\delta=\begin{cases}1, & \text{若 } \delta>(q^m-1)/(q-1);\\ 0, & \text{若 } \delta\leq(q^m-1)/(q-1).\end{cases} \tag{29}$$

3 BCH 码最小距离的猜测

文献 [1] 在第 201 页和第 247 页用两种方法给出了著名的 BCH 界定理。

BCH 界定理 让 C 是一个具有生成多项式为 $g(x)=\prod_{i\in K}(x-\alpha^i)$ 的循环码。若 K 包含有 $\delta-1$ 个连续整数 $b,b+1,\cdots,b+\delta-2$，则 C 的任何非零码字的重量至少为 δ（δ 称为该码的 BCH 界）。

因此由 BCH 界定理知，BCH 码的设计距离 δ 实际也是它的 BCH 界。

定义 4[3] 设 M 为 A_m 最大元，如果 $0<r<M$，称 $\min\{a|\ a>r, a\in A_m\}$ 为 A_m 中第一个大于 r 的元，记为 $M(r)$。这里 r 为整数。

定理 7 (1) BCH 码的 BCH 界 δ 是某个分圆陪集首。(2) 反之，任意一个分圆陪集首必是某个 BCH 码的 BCH 界。

证明 (1) $\delta=1$ 时，$\delta\in A_m$，此时 BCH 码是平凡的。下设 $\delta>1$。因为 δ 也是 BCH 码设计距离，故可由定义 2 知 (α 是 GF(q^m) 本原元)

$$g(\alpha)=g(\alpha^2)=\cdots=g(\alpha^{\delta-1})=0,\quad g(\alpha^\delta)\neq 0. \tag{30}$$

若 $\delta\notin A_m$，则必有 $a_\delta<\delta$ 或 $a_\delta\leq\delta-1$，故有 $g(\alpha^\delta)=g(\alpha^{a_\delta})=0$，这与 (30) 式矛盾，所以 $\delta\in A_m$。

(2) $\forall\delta\in A_m$，我们取生成多项式 $g(x)$ 满足

$$g(x)=\text{l.c.m.}\{M^{(1)}(x),M^{(2)}(x),\cdots,M^{(\delta-1)}(x)\}, \tag{31}$$

就可建立一个 BCH 界为 δ 的 BCH 码。

推论 4 不存在设计距离不是分圆陪集首的 BCH 码。

文献 [1] 在第 237 页证明了二元 BCH 码 (本原) 的最小距离特征是奇数。我们观察了文献 [1] 中第 267 页给出的二元 BCH 码参数表以及文献 [4] 中给出的二元 BCH 码参数表，结合文献 [4，5] 中给出的一些结论，给出了如下一个猜测。

猜测 1 q 元狭义本原 BCH 码的最小距离 $d\in A_m$。

BCH 码是一类在编码理论和实践中都很重要的码族。因此研究 BCH 码的最小距离的问题是十分有意义的。

早在 1967 年，W. W. Peterson 经过研究就曾提出如下一个猜想 [6]：二元狭义本原 BCH 码，其最小距离等于其 BCH 界。可是不久 T. Kasami 和 N. Tokura 在文献 [7] 中给出了否定的回答：当 $m\neq 8,12,\ m>6$ 时，存在一些二元狭义本原 BCH 码，其最小距离大于其 BCH 界。

为了方便人们继续探讨 BCH 码最小距离问题，文献 [1] 在第 261 页给人们留下了一个至今尚未得到解决的难题：关于码长 n 和设计距离 δ，找到使最小距离 d 等于 δ 的充要条件。文献 [5] 在 1980 年给出了几个 $d=\delta$ 的例子。而文献 [8] 在 1985 年证明了若 m 和 $t=\lfloor(\delta-1)/2\rfloor$ 相比充分大时，则有 $\delta=d$。最近，文献 [4] 讨论了 $n=255,511$ 时二元狭义本原 BCH 码的最小距离情况。给出了 $d>\delta$ 和 $d=\delta$ 更多的例子，补充并完善了文献 [1] 中第 267 页 BCH 码参数表。

通过对上述诸多文献结果观察与分析，我们给出了如下猜测。

猜测 2 对于 q 元狭义本原 BCH 码，若其设计距离 $\delta\leq T$ 时，其最小距离 $d=\delta$。

致谢 感谢杨义先教授、林须端教授的关心和帮助。感谢信号理论和密码学研究室诸同学有益的讨论。

参 考 文 献

[1] MacWilliams F J, Sloane N J A. The Theory of Error-Correcting Codes. Amsterdam: North-Holland, Publishing Company. 1977, 201–267.

[2] 岳殿武. 循环陪集结构及其应用，系统科学与数学， 1992, 12(1): 15–20.

[3] 岳殿武，纪青君. 关于 Goppa 码、Alternant 码最小距离下限的简化算法，通信学报， 1991, 12(3): 10–16.

[4] Augot D, Charpin P, Sendrier N. IEEE Trans. on IT, 1992, IT-38(3): 960–973.

[5] Cohen G. IEEE Trans. on IT, 1980, IT-26(3): 363.

[6] Peterson W W. J. IECE Japan, 1967, 50(6): 1183–1190.

[7] Kasami T, Tokura N. IEEE Trans. on IT, 1969, IT-15(3): 408–413.

[8] Helleseth T. Discrete Applied Mathematics, 1985, (11): 157–173.

ON THE DIMENSION AND MINIMUM DISTANCE OF BCH CODES OVER GF(q)

Yue Dianwu　　Hu Zhengming

(*Beijing University of Posts and Telecommunications, Beijing* 100088)

Abstract At first, a formula for computing the dimension of (narrow-sense, primitive) BCH codes over GF(q) is offered, which is better than the result given by F. J. MacWilliams et al. (1977). then a new method for calculating the dimension of BCH codes is proposed. Moreover, it is proved that BCH bound is a leader of cyclotomic cosets, and it is guessed that the minimum distance of BCH codes is also a leader of cyclotomic cosets.

Key words BCH codes, Cyclotomic cosets, Dimension, Minimum distance

岳殿武： 男， 1965 年生，博士生，从事编码和密码研究工作.

胡正名： 男， 1931 年生，教授，博士生导师，《通信学报》副主编，从事应用数学和信息科学的教学和研究工作.