第 13 卷 第 2 期
1991 年 3 月

电子科学学刊
JOURNAL OF ELECTRONICS

Vol. 13, No. 2
Mar., 1991

关于 Goppa 码的维数问题

岳殿武
(大连理工大学应用数学研究所,大连)

摘要 冯贵良(1983)给出了 Goppa 码维数的新下限. 本文首先给出了在一定条件下求这一下限的统一公式. 然后给出了 Goppa 码维数上限以及求这一上限的具体方法. 通过上、下限同时估计,能够求出特殊类型的 Goppa 码的维数.

关键词 Goppa 码; Goppa 码的维数;维数的限;

1. 引言

Goppa 码是一大类具有较好性质的纠错码. 因为它具有这样的特性, 几乎所有长的既约 Goppa 码都能满足 Gilbert-Varshamov 界[1-3]. 可是对于一个给定的Goppa码,如何求其最小距离和维数问题,至今尚未得到解决[3]. 冯贵良在文献[4]中给出了关于这个问题新的研究结果. 本文在文献[4]基础上着重研究了其中维数问题.

文献[4]给出了 Goppa 码维数的新下限,但是要求出这一下限需要进行有限域上求解共轭元复杂运算. 为了避免这一复杂运算过程, 本文给出了在一定条件下求下限的一般公式. 估计维数,至今只用下限来估计. 本文试用上限来估计它, 给出了 Goppa 码维数一个上限,以及求这一上限的具体方法. 通过上、下限同时估计,可以看出,特殊类型的 Goppa 码是能求出它的维数的.

2. Goppa 码维数的下限

设 $L=\{\alpha_1, \alpha_2, \cdots, \alpha_n\}\subset GF(q^m)$, $G(z)=\prod_{l=1}^{t}(z-\beta_l)^{r_l}$ 是 $GF(q^m)$ 上的多项式,且 $G(\alpha_i)\neq 0$, $i=1,2,\cdots n$, 则 Goppa 码是满足下式的 $GF(q)$ 上 n 元向量 $a=(a_1,a_2\cdots a_n)$ 的全体:

$$\sum_{i=1}^{n}\frac{a_i}{z-\alpha_i}\equiv 0 \pmod{G(z)} \tag{1}$$

由文献[5]知,其一致校验矩阵为

1989 年 4 月 27 日收到, 1990 年 9 月 17 日修改定稿.

$$H=\left[\begin{array}{cccc}(\alpha_1-\beta_1)^{-1} & (\alpha_2-\beta_1)^{-1} & \cdots & (\alpha_n-\beta_1)^{-1}\\ (\alpha_1-\beta_1)^{-2} & (\alpha_2-\beta_1)^{-2} & \cdots & (\alpha_n-\beta_1)^{-2}\\ \vdots & \vdots & & \vdots\\ (\alpha_1-\beta_1)^{-r_1} & (\alpha_2-\beta_1)^{-r_1} & \cdots & (\alpha_n-\beta_1)^{-r_1}\\ \hline \vdots & \vdots & & \vdots\\ \hline (\alpha_1-\beta_S)^{-1} & (\alpha_2-\beta_S)^{-1} & \cdots & (\alpha_n-\beta_S)^{-1}\\ (\alpha_1-\beta_S)^{-2} & (\alpha_2-\beta_S)^{-2} & \cdots & (\alpha_n-\beta_S)^{-2}\\ \vdots & \vdots & & \vdots\\ (\alpha_1-\beta_S)^{-r_S} & (\alpha_2-\beta_S)^{-r_S} & \cdots & (\alpha_n-\beta_S)^{-r_S}\end{array}\right]=(h_{ij}) \tag{2}$$

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

定义 1 设 β 是 $GF(q^m)$ 上的本原元，β^i，$i=1,2,\cdots r$，在 $GF(q^m)$ 上的所有共轭元的个数，称为 r 的广义维数，记为 $f(r)$。

定义 2 设对每个 $\alpha_j\in L$，$(\alpha_j-\beta_l)^i$，$i=1,2\cdots r_l$，在 $GF(q^m)$ 上的所有共轭元的个数，称为 r_l 的狭义维数，记为 $f_{L,l}(r_l)$。

定理 1[4] 给定如上的 Goppa 码，其维数

$$K\geqslant n-\sum_{l=1}^{s}f_{L,l}(r_l)\geqslant n-\sum_{l=1}^{s}f(r_l) \tag{3}$$

这就是 Goppa 码维数下限定理。下面引用文献[6]的结果，就可推出在一定条件下求其下限的一般公式。

定义 3 设 $0<s<q^m-1$，$s\cdot q^{m_s}=s \bmod(q^m-1)$，称集合 $\{s,sq,\cdots sq^{m_s-1}\}$ 为 $GF(g^m)$ 上关于 s 的循环陪集，记为 C_s。 记 $a_s=\min\{p|p\in C_s\}$，$A=\{a_s|C_s$ 为 $GF(q^m)$ 上任意一个循环陪集$\}$。称 A 为循环陪集的首集。

定义 4 给定一个正整数 t，如果集合 $\{s|s\leqslant t,s\neq k\cdot q$，$k$ 为任意正整数$\}\subset A$，则称 t 为 A 的一个连续界，所有这些 t 中最大者，称为 A 的最大连续界，记为 T。

引理 1[6] A 的最大连续界为

$$T=\begin{cases}q^{(m+1)/2}-1, & (m\text{ 为奇数})\\ 2q^{m/2}-1, & (m\text{ 为偶数})\end{cases} \tag{4}$$

引理 2[6] 如果 $s\leqslant T$，则有

$$|C_s|=\begin{cases}m, & (\text{当 }m\text{ 为奇数；或者 }m\text{ 为偶数，但 }s\neq q^{m/2}+1\text{ 时})\\ m/2, & (\text{当 }m\text{ 为偶数，且 }s=q^{m/2}+1\text{ 时})\end{cases} \tag{5}$$

定理 2 设 $r_l\leqslant T+1$，记 $r_l=r_l^{(q)}\cdot q+r_l^{(0)}$，$0\leqslant r_l^{(0)}<q$。则 Goppa 码维数下限

$$n-\sum_{l=1}^{s}f(r_l)=\begin{cases}n-m\cdot\left[\sum_{l=1}^{s}r_l^{(q)}(q-1)+r_l^{(0)}\right], & (m\text{ 为奇数})\\ n-m\cdot\left[\sum_{l=1}^{s}r_l^{(q)}(q-1)+r_l^{(0)}\right]+\dfrac{m}{2}\cdot e, & (m\text{ 为偶数})\end{cases} \tag{6}$$

这里 e 表示 $r_l\geqslant q^{m/2}+1$ 的 r_l 个数，$l=1,2,\cdots,s$。

证明　实际上，$f(r_l)$ 就是集合 $\bigcup_{p=1}^{r_l} C_p$ 所有元个数. 由引理 1 与引理 2 知，当 $r_l \leqslant T+1$ 时，如果 m 为奇数，则有 $|C_s| = m$. 因为若有 $p = k\cdot q$，则 $C_p = C_k$. 故可推得此时下式成立.

$$f(r_l) = r_l\cdot m - r_l^{(q)}\cdot m = [r_l^{(q)}\cdot(q-1) + r_l^{(0)}]\cdot m,\quad l=1,2,\cdots,s \tag{7}$$

对于 m 为偶数，因为 $p = q^{m/2}+1$ 时，$|C_p| = m/2$，故

$$f(r_l) = \begin{cases} [r_l^{(q)}\cdot(q-1) + r_l^{(0)}]\cdot m, & (r_l < q^{m/2}+1) \\ [r_l^{(q)}\cdot(q-1) + r_l^{(0)}]\cdot m - \dfrac{m}{2}, & (r_l \geqslant q^{m/2}+1) \end{cases} \tag{8}$$

由(7)与(8)式不难得到(6)式.

3. Goppa 码维数的上限

引理 3[4]　H^* 的行在 $GF(q^m)$ 上的秩等于 $n-K$.

设 $n = \sum_{i=1}^{s}\lambda_i$，$\lambda_i > 0, i = 1,2,\cdots,s$. 记

$$C(\lambda_1,\lambda_2,\cdots,\lambda_s) = \left[\begin{array}{cccc} (x_1+a_1)^{-1} & (x_1+a_2)^{-1} & \cdots & (x_1+a_n)^{-1} \\ (x_1+a_1)^{-2} & (x_1+a_2)^{-2} & \cdots & (x_1+a_n)^{-2} \\ \vdots & \vdots & & \vdots \\ (x_1+a_1)^{-\lambda_1} & (x_1+a_2)^{-\lambda_1} & & (x_1+a_n)^{-\lambda_1} \\ \hline \vdots & \vdots & & \vdots \\ \hline (x_s+a_1)^{-1} & (x_s+a_2)^{-1} & \cdots & (x_s+a_n)^{-1} \\ (x_s+a_1)^{-2} & (x_s+a_2)^{-2} & \cdots & (x_s+a_n)^{-2} \\ \vdots & \vdots & & \vdots \\ (x_s+a_1)^{-\lambda_s} & (x_s+a_2)^{-\lambda_s} & \cdots & (x_s+a_n)^{-\lambda_s} \end{array}\right] \tag{9}$$

引理 4[4]　若 $x_1,x_2\cdots x_s;a_1,a_2\cdots,a_n$ 各不相同，且 $x_i + a_j \neq 0$，$i=1,2,\cdots,s$；$j=1,2,\cdots,n$. 则 $C(\lambda_1,\lambda_2\cdots\lambda_s)$ 的秩为 n.

将 H^* 重复行拿走，并对行进行重排，所得矩阵记为 $\widetilde{H} = [\widetilde{H}_1,\widetilde{H}_2,\cdots,\widetilde{H}_s]$，这里

$$\widetilde{H}_l = \begin{bmatrix} (\alpha_1-\beta_l)^{-p_1} & (\alpha_2-\beta_l)^{-p_1} & \cdots & (\alpha_n-\beta_l)^{-p_1} \\ (\alpha_1-\beta_l)^{-p_2} & (\alpha_2-\beta_l)^{-p_2} & \cdots & (\alpha_n-\beta_l)^{-p_2} \\ \vdots & \vdots & & \vdots \\ (\alpha_1-\beta_l)^{-p_{b_l}} & (\alpha_2-\beta_l)^{-p_{b_l}} & \cdots & (\alpha_n-\beta_l)^{-p_{b_l}} \end{bmatrix} \tag{10}$$

其中 $p_1 < p_2 < \cdots < p_{b_l}$，$l = 1,2,\cdots s$. 各取 $\widetilde{H}_l$ 的一部分组成一个新矩阵 $\overline{H} = [\overline{H}_1, \overline{H}_2,\cdots,\overline{H}_s]$，这里

$$\overline{H}_l = \begin{bmatrix} (\alpha_1-\beta_l)^{-p_1} & (\alpha_2-\beta_l)^{-p_1} & \cdots & (\alpha_n-\beta_l)^{-p_1} \\ (\alpha_1-\beta_l)^{-p_2} & (\alpha_2-\beta_l)^{-p_2} & \cdots & (\alpha_n-\beta_l)^{-p_2} \\ \vdots & \vdots & & \vdots \\ (\alpha_1-\beta_l)^{-p_{n_l}} & (\alpha_2-\beta_l)^{-p_{n_l}} & \cdots & (\alpha_n-\beta_l)^{-p_{n_l}} \end{bmatrix} \tag{11}$$

其中 $r_l \leqslant n_l \leqslant b_l$，$l = 1,2\cdots s$.

定理 3　如果 $\sum_{l=1}^{s} p_{n_l} \leqslant n$，那么给定的 Goppa 码，其维数 $K \leqslant n - \sum_{l=1}^{s} n_l$

证明 记 $G=[G_1,G_2,\cdots,G_s]^T$，这里

$$G_1=\begin{bmatrix}(\alpha_1-\beta_1)^{-1} & \cdots & (\alpha_n-\beta_1)^{-1}\\ (\alpha_1-\beta_1)^{-2} & \cdots & (\alpha_n-\beta_1)^{-2}\\ \vdots & & \vdots\\ (\alpha_1-\beta_1)^{-g} & \cdots & (\alpha_n-\beta_1)^{-g}\end{bmatrix},\quad G_l=\begin{bmatrix}(\alpha_1-\beta_l)^{-1} & \cdots & (\alpha_n-\beta_l)^{-1}\\ (\alpha_1-\beta_l)^{-2} & \cdots & (\alpha_n-\beta_l)^{-2}\\ \vdots & & \vdots\\ (\alpha_1-\beta_l)^{-p_{n_l}} & \cdots & (\alpha_n-\beta_l)^{-p_{n_l}}\end{bmatrix}$$

$$l=2,3,\cdots,s \tag{12}$$

这里 $g=n-\sum_{l=2}^{s}p_{n_l}$. 因为 $g+\sum_{l=2}^{s}p_{n_l}=n$，所以$G$为 $n\times n$ 矩阵. 由于$G(\alpha_i)\neq 0$，$i=1,2,\cdots,s$，知 $\alpha_i-\beta_l\neq 0$，又 $\alpha_1,\cdots,\alpha_n;(-\beta_1),\cdots,(-\beta_s)$ 彼此不同,所以由引理 4 知,G的秩为 n. 由于$\bar{H}$ 所有行均为G中行,而$\bar{H}$ 所有行又是 $\tilde{H}$ 和 H^* 中的行,所以 H^* 的行秩必不小于$\bar{H}$ 的行秩.而$\bar{H}$ 的所有行线性无关,这样由引理 3 知 $n-K\geqslant\sum_{l=1}^{s}n_l$，即 $K\leqslant n-\sum_{l=1}^{s}n_l$.

通过上述定理,在保证 $\sum_{l=1}^{s}p_{n_l}\leqslant n$，我们选取 n_l，使 $\sum_{l=1}^{s}n_l$ 达到最大值 M，那么维数上限达到最优. 下面给出求 M 的一个方法.

称向量 $((\alpha_1-\beta_l)^{-p}\cdots(\alpha_n-\beta_l^{-p}))$中 p 为此向量幂次. 下面选取就是要从 $\tilde{H}_l$ 中选取尽可能多的行. 选取是从 $l=1$ 向 $l=s$，从行幂次低向行幂次高过渡.

(1) 首先选取行幂次之差为 1 的尽可能多的行,设从 $\tilde{H}_l$ 中选取了 $n_l^{(1)}$ 行，被选取行最高幂次达 $p_{n_l}^{(1)}$，则应有 $\sum_{l=1}^{s}p_{n_l}^{(1)}\leqslant n$. 如果还剩下幂差为 1 行不能再被选取，那么选取完毕. 否则进行下步.

(2) 其次选取剩下的行幂差至多为 2 的行，设从 $\tilde{H}_l$ 中又选取 $n_l^{(2)}$ 行，最高幂次已达 $p_{n_l}^{(2)}$，则还应有 $\sum_{l=1}^{s}p_{n_l}^{(2)}\leqslant n$. 如果不能再选取了，则选取完毕. 否则进行下步. 如此进行下去,直到不能再选取为止. 设从 $\tilde{H}_l$ 中总共选取了 $n_{L,l}$ 行,则有 $K\leqslant n-\sum_{l=1}^{s}n_{L,l}$.

定义 5 设β为 $GF(q^m)$ 本原元. 如果 β^i, $i=1,2\cdots r$. 在 $GF(q^m)$ 上共轭元集合中包含从β开始幂差至多为 t 的元素个数，称为 r 的幂差至多为 t 的广义指标，记为 $b^{(t)}(r)$.

例 1 设β为 $GF(2^5)$ 的本原元，β^i，$i=1,2,\cdots 7$,共轭元集合为$\{\beta^1,\beta^2,\beta^3,\beta^4,\beta^5,\beta^6,\beta^7,\beta^8,\beta^9,\beta^{10},\beta^{12},\beta^{14},\beta^{16},\beta^{17},\beta^{18},\beta^{19},\beta^{20},\beta^{24},\beta^{25},\beta^{28}\}$,由定义 5 易知，$b^{(1)}(7)=10$，$b^{(2)}(7)=17$，$b^{(3)}(7)=17$，$b^{(t)}(7)=20$，$(t\geqslant 4)$.

定义 6 对于每个 $\alpha_j\in L$，若 $(\alpha_j-\beta_l)^i$，$i=1,2,\cdots r_l$，在 $GF(q^m)$ 上共轭元集合中包含从 $(\alpha_j-\beta_l)$ 开始幂差至多为 t 的元素个数，称为 r_l 的幂差至多为 t 的狭义指标,记为 $n_{L,l}^{(t)}(r_l)$.

推论 1 设在选取过程中幂差至多为 t 的行全部被选入,则

$$K \leqslant n - \sum_{l=1}^{s} n_{L,l}^{(t)}(r_l) \leqslant n - \sum_{l=1}^{s} b^{(t)}(r_l) \tag{13}$$

4. Goppa 码维数的估计

由定理 1 和定理 3，我们有

定理 4 $n - \sum_{l=1}^{s} f_{L,l}(r_l)' \leqslant K \leqslant n - \sum_{l=1}^{s} n_l$

推论 2 如果 $\widetilde{H}_l$，$l = 1,2\cdots s$，所有行均能在选取过程中被选入，则

$$K = n - \sum_{l=1}^{s} f_{L,l}(r_l) \tag{14}$$

推论 3 如果 $G(z) = (z-\beta_1)^{r_1}$，$n = q^{m-1}$，则

$$K = n - f_{L,1}(r_1) \tag{15}$$

证明 设 p_{n_1} 为 $\{(\alpha_j - \beta_1)^{-p}\}$，$p = 1,2\cdots r_1$，在 $GF(q^m)$ 上所有共轭元最高幂次，则有 $p_{n_1} \leqslant n$，故 $\widetilde{H}$ 所有行都能在选取过程中被选入，因此由推论 2 易得 (15) 式成立。

取 $G(z) = z^{r_1}, L = \{1,\alpha,\cdots\alpha^{n-1}\}$，$n = q^m - 1$，此时 Goppa 码就是 BCH 码。其一致校验矩阵为

$$H = \begin{bmatrix} 1 & \alpha^{-r_1} & \alpha^{-2r_1} & \cdots & \alpha^{-(n-1)r_1} \\ 1 & \alpha^{-(r_1-1)} & \alpha^{-2(r_1-1)} & \cdots & \alpha^{-(n-1)(r_1-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(n-1)} \end{bmatrix} \tag{16}$$

推论 4 BCH 码的维数 $K = n - f_{L,1}(r_1)$

证明 由推论 3 即得证。

推论 4 给出了从新角度求 BCH 码维数的方法。

推论 5 如果 $G(z) = (z-\beta_1)^{r_1}$，$n = q^m - 1$；且 $r_1 \leqslant T$，$\alpha_j - \beta_1$ 为 $GF(q^m)$ 本原元，$j = 1,2,\cdots,n$，则 Goppa 码的维数

$$K = \begin{cases} n - m\cdot[r_1^{(q)}(q-1) + r_1^{(0)}] & (m \text{ 为奇数}) \\ n - m\cdot[r_1^{(q)}(q-1) + r_1^{(0)}] + mx/2 & (m \text{ 为偶数}) \end{cases} \tag{17}$$

这里 $r_1 = r_1^{(q)}\cdot(q)+r_1^{(0)}, r_1^{(0)} \geqslant 0$；$x = 1$，(若 $r_1 \geqslant q^{m/2}+1$)，$x = 0$，(若 $r_1 < q^{m/2}+1$)。

证明 如 $\alpha_j - \beta_1$ 为 $GF(q^m)$ 本原元，则 $f_{L,1}(r_1) = f(r_1)$，再由推论 3 和定理 2 即得证。

例 2 $G(z) = (z-1)^{15}$，$L = \{0,\alpha,\cdots,\alpha^{62}\}$，$\alpha$ 是 $GF(2^6)$ 的本原元。由推论 5 知，此 Goppa 码维数 $K = 63 + 6/2 - 6\cdot[(7\cdot(2-1) + 1] = 18$。而由文献[4](举例部分例 1) 只能得出 $K \geqslant 18$。

本文是在沈世镒教授悉心指导下完成的，在此谨致感谢！

参 考 文

[1] V. D. Goppa, *Probl. Peredach. Inform.*, 6(1970)3, 24—30.

[2] E. R. Berlekamp, *IEEE Trans. on IT*, IT-19(1973)9, 590—592.
[3] F. J. Macwillians, N. J. A. Sloane, Theory of Error-Correcting Codes, New York, North-Holland, (1977).
[4] 冯贵良，电子学报，1983 年，第 2 期，第 66—72 页.
[5] K. K. Tzeng, E. Iimmermann, *IEEE Trans. on IT*, IT-21(1975)11, 712—716.
[6] 岳殿武，循环陪集结构及其应用，系统科学与数学，待发表.

ON THE DIMENSIONS OF GOPPA CODES

Yue Dianwu
(Dalian University of Technology, Dalian)

Abstract A new lower bound on the dimensions of Goppa codes has been given by Feng Guiliang (1983). In this paper, at first, a formula for computing the lower bound in some cases is offered, and a upper bound on the dimensions of Goppa codes and a method of finding the upper bound are given. In some special cases, the dimensions of Goppa codes can be obtained by using the upper bound and the lower bound.

Key words Goppa codes; Dimensions of Goppa codes; Bound on dimensions