第7卷 第1期 电子科学学刊 Vol. 7, No. 1
1985 年 1 月 JOURNAL OF ELECTRONICS Jan., 1985

二元 Goppa 码最小距离的新下限*

冯 贵 良
(上海计算技术研究所)

提 要

二元 Goppa 码是一大类很有用的纠错码. 但是如何求二元 Goppa 码的真正最小距离至今没有解决. 本文将导出二元 Goppa 码最小距离的新下限, 这个新下限改进了 Y. Sugiyama 等(1976) 和作者 (1983) 文章的结果. 本文的方法不难推广到其他 Goppa 码中去.

一、引 言

Goppa 码是一大类十分重要的纠错码. 十几年来人们对 Goppa 码的研究十分活跃. 但是如何求 Goppa 码的真正最小距离,即使是如何求二元 Goppa 码的真正最小距离,至今没有较好的方法,看来这个问题十分困难. 因此象对 BCH 码那样,寻找 Goppa 码最小距离比较接近的下限就十分有必要了. 文献 [1, 2] 给出 Goppa 码最小距离下限的扩张定理,给出的下限在一定条件下比普通的下限有所提高,但提高得不多,适用性也不大,所得的下限离开真正的最小距离还有一定差距. 本文运用 BCH 码最小距离下限扩张的推广形式,得到求 Goppa 码最小距离新下限的方法. 为叙述方便,本文以 $G(z)=(z-\beta_1)^{2a}\cdot(z-\beta_2)^{2b}$ 为生成多项式的二元 Goppa 码为例进行说明,文中还举了几个例子说明新下限比文献 [2] 中给出的下限有较大的改进. 当然本文的方法与结果完全可以平行地推广到一般的多元 Goppa 码的情况.

二、一些引理和基本结果

本节介绍的二元 Goppa 码是这样的 Goppa 码: 它的生成多项式是 $G(z)=(z-\beta_1)^{2a}\cdot(z-\beta_2)^{2b}$, 位置集 $L=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$, 码长为 n. 令 $GF(2^m)$ 是包含 $\{\alpha_i-\beta_1,\alpha_i-\beta_2\}_{i=1}^n$ 的最小有限域,并令 F 是包含 $\{\alpha_i-\beta_1,\alpha_i-\beta_2\}_{i=1}^n$ 的 $GF(2^m)$ 的最小乘法子群, 即 $F\triangleq\{1,\beta^{q^*},\beta^{2q^*},\cdots,\beta^{(n^*-1)q^*}\}$, 这里 β 是 $GF(2^m)$ 的本原元, $n^*\cdot q^*=2^m-1$, $\{\alpha_i-\beta_1,\alpha_i-\beta_2\}_{i=1}^n\subseteq F$, 并且没有其他乘法子群能包含 $\{\alpha_i-\beta_1,\alpha_i-\beta_2\}_{i=1}^n$. 由 F 的定义,我们有:

* 1983 年 5 月 25 日收到. 1984 年 4 月 10 日修改定稿.

$$\alpha^j = \alpha^{j \bmod n^*}, \quad \text{对所有 } \alpha \in F. \tag{1}$$

由文献[3]知,这个二元 Goppa 码的一致校验阵为:

$$H = \begin{bmatrix} (\alpha_1-\beta_1)^{-2a} & (\alpha_2-\beta_1)^{-2a} & \cdots & (\alpha_n-\beta_1)^{-2a} \\ \vdots & \vdots & & \vdots \\ (\alpha_1-\beta_1)^{-1} & (\alpha_2-\beta_1)^{-1} & \cdots & (\alpha_n-\beta_1)^{-1} \\ \hline (\alpha_1-\beta_2)^{-2b} & (\alpha_2-\beta_2)^{-2b} & \cdots & (\alpha_n-\beta_2)^{-2b} \\ \vdots & \vdots & & \vdots \\ (\alpha_1-\beta_2)^{-1} & (\alpha_2-\beta_2)^{-1} & \cdots & (\alpha_n-\beta_2)^{-1} \end{bmatrix}. \tag{2}$$

为书写简单,本文以 $\overrightarrow{A(\alpha_i)}$ 表示行向量 $(A(\alpha_1), A(\alpha_2), \cdots, A(\alpha_n))$. 因此上面矩阵H可写成:

$$H = \begin{bmatrix} \overrightarrow{(\alpha_i-\beta_1)^{-2a}} \\ \vdots \\ \overrightarrow{(\alpha_i-\beta_1)^{-1}} \\ \hline \overrightarrow{(\alpha_i-\beta_2)^{-2b}} \\ \vdots \\ \overrightarrow{(\alpha_i-\beta_2)^{-1}} \end{bmatrix}. \tag{2'}$$

运用文献[2]的记号,令:

$$H^* = \begin{bmatrix} H^{(2^0)} \\ H^{(2^1)} \\ \vdots \\ H^{(2^{m-1})} \end{bmatrix}, \tag{3}$$

这里

$$H^{(2^j)} = \begin{bmatrix} \overrightarrow{(\alpha_i-\beta_1)^{-2a\cdot 2^j}} \\ \vdots \\ \overrightarrow{(\alpha_i-\beta_1)^{-1\cdot 2^j}} \\ \hline \overrightarrow{(\alpha_i-\beta_2)^{-2b\cdot 2^j}} \\ \vdots \\ \overrightarrow{(\alpha_i-\beta_2)^{-1\cdot 2^j}} \end{bmatrix}, \quad j = 0, 1, \cdots, m-1. \tag{3'}$$

再记 H_s^* 是由矩阵 H^* 的所有行向量所张成 $GF(2^m)$ 上的线性空间,很易证明:

引理 1: 若 $\overrightarrow{A_1(\alpha_i)}$, $\overrightarrow{A_2(\alpha_i)} \in H_s^*$; $a_1, a_2 \in GF(2^m)$, 则

$$\left.\begin{aligned} &a_1 \cdot \overrightarrow{A_1(\alpha_i)} + a_2 \cdot \overrightarrow{A_2(\alpha_i)} \in H_s^*; \\ &\overrightarrow{A_1(\alpha_i)^{2^j}} \in H_s^*, \quad j = 0, 1, \cdots, m-1. \end{aligned}\right\} \tag{4}$$

由文献[2]的定理1,我们有:

定理 1: 设 $\{\overrightarrow{A_i(\alpha_i)}\}_{i=1}^t$ 是 H_s^* 中的行向量集合,把它们排列成矩阵 $\tilde{H}$, 即

$$\widetilde{H}=\begin{bmatrix}\overrightarrow{A_t(\alpha_i)}\\ \overrightarrow{A_{t-1}(\alpha_i)}\\ \vdots\\ \overrightarrow{A_1(\alpha_i)}\end{bmatrix}. \tag{5}$$

若矩阵 $\widetilde{H}$ 的任意 $d'-1$ 个列在 $GF(2^m)$ 上线性无关，则二元 Goppa 码的最小距离 $\geqslant d'$. 因此 d' 可以看作二元 Goppa 码最小距离的一个下限.

注意，在定理 1 中，$\overrightarrow{A_i(\alpha_i)}$ 彼此之间可以是相同的. 最小距离下限扩张问题就是如何在 H_s^* 中寻找较多的 $\overrightarrow{A_i(\alpha_i)}$，使它们构成的矩阵 $\widetilde{H}$ 有较大的 d'. 这里有两个相辅相成的问题. 第一个问题是给出矩阵 $\widetilde{H}$ 后，如何求出较大的 d'，使 $\widetilde{H}$ 中的任意 $d'-1$ 个列在 $GF(2^m)$ 上线性无关；第二个问题是如何从线性空间 H_s^* 取 t 个向量 $\{\overrightarrow{A_i(\alpha_i)}\}_{i=1}^{t}$ 使它们构成的矩阵 $\widetilde{H}$ 有较大的 d'. 有时很有必要取几个相同的行向量，详见下面的例子. 下面我们给出解决上述二个问题的方法.

解决第一个问题最方便最简单的工具是 Vandermonde 矩阵和 Cauchy 矩阵，关于 BCH 码的设计距离和 Goppa 码通常的最小距离下限就是由这两个工具得出来的. 文献 [2] 运用广义 Vandermonde 矩阵和广义 Cauchy 矩阵可以扩张 BCH 码和 Goppa 码的最小距离下限. 但用这两个方法求得的 d' 还不是最大，为此文献 [4, 5] 独立地引进对矩阵 $\widetilde{H}$ 求较大 d' 的更有力的定理. 本文也运用这个定理来解决第一个问题. 设

$$C_{k'}^{*}=\left[\begin{array}{cccc}C_{11} & C_{12} & \cdots & C_{1n}\\ C_{11}x_1 & C_{12}x_2 & \cdots & C_{1n}x_n\\ \vdots & \vdots & & \vdots\\ C_{11}x_1^{\tau-1} & C_{12}x_2^{\tau-1} & \cdots & C_{1n}x_n^{\tau-1}\\ \hline \vdots & \vdots & & \vdots\\ \hline C_{k'1} & C_{k'2} & \cdots & C_{k'n}\\ C_{k'1}x_1 & C_{k'2}x_2 & \cdots & C_{k'n}x_n\\ \vdots & \vdots & & \vdots\\ C_{k'1}x_1^{\tau-1} & C_{k'2}x_2^{\tau-1} & \cdots & C_{k'n}x_n^{\tau-1}\end{array}\right], \tag{6}$$

记

$$\overrightarrow{C_j}=(C_{j1},C_{j2},\cdots,C_{jn}),\quad (j=1,2,\cdots,k');$$

并令

$$C=\begin{bmatrix}\overrightarrow{C_1}\\ \overrightarrow{C_2}\\ \vdots\\ \overrightarrow{C_{k'}}\end{bmatrix}.$$

由文献[4]的引理 2 或文献 [5] 的定理 1 知：

定理 2 若 $x_1, x_2, \cdots, x_n$ 各不相同，矩阵 C 的任意 $\tau + k' - 1$ 个列所组成的子矩阵的秩为 k'，则矩阵 $C^*_{k'}$ 的任意 $\tau + k' - 1$ 个列线性无关.

为书写方便，我们记

$$\begin{bmatrix} \overrightarrow{A_1} \\ \overrightarrow{A_2} \\ \vdots \\ \overrightarrow{A_\mu} \end{bmatrix} \odot \begin{bmatrix} \overrightarrow{B_1} \\ \overrightarrow{B_2} \\ \vdots \\ \overrightarrow{B_\lambda} \end{bmatrix} \triangleq \begin{bmatrix} \overrightarrow{A_1B_1} \\ \overrightarrow{A_1B_2} \\ \vdots \\ \overrightarrow{A_1B_\lambda} \\ \vdots \\ \overrightarrow{A_\mu B_1} \\ \overrightarrow{A_\mu B_2} \\ \vdots \\ \overrightarrow{A_\mu B_\lambda} \end{bmatrix}. \tag{7}$$

这样，矩阵 $C^*_{k'}$ 可以写成：

$$C^*_{k'} = \begin{bmatrix} \overrightarrow{C_1} \\ \overrightarrow{C_2} \\ \vdots \\ \overrightarrow{C_{k'}} \end{bmatrix} \odot \begin{bmatrix} \overrightarrow{1} \\ \overrightarrow{x} \\ \vdots \\ \overrightarrow{x^{\tau-1}} \end{bmatrix}, \tag{6'}$$

这里 $\overrightarrow{1} = (1, 1, \cdots, 1)$，$\overrightarrow{x^i} = (x_1^i, x_2^i, \cdots, x_n^i)$.

为了解决第二个问题，下面二个引理十分有用.

引理 2 当 p, q 不同时为 0，$0 \leqslant p \leqslant 2a$，$0 \leqslant q \leqslant 2b$，则

$$\overrightarrow{(\alpha_i - \beta_1)^{-p} \cdot (\alpha_i - \beta_2)^{-q}} \in H^*_s. \tag{8}$$

证明 由初等代数的待定系数法可知，当 p、q 不同时为 0，$0 \leqslant p \leqslant 2a$，$0 \leqslant q \leqslant 2b$，$(x - \beta_1)^{-p} \cdot (x - \beta_2)^{-q}$ 可以展开成 $\{(x - \beta_1)^{-\mu}, (x - \beta_2)^{-\lambda}\}_{\mu=1,\lambda=1}^{2a,2b}$ 乘以系数之和. (证毕)

引理 3 $\overrightarrow{(\alpha_i - \beta_1)^{-p} \cdot (\alpha_i - \beta_2)^{-q}}$，$\overrightarrow{(\alpha_i - \beta_1)^{-p+2i} \cdot (\alpha_i - \beta_2)^{-q}}$ 和 $\overrightarrow{(\alpha_i - \beta_1)^{-p} \cdot (\alpha_i - \beta_2)^{-q+2i}}$ 若有两个属于 H^*_s，则另一个也必属于 H^*_s.

证明 因为有关系式

$$\overrightarrow{(\alpha_i - \beta_1)^{-p} \cdot (\alpha_i - \beta_2)^{-q}} = (\beta_1 - \beta_2)^{-2i} [\overrightarrow{(\alpha_i - \beta_1)^{-p+2i} \cdot (\alpha_i - \beta_2)^{-q}} + \overrightarrow{(\alpha_i - \beta_1)^{-p} \cdot (\alpha_i - \beta_2)^{-q+2i}}]$$

再由引理 1 可得引理 3. (证毕)

用 (p, q) 表示向量 $\overrightarrow{(\alpha_i - \beta_1)^{-p} \cdot (\alpha_i - \beta_2)^{-q}}$. 因为 $(\alpha_i - \beta_1), (\alpha_i - \beta_2) \in F$，所以 $(\alpha_i - \beta_1)^{n^*} = (\alpha_i - \beta_2)^{n^*} = 1$. 故 (p, q) 中的 p, q 以 n^* 为循环周期，即 $(p, q) = (p \bmod n^*, q \bmod n^*)$. 运用这个记号我们得：由式 (2) 知，

$$(1,0),\cdots,(2a,0);(0,1),\cdots(0,2b)\in H_s^*. \tag{9}$$

再由引理 2 知，

$$(p,q)\in H_s^*，\text{这里 } p,q \text{ 不同时为 } 0，\ 0\leqslant p\leqslant 2a，\ 0\leqslant q\leqslant 2b. \tag{10}$$

由引理 1 知，

$$\text{若 } (p,q)\in H_s^*，\text{则 } (p2^j,q2^j)\in H_s^*. \tag{11}$$

由引理 3 知，

$$\text{若 } (p-2^j,q),(p,q),(p,q-2^j) \text{ 有两个属于 } H_s^*，\text{则另一个也属于 } H_s^*. \tag{12}$$

由式 (10)—(12) 和 $(p,q)=(p \bmod n^*,\ q \bmod n^*)$，我们可以求得 H_s^* 中所有 $\overrightarrow{(\alpha_i-\beta_1)^{-p}\cdot(\alpha_i-\beta_2)^{-q}}$ 型的向量．当然我们只对其中部分向量感兴趣．

例 1　考虑码长 $n=14$ 的二元 Goppa 码，其生成多项式 $G(z)=(z+\beta)^4\cdot z^2$，$\{\alpha_i+\beta,\alpha_i\}_{i=1}^{14}\subset GF(2^4)$，故 $n^*=15$．我们用 (p,q) 表示 $\overrightarrow{\alpha_i^{-q}\cdot(\alpha_i+\beta)^{-p}}$．运用式 (10)—(12)，我们可得到下面属于 H_s^* 部分向量，如图 1 所示．图中×标出的点是由式 (9) 决定的；○标出的点是由式 (11) 决定的；△标出的点是由式 (10) 决定的；●标出的点是由式 (12) 决定的．如 (6,0)，(4,2) $\in H_s^*$，故 $(6,2)\in H_s^*$．再如 $(12,4)\in H_s^*$，$(1,0)=(16,0)\in H_s^*$，故 $(16,4)=(1,4)\in H_s^*$．又如 $(0,4)\in H_s^*$，$(2,2)\in H_s^*$，故 $(2,4)\in H_s^*$．

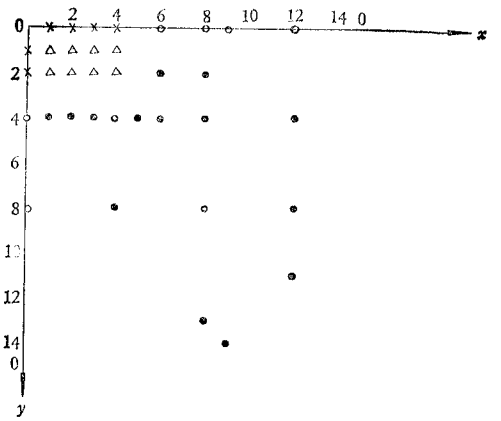

图 1　例 1 的 H_s^* 中部分向量

三、最小距离的新下限

对第二节的二元 Goppa 码，我们在原则上可以求出 H_s^* 中所有型如 $\overrightarrow{(\alpha_i-\beta_1)^{-p}}\ \overrightarrow{(\alpha_i-\beta_2)^{-q}}$ 的行向量．但在应用中只对其中部分向量感兴趣．这些部分向量构成矩阵 $\tilde{H}$，使它能运用定理 2，从而求得最大的 d'．下面用两个例子来说明详细过程．

例 2.　我们考虑例 1 中的二元 Goppa 码．由例 1 知，(8,0),(8,2)，(8,4)；(6,0)，

(6,2) (6,4); (4,0) (4,2), (4,4); (3,0), (3,2), (3,4); (2,0), (2,2), (2,4); (1,0), (1,2), (1,4)$\in H_s^*$, 由 (p,q) 的定义和式 (7) 的记号知:

$$\tilde{H}=\begin{bmatrix}\overrightarrow{(\alpha_i+\beta)^{-8}}\\ \overrightarrow{(\alpha_i+\beta)^{-6}}\\ \overrightarrow{(\alpha_i+\beta)^{-4}}\\ \overrightarrow{(\alpha_i+\beta)^{-3}}\\ \overrightarrow{(\alpha_i+\beta)^{-2}}\\ \overrightarrow{(\alpha_i+\beta)^{-1}}\end{bmatrix}\odot\begin{bmatrix}\overrightarrow{1}\\ \overrightarrow{\alpha_i^{-2}}\\ \overrightarrow{\alpha_i^{-4}}\end{bmatrix}\triangleq A\odot B. \tag{13}$$

因为矩阵 A 中加入两行 $\overrightarrow{(\alpha_i+\beta)^{-5}}$, $\overrightarrow{(\alpha_i+\beta)^{-7}}$ 后变成矩阵 A_E, 由 Vandermonde 矩阵性质知,矩阵 A_E 的任意 8 列线性无关, 由此矩阵 A 的任意 8 列的子矩阵秩为 6. 在矩阵 B 中,令 $x_i=\alpha_i^{-2}$, 再运用定理 2 知, 矩阵 $\tilde{H}$ 的任意 8 列线性无关, 再由定理 1 知, 这个二元 Goppa 码的最小距离 $\geqslant 9$. 但按文献 [2] 只能得到最小距离 $\geqslant 7$.

例 3 考虑 $G(z)=(z+1)^6\cdot z^4$, $L=GF(2^5)-\{0,1\}$ 的二元 Goppa 码, 它的码长 $n=30$, $n-k\leqslant 25$. 此时 $a=3$, $b=2$, $n^*=31$. 令 (p,q) 表示向量 $\overrightarrow{(\alpha_i+1)^{-p}\cdot\alpha_i^q}$, 则由式 (9) 知,

$$(5,0),\ (4,0),\ (1,0),\ (0,4),\ (3,0),\ (0,1),\ (0,3)\in H_s^*; \tag{14}$$

由式 (10) 知,

$$(5,4)\ (4,4),\ (1,4),\ (6,1),\ (5,1),\ (4,1),\ (5,2),\ (3,2),\ (3,1),$$
$$(2,1),\ (1,1),\ (1,2)\in H_s^*; \tag{15}$$

由式 (14) 运用式 (11) 知,

$$(9,0)=(5\cdot 8,\ 0\cdot 8),(24,0),\ (20,0),\ (16,0),\ (12,0),\ (8,0),(0,16),$$
$$(0,8),\ (0,12)\in H_s^*; \tag{16}$$

由式 (15) 运用式 (11) 知,

$$(24,4),\ (20,4),\ (16,4),\ (12,4),\ (8,4),\ (24,8),\ (20,8),\ (16,8)$$
$$(12,8),\ (8,8),\ (4,8)\in H_s^*; \tag{17}$$

由 $(1,0)=(32,0)\in H_s^*$ 和$(24,8)\in H_s^*$,运用式(12)知,$(32,8)=(1,8)\in H_s^*$; 再由$(5,4)\in H_s^*$,运用式 (12) 知, $(5,8)\in H_s^*$. 另一方面由$(9,0)\in H_s^*$, $(5,4)\in H_s^*$ 运用式 (12) 知 $(9,4)\in H_s^*$. 再由$(5,8)\in H_s^*$ 和$(9,4)\in H_s^*$运用式 (12) 知,

$$(9,8)\in H_s^*. \tag{18}$$

把式 (14)—(18) 中用~~~标志的属于 H_s^* 的组列于下面:

(0,4), (24,0), (20,0), (16,0), (12,0), (9,0), (8,0), (5,0), (4,0), (1,0)
(0,8), (24,4), (20,4), (16,4), (12,4), (9,4), (8,4), (5,4), (4,4), (1,4)
(0,12),(24,8), (20,8), (16,8), (12,8), (9,8), (8,8), (5,8), (4,8), (1,8)
(0,16).

由 (p,q) 的定义和式 (7) 的记号知:

$$\widetilde{H}=\begin{bmatrix}\overrightarrow{(\alpha_i+1)^{-24}}\\ \overrightarrow{(\alpha_i+1)^{-20}}\\ \overrightarrow{(\alpha_i+1)^{-16}}\\ \overrightarrow{(\alpha_i+1)^{-12}}\\ \overrightarrow{(\alpha_i+1)^{-9}}\\ \overrightarrow{(\alpha_i+1)^{-8}}\\ \overrightarrow{(\alpha_i+1)^{-5}}\\ \overrightarrow{(\alpha_i+1)^{-4}}\\ \overrightarrow{(\alpha_i+1)^{-1}}\\ \overrightarrow{(\alpha_i)^{-4}}\\ \overrightarrow{(\alpha_i)^{-8}}\end{bmatrix}\odot\begin{bmatrix}\overrightarrow{1}\\ \overrightarrow{(\alpha_i)^{-4}}\\ \overrightarrow{(\alpha_i)^{-8}}\end{bmatrix}\triangleq A\odot B. \tag{19}$$

因为 $(\alpha_i+1)^{-24}=(\alpha_i^4+1)^{-6}$, $(\alpha_i+1)^{-20}=(\alpha_i^4+1)^{-5}$, $(\alpha_i+1)^{-16}=(\alpha_i^4+1)^{-4}$, $(\alpha_i+1)^{-12}=(\alpha_i^4+1)^{-3}$, $(\alpha_i+1)^{-9}=(\alpha_i^4+1)^{-10}$, $(\alpha_i+1)^{-8}=(\alpha_i^4+1)^{-2}$, $(\alpha_i+1)^{-5}=(\alpha_i^4+1)^{-9}$, $(\alpha_i+1)^{-4}=(\alpha_i^4+1)^{-1}$, $(\alpha_i)^{-4}=(\alpha_i^4)^{-1}$, $(\alpha_i)^{-8}=(\alpha_i^4)^{-2}$. 若矩阵 A 中加入一行 $\overrightarrow{(\alpha_i^4+1)^{-7}}$, 并令 $\alpha_i^4=y_i$, 那么 A_E 变成广义 Cauchy 矩阵. 由文献[2]知, A_E 的任意 12 列线性无关. 由此, 矩阵 A 的任意 12 列的子矩阵的秩为 11, 更有 A 的任意 13 列的子矩阵的秩为 11. 在矩阵 B 中, 令 $\alpha_i^{-4}=x_i$, 再运用定理 2 知, 矩阵 $\widetilde{H}$ 的任意 13 列线性无关, 由此得, 该二元 Goppa 码的最小距离 $\geqslant 14$. 而文献[2]得到的下限为 11.

显然, 本文的方法也能用于获得其他二元 Goppa 码最小距离的新下限. 稍作推广, 本文的方法也可以用在其他多元 Goppa 码.

本文是在蔡长年教授的启发和帮助下完成的, 在此谨致衷心的感谢.

参　考　文　献

[1] Y. Sugiyama, M. Kasahara, S. Hirasawa and T. Namekawa, *IEEE Trans. on IT*, IT-**22**(1976), 518.
[2] 冯贵良, 电子学报, **11**(1983) 2, 65.
[3] K. K. Tzeng and E. Zimmermann, *IEEE Trans. on IT*, **IT-21**(1975), 712.
[4] 冯贵良, K. K. Tzeng, 中国科学, A辑 8(1983), 745.
[5] C. Roos, *IEEE Trans. on IT* **IT-29**(1983), 330.

A NEW LOWER BOUND FOR THE MINIMUM DISTANCE OF BINARY GOPPA CODES

Feng Guiliang

(Shanghai Institute of Computer Technology)

Binary Goppa codes are a large and powerful family of error-correcting codes. But how to find the true minimum distance of binary Goppa codes is not yet solved. This paper will give derivation of a new lower bound for the minimum distance of binary Goppa codes. This new lower bound improves the results obtained by Y. Sugiyama et al. (1976) and Feng Guiliang (1983). The method in this paper can be generalized for other Goppa codes easily.