中国科学: 数学 2024 年 第 54 卷 第 9 期: 1413 ~ 1420
SCIENTIA SINICA Mathematica
论 文

一类二元 Goppa 码及其诱导的新码

献给陆洪文教授 85 寿辰

吴严生[1], 李凤伟[2*], 胡丽琴[3], 岳勤[4]

1. 南京邮电大学计算机学院, 南京 210023;
2. 南京邮电大学理学院, 南京 210023;
3. 杭州电子科技大学网络空间学院, 杭州 310018;
4. 南京航空航天大学数学学院, 南京 210016

E-mail: yanshengwu@njupt.edu.cn, lfwzzu@126.com, huliqin@hdu.edu.cn, yueqin@nuaa.edu.cn

收稿日期: 2023-10-18; 接受日期: 2024-05-07; 网络出版日期: 2024-07-29; * 通信作者
国家自然科学基金 (批准号: 62372247, 12101326, 12171420 和 62172219)、江苏省自然科学基金 (批准号: BK20210575)、中国博士后科学基金 (批准号: 2023M740958) 和浙江省教育厅科研项目 (批准号: Y202249655) 资助项目

摘要 令 m 为正整数, $\mathbb{F}_{2^m}$ 是有限域. 设 L 为由 $\mathbb{F}_{2^m}$ 中的元素构成的子集, $G(x)=x^{3t}+1$, 其中 L 中的元素均不是 $G(x)$ 的根, 而且 $t\mid(2^m-1)$. 设 $\Gamma(L,G)$ 为以 $G(x)$ 作为 Goppa 多项式、L 为定义集的二元可分 Goppa 码. 本文证明该 Goppa 码的最小距离等于其设计距离, 即 $d=6t+1$. 这推广了 Bezzateev 和 Shekunova (1995) 的结果. 同时本文找到了许多新的二元线性码, 进一步扩充了 Grassl 的线上码表. 值得强调的是, 本文确定至少 3 个二元线性码是新发现的, 它们的参数分别为 $[32,16,8]$、$[62,43,8]$ 和 $[128,106,8]$. 这些码与 Grassl 码表中具有相同参数的码都不等价, 可被认为是具有该参数的已知最好的线性码.

关键词 Goppa 码 二元线性码 最小距离

MSC (2020) 主题分类 94B05

1 引言

1971 年, Goppa [12,13] 提出了 Goppa 码, 它是线性码中非常有趣的子类之一, 因为它渐近地满足 Varshamov-Gilbert 界 [3]. 这类码是广义 Reed-Solomon (generalized Reed-Solomon, GRS) 码的特定子域子码. 由于定义的复杂性和工具的缺乏, 关于 Goppa 码的文献并不多.

循环码是线性码的一个有趣的子类, 它们具有高效的编码和解码算法, 在电子商务、数据存储系统和通信系统中得到了广泛的应用. 这自然会令我们提出这样的问题: 什么情形下 Goppa 码是循环码? Goppa [12] 给出了 Goppa 码在一定对应关系下与循环码同构的充分必要条件. 之后, 一些结果陆续被发现 (参见文献 [2,4,7,19,23,24]), 但不得不说, 已知的循环 Goppa 码还是很少.

英文引用格式: Wu Y S, Li F W, Hu L Q, et al. A class of binary Goppa codes and induced new codes (in Chinese). Sci Sin Math, 2024, 54: 1413–1420, doi: 10.1360/SSM-2023-0284

McEliece [20] 提出了一种基于二元 Goppa 码的新公钥密码系统. 这使得 Goppa 码的研究在密码学中也引起了相当大的关注. 在美国国家标准与技术研究院 (National Institute of Standards and Technology, NIST) 后量子密码标准化的众多候选方案中, 其中一个就是以 McEliece 密码系统作为基础 [1], 这重新激发了学者们的研究兴趣.

最近, Gao 等 [11] 应用 Goppa 码的观点研究了 GRS 码的正交包; 紧接着, Huang 和 Yue [15]、Li 和 Yue [16,17]、Chen 和 Zhang [9,10] 研究了不可约 Goppa 码的数量; Sui 和 Yue [22] 给出了一种有效的扭 Goppa 码译码算法. López 和 Matthews [18] 介绍了多元 Goppa 码—经典 Goppa 码是它的一种特例, 还给出了多元 Goppa 码的校验矩阵, 并应用多元 Goppa 码得到了纠缠辅助量子纠错码、长码长的线性对偶互补码、自对偶码和自正交码.

综上所述, 关于 Goppa 码的研究还有许多工作要做. 特别地, 确定 Goppa 码的维数和最小距离是一件非常困难的事情. 已知最小距离的几类 Goppa 码罗列如下:

• 在文献 [21] 中, 假设码的长度与 Goppa 多项式的次数满足某个不等式时, Moreno 和 Moreno 通过指数和给出了最小距离等于 $2t+1$ 的 Goppa 码的一个子类.

• 在文献 [5] 中, Bezzateev 和 Shekunova 证明了可分多项式为 $G(x)=x^t+A$ 且定义集为 L 的二元 Goppa 码的最小距离等于 $2t+1$, 这里 L 中的元素都不是 $G(x)$ 的根, $t \mid (2^m-1)$, 且 A 为 $\mathbb{F}_{2^m}^*$ 中某元素的 t 次幂.

• 在文献 [6] 中, Bezzateev 和 Shekunova 证明了一些二元可分 Goppa 码形成一条链, 并且可以确定链上所有码的最小距离.

在上述一系列结果的启发下, 本文重点研究一类二元 Goppa 码, 并确定其最小距离. 特别地, 假设 $t \mid (2^m-1)$, 将 Bezzateev 和 Shekunova [5] 的结果推广到 $3t$ 的情形. 本文余下内容的结构如下. 第 2 节回顾 Goppa 码的定义及二元 Goppa 码的性质. 第 3 节给出本文的主要结果并且通过 Magma 给出具体的例子. 应用第 3 节构造的二元 Goppa 码, 第 4 节给出许多新二元线性码, 进一步扩充了 Grassl 的线上码表.

2 预备知识

令 n 为正整数, $\mathbb{F}_q^n$ 为有限域 $\mathbb{F}_q$ 上的所有 n 维向量构成的向量空间. 设向量 $\boldsymbol{x}=(x_0,x_1,\ldots,x_{n-1})$ 与 $\boldsymbol{y}=(y_0,y_1,\ldots,y_{n-1})\in\mathbb{F}_q^n$. 向量 $\boldsymbol{x}$ 的 Hamming 重量定义为

$$w_H(\boldsymbol{x})=|\{i: x_i\neq 0, 0\leqslant i\leqslant n-1\}|,$$

向量 $\boldsymbol{x}$ 与 $\boldsymbol{y}$ 的 Hamming 距离定义为

$$d_H(\boldsymbol{x},\boldsymbol{y})=|\{i: x_i\neq y_i, 0\leqslant i\leqslant n-1\}|.$$

称 $\mathbb{F}_q^n$ 在 $\mathbb{F}_q$ 上的一个 k 维线性子空间 $\mathcal{C}$ 为 $[n,k]$ q- 元线性码, 若 $\mathcal{C}$ 的最小 Hamming 距离等于 d, 记作 $[n,k,d]$ 线性码, 这里 $\mathcal{C}$ 的最小 Hamming 距离

$$d=d_H(\mathcal{C})=\min\{w_H(\boldsymbol{x}): \boldsymbol{x}\in\mathcal{C}, \boldsymbol{x}\neq\boldsymbol{0}\}.$$

下面介绍 Goppa 码的定义和一些性质.

定义 2.1 设 $G(x)$ 为多项式环 $\mathbb{F}_{q^m}[x]$ 中一个 t 次首 1 多项式, $L=\{\alpha_1,\alpha_2,\ldots,\alpha_n\}\subseteq\mathbb{F}_{q^m}$ 为 $\mathbb{F}_{q^m}$ 中 n 个不同元素组成的集合, 并且 $G(\alpha_i)\neq 0$, $i=1,\ldots,n$. 码长为 n 的 q 元 Goppa 码 $\Gamma(L,G)$ 定义为

$$\Gamma(L,G)=\left\{(c_1,c_2,\ldots,c_n)\in\mathbb{F}_q^n:\sum_{i=1}^{n}\frac{c_i}{x-\alpha_i}\equiv 0\ (\mathrm{mod}\ G(x)),c_i\in\mathbb{F}_q\right\},\tag{2.1}$$

这里 L 称为定义集, $G(x)$ 称为 Goppa 码 $\Gamma(L,G)$ 的 Goppa 多项式.

显然上面定义的 Goppa 码 $\Gamma(L,g)$ 是 $\mathbb{F}_q$ 上长度等于 $n=|L|$ 的线性码, 它的维数 $k\geqslant n-mt$, 最小距离 $d\geqslant t+1$ (参见文献 [19]). 令 $g_i=G(\alpha_i)^{-1}$, $1\leqslant i\leqslant n$, 则从方程 (2.1) 可以看出, $\Gamma(L,G)$ 的校验矩阵为

$$H=\begin{pmatrix}g_1 & g_2 & \cdots & g_n\\ g_1\alpha_1 & g_2\alpha_2 & \cdots & g_n\alpha_n\\ \vdots & \vdots & \ddots & \vdots\\ g_1\alpha_1^{t-1} & g_2\alpha_2^{t-1} & \cdots & g_n\alpha_n^{t-1}\end{pmatrix}.\tag{2.2}$$

定义 2.2 [19] 如果 Goppa 码的 Goppa 多项式 $G(x)$ 没有重根, 则称它为可分 Goppa 码.

对于二元 Goppa 码的情形, 有下面两个引理.

引理 2.1 [19] 设 $\Gamma(L,G)$ 为二元可分 Goppa 码, 其中 $L=\{\alpha\in\mathbb{F}_{2^m}:G(\alpha)\neq 0\}$ 且 $\deg(G(x))=t$, 则它的最小距离 $d\geqslant 2t+1$.

引理 2.2 [5] 设 $\Gamma(L,G)$ 为二元可分 Goppa 码, Goppa 多项式 $G(x)=x^t+A$, $L=\{\alpha\in\mathbb{F}_{2^m}:G(\alpha)\neq 0\}$. 若 $t\mid(2^m-1)$ 且 A 为 $\mathbb{F}_{2^m}^*$ 中元素的 t 次幂, 则它的最小距离 $d=2t+1$.

3 主要结果和例子

定理 3.1 设 $\Gamma(L,G)$ 为二元 Goppa 码, Goppa 多项式 $G(x)=x^{3t}+1$, 这里 $t\mid(2^m-1)$, $L=\{\alpha\in\mathbb{F}_{2^m}:G(\alpha)\neq 0\}$. 如果方程

$$\frac{x_1^t}{1+x_1^t+x_1^{2t}}+\frac{x_2^t}{1+x_2^t+x_2^{2t}}+\frac{x_3^t}{1+x_3^t+x_3^{2t}}=0\tag{3.1}$$

在集合 $\{\alpha\in\mathbb{F}_{2^m}^*:\alpha^t\neq 1\}^3$ 中至少有一个解 (x_1,x_2,x_3), 则二元 Goppa 码 $\Gamma(L,G)$ 的最小距离等于其设计距离, 即 $d=6t+1$.

证明 由引理 2.1 知, 仅需要证明在二元 Goppa 码 $\Gamma(L,G)$ 中存在一个码字的 Hamming 重量等于 $6t+1$.

为了方便证明, 引入几个记号. 令 $2^m-1=tl$, w 为 $\mathbb{F}_{2^m}$ 的一个本原元, 即 $\mathbb{F}_{2^m}^*=\langle w\rangle$, 则

$$\mathbb{F}_{2^m}^*=\bigcup_{i=0}^{l-1}w^i\langle w^l\rangle.$$

注意到, 如果 $3t\mid(2^m-1)$, 则从引理 2.2 直接可以得出结果. 下面总是假设 $3t\nmid(2^m-1)$. 由于 $t\mid(2^m-1)$, 所以有两种情形可能发生: $3\nmid(2^m-1)$, 即 m 为奇数; $v_3(t)=v_3(2^m-1)$ 且 m 为偶数, 这

里 $v_p(n)$ 表示整数 n 中素数 p 的指数. 则

$$\begin{aligned}\{\alpha \in \mathbb{F}_{2^m} : G(\alpha) = 0\} &= \{w^y, 0 \leqslant y \leqslant 2^m - 2 : w^{3yt} = 1\} \\ &= \{w^y, 0 \leqslant y \leqslant 2^m - 2 : 3yt \equiv 0 \pmod{2^m - 1}\} \\ &= \{w^y, 0 \leqslant y \leqslant 2^m - 2 : y \equiv 0 \pmod{l}\} \\ &= \langle w^l \rangle.\end{aligned}$$

因此该码的长度为 $n = |L| = 2^m - t = t(l-1) + 1$.

设 $L = \{\alpha_1, \ldots, \alpha_{n-1}, 0\} = \{0\} \cup \bigcup_{i=1}^{l-1} w^i \langle w^l \rangle$. 接下来从 (2.2) 得到此码的校验矩阵为

$$H = \begin{pmatrix} \frac{1}{\alpha_1^{3t}+1} & \frac{1}{\alpha_2^{3t}+1} & \cdots & \frac{1}{\alpha_{n-1}^{3t}+1} & 1 \\ \frac{\alpha_1}{\alpha_1^{3t}+1} & \frac{\alpha_2}{\alpha_2^{3t}+1} & \cdots & \frac{\alpha_{n-1}}{\alpha_{n-1}^{3t}+1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{\alpha_1^{3t-1}}{\alpha_1^{3t}+1} & \frac{\alpha_2^{3t-1}}{\alpha_2^{3t}+1} & \cdots & \frac{\alpha_{n-1}^{3t-1}}{\alpha_{n-1}^{3t}+1} & 0 \end{pmatrix}.$$

下面的证明思路是考虑选择 6 个不同的整数 $1 \leqslant i_1, i_2, i_3, i_4, i_5, i_6 \leqslant l-1$ 使得二元向量 $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ 的 Hamming 重量为 $6t+1$, 其中 $a_n = 1$ 且 $\boldsymbol{a}$ 的其他非零元与 L 的下列子集对应:

$$\{w^{i_j} \langle w^l \rangle : j = 1, \ldots, 6\}.$$

向量 $\boldsymbol{a} = (a_1, \ldots, a_n)$ 作为 $\Gamma(L, G)$ 的码字当且仅当 $H\boldsymbol{a}^{\mathrm{T}} = 0$.

固定 i, 对于 $w^i \langle w^l \rangle$ 中的任意元素 α, 因为 $(2^m - 1) = tl$, 故有 $\alpha^{3t} = w^{3it}$. 从而有

$$\frac{1}{w^{3it}+1} + \frac{1}{w^{3jt}+1} + 1 = \frac{1 + w^{3it}w^{3jt}}{(w^{3it}+1)(w^{3jt}+1)}. \tag{3.2}$$

方程 (3.2) 等于 0 当且仅当 $w^{3t(i+j)} = 1$, 即 $i + j \equiv 0 \pmod{l}$. 这样就得到了 6 个不同的整数 $1 \leqslant i_1, i_2, i_3, i_4, i_5, i_6 \leqslant l-1$ 满足

$$i_1 + i_2 = i_3 + i_4 = i_5 + i_6 = l. \tag{3.3}$$

由方程 (3.2) 和 (3.3), 有

$$\frac{1}{w^{3i_1t}+1} + \frac{1}{w^{3i_2t}+1} + \frac{1}{w^{3i_3t}+1} + \frac{1}{w^{3i_4t}+1} + \frac{1}{w^{3i_5t}+1} + \frac{1}{w^{3i_6t}+1} + 1 = 0. \tag{3.4}$$

对于固定的 i, $1 \leqslant j \leqslant 3t-1$, 且 $t \nmid j$, 可以得到

$$\sum_{z \in w^i \langle w^l \rangle} \frac{z^j}{z^{3t}+1} = \frac{w^{ij}(\sum_{i'=1}^{t} w^{li'j})}{w^{3it}+1} = 0. \tag{3.5}$$

因为 $w^{lj} \neq 1$, 所以最后一个方程成立. 对应 $t \mid j$, 需要考虑 $j = t$ 与 $j = 2t$. 通过方程 (3.2), 可得

$$\sum_{z \in w^{i_1} \langle w^l \rangle} \frac{z^t}{z^{3t}+1} + \sum_{z \in w^{i_2} \langle w^l \rangle} \frac{z^t}{z^{3t}+1} = \frac{tw^{i_1t}}{w^{3i_1t}+1} + \frac{tw^{-i_1t}}{w^{-3i_1t}+1} = \frac{w^{i_1t}}{w^{3i_1t}+1} + \frac{w^{-i_1t}}{w^{-3i_1t}+1} \tag{3.6}$$

且

$$\sum_{z\in w^{i_1}\langle w^l\rangle}\frac{z^{2t}}{z^{3t}+1}+\sum_{z\in w^{i_2}\langle w^l\rangle}\frac{z^{2t}}{z^{3t}+1}=\frac{tw^{2i_1t}}{w^{3i_1t}+1}+\frac{tw^{-2i_1t}}{w^{-3i_1t}+1}=\frac{w^{2i_1t}}{w^{3i_1t}+1}+\frac{w^{-2i_1t}}{w^{-3i_1t}+1}. \tag{3.7}$$

令 $\beta_1=w^{i_1t}$. 根据方程 (3.6) 与 (3.7), 有

$$\frac{\beta_1}{\beta_1^3+1}+\frac{\beta_1^{-1}}{\beta_1^{-3}+1}=\frac{\beta_1^2}{\beta_1^3+1}+\frac{\beta_1^{-2}}{\beta_1^{-3}+1}=\frac{\beta_1}{1+\beta_1+\beta_1^2}. \tag{3.8}$$

同理, 令 $\beta_3=w^{i_3t}$ 与 $\beta_5=w^{i_5t}$, 有

$$\frac{\beta_3}{\beta_3^3+1}+\frac{\beta_3^{-1}}{\beta_3^{-3}+1}=\frac{\beta_3^2}{\beta_3^3+1}+\frac{\beta_3^{-2}}{\beta_3^{-3}+1}=\frac{\beta_3}{1+\beta_3+\beta_3^2} \tag{3.9}$$

且

$$\frac{\beta_5}{\beta_5^3+1}+\frac{\beta_5^{-1}}{\beta_5^{-3}+1}=\frac{\beta_5^2}{\beta_5^3+1}+\frac{\beta_5^{-2}}{\beta_5^{-3}+1}=\frac{\beta_5}{1+\beta_5+\beta_5^2}. \tag{3.10}$$

根据方程 (3.4) 和 (3.8)–(3.10), 向量 $\boldsymbol{a}$ 为该码的码字当且仅当

$$\frac{\beta_1}{1+\beta_1+\beta_1^2}+\frac{\beta_3}{1+\beta_3+\beta_3^2}+\frac{\beta_5}{1+\beta_5+\beta_5^2}=0. \tag{3.11}$$

通过选择 6 个不同的整数 $1\leqslant i_1,i_2,i_3,i_4,i_5,i_6\leqslant l-1$ 使得方程 (3.3) 与 (3.11) 成立, 这样就完成了定理的证明. □

注 3.1 定理 3.1 将确定最小距离的困难问题转化为在有限域的某个子集上求解方程的问题. 看起来工作量似乎减少了, 但不得不说, 在有限域的子集上求解方程 (3.1) 也很困难.

注 3.2 在定理 3.1 中, 条件 $t\mid(2^m-1)$ 不可少. 例如, 令 $m=8$, $t=11$. 设

$$G(x)=x^{33}+1,\quad L=\{\alpha\in\mathbb{F}_{2^8}^*:G(\alpha)\neq0\},$$

由 Magma, 该二元 Goppa 码 $\Gamma(L,G)$ 的参数为 $[253,11,72]$.

接下来, 通过一些例子来说明主要结果.

例 3.1 令 $m=5$, $t=1$, 且 $\mathbb{F}_{2^5}^*=\langle w\rangle$. 由 Magma 可得

$$\frac{x_1}{1+x_1+x_1^2}+\frac{x_2}{1+x_2+x_2^2}+\frac{x_3}{1+x_3+x_3^2}=0$$

有解 $x_1=w^3$, $x_2=w^6$, $x_3=w^{11}$. 设 $G(x)=x^3+1$, $L=\{\alpha\in\mathbb{F}_{2^5}^*:G(\alpha)\neq0\}$. 根据定理 3.1, 该二元 Goppa 码 $\Gamma(L,G)$ 的最小距离为 7, 这一结果经过 Magma 验证. 事实上, 此二元线性码的参数为 $[31,16,7]$. 由文献 [14] 可知, 码长为 31、维数为 16 的二元线性码的最小距离下界是 8, 在文献 [14] 的线上码表中没有发现具有参数 $[31,16,7]$ 的二元线性码.

例 3.2 令 $m=7$, $t=1$, 且 $\mathbb{F}_{2^7}^*=\langle w\rangle$. 由 Magma 可得

$$\frac{x_1}{1+x_1+x_1^2}+\frac{x_2}{1+x_2+x_2^2}+\frac{x_3}{1+x_3+x_3^2}=0$$

有解 $x_1=w$, $x_2=w^4$, $x_3=w^{41}$. 设 $G(x)=x^3+1$, $L=\{\alpha\in\mathbb{F}_{2^7}^*:G(\alpha)\neq0\}$, 根据定理 3.1, 二元 Goppa 码 $\Gamma(L,G)$ 的最小距离为 7, 这一结果经过 Magma 验证. 事实上, 此二元线性码的参数为 $[127,106,7]$. 由文献 [14] 可知, 一个已知最好的二元线性码具有参数 $[127,106,8]$.

例 3.3 令 $m=8$, $t=3$, 且 $\mathbb{F}_{2^8}^*=\langle w\rangle$. 由 Magma 可得

$$\frac{x_1^3}{1+x_1^3+x_1^6}+\frac{x_2^3}{1+x_2^3+x_2^6}+\frac{x_3^3}{1+x_3^3+x_3^6}=0$$

有解 $x_1=w^4$, $x_2=w^5$, $x_3=w^{39}$. 设 $G(x)=x^9+1$, $L=\{\alpha\in\mathbb{F}_{2^8}^*: G(\alpha)\neq 0\}$, 根据定理 3.1, 二元 Goppa 码 $\Gamma(L,G)$ 的最小距离为 19, 这一结果经过 Magma 验证. 事实上, 此二元线性码的参数为 $[253,181,19]$. 由文献 [14] 可知, 码长为 253、维数为 181 的二元线性码的最小距离下界为 20, 在文献 [14] 的线上码表中没有发现具有参数 $[253,182,19]$ 的二元线性码.

例 3.4 令 $m=8$, $t=15$, 且 $\mathbb{F}_{2^8}^*=\langle w\rangle$. 由 Magma 可得

$$\frac{x_1^{15}}{1+x_1^{15}+x_1^{30}}+\frac{x_2^{15}}{1+x_2^{15}+x_2^{30}}+\frac{x_3^{15}}{1+x_3^{15}+x_3^{30}}=0$$

有 4 个解 $x_1=w^{i_1}$, $x_2=w^{i_2}$, $x_3=w^{i_3}$ 且 $\langle i_1,i_2,i_3\rangle\in\{\langle 2,5,7\rangle,\langle 3,4,7\rangle,\langle 3,6,8\rangle,\langle 1,5,6\rangle\}$. 设 $G(x)=x^{45}+1$, $L=\{\alpha\in\mathbb{F}_{2^8}^*: G(\alpha)\neq 0\}$, 根据定理 3.1, 二元 Goppa 码 $\Gamma(L,G)$ 的最小距离为 91, 这一结果经过 Magma 验证. 事实上, 此二元线性码的参数为 $[241,4,91]$. 由文献 [14] 可知, 一个已知最好的二元线性码具有参数 $[241,4,128]$.

例 3.5 令 $m=9$, $t=1$, 且 $\mathbb{F}_{2^9}^*=\langle w\rangle$. 由 Magma 可得

$$\frac{x_1}{1+x_1+x_1^2}+\frac{x_2}{1+x_2+x_2^2}+\frac{x_3}{1+x_3+x_3^2}=0$$

有解 $x_1=w$, $x_2=w^5$, $x_3=w^{69}$. 设 $G(x)=x^3+1$, $L=\{\alpha\in\mathbb{F}_{2^9}^*: G(\alpha)\neq 0\}$, 根据定理 3.1, 二元 Goppa 码 $\Gamma(L,G)$ 的最小距离为 7, 这一结果经过 Magma 验证. 事实上, 此二元线性码的参数为 $[511,484,7]$.

例 3.6 令 $m=10$, $t=3$, 且 $\mathbb{F}_{2^{10}}^*=\langle w\rangle$. 由 Magma 可得

$$\frac{x_1^3}{1+x_1^3+x_1^6}+\frac{x_2^3}{1+x_2^3+x_2^6}+\frac{x_3^3}{1+x_3^3+x_3^6}=0$$

有解 $x_1=w$, $x_2=w^6$, $x_3=w^{33}$. 设 $G(x)=x^9+1$, $L=\{\alpha\in\mathbb{F}_{2^{10}}^*: G(\alpha)\neq 0\}$, 根据定理 3.1, 二元 Goppa 码 $\Gamma(L,G)$ 的最小距离为 19, 这一结果经过 Magma 验证. 事实上, 此二元线性码的参数为 $[1021,931,19]$.

注 3.3 由于 Magma 计算能力的限制, 当 $m>9$ 且 $t>3$ 时, 我们没有给出更多的例子.

在 Magma 的帮助下, 通过大量例子, 验证了下面猜想在 $m\leqslant 8$ 时成立.

猜想 3.1 令 $\mathrm{rad}(t)$ 为 t 的所有不同素因子的乘积. 设 $G(x)=x^t+A$, $\mathrm{rad}(t)\mid(2^m-1)$, 则二元 Goppa 码 $\Gamma(L,G)$ 的最小距离为 $d=2t+1$, 这里 A 为 $\mathbb{F}_{2^m}^*$ 中某个元素的 t 次幂.

作为未来工作, 希望可以确定更多 Goppa 码的最小距离. 读者也可以考虑攻克上述猜想.

4 新的二元线性码

第 3 节已经给出了一些二元线性 Goppa 码. 本节将从中找出一些新的二元线性码.

注意到 Carrasquillo-López 等 [8] 根据 Goppa 多项式 $(x^{15}+1)^6$、$(x^{16}+1)^6$ 和 $(x^{17}+1)^6$, 成功找到了一些好的二元线性码. 设 $\mathcal{C}$ 为 $[n,k,d]$ 码, 自然可以构造出 $[n,n-k,d^\perp]$ 对偶码、$[n-1,k,d-1]$ 删节码和 $[n-1,k-1,d]$ 短化码.

表 1 定理 3.1 中的二元线性码

m	t	$[n,k,d]$	注记
4	1	$[13,2,7]$	几乎最优
5	1	$[31,16,7]$	几乎最优
6	1	$[61,43,7]$	几乎最优
6	3	$[55,16,19]$	几乎最优
7	1	$[127,106,7]$	几乎最优
8	1	$[253,229,7]$	几乎最优
8	3	$[253,181,19]$	
8	5	$[241,124,31]$	
8	15	$[241,4,91]$	
8	17	$[205,2,103]$	
9	1	$[511,484,7]$	

表 2 更多新二元线性码

$[n,k,d]$	来自表 1 构造的码
$[12,2,6]$	$[13,2,7]$ 在位置 1 处的删节码
$[14,2,8]$	$[13,2,7]$ 的扩展码
$[31,15,6]$	$[31,16,7]$ 的对偶码
$[30,16,6]$	$[31,16,7]$ 在位置 1 处的删节码
$[29,16,5]$	$[31,16,7]$ 在位置 1 和 2 处的删节码
$[30,15,7]$	$[31,16,7]$ 在位置 1 处的短化码
$[32,16,8]^*$	$[31,16,7]$ 的扩展码
$[61,18,16]$	$[61,43,7]$ 的对偶码
$[60,43,6]$	$[61,43,7]$ 在位置 1 处的删节码
$[60,42,7]$	$[61,43,7]$ 在位置 1 处的短化码
$[62,43,8]^*$	$[61,43,7]$ 的扩展码
$[126,105,7]$	$[127,106,7]$ 在位置 1 处的短化码
$[127,21,43]$	$[127,106,7]$ 的对偶码
$[128,106,8]^*$	$[127,106,7]$ 的扩展码

根据定理 3.1, 表 1 罗列出了一些线性码. 根据文献 [14] 中最新的线上码表, 标记出了几乎最优码, 几乎最优指的是 $[n,k,d]$ 码为距离几乎最优, 即 $[n,k,d+1]$ 码是最优的. 表 2 列出了一些新的二元线性码以及基于它们所构造出来的码, 其中 * 指该码与文献 [14] 中已知最好的参数相同的线性码不等价. 由于我们构造的二元线性码的码长可以很大, 无法与线上码表 [14] 中的参数进行比较, 但我们相信得到的二元码中包含了更多新码. 上面所得结果都已通过 Magma 验证.

参考文献

1 Albrecht M R, Bernstein D J, Chou T, et al. Classic McEliece: Conservative code-based cryptography. HAL Open Science, 2022, 1: hal-04288769

2 Berger T P. New classes of cyclic extended Goppa codes. IEEE Trans Inform Theory, 1999, 45: 1264–1266

3 Berlekamp E R. Goppa codes. IEEE Trans Inform Theory, 1973, 19: 590–592

4 Berlekamp E R, Moreno O. Extended double-error-correcting binary Goppa codes are cyclic. IEEE Trans Inform Theory, 1973, 19: 817–818
5 Bezzateev S V, Shekhunova N A. Subclass of binary Goppa codes with minimal distance equal to the design distance. IEEE Trans Inform Theory, 1995, 41: 554–555
6 Bezzateev S V, Shekhunova N A. Chain of separable binary Goppa codes and their minimal distance. IEEE Trans Inform Theory, 2008, 54: 5773–5778
7 Bezzateev S V, Shekhunova N A. Subclass of cyclic Goppa codes. IEEE Trans Inform Theory, 2013, 59: 7379–7385
8 Carrasquillo-López J L, Gómez-Flores A O, Soto C, et al. Introducing three best known binary Goppa codes. arXiv:2010.07278, 2020
9 Chen B, Zhang G. Enumeration of extended irreducible binary Goppa codes. IEEE Trans Inform Theory, 2022, 68: 5145–5153
10 Chen B, Zhang G. The number of extended irreducible binary Goppa codes. arXiv:2204.02083, 2022
11 Gao Y, Yue Q, Huang X, et al. Hulls of generalized Reed-Solomon codes via Goppa codes and their applications to quantum codes. IEEE Trans Inform Theory, 2021, 67: 6619–6626
12 Goppa V D. A new class of linear error correcting codes. Probl Inf Trans, 1970, 6: 24–30
13 Goppa V D. Rational representation of codes and $G(L, g)$ codes. Prohl Perehach Inform, 1971, 7: 41–49
14 Grassl M. Bounds on the minimum distance of linear codes. Http://www.codetables.de, 2021
15 Huang D, Yue Q. Extended irreducible binary sextic Goppa codes. IEEE Trans Inform Theory, 2022, 68: 230–237
16 Li X, Yue Q. Non-binary irreducible quasi-cyclic parity-check subcodes of Goppa codes and extended Goppa codes. Des Codes Cryptogr, 2022, 90: 1629–1647
17 Li X, Yue Q. Construction of expurgated and extended Goppa codes with dihedral automorphism groups. IEEE Trans Inform Theory, 2022, 68: 6472–6480
18 López H H, Matthews G L. Multivariate Goppa codes. IEEE Trans Inform Theory, 2022, 69: 126–137
19 MacWilliams F J, Sloane N J A. The Theory of Error-Correcting Codes. Amsterdam: North Holland, 1977
20 McEliece R J. A public-key cryptosystem based on algebraic coding theory. Deep Space Network Progress Report, 1978, 44: 114–116
21 Moreno C J, Moreno O. Exponential sums and Goppa codes. II. IEEE Trans Inform Theory, 1992, 38: 1222–1229
22 Sui J, Yue Q. Twisted Goppa codes with an efficient decoding algorithm and quasi-cyclic properties. IEEE Trans Inform Theory, 2023, 69: 5660–5669
23 Tzeng K K, Yu C Y. Characterization theorems for extending Goppa codes to cyclic codes. IEEE Trans Inform Theory, 1979, 25: 246–250
24 Tzeng K K, Zimmermann K. On extending Goppa codes to cyclic codes. IEEE Trans Inform Theory, 1975, 21: 712–716

A class of binary Goppa codes and induced new codes

Yansheng Wu, Fengwei Li, Liqin Hu & Qin Yue

Abstract Let m be a positive integer and $\mathbb{F}_{2^m}$ be a finite field. A binary Goppa code $\Gamma(L, G)$ is specified by a separable Goppa polynomial $G(x) = x^{3t} + 1$ and a locator set L of elements of $\mathbb{F}_{2^m}$, where no elements of L may be a root of $G(x)$ and $t \mid (2^m - 1)$. For the nontrivial code, we prove that its minimum distance is equal to the design distance, namely $d = 6t + 1$. This extends a result of Bezzateev and Shekunova (1995). We also present many new binary linear codes, which extend the codetable of Grassl as a byproduct. It is worth emphasizing that we have identified at least three binary linear codes with parameters $[32, 16, 8]$, $[62, 43, 8]$, and $[128, 106, 8]$, respectively. These codes are considered the best-known linear codes with these specific parameters and are not equivalent to any codes with the same parameters listed in the Grassl's codetable.

Keywords **Goppa code, binary linear code, minimum distance**

MSC(2020) **94B05**

doi: 10.1360/SSM-2023-0284