

基于 \mathbb{F}_q^* 的循环子群的极大距离可分码和近极大距离可分码的构造

杜小妮^{①②③} 薛婧^{*①} 乔兴斌^{①②} 赵紫薇^①

^①(西北师范大学数学与统计学院 兰州 730070)

^②(西北师范大学密码技术与数据分析重点实验室 兰州 730070)

^③(甘肃省数学与统计学基础学科研究中心 兰州 730070)

摘要: 极大距离可分(MDS)码和近极大距离可分(NMDS)码因其具有良好的代数结构和纠错能力, 在通信系统、数据存储和密钥共享方案等领域有广泛的应用。该文利用偶特征有限域 \mathbb{F}_{q^2} 的乘法群 $\mathbb{F}_{q^2}^*$ 的循环子群 U_{q+1} , 构造了几类码长为 $q+3$ 的MDS码和NMDS码, 并运用 U_{q+1} 的性质, 确定了所构造码的参数和重量计数器, 利用Magma程序举例验证了结论的正确性, 另外, 计算了NMDS码的最小局部度, 得到了几类最优的局部修复码。特别地, 所构造的码均是关于Griesmer界的最优码。

关键词: 极大距离可分码; 近极大距离可分码; 重量计数器; 局部修复码; Griesmer界

中图分类号: TN918.1; O157.4

文献标识码: A

文章编号: 1009-5896(2025)YU-0001-08

DOI: 10.11999/JEIT251204

CSTR: 32379.14.JEIT251204

1 引言

设 p 为素数, m 为正整数, $q = p^m$ 。 \mathbb{F}_q 是含有 q 个元素的有限域, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ 。记 \mathbb{F}_q^n 为 \mathbb{F}_q 上的 n 维向量空间, 则 \mathbb{F}_q 上参数为 $[n, k]$ 的线性码 C 是 \mathbb{F}_q^n 的一个 k 维子空间, 其中 n 为码长, k 为信息位数。若 C 的最小汉明距离(重量)为 d , 则记为 $[n, k, d]$ 线性码。定义 $[n, k]$ 线性码 C 的对偶码为 $C^\perp = \{\mathbf{y} \in \mathbb{F}_q^n : \langle \mathbf{x}, \mathbf{y} \rangle = 0, \forall \mathbf{x} \in C\}$, 其中 $\langle \mathbf{x}, \mathbf{y} \rangle$ 表示向量 \mathbf{x}, \mathbf{y} 的点积。显然 C^\perp 的参数为 $[n, n-k]$ 。 \mathbb{F}_q 上 $[n, k]$ 线性码 C 的一组基构成的 $k \times n$ 矩阵 \mathbf{G} 称为该码的生成矩阵。若 \mathbf{H} 是 \mathbb{F}_q 上的 $(n-k) \times n$ 矩阵且满足 $C = \{\mathbf{x} \in \mathbb{F}_q^n : \mathbf{H}\mathbf{x}^\top = 0\}$, 则称 \mathbf{H} 为 C 的校验矩阵, 其中“ \top ”表示向量的转置。码 C 中的每一个向量 $\mathbf{c} = (c_1, c_2, \dots, c_n)$ 称为码字, 其支撑定义为 $\text{supp}(\mathbf{c}) = \{i \in [n] : c_i \neq 0\}$, 其中 $[n] = \{1, 2, \dots, n\}$ 。显然, 码字 \mathbf{c} 的汉明重量 $\text{wt}(\mathbf{c}) = \#\text{supp}(\mathbf{c})$, 其中 $\#S$ 表示集合 S 的基数。设 A_i 表示长度为 n 的码 C 中汉明重量为 i 的码字个数, 其中 $i \in [n]$, C 的重量计数器定义为 $1 + \sum_{i=1}^n A_i x^i$ 。序列 $(1, A_1, A_2, \dots, A_n)$

称为码 C 的重量分布。线性码的重量分布包含了关于码的纠错能力、检错概率和纠错概率等重要信息。因此, 研究线性码的重量分布问题在编码理论中备受关注^[1-3]。

线性码 C 的参数 n, k, d 受到一些界的约束, 若 C 的参数恰好达到某个界, 则称 C 为最优码。码的Griesmer界^[4]定义为 $n \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil$, 其中 $\lceil x \rceil$ 表示大于等于 x 的最小整数。如果 C 的参数 n (或 $n-1$), k 和 d 达到Griesmer界, 则称其为Griesmer码(或near Griesmer码)。码的Singleton界定义为: $d \leq n - k + 1$ 。当 C 的最小距离 d 达到Singleton界时, 即 $d = n - k + 1$ 时, 码 C 被称为极大距离可分(Maximum Distance Separable, MDS)码。MDS码的对偶码也是MDS码。当 $d = n - k$ 时, 称 C 为几乎极大距离可分(Almost MDS, AMDS)码。AMDS码的对偶码不一定是AMDS码。若码 C 及其对偶码都是AMDS码, 则称其为近极距离可分(Near MDS, NMDS)码。NMDS码不仅在编码理论中具有重要地位, 而且在组合数学、密钥共享方案以及局部修复码(Locally Recoverable Code, LRC)等领域也有着广泛的应用。近年来, 构造最优或接近最优的线性码是编码理论中重要的研究课题之一。众多学者针对MDS码和NMDS码的构造问题进行了深入研究, 相关研究结果见文献^[5-9]。

设 C 是 \mathbb{F}_q 上 $[n, k, d]$ 线性码, 对任意 $i \in [n]$, 都存在大小为 r 的子集 $R_i \subseteq [n] \setminus \{i\}$ 以及 \mathbb{F}_q^* 上的函数 $f_i(x_1, x_2, \dots, x_r)$, 使得对于任意码字 $\mathbf{c} = (c_1, c_2, \dots, c_n) \in C$ 都有 $c_i = f_i(\mathbf{c}_{R_i})$, 其中 \mathbf{c}_{R_i} 是码字 \mathbf{c} 在集合 R_i 上的投影, R_i 称为 c_i 的修复集, 则称 C 是局部度

收稿日期: 2025-11-14; 改回日期: 2026-01-08; 网络出版: 2026-01-25

*通信作者: 薛婧 xjingmath@163.com

基金项目: 国家自然科学基金(62562055, 62172337), 甘肃省自然科学基金重点资助项目(23JRRA685), 甘肃省基础研究创新群体基金(23JRRA684)

Foundation Items: The National Natural Science Foundation of China (62562055, 62172337), The Key Project of Gansu Natural Science Foundation (23JRRA685), The Funds for Innovative Fundamental Research Group Project of Gansu Province (23JRRA684)

为 r 的局部修复码,记为 $(n, k, d, q; r)$ -LRC。使得 C 是 $(n, k, d, q; r)$ -LRC最小 r 称为 C 的最小局部度。局部修复码是一种通过局部修复提高存储节点修复效率的重要编码方法,可应用于分布式存储系统中,以保证存储系统的可靠性,近年来,该编码方法成为研究的热点。2021年, Luo等人^[10]提出了一种构造局部度为2的2元局部修复码的新方法。2023年, Tan等人^[6]研究了几类三维NMDS码的局部度,得到了几类距离最优和维数最优局部修复码。同年, Heng等人^[7]利用有限域上的某些特殊矩阵构造了无限族NMDS码,并得到了几类最优的局部修复码。2024年, Ding等人^[9]构造了4类四维NMDS码,确定了这些NMDS码的对偶码的局部度,得到了4类距离最优和维数最优的局部修复码。因此构造具有较小局部度的NMDS码是极具价值的研究课题。

本文受Tang等人^[11]和Yin等人^[8]工作的启发,令 $U_{q+1} = \{u \in \mathbb{F}_{q^2} : u^{q+1} = 1\} = \langle \alpha \rangle$,也称为单位圆盘,首先选取矩阵

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_q & \alpha_{q+1} \\ f(\alpha_1) & f(\alpha_2) & \cdots & f(\alpha_q) & f(\alpha_{q+1}) \end{bmatrix} \quad (1)$$

其中, $q = 2^m$, m 为正整数, $f(x) = x^2$, $\alpha_i = \alpha^i$, $1 \leq i \leq q+1$ 。其次,在 \mathbf{G} 中添加两个线性无关的列向量 $\mathbf{g}_j = (a_{1j}, a_{2j}, a_{3j}) \in \mathbb{F}_{q^2}^3$ 且 $j \in \{1, 2\}$,将其作为生成矩阵构造新的MDS码和NMDS码,并根据 $\mathbf{g}_1, \mathbf{g}_2$ 的重量取值,利用 U_{q+1} 的性质计算码的重量计数器。最后,作为应用,基于文献^[6]中计算NMDS码最小局部度的方法,判定了本文所构造的部分NMDS码均是满足Singleton-like界、Cadambe-Mazumdar界、Plotkin-like界和Griesmer-like界的最优局部修复码。

2 一些辅助引理

如下引理刻画了线性码的最小距离与其校验矩阵之间的关系。

引理1^[12] 设 C 是 \mathbb{F}_q 上 $[n, k]$ 线性码,其校验矩阵为 \mathbf{H} ,则 C 的最小距离为 d 当且仅当 \mathbf{H} 的任意 $d-1$ 列均 \mathbb{F}_q 线性无关,并且 \mathbf{H} 有 d 列是 \mathbb{F}_q 线性相关的。

引理2~引理5给出MDS码和NMDS码的一些相关性质。

引理2^[12] 设 C 是 \mathbb{F}_q 上 $[n, k]$ 线性码, \mathbf{G} 和 \mathbf{H} 分别是 C 的生成矩阵和校验矩阵,则以下条件等价。

- (1) C 是MDS码;
- (2) \mathbf{G} 的任意 k 列在 \mathbb{F}_q 上线性无关;
- (3) \mathbf{H} 的任意 $n-k$ 列在 \mathbb{F}_q 上线性无关;

(4) C^\perp 是MDS码。

引理3^[12] 设 C 是 \mathbb{F}_q 上的 $[n, k, d]$ MDS码,即 $d = n - k + 1$,则 C 的重量分布为当 $1 \leq i < d$ 时, $A_i = 0$;当 $d \leq i \leq n$ 时

$$A_i = \binom{n}{i} \sum_{j=0}^{i-d} (-1)^j \binom{i}{j} (q^{i+1-d-j} - 1) \quad (2)$$

引理4^[13] 设 C 是 \mathbb{F}_q 上的 $[n, k, n-k]$ NMDS码, $(1, A_1, A_2, \dots, A_n)$ 和 $(1, A_1^\perp, A_2^\perp, \dots, A_n^\perp)$ 分别是 C 和 C^\perp 的重量分布,则 $A_{n-k+s} = \binom{n}{k-s} \sum_{j=0}^{s-1} (-1)^j \binom{n-k+s}{j} (q^{s-j} - 1) + (-1)^s \binom{k}{s} A_{n-k}$, $s \in [k]$, $A_{k+s}^\perp = \binom{n}{k+s} \sum_{j=0}^{s-1} (-1)^j \binom{k+s}{j} (q^{s-j} - 1) + (-1)^s \binom{n-k}{s} A_k^\perp$, $s \in [n-k]$ 。

下面介绍NMDS码 C 的最小重量码字与 C^\perp 的最小重量码字之间的关系。

引理5^[14] 设 C 是NMDS码。则对于 C 中任意的最小重量码字 \mathbf{c} ,在 C^\perp 中存在唯一的最小重量码字 \mathbf{c}^\perp (在不考虑与 \mathbf{c}^\perp 线性相关的码字的情形下),使得 $\text{supp}(\mathbf{c}) \cap \text{supp}(\mathbf{c}^\perp) = \emptyset$ 。特别地,码 C 及其对偶码 C^\perp 的最小重量码字的数量相同。

设 $\text{Tr}_1^m(x) = x + x^2 + x^{2^2} + \dots + x^{2^{m-1}}$ 为 \mathbb{F}_{2^m} 到 \mathbb{F}_2 的迹函数,引理6给出了在特征为2的有限域中,利用迹函数判断2次方程解的个数的方法。

引理6^[15] 设 $f(x) = ax^2 + bx + c \in \mathbb{F}_{2^m}[x]$, $a \neq 0$,则

- (1) 如果 $b = 0$,那么 f 在 \mathbb{F}_{2^m} 中有一个解;
- (2) 如果 $b \neq 0$ 且 $\text{Tr}_1^m(ac/b^2) = 0$,那么 f 在 \mathbb{F}_{2^m} 中有两个解;
- (3) 如果 $b \neq 0$ 且 $\text{Tr}_1^m(ac/b^2) = 1$,那么 f 在 \mathbb{F}_{2^m} 中无解。

引理7 若局部修复码 $(n, k, d, q; r)$ -LRC的参数满足如下4个界之一,则称其为最优的LRC。

(1) Singleton-like界^[16]

$$d \leq n - k - \left\lfloor \frac{k}{r} \right\rfloor + 2 \quad (3)$$

(2) Cadambe-Mazumdar界^[17]

$$k \leq \min_{t \in \mathbb{Z}^+} [rt + k_{\text{opt}}^{(q)}(n - t(r+1), d)] \quad (4)$$

其中 $k_{\text{opt}}^{(q)}(n, d) = \max\{k : \text{在}\mathbb{F}_q\text{上存在}[n, k, d]\text{线性码}\}$, \mathbb{Z}^+ 表示正整数集合。

(3) Plotkin-like界^[18]

$$d \leq \min_{1 \leq \tau \leq \lfloor \frac{k}{r} \rfloor - 1} \frac{q^{k-\tau r - 1} (q-1) [n - \tau(r+1)]}{q^{k-\tau r} - 1} \quad (5)$$

(4)Griesmer-like界^[18]

$$n \geq \max_{1 \leq \tau \leq \lceil \frac{k}{r} \rceil - 1} \left\{ \tau(r+1) + \sum_{t=0}^{k-\tau r-1} \left\lceil \frac{d}{q^r} \right\rceil \right\} \quad (6)$$

记 C^\perp 的最小距离为 d^\perp ，下面给出非平凡线性码($d^\perp > 1$)有最小局部度的充要条件。

引理8^[6] 设 C 是码长为 n 的非平凡线性码，则 C 具有最小局部度 $d^\perp - 1$ 当且仅当 $\cup_{S \in \mathcal{B}_{d^\perp}(C^\perp)} S = [n]$ ，其中 $\mathcal{B}_{d^\perp} = \{\text{supp}(c) : c \in C^\perp, \text{wt}(c) = d^\perp\}$ 。

3 参数为 $[q+3, 3]$ 的MDS码和NMDS码

本节将利用式(1)定义的矩阵 \mathbf{G} ，构造几类长度为 $q+3$ 的3维MDS码和NMDS码，并确定其重量计数器。为方便起见，令 $\dim(C)$ 和 $d(C)$ 分别表示线性码 C 的维数和最小距离。

下文中总假设 $q = 2^m$ ， $m \geq 2$ 为正整数且 $(1, x, x^2)$ 与 $\mathbf{g}_1 = (a_{11}, a_{21}, a_{31})$ ， $\mathbf{g}_2 = (a_{12}, a_{22}, a_{32}) \in \mathbb{F}_q^3$ 线性无关。定义 \mathbb{F}_q^2 上的 $3 \times (q+3)$ 矩阵 $\mathbf{G}_1 = (\mathbf{G} | \mathbf{g}_1^\top | \mathbf{g}_2^\top)$ ，其中 \mathbf{G} 由式(1)给出。设 C_1 是由 \mathbf{G}_1 生成的线性码。下面为了计算 C_1 的频数，考虑 \mathbf{G}_1 的子矩阵 $\mathbf{T}_j = \begin{bmatrix} 1 & 1 & a_{1j} \\ x & y & a_{2j} \\ x^2 & y^2 & a_{3j} \end{bmatrix}$ ， $\mathbf{T}_3 = \begin{bmatrix} 1 & a_{11} & a_{12} \\ x & a_{21} & a_{22} \\ x^2 & a_{31} & a_{32} \end{bmatrix}$ 其中 $x, y \in U_{q+1}$ ， $x \neq y$ 且 $j \in \{1, 2\}$ 。显然 $|\mathbf{T}_j| = (x+y) \cdot (a_{1j}xy + a_{2j}(x+y) + a_{3j})$ ， $|\mathbf{T}_3| = (a_{11}a_{12} + a_{12}a_{21}) \cdot x^2 + (a_{12}a_{31} + a_{11}a_{32})x + a_{21}a_{32} + a_{31}a_{22}$ 。

本节的讨论总是基于假设：当 $a_{11}a_{32} + a_{12}a_{31} \neq 0$ 时

$$\text{Tr}_1^m \left(\frac{(a_{11}a_{22} + a_{12}a_{21})(a_{21}a_{32} + a_{22}a_{31})}{(a_{11}a_{32} + a_{12}a_{31})^2} \right) = 1 \quad (7)$$

事实上，Magma实验表明，如果式(7)不成立，则由 \mathbf{G}_1 生成的线性码 C_1 会出现五重的情况，不在本文的讨论范围之内。显然，由引理6式(3)和式(7)可得 $|\mathbf{T}_3|$ 在 \mathbb{F}_q^2 上恒不为0。

接下来按照 $\text{wt}(\mathbf{g}_1)$ ， $\text{wt}(\mathbf{g}_2)$ 的取值给出 C_1 的参数和重量计数器。首先讨论 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (3, 3)$ 的情形。要完成主要结论的证明，需要以下引理。

引理9^[19] 设 $\text{wt}(\mathbf{g}_j) = 3$ ， $a_j = a_{2j}a_{3j}^q + a_{1j}a_{2j}^q$ ， $b_j = a_{1j}^{q+1} + a_{3j}^{q+1}$ ， $c_j = a^q$ ，其中 $j \in \{1, 2\}$ ，则

(1) 若 $a_j = b_j = 0$ ，或 $a_j b_j \neq 0$ 且 $\text{Tr}_1^m(a_j c_j / b_j^2) = 1$ ，则 \mathbb{F}_q^2 上使得 $|\mathbf{T}_j| = 0$ 的 (x, y) 的个数分别为 $q/2$ 和1。

(2) 在其余情形下，在 \mathbb{F}_q^2 上恒有 $|\mathbf{T}_j| \neq 0$ 。

定理1 设 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (3, 3)$ ，则以下结论成立。

(1) 若 $|\mathbf{T}_j|$ 中至少有1个为0，其中 $j \in \{1, 2\}$ ，则

C_1 是 \mathbb{F}_q^2 上的 $[q+3, 3, q]$ NMDS码。特别地，以下5种情形码 C_1 的重量分布分别对应表1中第1~5行。

(a) $a_j = b_j = 0$;

(b) $a_j b_j \neq 0$ 且 $\text{Tr}_1^m(a_j c_j / b_j^2) = 1$;

(c) $a_i = b_i = 0$ ， $a_j b_j \neq 0$ 且 $\text{Tr}_1^m(a_j c_j / b_j^2) = 1$ ，

其中 $i, j \in \{1, 2\}$ 且 $i \neq j$;

(d) $a_i = b_i = 0$ 且 $|\mathbf{T}_j| \neq 0$ ，其中 $i, j \in \{1, 2\}$ 且 $i \neq j$;

(e) $a_i b_i \neq 0$ ， $\text{Tr}_1^m(a_i c_i / b_i^2) = 1$ 且 $|\mathbf{T}_j| \neq 0$ ，其中 $i, j \in \{1, 2\}$ 且 $i \neq j$ 。

(2) 若 $|\mathbf{T}_j| \neq 0$ ，其中 $j \in \{1, 2\}$ ，则 C_1 是 \mathbb{F}_q^2 上的 $[q+3, 3, q+1]$ MDS码，重量计数器为

$$A(z) = 1 + \frac{(q+3)(q+2)(q^2-1)}{2} z^{q+1} + (q+3) \cdot (q^2-1)(q^2-q-1) z^{q+2} + \frac{(q-1)(q+1)^2(2q^3-4q^2+q+2)}{2} z^{q+3} \quad (8)$$

证明 以下分3步给出证明。

步骤1 首先确定线性码 C_1 和 C_1^\perp 的维数。对于任意不同的元素 $x, y, z \in U_{q+1}$ ，有

$$\begin{vmatrix} 1 & 1 & 1 \\ x & y & z \\ x^2 & y^2 & z^2 \end{vmatrix} = (x+y)(x+z)(y+z) \neq 0 \quad (9)$$

因此矩阵 \mathbf{G}_1 的秩等于3，即 $\dim(C_1) = 3$ ，显然 $\dim(C_1^\perp) = q$ 。若 $\mathbf{g}_1, \mathbf{g}_2$ 的选取满足引理9(2)的条件，则有 $|\mathbf{T}_j| \neq 0$ ， $j \in \{1, 2\}$ 。又由 $|\mathbf{T}_3| \neq 0$ 可知， \mathbf{G}_1 中任意3列线性无关，故由引理2可知， C_1 为 $[q+3, 3, q+1]$ MDS码。

另外，根据引理9式(1)可得，当 $a_j = b_j = 0$ ，或者 $a_j b_j \neq 0$ 且 $\text{Tr}_1^m(a_j c_j / b_j^2) = 1$ 时，有 $|\mathbf{T}_j| = 0$ ， $j \in \{1, 2\}$ ，此时 \mathbf{G}_1 中存在3列线性相关。由引理1可知， $d(C_1^\perp) = 3$ ，即 C_1^\perp 是AMDS码。又由Singleton界知， C_1 是 $[q+3, 3, d(C_1)]$ 且 $d(C_1) \leq q+1$ 的线性码。

步骤2 证明 $d(C_1) = q$ 。若 $d(C_1) = q+1$ ，则 C_1 是参数为 $[q+3, 3, q+1]$ 的MDS码。由引理2可知， C_1^\perp 是 $[q+3, q, 4]$ MDS码，这与 $d(C_1^\perp) = 3$ 矛盾。因此不妨设 $d(C_1) \leq q-1$ ，且 $\mathbf{c} = a\mathbf{r}_1 + b\mathbf{r}_2 + c\mathbf{r}_3$ 是 C_1 中重量最小的非零码字，其中 $(a, b, c) \in \mathbb{F}_q^3$ ，且 $\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3$ 为 \mathbf{G}_1 的行向量，所以 \mathbf{c} 的 $q+3$ 个分量中至少存在4个分量为0。下面分两种情形讨论。

(1) 假设 \mathbf{c} 的最后两个分量为0。因为 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (3, 3)$ ，不妨假设 $a_{11} = a_{12} = 1$ 。则存在不

表1 NMDS码 C_1 的重量分布(不包括 A_0)

A_q	A_{q+1}	A_{q+2}	A_{q+3}
$q(q^2 - 1)$	$\frac{(q^2 - 1)(q^2 - q + 6)}{2}$	$(q^2 - 1)(q^3 + 2q^2 - q - 3)$	$\frac{(q - 1)^2(q + 1)(2q^3 - 3q - 2)}{2}$
$2(q^2 - 1)$	$\frac{(q^2 - 1)(q^2 + 5q - 6)}{2}$	$(q^2 - 1)(q^3 + 2q^2 - 4q + 3)$	$\frac{(q^2 - 1)(2q^4 - 2q^3 - 3q^2 + 3q - 2)}{2}$
$\frac{(q + 2)(q^2 - 1)}{2}$	$\frac{q(q^2 - 1)(q + 2)}{2}$	$\frac{q(q^2 - 1)(2q^2 + 4q - 5)}{2}$	$\frac{q(q^2 - 1)(2q^3 - 2q^2 - 3q + 2)}{2}$
$\frac{q(q^2 - 1)}{2}$	$\frac{(q^2 - 1)(q^2 + 2q + 6)}{2}$	$\frac{(q^2 - 1)(2q^3 + 4q^2 - 5q - 6)}{2}$	$\frac{(q^2 - 1)(2q^4 - 2q^3 - 3q^2 + 2q + 2)}{2}$
$q^2 - 1$	$\frac{(q^2 - 1)(q^2 + 5q)}{2}$	$q(q^2 - 1)(q^2 + 2q - 4)$	$\frac{q(q^2 - 1)(q - 1)(2q^3 - 3)}{2}$

同 $x, y \in U_{q+1}$ 使得 $a + bx + cx^2 = 0, a + by + cy^2 = 0, a + ba_{21} + ca_{31} = 0, a + ba_{22} + ca_{32} = 0$.

由 $|T_3| \neq 0$ 知, 上述方程组只有唯一解 $a = b = c = 0$, 从而码字 $\mathbf{c} = \mathbf{0}$, 矛盾.

(2)假设 \mathbf{c} 的最后两个分量至多有1个为0, 因此可以推断出 \mathbf{c} 的前 $q + 1$ 个分量中至少有3个0, 即存在不同的 $x, y, z \in U_{q+1}$ 满足 $a + bx + cx^2 = 0, a + by + cy^2 = 0, a + bz + cz^2 = 0$.

由式(9)可得, 上述方程组只有零解 $a = b = c = 0$. 因此 $\mathbf{c} = \mathbf{0}$, 矛盾.

综上可得, 当 $a_j = b_j = 0$, 或者 $a_j b_j \neq 0$ 且 $\text{Tr}_1^m(a_j c_j / b_j^2) = 1$ 时, $d(C_1) = q, j \in \{1, 2\}$. 此时 C_1 是参数为 $[q + 3, 3, q]$ 的NMDS码.

步骤3 确定NMDS码 C_1 的重量计数器. 首先计算 A_3^+ 的值, 设 $\mathbf{c} \in C_1^+$ 且 $\text{supp}(\mathbf{c}) = \{k_1, k_2, k_3\}$. 考虑以下3种情形.

(1)若 $\text{supp}(\mathbf{c}) \subseteq [q + 1]$, 由式(9)可得, C_1^+ 中不存在这样的码字 \mathbf{c} .

(2)若 $\text{supp}(\mathbf{c}) = \{k_1, k_2, k_3\}$, 其中 $\{k_1, k_2\} \subseteq [q + 1], k_3 \in \{q + 2, q + 3\}$. 根据 $\text{wt}(\mathbf{g}_1) = \text{wt}(\mathbf{g}_2) = 3$ 以及引理9可知, C_1^+ 中满足 $k_3 = q + 2$ 的码字 \mathbf{c} 的个数为 $q/2(q^2 - 1)$; 类似地, 满足 $k_3 = q + 3$ 的码字 \mathbf{c} 的个数为 $q^2 - 1$.

(3)由 $|T_3| \neq 0$ 可知, C_1^+ 中不存在 $\text{supp}(\mathbf{c}) = \{k_1, q + 2, q + 3\}$ 的码字, 其中 $k_1 \in [q + 1]$.

综上所述, 当 $a_j = b_j = 0$ 时, $A_3^+ = q(q^2 - 1)$; 当 $a_j b_j \neq 0$ 且 $\text{Tr}_1^m(a_j c_j / b_j^2) = 1$ 时, $A_3^+ = 2(q^2 - 1)$; 当 $a_i = b_i = 0, a_j b_j \neq 0$ 且 $\text{Tr}_1^m(a_j c_j / b_j^2) = 1, A_3^+ = (q + 2)(q^2 - 1)/2$, 其中 $i \in \{1, 2\}$ 且 $i \neq j$; 当 $a_i = b_i = 0$ 且 $|T_j| \neq 0$, 其中 $i, j \in \{1, 2\}$ 且 $i \neq j, A_3^+ = q/2(q^2 - 1)$; 当 $a_i b_i \neq 0, \text{Tr}_1^m(a_i c_i / b_i^2) = 1$ 且 $|T_j| \neq 0$, 其中 $i, j \in \{1, 2\}$ 且 $i \neq j, A_3^+ = q^2 - 1$. 最后利用引理4和引理5计算可得 C_1 的重量计数器.

特别地, 当码 C_1 是MDS码时, 由引理3可得 C_1 的重量计数器. 证毕

下面通过Magma实验验证定理1的正确性.

例1 (1)取 $m = 2, \mathbf{g}_1 = (\zeta^6, \zeta, \zeta^6)$ 以及 $\mathbf{g}_2 = (\zeta^7, \zeta, \zeta^5)$, 其中 ζ 是 $\mathbb{F}_{4^2}^*$ 的生成元. 此时 $a_1 = b_1 = 0, a_2 = \zeta, b_2 = 1$, 即 $a_2 b_2 = \zeta \neq 0$ 且 $\text{Tr}_1^m(a_2 c_2 / b_2^2) = \zeta^2 + \zeta = 1$, 则 C_1 是 $[7, 3, 4]$ NMDS码, 重量计数器为 $A(z) = 1 + 45z^4 + 180z^5 + 1290z^6 + 2580z^7$, 这与定理1(1)的结论一致.

(2)取 $m = 2, \mathbf{g}_1 = (\zeta^{14}, \zeta^{13}, \zeta^{10})$ 以及 $\mathbf{g}_2 = (\zeta^{14}, \zeta^8, \zeta^{14})$, 其中 ζ 是 $\mathbb{F}_{4^2}^*$ 的生成元. 此时 $a_1 = \zeta, b_1 = 1, \text{Tr}_1^m(a_1 c_1 / b_1^2) = \zeta^2 + \zeta = 1, a_2 = 1, b_2 = 0$, 则 C_1 是 $[7, 3, 4]$ NMDS码, 重量计数器为 $A(z) = 1 + 15z^4 + 270z^5 + 1200z^6 + 2610z^7$, 这与定理1(2)的结论一致.

(3)取 $m = 2, \mathbf{g}_1 = (\zeta, \zeta^{10}, \zeta^{12})$ 以及 $\mathbf{g}_2 = (\zeta^{11}, \zeta^{13}, \zeta^{11})$, 其中 ζ 是 $\mathbb{F}_{4^2}^*$ 的生成元. 此时 $a_1 = 1 \neq 0, b_1 = \zeta \neq 0, a_2 = b_2 = 0$ 且 $\text{Tr}_1^m(a_2 c_2 / b_2^2) = \zeta^2 + \zeta = 0$, 则 C_1 是 $[7, 3, 5]$ MDS码, 重量计数器为 $A(z) = 1 + 315z^5 + 1155z^6 + 2625z^7$, 这与定理1(3)的结论一致.

在继续讨论之前, 先给出两个必要的引理, 其用于判断在 $\text{wt}(\mathbf{g}_j) = 2$ 时 $|T_j|$ 是否为0.

引理10^[19] 设 $\text{wt}(\mathbf{g}_j) = 2$ 且 $\mathbf{g}_j = (a_{1j}, 0, a_{3j})$, 其中 $j \in \{1, 2\}$, 则以下结论成立.

(1)若 $a_{3j}/a_{1j} \in U_{q+1}$, 则 \mathbb{F}_{q^2} 上使得 $|T_j| = 0$ 的 (x, y) 个数为 $q/2$.

(2)若 $a_{3j}/a_{1j} \notin U_{q+1}$, 则在 \mathbb{F}_{q^2} 上恒有 $|T_j| \neq 0$. 下面令 $D = \{u_1 + u_2 : u_1, u_2 \in U_{q+1} \text{ 且 } u_1 \neq u_2\}$.

引理11^[19] 设 $\text{wt}(\mathbf{g}_j) = 2$ 且 $\mathbf{g}_j = (a_{1j}, a_{2j}, 0)$, 其中 $j \in \{1, 2\}$, 则以下结论成立:

(1)若 m 为偶数, $a_{1j}/a_{2j} \notin U_{q+1}$ 且 $a_{1j}/a_{2j} \in D$, 或者 m 为奇数且 $a_{1j}/a_{2j} \in D$, 则 \mathbb{F}_{q^2} 上使得 $|T_j| = 0$ 的 (x, y) 个数为1.

(2)在其余情形下, 在 \mathbb{F}_{q^2} 上恒有 $|T_j| \neq 0$.

特别地, 当 $\text{wt}(\mathbf{g}_j) = 2$ 且 $\mathbf{g}_j = (0, a_{2j}, a_{3j})$ 时, 结论与引理11类似, 此处不再赘述.

结合引理9~引理11, 并参照定理1的证明方法, 可得到定理2~定理9的结论。由于证明过程类似, 故而后续定理中不再赘述。定理2和定理3给出了 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (3, 2)$ 时线性码 C_1 的参数和重量计数器。

定理2 设 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (3, 2)$ 且 $a_{22} = 0$, 则以下结论成立。

(1)若 $|T_j|$ 中至少有1个为0, 其中 $j \in \{1, 2\}$, 则 C_1 是 \mathbb{F}_{q^2} 上的 $[q+3, 3, q]$ NMDS码。特别地, 以下5种情形码的重量分布分别对应表1中第1, 3, 4, 5, 4行。

(a) $a_1 = b_1 = 0$ 且 $a_{32}/a_{12} \in U_{q+1}$;

(b) $a_1 b_1 \neq 0$, $\text{Tr}_1^m(a_1 c_1 / b_1^2) = 1$ 且 $a_{32}/a_{12} \in U_{q+1}$;

(c) $a_1 = b_1 = 0$ 且 $a_{32}/a_{12} \notin U_{q+1}$;

(d) $a_1 b_1 \neq 0$, $\text{Tr}_1^m(a_1 c_1 / b_1^2) = 1$ 且 $a_{32}/a_{12} \notin U_{q+1}$;

(e) $|T_1| \neq 0$ 且 $a_{32}/a_{12} \in U_{q+1}$ 。

(2)若 $|T_1| \neq 0$ 且 $a_{32}/a_{12} \notin U_{q+1}$, 则 C_1 是 \mathbb{F}_{q^2} 上的 $[q+3, 3, q+1]$ MDS码, 重量计数器为式(8)。

定理3 设 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (3, 2)$ 且 $a_{32} = 0$, 则以下结论成立。

(1)若 $|T_j|$ 中至少有1个为0时, 其中 $j \in \{1, 2\}$, 则 C_1 是 \mathbb{F}_{q^2} 上的 $[q+3, 3, q]$ NMDS码。特别地, 在以下5种情形下, 码的重量分布分别对应表1中第3, 2, 4, 5, 5行。

(a)当 $a_1 = b_1 = 0$ 时, 若 m 为偶数, $a_{12}/a_{22} \notin U_{q+1}$ 且 $a_{12}/a_{22} \in D$, 或者 m 为奇数, $a_{12}/a_{22} \in D$;

(b)当 $a_1 b_1 \neq 0$, $\text{Tr}_1^m(a_1 c_1 / b_1^2) = 1$ 时, 若 m 为偶数, $a_{12}/a_{22} \notin U_{q+1}$ 且 $a_{12}/a_{22} \in D$, 或者 m 为奇数, $a_{12}/a_{22} \in D$;

(c) $a_1 = b_1 = 0$ 且 $|T_2| \neq 0$;

(d) $a_1 b_1 \neq 0$, $\text{Tr}_1^m(a_1 c_1 / b_1^2) = 1$ 且 $|T_2| \neq 0$;

(e)当 $|T_1| \neq 0$, 若 m 为偶数, $a_{12}/a_{22} \notin U_{q+1}$ 且 $a_{12}/a_{22} \in D$, 或者 m 为奇数且 $a_{12}/a_{22} \in D$ 。

(2)若 $|T_j| \neq 0$, 其中 $j \in \{1, 2\}$, 则 C_1 是 \mathbb{F}_{q^2} 上的 $[q+3, 3, q+1]$ MDS码, 重量计数器为式(8)。

当 $a_{12} = 0$ 时, 结论与定理3的结论类似, 此处不再讨论。

下面给出Magma实验验证定理2~定理3的正确性。

例2 (1)取 $m = 2$, $\mathbf{g}_1 = (\zeta^{12}, \zeta^5, \zeta^3)$ 以及 $\mathbf{g}_2 = (\zeta^4, 0, \zeta^7)$, 其中 ζ 是 $\mathbb{F}_{4^2}^*$ 的生成元。此时 $a_1 = b_1 = 0$, $\zeta^7/\zeta^{10} \in U_{q+1}$, 则 C_1 是 $[7, 3, 4]$ NMDS码, 重量计数器为 $A(z) = 1 + 60z^4 + 135z^5 + 1335z^6 + 2565z^7$, 这与定理2(1)的结论一致。

(2)取 $m = 2$, $\mathbf{g}_1 = (\zeta^4, \zeta^7, \zeta^9)$ 以及 $\mathbf{g}_2 = (1, 0, \zeta^9)$, 其中 ζ 是 $\mathbb{F}_{4^2}^*$ 的生成元。此时 $a_1 = \zeta^{14}$, $b_1 = \zeta^{10}$, $\text{Tr}_1^m(a_1 c_1 / b_1^2) = \zeta^5 + \zeta^{10} = 1$, 则 C_1 是 $[7, 3, 4]$ NMDS码, 重量计数器为 $A(z) = 1 + 45z^4 + 180z^5 + 1290z^6 + 2580z^7$, 这与定理2(1)的结论一致。

例3 (1)取 $m = 2$, $\mathbf{g}_1 = (\zeta^{10}, \zeta^5, \zeta^{10})$ 以及 $\mathbf{g}_2 = (\zeta^2, \zeta^{12}, 0)$, 其中 ζ 是 $\mathbb{F}_{4^2}^*$ 的生成元。此时 $a_1 = b_1 = 0$, $\zeta^2/\zeta^{12} \notin U_{q+1}$, 则 C_1 是 $[7, 3, 4]$ NMDS码, 重量计数器为 $A(z) = 1 + 45z^4 + 180z^5 + 1290z^6 + 2580z^7$, 这与定理3(1)的结论一致。

(2)取 $m = 2$, $\mathbf{g}_1 = (\zeta^8, \zeta^{12}, \zeta^{11})$ 以及 $\mathbf{g}_2 = (\zeta^3, \zeta^3, 0)$, 其中 ζ 是 $\mathbb{F}_{4^2}^*$ 的生成元。此时 $a_1 = b_1 = 0$, 则 C_1 是 $[7, 3, 4]$ NMDS码, 重量计数器为 $A(z) = 1 + 30z^4 + 225z^5 + 1245z^6 + 2595z^7$, 这与定理3(2)的结论一致。

下面确定 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (3, 1)$ 时码 C_1 的参数和重量计数器。注意到此时 $|T_2| \neq 0$ 。

定理4 设 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (3, 1)$, 则以下结论成立。

(1)若 $|T_1| = 0$, 则 C_1 是 \mathbb{F}_{q^2} 上的 $[q+3, 3, q]$ NMDS码, 特别地, 当 $a_1 = b_1 = 0$, 或者 $a_1 b_1 \neq 0$ 且 $\text{Tr}_1^m(a_1 c_1 / b_1^2) = 1$ 时, 码的重量分布分别对应表1第4, 5行。

(2)若 $|T_1| \neq 0$, 则 C_1 是 \mathbb{F}_{q^2} 上的 $[q+3, 3, q+1]$ MDS码, 重量计数器为式(8)。

定理5~定理7给出当 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (2, 2)$ 时线性码 C_1 的参数及其重量计数器, 具体结果如下。

定理5 设 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (2, 2)$ 且 $a_{21} = a_{32} = 0$, 则以下结论成立。

(1)若 $|T_j|$ 中至少有1个为0时, 其中 $j \in \{1, 2\}$, 则 C_1 是 \mathbb{F}_{q^2} 上的 $[q+3, 3, q]$ NMDS码。特别地, 以下3种情形码的重量分布分别对应表1第3, 4, 5行。

(a)当 $a_{31}/a_{11} \in U_{q+1}$, 若 m 为偶数, $a_{12}/a_{22} \notin U_{q+1}$ 且 $a_{12}/a_{22} \in D$, 或者若 m 为奇数, $a_{12}/a_{22} \in D$;

(b) $a_{31}/a_{11} \in U_{q+1}$ 且 $|T_2| \neq 0$;

(c)当 $a_{31}/a_{11} \notin U_{q+1}$, 若 m 为偶数, $a_{12}/a_{22} \notin U_{q+1}$ 且 $a_{12}/a_{22} \in D$, 或者 m 为奇数且 $a_{12}/a_{22} \in D$ 。

(2)若 $|T_1| \neq 0$, 其中 $j \in \{1, 2\}$, 则 C_1 是 \mathbb{F}_{q^2} 上的 $[q+3, 3, q+1]$ MDS码, 重量计数器为式(8)。

定理6 设 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (2, 2)$ 且 $a_{11} = a_{32} = 0$, 则以下结论成立。

(1)若 $|T_j|$ 中至少有1个为0时, 其中 $j \in \{1, 2\}$, 则 C_1 是 \mathbb{F}_{q^2} 上的 $[q+3, 3, q]$ NMDS码。特别地, 在以下3种情形下, 码的重量分布分别对应表1第2, 5, 5行。

(a)当 m 为偶数, $a_{31}/a_{21}, a_{12}/a_{22} \notin U_{q+1}$ 且 $a_{31}/$

$a_{21}, a_{12}/a_{22} \in D$, 或者 m 为奇数且 $a_{31}/a_{21}, a_{12}/a_{22} \in D$;

(b) 当 m 为偶数, $a_{31}/a_{21} \notin U_{q+1}, a_{31}/a_{21} \in D$ 且 $|T_2| \neq 0$, 或者当 m 为奇数, $a_{31}/a_{21} \in D$ 且 $|T_2| \neq 0$;

(c) 当 m 为偶数, $a_{12}/a_{22} \notin U_{q+1}, a_{12}/a_{22} \in D$ 且 $|T_1| \neq 0$, 或者当 m 为奇数, $a_{12}/a_{22} \in D$ 且 $|T_1| \neq 0$.

(2) 若 $|T_1| \neq 0$, 其中 $j \in \{1, 2\}$, 则 C_1 是 \mathbb{F}_{q^2} 上的 $[q+3, 3, q+1]$ MDS码, 重量计数器为式(8)。

定理7 设 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (2, 2)$ 且 $a_{2j} = 0$, 其中 $j \in \{1, 2\}$, 则以下结论成立。

(1) 若 $|T_j|$ 中至少有1个为0时, 其中 $j \in \{1, 2\}$, 则 C_1 是 \mathbb{F}_{q^2} 上的 $[q+3, 3, q]$ NMDS码。特别地, 对 $j \in \{1, 2\}$ 满足 $a_{3j}/a_{1j} \in U_{q+1}$, 或者对 $i, j \in \{1, 2\}$ 且 $i \neq j$ 满足 $a_{3i}/a_{1i} \in U_{q+1}$ 和 $a_{3j}/a_{1j} \notin U_{q+1}$, 码的重量分布分别对应表1第1, 4行。

(2) 若 $a_{3j}/a_{1j} \notin U_{q+1}, j \in \{1, 2\}$, 则 C_1 是 \mathbb{F}_{q^2} 上的 $[q+3, 3, q+1]$ MDS码, 重量计数器为式(8)。

以下借助 Magma实验的具体实例, 对定理5加以验证。

例4 (1) 取 $m = 2, \mathbf{g}_1 = (\zeta^{11}, 0, \zeta^8)$ 以及 $\mathbf{g}_2 = (\zeta^6, \zeta^5, 0)$, 其中 ζ 是 $\mathbb{F}_{4^2}^*$ 的生成元。此时 $\zeta^8/\zeta^{11} \in U_{q+1}, \zeta^6/\zeta^5 \notin U_{q+1}$, 则 C_1 是 $[7, 3, 4]$ NMDS码, 重量计数器为 $A(z) = 1 + 45z^4 + 180z^5 + 1290z^6 + 2580z^7$, 这与定理5(1)的结论一致。

(2) 取 $m = 2, \mathbf{g}_1 = (\zeta^{10}, 0, \zeta^7)$ 以及 $\mathbf{g}_2 = (1, \zeta^6, 0)$, 其中 ζ 是 $\mathbb{F}_{4^2}^*$ 的生成元。此时 $a_1 = b_1 = 0$, 则 C_1 是 $[7, 3, 4]$ NMDS码, 重量计数器为 $A(z) = 1 + 30z^4 + 225z^5 + 1245z^6 + 2595z^7$, 这与定理5(2)的结论一致。

注1 显然当 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (2, 2)$ 且满足 $a_{11} = a_{12} = 0$ 或者 $a_{31} = a_{32} = 0$ 时, 线性码 C_1 的参数及其重量计数器的结论与定理6一致, 故不再讨论。

定理8~定理10分别刻画了 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (2, 1), (1, 1)$ 时码 C_1 的性质, 此时 $|T_2| \neq 0$ 。

定理8 设 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (2, 1)$ 且 $a_{21} = 0$, 则以下结论成立。

(1) 若 $a_{31}/a_{11} \in U_{q+1}$, 则 C_1 是 \mathbb{F}_{q^2} 上的 $[q+3, 3, q]$ NMDS码, 重量计数器为表1第4行;

(2) 若 $a_{31}/a_{11} \notin U_{q+1}$, 则 C_1 是 \mathbb{F}_{q^2} 上 $[q+3, 3, q+1]$ MDS码, 重量计数器为式(8)。

注2 显然当定理8取 $a_{11} = a_{31} = a_{22} = 1$ 时, 即为文献[8]中定理5.2的线性码。

定理9 设 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (2, 1)$ 且 $a_{11} = 0$, 则以下结论成立。

(1) 若 m 为偶数, $a_{31}/a_{21} \notin U_{q+1}$ 且 $a_{31}/a_{21} \in D$,

或者 m 为奇数, $a_{31}/a_{21} \in D$, 则 C_1 是 \mathbb{F}_{q^2} 上的 $[q+3, 3, q]$ NMDS码, 重量计数器为表1第2行;

(2) 在其余情形下, C_1 是 \mathbb{F}_{q^2} 上 $[q+3, 3, q+1]$ MDS码, 重量计数器为式(8)。

当 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (2, 1)$ 且 $a_{31} = 0$ 时, 结论与定理9结论类似, 此处不再讨论。

定理10 设 $(\text{wt}(\mathbf{g}_1), \text{wt}(\mathbf{g}_2)) = (1, 1)$, 则 C_1 是 \mathbb{F}_{q^2} 上的 $[q+3, 3, q+1]$ MDS码, 重量计数器为式(8)。

注3 根据Griesmer界, 本文所构造的MDS码均为Griesmer码, NMDS码均为near Griesmer码。

4 在局部修复码中的应用

本节利用第3节中部分NMDS码构造最优局部修复码。

定理11 当满足如下两个条件之一时, 所构造的NMDS码 C_1 是 $(q+3, 3, q; 2)$ -LRC, 且关于引理7中所有界是最优的。

(1) 定理1(1)中 $a_j = b_j = 0$, 其中 $j = 1, 2$;

(2) 定理2(1)中 $a_1 = b_1 = 0$ 且 $a_{32}/a_{12} \in U_{q+1}$ 。

证明 当满足条件(1)时, 根据定理1证明容易得出, $\cup_{S \in \mathcal{B}_{d^\perp}(C^\perp)} S = [q+3]$ 。

又由引理8知, C_1 的最小局部度 r 为2。下证 C_1 是关于引理7中界的最优局部修复码。将 C_1 的参数 $(q+3, 3, q; 2)$ 分别代入式(3)~(6)可得 $d \leq q+3-3-\lceil 3/2 \rceil + 2 = q$

$$k \leq 2 + k_{\text{opt}}^{(q)}(q, q) = 3 \text{ (在式(4)中取 } t = 1 \text{)} \quad (10)$$

$$d \leq \frac{q^{3-1 \cdot 2-1}(q-1)[q+3-1 \cdot (2+1)]}{q^{3-1 \cdot 2-1}} = q, n \geq$$

$$\{1 \cdot (2+1) + \sum_{i=0}^{3-1 \cdot 2-1} \lceil q/q^i \rceil\} = q+3。$$

根据Singleton界得, $k_{\text{opt}}^{(q)}(q, q) = 1$, 所以式(10)成立。因此, C_1 关于引理7中所有界都是最优的。

当满足条件(2)时, 证明类似, 此处省略。证毕

5 结论

本文通过在Yin等人[8]定义的矩阵 \mathbf{G} 中添加两个新的列向量, 构造了 \mathbb{F}_{q^2} 上几类长度为 $q+3$ 的MDS码和NMDS码, 并确定了其参数及重量计数器。研究表明, 本文所构造的NMDS(或MDS)码都是near Griesmer(或Griesmer)码。特别地, 所构造的NMDS码包含了关于Singleton-like界、Cadambe-Mazumdar界、Plotkin-like界和Griesmer-like界的最优局部修复码。需要说明的是, 本文的构造推广了已有文献中的工作, 其中文献[8]中长度为 $q+3$ 的NMDS码的构造属于本文中定理1的特殊情形。

参 考 文 献

- [1] SUN Huan, YUE Qin, and JIA Xue. The weight distributions of several classes of few-weight linear codes[J]. *Advances in Mathematics of Communications*, 2025, 19(1): 69–90. doi: [10.3934/amc.2023037](https://doi.org/10.3934/amc.2023037).
- [2] QIAO Xingbin and DU Xiaoni. Weight distributions and weight hierarchies of a class of binary linear codes with a few weights[J]. *Advances in Mathematics of Communications*, 2025, 19(1): 245–258. doi: [10.3934/amc.2023056](https://doi.org/10.3934/amc.2023056).
- [3] 高健, 张耀宗, 孟祥蕊, 等. 几类指标为2的不可约拟循环码的重量分布[J]. *电子与信息学报*, 2022, 44(12): 4312–4318. doi: [10.11999/JEIT211104](https://doi.org/10.11999/JEIT211104).
GAO Jian, ZHANG Yaozong, MENG Xiangrui, et al. Weight distributions of some classes of irreducible quasi-cyclic codes of index 2[J]. *Journal of Electronics & Information Technology*, 2022, 44(12): 4312–4318. doi: [10.11999/JEIT211104](https://doi.org/10.11999/JEIT211104).
- [4] DINH Haiquang, WANG Xiaoqiang, LIU Hongwei, et al. Hamming distances of constacyclic codes of length $3p^s$ and optimal codes with respect to the Griesmer and Singleton bounds[J]. *Finite Fields and Their Applications*, 2021, 70: 101794. doi: [10.1016/j.ffa.2020.101794](https://doi.org/10.1016/j.ffa.2020.101794).
- [5] WANG Qiuyan and HENG Ziling. Near MDS codes from oval polynomials[J]. *Discrete Mathematics*, 2021, 344(4): 112277. doi: [10.1016/j.disc.2020.112277](https://doi.org/10.1016/j.disc.2020.112277).
- [6] TAN Pan, FAN Cuiling, DING Cunsheng, et al. The minimum locality of linear codes[J]. *Designs, Codes and Cryptography*, 2023, 91(1): 83–114. doi: [10.1007/s10623-022-01099-z](https://doi.org/10.1007/s10623-022-01099-z).
- [7] HENG Ziling and WANG Xinran. New infinite families of near MDS codes holding t -designs[J]. *Discrete Mathematics*, 2023, 346(10): 113538. doi: [10.1016/j.disc.2023.113538](https://doi.org/10.1016/j.disc.2023.113538).
- [8] YIN Yanan and YAN Haode. Constructions of several families of MDS codes and NMDS codes[J]. *Advances in Mathematics of Communications*, 2025, 19(4): 1222–1247. doi: [10.3934/amc.2024051](https://doi.org/10.3934/amc.2024051).
- [9] DING Yun, LI Yang, and ZHU Shixin. Four new families of NMDS codes with dimension 4 and their applications[J]. *Finite Fields and Their Applications*, 2024, 99: 102495. doi: [10.1016/j.ffa.2024.102495](https://doi.org/10.1016/j.ffa.2024.102495).
- [10] LUO Gaojun and CAO Xiwang. Constructions of optimal binary locally recoverable codes via a general construction of linear codes[J]. *IEEE Transactions on Communications*, 2021, 69(8): 4987–4997. doi: [10.1109/TCOMM.2021.3083320](https://doi.org/10.1109/TCOMM.2021.3083320).
- [11] TANG Chunming and DING Cunsheng. An infinite family of linear codes supporting 4-designs[J]. *IEEE Transactions on Information Theory*, 2021, 67(1): 244–254. doi: [10.1109/TIT.2020.3032600](https://doi.org/10.1109/TIT.2020.3032600).
- [12] HUFFMAN W C and PLESS V. *Fundamentals of Error-Correcting Codes*[M]. Cambridge: Cambridge University Press, 2003: 71–72. doi: [10.1017/CBO9780511807077](https://doi.org/10.1017/CBO9780511807077).
- [13] DODUNEKOV S and LANDGEV I. On near-MDS codes[J]. *Journal of Geometry*, 1995, 54(1): 30–43. doi: [10.1007/BF01222850](https://doi.org/10.1007/BF01222850).
- [14] FALDUM A and WILLEMS W. Codes of small defect[J]. *Designs, Codes and Cryptography*, 1997, 10(3): 341–350. doi: [10.1023/A:1008247720662](https://doi.org/10.1023/A:1008247720662).
- [15] LIDL R and NIEDERREITER H. *Finite Fields*[M]. 2nd ed. Cambridge: Cambridge University Press, 1997: 268–342.
- [16] GOPALAN P, HUANG Cheng, SIMTICI H, et al. On the locality of codeword symbols[J]. *IEEE Transactions on Information Theory*, 2012, 58(11): 6925–6934. doi: [10.1109/TIT.2012.2208937](https://doi.org/10.1109/TIT.2012.2208937).
- [17] CADAMBE V and MAZUMDAR A. An upper bound on the size of locally recoverable codes[C]. 2013 International Symposium on Network Coding (NetCod), Calgary, Canada, 2013: 1–5. doi: [10.1109/NetCod.2013.6570829](https://doi.org/10.1109/NetCod.2013.6570829).
- [18] HAO Jie, XIA Shutao, SHUM K W, et al. Bounds and constructions of locally repairable codes: Parity-check matrix approach[J]. *IEEE Transactions on Information Theory*, 2020, 66(12): 7465–7474. doi: [10.1109/TIT.2020.3021707](https://doi.org/10.1109/TIT.2020.3021707).
- [19] 杜小妮, 薛婧, 乔兴斌, 等. 几类MDS码和NMDS码的构造[J]. *西北师范大学学报(自然科学版)*, 2026, 62(1): 41–48. doi: [10.16783/j.cnki.nwnuz.2026.01.005](https://doi.org/10.16783/j.cnki.nwnuz.2026.01.005).
DU Xiaoni, XUE Jing, QIAO Xingbin, et al. Construction of several classes of MDS codes and NMDS codes[J]. *Journal of Northwest Normal University (Natural Science) (Chinese)*, 2026, 62(1): 41–48. doi: [10.16783/j.cnki.nwnuz.2026.01.005](https://doi.org/10.16783/j.cnki.nwnuz.2026.01.005).

杜小妮: 女, 博士, 教授, 博士生导师, 研究方向为密码学与信息安全等。

薛婧: 女, 硕士生, 研究方向为密码学与信息安全等。

乔兴斌: 男, 博士, 讲师, 研究方向为密码学与信息安全等。

赵紫薇: 女, 博士生, 研究方向为密码学与信息安全等。

责任编辑: 余蓉

Construction of Maximum Distance Separable Codes and Near Maximum Distance Separable Codes Based on Cyclic Subgroup of $\mathbb{F}_{q^2}^*$

DU Xiaoni^{①②③} XUE Jing^① QIAO Xingbin^{①②} ZHAO Ziwei^①

^①(College of Mathematics and Statistic, Northwest Normal University, Lanzhou 730070, China)

^②(Key Laboratory of Cryptography and Data Analytics, Northwest Normal University, Lanzhou 730070, China)

^③(Gansu Provincial Research Center for Basic Disciplines of Mathematics and Statistics, Lanzhou 730070, China)

Abstract:

Objective The demand for higher performance and efficiency in error-correcting codes has increased with the rapid development of modern communication technologies. These codes detect and correct transmission errors. Because of their algebraic structure, straightforward encoding and decoding, and ease of implementation, linear codes are widely used in communication systems. Their parameters follow classical bounds such as the Singleton bound: for a linear code with length n and dimension k , the minimum distance d satisfies $d \leq n - k + 1$. When $d = n - k + 1$, the code is a Maximum Distance Separable (MDS) code. MDS codes are applied in distributed storage systems and random error channels. If $d = n - k$, the code is Almost MDS (AMDS); when both a code and its dual are AMDS, the code is Near MDS (NMDS). NMDS codes have geometric properties that are useful in cryptography and combinatorics. Extensive research has focused on constructing structurally simple, high-performance MDS and NMDS codes. This paper constructs several families of MDS and NMDS codes of length $q + 3$ over the finite field \mathbb{F}_{q^2} of even characteristic using the cyclic subgroup U_{q+1} . Several families of optimal Locally Repairable Codes (LRCs) are also obtained. LRCs support efficient failure recovery by accessing a small set of local nodes, which reduces repair overhead and improves system availability in distributed and cloud-storage settings.

Methods In 2021, Wang et al. constructed NMDS codes of dimension 3 using elliptic curves over \mathbb{F}_q . In 2023, Heng et al. obtained several classes of dimension-4 NMDS codes by appending appropriate column vectors to a base generator matrix. In 2024, Ding et al. presented four classes of dimension-4 NMDS codes, determined the locality of their dual codes, and constructed four classes of distance-optimal and dimension-optimal LRCs. Building on these works, this paper uses the unit circle U_{q+1} in \mathbb{F}_{q^2} and elliptic curves to construct generator matrices. By augmenting these matrices with two additional column vectors, several classes of MDS and NMDS codes of length $q + 3$ are obtained. The locality of the constructed NMDS codes is also determined, yielding several classes of optimal LRCs.

Results and Discussions In 2023, Heng et al. constructed generator matrices with second-row entries in \mathbb{F}_q^* and with the remaining entries given by nonconsecutive powers of the second-row elements. In 2025, Yin et al. extended this approach by constructing generator matrices using elements of U_{q+1} and obtained infinite families of MDS and NMDS codes. Following this direction, the present study expands these matrices by appending two column vectors whose elements lie in \mathbb{F}_{q^2} . The resulting matrices generate several classes of MDS and NMDS codes of length $q + 3$. Several classes of NMDS codes with identical parameters but different weight distributions are also obtained. Computing the minimum locality of the constructed NMDS codes shows that some are optimal LRCs satisfying the Singleton-like, Cadambe–Mazumdar, Plotkin-like, and Griesmer-like bounds. All constructed MDS codes are Griesmer codes, and the NMDS codes are near Griesmer. These results show that the proposed constructions are more general and unified than earlier approaches.

Conclusions This paper constructs several families of MDS and NMDS codes of length $q + 3$ over \mathbb{F}_{q^2} using elements of the unit circle U_{q+1} and oval polynomials, and by appending two additional column vectors with entries in \mathbb{F}_q . The minimum locality of the constructed NMDS codes is analyzed, and some of these codes are shown to be optimal LRCs. The framework generalizes earlier constructions, and the resulting codes are optimal or near-optimal with respect to the Griesmer bound.

Key words: Maximum Distance Separable(MDS) code; NMDS code; Weight enumerator; Locally recoverable code; Griesmer bound