几类near MDS码和最优局部修复码的构造

王鑫然，衡子灵*
（长安大学理学院，陕西西安 710064）

摘 要： 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，在分布式存储和云存储中有重要应用．本文首先构造了几类维数为4或5的near MDS（near Maximum Distance Separable）码，精确计算出了它们的参数和重量分布．特别地，得到了一些参数相同但重量分布不同的near MDS码．此外，通过确定near MDS码的局部度，得到了几类距离最优和维数最优的局部修复码．这些局部修复码的参数和文献中已知最优局部修复码的参数不同．

关键词： near MDS码；重量分布；局部修复码；分布式存储

基金项目： 国家自然科学基金（No.11901049）；陕西省高校科协青年人才托举计划（No.20200505）；长安大学中央高校基本科研业务费专项（No.300102122202）

中图分类号： O236.2；TN911.22 **文献标识码：** A **文章编号：** 0372-2112(2024)03-0957-10

电子学报URL: http://www.ejournal.org.cn **DOI:** 10.12263/DZXB.20220634

Several Constructions of Near MDS Codes and Optimal Locally Recoverable Codes

WANG Xin-ran, HENG Zi-ling*
(*School of Science*, *Chang' an University*, *Xi' an*, *Shaanxi* 710064, *China*)

Abstract: Locally recoverable codes offer an efficient way to improve the repair efficiency of storage nodes by local recovery. They are widely used in distributed storage and cloud storage. In this paper, we first present several constructions of near MDS (near maximum distance separable) codes of dimension 4 or 5. The parameters and weight distributions of the codes are explicitly determined. In particular, some families of near MDS codes with the same parameters but different weight distributions are derived. Then the locality of the near MDS codes is also studied. Several families of distance-optimal and dimension-optimal locally recoverable codes are obtained. These locally recoverable codes have different parameters from those of known ones in the literature.

Key words: near MDS code; weight distribution; locally recoverable code; distributed storage

Foundation Item(s): National Natural Science Foundation of China (No.11901049); Young Talent Fund of University Association for Science and Technology in Shaanxi, China (No.20200505); Fundamental Research Funds for the Central Universities, CHD (No.300102122202)

1 引言

令 q 为素数 p 的方幂，$\mathbb{F}_q$ 表示有 q 个元素的有限域．记 $\mathbb{F}_q^*=\mathbb{F}_q\backslash\{0\}$．对于非空集合 $\mathcal{C}\subseteq\mathbb{F}_q^n$，若 $\mathcal{C}$ 是 $\mathbb{F}_q$ 上的 k 维线性子空间，则称 $\mathcal{C}$ 是 $\mathbb{F}_q$ 上 $[n,k,d]$ 线性码，其中 k 表示 $\mathcal{C}$ 的信息位数，d 为 $\mathcal{C}$ 的最小（汉明）距离．线性码最小距离恰好等于其非零码字的最小汉明重量．

$[n,k]$ 线性码 $\mathcal{C}$ 的对偶码定义如式（1）所示：

$$\mathcal{C}^{\perp}=\{\boldsymbol{c}^{\perp}\in\mathbb{F}_q^n:<\boldsymbol{c}^{\perp},\boldsymbol{c}>=0\ \forall\boldsymbol{c}\in\mathcal{C}\},\tag{1}$$

其中 $<\boldsymbol{c}^{\perp},\boldsymbol{c}>$ 表示这两个向量的欧氏内积．显然 $\mathcal{C}^{\perp}$ 是 $[n,n-k]$ 线性码．令 A_i 表示线性码 $\mathcal{C}$ 中重量为 i 的码字个数，则序列 $(1,A_1,A_2,\cdots,A_n)$ 称为码 $\mathcal{C}$ 的重量分布．$1+A_1z+A_2z^2+\cdots+A_nz^n$ 称为码 $\mathcal{C}$ 的重量计数器．重量分布可用于刻画线性码的检错和纠错能力，以及计算线性码纠错和检错的失误率．近年来，大量文献研究了线性码的重量分布[1~10]．

参数为 $[n,k,n-k+1]$ 的线性码称为极大距离可分（Maximum Distance Separable，MDS）码．MDS码的对偶码也是MDS码．参数为 $[n,k,n-k]$ 的线性码称为almost MDS码，简称AMDS码．AMDS码的对偶码不一定是

收稿日期：2022-05-31；修回日期：2022-08-11；责任编辑：梅志强
*通讯作者：衡子灵

AMDS码. 如果一个线性码及其对偶码都是AMDS码，那么该码称为Near MDS码，简称NMDS码. NMDS码不仅在编码理论中非常重要，而且在组合数学、密钥共享方案、局部修复码等方面应用广泛.

当前大数据时代背景下，数据的爆炸式增长对存储系统提出了新的挑战. 分布式存储系统将原始数据进行编码，分散存储在多个节点，因此用户访问部分节点即可获取信息. 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，近年来在大量文献中被研究[11~14]. 对于一个正整数n，定义$[n]=\{1,2,\cdots,n\}$. 设$\mathcal{C}$是在$\mathbb{F}_q$上$[n,k]$线性码，用$[n]$表示$\mathcal{C}$中码字分量的坐标集. 对任意$i\in[n]$和任意$\boldsymbol{c}=(c_1,c_2,\cdots,c_n)\in\mathcal{C}$，若存在长度为$r$的子集$R_i\subseteq[n]\backslash\{i\}$及$\mathbb{F}_q^r$上的函数$f_i(x_1,x_2,\cdots,x_r)$，使得$c_i=f_i(\boldsymbol{c}_{R_i})$，则称$\mathcal{C}$的局部度为$r$，其中$\boldsymbol{c}_{R_i}$是码字$\boldsymbol{c}$在集合$R_i$上的投影，$R_i$称为$c_i$的修复集. 若每一个$f_i(x_1,x_2,\cdots,x_r)$都是一次齐次函数，则称$r$为$\mathcal{C}$的线性局部度. 线性码$\mathcal{C}$线性局部度的最小值称为最小线性局部度. $\mathbb{F}_q$上参数为$[n,k,d]$且局部度为r的线性码称为$(n,k,d,q;r)$局部修复码，简记为$(n,k,d,q;r)$-LRC. 文献[15]证明了$(n,k,d,q;r)$-LRC的最小距离d满足如下Singleton-like界：

$$d\leqslant n-k-\left\lceil\frac{k}{r}\right\rceil+2 \tag{2}$$

刚好达到此界的码称为距离最优局部修复码. 满足$d=n-k-\left\lceil\frac{k}{r}\right\rceil+1$的$(n,k,d,q;r)$-LRC称为几乎距离最优局部修复码. 对于任意的$(n,k,d,q;r)$-LRC，Cadambe和Mazumdar在文献[16]中给出了维数k的上界：

$$k\leqslant\min_{t\in\mathbb{Z}^+}[rt+k_{\mathrm{opt}}^{(q)}(n-t(r+1),d)] \tag{3}$$

其中$\mathbb{Z}^+$代表正整数集合，$k_{\mathrm{opt}}^{(q)}(n,d)=\max\{k:$ 在$\mathbb{F}_q$上存在$[n,k,d]$线性码$\}$. 达到此界的局部修复码称为维数最优局部修复码.

构造具有较小局部度的NMDS码是非常有意义的研究课题. 文献[17]研究了几类维数为3的NMDS码局部度，得到了几类距离最优和维数最优局部修复码. 本文通过使用一些特殊矩阵构造了几类维数为4或5的NMDS码，并精确给出了其重量分布. 特别地，得到了几类参数相同但重量分布不同的near MDS码. 此外，通过确定near MDS码的局部度，得到了几类距离最优和维数最优的局部修复码.

2 预备知识

2.1 NMDS码的一些性质

引理1[18] 若$\mathcal{C}$是$\mathbb{F}_q$上$[n,k,n-k]$NMDS码，$(1,A_1,A_2,\cdots,A_n)$与$(1,A_1^\perp,A_2^\perp,\cdots,A_n^\perp)$分别表示$\mathcal{C}$和$\mathcal{C}^\perp$的重量分布，则$\mathcal{C}^\perp$以及$\mathcal{C}$的重量分布分别满足式(4)与式(5)：

$$A_{k+s}^\perp=\binom{n}{k+s}\sum_{j=0}^{s-1}(-1)^j\binom{k+s}{j}(q^{s-j}-1)+(-1)^s\binom{n-k}{s}A_k^\perp \tag{4}$$

其中$s\in\{1,2,\cdots,n-k\}$.

$$A_{n-k+s}=\binom{n}{k-s}\sum_{j=0}^{s-1}(-1)^j\binom{n-k+s}{j}(q^{s-j}-1)+(-1)^s\times\binom{k}{s}A_{n-k} \tag{5}$$

其中$s\in\{1,2,\cdots,k\}$.

引理2[19] 令$\mathcal{C}$是NMDS码，则对$\mathcal{C}$中任意最小重量码字$\boldsymbol{c}$，在$\mathcal{C}^\perp$的最小重量码字中存在唯一的$\boldsymbol{c}^\perp$(不考虑与$\boldsymbol{c}^\perp$线性相关的向量)使得$\mathrm{suppt}(\boldsymbol{c})\cap\mathrm{suppt}(\boldsymbol{c}^\perp)=\varnothing$，其中$\mathrm{suppt}(\boldsymbol{c})=\{1\leqslant i\leqslant n:c_i\neq0\}$表示码字$\boldsymbol{c}=(c_1,c_2,\cdots,c_n)$的支撑集. 特别地，码$\mathcal{C}$及其对偶码$\mathcal{C}^\perp$最小重量码字的数量相同.

2.2 oval多项式

定义1[20] 令$q=2^m,m\geqslant2$且m为整数. 若$f\in\mathbb{F}_q[x]$是满足以下条件的多项式，则称f为oval多项式.

(1) f是$\mathbb{F}_q$的置换多项式且满足$\deg(f)<q,f(0)=0,f(1)=1$.

(2)对任意$a\in\mathbb{F}_q$，$g_a(x):=\big(f(x+a)+f(a)\big)x^{q-2}$也是$\mathbb{F}_q$的置换多项式.

引理3[21] 令$q=2^m,m\geqslant2$且m为整数. 多项式$f(x)=x^h$，$\gcd(h,m)=1$为$\mathbb{F}_q$上的oval多项式.

由引理3易知，当$q=2^m,m\geqslant3$且m是奇数时，$f(x)=x^4$为$\mathbb{F}_q$上的oval多项式.

引理4[22] f为$\mathbb{F}_q$上的oval多项式当且仅当f为$\mathbb{F}_q$的一个置换且对任意两两互异的$x,y,z\in\mathbb{F}_q$都满足$\frac{f(x)+f(y)}{x+y}\neq\frac{f(x)+f(z)}{x+z}$.

2.3 有限域上多项式的根

引理5[20] 令$q=2^m,m$为正整数，$\mathrm{Tr}_{q/2}(x)=x+x^2+x^{2^2}+\cdots+x^{2^{m-1}}$为$\mathbb{F}_q$到$\mathbb{F}_2$的迹函数，$x\in\mathbb{F}_q$. 令$f(x)=ax^2+bx+c\in\mathbb{F}_q[x]$为2次多项式，则，(1)$f$在$\mathbb{F}_q$中仅有1个根当且仅当$b=0$;(2)$f$在$\mathbb{F}_q$中有2个根当且仅当$b\neq0$且$\mathrm{Tr}_{q/2}\left(\frac{ac}{b^2}\right)=0$;(3)$f$在$\mathbb{F}_q$中无根当且仅当$b\neq0$且$\mathrm{Tr}_{q/2}\left(\frac{ac}{b^2}\right)=1$.

引理6[23] 令$q=p^m$，m和h都是正整数且$\gcd(h,m)=l$. 定义$\mathbb{F}_q$上的多项式$f(x)=x^{p^h+1}+ax^{p^h}+bx+c$，$a,b,c\in\mathbb{F}_q$. 用$N_f$表示$f(x)$在$\mathbb{F}_q$中根的个数. 若$a=0,b=0$或$a\neq0,b=a^{p^h}$，则有式(6)：

$$N_f=\begin{cases}1 & ,若\dfrac{m}{l}是奇数,p=2\\ 0,\ 1或2 & ,若\dfrac{m}{l}是奇数,p是奇数\\ 0,\ 1或p^l+1 & ,若\dfrac{m}{l}是偶数\end{cases}\quad(6)$$

引理 7[20]　设 p 为素数，$q=p^m$. 对 $\alpha\in\mathbb{F}_q$，则 $\mathrm{Tr}_{q/p}(\alpha)=0$ 当且仅当存在 $\beta\in\mathbb{F}_q$ 使得 $\alpha=\beta^p-\beta$.

引理 8　令 $q=2^m,m\geqslant 3$ 且 m 是奇数，则 $g(x)$: $=x^2+(a+b)x+a^2+b^2+ab$, $a\neq b$ 在 $\mathbb{F}_q$ 中无根. 特别地，$\mathbb{F}_q$ 上任意两两互异的元素 a, b, c 都满足 $a^2+b^2+c^2+ab+ac+bc\neq 0$. 若 $c=0$，则 $a^2+b^2+ab\neq 0$.

证明　显然有 $\mathrm{Tr}_{q/2}\left(\dfrac{a^2+b^2+ab}{(a+b)^2}\right)=\mathrm{Tr}_{q/2}(1)+\mathrm{Tr}_{q/2}\left(\dfrac{ab}{a^2+b^2}\right)$. 令 $\beta=\dfrac{a}{a+b}\in\mathbb{F}_q$，容易验证 $\dfrac{ab}{a^2+b^2}=\beta^2-\beta$. 从而根据引理7，$\mathrm{Tr}_{q/2}\left(\dfrac{ab}{(a+b)^2}\right)=0$. 故当 m 是奇数时，$\mathrm{Tr}_{q/2}\left(\dfrac{a^2+b^2+ab}{(a+b)^2}\right)=\mathrm{Tr}_{q/2}(1)=1$. 由引理5得 $g(x)$ 在 $\mathbb{F}_q$ 中无根. 因此对任意 $c\in\mathbb{F}_q$，$g(c)\neq 0$. □

2.4　线性码的局部度

设 $\mathcal{C}$ 是码长为 n 的线性码，$d=d(\mathcal{C})$ 表示 $\mathcal{C}$ 的最小距离. 若 $d(\mathcal{C}^\perp)>1$，则称 $\mathcal{C}$ 为非平凡线性码. 对码字 $\boldsymbol{c}\in\mathcal{C}$，定义其支撑集为 $\mathrm{suppt}(\boldsymbol{c})=\{1\leqslant i\leqslant n:c_i\neq 0\}$，其中 $\boldsymbol{c}=(c_1,c_1,\cdots,c_n)$. 令 $\mathcal{B}_d(\mathcal{C})=\{\mathrm{suppt}(\boldsymbol{c}):\boldsymbol{c}\in\mathcal{C},\mathrm{wt}(\boldsymbol{c})=d\}$，其中 $\mathrm{wt}(\boldsymbol{c})$ 表示 $\boldsymbol{c}$ 的汉明重量.

引理 9[17]　设 $\mathcal{C}$ 是码长为 n 的非平凡线性码，$d^\perp=d(\mathcal{C}^\perp)$，码 $\mathcal{C}$ 具有最小线性局部度 $d^\perp-1$ 当且仅当 $\bigcup\limits_{S\in\mathcal{B}_{d^\perp}(\mathcal{C}^\perp)}S=[n]$.

引理 10[17]　设 $\mathcal{C}$ 是非平凡NMDS码，则 $\mathcal{C}$ 的最小线性局部度为 $d(\mathcal{C}^\perp)$ 或 $d(\mathcal{C}^\perp)-1$.

引理 11[17]　设 $\mathcal{C}$ 是非平凡NMDS码，$d^\perp=d(\mathcal{C}^\perp)$. 若 $\bigcap\limits_{S\in\mathcal{B}_{d^\perp}(\mathcal{C}^\perp)}S=\varnothing$，则 $\mathcal{C}^\perp$ 最小线性局部度为 $d(\mathcal{C})-1$.

3　几类NMDS码的构造

令 $q=2^m$，$\alpha_1,\cdots,\alpha_{q-1},\alpha_q$ 是有限域 $\mathbb{F}_q$ 的所有元素，其中 $\alpha_q=0$. 令 $\dim(\mathcal{C})$ 表示线性码 $\mathcal{C}$ 的维数.

3.1　参数为 $[q,4,q-4]$ 的NMDS码

定义 $\boldsymbol{G}_{(i,j)}=\begin{bmatrix}1&1&\cdots&1&1\\ \alpha_1^i&\alpha_2^i&\cdots&\alpha_{q-1}^i&\alpha_q^i\\ \alpha_1^j&\alpha_2^j&\cdots&\alpha_{q-1}^j&\alpha_q^j\\ \alpha_1^4&\alpha_2^4&\cdots&\alpha_{q-1}^4&\alpha_q^4\end{bmatrix}$，其中 $(i,j)=(1,3)$或$(2,3)$. 显然 $\boldsymbol{G}_{(i,j)}$ 是 $\mathbb{F}_q$ 上4行 q 列矩阵. 令 $\mathcal{C}_{(i,j)}$ 是由矩阵 $\boldsymbol{G}_{(i,j)}$ 生成的线性码.

3.1.1　$\mathcal{C}_{(1,3)}$ 的参数及重量分布

定理 1　令 $q=2^m$，$m\geqslant 3$ 且为奇数. 则 $\mathcal{C}_{(1,3)}$ 是 $\mathbb{F}_q$ 上 $[q,4,q-4]$NMDS码，其重量计数器如式(7)所示：

$$\begin{aligned}A(z)=1&+\frac{(q-1)^2(q-2)(q-4)}{24}z^{q-4}+\frac{2(q-1)^2(q-2)}{3}z^{q-3}\\&+\frac{(q-1)^2(q^2+8)}{4}z^{q-2}+\frac{(q-1)(q+2)(q^2+2)}{3}z^{q-1}\\&+\frac{(q-1)(9q^3+5q^2-6q+16)}{24}z^q\end{aligned}\quad(7)$$

证明　首先证明 $\dim(\mathcal{C}_{(1,3)})=4$. 令 $\boldsymbol{g}_k$ 代表矩阵 $\boldsymbol{G}_{(1,3)}$ 中第 k 行向量，$k=1,2,3,4$. 设在 $\mathbb{F}_q$ 上存在不全0的元素 a_1,a_2,a_3,a_4，使得 $\sum\limits_{k=1}^{4}a_k\boldsymbol{g}_k=\boldsymbol{0}$ 成立，则有式(8)：

$$\begin{cases}a_1+a_2\alpha_1+a_3\alpha_1^3+a_4\alpha_1^4=0\\ a_1+a_2\alpha_2+a_3\alpha_2^3+a_4\alpha_2^4=0\\ \quad\vdots\\ a_1+a_2\alpha_q+a_3\alpha_q^3+a_4\alpha_q^4=0\end{cases}\quad(8)$$

令 $f(x)=a_1+a_2x+a_3x^3+a_4x^4$，显然其在 $\mathbb{F}_q$ 上至多有4个根. 但由式(8)，$f(x)$ 有 q 个根，矛盾. 因此 $a_1=a_2=a_3=a_4=0$，即 $\mathrm{rank}(\boldsymbol{G}_{(1,3)})=4$. 故 $\dim(\mathcal{C}_{(1,3)})=4$.

然后证明 $\mathcal{C}_{(1,3)}^\perp$ 的参数为 $[q,q-4,4]$. 显然 $\dim(\mathcal{C}_{(1,3)}^\perp)=q-\dim(\mathcal{C}_{(1,3)})=q-4$. 只需证 $d(\mathcal{C}_{(1,3)}^\perp)=4$.

在矩阵 $\boldsymbol{G}_{(1,3)}$ 上任取三列向量如式(9)所示：

$$\boldsymbol{D}_{1.1}=\begin{bmatrix}1&1&1\\ x_1&x_2&x_3\\ x_1^3&x_2^3&x_3^3\\ x_1^4&x_2^4&x_3^4\end{bmatrix}\quad(9)$$

其中 x_1,x_2,x_3 是 $\mathbb{F}_q$ 中两两互异的元素. 取 $\boldsymbol{D}_{1.1}$ 的三阶子式如式(10)所示：

$$M_{1.1}=\begin{vmatrix}1&1&1\\ x_1&x_2&x_3\\ x_1^4&x_2^4&x_3^4\end{vmatrix}\quad(10)$$

令 $f(x)=x^4$，则 $M_{1.1}=(x_2+x_1)\big(f(x_3)+f(x_1)\big)+(x_3+x_1)\big(f(x_2)+f(x_1)\big)$. 由于 $f(x)$ 是 $\mathbb{F}_q$ 上的oval多项式，根据引理4，$M_{1.1}\neq 0$，则 $\mathrm{rank}(\boldsymbol{D}_{1.1})=3$. 由于矩阵 $\boldsymbol{G}_{(1,3)}$ 任取三列向量均线性无关，$d(\mathcal{C}_{(1,3)}^\perp)\geqslant 4$. 在矩阵 $\boldsymbol{G}_{(1,3)}$ 上任取四列向量如式(11)所示：

$$\boldsymbol{D}_{1.2}=\begin{bmatrix}1&1&1&1\\ x_1&x_2&x_3&x_4\\ x_1^3&x_2^3&x_3^3&x_4^3\\ x_1^4&x_2^4&x_3^4&x_4^4\end{bmatrix}\quad(11)$$

其中 x_1,x_2,x_3,x_4 是 $\mathbb{F}_q$ 上两两互异的元素.

$$\left|\boldsymbol{D}_{1.2}\right|=\prod_{1\leqslant j<i\leqslant 4}(x_i-x_j)(x_1x_2+x_1x_3+x_1x_4+x_2x_3+$$

$x_2x_4+x_3x_4$). 若取 $x_4=\alpha_q=0$，$x_3=\dfrac{x_1x_2}{x_1+x_2}$. 易证 x_1,x_2,x_3,x_4 两两互异，且此时 $|\boldsymbol{D}_{1.2}|=0$. 即矩阵 $\boldsymbol{G}_{(1,3)}$ 中存在四列线性相关的向量，则 $d(\mathcal{C}_{(1,3)}^{\perp})=4$. 故 $\mathcal{C}_{(1,3)}^{\perp}$ 的参数为 $[q,q-4,4]$.

下面计算 $\mathcal{C}_{(1,3)}^{\perp}$ 中重量为4的码字个数. $\mathcal{C}_{(1,3)}^{\perp}$ 的校验矩阵为 $\boldsymbol{G}_{(1,3)}$. 在 $\boldsymbol{G}_{(1,3)}$ 上任取四列向量得到 $\boldsymbol{D}_{1.2}$. 当且仅当 $|\boldsymbol{D}_{1.2}|=0$ 时，$\mathcal{C}_{(1,3)}^{\perp}$ 中存在重量为4的码字，且在此四个位置的分量非零. 考虑以下两种情形.

情形1：令 $x_4=\alpha_q$，则重量为4的码字第 q 个位置的分量非零，在前 $q-1$ 个位置中有3个分量非零. 此时 $|\boldsymbol{D}_{1.2}|=0\Leftrightarrow x_3=\dfrac{x_1x_2}{x_1+x_2}$. 在选定 x_1,x_2 后，可唯一确定 x_3 的值，且 x_1,x_2,x_3,x_4 两两互异. 在这种情形下，$\mathrm{rank}(\boldsymbol{D}_{1.2})=3$. 重量为4的码字个数为 $\dfrac{(q-1)^2(q-2)}{6}$.

情形2：令 $x_4\neq\alpha_q$，则重量为4码字的非零分量均在前 $q-1$ 个位置. 当 $x_3=x_1+x_2$ 时，由引理8，$|\boldsymbol{D}_{1.2}|=\prod\limits_{1\leqslant j<i\leqslant 4}(x_i-x_j)(x_1^2+x_2^2+x_1x_2)\neq 0$. 则此时不存在重量为4的码字. 当 $x_3\neq x_1+x_2$ 时，$|\boldsymbol{D}_{1.2}|=0\Leftrightarrow x_4=\dfrac{x_1x_2+x_1x_3+x_2x_3}{x_1+x_2+x_3}$ 且 $x_4\notin\{0,x_1,x_2,x_3\}$. 当 $x_4\neq 0$ 时，则有 $\dfrac{x_1x_2+x_1x_3+x_2x_3}{x_1+x_2+x_3}\neq 0\Leftrightarrow x_3\neq\dfrac{x_1x_2}{x_1+x_2}$. 同理 $x_4\notin\{x_1,x_2,x_3\}\Leftrightarrow x_3\notin\{\dfrac{x_1^2}{x_2},\dfrac{x_2^2}{x_1},a\}$，其中 $a^2=x_1x_2$. 由于对任意 $c\in\mathbb{F}_{2^m}$，方程 $x^2=c$ 在 $\mathbb{F}_{2^m}$ 上有且仅有一解，选定 x_1,x_2 后，a 的值唯一确定. 综上可得式(12)：

$$x_3\notin L=\{0,x_1,x_2,x_1+x_2,\frac{x_1x_2}{x_1+x_2},\frac{x_1^2}{x_2},\frac{x_2^2}{x_1},a\}\tag{12}$$

根据引理6与引理8，易证集合 L 中元素两两互异. 在此情形下，$\mathrm{rank}(\boldsymbol{D}_{1.2})=3$. 重量为4的码字个数为 $\dfrac{(q-1)^2(q-2)(q-8)}{24}$.

综合情形1与情形2，$\mathcal{C}_{(1,3)}^{\perp}$ 中重量为4的码字总数为 $\dfrac{(q-1)^2(q-2)(q-4)}{24}$.

最后证明 $\mathcal{C}_{(1,3)}$ 的最小距离 $d(\mathcal{C}_{(1,3)})=q-4$. 假设 $d(\mathcal{C}_{(1,3)})\leqslant q-5$. 令 $\boldsymbol{c}=\sum\limits_{k=1}^{4}a_k\boldsymbol{g}_k$ 是 $\mathcal{C}_{(1,3)}$ 中重量最小的非零码字，则 $\boldsymbol{c}$ 至少有5个分量为0，即存在两两互异的 $x_{i_1},x_{i_2},x_{i_3},x_{i_4},x_{i_5}\in\mathbb{F}_q$ 使得式(13)成立.

$$\begin{cases}a_1+a_2x_{i_1}+a_3x_{i_1}^3+a_4x_{i_1}^4=0\\ a_1+a_2x_{i_2}+a_3x_{i_2}^3+a_4x_{i_2}^4=0\\ \vdots\\ a_1+a_2x_{i_5}+a_3x_{i_5}^3+a_4x_{i_5}^4=0\end{cases}\tag{13}$$

令 $f(x)=a_1+a_2x+a_3x^3+a_4x^4$，显然其在 $\mathbb{F}_q$ 中至多有4个根. 但由式(13)，$f(x)$ 至少有5个根，矛盾. 故 $d(\mathcal{C}_{(1,3)})\geqslant q-4$. 由 Singleton 界，$d(\mathcal{C}_{(1,3)})\leqslant q-4+1=q-3$. 从而 $d(\mathcal{C}_{(1,3)})=q-3$ 或 $q-4$. 若 $d(\mathcal{C}_{(1,3)})=q-3$，则 $\mathcal{C}_{(1,3)}$ 是 $[q,4,q-3]$MDS码. 因此 $\mathcal{C}_{(1,3)}^{\perp}$ 也是MDS码，与前面所证结论矛盾，故 $d(\mathcal{C}_{(1,3)})=q-4$. 综上，$\mathcal{C}_{(1,3)}$ 是 $[q,4,q-4]$NMDS码.

由引理2，NMDS码 $\mathcal{C}_{(1,3)}$ 中码字重量为 $q-4$ 的个数等于 $\mathcal{C}_{(1,3)}^{\perp}$ 中码字重量为4的个数，再由引理1，可得 $\mathcal{C}_{(1,3)}$ 的重量计数器. □

3.1.2 $\mathcal{C}_{(2,3)}$ 的参数及重量分布

定理2 令 $q=2^m,m\geqslant 3$. 则 $\mathcal{C}_{(2,3)}$ 是 $\mathbb{F}_q$ 上 $[q,4,q-4]$ NMDS码，其重量计数器如式(14)所示：

$$\begin{aligned}A(z)=1&+\frac{(q-1)^2(q-2)(q-4)}{24}z^{q-4}\\&+\frac{2(q-1)^2(q-2)}{3}z^{q-3}+\frac{(q-1)^2(q^2+8)}{4}z^{q-2}\\&+\frac{(q-1)(q+2)(q^2+2)}{3}z^{q-1}\\&+\frac{(q-1)(9q^3+5q^2-6q+16)}{24}z^{q}\end{aligned}\tag{14}$$

证明 类似于定理1，容易证得线性码 $\mathcal{C}_{(2,3)}$ 的参数. 下面只计算 $\mathcal{C}_{(2,3)}^{\perp}$ 中重量为4的码字个数.

显然 $\mathcal{C}_{(2,3)}^{\perp}$ 的校验矩阵为矩阵 $\boldsymbol{G}_{(2,3)}$. 在矩阵 $\boldsymbol{G}_{(2,3)}$ 上任取四列向量得到式(15)：

$$\boldsymbol{D}_{2.1}=\begin{bmatrix}1&1&1&1\\x_1^2&x_2^2&x_3^2&x_4^2\\x_1^3&x_2^3&x_3^3&x_4^3\\x_1^4&x_2^4&x_3^4&x_4^4\end{bmatrix}\tag{15}$$

其中 x_1,x_2,x_3,x_4 是 $\mathbb{F}_q$ 中互不相同的元素，易证 $|\boldsymbol{D}_{2.1}|=\prod\limits_{1\leqslant j<i\leqslant 4}(x_i-x_j)(x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4)$.

当且仅当 $|\boldsymbol{D}_{2.1}|=0$ 时，$\mathcal{C}_{(2,3)}^{\perp}$ 中对应码字在此四个位置的分量非零. 考虑以下两种情形.

情形1：令 $x_4=\alpha_q=0$，则码字第 q 个位置是非零分量，在前 $q-1$ 个位置有3个非零分量. 此时 $|\boldsymbol{D}_{2.1}|=\prod\limits_{1\leqslant j<i\leqslant 4}(x_i-x_j)x_1x_2x_3\neq 0$. 故不存在重量为4的码字.

情形2：若 $x_4\neq\alpha_q$，即重量为4码字的非零分量均在前 $q-1$ 个位置. 当 $x_3=\dfrac{x_1x_2}{x_1+x_2}$ 时，$|\boldsymbol{D}_{2.1}|=\prod\limits_{1\leqslant j<i\leqslant 4}(x_i-x_j)\dfrac{x_1^2x_2^2}{x_1+x_2}\neq 0$. 此时不存在重量为4的码字. 当 $x_3\neq\dfrac{x_1x_2}{x_1+x_2}$ 时，$|\boldsymbol{D}_{2.1}|=0\Leftrightarrow x_4=\dfrac{x_1x_2x_3}{x_1x_2+x_1x_3+x_2x_3}$.

易证 $x_4\notin\{0,x_1,x_2,x_3\}$ 成立. 故 $x_3\notin L=\{0,x_1,x_2,$

$\frac{x_1x_2}{x_1+x_2}\}$. 显然集合 L 中元素两两互异且 $\mathrm{rank}(\boldsymbol{D}_{2.1})=3$, 故 $\mathcal{C}_{(2,3)}^{\perp}$ 中重量为 4 的码字总数为 $\frac{(q-1)^2(q-2)(q-4)}{24}$.

再根据引理 1 和 2,结论得证. □

根据定理 1 和 2 的证明过程, 当 $m\geqslant 3$ 且为奇数时, $\mathcal{C}_{(2,3)}$ 与 $\mathcal{C}_{(1,3)}$ 的最小重量码字的支撑集不同.

3.2　参数为 $[q,5,q-5]$ 的 NMDS 码

定义 $\boldsymbol{G}_{(i,j,k)}=\begin{bmatrix}1&1&\cdots&1&1\\ \alpha_1^i&\alpha_2^i&\cdots&\alpha_{q-1}^i&\alpha_q^i\\ \alpha_1^j&\alpha_2^j&\cdots&\alpha_{q-1}^j&\alpha_q^j\\ \alpha_1^k&\alpha_2^k&\cdots&\alpha_{q-1}^k&\alpha_q^k\\ \alpha_1^5&\alpha_2^5&\cdots&\alpha_{q-1}^5&\alpha_q^5\end{bmatrix}$, 其中 $(i,j,k)=(1,3,4),(1,2,3)$ 或 $(2,3,4)$. 显然 $\boldsymbol{G}_{(i,j,k)}$ 是 $\mathbb{F}_q$ 上 5 行 q 列矩阵. 令 $\mathcal{C}_{(i,j,k)}$ 是由矩阵 $\boldsymbol{G}_{(i,j,k)}$ 生成的线性码.

3.2.1　$\mathcal{C}_{(1,3,4)}$ 的参数及重量分布

定理 3　令 $q=2^m,m\geqslant 3$ 且为奇数. 则 $\mathcal{C}_{(1,3,4)}$ 是 $\mathbb{F}_q$ 上 $[q,5,q-5]$ NMDS 码, 其重量计数器如式(16)所示:

$$\begin{aligned}A(z)=1&+\frac{(q-1)^2(q-2)(q^2-8q+20)}{120}z^{q-5}\\&+\frac{5(q-1)^2(q-2)(q-4)}{24}z^{q-4}\\&+\frac{(q-1)^2(q-2)(q^2+20)}{12}z^{q-3}\\&+\frac{(q-1)^2(2q^3+7q^2+40)}{12}z^{q-2}\\&+\frac{(q-1)(9q^4+13q^3+14q^2+20q+40)}{24}z^{q-1}\end{aligned}\tag{16}$$

证明　首先证明 $\dim(\mathcal{C}_{(1,3,4)})=5$. 令 $\boldsymbol{g}_k$ 代表矩阵 $\boldsymbol{G}_{(1,3,4)}$ 中第 k 行向量, $k=1,2,3,4,5$. 设在 $\mathbb{F}_q$ 上存在不全为 0 的元素 a_1,a_2,a_3,a_4,a_5 使得 $\sum_{k=1}^{5}a_k\boldsymbol{g}_k=\boldsymbol{0}$ 成立, 则有式(17)成立:

$$\begin{cases}a_1+a_2\alpha_1+a_3\alpha_1^3+a_4\alpha_1^4+a_5\alpha_1^5=0\\ a_1+a_2\alpha_2+a_3\alpha_2^3+a_4\alpha_2^4+a_5\alpha_2^5=0\\ \quad\vdots\\ a_1+a_2\alpha_q+a_3\alpha_q^3+a_4\alpha_q^4+a_5\alpha_q^5=0\end{cases}\tag{17}$$

令 $f(x)=a_1+a_2x+a_3x^3+a_4x^4+a_5x^5$, 显然其在 $\mathbb{F}_q$ 中至多有 5 个互异根. 但由式(17), $f(x)$ 有 q 个互异根, 矛盾. 因此 $a_1=a_2=a_3=a_4=a_5=0$, 即 $\mathrm{rank}(\boldsymbol{G}_{(1,3,4)})=5$, $\dim(\mathcal{C}_{(1,3,4)})=5$.

然后证明 $\mathcal{C}_{(1,3,4)}^{\perp}$ 参数为 $[q,q-5,5]$. 显然 $\dim(\mathcal{C}_{(1,3,4)}^{\perp})=q-\dim(\mathcal{C}_{(1,3,4)})=q-5$. 下面证明 $d(\mathcal{C}_{(1,3,4)}^{\perp})\geqslant 5$.

在矩阵 $\boldsymbol{G}_{(1,3,4)}$ 上任取 4 列向量得到式(18):

$$\boldsymbol{D}_{3.1}=\begin{bmatrix}1&1&1&1\\ x_1&x_2&x_3&x_4\\ x_1^3&x_2^3&x_3^3&x_4^3\\ x_1^4&x_2^4&x_3^4&x_4^4\\ x_1^5&x_2^5&x_3^5&x_4^5\end{bmatrix}\tag{18}$$

其中 x_1,x_2,x_3,x_4 是 $\mathbb{F}_q$ 上两两互异的元素. 取 $\boldsymbol{D}_{3.1}$ 的两个四阶子矩阵的行列式, 如式(19)所示:

$$M_{3.1}=\begin{vmatrix}1&1&1&1\\ x_1&x_2&x_3&x_4\\ x_1^3&x_2^3&x_3^3&x_4^3\\ x_1^4&x_2^4&x_3^4&x_4^4\end{vmatrix},M_{3.2}=\begin{vmatrix}x_1&x_2&x_3&x_4\\ x_1^3&x_2^3&x_3^3&x_4^3\\ x_1^4&x_2^4&x_3^4&x_4^4\\ x_1^5&x_2^5&x_3^5&x_4^5\end{vmatrix}\tag{19}$$

易证式(20)与式(21)成立:

$$M_{3.1}=\prod_{1\leqslant j<i\leqslant 4}(x_i-x_j)(x_1x_2+x_1x_3+x_2x_3+(x_1+x_2+x_3)x_4)\tag{20}$$

$$\begin{aligned}M_{3.2}=x_1x_2x_3x_4\prod_{1\leqslant j<i\leqslant 4}(x_i-x_j)(x_1x_2x_3+(x_1x_2+x_1x_3\\+x_2x_3)x_4)\end{aligned}\tag{21}$$

下面分几种情形讨论.

情形 1: 令 $x_3=x_1+x_2$, 由引理 8, 则 $M_{3.1}=(x_1^2+x_2^2+x_1x_2)\prod_{1\leqslant j<i\leqslant 4}(x_i-x_j)\neq 0$. 故 $\mathrm{rank}(\boldsymbol{D}_{3.1})=4$.

情形 2: 令 $x_3\neq x_1+x_2$, $x_4=\frac{x_1x_2+x_1x_3+x_2x_3}{x_1+x_2+x_3}$. 由引理 5, 易得式(22):

$$\begin{aligned}M_{3.2}=&x_1x_2x_3x_4\times\\&\prod_{1\leqslant j<i\leqslant 4}(x_i-x_j)\frac{x_1^2(x_2^2+x_2x_3+x_3^2)+x_1(x_2^2x_3+x_2x_3^2)+x_2^2x_3^2}{x_1+x_2+x_3}\\&\neq 0\end{aligned}\tag{22}$$

情形 3: 令 $x_3\neq x_1+x_2$, $x_4\neq\frac{x_1x_2+x_1x_3+x_2x_3}{x_1+x_2+x_3}$, 显然 $M_{3.1}\neq 0$.

综上可得 $\mathrm{rank}(\boldsymbol{D}_{3.1})=4$. 故 $d(\mathcal{C}_{(1,3,4)}^{\perp})\geqslant 5$.

下面证明 $d(\mathcal{C}_{(1,3,4)}^{\perp})=5$ 并计算 $\mathcal{C}_{(1,3,4)}^{\perp}$ 中重量为 5 的码字个数. 显然 $\mathcal{C}_{(1,3,4)}^{\perp}$ 的校验矩阵为矩阵 $\boldsymbol{G}_{(1,3,4)}$. 在 $\boldsymbol{G}_{(1,3,4)}$ 上任取五列向量如(23)式所示:

$$\boldsymbol{D}_{3.2}=\begin{bmatrix}1&1&1&1&1\\ x_1&x_2&x_3&x_4&x_5\\ x_1^3&x_2^3&x_3^3&x_4^3&x_5^3\\ x_1^4&x_2^4&x_3^4&x_4^4&x_5^4\\ x_1^5&x_2^5&x_3^5&x_4^5&x_5^5\end{bmatrix}\tag{23}$$

其中 x_1,x_2,x_3,x_4,x_5 是 $\mathbb{F}_q$ 上互不相同的元素. 当且仅当 $|\boldsymbol{D}_{3.2}|=0$, 即 $\mathrm{rank}(\boldsymbol{D}_{3.2})=4$ 时, $\mathcal{C}_{(1,3,4)}^{\perp}$ 中存在重量为 5 的码字, 且其在对应五个位置的分量非零. 下面分类讨论 $|\boldsymbol{D}_{3.2}|$.

（1）令 $x_5=\alpha_q$，则 $\left|\boldsymbol{D}_{3.2}\right|=\prod\limits_{1\leqslant j<i\leqslant 4}(x_i-x_j)(x_1x_2x_3+(x_1x_2+x_1x_3+x_2x_3)x_4)$.

若 $x_3=\dfrac{x_1x_2}{x_1+x_2}$，则 $\left|\boldsymbol{D}_{3.2}\right|=\prod\limits_{1\leqslant j<i\leqslant 4}(x_i-x_j)x_1x_2x_3\neq 0$. 此时不存在重量为5的码字. 若 $x_3\neq\dfrac{x_1x_2}{x_1+x_2}$，则 $\left|\boldsymbol{D}_{3.2}\right|=0\Leftrightarrow x_4=\dfrac{x_1x_2x_3}{x_1x_2+x_1x_3+x_2x_3}$，易证 $x_4\notin\{0,x_1,x_2,x_3\}$ 成立. 故 $x_3\notin L=\{0,x_1,x_2,\dfrac{x_1x_2}{x_1+x_2}\}$. 显然集合 L 中元素两两互异且 $\mathrm{rank}(\boldsymbol{G}_{(1,3,4)})=4$，故重量为5且其中一个非零分量位于第 q 个位置的码字个数为 $\dfrac{(q-1)^2(q-2)(q-4)}{4!}$.

（2）令 $x_5\neq\alpha_q$，则重量为5码字的非零分量均在前 $q-1$ 个位置. 容易得出式(24)：

$$\left|\boldsymbol{D}_{3.2}\right|=\prod_{1\leqslant j<i\leqslant 4}(x_i-x_j)(x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4+(x_1x_2+x_1x_3+x_2x_3+x_1x_4+x_2x_4+x_3x_4)x_5) \tag{24}$$

从而 $\left|\boldsymbol{D}_{3.2}\right|=0\Leftrightarrow x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4+(x_1x_2+x_1x_3+x_2x_3+x_1x_4+x_2x_4+x_3x_4)x_5=0$.

为了讨论 x_5，需讨论 $x_1x_2+x_1x_3+x_2x_3+(x_1+x_2+x_3)\times x_4$ 是否非零. 进一步，需要讨论 $x_1+x_2+x_3$ 是否非零. 故下面分情形讨论.

情形1：$x_3=x_1+x_2$ 时，$x_1x_2+x_1x_3+x_2x_3+x_4\times(x_1+x_2+x_3)=x_1^2+x_1x_2+x_2^2\neq 0$. 则 $\left|\boldsymbol{D}_{3.2}\right|=0\Leftrightarrow x_5=\dfrac{(x_1+x_2)x_1x_2}{x_1^2+x_1x_2+x_2^2}+x_4$. 类似定理1的证明，易得 $x_5\notin\{0,x_1,x_2,x_3,x_4\}$ 等价于式(25)：

$$x_4\notin\left\{\frac{(x_1+x_2)x_1x_2}{x_1^2+x_1x_2+x_2^2},\frac{x_1^3}{x_1^2+x_1x_2+x_2^2},\frac{x_2^3}{x_1^2+x_1x_2+x_2^2},\frac{x_3^3}{x_1^2+x_1x_2+x_2^2}\right\} \tag{25}$$

故有式(26)成立：

$$x_4\notin L=\left\{0,x_1,x_2,x_1+x_2,\frac{(x_1+x_2)x_1x_2}{x_1^2+x_1x_2+x_2^2},\frac{x_1^3}{x_1^2+x_1x_2+x_2^2},\frac{x_2^3}{x_1^2+x_1x_2+x_2^2},\frac{x_3^3}{x_1^2+x_1x_2+x_2^2}\right\} \tag{26}$$

根据引理6与引理8，易证 L 中元素两两互异. 由于 $\mathrm{rank}(\boldsymbol{G}_{(1,3,4)})=4$，故重量为5的码字个数如式(27)所示.

$$\frac{(q-1)^2(q-2)(q-8)}{5!}=\frac{(q-1)^2(q-2)(q-8)}{120} \tag{27}$$

情形2：$x_3\neq x_1+x_2$ 时，$x_1x_2+x_1x_3+x_2x_3+x_4(x_1+x_2+x_3)=0\Leftrightarrow x_4=\dfrac{x_1x_2+x_1x_3+x_2x_3}{x_1+x_2+x_3}$. 由引理5易得出式(28)：

$$\left|\boldsymbol{D}_{3.2}\right|=\prod_{1\leqslant j<i\leqslant 5}(x_i-x_j)\times\left(\frac{x_1^2(x_2^2+x_2x_3+x_3^2)+x_1(x_2^2x_3+x_2x_3^2)+x_2^2x_3^2}{x_1+x_2+x_3}\right)\neq 0 \tag{28}$$

此时不存在重量为5的码字.

情形3：$x_3\neq x_1+x_2$，$x_1x_2+x_1x_3+x_2x_3+(x_1+x_2+x_3)x_4\neq 0$. 即 $x_4\neq\dfrac{x_1x_2+x_1x_3+x_2x_3}{x_1+x_2+x_3}$ 时，易得式(29)：

$$\left|\boldsymbol{D}_{3.2}\right|=0\Leftrightarrow x_5=\frac{x_1x_2x_3+(x_1x_2+x_1x_3+x_2x_3)x_4}{(x_1+x_2+x_3)x_4+x_1x_2+x_1x_3+x_2x_3} \tag{29}$$

令 $x_5=\dfrac{x_1x_2x_3+(x_1x_2+x_1x_3+x_2x_3)x_4}{(x_1+x_2+x_3)x_4+x_1x_2+x_1x_3+x_2x_3}$，且 $a^2=\dfrac{x_1x_2x_3}{x_1+x_2+x_3}$. 下面对 x_3 分类讨论如下.

① 当 $x_3=\dfrac{x_1x_2}{x_1+x_2}$ 时，$x_5=\dfrac{x_1x_2x_3}{(x_1+x_2+x_3)x_4}$，且可证 $x_5\notin\{0,x_1,x_2,x_3,x_4\}$. 类似定理2的证明，易得 $x_5\notin\{0,x_1,x_2,x_3,x_4\}$ 等价于式(30)：

$$x_4\notin\left\{\frac{x_1^2(x_2+x_3)}{x_1^2+x_2x_3},\frac{x_2^2(x_1+x_3)}{x_2^2+x_1x_3},\frac{x_3^2(x_1+x_2)}{x_3^2+x_1x_2},a\right\} \tag{30}$$

且 $\dfrac{x_1x_2+x_1x_3+x_2x_3}{x_1+x_2+x_3}=0$. 故有式(31)成立：

$$x_4\notin L_1=\left\{0,x_1,x_2,x_3,\frac{x_1^2(x_2+x_3)}{x_1^2+x_2x_3},\frac{x_2^2(x_1+x_3)}{x_2^2+x_1x_3},\frac{x_3^2(x_1+x_2)}{x_3^2+x_1x_2},a\right\} \tag{31}$$

现证明 a 与 L_1 中其他元素互异. 显然 $a^2\notin\{0,x_1^2,x_2^2,x_3^2\}$，故 $a\notin\{0,x_1,x_2,x_3\}$. 若 $a=\dfrac{x_1^2(x_2+x_3)}{x_1^2+x_2x_3}$，则 $a^2=\dfrac{x_1^4(x_2^2+x_3^2)}{x_1^4+x_2^2x_3^2}$，即 $\dfrac{x_1^2x_2^2}{x_1^2+x_1x_2+x_2^2}=\left(\dfrac{x_1x_2^2}{x_1^2+x_1x_2+x_2^2}\right)^2$. 整理该等式有 $x_1(x_1+x_2)=0$，则 $x_1=0$ 或 $x_1=x_2$，矛盾. 故 $a\neq\dfrac{x_1^2(x_2+x_3)}{x_1^2+x_2x_3}$. 同理易得 $a\neq\dfrac{x_2^2(x_1+x_3)}{x_2^2+x_1x_3},\dfrac{x_3^2(x_1+x_2)}{x_3^2+x_1x_2}$. 且 L_1 中其它元素两两互异.

② 当 $x_3=\dfrac{x_1^2}{x_2}$ 时，易得式(32)：

$$x_5=\frac{x_1(x_4(x_1+x_2)^2+x_1x_2(x_1+x_4))}{x_4(x_1+x_2)^2+x_1x_2(x_1+x_4)+x_1(x_1+x_2)^2} \tag{32}$$

且 $x_5\notin\{0,x_1,x_2,x_3,x_4\}$ 等价于式(33)：

$$x_4\notin\left\{\frac{x_1x_2x_3}{x_1x_2+x_1x_3+x_2x_3},\frac{x_2^2(x_1+x_3)}{x_2^2+x_1x_3},\frac{x_3^2(x_1+x_2)}{x_3^2+x_1x_2},a\right\}\tag{33}$$

且$\frac{x_1x_2+x_1x_3+x_2x_3}{x_1+x_2+x_3}=x_1$. 故有式(34)成立:

$$x_4\notin L_2=\left\{0,x_1,x_2,x_3,\frac{x_1x_2x_3}{x_1x_2+x_1x_3+x_2x_3},\frac{x_2^2(x_1+x_3)}{x_2^2+x_1x_3},\frac{x_3^2(x_1+x_2)}{x_3^2+x_1x_2},a\right\}\tag{34}$$

类似①中的证明,易证L_2中元素两两互异.

③ 当$x_3=\frac{x_2^2}{x_1}$时,易得式(35):

$$x_5=\frac{x_2(x_4(x_1+x_2)^2+x_1x_2(x_2+x_4))}{x_4(x_1+x_2)^2+x_1x_2(x_2+x_4)+x_2(x_1+x_2)^2}\tag{35}$$

且$x_5\notin\{0,x_1,x_2,x_3,x_4\}$等价于式(36):

$$x_4\notin\left\{\frac{x_1x_2x_3}{x_1x_2+x_1x_3+x_2x_3},\frac{x_1^2(x_2+x_3)}{x_1^2+x_2x_3},\frac{x_3^2(x_1+x_2)}{x_3^2+x_1x_2},a\right\}\tag{36}$$

且$\frac{x_1x_2+x_1x_3+x_2x_3}{x_1+x_2+x_3}=x_2$. 故有式(37)成立:

$$x_4\notin L_3=\left\{0,x_1,x_2,x_3,\frac{x_1x_2x_3}{x_1x_2+x_1x_3+x_2x_3},\frac{x_1^2(x_2+x_3)}{x_1^2+x_2x_3},\frac{x_3^2(x_1+x_2)}{x_3^2+x_1x_2},a\right\}\tag{37}$$

类似①中的证明,易证L_3中元素两两互异.

④当$x_3=b$且$b^2=x_1x_2$时,易得式(38):

$$x_5^2=\frac{x_1x_2(x_4^2(x_1^2+x_1x_2+x_2^2)+x_1^2x_2^2)}{x_4^2(x_1^2+x_1x_2+x_2^2)+x_1^2x_2^2+x_1x_2(x_1+x_2)^2}\tag{38}$$

$x_5\notin\{0,x_1,x_2,x_3,x_4\}$等价于式(39):

$$x_4\notin\left\{\frac{x_1x_2x_3}{x_1x_2+x_1x_3+x_2x_3},\frac{x_1^2(x_2+x_3)}{x_1^2+x_2x_3},\frac{x_2^2(x_1+x_3)}{x_2^2+x_1x_3},a\right\}\tag{39}$$

且$\frac{x_1x_2+x_1x_3+x_2x_3}{x_1+x_2+x_3}=x_3$. 故有式(40)成立:

$$x_4\notin L_4=\left\{0,x_1,x_2,x_3,\frac{x_1x_2x_3}{x_1x_2+x_1x_3+x_2x_3},\frac{x_1^2(x_2+x_3)}{x_1^2+x_2x_3},\frac{x_2^2(x_1+x_3)}{x_2^2+x_1x_3},a\right\}\tag{40}$$

类似①中的证明,易证L_4中元素两两互异.

⑤ 当 $x_3\notin L_5=\{0,x_1,x_2,x_1+x_2,\frac{x_1^2}{x_2},\frac{x_2^2}{x_1},\frac{x_1x_2}{x_1+x_2},b\}$, $b^2=x_1x_2$,则$x_5\notin\{0,x_1,x_2,x_3,x_4\}$等价于式(41):

$$x_4\notin\left\{\frac{x_1x_2x_3}{x_1x_2+x_1x_3+x_2x_3},\frac{x_1^2(x_2+x_3)}{x_1^2+x_2x_3},\frac{x_2^2(x_1+x_3)}{x_2^2+x_1x_3},\frac{x_3^2(x_1+x_2)}{x_3^2+x_1x_2},a\right\}\tag{41}$$

故有式(42)成立:

$$x_4\notin L_6=\left\{0,x_1,x_2,x_3,\frac{x_1x_2x_3}{x_1x_2+x_1x_3+x_2x_3},\frac{x_1^2(x_2+x_3)}{x_1^2+x_2x_3},\frac{x_1x_2+x_1x_3+x_2x_3}{x_1+x_2+x_3},\frac{x_2^2(x_1+x_3)}{x_2^2+x_1x_3},\frac{x_3^2(x_1+x_2)}{x_3^2+x_1x_2},a\right\}\tag{42}$$

现证明b与L_5中其它元素互异. 显然$b^2\notin\{0,x_1^2,x_2^2\}$,故$b\notin\{0,x_1,x_2\}$. 根据引理8,易证$b\neq x_1+x_2,\frac{x_1x_2}{x_1+x_2}$. 若$b=\frac{x_1^2}{x_2}$,则$b^2=\frac{x_1^4}{x_2^2}$,即$\left(\frac{x_1}{x_2}\right)^3=1$. 由引理6可得$x_1=x_2$,矛盾. 故$b\neq\frac{x_1^2}{x_2}$. 同理易得$b\neq\frac{x_2^2}{x_1}$且$L_5$中其它元素两两互异. 根据引理5和类似于①中的证明,可证明L_6中元素两两互异.

在情形3下,由于$\mathrm{rank}(\boldsymbol{G}_{(1,3,4)})=4$,故重量为5的码字个数为式(43)所示:

$$4\cdot\frac{(q-1)^2(q-2)(q-8)}{5!}+\frac{(q-1)^2(q-2)(q-8)(q-10)}{5!}=\frac{(q-1)^2(q-2)(q-6)(q-8)}{120}\tag{43}$$

综合对前面$|\boldsymbol{D}_{3,2}|$的分类讨论,$\mathcal{C}_{(1,3,4)}^{\perp}$中重量为5的码字个数为$\frac{(q-1)^2(q-2)(q^2-8q+20)}{120}$.

最后证明$\mathcal{C}_{(1,3,4)}$的最小重量$d(\mathcal{C}_{(1,3,4)})=q-5$. 假设$d(\mathcal{C}_{(1,3,4)})\leqslant q-6$. 令$\boldsymbol{c}=\sum_{k=1}^{5}a_k\boldsymbol{g}_k$是$\mathcal{C}_{(1,3,4)}$中重量最小的非零码字,则$\boldsymbol{c}$至少有6个分量为0,从而存在两两互异的$x_{i_1},x_{i_2},x_{i_3},x_{i_4},x_{i_5},x_{i_6}\in\mathbb{F}_q$,使得式(44)成立:

$$\begin{cases}a_1+a_2x_{i_1}+a_3x_{i_1}^3+a_4x_{i_1}^4+a_5x_{i_1}^5=0\\a_1+a_2x_{i_2}+a_3x_{i_2}^3+a_4x_{i_2}^4+a_5x_{i_2}^5=0\\\quad\vdots\\a_1+a_2x_{i_6}+a_3x_{i_6}^3+a_4x_{i_6}^4+a_5x_{i_6}^5=0\end{cases}\tag{44}$$

令$f(x)=a_1+a_2x+a_3x^3+a_4x^4+a_5x^5$,显然其在$\mathbb{F}_q$上至多有5个根. 但由上面方程组,$f(x)$至少有6个根,矛盾. 故$d(\mathcal{C}_{(1,3,4)})\geqslant q-5$. 由Singleton界,$d(\mathcal{C}_{(1,3,4)})\leqslant q-5+1=q-4$. 则$d(\mathcal{C}_{(1,3,4)})=q-4$或$q-5$. 若$d(\mathcal{C}_{(1,3,4)})=q-4$. 此时$\mathcal{C}_{(1,3,4)}$是$[q,5,q-4]$MDS码,则$\mathcal{C}_{(1,3,4)}^{\perp}$也是MDS码,矛盾. 因此$d(\mathcal{C}_{(1,3,4)})=q-5$. 综上,$\mathcal{C}_{(1,3,4)}$是$[q,5,q-5]$NMDS码.

由引理2可知,NMDS码$\mathcal{C}_{(1,3,4)}$中码字重量为$q-5$的个数等于$\mathcal{C}_{(1,3,4)}^{\perp}$中码字重量为5的个数. 再由引理1,可得$\mathcal{C}_{(1,3,4)}$的重量计数器. 此外,$\mathcal{C}_{(1,3,4)}^{\perp}$中所有重量为5的码字支撑集的并集为$[q]$,其中$[q]=\{1,2,\cdots,q\}$. □

在定理3中,$\mathcal{C}_{(1,3,4)}^{\perp}$中重量为5码字的非零分量既可取在第$q$个位置,也可出现在前$q-1$位置. $\mathcal{C}_{(1,3,4)}^{\perp}$中

所有重量为5的码字支撑集的并集为$[q]$. 特别地，当$m>3$时，$\mathcal{C}_{(1,3,4)}^{\perp}$中所有重量为5的码字支撑集的交集为空集.

3.2.2 $\mathcal{C}_{(1,2,3)}$的参数及重量分布

定理4 令$q=2^m, m\geqslant 3$. 则$\mathcal{C}_{(1,2,3)}$是$\mathbb{F}_q$上$[q,5,q-5]$NMDS码，其重量计数器如式(45)所示：

$$\begin{aligned}A(z)=1&+\frac{(q-1)^2(q-2)(q-3)(q-4)}{120}z^{q-5}\\&+\frac{(q-1)^2(q-2)(q-3)}{6}z^{q-4}\\&+\frac{(q-1)^2(q-2)(q^2+q+12)}{12}z^{q-3}\\&+\frac{(q-1)^2(q^3+3q^2+5q+12)}{6}z^{q-2}\\&+\frac{(q-1)(9q^4+14q^3+3q^2+46q+24)}{24}z^{q-1}\\&+\frac{(q-1)(11q^4+5q^3+10q^2-20q+24)}{30}z^{q}\end{aligned}\tag{45}$$

证明 证明方法与定理3类似，故略去. 且因证明过程中未使用引理6及引理8，故该定理仅要求$m\geqslant 3$即可. □

在定理4中，$\mathcal{C}_{(1,2,3)}^{\perp}$中重量为5码字的非零分量既可取在第$q$个位置，也可出现在前$q-1$位置. $\mathcal{C}_{(1,2,3)}^{\perp}$中所有重量为5的码字支撑集的并集为$[q]$. 特别地，当$m>3$时，$\mathcal{C}_{(1,2,3)}^{\perp}$中所有重量为5的码字支撑集的交集为空集.

3.2.3 $\mathcal{C}_{(2,3,4)}$的参数及重量分布

定理5 令$q=2^m$，$m>3$. 则$\mathcal{C}_{(2,3,4)}$是$\mathbb{F}_q$上$[q,5,q-5]$NMDS码，其重量计数器如式(46)所示：

$$\begin{aligned}A(z)=1&+\frac{(q-1)^2(q-2)(q-4)(q-8)}{120}z^{q-5}\\&+\frac{(q-1)^2(q-2)(9q-32)}{24}z^{q-4}\\&+\frac{(q-1)^2(q-2)(q^2-4q+32)}{12}z^{q-3}\\&+\frac{(q-1)^2(2q^3+11q^2-20q+64)}{12}z^{q-2}\\&+\frac{(q-1)(9q^4+9q^3+38q^2-24q+64)}{24}z^{q-1}\\&+\frac{(q-1)(44q^4+25q^3+5q^2-10q+56)}{120}z^{q}\end{aligned}\tag{46}$$

证明 证明方法与定理3类似，故略去. 且因证明过程中未使用引理6及引理8，故该定理仅要求$m>3$即可. □

在定理5中，$\mathcal{C}_{(2,3,4)}^{\perp}$中重量为5码字的非零分量仅出现在前$q-1$位置. 因此，由引理2，$\mathcal{C}_{(2,3,4)}$中所有重量最小的码字在第$q$位置的分量恒不为0.

4 几类最优局部修复码

下面利用第3节中NMDS码构造最优局部修复码.

定理6 令$q=2^m$，$m>3$且m为奇数. 则$\mathcal{C}_{(1,3)}$为$(q,4,q-4,q;3)$-LRC，$\mathcal{C}_{(1,3)}^{\perp}$为$(q,q-4,4,q;q-5)$-LRC. 此外，$\mathcal{C}_{(1,3)}$和$\mathcal{C}_{(1,3)}^{\perp}$都是距离最优且维数最优局部修复码.

证明 根据定理1的证明过程，容易得出：$\bigcap\limits_{S\in\mathcal{B}_4(\mathcal{C}_{(1,3)}^{\perp})}S=\varnothing$，$\bigcup\limits_{S\in\mathcal{B}_4(\mathcal{C}_{(1,3)}^{\perp})}S=[q]$. 由引理9，$\mathcal{C}_{(1,3)}$的最小线性局部度为$d(\mathcal{C}_{(1,3)}^{\perp})-1=3$. 由引理11，$\mathcal{C}_{(1,3)}^{\perp}$的最小线性局部度为$d(\mathcal{C}_{(1,3)})-1=q-5$.

下面证明$\mathcal{C}_{(1,3)}$是距离最优且维数最优的局部修复码. 将$\mathcal{C}_{(1,3)}$的参数$(q,4,q-4,q;3)$代入Singleton-like界，即式(2)的右侧，得式(47)：

$$n-k-\left\lceil\frac{k}{r}\right\rceil+2=q-4-\left\lceil\frac{4}{3}\right\rceil+2=q-4\tag{47}$$

因此$\mathcal{C}_{(1,3)}$是距离最优的局部修复码. 令$t=1$，然后将$\mathcal{C}_{(1,3)}$的参数代入式(3)，得式(48)：

$$k\leqslant r+k_{opt}^{(q)}\left(n-(r+1),d\right)=3+k_{opt}^{(q)}(q-4,q-4)=4\tag{48}$$

其中根据Singleton界可得$k_{\mathrm{opt}}^{(q)}(q-4,q-4)=1$. 因此$\mathcal{C}_{(1,3)}$是维数最优的局部修复码.

类似可证$\mathcal{C}_{(1,3)}^{\perp}$是距离最优且维数最优的局部修复码. □

定理7 令$q=2^m$，$m\geqslant 3$. 则NMDS码$\mathcal{C}_{(2,3)}$是$(q,4,q-4,q;4)$-LRC且$\mathcal{C}_{(2,3)}^{\perp}$是$(q,q-4,4,q;q-5)$-LRC. $\mathcal{C}_{(2,3)}^{\perp}$是距离最优且维数最优的局部修复码，$\mathcal{C}_{(2,3)}$是几乎距离最优、维数最优的局部修复码.

证明 由定理2的证明过程，容易得出：$\bigcup\limits_{S\in\mathcal{B}_4(\mathcal{C}_{(2,3)}^{\perp})}S\neq[q]$，$\bigcap\limits_{S\in\mathcal{B}_4(\mathcal{C}_{(2,3)}^{\perp})}S=\varnothing$. 根据引理9~11，$\mathcal{C}_{(2,3)}$的最小线性局部度为$d(\mathcal{C}_{(2,3)}^{\perp})=4$，$\mathcal{C}_{(2,3)}^{\perp}$的最小线性局部度为$d(\mathcal{C}_{(2,3)})-1=q-5$. 根据式(2)和式(3)，容易验证它们的最优性，证明略去. □

定理8 令$q=2^m, m>3$且为奇数. 则NMDS码$\mathcal{C}_{(1,3,4)}$是$(q,5,q-5,q;4)$-LRC且$\mathcal{C}_{(1,3,4)}^{\perp}$是$(q,q-5,5,q;q-6)$-LRC. 此外，$\mathcal{C}_{(1,3,4)}$和$\mathcal{C}_{(1,3,4)}^{\perp}$都是距离最优且维数最优的局部修复码.

证明 证明与定理6类似，故略去. □

定理9 令$q=2^m, m>3$. 则NMDS码$\mathcal{C}_{(1,2,3)}$是$(q,5,q-5,q;4)$-LRC且$\mathcal{C}_{(1,2,3)}^{\perp}$是$(q,q-5,5,q;q-6)$-LRC. 此外，$\mathcal{C}_{(1,2,3)}$和$\mathcal{C}_{(1,2,3)}^{\perp}$都是距离最优且维数最优的局部修复码.

证明 由定理4的证明过程可得，当$m>3$时，$\bigcup\limits_{S\in\mathcal{B}_5(\mathcal{C}_{(1,2,3)}^{\perp})}S=[q]$，$\bigcap\limits_{S\in\mathcal{B}_5(\mathcal{C}_{(1,2,3)}^{\perp})}S=\varnothing$. 其余证明与定理6类似，故略去. □

定理10 令$q=2^m$，$m>3$. 则NMDS码$\mathcal{C}_{(2,3,4)}$是$(q,5,q-5,q;5)$-LRC且$\mathcal{C}_{(2,3,4)}^{\perp}$是$(q,q-5,5,q;q-6)$-

LRC. 此外，$\mathcal{C}_{(2,3,4)}^{\perp}$是距离最优且维数最优的局部修复码．$\mathcal{C}_{(2,3,4)}$是几乎距离最优、维数最优的局部修复码．

证明　证明与定理6类似，故略去．□

5　总结

本文基于两类特殊的矩阵，构造了一些维数为4或5的NMDS码，并确定了其参数及重量分布．特别地，定理3~6中构造的NMDS码$\mathcal{C}_{(1,3,4)}$、$\mathcal{C}_{(1,2,3)}$、$\mathcal{C}_{(2,3,4)}$参数相同但重量分布不同；定理1与定理2中构造的NMDS码$\mathcal{C}_{(1,3)}$和$\mathcal{C}_{(2,3)}$参数与重量分布都相同，但具有不同的码字结构．此外，本文构造的NMDS码大部分都为距离最优与维数最优的局部修复码．

本文中构造的距离为4的最优局部修复码与文献[24]、文献[25]中构造的距离为4的最优局部修复码参数不同．文献[26]中构造了两类距离为5的最优局部修复码，通过比较可知本文中构造的距离为5最优局部修复码参数与其不同．最近，文献[27, 28]利用NMDS码构造了几类最优的局部修复码，但参数与本文不同．

参考文献

[1] LI C J, YUE Q, LI F W. Weight distributions of cyclic codes with respect to pairwise coprime order elements[J]. Finite Fields and Their Applications, 2014, 28: 94-114.

[2] DING C S. Designs from Linear Codes[M]. Singapore: World Scientific, 2019.

[3] HENG Z L, DING C S, ZHOU Z C. Minimal linear codes over finite fields[J]. Finite Fields and Their Applications, 2018, 54: 176-196.

[4] 杜小妮, 吕红霞, 王蓉, 等. 两类四重线性码的构造[J]. 西北师范大学学报(自然科学版), 2018, 54(6): 1-4.
DU X N, LÜ H X , WANG R, et al. A construction of two classes of linear codes with four-weights[J]. Journal of Northwest Normal University (Natural Science), 2018, 54 (6): 1-4. (in Chinese)

[5] 杨淑娣, 岳勤. 一类线性码的完全重量分布[J]. 计算机工程与科学, 2019, 41(2): 281-285.
YANG S D, YUE Q. Complete weight enumerators of a class of linear codes[J]. Computer Engineering and Science, 2019, 41(2): 281-285. (in Chinese)

[6] YANG S D, YAO Z G. Complete weight enumerators of a family of three-weight linear codes[J].Designs, Codes and Cryptography, 2017, 82(3): 663-674.

[7] 杜小妮, 李晓丹, 吕红霞, 等. 几类二重和三重线性码的构造[J]. 西北师范大学学报(自然科学版), 2018, 54(2): 30-35.
DU X N, LI X D, LÜ H X, et al. A construction of several classes of two-weight and three-weight linear codes[J]. Journal of Northwest Normal University (Natural Science), 2018, 54(2): 30-35. (in Chinese)

[8] 杜小妮, 吕红霞, 王蓉. 一类四重和六重线性码的构造[J]. 电子与信息学报, 2019, 41(12): 2995-2999.
DU X N, LÜ H X, WANG R. Construction of a class of linear codes with four-weight and six-weight[J]. Journal of Electronics & Information Technology, 2019, 41(12): 2995-2999. (in Chinese)

[9] 杨淑娣, 唐春明. 循环码的完全重量分布[J]. 江苏师范大学学报(自然科学版), 2018, 36(2): 64-68.
YANG S D, TANG C M. The complete weight enumerator of cyclic codes[J]. Journal of Jiangsu Normal University (Natural Science Edition), 2018, 36(2): 64-68. (in Chinese)

[10] 胡丽琴, 岳勤, 朱小萌. 具有两个非零点循环码的权重分布[J]. 中国科学(数学), 2014, 44(9): 1021-1034.
HU L Q, YUE Q, ZHU X M. Weight distribution of cyclic codes with two non-zero points[J]. Scientia Sinica (Mathematica), 2014, 44(9): 1021-1034. (in Chinese)

[11] 李瑞虎, 展秀珍, 付强, 等. 短码长四元最优局部修复码的构造[J]. 电子与信息学报, 2021, 43(12): 3749-3757.
LI R H, ZHAN X Z, FU Q, et al. Constructions of quaternary optimal locally repairable code with short length[J]. Journal of Electronics & Information Technology, 2021, 43(12): 3749-3757. (in Chinese)

[12] 杨森, 李瑞虎, 付强, 等. 二元局部修复码的新构造[J]. 空军工程大学学报(自然科学版), 2019, 20(6): 104-108.
YANG S, LI R H, FU Q, et al. The new constructions of binary locally repairable codes[J]. Journal of Air Force Engineering University (Natural Science Edition), 2019, 20(6): 104-108. (in Chinese)

[13] 展秀珍, 李瑞虎, 付强, 等. 低维四元局部修复码的构造[J]. 空军工程大学学报(自然科学版), 2021, 22(3): 104-110.
ZHAN X Z, LI R H, FU Q, et al. Construction of quaternary locally repairable code with low dimension[J]. Journal of Air Force Engineering University (Natural Science Edition), 2021, 22(3): 104-110. (in Chinese)

[14] LUO G J, CAO X W. Constructions of optimal binary locally recoverable codes via a general construction of linear codes[J]. IEEE Transactions on Communications, 2021, 69(8): 4987-4997.

[15] GOPALAN P, HUANG C, SIMITCI H, et al. On the locality of codeword symbols[J]. IEEE Transactions on Information Theory, 2012, 58(11): 6925-6934.

[16] CADAMBE V, MAZUMDAR A. An upper bound on the size of locally recoverable codes[C]//2013 International Symposium on Network Coding (NetCod). Piscataway: IEEE, 2013: 1-5.
[17] TAN P, FAN C L, DING C S, et al. The minimum linear locality of linear codes[J]. Designs, Codes and Cryptography, 2023, 91(1): 83-114.
[18] DODUNEKOV S, LANDGEV I. On near-MDS codes[J]. Journal of Geometry, 1995, 54(1/2): 30-43.
[19] FALDUM A, WILLEMS W. Codes of small defect[J]. Designs, Codes and Cryptography, 1997, 10(3): 341-350.
[20] Pommerening K. Quadratic equations in finite fields of characteristic 2[EB/OL]. (2022-04-26) [2022-05-20]. https://www.staff.unimainz.de/pommeren/MathMisc/QuGlChar2.pdf.
[21] WANG Q Y, HENG Z L . Near MDS codes from oval polynomials[J]. Discrete Mathematics, 2021, 344(4): 112277.
[22] MASCHIETTI A. Difference sets and hyperovals[J]. Designs, Codes and Cryptography, 1998, 14(1): 89-98.
[23] XU G K, CAO X W, QU L J. Infinite families of 3-designs and 2-designs from almost MDS codes[J]. IEEE Transactions on Information Theory, 2022, 68(7): 4344-4353.
[24] LUO Y, XING C P, YUAN C. Optimal locally repairable codes of distance 3 and 4 via cyclic codes[J]. IEEE Transactions on Information Theory, 2019, 65(2): 1048-1053.
[25] FU Q, LI R H, GUO L B, et al. Singleton-type optimal LRCs with minimum distance 3 and 4 from projective code[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2021, E104.A(1): 319-323.
[26] JIN L F. Explicit construction of optimal locally recoverable codes of distance 5 and 6 via binary constant weight codes[J]. IEEE Transactions on Information Theory, 2019, 65(8): 4658-4663.
[27] LI X R, HENG Z L. Constructions of near MDS codes which are optimal locally recoverable codes[J]. Finite Fields and Their Applications, 2023, 88: 102184.
[28] LI X R, HENG Z L. A construction of optimal locally recoverable codes[J]. Cryptography and Communications, 2023, 15: 553-563.

作者简介

王鑫然 男,1999年2月出生于山东省聊城市,现为长安大学理学院硕士研究生,主要研究方向为代数编码.
E-mail: wxr782751966@163.com

衡子灵 男,1990年出生,河南南阳人.现为长安大学理学院教授,硕士生导师.主要研究方向为编码与密码、序列设计等.
E-mail: zilingheng@chd.edu.cn