arXiv:2302.02037v1 [cs.IT] 4 Feb 2023

二元 Niederreiter-Rosenbloom-Tsfasman LCD 码的界

Welington Santos

美国弗吉尼亚州布莱克斯堡，VirginiaTech 数学系，Stanger 街 225 号，邮编 204061。

贡献作者：welington@vt.edu；

摘要

线性互补对偶码（LCD码）是指与其对偶码的交集仅含零向量的码。Massey 于 1992年 引入了这类码。LCD码在数据存储、通信系统和密码学中有广泛应用。Heqian、Guangku 和 Wei 将 Niederreiter-Rosenbloom-Tsfasman LCD 码（NRT-LCD 码）作为 LCD码在 NRT 度量空间 $M_{n,\ s}(\mathbb{F}_q)$ 中的推广引入。本文研究 LCD $[n \times s, k]$，即所有二元 $[n \times s, k]$ NRT-LCD 码中的最大最小 NRT 距离。我们证明了在 $M_{1,\ s}(\mathbb{F}_2)$ 中二元最大距离可分 NRT-LCD 码的存在性（非存在性）。我们给出了 $M_{n,\ 2}(\mathbb{F}_2)$ 中二元 NRT-LCD 码的一个线性规划界。我们还给出了构造二元 NRT-LCD 码的两种方法。

关键词：线性互补码，Niederreiter-Rosenbloom-Tsfasman 度量，线性规划界

1 引言

若 $[s, k]$ 线性码 $\mathcal{C}$ 满足 $\mathcal{C} \cap \mathcal{C}^{\perp_E} = \{0_s\}$，则称其为欧几里得线性互补对偶码（简称 LCD 码），其中 $\mathcal{C}^{\perp_E}$ 是 $\mathcal{C}$ 的欧几里得对偶码，0_s 是长度为 s的零向量。Massey [10],引入了 LCD 码，并证明 LCD 码为双用户二元加法信道提供了最优线性编码方案，且将其应用于最近邻

译码问题。此外， [10] 研究证明，渐近良好的 LCD 码存在。近年来，出于理论和实际方面的原因，人们对 LCD 码的兴趣日益浓厚（参见 [3, 4, 12–14]）。特别是，Carlet 和 Guilley 在 [3] 中指出，LCD 码对于信息保护以及防范侧信道攻击和非侵入式故障攻击的防护实现至关重要。一个重要问题是，如何确定给定码类中所有 $[s,k]$ 码的最大最小重量，这些码属于由给定的一对（s, k）所确定的某个码类。

编码理论也针对其他度量发展起来。其中一种度量是 Niederreiter-Rosenbloom-Tsfasman（简称 NRT）度量，由 [17] 引入，用于对经受衰落的并行信道集合上的传输进行建模。独立地，Niederreiter [5] 在有限维向量空间中研究了一类最大化问题；正如 Brualdi、Graves 和 Lawrence [19]所证明的，这类问题等价于 Niederreiter-Rosenbloom-Tsfasman 度量空间中的编码理论问题。

对于在前几个坐标中以较高概率发生的随机错误，NRT 度量更适用于纠正。自该度量提出以来，针对 Niederreiter-Rosenbloom-Tsfasman 度量，人们研究了若干编码理论问题，例如界 [1, 11],重量分布和 MacWilliams 恒等式 [2, 9, 22]，自对偶码[25, 26], MDS 码 [16, 23, 24], 突发错误计数 [8, 21], BCH 码[28], 以及译码 [18, 20, 27]。

最近，Heqian、Guangkui 和 Wei 在 [7] 中定义了 NRT-LCD 码。在同一篇论文中，他们研究了 NRT 度量码成为 NRT-LCD 码的基本条件。本文旨在研究 $LCD[n\times s,k]$，它是所有二元 $[n\times s,k]$ NRT-LCD 码 $\mathcal{C}\subseteq M_{n,\ s}(\mathbb{F}_2)$ 的可能最小 NRT 距离的最大值。

本文结构如下。第2 节介绍 Niederreiter Rosenbloom-Tsfasman 度量空间中的码以及 NRT-LCD 码的一些基本事实和定义。第3节研究 $LCD[1\times s,k]$。第4节给出 $M_{n,\ 2}(\mathbb{F}_2)$ 中 NRT-LCD 码的线性规划界，并研究 $LCD[n\times 2,2]$。最后，第5节给出 $M_{1,\ s}(\mathbb{F}_2)$ 中二元 NRT-LCD 码的新构造，以及 $M_{n,\ s}(\mathbb{F}_2)$ 中二元 NRT-LCD 码的新构造。

2 预备知识

2.1 Niederreiter-Rosenbloom-Tsfasman 度量码

令 $M_{n,s}(\mathbb{F}_q)$ 表示有限域 $\mathbb{F}_q$ 上所有 $n\times s$ 矩阵的集合。

给定矩阵 $v=[v_{i,j}]_{n\times s}\in M_{n,s}(\mathbb{F}_q)$，记 $v=[v_1;\ v_2;\ \ldots;\ v_n]$或 $v=[w_1\mid w_2\mid\cdots\mid w_s]$，其中 $v_i=[v_{i,1},\ldots,v_{i,s}]$ 是 v的第 i行，并且$w_j=[w_{1,j},w_{2,j},\ldots;\ w_{n,j}]$ 是 v的第 j列。

v 的 Niederreiter-Rosenbloom-Tsfasman（简称 NRT）权重定义为

$$\rho(v) = \sum_{i=1}^{n} \rho(v_i) \tag{1}$$

其中,

$$\rho(v_i) = \begin{cases} \max\{j : v_{i,j} \neq 0\} & \text{if } v_i \neq 0 \\ 0 & \text{if } v_i = 0. \end{cases} \tag{2}$$

对于 $i = 1$、2、.....、n。

NRT 度量定义为 $d_N(u, v) = \rho(u - v)$，其中 $u, v \in M_{n,\ s}(\mathbb{F}_q)$。注意，当 $s = 1$ 时，也就是说，当 $v \in M_{n,\ 1} \cong \mathbb{F}_q^n$ 时，NRT 度量就变为通常的汉明度量。

给定子集 $\mathcal{C} \subseteq M_{n,\ s}(\mathbb{F}_q)$，$\mathcal{C}$ 的最小 NRT 距离定义为:

$$d_N(\mathcal{C}) = \min\{d_N(v, u) : d_N(v, u) \neq 0\}. \tag{3}$$

We 如果根据上下文可以明确代码，则有时写作 d_N，而不写作 $d_N(\mathcal{C})$ t.

给定 $\mathcal{C} \subseteq M_{n,\ s}(\mathbb{F}_q)$，容易验证 $d_H(\mathcal{C}) \leq d_N(\mathcal{C})$，其中 d_H 是 $\mathcal{C}$的最小汉明距离。

定义 1 NRT度量码是维数为 k 且最小NRT距离为 d_N 的线性子空间 $\mathcal{C} \subseteq M_{n,s}(\mathbb{F}_q)$。

注意，NRT度量码 $\mathcal{C} \subseteq M_{n,s}(\mathbb{F}_q)$ 的最小距离由 $d_N(\mathcal{C}) = \min\{\rho(v) : v \in \mathcal{C}, v \neq 0\}$ 给出。此外，NRT度量码满足以下 Singleton界:

$$d_N(\mathcal{C}) \leq ns - k + 1. \tag{4}$$

满足 $d_N(\mathcal{C}) = ns - k + 1$ 的 NRT度量码称为最大距离可分码。

2.2 Niederreiter-Rosenbloom-Tsfasman LCD 码

Niederreiter-Rosenbloom-Tsfasman 线性互补对偶（NRT-LCD）码定义于 [7]。为了研究 NRT-LCD 码，我们引入以下定义。

De义 2 NRT度量码 $\mathcal{C}$ 的对偶码 $\mathcal{C}^{\perp_N}$ 定义为 s

$$\mathcal{C}^{\perp_N} = \{u \in M_{n,s}(\mathbb{F}_q) \mid \langle u, v\rangle_N = 0 \text{ for all } v \in \mathcal{C}\},$$

其中，$u = [u_1;\ .....;\ u_n]$、$v = [v_1;\ .....;\ v_n] \in M_{n,\ s}(\mathbb{F}_q)$

$$\langle u, v\rangle_N = \sum_{i=1}^{n} \langle u_i, v_i\rangle_N,\ \langle u_i, v_i\rangle_N = \sum_{j=1}^{s} u_{i,j} u_{i,s-j+1}. \tag{5}$$

4 二元 Niederreiter-Rosenbloom-Tsfasman LCD 码的界

定义 **3** [7] $[n\times s,k,d_N]$ $\mathcal{C}$ *NRT linear* () 如果满足条件，则称 *complementary dual code (NRT-LCD code for short)* $\mathcal{C}\cap\mathcal{C}^{\perp_N}=\{0\}$ NRT 度量码为。

定义 **4** ([25]) 设 $A=[a_{ij}]\in M_{k,}$ ^{s} $=(\mathbb{F}_q)$。 $[a_{il}]$ $l=s-j+1$ $1\le i\le k$ $1\le j\le s$ $flip\ A$ A 的翻转定义为 $flip(A)$，其中 for and 。() 的转置记为 A°。

定义 5（[26]）设 $A=[A_1\mid A_2\mid\cdots\mid A_n]\in M_k,\ _{ns}(\mathbb{F}_q)$，其中 A_i 是一个 $k\times s$ 矩阵，适用于 $i=1$、2、.....、n。A 的有序翻转定义为

$$Oflip(A)=[flip(A_1)\mid flip(A_2)\mid\cdots\mid flip(A_n)].$$

$Oflip(A)$ 的转置记为

$$A^{\dagger}=[Oflip(A)]^T=\begin{bmatrix}A_1^{\circ}\\A_2^{\circ}\\\vdots\\A_n^{\circ}\end{bmatrix}. \tag{6}$$

注意，若 $n=1$，则 $A^{\dagger}=A^{\circ}$。

Example 1 设 $A\in M_{3,\ 4}(\mathbb{F}_q)$ 是任意一个由下式给出的矩阵

$$A=\begin{bmatrix}a_{1,1}&a_{1,2}&a_{1,3}&a_{1,4}\\a_{2,1}&a_{2,2}&a_{2,3}&a_{2,4}\\a_{3,1}&a_{3,2}&a_{3,3}&a_{3,4}\end{bmatrix}.$$

那么，$flip(A)$ 和 A° 由下式给出

$$flip(A)=\begin{bmatrix}a_{1,4}&a_{1,3}&a_{1,2}&a_{1,1}\\a_{2,4}&a_{2,3}&a_{2,2}&a_{2,1}\\a_{3,4}&a_{3,3}&a_{3,2}&a_{3,1}\end{bmatrix},\ A^{\circ}=\begin{bmatrix}a_{1,4}&a_{2,4}&a_{3,4}\\a_{1,3}&a_{2,3}&a_{3,3}\\a_{1,2}&a_{2,2}&a_{3,2}\\a_{1,1}&a_{2,1}&a_{3,1}\end{bmatrix}.$$

设 $A\in M_{3,4}(\mathbb{F}_q)$ 为任意一个矩阵，写作

$$A=\left[\begin{array}{cc|cc}a_{1,1}&a_{1,2}&a_{1,3}&a_{1,4}\\a_{2,1}&a_{2,2}&a_{2,3}&a_{2,4}\\a_{3,1}&a_{3,2}&a_{3,3}&a_{3,4}\end{array}\right].$$

那么，$Oflip(A)$ 和 $A^{\dagger}$ 由下式给出

$$Oflip(A)=\left[\begin{array}{cc|cc}a_{1,2}&a_{1,1}&a_{1,4}&a_{1,3}\\a_{2,2}&a_{2,1}&a_{2,4}&a_{2,3}\\a_{3,2}&a_{3,1}&a_{3,4}&a_{3,3}\end{array}\right],\ A^{\dagger}=\left[\begin{array}{ccc}a_{1,2}&a_{2,2}&a_{3,2}\\a_{1,1}&a_{2,1}&a_{3,1}\\\hline a_{1,4}&a_{2,4}&a_{3,4}\\a_{1,3}&a_{2,3}&a_{3,3}\end{array}\right].$$

在 [15], Muniz 证明了，$\mathcal{C}\subseteq M_{n,s}(\mathbb{F}_q)$ 的 $[n\times s,k]$ NRT 度量码的生成矩阵等价于一个具有特殊生成矩阵的 NRT 度量码。

定理

1 *([15], Theorem 3.5). Let $\mathcal{C} \subseteq M_{n\ s}\ \mathbb{F}_q$ be an $[n \times s, k]$ NRT-metric $(\ )$ code. Then $\mathcal{C}$ is equivalent to a code that has a generator matrix*

$$G = [G_1 \mid G_2 \mid \cdots \mid G_n], \tag{7}$$

where

i) G_1 的非零行是互不相同的典范向量，并按 NRT 权递增的顺序排列。
ii) G 为分块阶梯形，即如果 G_i 的最后 t 行为零，那么 G_1、……、G_{i-1} 的最后 t 行也为零。

Heqian、Guangkui 和 Wei 在[7]中根据生成矩阵刻画了 Niederreiter-Rosenbloom-Tsfasman 线性互补对偶码。

引理**1** *([7]) Let $\mathcal{C}$ be an $[n \times s, k, d_N]$ NRT metric code. Let $G \in M_{k,ns}(\mathbb{F}_q)$ be a generator matrix of $\mathcal{C}$ write as*

$$G = [G_1 \mid G_2 \mid \cdots \mid G_n], \tag{8}$$

where $G_i \in M_{k\ s}\ \mathbb{F}_q$ for $i = 1\ 2\ \ldots\ n$. Then $\mathcal{C}$ is an NRT-LCD if and only if $GG^{\dagger}$ $(\ )_{\ ,}$ is nonsingular.

Example 2 令 $\mathcal{C}$ 为由以下内容生成的二元 $1 \times g$, 2 码

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

如果 $\mathcal{C}$ 被视为汉明度量空间 $\mathbb{F}_2^4$中的线性码，可以验证 GG^T 是非奇异的，因此 $\mathcal{C}$ 是欧几里得线性互补对偶码。然而， $GG^{\dagger} = 0$ 是奇异的。根据引理 1， $\mathcal{C}$ 不是 NRT-LCD 码。

Example 3 令 $\mathcal{C}$ 为由以下内容生成的二元 $1 \times g$, 2 码

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

如果 $\mathcal{C}$ 被视为汉明度量空间 $\mathbb{F}_2^4$中的线性码，可以验证 $GG^T = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ 和 GG^T 是奇异的。也就是说， $\mathcal{C}$ 不是欧几里得线性互补对偶码。然而， $GG^{\circ} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ 和 GG° 是非奇异的。根据引理 1， $\mathcal{C}$ 是 NRT-LCD 码。

定义 6 设 n、 s、 k 为正整数。我们定义

$$LCD[n\times s, k] := \max\{d_N \mid \text{存在一个二元 } [n \times s, k] \text{ NRT-LCD 码 } \mathcal{C} \subseteq M_{n,\ s}(\mathbb{F}_2)\}. \tag{9}$$

Remark 1 注意，如果 $s = 1$，那么
$LCD[n\times 1, k] := \max\{d_H \mid \text{存在一个二元 } [n, k] \text{ LCD 汉明度量码 } \mathcal{C} \subseteq \mathbb{F}_2^n\}$.因此，我们将重点关注 $s > 1$的情形。

3 $M_{1,\ s}(\mathbb{F}_2)$ 中二元 NRT-LCD 码的初等界

Ozen 和 Siap 在 [18], 为$[1\times s,k,d_N]$ NRT 度量码$\mathcal{C}\subseteq M_{1,\ s}(\mathbb{F}_q)$定义了如下标准形生成矩阵。

定义 7 （[18]）设 $\mathcal{C}\subseteq M_{1,\ s}(\mathbb{F}_q)$ 是一个 $[1\times s,k,d_N]$ NRT 度量码，G 是 $\mathcal{C}$的生成矩阵。通过某些初等行变换，总能将 G 变换为以下形式:

$$G'=\begin{bmatrix} g_{1,1} & \cdots & g_{1,d_1-1} & g_{1,d_1} & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & \cdots & 0 \\ g_{2,1} & \cdots & g_{2,d_1-1} & 0 & g_{2,d_1+1} & \cdots & g_{1,d_2-1} & g_{2,d_2} & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{k,1} & \cdots & g_{k,d_1-1} & 0 & g_{k,d_1+1} & \cdots & g_{k,d_2-1} & 0 & g_{k,d_2+1} & \cdots & g_{k,d_k} & \cdots & 0 \end{bmatrix}, \tag{10}$$

其中 $g_{i,\ d_i}=1$，$d_{j,\ d_i}=0$ 适用于 $i\neq j$，且 $\{d_1,d_2,\ldots,d_k\}$ 是可能的非零 NRT 权重集合，使得 $d_N=d_1<d_2<\ldots<d_k$。

线性码 $\mathcal{C}$ 的任意生成矩阵都等价于 G'。该 G' 称为标准形生成矩阵。以 G' 作为标准形生成矩阵的线性码称为类型为（d_1，d_2，.....，d_k）的码。

Remark 2 在本文中，我们假设 $\mathcal{C}\subseteq M_{1,\ s}(\mathbb{F}_q)$ 总是包含一个具有满 NRT 权重 s 的码字，其中 s 是码长。也就是说，$\mathcal{C}$ 的类型为 $(d_N,d_2,\ldots,s)$。

引理 **2** *For any s,k greater than zero,*

$$LCD[1\times(s+2),k]\geq LCD[1\times s,k]+1. \tag{11}$$

Proof 设 G 是一个 $[1\times s,k,d_N]$ NRT-LCD码 $\mathcal{C}$ 的标准形生成矩阵。由于 $\mathcal{C}$ 是 NRT-LCD，故 GG° 非奇异。令 $\tilde{G}=\left[\,0\middle|G\middle|e_k\,\right]$，其中 e_k^T 由 $e_k^T=\begin{bmatrix}0&0&\cdots&0&1\end{bmatrix}$给出。注意，$\tilde{G}$ 是一个 $[1\times(s+2)\ k,d_N+1]$ NRT 度量码 $\tilde{\mathcal{C}}$ 的标准形生成矩阵。此外,

$$flip(\tilde{G})=\left[\,e_k\middle|flip(G)\middle|0\,\right]\ \text{and}\ \tilde{G}^{\circ}=\left[\begin{array}{c}e_k^T\\\hline G^{\circ}\\\hline 0\end{array}\right].$$

So,

$$\tilde{G}\tilde{G}^{\circ}=\left[\,0\middle|G\middle|e_k\,\right]\left[\begin{array}{c}e_k^T\\\hline G^{\circ}\\\hline 0\end{array}\right]=GG^{\circ}. \tag{12}$$

因此，$\tilde{G}\tilde{G}^{\circ}$ 是非奇异的，且 $\tilde{G}$ 生成一个 $[1\times(s+2)\ k$、$d_N+1]$ NRT-LCD 码。□

命题 **2** *For s odd, and dimension $k=1$ or $k=s-1$ we have:*

i) $LCD[1\times s,1]=s$;
ii) $LCD[1\times s,s-1]=1$。

Proof Singleton界（4）指出，任何 $[1\times s,1]$ NRT 度量码的最小距离至多为 s。我们将证明存在一个 $[1\times s,1]$ NRT-LCD 码 $\mathcal{C}_1$ 使得 $d_N(\mathcal{C}_1)=s$。令 $\mathcal{C}_1$ 为生成矩阵如下的二元 $[1\times s,1,s]$ NRT 度量码：

$$G_1=\begin{bmatrix}1 & \cdots & 1\end{bmatrix}.$$

注意，$G_1^{\circ}=\begin{bmatrix}1 & & \\ & \cdots\cdots & \\ & & 1\end{bmatrix}$。因此，$G_1G_1^{\circ}=1$，因为 s 是奇数。也就是说，$G_1G_1^{\circ}$ 是非奇异的，且 $\mathcal{C}$ 是一个 $[1\times s,1,s]$ NRT-LCD 码。证明 $LCD[1\times s,1]=s$。

再次由 Singleton界（4）可知，任何 $[1\times s,s-1]$ NRT 度量码的最小距离至多为 2。我们将证明存在一个 $[1\times s,s-1]$ NRT-LCD 码 $\mathcal{C}_2$ 使得 $d_N(\mathcal{C}_2)=2$。令 $\mathcal{C}_2$ 为一个二元 $[1\times s,s-1]$ NRT 度量码，其生成矩阵由下列标准形生成矩阵给出：

$$G_2=\begin{bmatrix}1&1&0&0&\ldots&0\\1&0&1&0&\ldots&0\\1&0&0&1&\ldots&0\\\vdots&\vdots&\vdots&\vdots&\ddots&\vdots\\1&0&0&0&\ldots&1\end{bmatrix}.$$

于是，

$$G_2^{\circ}=\begin{bmatrix}0&0&0&\ldots&1\\\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&1&\ldots&0\\0&1&0&\ldots&0\\1&0&0&\ldots&0\\1&1&1&\ldots&1\end{bmatrix}.$$

我们可以验证 $G_2G_2^{\circ}$ 是非奇异的，并且 $\mathcal{C}_2$ 是一个二元 $[1\times s,s-1,2]$ NRT-LCD 码。□

定理 **3** *If s is even, then there is no binary $[1\times s,1]$ NRT-LCD code.*

Proof 设 $\mathcal{C}$ 是一个二元 $[1\times s,1]$ NRT 度量码。因此，$\mathcal{C}$ 的任意生成矩阵 G 具有如下形式

$$G=\begin{bmatrix}x_1 & x_2 & \cdots & x_{s-1} & x_s\end{bmatrix}.$$

这意味着，

$$G^{\circ}=\begin{bmatrix}x_s\\x_{s-1}\\\vdots\\x_2\\x_1\end{bmatrix}.$$

So,

$$\begin{aligned} GG^{\circ} &= 2\sum_{i=1}^{s} x_i x_{s-i+1} \\ &= 0. \end{aligned}$$

证明不存在二元 $[1 \times s, 1]$ NRT-LCD 码。 □

推论 **1** *If s is even, then there is no binary $[1 \times s, s-1]$ NRT-LCD code.*

定理 **4** *There is a binary maximum distance separable $[1 \times s, 2]$ NRT-LCD code.*

Proof 若 $\mathcal{C}$ 是维数为二的二元最大距离可分码，则 $d_N = s-1$。因此， $\mathcal{C}$ 的标准形生成矩阵为

$$G = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,s-2} & 1 & 0 \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,s-2} & 0 & 1 \end{bmatrix},$$

其中 $a_{1,\ j}, a_{2,\ j} \in \mathbb{F}_2$，对于 $1 \le j \le s-2$。于是，

$$G^{\circ} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ a_{1,s-2} & a_{2,s-2} \\ \vdots & \vdots \\ a_{1,3} & a_{2,3} \\ a_{1,2} & a_{2,2} \\ a_{1,1} & a_{2,1} \end{bmatrix}.$$

因此， $GG^{\circ} = \begin{bmatrix} A_{1,\ 1} & A_{1,\ 2} \\ A_{2\ 1} & A_{2\ ,\ 2} \end{bmatrix}$，其中

i) 若 s 为偶数：$A_{1,\ 1} = A_{2,\ 2} = 0$，且

$$\begin{aligned} A_{1,2} &= a_{1,1} + a_{1,3}a_{2,s-2} + \ldots + a_{1,s-2}a_{2,3} + a_{2,2} \\ A_{2,1} &= a_{2,2} + a_{2,3}a_{1,s-2} + \ldots + a_{2,s-2}a_{1,3} + a_{1,1}. \end{aligned}$$

对于 $(i,\ j) \neq (1,1)$，选取 $a_{1,\ 1} = 1$ 和 $a_{i,\ j} = 0$，我们有

$$G = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix}$$

是一个二元最大距离可分 $[1 \times s, 2]$NRT-LCD 码的生成矩阵，因为 $GG^{\circ} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$。

ii) 若 n 为奇数：$A_{1,1} = a_{1,\frac{s+1}{2}}$, $A_{2,2} = a_{2,\frac{s+1}{2}}$，且

$$\begin{aligned} A_{1,2} &= a_{1,1} + a_{1,3}a_{2,s-2} + \ldots + a_{1,\frac{s+1}{2}}a_{2,\frac{s+1}{2}} + \ldots + a_{1,s-2}a_{2,3} + a_{2,2} \\ A_{2,1} &= a_{2,2} + a_{2,3}a_{1,s-2} + \ldots + a_{1,\frac{s+1}{2}}a_{2,\frac{s+1}{2}} + \ldots + a_{2,s-2}a_{1,3} + a_{2,2}. \end{aligned}$$

对所有 $j \neq \frac{s+1}{2}$，取 $a_{1,1} = a_{1,\frac{s+1}{2}} = a_{2,\frac{s+1}{2}} = 1$ 和 $a_{1,j} = a_{2,j} = 0$，则有

$$G = \begin{bmatrix} 1\ 0\ 0 \cdots\ 0\ 1\ 0 \cdots\ 0\ 1\ 0 \\ 0\ 0\ 0 \cdots\ 0\ 1\ 0 \cdots\ 0\ 0\ 1 \end{bmatrix}$$

是一个二元最大距离可分 $[1 \times s, 2]$NRT 线性互补对偶码的生成矩阵，因为 $GG^{\circ} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$。

□

推论 **2** *$LCD[1 \times s, 2] = s - 1$ and $LCD[1 \times s, s-2] = 3$.*

定理

5 *There is no binary maximum distance separable $[1 \times s, 3]$ NRT-LCD code for even s.*

Proof $\mathcal{C}$ 3, $d_N =$若 是一个维数为 的二元最大 $s-2$ 距离可分码，则 。因此， 的标准形$\mathcal{C}$生成矩阵为

$$G = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & \cdots & a_{1,s-3} & 1 & 0 & 0 \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & \cdots & a_{2,s-3} & 0 & 1 & 0 \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & \cdots & a_{3,s-3} & 0 & 0 & 1 \end{bmatrix}.$$

And,

$$G^{\circ} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ a_{1,s-3} & a_{2,s-3} & a_{3,s-3} \\ a_{1,s-4} & a_{2,s-4} & a_{3,s-4} \\ \vdots & \vdots & \vdots \\ a_{1,4} & a_{2,4} & a_{3,4} \\ a_{1,3} & a_{2,3} & a_{3,3} \\ a_{1,2} & a_{2,2} & a_{3,2} \\ a_{1,1} & a_{2,1} & a_{3,1} \end{bmatrix}.$$

So, $GG^{\circ} = \begin{bmatrix} A_{1,1} & A_{1,2} & A_{1,3} \\ A_{2,1} & A_{2,2} & A_{2,3} \\ A_{3,1} & A_{3,2} & A_{3,3} \end{bmatrix}$, where $A_{1,1} = A_{2,2} = A_{3,3} = 0$, and

$$A_{1,2} = A_{2,1} = a_{1,2} + a_{2,3} + \sum_{j=4}^{s-3} a_{1,j} a_{2,s-j+1}$$

$$A_{1,3} = A_{3,1} = a_{1,1} + a_{3,3} + \sum_{j=4}^{s-3} a_{1,j} a_{3,s-j+1}$$

$$A_{2,3} = A_{3,2} = a_{2,1} + a_{3,2} + \sum_{j=4}^{s-3} a_{2,j} a_{3,s-j+1}.$$

最后，我们可以验证 $\det(GG^{\circ}) = 0$。也就是说， $\mathcal{C}$ 不是一个 $[1 \times s, 3]$ NRT-LCD 码。□

10 二元 Niederreiter-Rosenbloom-Tsfasman LCD 码的界 s

定理

6 *There is a binary maximum distance separable* $[1\times s,3]$ *NRT-LCD code for odd* s.

Proof 设 G 是 $\mathcal{C}$ 的标准形生成矩阵。也就是说,

$$G=\begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & \cdots & a_{1,s-3} & 1 & 0 & 0 \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & \cdots & a_{2,s-3} & 0 & 1 & 0 \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & \cdots & a_{3,s-3} & 0 & 0 & 1 \end{bmatrix}.$$

于是,

$$G^{\circ}=\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ a_{1,s-3} & a_{2,s-3} & a_{3,s-3} \\ a_{1,s-4} & a_{2,s-4} & a_{3,s-4} \\ \vdots & \vdots & \vdots \\ a_{1,4} & a_{2,4} & a_{3,4} \\ a_{1,3} & a_{2,3} & a_{3,3} \\ a_{1,2} & a_{2,2} & a_{3,2} \\ a_{1,1} & a_{2,1} & a_{3,1} \end{bmatrix}.$$

因此, $GG^{\circ}=\begin{bmatrix} A_{1,1} & A_{1,2} & A_{1,3} & A_{2,1} & A_{2,2} & A_{2,3} & A_{3,1} & A_{3,2} & A_{3,3} \end{bmatrix}$, 其中 $A_{i,i}=a_{i,\frac{s+1}{2}}$ 对于 $i=1$、2、3, 且

$$A_{1,2}=A_{2,1}=a_{1,2}+a_{2,3}+\sum_{j=4}^{s-3}a_{1,j}a_{2,s-j+1}$$

$$A_{1,3}=A_{3,1}=a_{1,1}+a_{3,3}+\sum_{j=4}^{s-3}a_{1,j}a_{3,s-j+1}$$

$$A_{2,3}=A_{3,2}=a_{2,1}+a_{3,2}+\sum_{j=4}^{s-3}a_{2,j}a_{3,s-j+1}.$$

我们可以验证 $\det(GG^{\circ}=a_{1,\frac{s+1}{2}}a_{2,\frac{s+1}{2}}a_{3,\frac{s+1}{2}}+a_{1,\frac{s+1}{2}}A_{2,3}+a_{2,\frac{s+1}{2}}A_{1,3}+a_{3,\frac{s+1}{2}}A_{1,2}$, $a_{2,1}=a_{1,\frac{s+1}{2}}=1$, $a_{i,j}=0$, , , , , , , , , 。因此, 例如, 若我们选择 , , , 并且对所有 $(i,j)\notin\{(2,1)(1,\frac{s+1}{2})\}$, 则

$$G=\begin{bmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 \end{bmatrix}$$

满足 $\det(GG^{\circ})=1$。也就是说, G 是一个 $[1\times s,3]$ NRT-LCD码的生成矩阵。□

推论 **3** *If* s *is odd, then* $LCD[1\times s,3]=s-2$ *and* $LCD[1\times s,s-3]=4$.

一般而言, 对于 k 偶数, 我们有以下结果。

定理 **7** *There is a binary maximum distance separable* $[1\times s,k]$ *NRT-LCD code for* k *is even. In other words if* k *is even then* $LCD[1\times s,k]=s-k+1$. ,

*Proof*令 $\mathcal{C}$为由下列标准形生成矩阵给出的二元 $[1\times s,k,s-k+1]$NRT 度量码

$$G=\begin{bmatrix} e_1+e_{s-k+1}\\ e_2+e_{s-k+2}\\ \vdots\\ e_{\frac{k}{2}}+e_{s-\frac{k}{2}}\\ e_{s-\frac{k}{2}+1}\\ e_{s-\frac{k}{2}+2}\\ \vdots\\ e_{s-1}\\ e_s \end{bmatrix}, \tag{13}$$

其中， e_i 是 $\mathbb{F}_2^s$ 的第 i个典范向量，且 $1\le i\le s$。因此,

$$flip(G)=\begin{bmatrix} e_s+e_k\\ e_{s-1}+e_{k-1}\\ \vdots\\ e_{s-\frac{k}{2}+1}+e_{\frac{k}{2}-1}\\ e_{\frac{k}{2}}\\ e_{\frac{k}{2}-1}\\ \vdots\\ e_2\\ e_1 \end{bmatrix}, \tag{14}$$

and

$$G^{\circ}=\left[\, e_s^T+e_k^T \middle| e_{s-1}^T+e_{k-1}^T \middle| \cdots \middle| e_{s-\frac{k}{2}+1}^T+e_{\frac{k}{2}-1}^T \middle| e_{\frac{k}{2}}^T \middle| e_{\frac{k}{2}-1} \middle| \cdots \middle| e_2^T \middle| e_1^T \,\right]. \tag{15}$$

最后,

$$GG^{\circ}=\begin{bmatrix} 0&0&\cdots&0&1\\ 0&0&\cdots&1&0\\ \vdots&\vdots&\vdots&\vdots&\vdots\\ 0&1&\cdots&0&0\\ 1&0&\cdots&0&0 \end{bmatrix}. \tag{16}$$

GG° 显然是非奇异的。证明 $\mathcal{C}$ 是一个二元最大距离可分 $[1\times s,k]$ NRT-LCD 码。□

s 和 k 均为奇数的情况由以下定理描述 .

定理 **8** *There is a binary maximum distance separable* $[1\times s,k]$ *NRT-LCD code for* s *and* k *odd. In other words if* s *and* k *are odd then* $LCD[1\times s,k]=s-k+1$. ,

*Proof*设 $\mathcal{C}$为由以下标准形生成矩阵给出的二元 $[1\times s, k, s-k+1]$ NRT 度量码

$$G=\begin{bmatrix} e_{\frac{s+1}{2}}+e_{s-k+1} \\ e_1+e_{s-k+2} \\ e_2+e_{s-k+3} \\ \vdots \\ e_{\frac{k+1}{2}-1}+e_{s-k+\frac{k+1}{2}} \\ e_{s-k+\frac{k+1}{2}} \\ e_{s-k+\frac{k+1}{2}+1} \\ \vdots \\ e_{s-1} \\ e_s \end{bmatrix}, \tag{17}$$

其中， e_i 是 $\mathbb{F}_2^s$ 的第 i个典范向量，其中 $1\le i\le s$。因此，

$$flip(G)=\begin{bmatrix} e_{\frac{s+1}{2}}+e_k \\ e_s+e_{k-1} \\ e_{s-1}+e_{k-2} \\ \vdots \\ e_{s-\frac{k-3}{2}}+e_{\frac{k+1}{2}} \\ e_{\frac{k+1}{2}-1} \\ e_{\frac{k+1}{2}-2} \\ \vdots \\ e_2 \\ e_1 \end{bmatrix}, \tag{18}$$

and

$$G^{\circ}=\left[\, e^T_{\frac{s+1}{2}}+e^T_k \,\middle|\, e^T_s+e^T_{k-1} \,\middle|\, e^T_{s-1}+e^T_{k-2} \,\middle|\cdots\middle|\, e^T_{s-\frac{k-3}{2}}+e^T_{\frac{k+1}{2}} \,\middle|\, e^T_{\frac{k+1}{2}-1} \,\middle|\, e_{\frac{k+1}{2}-2} \,\middle|\cdots\middle|\, e^T_2 \,\middle|\, e^T_1 \,\right]. \tag{19}$$

最后，

$$GG^{\circ}=\begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \end{bmatrix}. \tag{20}$$

GG° 显然是非奇异的。证明 $\mathcal{C}$ 是一个二元最大距离可分$[1\times s, k]$ NRT-LCD 码。□

4 二元 NRT-LCD 码的基本界 $M_{n,\ 2}(\mathbb{F}_2)$

本节将证明二元最大距离可分 $[n\times 2, k]$ NRT-LCD 码不存在的一个条件。为此，我们将考虑[17] NRT 度量码的 Plotkin 界。

定理 **9** *([17], Plotkin bound for NRT metric codes). Let $\mathcal{C}$ be an $[n\times s,k,d_N]$ NRT metric code such that $d_N > ns\delta_{crit}$, where $\delta_{crit}=1-\frac{1}{sq^s}\frac{q^s-1}{q-1}$. Then,*

$$q^k \leq \frac{d_N}{d_N - ns\delta_{crit}}. \tag{21}$$

引理 **3** *$LCD[n\times 2,k]\leq\left(\frac{5}{2^k-1}\right)n<2n-k+1$ for $n>\left(\frac{2^k-1}{2^{k+1}-7}\right)(k-1)$。*

*Proof*我们先证明 $LCD[n\times 2,k]\leq\left(\frac{5}{2^k-1}\right)n$。根据 Plotkin 界（21），任意二元 $[n\times 2,k,d_N]$ NRT 度量码，只要满足 $d_N>2n\delta_{crit}=\frac{5}{4}n$，就有

$$2^k \leq \frac{d_N}{d_N-\frac{5n}{4}}. \tag{22}$$

解出 d_N，得 $d_N\leq\left(\frac{5}{2^k-1}\right)n$。因此，任意 $[n\times 2,k,d_N]$ NRT-LCD 码都必须满足这个不等式。由此证明 $LCD[n\times 2,k]\leq\left(\frac{5}{2^k-1}\right)n$。现在，注意到

$$2n-k+1-\left(\frac{5}{2^k-1}\right)n>0\Longleftrightarrow\left(\frac{2^{k+1}-7}{2^k-1}\right)>k-1\Longleftrightarrow n>\left(\frac{2^k-1}{2^{k+1}-7}\right)(k-1). \tag{23}$$

证明：如果 $\left(\frac{5}{2^k-1}\right)n<2n-k+1$ $n>\left(\frac{2^k-1}{2^{k+1}-7}\right)(k-1)$。 □

推论 **4** *Let n,k be positive integers such that $n>\left(\frac{2^k-1}{2^{k+1}-7}\right)(k-1)$. Then, there is no binary maximum distance separable $[n\times 2,k]$ NRT-LCD code.*

推论 **5** *Let n,k be positive integers such that $n>\left(\frac{2^k-1}{2^{k+1}-7}\right)(k-1)$. Then*

$$LCD[n\times 2,k]<2n-k+1.$$

定理 **10** *We have the following:*

i) $LCD[2\times 2,2]=2$;
ii) $LCD[3\times 2,2]=5$;

Proof i) 设 $\mathcal{C}$ 为由以下生成矩阵给出的二元 $[2\times 2,2]$ NRT 度量码

$$G=\left[\begin{array}{cc|cc} 1&0&1&1\\ 0&1&1&1\end{array}\right].$$

容易验证，$GG^\dagger$ 是非奇异的，且 $d_N(\mathcal{C})=2$。

我们来证明不存在二元 $[2\times 2,2,3]$ NRT-LCD 码。注意，根据定理 1，如果 $\mathcal{C}$ 是一个二元 $[2\times 2,2]$ NRT 度量码，那么 $\mathcal{C}$ 等价于一个生成矩阵如下的码 $G=[G_1\mid G_2]$，其中 G_1 的非零行是

互不相同的典范向量，按 NRT 权递增排列，并且 G 为分块阶梯形。此外， G_2 的最后一行非零，因为 $\dim(\mathcal{C}) = 2$。

如果 G_1 的最后一行是零，那么 $\mathcal{C}$ 有一个含零行的码字。也就是说，在这种情况下， $d_N(\mathcal{C}) \leq 2$。

因此，我们只需分析以下情况：

$$G = \left[\begin{array}{cc|cc} 1 & 0 & a & b \\ 0 & 1 & c & d \end{array}\right], \tag{24}$$

其中 $(c, d) \neq (0, 0)$。在这种情况下，

$$GG^{\dagger} = \begin{bmatrix} 0 & 1+ad+bc \\ 1+ad+bc & 0 \end{bmatrix}$$

以及生成矩阵 G 形式为 (24)，且满足 $GG^{\dagger}$ 非奇异的矩阵为

$$\left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right], \left[\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{array}\right], \left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{array}\right], \left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right].$$

可以验证，这些矩阵生成了 $[2 \times 2, 2]$ NRT-LCD 码，且 $d_N(\mathcal{C}) \leq 2$。

ii) 令 $\mathcal{C}$ 为二元 $[2 \times 2, 2]$ NRT 度量码，其生成矩阵为

$$G = \left[\begin{array}{cc|cc|cc} 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right].$$

容易验证 $GG^{\dagger} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$。也就是说， $\mathcal{C}$ 是一个二元 $[3 \times 2, 2]$ NRT-LCD 码。此外，

$$\mathcal{C} = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

且 $d_N(\mathcal{C}) = 5$。 □

推论

6 *There is a binary maximum distance separable* $[n \times 2, 2]$ *NRT-LCD code if and only if* $n = 3$.

定理 **11** *Let* $n \neq 3$ *be a positive integer. Then*

$$n \leq LCD[n \times 2, 2] \leq 2n - 1.$$

Proof $LCD[n \times 2, 2] \leq 2n - 1$ 根据推论6。我们来验证 $LCD[n \times 2, 2] \geq n$。注意，若 n 为奇数，则二元 $[n \times 2, 2]$ NRT-LCD 码

$$\mathcal{C} = \left\{0, \left[\begin{array}{c|c} \sum_{i=1}^{n} e_i^T & 0^T \end{array}\right], \left[\begin{array}{c|c} 0^T & \sum_{i=1}^{n} e_i^T \end{array}\right], \left[\begin{array}{c|c} \sum_{i=1}^{n} e_i^T & \sum_{i=1}^{n} e_i^T \end{array}\right]\right\}.$$

满足 $d_N(\mathcal{C}) = n$。

现在，若 n 为偶数，则二元 $[n \times 2, 2]$ NRT-LCD 码

$$\mathcal{C} = \left\{0, \left[\begin{array}{c|c} \sum_{i=1}^{n} e_i^T & 0^T \end{array}\right], \left[\begin{array}{c|c} 0^T & \sum_{i=1}^{n-1} e_i^T \end{array}\right], \left[\begin{array}{c|c} \sum_{i=1}^{n} e_i^T & \sum_{i=1}^{n-1} e_i^T \end{array}\right]\right\}.$$

使得 $d_N(\mathcal{C}) = n$。 □

4.1 二元 NRT-LCD 码在$M_{n,2}(\mathbb{F}_2)$中的线性规划界

本节中，我们将给出二元 NRT-LCD 码的线性规划界。我们将利用 NRT 度量码的广义 MacWilliams 恒等式。该 MacWilliams 恒等式已通过不同方法证明，见 [1,6, 9, 22]。为契合本文的语境，我们将给出该恒等式在 $s = 2$ 情况下的表述。

定义 8 设 $v \in M_{n,2}(\mathbb{F}_2)$写作 $[v_1;\ v_2; \ldots, v_n]$，其中 $v_i = [v_{i,1}, v_{i,2}]$ for $i = 1, \ldots, n$。关于 NRT 权，v的形状是一个 2-向量$shape(v) = (e_1, e_2)$，其中

$$e_j = \mid \{i : 1 \leq i \leq n \text{ and } \rho(v_i) = j\} \mid . \tag{25}$$

另定义 $e_0 = n - \mid shape(v) \mid$，其中 $\mid shape(v) \mid = e_1 + e_2$。

组合计算表明，满足 $shape(e_1, e_2)$ 的$v \in M_{n,2}(\mathbb{F}_2)$ 的数量为

$$\binom{n}{e_0, e_1, e_2} 2^{e_2}. \tag{26}$$

注意，若对于 $v \in M_{n,2}(\mathbb{F}_2)$，定义 $\mid shape(e) \mid' = e_1 + 2e_2$，则$\rho(v) = \mid shape(e) \mid'$。

$\mathcal{C} \subseteq M_{n,2}(\mathbb{F}_2)$ 的形状枚举多项式为

$$H_{\mathcal{C}}(z_0, z_1, z_2) = \sum_{e \in \Delta_{n,2}} \mathcal{A}_e z_0^{e_0} z_1^{e_1} z_2^{e_2},$$

其中 $\mathcal{A}_e := \mid \{v \in \mathcal{C} \colon shape(v) = e\} \mid$ 且 $\Delta_{n,2} = \{e \in \mathbb{N}^2 \colon e_0 + e_1 + e_2 = n\}$。

定理 **12** *([6]) Let $\mathcal{C} \subseteq M_{n,2}(\mathbb{F}_2)$ be an $[n \times 2, k]$ NRT metric code. Further onlet $(\mathcal{A}_e)$ be the shape distribution of $\mathcal{C}$ and $(\mathcal{A}'_e)$ be the shape distribution of $\mathcal{C}^{\perp_N}$.Then*

$$\mathcal{A}'_e = \frac{1}{2^k} \sum_{e^\star \in \Delta_{n,2}} B_e(e^\star) \mathcal{A}_{e^\star},$$

where

$$B_e(e^\star) = 2^{e_2} \prod_{t=1}^{2} \left(\sum_{j_t=0}^{e_t} (-1)^{j_t} \binom{e^\star_{3-t}}{j_t} \binom{\sum_{r=0}^{2-t} e^\star_r - \sum_{r=t+1}^{2} e^\star_r}{e_t - j_t} \right).$$

注意，若 $\mathcal{C}$ 是一个二元 $[n \times 2, k]$ NRT-LCD 码，且 $\mathcal{A}_e$ 是其形状分布。令 $\mathcal{A}'_e$ 为其对偶码 $\mathcal{C}^{\perp_N}$ 的形状分布。根据

NRT-LCD 码的定义，若 $v \in \mathcal{C}$，则 $v \notin \mathcal{C}^{\perp_N}$，因此

$$\mathcal{A}_e + \mathcal{A}'_e \leq \binom{n}{e_0, e_1, e_2} 2^{e_2}. \tag{27}$$

根据定理12，我们有

$$\mathcal{A}'_e = \frac{1}{2^k} \sum_{e^\star \in \Delta_{n,2}} B_e(e^\star) \mathcal{A}_{e^\star}. \tag{28}$$

此外，由于 $\dim \mathcal{C} = k$，我们有

$$2^k = \sum_{e^\star \in \Delta_{n,2}} \mathcal{A}_{e^\star}. \tag{29}$$

结合（27）、（28）和（29），我们得到二元 NRT-LCD码的以下界。

定理 **13** *If $\mathcal{C}$ is a binary $[n \times 2, k]$ NRT-LCD code. Then,*

$$2^k \mathcal{A}_e \leq \sum_{e^\star \in \Delta_{n,2}} \mathcal{A}_{e^\star} \left[\binom{n}{e_0, e_1, e_2} - B_e(e^\star) \right]. \tag{30}$$

5 构造

本节中，我们介绍二元 Niederreiter-Rosenbloom-Tsfasman 线性互补对偶码的两种新构造。

第一种构造（定理 14）由一个$M_{1,s+2}(\mathbb{F}_2)$中的二元 NRT-LCD 码，得到一个$M_{1,s+2}(\mathbb{F}_2)$中的二元 NRT-LCD 码，其中 s 为奇数。第二种构造（定理 15）由一个 $M_{1,s}(\mathbb{F}_2)$中的二元 NRT-LCD 码，得到一个 $M_{n,s+2}(\mathbb{F}_2)$ 中的二元 NRT-LCD 码，其中 s 和 n 为奇数。

定理 **14** *Let $\mathcal{C}$ be a binary $[1 \times s, k]$ NRT-LCD code with generator matrix*

$$G := \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{bmatrix} = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,s} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,s} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,s} \end{bmatrix}. \tag{31}$$

Let $x = (x_1, x_2, \ldots, x_s) \in \mathbb{F}_2^s$ and $\mathcal{C}(x)$ be the binary code with the following generatormatrix

$$G(x) = \left[\begin{array}{c|ccc|c} 1 & x_1 & \ldots & x_s & 0 \\ \hline \langle x, g_1 \rangle_N & g_{1,1} & \cdots & g_{1,s} & \langle x, g_1 \rangle_N \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \langle x, g_k \rangle_N & g_{k,1} & \cdots & g_{k,s} & \langle x, g_k \rangle_N \end{array}\right]. \tag{32}$$

If s is odd and $x_{\frac{s+1}{2}} = 1$ and $x_j = 0$ for $j > \frac{s+1}{2}$. Then $\mathcal{C}$ x is a binary $[1 \times s+, 0()$ $2 \quad k+1]$ NRT-LCD code.

Proof 显然， $\mathcal{C}(x)$ 是一个二元 $[1 \times (s+2)\ k+1]$ NRT 度量码。注意

$$G^{\circ}(x) = \left[\begin{array}{c|ccc|c} 0 & \langle x, g_1\rangle_N & \cdots & \langle x, g_{k-1}\rangle_N & \langle x, g_k\rangle_N \\ \hline x_s & g_{2,s} & \cdots & g_{k-1,s} & g_{k,s} \\ x_{s-1} & g_{2,s-1} & \cdots & g_{k-1,s-1} & g_{k,s-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_1 & g_{1,1} & \cdots & g_{k-1,1} & g_{k,1} \\ \hline 1 & \langle x, g_1\rangle_N & \cdots & \langle x, g_k\rangle_N & \langle x, g_k\rangle_N \end{array}\right]. \tag{33}$$

因此，

$$G(x)G^{\circ}(x) = \left[\begin{array}{c|c} \langle x, x\rangle_N & \mathbf{0} \\ \hline \mathbf{0}^T & GG^{\circ} \end{array}\right]^2, \text{ where } \mathbf{0} = (0, 0, \ldots, 0) \in \mathbb{F}_2^k.$$

另请注意， $\langle x, x\rangle_{RT} = \left(x_{\frac{s+1}{2}}\right)^2 = 1$。也就是说， $G(x)G^{\circ}(x)$ 是非奇异的。证明 $\mathcal{C}(x)$ 是一个二元 $[1 \times (s+2)\ k+1]$ NRT-LCD 码。□

定理 **15** *Let $\mathcal{C}$ be a binary $[1 \times s, k]$ NRT-LCD code with generator matrix*

$$G := \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{bmatrix} = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,s} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,s} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,s} \end{bmatrix}. \tag{34}$$

Let $x = (x_1, x_2, \ldots, x_s) \in \mathbb{F}_2^s$, and $\mathcal{C}(x)$ be the binary $[1 \times (s+2)\ k+1]$ NRT code with the following generator matrix

$$G(x) = \left[\begin{array}{c|ccc|c} 1 & x_1 & \cdots & x_s & 0 \\ \hline \langle x, g_1\rangle_N & g_{1,1} & \cdots & g_{1,s} & \langle x, g_1\rangle_N \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \langle x, g_k\rangle_N & g_{k,1} & \cdots & g_{k,s} & \langle x, g_k\rangle_N \end{array}\right]. \tag{35}$$

If s and n are odd, $x_{\frac{s+1}{2}} = 1$ and $x_j = 0$ for $j > \frac{s+1}{2}$. Then, the code $\mathcal{C}_n$ (x) generated by

$$G_{(n)} := G(x, x, \ldots, x) = [G(x) \mid G(x) \mid \cdots \mid G(x)] \tag{36}$$

is a binary $[n \times (s+2) \quad k+1]$ NRT-LCD code.

Proof 显然， $\mathcal{C}_n(x)$ 的长度为 $[n \times (s+2)\ k+1]$，这是一个二元 NRT 度量码。注意，

$$G_{(n)}^{\dagger} = \begin{bmatrix} G^{\circ}(x) \\ G^{\circ}(x) \\ \vdots \\ G^{\circ}(x) \end{bmatrix}. \tag{37}$$

18 二元 Niederreiter-Rosenbloom-Tsfasman LCD 码的界 s

因此，

$$\begin{aligned} G_{(n)}G_{(n)}^{\dagger} &= G(x)G^{\circ}(x) + G(x)G^{\circ}(x) + \cdots + G(x)G^{\circ}(x) \\ &= G(x)G^{\circ}(x) \end{aligned}$$

由于 n $G_{(n)}G_{n}^{\dagger}$ $\mathcal{C}_n$ x $[1\times$ $s+$ 为奇数。因此，

2 □

() 是非奇异的。由此证明 ( ) 是一个二元 ( ) $k+1]$ NRT-LCD 码。

6 结论

本文研究了二元 NRT-LCD 码的最大最小距离。特别地，我们证明了当 k 为偶数，或 s 和 k 均为奇数时，二元最大距离可分 $[1\times s, k]$ NRT-LCD 码的存在性。我们推导了二元 $[n\times 2, k]$ NRT-LCD 码存在时 n 所需满足的条件。最后，我们给出了二元 $[n\times 2, k]$NRT-LCD 码的线性规划界及两种新的构造方法。对于那些无法构造最大距离可分 NRT-LCD 码的参数，寻找具有小核的最大距离可分码构造方法将会很有意义。

参考文献

[1] A. Barg, P. Purkayastha，《有序码与正交阵的界》，《莫斯科数学杂志》，第9卷，第211-243页，2009年。[2] A. K. Sharma, A. Sharma，关于RT度量下重量枚举子的MacWilliams恒等式，《离散数学：算法与应用》，第6卷，文章编号1450030，共11页，2014年。[3] C. Carlet, S. Guilley，用于防御侧信道攻击的互补对偶码，《通信数学进展》，第10卷，第131-150页，2016年。[4]C. Carlet, S. Mesnager, C. Tang, Y. Qi，LCD码的新刻画与参数化，《IEEE信息论汇刊》，第65卷，第39-49页，2019年。[5] H. Niederreiter，有限域上向量空间的一个组合问题，《离散数学》，第96卷，第221-228页，1991年。[6] H. Trinker，线性有序码与正交阵的MacWilliams恒等式的一种简明推导，《设计、编码与密码学》，第50卷，第229-234页，2009年。[7]H. Xu, G. Xu, W. Du, Niederreiter-Rosenbloom-Tsfasman LCD 码，《通信数学进展》，2022年。

[8] I. Siap，阵列码的CT突发错误重量枚举，《阿尔巴尼亚数学杂志》，第2卷，第171-178页，2008年。[9]I. Siap, M. Ozen，关于$M_{n\times s}(R)$上码的完全重量枚举子，《应用数学快报》，第17卷，第65-69页，2004年。[10] J. L. Massey，具有互补对偶的线性码，《离散数学》，第106卷，第337-342页，1992年。[11] J. Quistorff，论Rosenbloom和Tsfasman对汉明空间的推广，《离散数学》，第307卷，第2514-2524页，2007年。[12] M. Araya, M. Harada，线性互补对偶码的分类，《离散数学》，第342卷，第270-278页，2019年。[13] M. Araya, M. Harada，二元线性互补对偶码的最小重量，《密码学通讯》，第12卷，第285-300页，2020年。[14] M. Araya, M. Harada, K. Saito，最优LCD码的刻画与分类，《设计、编码与密码学》，第89卷，第617-640页，2021年。[15]M. M. S. Alves，关于Niederreiter-Rosenbloom-Tsfasman度量的生成矩阵标准形，2011年IEEE信息论研讨会，巴西帕拉蒂，2011年，第486-489页，doi: 10.1109/ITW.2011.6089508。[16] M. M. Skriganov，编码理论与均匀分布，《圣彼得堡数学杂志》，第13卷，第310-337页，2002年。[17] M. Yu. Rosenbloom, M. A. Tsfasman，m-度量下的码，《信息传输问题》，第33卷，第55-63页（俄文），1997年。MR 98c:94023。英文译本载于《信息传输问题》，第33卷，第45-52页，1997年。[18] M. Ozen和I. Siap，关于Rosenbloom-Tsfasman度量下线性码的结构与译码，《Selçuk应用数学杂志》，第5卷，第2期，第25-31页，2004年。[19] R. A. Brualdi, J. S. Graves和K. M. Lawrence，具有偏序集度量的码，《离散数学》，第147卷，第57-72页，1995年。[20] R. Refslund Nielsen，一类Sudan可译码，载于《IEEE信息论汇刊》，第46卷，第4期，第1564-1572页，2000年7月，doi: 10.1109/18.850696。[21] S. Jain， m度量阵列码中的突发，《线性代数及其应用》，第418卷，第130-141页，2006年。

[22]S. T. Dougherty、M. M. Skriganov，MacWilliams 对偶性与 Rosenbloom-Tsfasman 度量，《莫斯科数学杂志》，第 2 卷，第 81-97 页，2002 年。[23]S. T. Dougherty 和 K. Shiromoto，具有非汉明度量和均匀分布的$Mat_{N,S}(Z(K))$中的最大距离码，《设计、编码与密码学》，第 33 卷，第 45-61 页，2004 年。[24] S. T. Dougherty 和 M. M. Skriganov，任意字母表上 ρ 度量中的最大距离可分码，《代数组合学杂志》，第 16 卷，第 71-81 页，2002 年。[25]V. Marka、R.S. Selvaraj 和 I. Gnanasudha，Rosenbloom-Tsfasman 度量中的自对偶码，《数学通讯》，第 22 卷，第 75-87 页，2017 年。[26] W. Santos 和 M. M. Alves，NRT 度量中自对偶码的多项式不变理论与形状枚举多项式，载于《IEEE 信息论汇刊》，第 66 卷，第 7 期，第 4061-4074 页，2020年7月，doi：10.1109/TIT.2020.2971989。[27] W. Santos 和 M. M. Alves，Rosenbloom-Tsfasman 度量码的分数译码，审稿中。[28]W. Zhou、S. Lin 和 K. A. S. Abdel-Ghaffar，Rosenbloom-Tsfasman 度量的 BCH 码，载于《IEEE 信息论汇刊》，第 62 卷，第 12 期，第 6757-6767 页，2016 年 12 月，doi：10.1109/TIT.2016.2617312。