

一类定秩集秩度量码的上界

卫烨铭, 王知庶

苏州科技大学数学科学学院, 江苏 苏州

收稿日期: 2024年10月27日; 录用日期: 2024年11月21日; 发布日期: 2024年11月28日

摘 要

常维码因其在网络编码中的重要作用受到广大学者的关注。为了构造好的常维码, Liu等人通过引入定秩集秩度量码提出了并行构造法。本文主要通过计算当 q 是任意素数幂时 $Q_{1,1,1}$, $Q_{1,2,1}$, $Q_{2,1,1}$, $Q_{2,2,1}$ 的值, 得到参数为 $(n \times n, 3, [1, 2])_q$ 的定秩集秩度量码的球填充上界。

关键词

秩距离, 秩度量码, 常维码

New Upper Bounds of Some Rank Metric Codes with Given Ranks

Yeming Wei, Zhishu Wang

School of Mathematical Sciences, Suzhou University of Science and Technology, Suzhou Jiangsu

Received: Oct. 27th, 2024; accepted: Nov. 21st, 2024; published: Nov. 28th, 2024

Abstract

Constant dimension codes (CDCs) have received a lot of attention due to their application in random network coding. To construct good CDCs, Liu *et al.* raised the parallel construction by rank metric codes with given ranks (GRMCs). This paper calculates the value of $Q_{1,1,1}$, $Q_{1,2,1}$, $Q_{2,1,1}$, $Q_{2,2,1}$ when q is prime power, and the Gilbert-Hamming upper bounds of $(n \times n, 3, [1, 2])_q$ GRMCs.

Keywords

Rank Distance, Rank-Metric Code, Constant Dimension Code



1. 引言

伴随计算机网络的飞速发展, 编码与加密在现代网络通信中有着广泛的应用。网络编码[1]是一种新型网络数据传输方式, 网络节点不仅能执行数据的复制和转发这两项操作, 而且可以对接收到的数据进行相应的线性、非线性的编码操作。网络编码具有提高网络的组播吞吐量、提高宽带的利用率、降低节点的传输能耗等优点。因此, 网络编码被看作是未来网络的核心技术, 受到各国学者的高度重视。

随机网络编码方法是无线网络环境中非常有效的工具, 但容易造成数据包的丢失和错误。因此, 在无线网络编码中进行纠错控制是非常必要的。为了解决此问题, Kotter [2]提出了常维码(CDCs)。

为了获得最优的常维码, Silva、Kschischang 和 Kotter [3]指出提升最大秩距离(MRD)码可以产生渐近最优的常维码。Xu 等人[4]和 Liu 等人[5]通过引入一种新的辅助码——定秩集秩度量码, 并提出并行构造法。关于本课题的更多资料, 有兴趣的读者可以查阅文献[2] [4] [6]-[10]。

本文通过计算当 q 是任意素数幂时, 相关参数 $Q_{1,1,1}$, $Q_{1,2,1}$, $Q_{2,1,1}$, $Q_{2,2,1}$ 的值, 并利用定秩集秩度量码的球填充界和上述参数值, 获得参数为 $(n \times n, 3, [1, 2])_q$ 的上界, 推广了 Liu 等人的结论。

2. 预备知识

令 $\mathbb{F}_q$ 表示 q 阶有限域, $\mathbb{F}_q^{m \times n}$ 表示 $\mathbb{F}_q$ 上所有尺寸为 $m \times n$ 的矩阵的集合。记 $[t_1, t_2] = \{i \in \mathbb{N} : t_1 \leq i \leq t_2\}$ 。

定义 2.1 [11]-[13]: 对于矩阵 $A, B \in \mathbb{F}_q^{m \times n}$, 它们的秩距离定义如下:

$$d_R(A, B) = \text{rank}(A - B)。$$

定义 2.2 [5]: 对于 $K \subseteq \{0, 1, \dots, n-1\}$, $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ 是一个参数为 $(m \times n, \delta, K)_q$ -w 定秩集秩度量码(GRMC), 如果 $\mathcal{C}$ 满足

- 1) 对于任意的 $C \in \mathcal{C}$, $\text{rank}(C) \in K$;
- 2) 对于任意的 $C_1, C_2 \in \mathcal{C}$, 且 $C_1 \neq C_2$, 有 $d_R(C_1, C_2) \geq \delta$ 。

如果 $|\mathcal{C}| = M$, 则一个参数为 $(m \times n, \delta, K)_q$ -GRMC 可以表示为 $(m \times n, M, \delta, K)_q$ -GRMC。给定 m, n, K 和 δ , 其中 $m \geq n$, 记号 $A_q^R(m \times n, \delta, K)$ 表示所有参数为 $(m \times n, \delta, K)_q$ -GRMCs 中码字数的最大值。下面的命题给出了定秩集秩度量码的球填充界。

命题 2.3 [14]: 对于 $m \geq n \geq r_2 \geq r_1$, 且 $n \geq d_R$,

$$A_q^R(m \times n, d_R, [r_1, r_2]) \leq g,$$

其中,

$$\max : g = \sum_{j=r_1}^{r_2} x_j ;$$

$$\begin{cases} \sum_{j=r_1}^{r_2} Q_{i,j,l} \left\lfloor \frac{d_R-1}{2} \right\rfloor \cdot x_j \leq P_i^{m \times n}, \text{ 对于任意的 } \max \left\{ r_1 - \left\lfloor \frac{d_R-1}{2} \right\rfloor, 0 \right\} \leq i \leq \min \left\{ r_2 + \left\lfloor \frac{d_R-1}{2} \right\rfloor, n \right\}; \\ x_j \geq 0, x_j \in \mathbb{Z}, \text{ 对任意的 } r_1 \leq j \leq r_2, \end{cases}$$

记 $Q_{i,j,l} = \left| \left\{ B \in \mathbb{F}_q^{m \times n} : \text{rank}(B) = i \text{ 且 } \text{rank}(B - E_j) \leq l \right\} \right|$, x_j 表示 $(m \times n, d_R, [r_1, r_2])_q$ -GRMCs 中秩为 j 的码字

个数, $P_r^{m \times n} = \sum_{(i_1, \dots, i_r) \in [n]^r} q^{rm - \sum_{j=1}^r i_j} \prod_{j=1}^r (q^{n-j+1} - 1)$ 。

3. 定秩集秩度量码的界

命题 2.3 虽然给出定秩集秩度量码的球填充界, 但是 $Q_{i,j,l}$ 的值不易计算。本章主要通过计算当 q 是任意素数幂时, 相关参数 $Q_{1,1,1}$, $Q_{1,2,1}$, $Q_{2,1,1}$, $Q_{2,2,1}$ 的值, 得到参数为 $(n \times n, 3, [1, 2])_q$ 的上界。

定理 3.1:

- (1) $Q_{1,1,1} = \left| \left\{ \mathbf{B} \in \mathbb{F}_q^{m \times n} : \text{rank}(\mathbf{B}) = 1 \text{ 且 } \text{rank}(\mathbf{B} - \mathbf{E}_1) \leq 1 \right\} \right| = q^m + q^n - q - 1;$
- (2) $Q_{1,2,1} = \left| \left\{ \mathbf{B} \in \mathbb{F}_q^{m \times n} : \text{rank}(\mathbf{B}) = 1 \text{ 且 } \text{rank}(\mathbf{B} - \mathbf{E}_2) \leq 1 \right\} \right| = q^2 + q;$
- (3) $Q_{2,1,1} = \left| \left\{ \mathbf{B} \in \mathbb{F}_q^{m \times n} : \text{rank}(\mathbf{B}) = 2 \text{ 且 } \text{rank}(\mathbf{B} - \mathbf{E}_1) \leq 1 \right\} \right| = \frac{(q^n - q)(q^m - q)}{q - 1};$
- (4) $Q_{2,2,1} = \left| \left\{ \mathbf{B} \in \mathbb{F}_q^{m \times n} : \text{rank}(\mathbf{B}) = 2 \text{ 且 } \text{rank}(\mathbf{B} - \mathbf{E}_2) \leq 1 \right\} \right| = q^{m+1} + q^{n+1} + q^m + q^n - q^3 - 2q^2 - 2q。$

证明 (1) 设 $\mathbf{C} = \mathbf{B} - \mathbf{E}_1$ 。

若 $\text{rank}(\mathbf{C}) = 0$, 则 $\mathbf{B} = \mathbf{E}_1$, 满足要求 $\text{rank}(\mathbf{B}) = 1$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 1。下面讨论 $\text{rank}(\mathbf{C}) = 1$ 的情况。假设 $\mathbf{C}$ 的第 $i_1, i_2, \dots, i_h$ 行是非零行向量, 设

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}, \text{ 则 } \mathbf{C} = \mathbf{B} - \mathbf{E}_1 = \begin{pmatrix} b_{11} - 1 & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}。$$

(1.1) 当 $h=1$ 且 $i_1=1$ 时, 我们有

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

其中 $(b_{11}, b_{12}, \dots, b_{1n}) \in \mathbb{F}_q^n \setminus \{(0, 0, \dots, 0), (1, 0, \dots, 0)\}$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 $q^n - 2$ 。

(1.2) 当 $h>1$ 且 $i_1=1$ 时, 记 $i=1, 2, \dots, m-1$, 不妨设

$$(b_{i+1,1}, b_{i+1,2}, \dots, b_{i+1,n}) = k_i (b_{11} - 1, b_{12}, \dots, b_{1n}),$$

其中 $k_1, k_2, \dots, k_{m-1} \in \mathbb{F}_q$ 且不全为 0。我们有

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix} \rightarrow \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ -k_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -k_{m-1} & 0 & \cdots & 0 \end{pmatrix},$$

由于 $\text{rank}(\mathbf{B}) = 1$, 从而 $b_{11} \neq 1$, $b_{12} = \dots = b_{1n} = 0$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 $(q^{m-1} - 1)(q - 1)$ 。

(1.3) 当 $i_1 > 1$ 时, 此时 $\mathbf{C}$ 的第一行是零行, 即 $b_{11} = 1$, $b_{12} = \dots = b_{1n} = 0$ 又 $\text{rank}(\mathbf{B}) = 1$, 我们有

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ b_{21} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & 0 & \cdots & 0 \end{pmatrix},$$

又 $\text{rank}(\mathbf{C})=1$, 故 $b_{21}, \dots, b_{m1} \in \mathbb{F}_q$ 且不全为 0。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 $q^{m-1}-1$ 。

故, $Q_{1,1,1} = q^m + q^n - q - 1$ 。

(2) 设 $\mathbf{C} = \mathbf{B} - \mathbf{E}_2$ 。

若 $\text{rank}(\mathbf{C})=0$, 则 $\mathbf{B} = \mathbf{E}_2$, 从而 $\text{rank}(\mathbf{B})=2$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 0。

下面讨论 $\text{rank}(\mathbf{C})=1$ 的情况。假设 $\mathbf{C}$ 的第 $i_1, i_2, \dots, i_h$ 行是非零行向量, 设

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}, \text{ 则 } \mathbf{C} = \mathbf{B} - \mathbf{E}_2 = \begin{pmatrix} b_{11}-1 & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22}-1 & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}。$$

(2.1) 当 $i_1 > 2$ 时, 此时

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix},$$

从而 $\text{rank}(\mathbf{B}) \geq 2$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 0。

(2.2) 当 $h > 2$, $i_1 = 1$ 且 $i_2 = 2$ 时, 记 $i = 1, 2, \dots, m-2$, 不妨设

$$(b_{21}, b_{22}-1, \dots, b_{2n}) = k_1(b_{11}-1, b_{12}, \dots, b_{1n}),$$

$$(b_{i+2,1}, b_{i+2,2}, \dots, b_{i+2,n}) = k_{i+1}(b_{11}-1, b_{12}, \dots, b_{1n}),$$

其中 $k_1, k_2, \dots, k_{m-1} \in \mathbb{F}_q$, $k_1 \neq 0$ 且 $k_2, \dots, k_{m-1}$ 不全为 0, 我们有

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix} \rightarrow \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ -k_1 & 1 & \cdots & 0 \\ -k_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -k_{m-1} & 0 & \cdots & 0 \end{pmatrix},$$

从而 $\text{rank}(\mathbf{B}) \geq 2$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 0。

(2.3) 当 $h=1$ 且 $i_1=1$ 时, 我们有

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

其中 $b_{11}=b_{13}=\dots=b_{1n}=0$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 q 。

(2.4) 当 $h \geq 2$, $i_1=1$ 且 $i_2 > 2$ 时, 我们有

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ b_{i_2 1} & b_{i_2 2} & \cdots & b_{i_2 n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix},$$

要使 $\text{rank}(\mathbf{B})=1$, 记 $r=2,3,\dots,h$, 则有

$$b_{11}=b_{13}=\dots=b_{1n}=0,$$

$$b_{i_r,1}=b_{i_r,3}=\dots=b_{i_r,n}=0,$$

此时 $\text{rank}(\mathbf{C})=2$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 0。

(2.5) 当 $h=1$ 且 $i_1=2$ 时, 我们有

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ b_{21} & b_{22} & \cdots & b_{2n} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

其中 $b_{22}=b_{23}=\dots=b_{2n}=0$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 q 。

(2.6) 当 $h>1$ 且 $i_1=2$ 时, 我们有

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ b_{21} & b_{22} & \cdots & b_{2n} \\ b_{31} & b_{32} & \cdots & b_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & \cdots & 0 \\ b_{21} & b_{22} & \cdots & b_{2n} \\ b_{i_2,1} & b_{i_2,2} & \cdots & b_{i_2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

要使 $\text{rank}(\mathbf{B})=1$, 记 $r=2,3,\dots,h$, 则有

$$b_{22}=b_{23}=\dots=b_{2n}=0,$$

$$b_{i_r,2}=b_{i_r,3}=\dots=b_{i_r,n}=0,$$

此时 $\text{rank}(\mathbf{C})=2$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 0。

(2.7) 当 $h=2$, $i_1=1$ 且 $i_2=2$ 时, 我们有

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & 0 \\ b_{21} & b_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \quad \mathbf{C} = \begin{pmatrix} b_{11}-1 & b_{12} & \cdots & 0 \\ b_{21} & b_{22}-1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

由于 $\text{rank}(\mathbf{B})=1$, $\text{rank}(\mathbf{C})=1$, 则有 $(b_{11}-1)(b_{22}-1)=b_{12}b_{21}$ 且 $b_{11}b_{22}=b_{12}b_{21}$, 从而 $b_{11}+b_{22}=1$, 我们设 $(b_{21}, b_{22}-1)=k_1(b_{11}-1, b_{12}) (k_1 \neq 0)$, 则有

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & 0 & \cdots & 0 \\ b_{21} & b_{22} & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \rightarrow \begin{pmatrix} b_{11} & b_{12} & 0 & \cdots & 0 \\ -k_1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

由于 $\text{rank}(\mathbf{B})=1$, 则 $b_{11}=-k_1b_{12} (k_1 \neq 0)$ 。

(2.7.1) 若 $b_{12}=0$, 则 $b_{11}=0$, 从而 $b_{22}=1$ 。我们有

$$\mathbf{B} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ b_{21} & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \quad \mathbf{C} = \begin{pmatrix} -1 & 0 & \cdots & 0 \\ b_{21} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 $q-1$ 。

(2.7.2) 若 $b_{12} \neq 0$, 则 $b_{11} \neq 0$ 。根据 $b_{11} = -k_1 b_{12} (k_1 \neq 0)$, k_1 可取 $\mathbb{F}_q$ 中任意非零值, b_{12} 亦可取 $\mathbb{F}_q$ 中任意非零值。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 $(q-1)^2$ 。

故, $Q_{1,2,1} = q^2 + q$ 。

(3) 设 $\mathbf{C} = \mathbf{B} - \mathbf{E}_1$ 。

若 $\text{rank}(\mathbf{C}) = 0$, 则 $\mathbf{B} = \mathbf{E}_1$, 从而 $\text{rank}(\mathbf{B}) = 1$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 0。

下面讨论 $\text{rank}(\mathbf{C}) = 1$ 的情况。假设 $\mathbf{C}$ 的第 $i_1, i_2, \dots, i_h$ 行是非零行向量, 设

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}, \quad \text{则 } \mathbf{C} = \begin{pmatrix} b_{11}-1 & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}。$$

(3.1) 当 $h=1$ 且 $i_1=1$ 时, 我们有

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

其中 $(b_{11}, b_{12}, \dots, b_{1n}) \in \mathbb{F}_q^n \setminus \{(1, 0, \dots, 0)\}$, 则此时 $\text{rank}(\mathbf{B}) \leq 1$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 0。

(3.2) 当 $h > 1$ 且 $i_1=1$ 时, 记 $i=1, 2, \dots, m-1$, 可设

$$(b_{i+1,1}, b_{i+1,2}, \dots, b_{i+1,n}) = k_i (b_{11}-1, b_{12}, \dots, b_{1n}),$$

其中 $k_1, k_2, \dots, k_{m-1} \in \mathbb{F}_q$ 且不全为 0。我们有

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix} \rightarrow \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ -k_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -k_{m-1} & 0 & \cdots & 0 \end{pmatrix},$$

其中 $(b_{12}, \dots, b_{1n}) \in \mathbb{F}_q^{n-1} \setminus \{(0, 0, \dots, 0)\}$, b_{11} 可取 $\mathbb{F}_q$ 中任意值。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 $q(q^{n-1}-1)(q^{m-1}-1)$ 。

(3.3) 当 $i_1 > 1$ 时,

由于 $\text{rank}(\mathbf{C}) = 1$, 从而 $(b_{i_1}, b_{i_2}, \dots, b_{i_n})$ 是非零行向量, 即 $(b_{i_1}, b_{i_2}, \dots, b_{i_n}) \in \mathbb{F}_q^n \setminus \{(0, 0, \dots, 0)\}$, 我们有

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & \cdots & 0 \\ b_{i_1} & b_{i_2} & \cdots & b_{i_n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

由于 $\text{rank}(\mathbf{B})=2$, 则 $(b_{i_2}, \dots, b_{i_n}) \in \mathbb{F}_q^{n-1} \setminus \{(0, 0, \dots, 0)\}$, 此时对任意的 $\{i_1, i_2, \dots, i_h\} \subset \{2, 3, \dots, m\}$, 在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 $\frac{q(q^{n-1}-1)(q^{m-1}-1)}{q-1}$ 。

$$\text{故, } Q_{2,1,1} = \frac{(q^n - q)(q^m - q)}{q-1}.$$

(4) 设 $\mathbf{C} = \mathbf{B} - \mathbf{E}_2$ 。

若 $\text{rank}(\mathbf{C})=0$, 则 $\mathbf{B} = \mathbf{E}_2$, 满足要求 $\text{rank}(\mathbf{B})=2$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 1。

下面讨论 $\text{rank}(\mathbf{C})=1$ 的情况。假设 $\mathbf{C}$ 的第 $i_1, i_2, \dots, i_h$ 行是非零行向量, 设

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}, \text{ 则 } \mathbf{C} = \mathbf{B} - \mathbf{E}_2 = \begin{pmatrix} b_{11}-1 & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22}-1 & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}.$$

(4.1) 当 $h=1$ 且 $i_1=1$ 时, 我们有

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

其中 $(b_{11}, b_{12}, \dots, b_{1n}) \in \mathbb{F}_q^n \setminus \{(1, 0, \dots, 0)\}$ 且 $(b_{11}, b_{13}, \dots, b_{1n}) \in \mathbb{F}_q^{n-1} \setminus \{(0, 0, \dots, 0)\}$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 $q^n - q - 1$ 。

(4.2) 当 $h=1$ 且 $i_1=2$ 时, 我们有

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

与(4.1)同理, 在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 $q^n - q - 1$ 。

(4.3) 当 $i_1 > 2$ 时, 我们有

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ b_{31} & b_{32} & \cdots & b_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ b_{i_1 1} & b_{i_1 2} & \cdots & b_{i_1 n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

其中 $b_{i_1 1}, b_{i_1 2}$ 不全为 0, $b_{i_1 3} = \dots = b_{i_1 n} = 0$, 由于对任意的 $\{i_1, i_2, \dots, i_h\} \subset \{3, 4, \dots, m\}$, 则在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 $q^{m-1} + q^{m-2} - q - 1$ 。

(4.4) 当 $h > 1$, $i_1=1$ 且 $i_2 > 2$ 时, 记 $i=1, 2, \dots, m-2$, 不妨设

$$(b_{i+2,1}, b_{i+2,2}, \dots, b_{i+2,n}) = k_i (b_{11}-1, b_{12}, \dots, b_{1n}),$$

其中 $k_1, k_2, \dots, k_{m-2} \in \mathbb{F}_q$ 且不全为 0。我们有,

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ 0 & 1 & \cdots & 0 \\ b_{31} & b_{32} & \cdots & b_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix} \rightarrow \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ 0 & 1 & \cdots & 0 \\ -k_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -k_{m-1} & 0 & \cdots & 0 \end{pmatrix},$$

其中 $b_{11}-1$, b_{12} 不全为 0 且 $b_{13}=\cdots=b_{1n}=0$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 $q^m - q^{m-2} - q^2 + 1$ 。

(4.5) 当 $h>1$ 且 $i_1=2$ 时, 我们有

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix},$$

与(4.4)同理, 在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 $q^m - q^{m-2} - q^2 + 1$ 。

(4.6) 当 $h>2$, $i_1=1$ 且 $i_2=2$ 时, 记 $i=2, \cdots, m-1$, 不妨设

$$(b_{21}, b_{22}-1, \cdots, b_{2n}) = l_1(b_{11}-1, b_{12}, \cdots, b_{1n}),$$

$$(b_{i+1,1}, b_{i+1,2}, \cdots, b_{i+1,n}) = l_i(b_{11}-1, b_{12}, \cdots, b_{1n}),$$

其中 $l_1 \in \mathbb{F}_q$, $l_1 \neq 0$, $l_2, \cdots, l_{m-1} \in \mathbb{F}_q$ 且不全为 0。

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix} \rightarrow \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ -l_1 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -l_{m-1} & 0 & \cdots & 0 \end{pmatrix},$$

从而 $b_{11}-1, b_{12}$ 不全为 0 且 $b_{13}=\cdots=b_{1n}=0$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 $(q^2-1)(q-1)(q^{m-2}-1)$ 。

(4.7) 当 $h=2$, $i_1=1$ 且 $i_2=2$ 时, 我们有

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

其中 $(b_{11}, b_{12}, \cdots, b_{1n}) \in \mathbb{F}_q^n \setminus \{(1, 0, \cdots, 0)\}$ 且 $(b_{21}, b_{22}, \cdots, b_{2n}) \in \mathbb{F}_q^n \setminus \{(0, 1, \cdots, 0)\}$,

由于 $\text{rank}(\mathbf{C})=1$, 不妨设

$$(b_{21}, b_{22}-1, \cdots, b_{2n}) = l'_1(b_{11}-1, b_{12}, \cdots, b_{1n}),$$

其中 $l'_1 \in \mathbb{F}_q$ 且 $l'_1 \neq 0$ 。我们有

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \rightarrow \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ -l'_1 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

(4.7.1) 当 $(b_{13}, \cdots, b_{1n}) \in \mathbb{F}_q^{n-2} \setminus \{(0, 0, \cdots, 0)\}$ 时, b_{11}, b_{12} 可取 $\mathbb{F}_q$ 中任意值, 且 $l'_1 \neq 0$ 。在这种情况下, 满

足条件的 $\mathbf{B}$ 的个数为 $(q-1)(q^{n-2}-1)q^2$ 。

(4.7.2) 当 $b_{13}=\cdots=b_{1n}=0$ 时, 此时 $b_{11}=1$, b_{12} 不全为 0, $l'_1 \neq 0$ 且 $b_{11}+l'_1 b_{12} \neq 0$ 。在这种情况下, 满足条件的 $\mathbf{B}$ 的个数为 $(q-1)(q^2-q-1)$ 。

故, $Q_{2,2,1} = q^{m+1} + q^{n+1} + q^m + q^n - q^3 - 2q^2 - 2q$ 。

证毕。

推论 3.2:

$$A_q^R(n \times n, 3, [1, 2]) \leq g$$

其中

$$\begin{aligned} \max : g &= x_1 + x_2 ; \\ \begin{cases} Q_{1,1,1}x_1 + Q_{1,2,1}x_2 \leq P_1^{n \times n} = \frac{(q^n-1)^2}{q-1}; \\ Q_{2,1,1}x_1 + Q_{2,2,1}x_2 \leq P_2^{n \times n} = \sum_{1 \leq i < j \leq n} q^{2n-i-j} (q^n-1)(q^{n-1}-1); \\ x_1 \geq 0, x_2 \geq 0, x_1, x_2 \in \mathbb{Z}. \end{cases} \\ Q_{1,1,1} &= q^m + q^n - q - 1; \quad Q_{1,2,1} = q^2 + q; \\ Q_{2,1,1} &= \frac{(q^n-q)(q^m-q)}{q-1}; \\ Q_{2,2,1} &= q^{m+1} + q^{n+1} + q^m + q^n - q^3 - 2q^2 - 2q. \end{aligned}$$

证明 利用命题 2.3 和定理 3.1, 当 $m=n$, $r_1=1$, $r_2=2$ 且 $d_R=3$, 我们即可得到结果。

4. 结语

本文通过计算当 q 是任意素数幂时, 相关参数 $Q_{1,1,1}$, $Q_{1,2,1}$, $Q_{2,1,1}$, $Q_{2,2,1}$ 的值, 得到参数为 $(n \times n, 3, [1, 2])_q$ 定秩集秩度量码的球填充上界, 对 Liu 等人的结论做了进一步的推广, 但是对于一般的 $Q_{i,j,l}$ ($i, j, l \geq 3$), 其值仍然是未知的。

基金项目

江苏省大学生创新创业项目(202310332089Y)。

参考文献

- [1] Ahlswede, R., Cai, N., Li, S.-R. and Yeung, R.W. (2000) Network Information Flow. *IEEE Transactions on Information Theory*, **46**, 1204-1216. <https://doi.org/10.1109/18.850663>
- [2] Koetter, R. and Kschischang, F.R. (2008) Coding for Errors and Erasures in Random Network Coding. *IEEE Transactions on Information Theory*, **54**, 3579-3591. <https://doi.org/10.1109/tit.2008.926449>
- [3] Silva, D., Kschischang, F.R. and Koetter, R. (2008) A Rank-Metric Approach to Error Control in Random Network Coding. *IEEE Transactions on Information Theory*, **54**, 3951-3967. <https://doi.org/10.1109/tit.2008.928291>
- [4] Xu, L. and Chen, H. (2018) New Constant-Dimension Subspace Codes from Maximum Rank Distance Codes. *IEEE Transactions on Information Theory*, **64**, 6315-6319. <https://doi.org/10.1109/tit.2018.2839596>
- [5] Liu, S., Chang, Y. and Feng, T. (2020) Parallel Multilevel Constructions for Constant Dimension Codes. *IEEE Transactions on Information Theory*, **66**, 6884-6897. <https://doi.org/10.1109/tit.2020.3004315>
- [6] Etzion, T. and Silberstein, N. (2009) Error-Correcting Codes in Projective Spaces via Rank-Metric Codes and Ferrers Diagrams. *IEEE Transactions on Information Theory*, **55**, 2909-2919. <https://doi.org/10.1109/tit.2009.2021376>

- [7] Trautmann, A.-L. and Rosenthal, J. (2010) New Improvements on the Echelon-Ferrers Construction. *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems*, Budapest, 5-9 July 2010, 405-408.
- [8] Ahlswede, R. and Aydinian, H. (2009) On Error Control Codes for Random Network Coding. *2009 Workshop on Network Coding, Theory, and Applications*, Lausanne, 15-16 June 2009, 68-73. <https://doi.org/10.1109/netcod.2009.5191396>
- [9] Xia, S. and Fu, F. (2008) Johnson Type Bounds on Constant Dimension Codes. *Designs, Codes and Cryptography*, **50**, 163-172. <https://doi.org/10.1007/s10623-008-9221-7>
- [10] 刘双庆. 子空间码的组合和代数构造方法[D]: [博士学位论文]. 北京: 北京交通大学, 2020.
- [11] Delsarte, P. (1978) Bilinear Forms over a Finite Field, with Applications to Coding Theory. *Journal of Combinatorial Theory, Series A*, **25**, 226-241. [https://doi.org/10.1016/0097-3165\(78\)90015-8](https://doi.org/10.1016/0097-3165(78)90015-8)
- [12] Gabidulin, È.M. (1985) Theory of Codes with Maximum Rank Distance. *Problems of Information Transmission*, **21**, 3-16.
- [13] Roth, R.M. (1991) Maximum-rank Array Codes and Their Application to Crisscross Error Correction. *IEEE Transactions on Information Theory*, **37**, 328-336. <https://doi.org/10.1109/18.75248>
- [14] Gluesing-Luerssen, H. and Ravagnani, A. (2020) Partitions of Matrix Spaces with an Application to q -Rook Polynomials. *European Journal of Combinatorics*, **89**, Article 103120. <https://doi.org/10.1016/j.ejc.2020.103120>