

定秩集秩度量码的Singleton型上界

刘翊文¹, 陈炫燃¹, 宋谭夕¹, 朱博华²

¹苏州科技大学数学科学学院, 江苏 苏州

²石家庄铁道大学数理系, 河北 石家庄

收稿日期: 2026年1月10日; 录用日期: 2026年2月4日; 发布日期: 2026年2月12日

摘 要

为了推动网络编码实用化, 2006年Médard等人提出随机网络编码概念, 2008年Kschischang等人针对错误纠正与数据恢复需求, 提出子空间码模型, 而定秩集秩度量码是用来构造子空间码的一类辅助码。我们的研究围绕网络编码范畴展开, 主要针对常维码与定秩集秩度量码这两类核心研究对象。在网络编码基本原理的基础上, 本文系统地研究了定秩集秩度量码的代数性质, 给出了定秩集秩度量码的Singleton界, 证明了定秩集秩度量码的渐近最优性。

关键词

常维码, 定秩集秩度量码, 子空间码

Singleton Upper Bound of Rank Metric Codes with Given Ranks

Yiwen Liu¹, Xuanran Chen¹, Tanxi Song¹, Bohua Zhu²

¹School of Mathematical Sciences, Suzhou University of Science and Technology, Suzhou Jiangsu

²Department of Mathematics, Shijiazhuang Tiedao University, Shijiazhuang Hebei

Received: January 10, 2026; accepted: February 4, 2026; published: February 12, 2026

Abstract

To promote the practical application of network coding, Médard *et al.* proposed the concept of random network coding in 2006. In 2008, to address the requirements of error correction and data recovery, Kschischang *et al.* put forward the subspace code model, where rank metric codes with given ranks serve as a class of auxiliary codes for constructing subspace codes. Our research focuses on the field of network coding, with its primary focus on two core research objects: constant dimension codes and rank metric codes with given ranks. Based on the fundamental principles of network

coding, this paper systematically investigates the algebraic properties of rank metric codes with given ranks, derives the Singleton upper bound for such codes, and proves their asymptotic optimality.

Keywords

Constant Dimension Codes, Rank Metric Codes with Given Ranks, Subspace Codes

Copyright © 2026 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

网络编码[1]是在网络中进行信息传播时在中间节点进行编码的技术。为了提高通信性能,中间节点应该转发它们接收到的数据包的随机线性组合。因此,当没有错误发生时,其数据包所张成的向量空间是全局不变的。因为线性组合下的线性空间是不变的,所以它们正好是解码所需的码字[2]。本文考虑所有子空间的维数都是一致的,也就是常维码(CDCs)。

设 Grassmann 空间 $G_q(n, k)$ 表示 F_q^n 中所有维度为 k 的子空间的集合。众所周知, Grassmann 空间 $G_q(n, k)$ 的基数由 q 元高斯系数给出:

$$|G_q(n, k)| = \begin{bmatrix} n \\ k \end{bmatrix}_q \triangleq \prod_{i=0}^{k-1} \frac{q^{n-i} - 1}{q^{k-i} - 1}.$$

一个参数为 (n, M, d, k) 的常维码 C 是 $G_q(n, k)$ 的一个子集,满足对于任意两个子空间 $U, V \in C$, 子空间距离为:

$$d_l(U, V) = \max\{\dim U, \dim V\} - \dim(U \cap V) \geq d.$$

其中 $U, V \in F_q^{k \times n}$ 是矩阵, 满足 $U = \text{rowspace}(U)$ 且 $V = \text{rowspace}(V)$ 。

令 $A_q(n, d, k)$ 表示 (n, M, d, k) 常维码 C 的最大可能个数。由于 $A_q(n, d, k) = A_q(n, d, n-k)$ (见文献[3]), 在不损失一般性的情况下, 我们总是假设 $n \geq 2k$ 。 F_q^n 的一个 k 维子空间 U 可以由一个 $k \times n$ 的生成矩阵表示, 该矩阵的行构成 U 的一个基。如果 $U, V \in G_q(n, k)$, 那 $G_q(n, k)$ 上的子空间距离也可以表示为:

$$d_s(U, V) = 2\text{rank}\begin{pmatrix} U \\ V \end{pmatrix} - 2k.$$

这两个矩阵通常不是唯一的。实际上, 人们可以注意到, 对于任何 $A \in GL_k(F_q)$, $U = \text{rowspace}(AU)$ 。然而, Grassmann 流形元素存在唯一的矩阵表示, 即行简化阶梯形。一个秩为 k 的 $k \times n$ 矩阵是行简化阶梯形, 如果:

- 1) 一行的前导系数在该行中位于前一行前导系数的右侧;
- 2) 所有前导系数都是 1;
- 3) 每个前导系数都是其所在列中唯一的非零元素。

为了获得最优的常维码, Silva、Kschischang 和 Kötter 在文献[4]中指出, 最大秩距离码(MRDs)可以导致渐近最优的 CDCs [2] [3], 并且在随机线性网络编码的背景下可以高效解码。许丽卿等学者[5]和刘双庆等学者[6]选择定秩集秩度量码这种新的辅助码, 将其运用于子空间码的构造实践中。对于子空间码的

更多构造和界的相关信息,感兴趣的读者可以参考文献[2] [3] [6]-[18]。

本文系统研究了文献[6]中引入的定秩集秩度量码,并给出了定秩集秩度量码的 Singleton 界,证明了定秩集秩度量码的渐近最优性。我们还建立了定秩集秩度量码和子空间码之间的联系。

2. 预备知识

令 q 是一个素数幂, F_q 表示 q 阶有限域, $F_q^{m \times n}$ 表示 F_q 上所有尺寸为 $m \times n$ 的矩阵的集合。对于矩阵 $A \in F_q^{m \times n}$, 用 $\text{rank}(A)$ 表示 A 的秩。

定义 2.1:

$[m, n]$: 表示大于等于 m 并且小于等于 n 的连续整数。

定义 2.2:

对于矩阵 $A, B \in F_q^{m \times n}$, 它们的秩距离定义如下:

$$d_R(A, B) = \text{rank}(A - B),$$

并且秩分布已经确定。

定义 2.3 [19]:

$[m \times n, k, \delta]_q$ - 秩度量码 C 是 $F_q^{m \times n}$ 上的 k 维线性子空间, 且满足最小秩距离 $\geq \delta$ 。

对于 $[m \times n, k, \delta]_q$ - 秩度量码, 它的 Singleton 型上界为:

$$k \leq m(n - \delta + 1),$$

当等号成立时, 称为最大秩度量(MRD)码, 记为 $\text{MRD}[m \times n, \delta]_q$ 码。Delsarte [20] (1978)和 Gabidulin [21] (1985)分别证明了任何参数的最大秩度量码都是存在的。

定理 2.4: (最大秩度量码的秩分布[20] [21])

对于任意的 $\text{MRD}[m \times n, \delta]_q$ 码, 其秩分布由以下式子给出: $A_0 = 1$, 当 $1 \leq i \leq \delta - 1$ 时, $A_i = 0$, 并且有

$$A_{\delta+i} = \begin{bmatrix} n \\ \delta+i \end{bmatrix}_q \sum_{j=0}^i (-1)^{j-i} \begin{bmatrix} \delta+i \\ i-j \end{bmatrix}_q q^{\binom{i-j}{2}} (q^{m(j+1)} - 1),$$

其中 $0 \leq i \leq n - \delta$ 。

进一步, 对码字的秩进行限制, 则得到了定秩集秩度量码。

定义 2.5:

对于 $K \subseteq \{0, 1, \dots, n-1\}$, $C \subseteq F_q^{m \times n}$ 是一个参数为 $(m \times n, \delta, K)_q$ - 定秩集秩度量码, 如果 C 满足

1) 对于任意的 $C \in C$, $\text{rank}(C) \in K$;

2) 对于任意的 $C_1, C_2 \in C$, 且 $C_1 \neq C_2$, 有 $d_R(C_1, C_2) \geq \delta$ 。

如果 $|C| = M$, 则一个参数为 $(m \times n, \delta, K)_q$ - 定秩集秩度量码可以表示为 $(m \times n, M, \delta, K)_q$ - 定秩集秩度量码。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 $(m \times n, \delta, K)_q$ - 定秩集秩度量码中码字个数的最大值。最近, 季利均等人给出了定秩集秩度量码的球填充上界。

3. 定秩集秩度量码(GRMCs)的 Singleton 界

本章主要研究定秩集秩度量码的 Singleton 型上界, 并且证明出当参数满足 $m \geq n \geq \dots \geq r \geq d_R > 1$ 时, $(m \times n, M, d, [r, \dots, n])_q$ 定秩集秩度量码的渐进性是最优的。进一步, 对一类特殊的定秩集秩度量码进行研究, 即 $(n \times n, M, n-2, \{n-1, n\})_q$ - 定秩集秩度量码, 并展示了其上、下界的比。已有文献中定秩集秩度量码的球填充界需依赖于对集合 $\{B \in \mathbb{F}_q^{m \times n} : \text{rank}(B) = i \text{ 且 } \text{rank}(B - E_j) \leq l\}$ 的估计, 目前学界尚未形成对该

集合的有效估计方法, 导致球填充界难以给出显式表达, 而本文提出的 Singleton 界是显式的表达式, 且对于部分类别的定秩集秩度量码而言, 该界能够达到渐近最优。

引理 3.1 (定理 8 [12]):

当 $m \geq n \geq r \geq d_R > 1$ 时,

$$A_R(m \times n, d_R, r) \leq \begin{bmatrix} n \\ r \end{bmatrix}_q \cdot \alpha(m, r - d_R + 1)。$$

其中 $\alpha(m, i) = \prod_{j=0}^{i-1} (q^m - q^j)$ 。

定理 3.2 (定秩集秩度量码的 Singleton 界):

当 $m \geq n \geq r \geq d_R > 1$ 时,

$$A_q^R(m \times n, d_R, [r, n]) \leq \sum_{i=r-d_R+1}^{n-d_R+1} \begin{bmatrix} n-d_R+1 \\ i \end{bmatrix}_q \alpha(m, i)。$$

证明 设 C 是任意一个 $(m \times n, M, d_R, [r, n])_q$ -定秩集秩度量码。考虑通过对 C 中的所有码字任意删除 $d_R - 1$ 列得到的码 C' 。此时 C' 是一个 $(m \times (n - d_R + 1), M, 1, [r - d_R + 1, n - d_R + 1])_q$ -定秩集秩度量码。

将 C' 分解为不同秩的码字集合 $C' = \sum_{i=r-d_R+1}^{n-d_R+1} C'_i$, C'_i 表示 C' 中秩为 i 的所有码字。由上述引理,

$$|C'_i| \leq \begin{bmatrix} n-d_R+1 \\ i \end{bmatrix}_q \alpha(m, i)。$$

因此,

$$|C| = |C'| \leq \sum_{i=r-d_R+1}^{n-d_R+1} \begin{bmatrix} n-d_R+1 \\ i \end{bmatrix}_q \alpha(m, i)。$$

证毕。

推论 3.3:

当 $m \geq n \geq r \geq d_R > 1$ 时, 存在 $(m \times n, M, d_R, [r, n])_q$ -定秩集秩度量码, 使

$$\lim_{q \rightarrow \infty} \frac{M}{\sum_{i=r-d_R+1}^{n-d_R+1} \begin{bmatrix} n-d_R+1 \\ i \end{bmatrix}_q \cdot \alpha(m, i)} = 1。$$

证明 设 $C = \bigcup_{i=r}^n C_i$, C_i 表示一个 $\text{MRD}[m \times n, d_R]_q$ 码中秩为 i 的所有码字。根据定理 2.3, 有 $|C| = \sum_{i=1}^n A_i$ 。考虑 $A_n = \sum_{j=0}^{n-d_R} (-1)^{i-n+d_R} \begin{bmatrix} n \\ n-d_R-j \end{bmatrix}_q q^{\binom{n-d_R-j}{2}} (q^{m(j+1)} - 1)$ 。

设 $f_j(q) = \begin{bmatrix} n \\ n-d_R-j \end{bmatrix}_q q^{\binom{n-d_R-j}{2}} (q^{m(j+1)} - 1)$, 则

$$\begin{aligned} \deg(f_j(q)) &= (n-d_R-j)(d_R+j) + \frac{(n-d_R-j)(n-d_R-j-1)}{2} + m(j+1) \\ &= -\frac{1}{2}j^2 + \left(m-d_R + \frac{1}{2}\right)j + \frac{(n-d_R)(n+d_R-1)+2m}{2} \end{aligned}$$

对于 $0 \leq j \leq m-d_R + \frac{1}{2}$, $\deg(f_j(q))$ 是 j 的增函数, 并且

$$\deg(f_{n-d_R-1}(q)) = m(n-d_R+1)。$$

令 $|C| = q^{m(n-d_R+1)} - h_1(q)$ ，其中 $\deg(h_1(q)) < m(n-d_R+1)$ 且 $h_1(q) > 0$ 。根据定理 3.2，有

$$A_q^R(m \times n, d_R, [r, n]) \leq \sum_{i=r-d_R+1}^{n-d_R+1} \begin{bmatrix} n-d_R+1 \\ i \end{bmatrix}_q \cdot \alpha(m, i)。$$

设 $g_i(q) = \begin{bmatrix} n-d_R+1 \\ j \end{bmatrix}_q \alpha(m, j)$ ，则

$$\deg(g_j(q)) = (n-d_R+1-j) \cdot j + mj = -j^2 + (m+n-d_R+1)j。$$

由于当 j 为主元时， $\deg(f_j(q))$ 在 $j \leq \frac{m+n-d_R+1}{2}$ 时是增函数，所以对于 $r-d_R+1 \leq j \leq n-d_R+1$ ，

$$\deg(g_{n-d_R+1}(q)) = m(n-d_R+1)。$$

可得

$$\sum_{i=r-d_R+1}^{n-d_R+1} \begin{bmatrix} n-d_R+1 \\ j \end{bmatrix}_q \alpha(m, j) = q^{m(n-d_R+1)} - h_2(q)，$$

其中 $\deg(h_2(q)) < m(n-d_R+1)$ 且 $h_2(q) > 0$ 。

因此，

$$\lim_{q \rightarrow \infty} \frac{M}{\sum_{i=r-d_R+1}^{n-d_R+1} \begin{bmatrix} n-d_R+1 \\ i \end{bmatrix}_q \cdot \alpha(m, i)} = \lim_{q \rightarrow \infty} \frac{q^{m(n-d_R+1)} - h_1(q)}{q^{m(n-d_R+1)} - h_2(q)} = 1。$$

证毕。

推论 3.4:

对于任意 $(n \times n, A_{n-1} + A_n, n-2, \{n-1, n\})_q$ -定秩集秩度量码，其中 A_i 表示在 $\text{MRD}[n \times n, n-2]_q$ 码中秩为 i 的码字个数，有

$$\frac{|C|}{\sum_{i=2}^3 \begin{bmatrix} 3 \\ i \end{bmatrix}_q \cdot \alpha(n, i)} > 0.83。$$

证明 根据定理 2.3，可知

$$A_n = \frac{(q^n-1)(q^{n-1}-1)}{(q^2-1)(q-1)} \cdot q \cdot (q^n-1) - \frac{q^n-1}{q-1} (q^{2n}-1) + q^{3n}-1，$$

$$A_{n-1} = \frac{q^n-1}{q-1} \cdot \left(-\frac{(q^{n-1}-1)(q^n-1)}{q-1} + q^{2n}-1 \right)。$$

根据定理 3.2 中 GRMCs 中的 Singleton 界，有

$$\sum_{i=2}^3 \begin{bmatrix} 3 \\ i \end{bmatrix}_q \cdot 2 \cdot (n, i) = q^{3n} - q^{n+2} - q^{n+1} - q^n + q^2 + q。$$

由于 $|C| = A_{n-1} + A_n$ ，所以

$$\begin{aligned}
\frac{|C|}{\sum_{i=2}^3 \begin{bmatrix} 3 \\ i \end{bmatrix}_q \cdot \alpha(n, i)} &= \frac{A_{n-1} + A_n}{\sum_{i=2}^3 \begin{bmatrix} 3 \\ i \end{bmatrix}_q \cdot \alpha(n, i)} \\
&= \frac{q^{3n+3} - q^{3n+2} - q^{3n+1} + q^{3n} - q^{3n-1} - q^n + 2q_l^{2n-1} - q^{n-1} + q^3 + q^2 + q}{q^{3n+3} - q^{3n+2} - q^{3n+1} + q^{3n} - q^{n+5} + q^{n+3} + q^{n+2} - q^n + q^5 - 2q^3 + q} \\
&= 1 - \frac{q^{3n-1} - q^{2n} - 2q^{2n-1} - q^{n+5} + q^{n+3} + q^{n+2} + q^n + q^{n-1} + q^5 - q^3 - q}{q^{3n+3} - q^{3n+2} - q^{3n+1} + q^{3n} - q_l^{n+5} + q^{n+3} + q^{n+2} - q^n + q^5 - 2q^3 + q} \\
&\geq 1 - \frac{q^{3n-1}}{q^{3n+3} - q^{3n+2} - q^{3n+1} + q^{3n}} = 1 - \frac{1}{q^4 - q^3 - q^2 + q}
\end{aligned}$$

设函数 $f(q) = 1 - \frac{1}{q^4 - q^3 - q^2 + q}$, 根据链式法则, 对 $f(q)$ 求导, 得到

$$f'(q) = \frac{4q^3 - 3q^2 - 2q + 1}{(q^4 - q^3 - q^2 + q)^2}.$$

令

$$D(q) = 4q^3 - 3q^2 - 2q + 1, \quad D'(q) = 12q^2 - 6q - 2,$$

对于 $q \in [2, +\infty)$, $D'(q) \geq 0$, 则 $D(q)$ 单调递增, 即 $D(q) \geq D(2) = 17$ 。可知 $f'(q) > 0$, 即 $f(q)$ 在 $[2, +\infty)$ 上单调递增。

所以当 $q = 2$ 时, 可知

$$1 - \frac{1}{q^4 - q^3 - q^2 + q} > 0.83.$$

因此,

$$\frac{|C|}{\sum_{i=2}^3 \begin{bmatrix} 3 \\ i \end{bmatrix}_q \cdot \alpha(n, i)} > 0.83.$$

证毕。

4. 结语

尽管定秩集秩度量码在常维码的构造中扮演着不可或缺的角色, 但其渐近最优性问题还未完全解决。在现有的研究成果中, 仅经典 MRD 码与部分特殊常秩码的最优性得到了验证, 其余定秩集秩度量码的最优性则仍有待进一步探究。

基金项目

江苏省大学生创新创业项目(202410332137Y)。

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] Etzion, T. and Vardy, A. (2011) Error-Correcting Codes in Projective Space. *IEEE Transactions on Information Theory*, **57**, 1165-1173. <https://doi.org/10.1109/tit.2010.2095232>
- [4] 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>
- [5] 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>
- [6] 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>
- [7] 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>
- [8] Delsarte, P. (1973) An Algebraic Approach to the Association Schemes of Coding Theory. Ph.D. Thesis, Philips Research Laboratories.
- [9] 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>
- [10] Etzion, T. and Silberstein, N. (2013) Codes and Designs Related to Lifted MRD Codes. *IEEE Transactions on Information Theory*, **59**, 1004-1017. <https://doi.org/10.1109/tit.2012.2220119>
- [11] Frankl, P. and Wilson, R.M. (1986) The Erdős-Ko-Rado Theorem for Vector Spaces. *Journal of Combinatorial Theory, Series A*, **43**, 228-236. [https://doi.org/10.1016/0097-3165\(86\)90063-4](https://doi.org/10.1016/0097-3165(86)90063-4)
- [12] Gadouleau, M. and Yan, Z. (2010) Constant-Rank Codes and Their Connection to Constant-Dimension Codes. *IEEE Transactions on Information Theory*, **56**, 3207-3216. <https://doi.org/10.1109/tit.2010.2048447>
- [13] Heinlein, D., Kiermaier, M., Kurz, S. and Wassermann, A. (2016) Tables of Subspace Codes. arXiv: 1601.02864v2.
- [14] Liu, S. and Ji, L. (2023) Double Multilevel Constructions for Constant Dimension Codes. *IEEE Transactions on Information Theory*, **69**, 157-168. <https://doi.org/10.1109/tit.2022.3200052>
- [15] Silberstein, N. and Etzion, T. (2011) Enumerative Coding for Grassmannian Space. *IEEE Transactions on Information Theory*, **57**, 365-374. <https://doi.org/10.1109/tit.2010.2090252>
- [16] 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.
- [17] 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>
- [18] Yu, S., Ji, L. and Liu, S. (2022) Bilateral Multilevel Construction of Constant Dimension Codes. *Advances in Mathematics of Communications*, **16**, 1165-1183. <https://doi.org/10.3934/amc.2022056>
- [19] 刘双庆. 子空间码的组合和代数结构方法[D]: [博士学位论文]. 北京: 北京交通大学, 2020.
- [20] 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)
- [21] Gabidulin, E.M. (1985) Theory of Codes with Maximum Rank Distance. *Problems of Information Transmission*, **21**, 3-16.