arXiv:2302.00979v1 [cs.IT] 2 Feb 2023

线性秩度量码的最大权码字

Olga Polverino、Paolo Santonastaso 和 Ferdinando Zullo

摘要

设 $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ 是一个维数为 k 的 $\mathbb{F}_{q^m}$-线性非退化秩度量码。本文研究确定 $\mathcal{C}$ 中具有最大重量（即 $\min\{m,n\}$）的码字数量 $M(\mathcal{C})$ 的问题，并刻画使 $M(\mathcal{C})$ 取最大值和最小值的码字。

MSC2020：94B05；94B65；94B27 关键词：秩

度量码；重量分布； q- stem

1 引言

过去几十年间，秩度量码因其众多应用以及与有趣数学对象的联系而备受关注。事实上，Silva、K¨otter 和 Kschischang 在 [46] 提出了将秩度量码用于线性随机网络编码的方案。不过，秩度量码的起源可追溯到 Delsarte [21]于 1978 年的工作；数年后，Gabidulin 在 [23] 和 Roth 在 [43]重新发现了这类码。此后，这类码在交叉错误纠正、密码学和网络编码中的应用相继出现，参见例如 [13]。秩度量码还与一些经过深入研究的代数和组合对象相关，例如半域 [44], 、有限几何中的线性集 [39], 、张量代数 [18],、斜代数 [6, 22]、 q 类似拟阵的对象 [26] ，以及许多其他对象，参见 [25] 和 [45]。

本文主要关注线性码的情形，即 $\mathbb{F}_{q^m}$- $\mathbb{F}_{q^m}^n$ 的子空间。这里，我们在 $\mathbb{F}_{q^m}^n$ 上赋予秩距离，其定义如下：对任意 $u = (u_1, \dots, u_n)$ $v = (v_1, \dots, v_n) \in \mathbb{F}_{q^m}^n$，则

$$d(u,v) = \dim_{\mathbb{F}_q}(\langle u_1 - v_1, \dots, u_n - v_n \rangle_{\mathbb{F}_q}).$$

我们的目标是提供关于 $\mathbb{F}_{q^m}$-线性非退化秩度量码重量分布的信息，也就是说，研究那些无法嵌入到更小空间、同时保持其重量分布不变的 $\mathbb{F}_{q^m}$-线性秩度量码。某些类别的秩度量码，其重量分布是众所周知的，例如最大秩距离码或少重量码类别，但总体而言，相关研究仍然很少。在汉明度量下，Ball 和 Blokhuis 在 [9] 中利用仿射空间中 t-重阻挡集的几何性质，研究了能够保证码中包含一个重量等于码长的码字的条件。对于非退化秩度量码，作者在 [4, 命题 3.11] 中证明，总存在一个最大重量为 $\min\{m,n\}$ 的码字，从而得以简洁地证明

最优 $\mathbb{F}_{q^m}$-线性反码的刻画，该刻画最初由 [41, 定理18]证明。最大权码字似乎也与 Crapo 和 Rota 提出的秩度量版临界问题有关（参见 [2,3]，另见 [28]），并且与 q-多拟阵有关，参见 [24]。

设 $\mathcal{C}$ 是 $\mathbb{F}_{q^m}^n$ 中一个维数为 k 的 $\mathbb{F}_{q^m}$-线性非退化秩度量码，并定义 $M(\mathcal{C})$ 为 $\mathcal{C}$ 中重量为 $\min\{m,n\}$ 的码字数量。本文研究以下两个问题：

问题 1.1. 确定 $M(\mathcal{C})$ 的上界和下界。

问题 1.2. 刻画所得 $M(\mathcal{C})$ 界中的极值情形 .

本文主要使用的工具来自组合学：我们采用系统的射影版本，即线性集，它们是射影空间中的点集。随后，我们利用关于线性集大小和重量分布的新旧界，得到所需的界。因此，已知 m、n、k、q、$M(\mathcal{C})$ 和第二大权重这六个值中的任意五个值后，我们便能确定剩下的一个值。接着，我们利用线性集的对偶理论以及新旧构造，给出示例，并刻画所得界中的等号情形。为说明我们的结果，我们证明了在二维情形下，当且仅当 $\mathcal{C}$ 或其几何对偶是最大秩距离码时，$M(\mathcal{C})$ 取最小值；我们还证明，只有当码的长度为 $mk/2$ 时，这一结论才能推广到更高维数。

本文结构如下。第2节介绍本文结果所需的秩度量码和线性集的定义与相关结果。第3节讨论 $M(\mathcal{C})$ 的上界和下界，并根据码的维数以及 n 与 m 之间的关系，将讨论分为四部分。第4节通过考察这些码的几何结构，分析下界取等号的情形。这些码与散布线性集密切相关，因此在某些情况下也与最大秩距离码有关。第5节致力于研究上界取等号的情形：此时的几何结构要么与典范子几何有关，要么与具有最小大小的线性集有关。最后，我们列出一些开放问题，为本文作结。

2 预备知识

我们先固定以下记号。设 p 为素数，h 为正整数。固定 $q=p^h$，并用 $\mathbb{F}_q$ 表示具有 q 个元素的有限域。此外，若 m 为正整数，则可考虑 $\mathbb{F}_{q^m}$，它是 $\mathbb{F}_q$ 的 m 次扩域。回顾一下，对于扩域 $\mathbb{F}_{q^m}/\mathbb{F}_q$，元素 $\alpha\in\mathbb{F}_{q^m}$ 的迹定义为

$$\mathrm{Tr}_{q^m/q}(\alpha):=\sum_{i=0}^{m-1}\alpha^{q^i}.$$

我们列出一些将在本文中反复使用的记号。

- $V = V(k, q)$ 表示一个 k 维的 $\mathbb{F}_q$-向量空间;
- $\langle U\rangle_{\mathbb{F}_q}$表示由 U张成的 $\mathbb{F}_q$张成空间，其中 U是向量空间 V的子集;
- PG$(k-1, q)$表示维数为 $k-1$ 、阶为q的射影笛沙格空间;

- PG$(V, \mathbb{F}_q)$表示由 V得到的射影空间，其中 V是一个 $\mathbb{F}_q$向量空间;
- $\langle S\rangle$ 表示 S中各点的张成空间，其中 S 是PG$(k-1, q)$的子集;
- GL(k, q)表示一般线性群;
- ΓL(k, q)表示一般半线性群;
- colsp(A) 是矩阵 A 的列在 $\mathbb{F}_q$ 上的张成空间。

2.1 秩度量码与 q-系统

2.1.1 秩度量码概述

向量 $v = (v_1, \ldots, v_n)$ 的秩（重量） $w(v)$ 是其各项在 $\mathbb{F}_q$ 上生成的向量空间的维数，即 $w(v) = \dim_{\mathbb{F}_q}(\langle v_1, \ldots, v_n\rangle_{\mathbb{F}_q})$。

秩度量码（线性向量码） $\mathcal{C}$ 是 $\mathbb{F}_{q^m}^n$ 的一个 $\mathbb{F}_{q^m}$-子空间，并赋予如下定义的秩距离:

$$d(x, y) = w(x - y),$$

其中 $x, y \in \mathbb{F}_{q^m}^n$。

设 $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ 是一个 $\mathbb{F}_{q^m}$ 线性秩度量码。若 k 是 $\mathcal{C}$ 的 $\mathbb{F}_{q^m}$ 维数，且 d 是其最小距离，则称 $\mathcal{C}$ 为一个 $[n, k, d]_{q^m/q}$ 码（或 $[n, k]_{q^m/q}$ 码），即

$$d = \min\{d(x, y) \colon x, y \in \mathcal{C}, x \neq y\}.$$

此外，我们用 $A_i(\mathcal{C})$（或简写为 A_i）表示 $\mathcal{C}$ 中重量为 $i \in \{0, \ldots, n\}$ 的码字数，而 $(A_0, \ldots, A_n)$ 称为 $\mathcal{C}$ 的重量分布。

可以为秩度量码证明一个类 Singleton 界。对于 $\mathbb{F}_{q^m}$ 线性码，该界如下所示。

定理 2.1. *[21]* 设 $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ 是一个 $[n, k, d]_{q^m/q}$ 码，则

$$mk \leq \max\{m, n\}(\min\{n, m\} - d + 1). \tag{1}$$

若一个 $[n, k, d]_{q^m/q}$ 码的参数达到界 (1)，则称其为最大秩距离码（简称 MRD 码）。

回顾一下，两个整数 s 和 t 的 q-二项式系数为

$$\begin{bmatrix} s \\ t \end{bmatrix}_q = \begin{cases} 0 & \text{if } s < 0, \text{ or } t < 0, \text{ or } t > s, \\ 1 & \text{if } t = 0 \text{ and } s \geq 0, \\ \prod_{i=1}^{t} \dfrac{q^{s-i+1} - 1}{q^i - 1} & \text{otherwise.} \end{cases}$$

这个数表示一个 s 维 $\mathbb{F}_q$-向量空间中 t 维 $\mathbb{F}_q$-子空间的数量。

Delsarte 在 [21] 中，以及随后 Gabidulin 在 [23] 中，确定了秩度量码的麦克威廉姆斯恒等式；对于最大秩距离码，这些恒等式可用于确定最大秩距离码的重量分布，另见 [42]。

定理 2.2。设 $\mathcal{C}$ 是一个参数为 $[n,k,d]_{q^m/q}$ 的最大秩距离码。设 $m' = \min\{m,n\}$ 且 $n' = \max\{m,n\}$。则

$$A_{d+\ell} = \begin{bmatrix} m' \\ d+\ell \end{bmatrix}_q \sum_{t=0}^{\ell} (-1)^{t-\ell} \begin{bmatrix} \ell+d \\ \ell-t \end{bmatrix}_q q^{\binom{\ell-t}{2}} (q^{n'(t+1)}-1)$$

对于任意 $\ell \in \{0,1,\ldots,n'-d\}$。

另一个重要概念是码字的秩支撑。设 $\Gamma = (\gamma_1,\ldots,\gamma_m)$ 是 $\mathbb{F}_{q^m}$ 的一组有序 $\mathbb{F}_q$-基。对于任意向量 $x = (x_1,\ldots,x_n) \in \mathbb{F}_{q^m}^n$，定义矩阵 $\Gamma(x) \in \mathbb{F}_q^{n\times m}$，其中

$$x_i = \sum_{j=1}^{m} \Gamma(x)_{ij}\gamma_j, \qquad \text{for all } i \in \{1,\ldots,n\},$$

即 $\Gamma(x)$ 是向量 x 相对于 $\mathbb{F}_{q^m}$ 的 Γ 的矩阵展开，并且这显然保持其秩，即 $w(x) = \mathrm{rk}(\Gamma(x))$。

定义 2.3. 设 $x = (x_1,\ldots,x_n) \in \mathbb{F}_{q^m}^n$ 和 $\Gamma = (\gamma_1,\ldots,\gamma_m)$ 是 $\mathbb{F}_{q^m}$ 的一个 $\mathbb{F}_q$ 阶基。x 的秩支撑定义为 $\Gamma(x)$ 的列空间：

$$\mathrm{supp}(x) = \mathrm{colsp}(\Gamma(x)) \subseteq \mathbb{F}_q^n.$$

如 [4, 命题 2.1]，所证，支撑不依赖于 Γ 的选择，因此我们可以直接讨论向量的支撑，而不必提及 Γ。

更多详情请参见 [32]。

2.1.2 秩度量码的几何

现在，我们回顾 $\mathbb{F}_{q^m}^n$ 中秩度量码之间等价的定义。$\mathbb{F}_{q^m}^n$ 的一个 $\mathbb{F}_{q^m}$-线性等距变换 ϕ 是一个保持距离的 $\mathbb{F}_{q^m}^n$ 的 $\mathbb{F}_{q^m}$-线性映射，即对于每个 $x \in \mathbb{F}_{q^m}^n$，都有 $w(x) = w(\phi(x))$；等价地，对于每个 $x,y \in \mathbb{F}_{q^m}^n$，都有 $d(x,y) = d(\phi(x)\ \phi(y))$。已有证明表明，赋予秩距离的 $\mathbb{F}_{q^m}^n$ 的 $\mathbb{F}_{q^m}$-线性等距变换群由 $\mathbb{F}_{q^m}$ 的（非零）标量乘法和线性群 $\mathrm{GL}(n,\mathbb{F}_q)$ 生成，参见例如 [14]。因此，若存在等距变换 ϕ 使得 $\phi(\mathcal{C}) = \mathcal{C}'$，则称两个秩度量码 $\mathcal{C},\mathcal{C}' \subseteq \mathbb{F}_{q^m}^n$（线性）等价。显然，在研究 $[n,k]_{q^m/q}$ 码的等价性时，$\mathbb{F}_{q^m}^*$ 的作用是平凡的。这意味着，两个 $[n,k]_{q^m/q}$ 码 $\mathcal{C}$ 和 $\mathcal{C}'$ 等价，当且仅当存在 $A \in \mathrm{GL}(n,q)$ 使得 $\mathcal{C}' = \mathcal{C}\ A = \{vA : v \in \mathcal{C}\}$。我们将要考虑的大多数码都是非退化的。

定义 2.4. 若 $\mathcal{C}$ 的任意生成矩阵的列均为 $\mathbb{F}_q$-线性无关，则称 $\mathcal{C}$ 是一个非退化的 $[n,k]_{q^m/q}$ 秩度量码。我们用 $\mathfrak{C}[n,k,d]_{q^m/q}$ 表示 $[n,k,d]_{q^m/q}$ 非退化秩度量码的等价类集合。

秩度量的几何对应物是系统。

定义 2.5. 系统 $[n,k,d]_{q^m/q}$ 是 $\mathbb{F}_q$的一个 $\mathbb{F}_{q^m}^k$ -子空间，其维数为 n，满足 $\langle U\rangle_{\mathbb{F}_{q^m}} = \mathbb{F}_{q^m}^k$ 且

$$d = n - \max\left\{\dim_{\mathbb{F}_q}(U\cap H) \mid H \text{ is an } \mathbb{F}_{q^m}\text{-hyperplane of } \mathbb{F}_{q^m}^k\right\}.$$

此外，两个系统 $[n,k,d]_{q^m/q}$和 U'等价，当且仅当存在一个 $\mathbb{F}_{q^m}$-同构 $\varphi\in \mathbf{GL}(k, \mathbb{F}_{q^m})$，使得

$$\varphi(U) = U'.$$

我们用 $\mathfrak{U}[n,k,d]_{q^m/q}$表示系统 $[n,k,d]_{q^m/q}$ 的等价类集合。

下面的结果使我们能够建立秩度量码与系统之间的对应关系。

定理 2.6. *[40]* 设 $\mathcal{C}$ 是一个非退化的秩度量码， G 是其生成矩阵。令 $U\subseteq\mathbb{F}_{q^m}^k$ 为 G的列所张成的 $\mathbb{F}_q$-空间。元素 $xG\in\mathcal{C}$的秩权，其中 $x=(x_1,\dots,x_k)\in\mathbb{F}_{q^m}^k$为

$$w(xG) = n - \dim_{\mathbb{F}_q}(U\cap x^{\perp}), \tag{2}$$

其中 $x^{\perp} = \{y=(y_1,\dots,y_k)\in\mathbb{F}_{q^m}^k\colon \sum_{i=1}^k x_iy_i = 0\}$. 特别是,

$$d = n - \max\left\{\dim_{\mathbb{F}_q}(U\cap H)\colon H \textit{ is an } \mathbb{F}_{q^m}\textit{-hyperplane of } \mathbb{F}_{q^m}^k\right\}. \tag{3}$$

借助上述定理，我们得到了非退化 $[n,k,d]_{q^m/q}$ 码与 $[n,k,d]_{q^m/q}$ 系统之间的完整对应关系。

定理 2.7. 非退化 $[n,k,d]_{q^m/q}$码的等价类与 $[n,k,d]_{q^m/q}$系统的等价类之间存在一一对应关系。

该对应关系可通过以下两个映射形式化

$$\Psi : \mathfrak{C}[n,k,d]_{q^m/q}\to\mathfrak{U}[n,k,d]_{q^m/q}$$
$$\Phi : \mathfrak{U}[n,k,d]_{q^m/q}\to\mathfrak{C}[n,k,d]_{q^m/q},$$

其作用如下。设 $[\mathcal{C}]\in\mathfrak{C}[n,k,d]_{q^m/q}$ 和 G 是 $\mathcal{C}$的生成矩阵。那么$\Psi([\mathcal{C}])$ 是 $[n,k,d]_{q^m/q}$系统 $[U]$的等价类，其中 U是 G各列的 $\mathbb{F}_q$-张成空间。在这种情况下， U 也称为与 $\mathcal{C}$相关联的系统。反过来，给定$[U]\in\mathfrak{U}[n,k,d]_{q^m/q}$。定义 G为其列构成 U的一个 $\mathbb{F}_q$-基的矩阵，并令 $\mathcal{C}$

为由 G生成的码。那么 $\Phi([U])$ 是 $[n,k,d]_{q^m/q}$码$[\mathcal{C}]$的等价类。 $\mathcal{C}$ 也称为与 U相关联的码。 Ψ 和 Φ 定义良好，且互为逆映射。另见 [4]。

一种重要的码，其定义自然源于几何观点，即单纯形码；在 [4] 中，它被定义为任意非退化的 $[mk,k]_{q^m/q}$ 码，也就是说，其关联系统 $\mathbb{F}_{q^m}^k$ 可视为维数为 mk 的 $\mathbb{F}_q$-向量空间。

广义秩权曾以不同的定义多次被引入，参见例如 [30], ；它们也被用作判定码族不等价性的工具，如 [12] 中所做的那样。

本文将采用 [40] 中给出的定义，更准确地说，采用 [4, 定理 3.14], 中给出的等价定义，该定义与系统直接相关。

定义 2.8. 设 $\mathcal{C}$ 是一个非退化的 $[n,k,d]_{q^m/q}$ 秩度量码，且 U 是一个关联系统。对于任意 $r\in\{1,\dots,k\}$，第 r 个广义秩权为

$$d_r^{\mathrm{rk}}(\mathcal{C})=n-\max\left\{\dim_{\mathbb{F}_q}(U\cap H)\colon H \textit{ is an } \mathbb{F}_{q^m}\textit{-subspace of codim. } r \textit{ of } \mathbb{F}_{q^m}^k\right\}. \quad (4)$$

注意，当 $r=1$ 时，根据上述定义，我们得到最小距离。
接下来，我们将回顾码字的支撑与和该码相关的系统的交集之间的关系。

设 $G\in\mathbb{F}_{q^m}^{k\times n}$，其列 $\mathbb{F}_q$-线性无关，并令 U 为 G各列的 $\mathbb{F}_q$-张成空间。定义映射

$$\begin{array}{rccc}\psi_G\colon & \mathbb{F}_q^n & \longrightarrow & U\\ & \lambda & \longmapsto & \lambda G^\top,\end{array}$$

事实证明，该映射是一个 $\mathbb{F}_q$-线性同构。

定理 2.9。 *[36, 定理 3.1]* 设 $\mathcal{C}$ 是一个非退化的 $[n,k]_{q^m/q}$ 码，其生成矩阵为 $G\in\mathbb{F}_{q^m}^{k\times n}$，并令 U 为 G各列的 $\mathbb{F}_q$-张成空间。那么，对于每个 $x\in\mathbb{F}_{q^m}^k$

$$\psi_G^{-1}(U\cap x^\perp)=\mathrm{supp}(vG)^\perp,$$

其中，$\mathrm{supp}(vG)^\perp$ 是 $\mathrm{supp}(vG)$ 关于 $\mathbb{F}_q^n$中的标准标量积的正交补。

2.2 线性集

本文将经常借助线性集的概念，以射影方式研究这些系统。设 V是 $\mathbb{F}_{q^m}$上的 k 维向量空间，且 $\Lambda=\mathrm{PG}(V,\mathbb{F}_{q^m})=\mathrm{PG}(k-1,q^m)$。回顾一下，若 U 是 V中维数为 n的 $\mathbb{F}_q$ 子空间，则点集

$$L_U=\{\langle u\rangle_{\mathbb{F}_{q^m}}:u\in U\setminus\{0\}\}\subseteq\Lambda$$

称为秩为 n 的 $\mathbb{F}_q$-线性集。设 $\Omega = \mathrm{PG}(W, \mathbb{F}_{q^m})$ 是 Λ的一个射影子空间。Ω 在 L_U 中的重量定义为

$$w_{L_U}(\Omega) = \dim_{\mathbb{F}_q}(U \cap W).$$

若 N_i表示 L_U中重量为 $i \in \{0, \ldots, n\}$的 Λ的数量，则有以下关系：

$$|L_U| \leq \frac{q^n - 1}{q - 1}, \tag{5}$$

$$|L_U| = N_1 + \ldots + N_n, \tag{6}$$

$$N_1 + N_2(q+1) + \ldots + N_n(q^{n-1} + \ldots + q + 1) = q^{n-1} + \ldots + q + 1. \tag{7}$$

此外，若 $L_U \neq \emptyset$，则

$$|L_U| \equiv 1 \pmod{q}, \tag{8}$$

并且若 $\langle L_U \rangle = \mathrm{PG}(k-1, q^m)$，则

$$|L_U| \geq \frac{q^k - 1}{q - 1}. \tag{9}$$

还需注意，若 P_1，...，$P_j \in L_U$是独立点（即 $\langle P_1$，...，$P_j \rangle$ 是 $\mathrm{PG}(k-1, q^m)$ 的一个 $(j-1)$ 维子空间），则

$$w_{L_U}(P_1) + \ldots + w_{L_U}(P_j) \leq n. \tag{10}$$

注 2.10。在存在 j 个独立点属于 L_U，使得式 (10) 中等号成立的情况下，L_U 中各点的最大重量为

$$\max\{w_{L_U}(P_i) \colon i \in \{1, \ldots, j\}\}.$$

此外，若 L_U 和 U 具有点数最大值 $\frac{q^n-1}{q-1}$，则称其为散布的；等价地说，L_U 的所有点的重量均为 1。$\mathrm{PG}(k-1, q^m)$ 的典范子几何定义为秩为 k 、张成整个空间的 $\mathbb{F}_q$-线性集 L_U，它们是散布的 $\mathbb{F}_q$-线性集的例子。Blokhuis 和 Lavrauw 给出了散布线性集秩的以下界。

Theorem 2.11. *[15]*设 L_U是 $\mathrm{PG}(k-1, q^m)$ 中秩为 n 的散布的 $\mathbb{F}_q$-线性集，则

$$n \leq \frac{mk}{2}.$$

$\mathrm{PG}(k-1, q^m)$ 中秩为 $km/2$ 的散布的 $\mathbb{F}_q$-线性集称为最大散布线性集，而 U 也称为最大散布的 $\mathbb{F}_q$-子空间。

非空线性集 L_U 的点数有一个显然的下界，即 $|L_U| \geq 1$。添加一些假设后，可以改进这个下界。

定理 2.12（ [20, 定理 1.2] 和 [16, 引理 2.2]）。若 L_U 是一个秩为 n 的 $\mathbb{F}_q$-线性集，位于 PG(1, q^m) 上，且 L_U 至少包含一个重量为 1 的点，则 $|L_U| \geq q^{n-1}+1$。

下面的结果讨论一个具有最少点数的示例族，即满足定理 2.12 中界限的示例族。

定理 2.13. *[29, 定理 2.7]* 设 $\lambda \in \mathbb{F}_{q^m}$ 是生成 $\mathbb{F}_{q^m}$ 的一个元素，且

$$L_U = \{\langle(\alpha_0+\alpha_1\lambda+\ldots+\alpha_{t_1-1}\lambda^{t_1-1}, \beta_0+\beta_1\lambda+\ldots+\beta_{t_2-1}\lambda^{t_2-1})\rangle_{\mathbb{F}_{q^m}} : \alpha_i, \beta_i \in \mathbb{F}_q,$$
$$not\ all\ zero,\ 1 \leq t_1, t_2, t_1+t_2 \leq m\},$$

其中

$$U = \langle 1, \lambda, \ldots, \lambda^{t_1-1}\rangle_{\mathbb{F}_q} \times \langle 1, \lambda, \ldots, \lambda^{t_2-1}\rangle_{\mathbb{F}_q}.$$

则 L_U 是 PG(1, q^m) 中一个秩为 $k = t_1+t_2$、具有 $q^{k-1}+1$ 个点的 $\mathbb{F}_q$-线性集。设$t_1 \leq t_2$，则

- 点 $\langle$(0, 1)$\rangle_{\mathbb{F}_{q^n}}$ 的重量为 t_2;
- 存在 $q^{t_2-t_1+1}$ 个重量为 t_1 且不同于 $\langle$(0,1)$\rangle_{\mathbb{F}_{q^n}}$ 的点;
- 有 $q^{k-2i+1}-q^{k-2i-1}$ 个重量为 $i \in \{1, \ldots, t_1-1\}$ 的点。

最近，在 [20], 中的结果基础上扩展，已证明线性集大小的如下下界。

定理 2.14. *[1, 20]* 设 L_U 是 PG($k-1, q^m$) 中秩为 n、张成整个空间的一个 $\mathbb{F}_q$-线性集。假设存在某个 $(r-1)$-空间 Ω，其中 $r < k-1$，使得 L_U 与 Ω 相交于 Ω 的一个典范 $\mathbb{F}_q$-子几何。那么

$$|L_U| \geq q^{n-1}+\ldots+q^{n-r}+\frac{q^{k-r}-1}{q-1}. \tag{11}$$

若 $r < k-1$，当且仅当 L_U 是 PG($k-1, q^m$) 中的一个典范子几何 PG($k-1, q$) 时，等号成立。

此外，线性集的秩由其大小及其点的最小重量决定，具体如下。

命题 2.15. *[1, 命题 3.17]* 设 L_U 是 PG($k-1, q^m$) 中一个包含多个点的 $\mathbb{F}_q$-线性集。记 $e = \min_{P \in L_U} w_{L_U}(P)$。那么 L_U 的秩是满足以下条件的唯一整数 n

$$q^{n-e} < |L_U| \leq \frac{q^n-1}{q^e-1},$$

即 $n = \lfloor \log_q(|L_U|) \rfloor + e$。此外，如果 L_U 张成整个空间，那么

$$q^{n-e}+\frac{q^{k-1}-1}{q-1} \leq |L_U| \leq \frac{q^n-1}{q^e-1},$$

2.3 线性集与 $\mathbb{F}_q$-子空间的对偶性

现在，我们回顾线性集的对偶这一概念。设 σ： $V\times V\to\mathbb{F}_{q^m}$ 是定义在 k 维 $\mathbb{F}_{q^m}$-向量空间 V 上的非退化反射半双线性形式，并考虑

$$\begin{array}{rccc}\sigma': & V\times V & \longrightarrow & \mathbb{F}_q\\ & (x,y) & \longmapsto & \mathrm{Tr}_{q^m/q}(\sigma(x,y)).\end{array}$$

因此， σ' 是定义在 V 上的非退化反射半双线性形式，其中 V 视为维数为 km的 $\mathbb{F}_q$-向量空间。于是，我们可以分别将 $\perp$ 和 $\perp'$ 视为由 σ和 σ'定义的正交补映射，并将 τ和 τ'视为分别由 σ和 σ'诱导的 PG$(V,\mathbb{F}_{q^m})$ 和 PG$(V,\mathbb{F}_q)$ 的极性。对于 PG$(V,\mathbb{F}_{q^m})$ 中秩为 n的 $\mathbb{F}_q$-线性集，其在 PG$(V,\mathbb{F}_{q^m})$ 中秩为 $km-n$ 的 $\mathbb{F}_q$-线性集$L_U^\tau=L_{U^{\perp'}}$称为 L_U关于极性 τ的对偶线性集。对偶线性集的定义不取决于所选的极性。事实上， [37, 命题 2.5] 证明了，若 τ_1 和 τ_2 是两个极性，且$\perp_1'$ 和 $\perp_2'$ 是如上所述的正交补映射，则对偶线性集 $U^{\perp_1'}$和 $U^{\perp_2'}$是 ΓL(k,q^m)-等价的。

此外，关于线性集，子空间的重量与关于对偶线性集，其极空间的重量之间存在如下关系。此性质主要依赖于这样一个事实：对于 $\mathbb{F}_{q^m}$ 的任意 V 子空间，均有 $W^{\perp'}=W^{\perp}$。

命题 2.16. *[37, 性质 2.6]*设 $L_U\subseteq$ PG$(k-1,q^m)$ 是秩为 n 的 $\mathbb{F}_q$-线性集。设 $\Omega_s=$ PG$(W,\mathbb{F}_{q^m})$ 是 PG$(k-1,q^m)$ 的一个 s-空间。那么

$$w_{L_U^\tau}(\Omega_s^\tau)=w_{L_U}(\Omega_s)+km-n-(s+1)m,$$

i.e.

$$\dim_{\mathbb{F}_q}(U^{\perp'}\cap W^{\perp})=\dim_{\mathbb{F}_q}(U\cap W)+\dim_{\mathbb{F}_q}(V)-\dim_{\mathbb{F}_q}(U)-\dim_{\mathbb{F}_q}(W).$$

我们可以通过其对偶来刻画最大散布线性集。

命题 2.17. *[37, 定理 3.5]*设 $L_U\subseteq$ PG$(k-1,q^m)$ 是秩为 $mk/2$ 的 $\mathbb{F}_q$-线性集。那么， L_U 是散布的，当且仅当 $L_{U^{\perp'}}$ 是散布的。

2.4 秩度量码的几何对偶

我们回顾一种近期引入的、针对秩度量码的运算，称为几何对偶。该运算将 $\mathfrak{C}[n,k,d]_{q^m/q}$ 中的任意元素映射为 $\mathfrak{C}[mk-n,k,d']_{q^m/q}$中的另一个元素。

定义 2.18. 设 $\mathcal{C}$ 是一个非退化的 $[n,k,d]_{q^m/q}$ ，且 U 是与 $\mathcal{C}$相关联的系统。再设 $d_{k-1}^{\mathrm{rk}}(\mathcal{C})\geq n-m+1$。则 $\mathcal{C}$ 关于 $\perp'$的几何对偶 $\mathcal{C}^{\perp_{\mathcal{G}}}$ 定义为 $\mathcal{C}'$，其中 $\mathcal{C}'$ 是与系统 $U^{\perp'}$ 相关联的任意一个码，而$\perp'$ 按第2.3节中的定义给出。

以下结果为该定义提供了依据。

定理 2.19。 *[17]* 设 $\mathcal{C}$ 是一个 $[n,k,d]_{q^m/q}$ 码， U 是与$\mathcal{C}$相关联的系统。另设 $d_{k-1}^{\mathrm{rk}}(\mathcal{C}) \geq n-m+1$。那么，在等价意义下， $\mathcal{C}$ 的几何对偶 $\mathcal{C}^{\perp_{\mathcal{G}}}$不依赖于关联系统的选择，也不依赖于[$\mathcal{C}$]中的码的选择，因此 $\perp_{\mathcal{G}}$是良定义的。此外，对于某个 d'，有 $[\mathcal{C}^{\perp_{\mathcal{G}}}] \in \mathfrak{C}[km-n,k,d']_{q^m/q}$。

注 2.20. 注意到 $U^{\perp'}$是一个系统，当且仅当 $U^{\perp'}$不包含在 $\mathbb{F}_{q^m}^k$的任何超平面中；对偶地，这对应于 U 不包含 $\mathbb{F}_{q^m}^k$的任何一维 $\mathbb{F}_{q^m}$子空间。根据 (4)，这对应于要求 $d_{k-1}^{\mathrm{rk}}(\mathcal{C}) \geq n-m+1$。

在和秩度量码的背景下， [17] 中已利用过这一操作。

3 最大权码字数量的界

本节利用关于线性集的新旧界，给出 $M(\mathcal{C})$ 的上界和下界。为阐明所涉及的技巧和论证，我们根据 $\dim_{\mathbb{F}_{q^m}}(\mathcal{C})$ 是二还是大于二，以及 $n \leq m$ 还是 $n \geq m$，分别进行分析。

3.1 二维情形以及 $n \leq m$

我们先描述 $M(\mathcal{C})$ 的几何意义。

命题 3.1. 设 $\mathcal{C}$ 是一个非退化的 $[n,2]_{q^m/q}$ 码，且 U 是其任意一个关联系统。假设 $n \leq m$。那么

$$M(\mathcal{C}) = (q^m-1)|\mathrm{PG}(1,q^m) \setminus L_U|.$$

证明. 设 G 是 $\mathcal{C}$ 的生成矩阵，其列的 $\mathbb{F}_q$-张成空间为 U。那么由 (2) 可知，对于任意非零的 $u \in \mathbb{F}_{q^m}^2$，有

$$w_{L_U}(P) = n - w(uG),$$

其中 $P = \langle u^{\perp} \rangle_{\mathbb{F}_{q^m}} \in \mathrm{PG}(1,q^m)$，因此，由以下事实可得出该断言：当且仅当 $P \notin L_U$时，$w_{L_U}(P) = 0$。 □

现在，我们可以给出 $M(\mathcal{C})$ 的界了。

The定理 3.2. 设 $\mathcal{C}$ 是一个非退化的 $[n,2]_{q^m/q}$ 码，并假设 $n \leq m$。那么

$$q^{2m} - 1 - (q^m-1)\frac{q^n-1}{q-1} \leq M(\mathcal{C}) \leq q^{2m} - 1 - (q^m-1)(q+1). \tag{12}$$

此外，如果 $\mathcal{C}$ 包含一个重量为 $n-1$ 的码字，

$$M(\mathcal{C}) \leq q^{2m} - 1 - (q^m-1)(q^{n-1}+1), \tag{13}$$

也就是说

$$q^{2m} - q^{m+n-1} - \ldots - q^m + q^{n-1} + \ldots + q \leq M(\mathcal{C}) \leq q^{2m} - q^{m+n-1} - q^m + q^{n-1}.$$

证明。设 U 是一个与 $\mathcal{C}$ 相关的任意关联系统。由于 $\langle U\rangle_{\mathbb{F}_{q^m}} = \mathbb{F}_{q^m}^2$，因此 L_U 不可能是一个点，由 (8) 可得

$$|L_U| \geq q+1.$$

此外，根据 (5)

$$|L_U| \leq \frac{q^n-1}{q-1}.$$

因此，根据命题 3.1，断言的第一部分得证。现在，设 G 是 $\mathcal{C}$ 的任意生成矩阵，并假设 $\mathcal{C}$ 包含一个重量为 $n-1$ 的码字 uG。由 (2) 可知，存在一个点 $P \in L_U$，使得 $w_{L_U}(P) = 1$。根据定理 2.12，有

$$|L_U| \geq q^{n-1}+1$$

因此，命题 3.1 再次给出了 $M(\mathcal{C})$ 的上界。 □

一旦知道该码的第二大权重，就可以改进上述界 (12)，从而推广上述定理的第二部分。

定理 3.3。设 $\mathcal{C}$ 是一个非退化的 $[n,2]_{q^m/q}$ 码。假设 $n \leq m$，且 $n-e$ 是第二大权重。则

$$q^{2m}-1-(q^m-1)\frac{q^n-1}{q^e-1} \leq M(\mathcal{C}) \leq q^{2m}-1-(q^m-1)(q^{n-e}+1),$$

即 $n = \lfloor \log_q(q^m+1-M(\mathcal{C})\overline{q^m-1}) \rfloor + e$。

此外，若 $m=n$，则 $e \mid m$。

证明。设 U 是任意一个满足 $\mathcal{C}$ 的关联系统。(2) 意味着 $e = \min_{P\in L_U} w_{L_U}(P)$。于是，由命题 2.15 可得

$$q^{n-e}+1 \leq |L_U| \leq \frac{q^n-1}{q^e-1}.$$

由命题 3.1 可得这些界。特别地，当 $m=n$ 时，则 [38, 命题 3.1] 意味着 $e \mid m$，且 U 是 $\mathbb{F}_{q^m}^2$ 的一个 $\mathbb{F}_{q^e}$-子空间。 □

注 3.4。在 $m=n$ 且 $n-e$ 为第二大权重的情形下，码 $\mathcal{C}$ 恰为 e-可除码，即码字的所有重量都是 e 的倍数；参见 *[38]*。

3.2 二维情形与 $n > m$

现在我们来处理 $n > m$ 的情形。为此，我们需要借助线性集的对偶。

定理 3.5. 设 $\mathcal{C}$ 是一个非退化的 $[n,2]_{q^m/q}$ 码，并假设 $m < n$ 和$d(\mathcal{C}) \geq n-m+1$。那么

$$q^{2m}-1-(q^m-1)\frac{q^{2m-n}-1}{q-1} \leq M(\mathcal{C}) \leq q^{2m}-1-(q^m-1)(q+1). \tag{14}$$

若 $m-e$ 是 $\mathcal{C}$的第二大重量，则

$$q^{2m}-1-(q^m-1)\frac{q^{2m-n}-1}{q^e-1} \leq M(\mathcal{C}) \leq q^{2m}-1-(q^m-1)(q^{2m-n-e}+1),$$

和 $n = 2m - \lfloor \log_q(q^m+1-{}^{M(\mathcal{C})}\overline{q^m-1}) \rfloor - e$。

证明。设 U 是与 $\mathcal{C}$相关联的任意系统。与命题 3.1 类似，我们可以通过确定 L_U中重量为 $n-m$ 的点的数量来确定 $M(\mathcal{C})$。考虑 L_U 的对偶线性集 $L_{U^{\perp'}}$。命题 2.16 表明，点 P 满足 $w_{L_U}(P) = n-m$ 当且仅当 ${}^{w_{L_{U^{\perp'}}}}(P^\tau) = 0$。因此，

$$M(\mathcal{C}) = (q^m-1)|\mathrm{PG}(1,q^m) \setminus L_{U^{\perp'}}|. \tag{15}$$

由于 $L_{U^{\perp'}}$的秩为 $2m-n<m$，由 (5) 可得

$$q+1 \leq |L_{U^{\perp'}}| \leq \frac{q^{2m-n}-1}{q-1},$$

根据注 2.20，$|L_{U^{\perp'}}| > 1$。若 $\mathcal{C}$ 包含一个重量为 $m-e$的码字，则存在一个点 P，使得 $w_{L_U}(P) = n-m+e$，因而由命题 2.16 可得 ${}^{w_{L_{U^{\perp'}}}}(P^\tau) = e$。现在，应用命题 2.15

$$|L_{U^{\perp'}}| \geq q^{2m-n-e}+1.$$

由（15）可得这些界。 □

3.3 更大维数情形与 $n \leq m$

在本节中，我们假设 $n \leq m$ 和 $k > 2$。为了突出 $M(\mathcal{C})$ 中的二阶量级，我们将不直接对 $M(\mathcal{C})$ 给出这些界，而是对 ${}^{M(\mathcal{C})}\overline{q^m-1}$ 给出。在这些假设下，$M(\mathcal{C})$ 对应于确定一个线性集的外部超平面数量。

命题 3.6. 设 $\mathcal{C}$ 为一个非退化的 $[n,k]_{q^m/q}$ 码，且 U 为任意一个关联系统。假设 $n \leq m$。则

$$M(\mathcal{C}) = (q^m-1)|\{H = \mathrm{PG}(k-2,q^m)\colon H \cap L_U = \emptyset\}|.$$

证明. 设 G 为 $\mathcal{C}$ 的一个生成矩阵，其列的 $\mathbb{F}_q$-张成空间为 U。根据 (2)，码字 $c = uG$ 具有最大重量，当且仅当

$$w_{L_U}(u^{\perp}) = n - w(uG) = 0,$$

由此即可得到所述结论。 □

为了证明我们的界，需要以下两个几何引理。

引理 3.7。设 $\Sigma =$PG($k-1, q$) 是 PG($k-1, q^m$) 中的一个典范子几何，且 $k \leq m$。那么，PG($k-1, q^m$) 中与 Σ 至少有一个点相交的超平面数为

$$\alpha = \frac{q^{mk}-1}{q^m-1} - \prod_{i=1}^{k-1}(q^m - q^i),$$

而 PG(k, q^m) 中与 Σ 至少有两个点相交（因而至少有 $q+1$）的超平面数为

$$\beta = \frac{q^{mk}-1}{q^m-1} - \prod_{i=1}^{k-1}(q^m - q^i) - \frac{q^k-1}{q-1}\prod_{i=0}^{k-2}(q^m - q^i).$$

证明。设 U 是 $\mathbb{F}_{q^m}^k$ 中任意一个满足 $L_U = \Sigma$ 的 k 维 $\mathbb{F}_q$ 子空间。显然， U 是一个 $[k, k, 1]_{q^m/q}$ 系统。那么，与 U 相关联的任一码 $\mathcal{C}$ 都与 $\mathbb{F}_{q^m}^k$ 相同（且显然是一个最大秩距离码）。此外，由 (2) 可知，外部超平面的数目 γ 对应于 $\mathcal{C}$ 中重量为 k 的码字数除以 $q^m - 1$，更确切地说，

$$\gamma = \frac{A_k}{q^m-1},$$

其中 A_k 表示 $\mathbb{F}_{q^m}^k$ 中重量为 k的向量数。通过简单计算可得

$$A_k = \prod_{i=0}^{k-1}(q^m - q^i).$$

因此，

$$\gamma = \prod_{i=1}^{k-1}(q^m - q^i)$$

从而

$$\alpha = \frac{q^{mk}-1}{q^m-1} - \gamma.$$

β 的值也可以通过从 PG($k-1, q^m$) 中超平面的数量减去 γ 的值以及与 Σ相切的切超平面的数量 δ 来得到。与之前一样，可以看出

$$\delta = \frac{A_{k-1}}{q^m-1},$$

其中， A_{k-1} 表示 $\mathbb{F}_{q^m}^k$ 中重量为 $k-1$的向量数量。根据定理 2.2 以及 [33], , 可得

$$A_{k-1} = \begin{bmatrix} k \\ 1 \end{bmatrix}_q \sum_{t=0}^{k-2} (-1)^{t-k} \begin{bmatrix} k-1 \\ k-2-t \end{bmatrix}_q q^{\binom{k-2-t}{2}} (q^{m(t+1)}-1) = \frac{q^k-1}{q-1} \prod_{i=0}^{k-2} (q^m - q^i).$$

□

引理 3.8. 设 L_U 是一个张成 PG($k-1, q^m$) 的 $\mathbb{F}_q$-线性集，其秩为 n，且满足 $3 \le k \le n \le m$。那么对每个点 $P \in L_U$，存在一个经过 P 的 r-空间，与 L_U 恰好交于 P，对每个 $r \in \{0, \ldots, k-2\}$ 均如此。特别地，存在一个经过 P 且与 L_U 相切的超平面。

证明. 反设所有经过 P 的直线都不与 P 相切，因此它们与 L_U 至少交于 $q+1$ 个点。那么

$$q\frac{q^{m(k-1)}-1}{q^m-1} + 1 \le |L_U| \le \frac{q^n-1}{q-1},$$

因此我们得到矛盾，因为 $n \le m$。现在，设该断言对任意 $r \in \{1, \ldots, t\}$ 均成立，并设 π 是一个经过 P 且与 L_U 相切的 t-空间。反设所有经过 π 的 q^m+1 $(t+1)$-空间都不与 L_U 相切，则

$$q(q^m+1) + 1 \le |L_U| \le \frac{q^n-1}{q-1},$$

这再次与 $n \le m$ 矛盾。 □

我们可以利用引理 3.7 得到上界和下界，这是基于如下事实：在系统 U in $\mathbb{F}_{q^m}^k$ 中，我们总能找到 k $\mathbb{F}_{q^m}$-线性无关的向量；从几何上看，这意味着 L_U iscontained 一个典范子几何。

定理 3.9. 设 $\mathcal{C}$ be 一个非退化的 $[n,k]_{q^m/q}$ 码。假设 $n \le m$。那么

$$\frac{q^{mk}-1}{q^m-1} - \frac{q^n-1}{q-1}\frac{q^{(k-1)m}-1}{q^m-1} + q\beta \le \frac{M(\mathcal{C})}{q^m-1} \le \prod_{i=1}^{n-1}(q^m-q^i) \tag{16}$$

其中

$$\beta = \frac{q^{mk}-1}{q^m-1} - \prod_{i=1}^{k-1}(q^m-q^i) - \frac{q^k-1}{q-1}\prod_{i=1}^{k-2}(q^m-q^i).$$

证明。设 U 是任意一个具有 $\mathcal{C}$ 的关联系统。根据命题 3.6，我们需要计算 PG($k-1, q^m$) 中与 L_U 不相交的超平面的数量。记 τ_0、τ_1 和 τ_s 分别为 PG($k-1, q^m$) 中与 L_U 相交于 0 个点、1 个点和至少两个点的超平面数量。显然， $\tau_0+\tau_1+\tau_s = \frac{q^{mk}-1}{q^m-1}$。注意，根据 (8)，如果一个超平面与 L_U 相交于至少两个

个点，那么交集将包含至少 $q+1$ 个点。因此，通过对集合进行双重计数

$$\{(P,H)\colon P \text{ point}, H \text{ hyperplane and } P \in L_U \cap H\},$$

并利用任意割超平面与 L_U 至少相交于 $q+1$ 个点这一事实，我们得到

$$\tau_1 + \tau_s(q+1) \leq |L_U| \frac{q^{(k-1)m}-1}{q^m-1},$$

由此可得

$$\tau_1 + \tau_s \leq |L_U| \frac{q^{(k-1)m}-1}{q^m-1} - q\tau_s.$$

注意，U 包含 k 个向量 $u_1, \ldots, u_k$，它们在 $\mathbb{F}_{q^m}$ 上线性无关。记为 $W = \langle u_1, \ldots, u_k \rangle_{\mathbb{F}_q}$，则 PG$(k-1,q)$ 是包含于 L_U 中的一个典范子几何。因此，$L_W =$

$$\tau_s \geq \beta,$$

其中 β 是 L_W 的割超平面数量（由引理 3.7 计算得出）。因此，我们有

$$\tau_1 + \tau_s \leq |L_U| \frac{q^{(k-1)m}-1}{q^m-1} - q\tau_s \leq \frac{q^n-1}{q-1}\frac{q^{(k-1)m}-1}{q^m-1} - q\beta, \tag{17}$$

因此

$$\tau_0 \geq \frac{q^{mk}-1}{q^m-1} - \frac{q^n-1}{q-1}\frac{q^{(k-1)m}-1}{q^m-1} + q\beta.$$

此外，我们可以用 $\mathbb{F}_q^{m\times n}$ 中秩为 n 的矩阵数量来给 $M(\mathcal{C})$ 一个上界，该数量为 $(q^m-1)\prod_{i=1}^{n-1}(q^m-q^i)$。 □

注 3.10。注意，当 $n=k$

$$(q^m-1)\prod_{i=1}^{k-1}(q^m-q^i) = q^{mk}-1-(q^m-1)\alpha,$$

其中 α 是 PG$(k-1,q^m)$ 中与 PG$(k-1,q)$ 至少有一个点相交的超平面的数量。

我们可以证明关于 $M(\mathcal{C})$ 的另一个上界。与前一个上界不同，该上界还涉及码的长度。

定理 3.11。设 $\mathcal{C}$ 是一个非退化的 $[n,k]_{q^m/q}$ 码。假设 $n \leq m$，且 $n-e$ 是 $\mathcal{C}$ 的第二大权重。那么

$$q^{m(k-1)} - q^{m(k-2)+n-e} - q^{m(k-2)}\left(\frac{q^{n-e}-1}{q^e-1}\right) \leq \frac{M(\mathcal{C})}{q^m-1} \leq q^{m(k-1)} - q^{m(k-2)+n-e},$$

即，$m(k-2)+n = \lfloor \log_q(q^{m(k-1)} - {}^{M(\mathcal{C})}\overline{q^m-1}) \rfloor + e$。

证明。设 U 是满足 $\mathcal{C}$ 的任意关联系统，并设 $c \in \mathcal{C}$ 满足 $w(c) = n-e$。我们确定 $\mathrm{PG}(k-1, q^m)$ 中相对于 L_U 的外部超平面数量的下界和上界。由于 $n-e$ 是 $\mathcal{C}$ 中的第二大权重，根据定理 2.6，我们有

$$e = \min\{\dim_{\mathbb{F}_q}(U \cap H) \colon H \text{ is an } \mathbb{F}_{q^m}\text{-hyperplane of } \mathbb{F}_{q^m}^k \text{ such that } U \cap H \neq \{0\}\}. \quad (18)$$

我们证明，$e = \min\{w_{L_U}(P) \colon P \in L_U\}$。假设存在一个点 $Q \in L_U$，使得 $w_{L_U}(Q) = e' < e$。那么根据引理 3.8，存在一个经过 Q 且与 L_U 相切的超平面 H'。这意味着 $\dim^{\mathbb{F}_q}(U \cap H') = e'$，与 (18) 矛盾。另一方面，如果对于每个 $P \in L_U$，都有 $w_{L_U}(P) \geq e+1$，那么对于每个满足 $U \cap H \neq \{0\}$ 的 $\mathbb{F}_{q^m}^k$ 的超平面 H，都有 $\dim^{\mathbb{F}_q}(U \cap H) \geq e+1$，再次与 (18) 矛盾。

由于 $w(c) = n-e$，根据定理 2.6，存在一个射影超平面 $\pi = \mathrm{PG}(H, \mathbb{F}_{q^m})$，使得 $w_{L_U}(\pi) = e$。由于对于任意点 $Q \in L_U$，都有 $w_{L_U}(Q) \geq e$，因此对于某个点 P，有 $\pi \cap L_U = \{P\}$。令 $\mathrm{PG}(k-3, q^m) = \mathrm{PG}(W, \mathbb{F}_{q^m})$ 为 π 中任意一个不包含 P 的射影超平面，即 $W \cap U = \{0\}$，并令 $\overline{U} = (U+W)/W$，它是商空间 $V = \mathbb{F}_{q^m}^k/W = V(2, q^m)$ 的一个 $\mathbb{F}_q$-子空间。由于 $U \cap W = \{0\}$，$L_{\overline{U}}$ 是一个秩为 n、包含于 $\mathrm{PG}(1, q^m) = \mathrm{PG}(V, \mathbb{F}_{q^m})$ 中的 $\mathbb{F}_q$-线性集，其中 $\langle (U \cap H + W)/W \rangle_{\mathbb{F}_{q^m}}$ 是一个重量为 e 的点，而所有其他点的重量均大于或等于 e。因此，根据命题 2.15

$$q^{n-e} + 1 \leq |L_{\overline{U}}| \leq \frac{q^n - 1}{q^e - 1}.$$

因此，

$$|L_{\overline{U}}| = q^{n-e} + c + 1, \quad (19)$$

对于某个整数 c，使得

$$0 \leq c \leq \frac{q^{n-e} - 1}{q^e - 1} - 1. \quad (20)$$

现在，$L_{\overline{U}}$ 的大小是与 L_U 至少有一个点相交的 $\mathrm{PG}(W, \mathbb{F}_{q^m})$ 中射影超平面的数量。$\mathrm{PG}(k-1, q^m)$ 中经过 P 的射影超平面数量为

$$\frac{q^{m(k-1)} - 1}{q^m - 1},$$

而 π 中不经过 P 的射影超平面数量为

$$\frac{q^{m(k-1)} - 1}{q^m - 1} - \frac{q^{m(k-2)} - 1}{q^m - 1} = q^{m(k-2)}.$$

将不经过 P 的 π 射影超平面记为 $\pi'_1 = \mathrm{PG}(W_1, \mathbb{F}_{q^m}) \ldots, \pi'_{q^{m(k-2)}} = \mathrm{PG}(W_{q^{m(k-2)}}, \mathbb{F}_{q^m})$，并且根据 (19)，我们可以写成

$$|L_{(U+W_i)/W_i}| = q^{n-e} + c_i + 1,$$

对于任意 i。综合以上所有信息，与 L_U 至少有一个点相交的射影超平面数量为

$$\frac{q^{m(k-1)}-1}{q^m-1}+\sum_{i=1}^{q^{m(k-2)}}(q^{n-e}+c_i)$$

也就是说

$$q^{m(k-2)+n-e}+\sum_{i=1}^{q^{m(k-2)}}c_i+\frac{q^{m(k-1)}-1}{q^m-1}.$$

因此， L_U 的外部超平面数量为

$$\frac{M(\mathcal{C})}{q^m-1}=\frac{q^{mk}-1}{q^m-1}-q^{m(k-2)+n-e}-\sum_{i=1}^{q^{m(k-2)}}c_i-\frac{q^{m(k-1)}-1}{q^m-1},$$

即,

$$\frac{M(\mathcal{C})}{q^m-1}=q^{m(k-1)}-q^{m(k-2)+n-e}-\sum_{i=1}^{q^{m(k-2)}}c_i,$$

因此，由 (20) 可得所述结论。 □

注 3.12。上述定理的界取决于第二大权重，而 $M(\mathcal{C})$ 的可能取值位于互不相交的区间内（根据 e）。此外，一旦已知 m、n、q、$M(\mathcal{C})$ 中的四个值以及第二大权重 $m-e$，便可直接由关系式 $m(k-2)+n=\lfloor\log_q(q^{m(k-1)}-M(\mathcal{C})\overline{q^m-1})\rfloor+e$ 确定剩下的一个值。

3.4 较大维数情形及 $m \le n$

本节将讨论 $n \ge m$ 的情形。与上一节一样，我们将对 $M(\mathcal{C})$ 的值给出几何解释；该值对应于计算由与 $\mathcal{C}$ 相关联的系统所定义的线性集的对偶外部点的数量。

命题 3.13. 设 $\mathcal{C}$ 是一个非退化的 $[n,k]_{q^m/q}$ 码，且 U 是任意一个相关联的系统。假设 $m \le n$。则

$$\begin{aligned}M(\mathcal{C})&=(q^m-1)|\{H=\mathrm{PG}(k-2,q^m)\colon w_{L_U}(H)=n-m\}|\\&=(q^m-1)|\mathrm{PG}(k-1,q^m)\setminus L_{U^{\perp'}}|.\end{aligned}$$

证明. 设 G 是 $\mathcal{C}$ 的一个生成矩阵，使得其列的 $\mathbb{F}_q$-张成空间为 U。那么根据 (3)，码字 $c=uG$ 具有最大重量当且仅当

$$w_{L_U}(u^\perp)=n-w(uG)=n-m,$$

因此，第一个等式成立。第二个等式由应用命题 2.16 得出。

□

现在，我们可以利用线性集的点数界，推导出 $M(\mathcal{C})$ 的界。

定理 3.14. 设 $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ 是一个非退化的 $[n,k]_{q^m/q}$ 码。假设 $m \le n$ 和$d_{k-1}^{\mathrm{rk}}(\mathcal{C}) \ge n-m+1$。那么

$$\frac{q^{km}-1}{q^m-1} - \frac{q^{km-n}-1}{q-1} \le \frac{M(\mathcal{C})}{q^m-1} \le \frac{q^{km}-1}{q^m-1} - \frac{q^k-1}{q-1}. \tag{21}$$

特别地，若 $\mathcal{C}$ 的第二大权重为 $m-e$,

$$\frac{q^{km}-1}{q^m-1} - \frac{q^{km-n}-1}{q^e-1} \le \frac{M(\mathcal{C})}{q^m-1} \le \frac{q^{km}-1}{q^m-1} - \left(q^{km-n-e} + \frac{q^{k-1}-1}{q-1}\right), \tag{22}$$

即 $km-n = \lfloor \log_q(\frac{q^{mk}-1}{q^m-1} - {}^{M}_{(\mathcal{C})}\overline{q^m-1}) \rfloor + e$。

证明。设 U 是与 $\mathcal{C}$相关联的任意系统。由命题 3.13,

$$M(\mathcal{C}) = (q^m-1)|\mathrm{PG}(k-1,q^m) \setminus L_{U^{\perp'}}|.$$

Since $L_{U^{\perp'}}$的秩为 $km-n \le (k-1)m$，并且由注 2.20，t PG$(k-1,q^m)$ hen

$$\frac{q^k-1}{q-1} \le |L_{U^{\perp'}}| \le \frac{q^{km-n}-1}{q-1}.$$

此外，若 $\mathcal{C}$中的第二大权重为 $m-e$，则这意味着存在一个点 P，使得 ${}^{w}_{L_{U^{\perp'}}}(P) = e$，并且对任意点 $Q \in L_{U^{\perp'}}$，${}^{w}_{L_{U^{\perp'}}}(Q) \ge e$，这是由 (2) 和命题 2.16 得出的。因此，由命题 2.15 可得

$$q^{km-n-e} + \frac{q^{k-1}-1}{q-1} \le |L_{U^{\perp'}}| \le \frac{q^{km-n}-1}{q^e-1}$$

于是得到 (22)。 □

注 3.15. 对于界 (22)，注 3.12 中的相同评论同样适用。

上述下界 (22) 可以在假设限制较少、但条件更复杂的情况下证明。

定理 3.16. 设 $\mathcal{C}$ 是一个非退化的 $[n,k]_{q^m/q}$ 码，并假设 $m \le n$ 和$d_{k-1}^{\mathrm{rk}}(\mathcal{C}) \ge n-m+1$。设 G' 是 $\mathcal{C}^{\perp_{\mathcal{G}}}$的任意一个生成矩阵。假设存在 $r \ge 1$个码字 $c_1,\ldots,c_r \in \mathcal{C}^{\perp_{\mathcal{G}}}\ \mathbb{F}_{q^m}$，它们线性无关，使得 $\mathbb{F}_q$-子空间

$$W = \psi_{G'}\left(\bigcap_{i=1}^{r} \mathrm{supp}(c_i)^{\perp}\right)$$

满足 $\dim^{\mathbb{F}_q}(W) = \dim^{\mathbb{F}_{q^m}}(\langle W\rangle_{\mathbb{F}_{q^m}}) = k-r$。那么

$$\frac{M(\mathcal{C})}{q^m-1} \le \frac{q^{km}-1}{q^m-1} - \left(q^{km-n-1} + \ldots + q^{km-n-k+r} + \frac{q^r-1}{q-1}\right). \tag{23}$$

证明。设 U为与 $\mathcal{C}$相关联的系统，使得 $U^{\perp'}$是由 G' 的列构成的 $\mathbb{F}_q$-张成空间。注意到 $U^{\perp'}$的维数为 $km-n$。由于 $c_i \in \mathcal{C}^{\perp_\mathcal{G}}$，对于任意 $i \in \{1,\ldots,r\}$，存在 $v_i \in \mathbb{F}_{q^m}^k$，使得 $c_i = v_i G'$，且 v_1，…，v_r 线性无关。因此，根据定理 2.9

$$W = \psi_{G'}\left(\bigcap_{i=1}^{r} \mathrm{supp}(c_i)^{\perp}\right) = (U^{\perp'} \cap v_1^{\perp}) \cap \ldots (U^{\perp'} \cap v_r^{\perp}) = U^{\perp'} \cap (v_1^{\perp} \cap \ldots \cap v_r^{\perp}),$$

并注意到 $v_1^{\perp} \cap \ldots \cap v_r^{\perp} = \langle v_1,\ldots,v_r\rangle_{\mathbb{F}_{q^m}}^{\perp}$是 $\mathbb{F}_{q^m}^k$的一个 $\mathbb{F}_{q^m}$-子空间，维数为$k-r$，与 $U^{\perp'}$相交于 W；后者是一个 $\mathbb{F}_q$-子空间，满足 $\dim^{\mathbb{F}_q}(W) = \dim^{\mathbb{F}_{q^m}}(\langle W\rangle_{\mathbb{F}_{q^m}}) = k-r$，且包含于 $L_{U^{\perp'}}$中。因此，L_W是 PG($v_1^{\perp} \cap \ldots \cap v_r^{\perp}, \mathbb{F}_{q^m}$) 中的一个典范子几何 PG($k-r-1, q$)，并且包含于 $L_{U^{\perp'}}$中。由定理 2.14 可得

$$|L_{U^{\perp'}}| \geq q^{km-n-1} + \ldots + q^{km-n-k+r} + \frac{q^r-1}{q-1}.$$

该界由命题 3.13 得出。 □

注 3.17。注意，定理 3.16 扩展了定理 3.14 中的 (22)，因为包含一个重量为 $m-1$的码字这一性质，等价于要求 $\mathcal{C}^{\perp_\mathcal{G}}$ 中存在 $k-1$ $\mathbb{F}_{q^m}$-线性无关的码字，使得

$$\dim_{\mathbb{F}_q}\left(\psi_{G'}\left(\bigcap_{i=1}^{r} \mathrm{supp}(c_i)^{\perp}\right)\right) = 1,$$

因此显然满足上述定理的假设。

注 3.18. 按照上述结果的证明，假设 $\dim^{\mathbb{F}_q}(W) = \dim^{\mathbb{F}_{q^m}}(\langle W\rangle_{\mathbb{F}_{q^m}}) = k-r$ 等价于存在一个余维为 r 的射影子空间 Ω，使得 $L_{U^{\perp'}}$ 是 Ω 的典范子几何。事实上，这使我们得以使用定理 2.14。

4 下界的等号情形

本节研究上一节所确定下界的等号情形。我们首先对 $\mathbb{F}_{q^m}^n$ 中维数二的 $\mathbb{F}_{q^m}$-线性最大秩距离码给出几何刻画，这直接源于第 2.1.2 节所述的几何对应关系。

命题 4.1. 设 $\mathcal{C}$ 是一个非退化的 $[n,2,d]_{q^m/q}$码，U 是任意一个关联系统。若 $\mathcal{C}$ 不是单纯形码，则 $\mathcal{C}$ 是最大秩距离，当且仅当 U 是一个散布子空间且 $n \leq m$。

证明。由于 $\dim_{\mathbb{F}_{q^m}}(\mathcal{C}) = 2$，根据定理 2.1，码 $\mathcal{C}$ 是最大秩距离，当且仅当 $2m = \max\{m,n\}(\min\{m,n\} - d + 1)$。若 $n \le m$，则 $d = n-1$，由 (3) 可知，这等价于要求 U 是一个散布的 $\mathbb{F}_q$-子空间。若 $m < n$，则根据 (3)，$n \mid 2m$，因此 $n = 2m$，这意味着 $U = \mathbb{F}_{q^m}^2$。 □

现在，我们可以刻画满足关于 $M(\mathcal{C})$ 的下界的维数二秩度量码。

定理 4.2. 设 $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ 是一个非退化的 $[n,2,d]_{q^m/q}$ 码，并假设 $d \ge n-m+1$。那么，$M(\mathcal{C})$ 是最小的，当且仅当 $\mathcal{C}$ 或 $\mathcal{C}^{\perp_\mathcal{G}}$ 是最大秩距离码。

证明. 设 U 是与 $\mathcal{C}$ 相关联的任意系统。首先假设 $n \le m$。$M(\mathcal{C})$ 在定理 3.2 的下界中取等号，当且仅当

$$M(\mathcal{C}) = q^{2m} - 1 - (q^m - 1)\frac{q^n - 1}{q-1},$$

即 $|L_U| = (q^n-1)/(q-1)$，也就是说，当且仅当 U 是 $\mathbb{F}_{q^m}^2$ 中一个散布的 $\mathbb{F}_q$-子空间。根据命题 4.1，这意味着 $\mathcal{C}$ 是一个最大秩距离码。现在假设 $n \ge m$。$M(\mathcal{C})$ 在定理 3.5 的下界中取等号，当且仅当

$$M(\mathcal{C}) = q^{2m} - 1 - (q^m - 1)\frac{q^{2m-n} - 1}{q-1},$$

根据 (15)，这等价于说

$$|L_{U^{\perp'}}| = \frac{q^{2m-n}-1}{q-1}.$$

由于 $L_{U^{\perp'}}$ 的秩为 $2m-n$，因此 $L_{U^{\perp'}}$ 是散布的，且 $\langle L_{U^{\perp'}} \rangle = \mathrm{PG}(1, q^m)$，所以与 $U^{\perp'}$ 相关联的任一码都是最大秩距离码。 □

当码的维数较大时，具有最少最大重量码字的秩度量码种类要比最大秩距离码族丰富得多。

定理 4.3. 设 $\mathcal{C}$ 是一个非退化的 $[n,k]_{q^m/q}$ 码，且 U 是任意一个关联系统。假设 $m \le n$。那么，$M(\mathcal{C})$ 关于 (21) 取最小值，当且仅当 $U^{\perp'}$ 是 $\mathbb{F}_{q^m}^k$ 中的一个散布的 $\mathbb{F}_q$-子空间。特别地，如果 $M(\mathcal{C})$ 取最小值，那么 $n \ge km/2$。

证明. 在这种情况下，由定理 3.14，

$$M(\mathcal{C}) = q^{km} - 1 - (q^m - 1)\frac{q^{km-n} - 1}{q-1},$$

根据命题 3.13，我们有

$$|L_{U^{\perp'}}| = \frac{q^{km-n}-1}{q-1}.$$

由于 $L_{U^{\perp'}}$ 的秩为 $km-n$，上述等式意味着 $L_{U^{\perp'}}$ 是散布的。最后一部分可通过将定理 2.11 应用于 $U^{\perp'}$ 得出。 □

如前所述，对于维数二的秩度量码，最大距离可达最大重量码字数量下界的最大秩距离码。在 $\mathbb{F}_{q^m}^n$ 中，维数为 k 且满足 $m \leq n$ 的一个 $\mathbb{F}_{q^m}$-线性最大秩距离码 $\mathcal{C}$ 的最大重量码字数量（注意，其最小距离为 $d = m - km/n + 1$）由定理 2.2 给出，即

$$M(\mathcal{C}) = \sum_{t=0}^{\frac{km}{n}-1} (-1)^{t-\frac{km}{n}+1} \begin{bmatrix} m \\ \frac{km}{n} - 1 - t \end{bmatrix}_q q^{\binom{\frac{km}{n}-1-t}{2}} (q^{n(t+1)} - 1).$$

在下一个结果中，我们证明当且仅当 $n = mk/$ 时，该值为最小值 2.

命题 4.4. 设 $\mathcal{C}$ 是一个非退化的 $[n,k]_{q^m/q}$ 最大秩距离码，并假设 $m \leq n$。那么，关于式 (21)， $M(\mathcal{C})$ 为最小值当且仅当 $n = mk/2$。

证明. 设 U 是与 $\mathcal{C}$ 相关联的任意系统。对于具有这些参数的最大秩距离码，其最小距离为 $d = m - km/n + 1$。由 (3) 可得

$$w_{L_U}(H) \leq n - (m - km/n + 1),$$

对于 PG$(k-1, q^m)$ 中的任意超平面 H，至少存在一个使等式成立的超平面。由命题 2.16,

$$w_{L_{U^{\perp'}}}(P) \leq km - n - m(k-1) + n - (m - km/n + 1) = \frac{km}{n} - 1,$$

对于 PG$(k-1, q^m)$ 中的任意点 $P \in$。由定理 4.3， $M(\mathcal{C})$ 为最小值当且仅当 $L_{U^{\perp'}}$ 是散布的，而这当且仅当 $\frac{km}{n} - 1 = 1$，即 $n = km/2$。 □

若 $n = mk/2$，所有具有最大重量码字且码字数最少的码都是最大秩距离码。

命题 4.5. 设 $\mathcal{C}$ 是一个非退化的 $[n,k]_{q^m/q}$ 码，并假设 $n = mk/2$。那么， $M(\mathcal{C})$ 关于 (21) 取最小值，当且仅当 $\mathcal{C}$ 是最大秩距离码。

证明。设 U 是与 $\mathcal{C}$ 关联的任意系统。根据定理 4.3， $M(\mathcal{C})$ 取最小值，当且仅当 $L_{U^{\perp'}}$ 是散布的。由于 $L_{U^{\perp'}}$ 的秩为 $km/2$ ，根据命题 2.17，线性集 L_U 也散布。因此，根据 [19, 定理 3.2], , 码 $\mathcal{C}$ 是最大秩距离码。反向结论由上述命题得出。 □

注 4.6. 命题 4.5 中参数取值下的最大秩距离码，与 PG$(k-1, q^m)$ 中的最大散布 $\mathbb{F}_q$-线性集（$\mathbb{F}_q$-子空间）相对应（在 $\mathbb{F}_{q^m}^k$ 中），参见 *[39,* 定理 4.*8]*，另见 *[31, 47]*。当 mk 为偶数时，对于任意取值的 q、m、k，这类子空间都存在，已有一系列论文证明了这一点 *[10, 11, 15, 19]*。

正如我们将在下一个备注中讨论的，并非所有散布空间都能产生最大秩距离码，因此无法将定理 4.2 推广到更大的维数。

备注 4.7。考虑 $W = \{(x, x^q, a) : x \in \mathbb{F}_{q^m}, a \in \mathbb{F}_q\} \subseteq \mathbb{F}_{q^m}^3$，其中 $m \geq 2$。结果表明，它是一个维数为 $m+1$ 的散布 $\mathbb{F}_q$-子空间（并且 L_W 定义了 PG$(2, q^m)$ 中一个 R´edei 型阻塞集）。接着选择 $U = W^{\perp'}$，使得 $\dim^{\mathbb{F}_q}(U) = 2m-1$。于是 $\langle U\rangle_{\mathbb{F}_{q^m}} = \mathbb{F}_{q^m}^3$，否则根据命题 2.16，将存在一个点 $P \in$ PG$(2, q^m)$，使得 $w_{L_W}(P) = m$，这与 W 是散布的这一事实矛盾。然后我们可以考虑与 U 相关联的一个 $[2m-1, 3]_{q^m/q}$ 秩度量码 $\mathcal{C}$，并且 $M(\mathcal{C})$ 是最小的，因为 $U^{\perp'} = W$ 是散布的（参见定理 4.3）。$\mathcal{C}$ 的最小距离为

$$d = 2m - 1 - \max\{w_{L_U}(H) \colon H = \mathrm{PG}(1, q^m)\}$$

$$= m - \max\{w_{L_W}(P) \colon P \in \mathrm{PG}(2, q^m)\} = m - 1,$$

再次利用命题 2.16。容易看出，码 $\mathcal{C}$ 不是最大秩距离码，因为其参数不满足式 (1) 中的等式。

备注 4.8. 在定理 3.3 中，我们还给出了另一个下界，该下界取决于一个 2 维 $\mathbb{F}_{q^m}$-线性非退化秩度量码的第二小重量。达到此下界等号的码的例子包括与散布的 $\mathbb{F}_{q^e}$-线性集 L_U 在 PG$(1, q^m)$ 中的对偶相关联的码，其中 $e \mid m$。遗憾的是，我们不知道这是否是唯一的情形。

我们分析定理 3.9 中下界取等号的情形。首先，我们证明关于子几何外部点的一个性质。

引理 4.9. 设 $\Sigma =$ PG$(k-1, q)$ 是 PG$(k-1, q^m)$ 中的典范子几何 PG$(k-1, q)$，并假设 $3 \leq k \leq m$。那么，对于每个点 $P \in$ PG$(k-1, q^m) \setminus \Sigma$，对每个 $r \in \{0, \ldots, k-2\}$，都存在一个经过 P 的 r-维空间与 Σ 恰好交于一点。特别地，存在一个经过 P 且与 Σ 相切的超平面。

证明。设 $P = \langle v\rangle_{\mathbb{F}_{q^m}} \in$ PG$(k-1, q^m) =$ PG$(V, \mathbb{F}_{q^m}) \setminus \Sigma$。我们将对 r 进行归纳证明。设 $\Sigma = L_W$，其中 W 是 V 的一个 k 维 $\mathbb{F}_q$ 子空间，且满足 $\langle W\rangle_{\mathbb{F}_{q^m}} = V$。反设所有经过 P 的直线要么是外部直线，要么与 Σ 至少交于 $q+1$ 个点。考虑 PG$(V/\langle v\rangle_{\mathbb{F}_{q^m}}, \mathbb{F}_{q^m})$ 中由 $W' = W + \langle v\rangle_{\mathbb{F}_{q^m}}/\langle v\rangle_{\mathbb{F}_{q^m}} \subseteq V/\langle v\rangle_{\mathbb{F}_{q^m}}$ 定义的 $\mathbb{F}_q$ 线性集 $L_{W'} =$ PG$(k-2, q^m)$。由于 $P \notin \Sigma$，因此 $L_{W'}$ 的秩为 k。此外，由于每条经过 P 且与 Σ 至少交于一个点的直线，其重量至少为 2，因此对每个 $P' \in L_{W'}$，都有 $w_{L_{W'}}(P') \geq 2$。此外，由于 L_W 张成 PG$(k-1, q^m)$，因此 $L_{W'}$ 也张成 PG$(k-2, q^m)$。于是由 (10) 得到 $k \geq 2(k-1)$，矛盾。因此该命题对 $r = 1$ 成立。现在假设我们的断言对 $r-1$ 成立，并证明它对 r 成立。根据假设，存在一个经过 P 的 $(r-1)$ 维空间 Ω，与 Σ 恰好交于一点 Q。假设每个经过 Ω 的 r 空间都与 Σ 至少还交于一个不同于 Q 的点。那么

$$q\frac{q^{m(k-r)}-1}{q^m-1} + 1 \leq \frac{q^k-1}{q-1},$$

这就与 $k \leq m$ 矛盾。 □

现在我们将使用上述几何引理，证明定理 3.9 中下界的等号情形。

定理 4.10. 设 $\mathcal{C}$ 是一个非退化的 $[n,k]_{q^m/q}$ 码。假设 $n<m$ 和

$$M(\mathcal{C})=(q^{mk}-1)-\frac{q^n-1}{q-1}(q^{(k-1)m}-1)+q(q^m-1)\beta,$$

其中

$$\beta=\frac{q^{mk}-1}{q^m-1}-\prod_{i=1}^{k-1}(q^m-q^i)-\frac{q^k-1}{q-1}\prod_{i=1}^{k-2}(q^m-q^i).$$

则 $n=k$ 和 $\mathcal{C}=\mathbb{F}_{q^m}^k$。

证明。设 U 是与 $\mathcal{C}$ 相关联的任意一个系统。与定理 3.9 的证明类似，记 τ_0、τ_1 和 τ_s 分别为 PG($k-1,q^m$) 中与 L_U 相交于 0 个、1 个和至少 2 个点的超平面数，并设 W 是 U 的一个 $\mathbb{F}_q$-子空间，使得 $L_W=$ PG($k-1,q$)。根据假设及 (3),

$$\tau_0=\frac{q^{mk}-1}{q^m-1}-\frac{q^n-1}{q-1}\frac{q^{(k-1)m}-1}{q^m-1}+q\beta,$$

因此，在 (17) 中等号成立：

$$\tau_1+\tau_s=|L_U|\frac{q^{(k-1)m}-1}{q^m-1}-q\tau_s=\frac{q^n-1}{q-1}\frac{q^{(k-1)m}-1}{q^m-1}-q\beta.$$

上述等式意味着

$$\frac{q^{(k-1)m}-1}{q^m-1}\left(|L_U|-\frac{q^n-1}{q-1}\right)-q(\tau_s-\beta)=0,$$

因此 $|L_U|=\frac{q^n-1}{q-1}$和 $\beta=\tau_s$。假设存在一个点 $P\in L_U\setminus L_W$。由引理 4.9，存在 PG($k-1,q^m$) 中经过 P的超平面 π，它与 L_W恰好交于一点。因此，π 是 L_U 的割线，却是 L_W的切线，这与 $\tau_s=\beta$矛盾。因此$L_U=L_W$，断言得证。

□

5 上界中的等号情形

$M(\mathcal{C})$的最大值可取，当且仅当 $\mathcal{C}$ 或其几何对偶是整个空间。

定理 5.1. 设 $\mathcal{C}$ 是一个非退化的 $[n,k]_{q^m/q}$ 码，并假设 $d_{k-1}^{\mathrm{rk}}(\mathcal{C})\geq n-m+1$。

- 若 $n<m$，则 $M(\mathcal{C})$ 关于 (16) 取最大值，当且仅当 $n=k$ 且$\mathcal{C}=\mathbb{F}_{q^m}^k$。

• 若 $n \geq m$，则 $M(\mathcal{C})$ 关于 (21) 取最大值，当且仅当 $n = mk - k$ 且$\mathcal{C}^{\perp_{\mathcal{G}}} = \mathbb{F}_{q^m}^k$。

证明。设 U 是与 $\mathcal{C}$ 相关联的任意系统。先假设 $n < m$ 和 $k = 2$，则由定理 3.2，$M(\mathcal{C})$ 取最大值当且仅当 L_U 的大小为 $q+1$；如前所述，这等价于要求 $\mathcal{C}$ 是 $\mathbb{F}_{q^m}^2$。若 $k > 2$，则由定理 3.9 M，$\mathcal{C}$(M) 取最大值当且仅当 $\mathcal{C} = \prod_{i=0}^{n-1}(q^m - q^i)$。设 $k < n$，则

$$M(\mathcal{C}) > \prod_{i=0}^{k-1}(q^m - q^i),$$

也就是说，根据注 3.10 和命题 3.13，L_U 的外部超平面数大于 L_W 的外部超平面数，其中 L_W 是包含于 L_U 中的典范子几何。由于 $L_W \subseteq L_U$，这就产生矛盾。因此 $k = n$，并由此得到所述结论。设 $n \geq m$。由 (21) 和命题 3.13 可知，$L_{U^{\perp'}}$ 的大小为 $\frac{q^k-1}{q-1}$。根据引理 3.2], $[1,$, PG$(k-1,q)$ 是 PG$(k-1,q^m)$ 的典范子几何，且 $\dim^{\mathbb{F}_q}(U^{\perp'}) = k$。因此，$\dim^{\mathbb{F}_{q^m}}(\mathcal{C}^{\perp_{\mathcal{G}}}) = k$，即 $\mathcal{C}^{\perp_{\mathcal{G}}} = \mathbb{F}_{q^m}^k$。 □

我们还可以刻画定理 3.16 中的等号情形。

命题 5.2. 设 $\mathcal{C}$ 是一个非退化的 $[n,k]_{q^m/q}$ 码，并假设 $m \leq n$ 和 $d_{k-1}^{\mathrm{rk}}(\mathcal{C}) \geq n - m + 1$。设 G' 是 $\mathcal{C}^{\perp_{\mathcal{G}}}$ 的任意生成矩阵。假设存在 $r > 1$ 个码字 c_1，……，$c_r \in \mathcal{C}^{\perp_{\mathcal{G}}}$ $\mathbb{F}_{q^m}$-线性无关，使得

$$W = \psi_{G'}\left(\bigcap_{i=1}^{r} \mathrm{supp}(c_i)^{\perp}\right)$$

满足 $\dim^{\mathbb{F}_q}(W) = \dim^{\mathbb{F}_{q^m}}(\langle W\rangle_{\mathbb{F}_{q^m}}) = k - r$，且

$$M(\mathcal{C}) = q^{km} - 1 - (q^m - 1)\left(q^{km-n} + \ldots + q^{km-n-k+r} + \frac{q^r - 1}{q-1}\right).$$

那么 $n = mk - k$ 和 $\mathcal{C}^{\perp_{\mathcal{G}}} = \mathbb{F}_{q^m}^k$。

证明. 设 U 是与 $\mathcal{C}$ 相关联的任意系统。那么

$$M(\mathcal{C}) = (q^m - 1)|\mathrm{PG}(k-1,q^m) \setminus L_{U^{\perp'}}|,$$

因此

$$|L_{U^{\perp'}}| = q^{km-n-1} + \ldots + q^{km-n-k+r} + \frac{q^r - 1}{q-1}.$$

仿照定理 3.16 的证明，存在一个 $\mathbb{F}_{q^m}$-子空间 S，它是 $\mathbb{F}_{q^m}^k$ 的维数为$k - r < k - 1$的子空间，使得 $L_{W\cap U^{\perp'}}$是 PG$(W,\mathbb{F}_{q^m})$ 中的典范子几何，因此$L_{U^{\perp'}}$ 满足定理 2.14 的假设，且取下界等号；进而由定理 2.14 的第二部分可得$L_{U^{\perp'}} = $ PG$(k-1,q)$。 □

下面我们将研究这样一种情形：在某些假设下， $M(\mathcal{C})$ 的上界得到了改进。此时情况要复杂得多，而且似乎很难给出一般性的完整答案。事实上，对于这种情形，我们将展示一些例子，这些例子表明要对其进行完整分类并不容易。

我们先介绍一些码的构造。

构造 5.3. 设 $\lambda \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$ 是生成 $\mathbb{F}_{q^m}$ 的一个元素，并且

$$G = \begin{pmatrix} 1 & \lambda & \dots & \lambda^{t_1-1} & 0 & \dots & & & & & 0 \\ 0 & 0 & \dots & 0 & 1 & \lambda & \dots & \lambda^{t_2-1} & 0 & \dots & 0 \\ \vdots & & & & & & & & \ddots & & \\ 0 & \dots & & & & & & & 0 & 1 \dots & \lambda^{t_k-1} \end{pmatrix} \in \mathbb{F}_{q^m}^{k \times (t_1+\dots+t_k)}.$$

设 $\mathcal{C}_{\lambda,\ t_1,\ \dots\dots,\ t_k}$ 是 $\mathbb{F}_{q^m}^{t_1+\dots+t_k}$ 上维数为 k 、以 G 为生成矩阵的 $\mathbb{F}_{q^m}$-线性秩度量码。

现在我们确定这些码的参数。

定理 5.4. 设 $\lambda \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$ 是生成 $\mathbb{F}_{q^m}$ 的一个元素，并设 $\mathcal{C}_{\lambda,\ t_1,\ \dots\dots,\ t_k}$ 如构造 5.3 中所述。假设 $t_1 \le t_2 \le \dots \le t_k \le m-1$。那么 $\mathcal{C}_{\lambda,\ t_1,\ \dots\dots,\ t_k}$ 是一个 $[t_1+\dots+t_k, k, t_1]_{q^m/q}$ 码。此外，若 $k=2$，则

- 构造 5.3 中 G 的第一行，其非零 $\mathbb{F}_{q^m}$-成比例向量的重量为 t_1;
- 重量为 t_2 的码字数量（不同于上一项中的码字）为 $q^{t_2-t_1+1}(q^m-1)$;

对于任意 $i \in \{1, \dots, t_1-1\}$，$\mathcal{C}_\lambda$ 中重量为 $\min\{m,n\}-i$ 的码字数量为 $(q^m-1)(q^{n-2i+1}-q^{n-2i-1})$。

证明。 由于 G的结构，显然 $\mathcal{C}_{\lambda,t_1,\dots,t_k}$的长度为 $n = t_1+\dots+t_k$，其维数为 k。考虑与 $\mathcal{C}_{\lambda,t_1,\dots,t_k}$ 相关联的以下系统

$$U = S_1 \times \dots \times S_k = \langle 1, \lambda, \dots, \lambda^{t_1-1} \rangle_{\mathbb{F}_q} \times \dots \times \langle 1, \lambda, \dots, \lambda^{t_k-1} \rangle_{\mathbb{F}_q}.$$

为了确定该码的重量分布，我们需要确定 L_U 相对于超平面的重量分布。为此，我们将考虑其对偶，并根据其对偶中点的重量分布还原该分布。考虑

$$\sigma\colon ((u_1,\dots,u_k),(v_1,\dots,v_k)) \in (\mathbb{F}_{q^m}^k)^2 \mapsto u_1v_1+\dots+u_kv_k \in \mathbb{F}_{q^m},$$

以这种方式

$$\sigma'\colon ((u_1,\dots,u_k),(v_1,\dots,v_k)) \in (\mathbb{F}_{q^m}^k)^2 \mapsto \mathrm{Tr}_{q^m/q}(u_1v_1+\dots+u_kv_k) \in \mathbb{F}_q.$$

记为

$$\overline{S}_i = \{a \in \mathbb{F}_{q^m} \colon \mathrm{Tr}_{q^m/q}(ab) = 0,\ \forall b \in S_i\},$$

对于任意 $i \in \{1, \ldots, k\}$。容易看出 $U^{\perp'} = \overline{S}_1 \times \ldots \times \overline{S}_k$。根据 [34, 命题 2.9]，存在 $\alpha \in \mathbb{F}_{q^m}^*$ 使得

$$\overline{S}_i = \alpha\langle 1, \lambda, \ldots, \lambda^{m-t_i-1}\rangle_{\mathbb{F}_q},$$

对于 $i \in \{1, \ldots, k\}$。因此，$U^{\perp'}$ 是 $\mathbb{F}_q$ 的一个维数为 $km - n$ 的子空间，它在 GL(k, q^m) 作用下与 W 等价，其中

$$W = \langle 1, \lambda, \ldots, \lambda^{m-t_1-1}\rangle_{\mathbb{F}_q} \times \ldots \times \langle 1, \lambda, \ldots, \lambda^{m-t_k-1}\rangle_{\mathbb{F}_q}.$$

因此，$L_{U^{\perp'}}$ 和 L_W 的重量分布相同。所以，根据注 2.10

$$\max\{w_{L_{U^{\perp'}}}(P) \colon P \in \mathrm{PG}(k-1, q^m)\} = \max\{w_{L_W}(P) \colon P \in \mathrm{PG}(k-1, q^m)\} = m - t_1,$$

因此，根据命题 2.16，我们有

$$\max\{w_{L_U}(H) \colon H = \mathrm{PG}(k-2, q^m) \subset \mathrm{PG}(k-1, q^m)\} = m - t_1 + n - m = t_2 + \ldots + t_k$$

因此，可以通过定理 2.6 确定最小距离。当 $k = 2$ 和$n \leq m$时，根据定理 2.6，可以利用定理 2.13 中线性集的重量分布来确定该码的重量分布。如果 $n \geq m$ ，我们可以像之前一样利用对偶性进行论证，使得 U 的对偶满足定理 2.13 的假设。 □

注 5.5. 对于更一般的维数，在假设任意$i \neq j$都满足 $t_1 + \ldots + t_k \geq m$ 和 $t_i + t_j \geq m - 1$ 的条件下，可以利用上述定理证明中的对偶性以及 *[29,* 定理 2.*17]*（另见 *[1,*注 4.*3]*）来确定该码的重量分布。

注 5.6. 构造 5.3 中的码族在关于 σ 取几何对偶的运算下封闭，这与定理 5.4 的证明类似。更确切地说，$\mathcal{C}_{\lambda,t_1,\ldots,t_k}^{\perp_\mathcal{G}}$等价于$\mathcal{C}_{\lambda,m-t_1,\ldots,m-t_k}$。

我们先证明构造 5.3 中维数为 2 的例子在 $M(\mathcal{C})$下取得最大值。

定理 5.7. 设 $\lambda \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$ 是生成 $\mathbb{F}_{q^m}$的一个元素。码$\mathcal{C}_{\lambda,t_1,t_2} \subseteq \mathbb{F}_{q^m}^n$，其中 $n = t_1 + t_2$ 且 $3 \leq n \leq 2m - 3$，含有一个重量为 $\min\{m, n\} - 1$ 的码字，并且$\mathcal{C}_{\lambda,t_1,t_2}$在具有重量为 $\min\{m, n\} - 1$的码字的 $[n, 2]_{q^m/q}$码中，使 $M(\mathcal{C}_{\lambda,t_1,t_2})$达到最大值。

证明。 考虑与以下内容相关的系统 $\mathcal{C}_{\lambda,t_1,t_2}$

$$U = S_1 \times S_2 = \langle 1, \lambda, \ldots, \lambda^{t_1-1}\rangle_{\mathbb{F}_q} \times \langle 1, \lambda, \ldots, \lambda^{t_2-1}\rangle_{\mathbb{F}_q}.$$

假设 $n \le m$ 那么 $t_1 + t_2 \le m$ 和 L_U 是一个秩为 n 的 $\mathbb{F}_q$-线性集，其形式如定理 2.13 所示，这意味着 $|L_U| = q^{n-1} + 1$ 和 L_U 有 $q^{n-1} - q^{n-3} \ge 1$ 个权为一的点。根据 (2)，后一个事实可表述为 $\mathcal{C}_{\lambda,\ t_1,\ t_2}$ 至少有一个重量为 $n-1$的码字，并且根据命题 3.1

$$M(\mathcal{C}_{\lambda,t_1,t_2}) = q^{2m} - 1 - (q^m - 1)(q^{n-1} + 1),$$

也就是说，等式 (13) 成立。现在，假设 $n > m$ ，并考虑证明定理 5.4 中的 $U^{\perp'}$。因此，我们有 $U^{\perp'}$ 是 $\mathbb{F}_q$ 的一个维数为 $2m-n$ 的子空间，包含于 $\mathbb{F}_{q^m}^2$ 中，且与 W 在 GL(2, q^m) 的作用下等价，其中

$$W = \langle 1, \lambda, \ldots, \lambda^{m-t_1-1} \rangle_{\mathbb{F}_q} \times \langle 1, \lambda, \ldots, \lambda^{m-t_2-1} \rangle_{\mathbb{F}_q}.$$

因此，$|L_{U^{\perp'}}| = |L_W|$。我们再次对 L_W 应用定理 2.13，得到 $L_{U^{\perp'}}$ 有 $q^{2m-n-1} - q^{2m-n-3} \ge 1$ 个权为一的点，且大小为 $q^{2m-n-1} + 1$。结合命题 2.16 和 (2)，我们有 $\mathcal{C}_{\lambda,\ t_1,\ t_2}$ 至少有一个重量为 $m-1$ 的码字。由 (15)，我们有

$$M(\mathcal{C}_{\lambda,t_1,t_2}) = q^{2m} - 1 - (q^m - 1)(q^{2m-n-1} + 1),$$

也就是说，定理 3.5 中的 (14) 式取等号。 □

在一定假设下，上述结果可以推广到更高维数。

定理 5.8。设 $\lambda \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$ 是生成 $\mathbb{F}_{q^m}$ 的元素。考虑码 $\mathcal{C}_{\lambda,\ t_1,\ldots,t_k} \subseteq \mathbb{F}_{q^m}^n$，其中 $n = t_1 + \ldots + t_k$、$m \le n$ 和 $km - n \le m + k$。设 $\{m - t_1 - 1,\ \ldots,\ m - t_k - 1\} = \{s_{i_1}, \ldots, s_{i_\ell}\}$，且 $s_{i_1} > \ldots > s_{i_\ell}$。那么，若满足以下任一条件

$$k \le \sum_{j=1}^{\ell} \frac{q^{s_{i_j}} - 2q^{s_{i_j}/2}}{s_{i_j}}$$

or

$$mk - k - t_1 - \ldots - t_k \le q,$$

码 $\mathcal{C}_{\lambda,\ t_1,\ldots,t_k}$ 满足定理 3.16 关于 $r = 1$ 的假设，并且在满足定理 3.16 关于 $r = 1$ 的假设的 $[n,k]_{q^m/q}$码中，$M(\mathcal{C}_{\lambda,\ t_1,\ldots,t_k})$ 达到最大值。

证明。与二维情形一样，与 $\mathcal{C}_{\lambda,\ t_1,\ldots,t_k}$ 相关联的系统为

$$U = S_1 \times \ldots \times S_k = \langle 1, \lambda, \ldots, \lambda^{t_1-1} \rangle_{\mathbb{F}_q} \times \ldots \times \langle 1, \lambda, \ldots, \lambda^{t_k-1} \rangle_{\mathbb{F}_q}.$$

考虑定理 5.4 的证明中的 $U^{\perp'}$。因此，我们有 $U^{\perp'}$ 是 $\mathbb{F}_m^k$ 中一个维数为 $km-n$ 的 $\mathbb{F}_q$-子空间，且在 GL(k, q^m) 作用下等价于 W，其中

$$W = \langle 1, \lambda, \ldots, \lambda^{m-t_1-1} \rangle_{\mathbb{F}_q} \times \ldots \times \langle 1, \lambda, \ldots, \lambda^{m-t_k-1} \rangle_{\mathbb{F}_q}.$$

根据 [1, 定理 4.5、命题 4.6、注 4.7], ，存在一个超平面 H ，使得$L_W \cap H = \mathrm{PG}(k-2, q)$, 因此存在一个码字属于与陈述中所述 $\mathcal{C}^{\perp_\mathcal{G}}$ 等价的码，也因此属于 $\mathcal{C}^{\perp_\mathcal{G}}$。 [1, 定理 4.5] ，并结合 [1, 命题 4.6] 和 [1,推论 4.8] ，还可推出

$$|L_W| = |L_{U^{\perp'}}| = q^{km-n-1} + \ldots + q^{km-n-k+1} + 1,$$

这意味着，根据 (23)， $r = 1$、 M（$\mathcal{C}_{\lambda,\ t_1,\ \ldots\ldots t_k}$）是最大值。 □

注 5.9。特别是，如果 $t_1 \geq \ldots \geq t_k$ 且

$$k \leq \frac{q^{m-t_1-1} - 2q^{\frac{m-t_1-1}{2}}}{m - t_k - 1}$$

满足定理 5.8 的假设。

注 5.10。利用 *[1,* 命题 4.*9]* 并假设 $t_0 \leq \ldots \leq t_k$，还可以证明，将假设 $km - n \leq m + k$ 替换为 $3m - t_0 - t_{k-1} - t_k \leq m + 2$、$\mathcal{C}_{\lambda,\ t_1,\ \ldots\ldots t_k}$满足定理 3.16 的假设，其中 $r = k - 1$且 M（$\mathcal{C}_{\lambda,\ t_1,\ \ldots\ldots t_k}$）也是具有此性质的码中的最大值。

当 m 是素数且 $k = 2$时，只要要求存在足够多具有某一重量的码字，我们就可以利用 [34] 中的结果，对达到 M（$\mathcal{C}$）最大值的码给出刻画。这些结果的关键是 Cauchy-Davenport 不等式的线性类比和 Vosper 定理，见 [7, 8]。

定理 5.11. 设 $\mathcal{C}$ 是一个非退化的 $[n, 2]_{q^m/q}$ 码，且假设 m 是素数。记 A_i 为 $\mathcal{C}$中重量为 $i \in \{0, \ldots, \min\{m, n\}\}$ 的码字数量。假设以下条件之一成立：

- $n \leq m$，存在两个在 $\mathcal{C}$ 中不成 $\mathbb{F}_{q^m}$比例的码字，其重量分别为 r 和 $n - r$（其中 $r \leq n - r$），且 $A_{n-r} \geq (q^m - 1)(q^{n-2r} + 2)$;
- $n > m$，存在两个在 $\mathcal{C}$ 中不成 $\mathbb{F}_{q^m}$比例的码字，其重量分别为 $m + r - n$ 和$m - r$（其中 $r \leq n - r$），且 $A_{m-r} \geq (q^m - 1)(q^{2m-n-2r} + 2)$。

那么 $\mathcal{C}$ 等价于构造 5.3 中的码，因此在至少含有一个重量为 $\min\{m, n\} - 1$的码字的非退化 $[n, 2]_{q^m/q}$码中，它使 $M(\mathcal{C})$达到最大值。

证明。令 U 为与 $\mathcal{C}$ 相关联的任意系统。假设 $n \leq m$，那么根据 (2)，存在 $\mathrm{PG}(1, q^m)$ 中两个不同点 P 和 Q，使得 $w_{L_U}(P) = n - r$ 且 $w_{L_U}(Q) = r$。此外，根据关于 A_{n-r} 的假设以及 (2)，可知 L_U 中重量为 r 的点数至少为

$$q^{n-2r} + 2.$$

因此，现在可以应用 [34, 定理 3.12]，由此可知 U 与以下对象 GL(2, q^m)-等价:

$$\langle 1, \lambda, \ldots, \lambda^{n-r-1} \rangle_{\mathbb{F}_q} \times \langle 1, \lambda, \ldots, \lambda^{r-1} \rangle_{\mathbb{F}_q},$$

对于某个 $\lambda \in \mathbb{F}_{q^m} \backslash \mathbb{F}_q$，因此 $\mathcal{C}$等价于 $\mathcal{C}_{\lambda,\ n-r,\ r}$。假设 $n > m$并考虑 $U^{\perp'}$。根据这些假设、(2) 和命题 2.16，存在 PG(1, q^m) 中两个不同点P和 Q，使得 ${}^{w}L_{U^{\perp'}}(P) = n-r$且 ${}^{w}L_{U^{\perp'}}(Q) = r$，$L_{U^{\perp'}}$ 中重量为 r 的点数至少为

$$q^{2m-n-2r} + 2.$$

由于 $L_{U^{\perp'}}$的秩为 $2m-n$，我们可以应用 [34, 定理 3.12]，从而得到 $U^{\perp'}$ 与以下对象在 GL(2, q^m) 下等价:

$$\langle 1, \lambda, \ldots, \lambda^{n-r-1} \rangle_{\mathbb{F}_q} \times \langle 1, \lambda, \ldots, \lambda^{r-1} \rangle_{\mathbb{F}_q},$$

对于某个 $\lambda \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$。那么 U与 $S \times T$在 GL(2, q^m) 下等价，其中

$$S = \{a \in \mathbb{F}_{q^m} : \mathrm{Tr}_{q^m/q}(ab) = 0, \forall b \in \langle 1, \lambda, \ldots, \lambda^{n-r-1} \rangle_{\mathbb{F}_q}\}$$

and

$$T = \{a \in \mathbb{F}_{q^m} : \mathrm{Tr}_{q^m/q}(ab) = 0, \forall b \in \langle 1, \lambda, \ldots, \lambda^{r-1} \rangle_{\mathbb{F}_q}\}.$$

根据 [35, 推论 2.7]，$S \times T$与以下对象在 GL(2, q^m) 下等价:

$$\langle 1, \lambda, \ldots, \lambda^{m-n+r-1} \rangle_{\mathbb{F}_q} \times \langle 1, \lambda, \ldots, \lambda^{m-r-1} \rangle_{\mathbb{F}_q}.$$

因此，根据定理 2.7 $\mathcal{C}$ 等价于 $\mathcal{C}_{\lambda,m-n+r,m-r}$。
最后一部分由定理 5.7 得出。 □

当 m 不是素数时，对于定理 3.16 中的上界，也存在其他非等价的码，其 $M(\mathcal{C})$ 达到最大值。

构造 5.12。设 $m = \ell' t$。令 $\mu \in \mathbb{F}_{q^m}$ 满足 $\mathbb{F}_{q^t} = \mathbb{F}_q(\mu)$，$\overline{S}$ 为 $\mathbb{F}_{q^m}$的一个 $\mathbb{F}_{q^t}$-子空间，其维数为 $\ell < \ell'$，且满足 $1 \notin \overline{S}$和 $\overline{S} \cap \mathbb{F}_{q^t} = \{0\}$。令 $t_1, \ldots, t_k$为正整数，满足 $t_i + t_j \leq t+1$，对每个 $i \neq j$均成立。对于 $c_1, \ldots, c_{\ell t}$，取 $\overline{S}$的一个 $\mathbb{F}_q$-基，考虑

$$G = \begin{pmatrix} c_1 & \ldots & c_{\ell t} & 1 & \mu & \ldots & \mu^{t_1-1} & 0 & \cdots & & & & & 0 \\ 0 & \ldots & & \ldots & & \ldots & 0 & 1 & \mu & \ldots & \mu^{t_2-1} & 0 & \ldots & 0 \\ \vdots & & & & & & & & & & & \ddots & & \\ 0 & \ldots & & & & & & & & & & 0 & 1 \ \ldots & \mu^{t_k-1} \end{pmatrix} \in \mathbb{F}_{q^m}^{k \times n},$$

其中 $n = \ell t + t_1 + \ldots + t_k$。定义 $\mathcal{C}_{\overline{S},\mu,t_1,\ldots,t_k}$为 $\mathbb{F}_{q^m}^n$中的 $\mathbb{F}_{q^m}$-线性秩度量码，其生成矩阵为 G 。

上述构造的参数如下。

定理 5.13. 设 $\mathcal{C}_{\overline{S},\ \mu,\ t_1,\ \ldots,\ t_k} \subseteq \mathbb{F}_{q^m}^n$ 如构造 5.12 中所述。则 $\mathcal{C}_{\overline{S},\ \mu,\ t_1,\ \ldots,\ t_k}$ 是一个非退化 $[n,k,t_j]_{q^m/q}$码，其中 $t_j = \min\{t_i\colon\ i>1\}$，且 $\mathcal{C}_{\overline{S}}^{\perp_{\mathcal{G}},\ \mu,\ t_1,\ \ldots,\ t_k}$ 是一个非退化的 $[km-n,k,t(\ell'-\ell)\ -t_1]_{q^m/q}$码。

在 $k=2$ 且 $n\le m$的情况下，构造 5.12 中 G 的第二行及其非零的 $\mathbb{F}_{q^m}$-比例向量恰好是所有重量为 t_2的码字。并且若 $t_1\ge t_2$，则

- $\mathcal{C}_{\overline{S}、\ \mu、\ t_1、\ \ldots、\ t_k}$ 中重量为 $n-t_2$ 的码字数量为 $q^{\ell t+t_1-t_2+1}(q^m-1)$;
- $\mathcal{C}_{\overline{S}、\ \mu、\ t_1、\ \ldots、\ t_k}$ 中重量为 $n-i$ 的码字数量为 $(q^m-1)(q^{n-2i+1}-q^{n-2i-1})$，对任意 $i\in\{1,\ldots,t_2-1\}$均成立。

若 $t_1<t_2$，则

- $\mathcal{C}_{\overline{S}、\ \mu、\ t_1、\ \ldots、\ t_k}$ 中重量为 $\ell t+t_1$ 的码字数量为 $q^{\ell t}(q^m-1)$;
- $\mathcal{C}_{\overline{S}、\ \mu、\ t_1、\ \ldots、\ t_k}$ 中重量为 $\ell t+t_2$ 的码字数量为 $(q^{\ell t+t_2-t_1+1}-q^{\ell t})(q^m-1)$;
- 重量为 $n-i$ 的码字数目，在 $\mathcal{C}_{\overline{S},\mu,t_1,\ldots,t_k}$ 中为 $(q^m-1)(q^{n-2i+1}-q^{n-2i-1})$，对任意 $i\in\{1,\ldots,t_1-1\}$均成立。

证明。与 $\mathcal{C}_{\overline{S},\mu,t_1,\ldots,t_k}$ 相关联的系统为

$$U=(\overline{S}\oplus\langle 1,\mu,\ldots,\mu^{t_1-1}\rangle_{\mathbb{F}_q})\times\ldots\times\langle 1,\mu,\ldots,\mu^{t_k-1}\rangle_{\mathbb{F}_q}.$$

设 $U_1=\overline{S}\oplus\langle 1,\mu,\ldots,\mu^{t_1-1}\rangle_{\mathbb{F}_q}$和 $U_i=\langle 1,\mu,\ldots,\mu^{t_i-1}\rangle_{\mathbb{F}_q}$，其中 $i>1$。如定理 5.4 中所述，考虑

$$\sigma\colon((u_1,\ldots,u_k),(v_1,\ldots,v_k))\in(\mathbb{F}_{q^m}^k)^2\mapsto u_1v_1+\ldots+u_kv_k\in\mathbb{F}_{q^m},$$

因此

$$\sigma'\colon((u_1,\ldots,u_k),(v_1,\ldots,v_k))\in(\mathbb{F}_{q^m}^k)^2\mapsto \mathrm{Tr}_{q^m/q}(u_1v_1+\ldots+u_kv_k)\in\mathbb{F}_q.$$

记为

$$\overline{U}_i=\{a\in\mathbb{F}_{q^m}\colon \mathrm{Tr}_{q^m/q}(ab)=0,\ \forall b\in U_i\},$$

对任意 $i\in\{1,\ldots,k\}$均成立。显然，对每个 $i>1$，$\dim^{\mathbb{F}_q}(\overline{U}_1)=m-\ell t-t_1$，$\dim^{\mathbb{F}_q}(\overline{U}_i)=m-t_i$。此外，容易看出 $U^{\perp'}=\overline{U}_1\times\ldots\times\overline{U}_k$。因此，由命题 2.16 可得

$$\max\{w_{L_U}(H)\colon H=\mathrm{PG}(k-2,q^m)\subset\mathrm{PG}(k-1,q^m)\}=$$

$$n-m+\max\{w_{L_{U^{\perp'}}}(P)\colon P\in\mathrm{PG}(k-1,q^m)\}=n-t_j,$$

其中 $t_j=\min\{t_i\colon\ i>1\}$。因此，$d=n-(n-t_j)=t_j$。这意味着 $\mathcal{C}_{\overline{S},\ \mu,\ t_1,\ \ldots t_k}$ 是一个非退化 $[n,k,t_j]_{q^m/q}$码。现在，考虑 $\mathcal{C}_{\overline{S}}^{\perp_{\mathcal{G}},\ \mu,\ t_1,\ \ldots t_k}$ 与之关联的系统

$\mathcal{C}_{\overline{S}}^{\perp_{\mathcal{G}}}$, μ, t_1, ...t_k 是 $U^{\perp'}$，因此它是一个 $[km-n,k]_{q^m/q}$码。此外，根据命题 2.16，我们有

$$\max\{w_{L_{U^{\perp'}}}(H)\colon H=\mathrm{PG}(k-2,q^m)\subset\mathrm{PG}(k-1,q^m)\}$$
$$=(k-1)m-n+\max\{w_{L_U}(P)\colon P\in\mathrm{PG}(k-1,q^m)\}=(k-1)m-n+\ell t+t_1,$$

这意味着 $d(\mathcal{C}_{\overline{S}、\mu、t_1、.....、t_k})=t(\ell'-\ell)-t_1$。当 $k=2$ 且 $n\le m$时，根据定理 2.6，利用由 U 定义的线性集的重量分布，可以确定该码的重量分布；该线性集的重量分布已在 [34, 推论 4.2] 中完全确定。□

我们证明，上述构造仍能得到一个码，其 $M(\mathcal{C})$ 的值达到可能的最大值。

命题 5.14。设 $\mathcal{C}_{\overline{S}、\mu、t_1、t_2}\subseteq\mathbb{F}_{q^m}^n$ 如构造 5.12 中所述，并假设 $n\le m$。则 $\mathcal{C}_{\overline{S}、\mu、t_1、t_2}$有一个重量为 $n-1$ 的码字，并且在至少含有一个重量为 $n-1$ 的码字的非退化 $[n,2]_{q^m/q}$码中，$\mathcal{C}_{\overline{S}、\mu、t_1、t_2}$的 $M(\mathcal{C})$ 达到最大值。

证明。 考虑与以下对象相关联的系统：$\mathcal{C}_{\overline{S},\mu,t_1,t_2}$

$$U=(\overline{S}\oplus\langle 1,\mu,\dots,\mu^{t_1-1}\rangle_{\mathbb{F}_q})\times\langle 1,\mu,\dots,\mu^{t_2-1}\rangle_{\mathbb{F}_q}.$$

注意到 L_U 是一个秩为 n、形如 [34, 推论 4.2], 的 $\mathbb{F}_q$-线性集，这意味着 $|L_U|=q^{n-1}+1$ 和 L_U 具有 $q^{n-1}-q^{n-3}\ge 1$ 个权为一的点。根据 (2)，后一个事实可表述为 $\mathcal{C}_{\overline{S},\ \mu,\ t_1,\ t_2}$ 至少具有一个重量为 $n-1$ 的码字，并且根据命题 3.1，我们得到 (13) 中的等式。□

注 5.15. 设 U 和 U' 分别是与构造 5.3 和构造 5.12 相关联的两个系统。根据 *[34,* 定理 5.*1]*， U和 U'是 ΓL(2, q^m)-不等价的，因此根据定理 2.7，码 $\mathcal{C}$ 和 $\mathcal{C}'$ 是不等价的。

现在我们给出更多满足上界 3.16 中等式的秩度量码示例。

定理 **5 16** $\mathcal{C}_{\overline{S}\,\mu\,t_1\,\dots\,t_k}\subseteq\mathbb{F}_{q^m}^n$ *5 12* t_1+.. 设 ,,,,如构造 . 中所述, ... $+t_k\le t+k$ $\{t_1-1,\dots,t_k-1\}=\{s_{i_1},\dots,s_{i_\ell}\}$ $s_{i_1}>\dots>s_{i_\ell}$ 并假设 . 设 , 且满足 . 若

$$k\le\sum_{j=1}^{\ell}\frac{q^{s_{i_j}}-2q^{s_{i_j}/2}}{s_{i_j}}$$

or

$$t_1+\dots+t_k-k\le q,$$

那么，码 $\mathcal{C}_{\overline{S}}^{\perp_{\mathcal{G}}}{}_{,\mu,t_1,\dots,t_k}\subseteq\mathbb{F}_{q^m}^{km-n}$满足定理 3.16 的假设，其中 $r=1$ ，并且 $\mathcal{C}_{\overline{S}}^{\perp_{\mathcal{G}}}{}_{,\mu,t_1,\dots,t_k}$ 在满足定理 3.16 中关于 $r=1$ 的假设的码中，达到 $M(\mathcal{C})$ 的最大值。

证明。注意，$(\mathcal{C}_{\overline{S}}^{\perp_{\mathcal{G}}}{}_{,\mu,t_1,\ldots,t_k})^{\perp_{\mathcal{G}}}$ 等价于码 $\mathcal{C}_{\overline{S},\mu,t_1,\ldots,t_k}$ ，其关联系统为

$$U = (\overline{S} \oplus \langle 1, \mu, \ldots, \mu^{t_1-1} \rangle_{\mathbb{F}_q}) \times \ldots \times \langle 1, \mu, \ldots, \mu^{t_k-1} \rangle_{\mathbb{F}_q}.$$

由于 $t_1 + \ldots + t_k \leq t + k$，根据 $[1,$ 推论 4.16$]$，，存在一个超平面 H，使得$L_U \cap H =$ PG$(k-2,q)$，因此存在一个码字，属于 $\mathcal{C}_{\overline{S}}^{\perp_{\mathcal{G}}}{}_{,\ \mu,\ t_1,\ \ldots\ldots t_k}$，如定理 3.16 的陈述所示，因此也属于 $(\mathcal{C}^{\perp_{\mathcal{G}}})^{\perp_{\mathcal{G}}}$。此外，$[1,$定理 4.14$]$还表明

$$|L_U| = q^{n-1} + \ldots + q^{n-k+1} + 1,$$

这意味着 $M(\mathcal{C}_{\overline{S}}^{\perp_{\mathcal{G}}}{}_{,\ \mu,\ t_1,\ \ldots\ldots t_k})$ 取最大值。 □

注记 5.17。特别地，若 $t_1 \geq \ldots \geq t_k$ 且 $k \leq \frac{q^{t_k-1}-2q^{\frac{t_k-1}{2}}}{t_1-1}$，则满足定理 5.8 的假设。

6 结论与开放问题

本文给出了具有最大重量的 $\mathbb{F}_{q^m}$-线性非退化秩度量码的码字数量的上界和下界。在某些假设下，我们改进了这些上界。随后，我们给出了一些刻画结果，尽管在某些情况下，我们并不知道所得界是否是紧的。

这里列出一些可能令读者感兴趣的开放问题。

- 我们不知道定理 3.11 中的下界是否是紧的。因此，构造满足等号的例子，或改进这个下界，都将很有意义。

- 将定理 5.11 中的刻画推广到更大的维数。

- 对于 $M(\mathcal{C})$，具有极值的码的密度如何？如果能了解 $[5,27]$ 中提出的技巧是否也能应用于这种情况，将会很有意义。

- $M(\mathcal{C})$的平均值是多少?

参考文献

[1] S. Adriaensen 和 P. Santonastaso。关于线性集的最小大小。arXiv 预印本 math/2301.13001，2023。

[2] G. Alfarano。拟阵方法编码理论。苏黎世大学编码理论与密码学工作组研讨会，2022年。

[3] G 。Alfarano 和 E. Byrne。拟阵方法编码理论。准备中，20 23.

[4] G. N. Alfarano、M. Borello、A. Neri 和 A. Ravagnani。秩度量中的线性截断阻挡集与极小码。组合理论杂志 A 辑，192：105658，2022年。[5] J. Antrobus 和 H. Gluesing-Luerssen。最大费雷尔图码：构造与一般性考量。IEEE 信息论汇刊，65(10)：6204– 6223，2019年。[6] D. Augot、A. Couvreur、J. Lavauzelle 和 A. Neri。任意伽罗瓦扩张上的秩度量码及秩类 Reed–Muller 码。SIAM 应用代数与几何期刊，5(2)：165–199，2021年。[7] C. Bachoc、O. Serra 和 G. Z´emor。扩域上的 Vosper 定理类比。在《剑桥哲学学会数学学报》，第163卷，423–452页。剑桥大学出版社，2017年。[8] C. Bachoc、O. Serra 和 G. Z´emor。重新审视扩域上的 Kneser 定理。Combinatorica，38(4)：759–777，2018年。[9] S. Ball 和 A. Blokhuis。线性码最大重量的一个界。SIAM 离散数学期刊，27(1)：575–583，2013年。[10] S. Ball、A. Blokhuis 和 M. Lavrauw。PG(2, q^4) 中的线性（$q+1$）重阻挡集。有限域及其应用，6(4)：294–301，2000年。[11] D. Bartoli、M. Giulietti、G. Marino 和 O. Polverino。伽罗瓦空间中的最大散布线性集与完全帽。Combinatorica，38(2)：255–278，2018年。[12] D. Bartoli、G. Marino 和 A. Neri。由线性截断阻挡集构造的新最大秩距离码。纯粹与应用数学年刊（1923-），第1–28页，2022年。[13] H. Bartz、L. Holzbaur、H. Liu、S. Puchinger、J. Renner 和 A. Wachter-Zeh。秩度量码及其应用。《通信与信息论基础与趋势》®，19(3)：390–546，2022年。[14] T. P. Berger。秩距离的等距变换与 Gabidulin 码的置换群。IEEE 信息论汇刊，49(11)：3016–3019，2003年。[15] A. Blokhuis 和 M. Lavrauw。相对于 PG(n, q) 中铺展的散布空间。专论几何，81(1)：231–243，2000年。[16] G. Bonoli 和 O. Polverino。PG(2, q^4) 中的 $\mathbb{F}_q$-线性阻挡集。《关联几何创新：代数、拓扑与组合》，2(1)：35–56，2005年。[17] M. Borello 和 F. Zullo。几何对偶与和秩度量极小码。准备中，2023。

[18] E. Byrne、A. Neri、A. Ravagnani 和 J. Sheekey。《秩度量码的张量表示》。SIAM 应用代数与几何期刊，3(4)：614–643，2019年。[19] B. Csajb´ok、G. Marino、O. Polverino 和 F. Zullo。《最大散布线性集与最大秩距码》。代数组合学杂志，46(3)：517–531，2017年。[20] J. De Beule 和 G. Van de Voorde。《线性集的最小大小》。组合理论杂志 A 辑，164：109–124，2019年。[21] P. Delsarte。《有限域上的双线性形式及其在编码理论中的应用》。组合理论杂志 A 辑，25(3)：226–241，1978年。[22] Y. El Maazouz、M. A. Hahn、A. Neri 和 M. Stanojkovski。《赋值秩度量码》。arXiv:2104.03216，2021年。[23] E. M. Gabidulin。《最大秩距离码理论》。Problemy Peredachi Informatsii，21(1)：3–16，1985年。[24] H. Gluesing-Luerssen 和 B. Jany。《 q-多拟阵及其与秩度量码的关系》。代数组合学杂志，页码 1–29，2022年。[25] E. Gorla。《秩度量码》。载于《编码理论简明百科全书》，页码 227–250。Chapman and Hall/CRC，2021年。[26] E. Gorla、R. Jurrius、H. H. L´opez 和 A. Ravagnani。《秩度量码与 q-多拟阵》。代数组合学杂志，52(1)：1–19，2020年。[27] A. Gruica 和 A. Ravagnani。《线性子空间的公共补空间与最大秩距离码的稀疏性》。SIAM 应用代数与几何期刊，6(2)：79–110，2022年。[28] A. Gruica、A. Ravagnani、J. Sheekey 和 F. Zullo。《秩度量码、半域与平均临界问题》。arXiv 预印本 arXiv:2201.07193，即将发表于 SIAM 离散数学期刊，2022年。[29] D. Jena 和 G. Van de Voorde。《论最小大小线性集》。离散数学，344(3)：112230，2021年。[30] R. Jurrius 和 R. Pellikaan。《论广义秩权的定义》。通信数学进展，11(1)：225–235，2017年。[31] G. Marino、A. Neri 和 R. Trombetti。《逃逸子空间、广义秩权与近似 MRD 码》。arXiv 预印本 arXiv:2204.11791，2022年。[32] U. Mart´ınez-Pe˜nas。《赋予和秩度量的线性码的支撑理论》。设计、编码与密码学，87(10)：2295–2320，2019年。

[33] T. Migler、K. E. Morrison 和 M. Ogle。《有限域上矩阵的重量与秩》。arXiv 预印本 math/0403314，2004年。[34] V. Napolitano、O. Polverino、P. Santonastaso 和 F. Zullo。《最小大小线性集的分类与构造》。arXiv 预印本 arXiv:2201.02003，2022年。[35] V. Napolitano、O. Polverino、P. Santonastaso 和 F. Zullo。《具有互补权重的射影直线上的线性集》。离散数学，345(7)：112890，2022年。[36] A. Neri、P. Santonastaso 和 F. Zullo。《和秩度量下单重量码的几何学》。组合理论杂志 A 辑，194：105703，2023。[37]O. Polverino。《有限射影空间中的线性集》。离散数学，310(22)：3096–3107，2010年。[38] O. Polverino、P. Santonastaso、J. Sheekey 和 F. Zullo。《可整除线性秩度量码》。arXiv 预印本 arXiv:2211.08180，即将发表于 IEEE 信息论汇刊，2023。[39] O. Polverino 和 F. Zullo。《散布线性集与最大秩距码之间的联系》。组合学及其应用研究所通报，89：46–74，2020年。[40] T. H. Randrianarisoa。《秩度量码的几何方法及恒重码的分类》。设计、编码与密码学，88：1331–1348，2020年。[41] A. Ravagnani。《广义权重：反码方法》。纯粹与应用代数杂志，220(5)：1946–1962，2016年。[42] A. Ravagnani。《秩度量码及其对偶理论》。设计、编码与密码学，80(1)：197–216，2016年。[43] R. M. Roth。《最大秩阵列码及其在交叉错误纠正中的应用》。IEEE 信息论汇刊，37(2)：328–336，1991年。[44] J. Sheekey。《一类新的线性最大秩距码》。通信数学进展，10(3)：475，2016年。[45] J. Sheekey。《最大秩距离码：构造与联系》。载于《组合学与有限域：差集、多项式、伪随机性及其应用》，23，2019年。[46] D. Silva、F. R. Kschischang 和 R. Koetter。《随机网络编码中错误控制的秩度量方法》。IEEE 信息论汇刊，54(9)：3951–3967，2008年。[47] G. Zini 和 F. Zullo。《散布子空间与相关码》。设计、编码与密码学，89(8)：1853–1873，2021年。

Olga Polverino、Paolo Santonastaso 和 Ferdinando Zullo
数学与物理系，坎帕尼亚大学“Luigi Vanvitelli”，I–81100 卡塞塔，
意大利{olga.polverino,paolo.santonastaso,ferdinando.zullo}
@unicampania.it