高次对称秩度量码

ARTHUR BIK 和 Alessandro Neri

ABSTRACT. 在特征不等于 2 的域上，我们可以将对称矩阵与次数为 2 的齐次多项式对应起来。这使我们能够将对称秩度量码视为存在于此类多项式构成的空间中。在本文中，我们将对称 Gabidulin 码的构造推广到次数为 $d > 2$ 的多项式，其中域的特征为 0 或 $> d$。为此，我们赋予次数为 $d \geq 2$ 的齐次多项式空间一种由本质秩诱导的度量，其中本质秩是表示一个多项式所需的线性形式的最少数量。我们给出了所构造的本质秩度量码的最小距离和维数的界，并提供了一种高效的译码算法。最后，我们展示了如何将本质秩度量码视为秩度量码的特殊实例，并将我们的构造与具有相同参数的已知秩度量码进行比较。

1. INTRODUCTION

秩度量码 $\mathcal{C}$ 是域 $\mathbb{F}$ 上的一个矩阵线性空间，其中任意非零矩阵的秩都有一个固定的下界 $r > 0$，称为该码的最小距离 $\mathcal{C}$。秩度量码的定义可追溯至 Delsarte [9] ，他研究这类码时将其与关联方案理论联系起来。此后，秩度量码出现在各种各样的研究背景中。例如，它们被用作交叉错误纠正 [19] 和随机网络编码 [23]中的纠错码 [24] 。关于秩度量码理论及其数学见解的介绍，请参阅 [3] ；关于其应用的更完整列表，请参阅。

秩度量码中最著名的一类是 Gabidulin 码 [9, 11], ，为完整起见，我们在此重述其构造：设 $\mathbb{L}/\mathbb{F}$ 是一个循环伽罗瓦扩张，记 $n = [\mathbb{L} : \mathbb{F}]$ 为其次数，并令 σ 为 $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ 的一个生成元。于是，选取 α_1、……、α_n 作为 $\mathbb{L}$ 在 $\mathbb{F}$上的一组基后，我们可以将 $\mathrm{End}_{\mathbb{F}}(\mathbb{L})$ 中的 $\mathbb{F}$-线性自同态空间与 $\mathbb{F}$上的 $n \times n$ 矩阵空间 $\mathbb{F}^{n\times n}$ 对应起来。现在，任意一对满足 $k + \ell \leq n - 1$ 的整数 k、$\ell \geq 0$，都可以通过考察 $\mathbb{F}^{n\times n}$中对应于该子空间的矩阵空间来定义一个 Gabidulin 码

$$\{c_{-k}\sigma^{-k} + \ldots + c_\ell\sigma^\ell \mid c_{-k}, \ldots, c_\ell \in \mathbb{L}\} \subseteq \mathrm{End}_{\mathbb{F}}(\mathbb{L}).$$

这是一个维数为 $n(k + \ell + 1)$、最小距离为 $n - (k + \ell)$ 的码。事实上，非零端同态 $c_{-k}\sigma^{-k} + \ldots + c_\ell\sigma^\ell$ 的核中的元素，也是 $\sigma^k(c_{-k})\sigma^0(x) + \ldots + \sigma^k(c_\ell)\sigma^{k+\ell}(x)$ 的核中的元素。当 $\mathbb{F} = \mathbb{F}_q$ 是有限域且 σ 是弗罗贝尼乌斯自同构时，这是一个次数为 $\leq q^{k+\ell}$ 的多项式。该多项式的根的数量至多为其次数，因此该端同态的核的维数至多为 $k + \ell$。基于 Artin 定理的特征标的线性无关性的更深入论证表明，一般而言，该端同态的核的维数不可能大于 $k + \ell$ ；例如参见 [17, 20]。

Gabidulin 码的构造已沿多个不同方向得到推广。其中，在 [20] 中，该构造从矩阵空间扩展到了 d路张量空间（ $d \geq 2$）；而在 [22] 中，该构造经过修改，使所得的码仅由对称矩阵组成，即该码是对称秩度量码；另见 [21]。在这一方向上，de Boer 首先研究了对称秩度量码，并给出了具有较大最小秩的码的构造 [8]。他的研究成果也受到经典纠错码纯粹应用的推动。在秩度量码的背景下研究对称矩阵的重要性还体现在其应用上，

由于解码算法效率的提高 [7, 12]。在一个 $\mathbb{F}$ 特征不为 2 的域上，我们可以将对称矩阵与次数为 2 的齐次多项式对应起来。这使我们能够将对称秩度量码视为位于此类多项式空间中的码。更准确地说，对于一个次数为 2 的齐次多项式

$$f = \sum_{1 \le i \le j \le n} a_{i,j} x_i x_j \in \mathbb{F}[x_1, \dots, x_n]_2,$$

我们可以将其与矩阵关联起来

$$C_f = \begin{pmatrix} 2a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{1,2} & 2a_{2,2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{n-1,n} \\ a_{1,n} & \cdots & a_{n-1,n} & 2a_{n,n} \end{pmatrix}.$$

反之，如果 $\mathrm{char}(\mathbb{F}) \neq 2$，则每个对称矩阵都可以通过反转上述映射得到一个次数为 2 的齐次多项式。

在这种对应关系下，对称矩阵 C_f 的秩可以由 f 直接计算，因为有

$$\mathrm{rk}(C_f) = \min\{r \in \mathbb{Z}_{\ge 0} \mid f = g(\ell_1, \dots, \ell_r), \ell_1, \dots, \ell_r \in \mathbb{F}[x_1, \dots, x_n]_1,\ g \in \mathbb{F}[y_1, \dots, y_r]_2\}. \tag{1}$$

换句话说，对称矩阵 C_f 的秩等于表示 f 所需的最少变量数，其中允许进行变量的线性变换。这是研究对称秩度量码的一个等价框架。

本文旨在将对称秩度量码的研究扩展到更高的对称次数。为此，我们赋予次数为d 的多项式空间一种由本质秩诱导的度量。次数为d 的多项式 $f \in \mathbb{F}[x_1, \dots, x_n]_d$的本质秩可以定义为（1）的自然推广，并表示为

$$\mathrm{ess}(f) = \min\{r \in \mathbb{Z}_{\ge 0} \mid f = g(\ell_1, \dots, \ell_r),\ \ell_1, \dots, \ell_r \in \mathbb{F}[x_1, \dots, x_n]_1, g \in \mathbb{F}[y_1, \dots, y_r]_d\}.$$

因此，多项式的本质秩等于表示该多项式所需的最少变量数，其中允许进行变量的线性变换。在这一框架下，我们将本质秩度量码作为 $\mathbb{F}[x_1, \dots, x_n]_d$ 的子空间进行研究。对于每个 $1 \le \rho \le n$，我们给出一族本质秩度量码 $\mathcal{C}^{n,d}_{\rho}(\alpha)$ 的一般构造，其本质秩以下界 ρ 为下界；见定理 3.1。正如我们所展示的，这一构造可以看作对称 Gabidulin 码族的推广：当 $d = 2$ 时，$\mathcal{C}^{n,2}_{\rho}(\alpha)$ 的构造与对称 Gabidulin 码的构造可以相互对应。此外，我们为这族码配备了一种译码算法，能够纠正所有本质秩至多为 $\lfloor \frac{\rho-1}{2} \rfloor$ 的错误；见算法 1。随后，我们利用 Carlini 的一个结果 [6]，探讨本质秩度量码与秩度量码之间的联系。当域的特征大于 d （或等于 0）时，通过其首个催化矩阵，本质秩度量码可以看作秩度量码的特殊族；见推论 5.4。我们的工作主要有两个动机：一方面，我们研究次数为 d 的对称秩度量码的数学性质，将经典结果推广到 $d = 2$；另一方面，我们旨在推动对齐次多项式的其他秩概念所诱导的度量进行研究，这些秩概念是当代应用代数几何的典型对象，例如强度和切片秩。

概要。 在第 2 节中，我们讨论本质秩的性质及其与零化理论的联系。随后，在第 3 节中，我们给出一类本质秩度量码的构造。我们还给出其维数和最小距离的下界。在第 4 节中，我们给出一种译码算法，能够高效地恢复在一定有界误差下给出的码字。在第 5 节中，我们说明如何将我们的码视为一类特殊的秩度量码。对于 $d = 2$，我们证明我们的构造产生对称 Gabidulin 码；对于 $d > 2$ ，我们将我们的码的参数与由秩度量码理论得到的界进行比较

。最后，在第 6 节中，我们列出秩的其他概念；这些概念有望产生能够构造实用码的度量。

致谢。AB 部分获得瑞士国家科学基金会 Postdoc.Mobility Fellowship（编号 P400P2 199196）以及西蒙斯基金会资助（816048，LC）。AN 获得 FWO（弗兰德斯研究基金会）资助，项目编号为 12ZZB23N。

2. Essential rank of homogeneous polynomials

本节将简要回顾 Carlini 在[6]中所描述的多项式本质秩理论。请注意，在该论文中，作者假设 $\mathrm{char}(\mathbb{F}) = 0$，尽管所有结果在 $\mathrm{char}(\mathbb{F}) > d$时同样成立。因此，在本节中，我们将作出 $\mathrm{char}(\mathbb{F}) > d$ 或 $\mathrm{char}(\mathbb{F}) = 0$ 的假设。

设 $S_n(\mathbb{F}) = \mathbb{F}[x_1, \ldots, x_n]$，并设 $T_n(\mathbb{F}) = \mathbb{F}[\partial_1, \ldots, \partial_n]$ 为作用于 $S_n(\mathbb{F})$ 上的微分算子环。这意味着，$S_n(\mathbb{F})$ 具有一个通过微分作用的 $T_n(\mathbb{F})$-模结构，即 $T_n(\mathbb{F})$ 在 $S_n(\mathbb{F})$ 上的作用定义为

$$\partial_i \circ f \coloneqq \frac{\partial}{\partial x_i} f, \qquad \text{for every } f \in S_n(\mathbb{F}).$$

我们将主要关注这些环的齐次分量，分别记为 $S_{n,\,d}(\mathbb{F})$ 和$T_{n,\,d}(\mathbb{F})$，其中 d 表示次数。按照约定，我们始终将零多项式 0 视为属于 $S_{n,\,d}(\mathbb{F})$，并将零算子 0 视为属于 $T_{n,\,d}(\mathbb{F})$。限制在齐次分量上时，对于所有 $0 \le b \le a$，我们有一个满射的 $\mathbb{F}$-双线性映射

$$\begin{array}{rccc} \Phi_{n,a,b}\colon & S_{n,a}(\mathbb{F}) \times T_{n,b}(\mathbb{F}) & \longrightarrow & S_{n,a-b}(\mathbb{F}) \\ & (f, D) & \longmapsto & D \circ f. \end{array}$$

在 $a = b = d$ 情形下，这给出了一个自然的非退化 $\mathbb{F}$-双线性映射

$$\begin{array}{rccc} \Phi_{n,d}\colon & S_{n,d}(\mathbb{F}) \times T_{n,d}(\mathbb{F}) & \longrightarrow & \mathbb{F} \\ & (f, D) & \longmapsto & D \circ f. \end{array} \tag{2}$$

显然，双线性型（2）诱导出一个对偶。对于给定的子集 $A \subseteq S_{n,\,d}(\mathbb{F})$ 和 $B \subseteq T_{n,\,d}(\mathbb{F})$，其正交子空间

$$A^{\perp} \coloneqq \{D \in T_{n,d}(\mathbb{F}) \mid D \circ f = 0 \text{ for all } f \in A\} \subseteq T_{n,d}(\mathbb{F}),$$
$$B^{\perp} \coloneqq \{f \in S_{n,d}(\mathbb{F}) \mid D \circ f = 0 \text{ for all } D \in B\} \subseteq S_{n,d}(\mathbb{F})$$

满足

$$\dim_{\mathbb{F}}(\langle A \rangle_{\mathbb{F}}) + \dim_{\mathbb{F}}(A^{\perp}) = \dim_{\mathbb{F}}(S_{n,d}(\mathbb{F})) = \dim_{\mathbb{F}}(T_{n,d}(\mathbb{F})) = \dim_{\mathbb{F}}(\langle B \rangle_{\mathbb{F}}) + \dim_{\mathbb{F}}(B^{\perp}).$$

注意，$S_{n,\,1}(\mathbb{F})$ 正是线性多项式的空间，而 $T_{n,\,1}(\mathbb{F})$ 则是所有方向导数的空间。这些空间自然同构于 $\mathbb{F}^n$；对于给定的向量$v = (v_1, \ldots, v_n) \in \mathbb{F}^n$，我们记

$$v(x) \coloneqq v_1 x_1 + \ldots + v_n x_n \in S_{n,1}(\mathbb{F}),$$
$$v(\partial) \coloneqq v_1 \partial_1 + \ldots + v_n \partial_n \in T_{n,1}(\mathbb{F}).$$

定义 2.1. 设 $f \in S_{n,\,d}(\mathbb{F})$。$f$ 的本质秩是整数

$$\mathrm{ess}(f) \coloneqq \min\{r \in \mathbb{Z}_{\ge 0} \mid f \in \mathbb{F}[\ell_1, \ldots, \ell_r]_d, \ell_1, \ldots, \ell_r \in S_{n,1}(\mathbb{F})\}.$$

f 的本质秩就是在线性变量变换后表达 f所需的最少变量数。

引理 2.2. 设 $f \in S_{n,\,d}(\mathbb{F})$ 满足 $\mathrm{ess}(f) = r$。设 $\ell_1, \ldots\ldots, \ell_r$、$h_1, \ldots\ldots, h_r \in S_{n,\,1}(\mathbb{F})$ 满足 $f \in \mathbb{F}[\ell_1, \ldots, \ell_r]$ 和 $f \in \mathbb{F}[h_1, \ldots, h_r]$。则 $\langle \ell_1, \ldots\ldots, \ell_r \rangle_{\mathbb{F}} = \langle h_1, \ldots\ldots, h_r \rangle_{\mathbb{F}}$。

证明。假设 $\langle \ell_1, \ldots, \ell_r \rangle_{\mathbb{F}} \neq \langle h_1, \ldots, h_r \rangle_{\mathbb{F}}$，并设 $0 \leq s < r$ 为交集维数。根据 r 的最小性，$\ell_1, \ldots, \ell_r$ 和 $h_1, \ldots, h_r$ 都是线性无关集。经过坐标变换，我们可以假设 $\ell_1 = h_1, \ldots, \ell_s = h_s$，因此

$$V := \langle \ell_1, \ldots, \ell_r \rangle_{\mathbb{F}} \cap \langle h_1, \ldots, h_r \rangle_{\mathbb{F}} = \langle \ell_1, \ldots, \ell_s \rangle_{\mathbb{F}} = \langle h_1, \ldots, h_s \rangle_{\mathbb{F}}.$$

我们断言，形式 ℓ_1、……、ℓ_r、h_{s+1}、……、h_r 是线性无关的。事实上，当

$$c_1\ell_1 + \ldots + c_r\ell_r + b_{s+1}h_{s+1} + \ldots + b_rh_r = 0, \quad c_1, \ldots, c_r, b_{s+1}, \ldots, b_r \in \mathbb{F},$$

我们看到 $b_{s+1}h_{s+1} + \ldots + b_rh_r \in V$，因此 b_{s+1}、……、$b_r = 0$ 关于 h_1、……、h_r 是线性无关的。于是 $c_1\ell_1 + \ldots + c_r\ell_r = 0$，因此 c_1、……、$c_r = 0$ 关于 ℓ_1、……、ℓ_r 也同样是线性无关的。这就证明了该断言。现在，我们可以写成

$$f_1(\ell_1, \ldots, \ell_r) = f = f_2(h_1, \ldots, h_r)$$

并将两边都解释为关于 ℓ_1、……、ℓ_r、h_{s+1}、……、h_r 的多项式。左边不依赖于形式 h_{s+1}、……、h_r，而右边不依赖于 ℓ_{s+1}、……、ℓ_r。由于两边实际上是同一个多项式，这意味着 f 仅是 ℓ_1、……、ℓ_s 的多项式。这与 r 的最小性矛盾。因此 $\langle \ell_1$、……、$\ell_r \rangle_{\mathbb{F}} = \langle h_1$、……、$h_r \rangle_{\mathbb{F}}$。□

定义 2.3. 设 $f \in S_{n,d}(\mathbb{F})$ 的本质秩 $\mathsf{ess}(f) = r$。我们将 f 的本质变量空间定义为

$$V_{\mathrm{ess}}(f) \coloneqq \langle \ell_1, \ldots, \ell_r \rangle_{\mathbb{F}} \subseteq S_{n,1}(\mathbb{F}),$$

其中 $\ell_1, \ldots, \ell_r \in S_{n,1}(\mathbb{F})$ 满足 $f \in \mathbb{F}[\ell_1, \ldots, \ell_r]$。

注 2.4. 引理 2.2 的证明实际上表明，若 $h_1, \ldots, h_s \in S_{n,1}(\mathbb{F})$ 满足 $f \in \mathbb{F}[h_1, \ldots, h_s]$，则 $V_{\mathrm{ess}}(f) \subseteq \langle h_1, \ldots, h_s \rangle_{\mathbb{F}}$。

例 2.5. 设 $\mathbb{F}$ 是一个特征 $\mathrm{char}(\mathbb{F}) \neq 2$、3 的域，并设

$$f = 3x_1^3 + 8x_1^2x_2 + 5x_1^2x_3 + 12x_1x_2^2 + 4x_1x_2x_3 + 4x_1x_3^2 + 8x_2^3 + 2x_2x_3^2 + x_3^3 \in S_{3,3}(\mathbb{F}).$$

乍一看，f 的本质秩等于什么并不明显，但可以验证

$$\begin{aligned} f &= (x_1 + 2x_2)(x_1 + x_3)^2 + (x_1 + 2x_2)^3 + (x_1 + x_3)^3 \\ &=: g(x_1 + 2x_2, x_1 + x_3). \end{aligned}$$

这意味着 $V_{\mathrm{ess}}(f) \subseteq \langle x_1 + 2x_2, x_1 + x_3 \rangle_{\mathbb{F}}$ 且 $\mathsf{ess}(f) \leq 2$。我们将在例 5.3中看到，这些实际上都是等式。

注 2.6. 设 $f, g \in S_{n,\,d}(\mathbb{F})$，并设 $\lambda \in \mathbb{F}^*$。以下性质成立。

(1) $\mathsf{ess}(f) \geq 0$，且 $\mathsf{ess}(f) = 0$ 当且仅当 $f = 0$。(2) $\mathsf{ess}(f + g) \leq \mathsf{ess}(f) + \mathsf{ess}(g)$。(3) $\mathsf{ess}(f) = \mathsf{ess}(\lambda f)$。(4) $\mathsf{ess}(f) \leq n$。(5) $\mathsf{ess}(f) = 1$ 当且仅当 $f = \lambda \ell^d$，其中某个 $\lambda \in \mathbb{F}^*$ 和 $\ell \in S_{n,\,1}(\mathbb{F})$。

注意，由于性质 (1)、(2) 和 (3)，本质秩的概念在 $S_{n,\,d}(\mathbb{F})$ 上诱导出一个度量，定义为

$$\mathrm{d}_{\mathrm{ess}}(f, g) \coloneqq \mathrm{ess}(f - g).$$

这使我们能够基于这一度量发展纠错码理论。

定义 2.7. [(n, d) k本质秩度量码 $\mathcal{C}$ 是 $S_{n,\,d}(\mathbb{F})$ 的一个 k 维 $\mathbb{F}$ 子空间，并配备本质秩度量。整数 r 定义为

$$r := \min\{\mathrm{d}_{\mathrm{ess}}(f, g) \mid f, g \in \mathcal{C}, f \neq g\} = \min\{\mathrm{ess}(f) \mid f \in \mathcal{C} \setminus \{0\}\}$$

并称为 $\mathcal{C}$ 的最小本质秩距离。

例 2.8。设 $\mathbb{F}$ 是一个特征为 $\mathrm{char}(\mathbb{F}) \neq 2$的域，3，并考虑 $[(3,3)2,\ 2]_{\mathbb{F}}$ 本质秩度量码 $\mathcal{C} = \langle f_1, f_2\rangle_{\mathbb{F}}$，其中 f_1 是例 2.5中的多项式，即

$$f_1 = 3x_1^3 + 8x_1^2x_2 + 5x_1^2x_3 + 12x_1x_2^2 + 4x_1x_2x_3 + 4x_1x_3^2 + 8x_2^3 + 2x_2x_3^2 + x_3^3$$

and

$$f_2 = x_1^3 + 2x_1x_2^2 + x_3^3.$$

事先确定 $\mathcal{C}$ 的最小本质秩距离为 2 并不容易。显然，≤ 2，因为 $\mathrm{ess}(f_1) \leq 2$。在第 5 节中，我们将说明如何确定其精确值；参见例5.5。

码的参数 n, d, k, r 并非彼此独立，而是相互依赖的。具体而言，四个整数并非所有可能的取值组合都能由某个码实现。下面的结果给出了它们必须满足的条件。

命题 2.9（类 Singleton 界）。设 $\mathcal{C}$ 是一个 $[(n,d)\ k,r]_{\mathbb{F}}$ 码。那么

$$k \leq \binom{n+d-1}{d} - \binom{r+d-2}{d}.$$

证明。将空间 $S_{r-1,\ d}(\mathbb{F})$ 视为 $S_{n,\ d}(\mathbb{F})$ 的子空间。由于 $S_{r-1,\ d}(\mathbb{F})$ 中的每个非零多项式的本质秩都严格小于 r，因此 $\mathcal{C} \cap S_{r-1,\ d}(\mathbb{F}) = \{0\}$。于是

$$k + \binom{r+d-2}{d} = \dim(\mathcal{C}) + \dim(S_{r-1,d}(\mathbb{F})) \leq \dim(S_{n,d}(\mathbb{F})) = \binom{n+d-1}{d}.$$

□

在第5 节中，我们将借助秩度量码理论给出另一个将这些参数联系起来的界。不过，我们也会看到，它永远不会优于命题2.9中的界。

2.1. 非退化性与等价。本节中，我们为本质秩度量码引入退化性与等价的概念。前者刻画了应当考察该码的有效环境空间，后者则旨在识别可视为相同的码。

定义 2.10. 对于一个 $[(n,d)\ k,r]_{\mathbb{F}}$ 本质秩度量码 $\mathcal{C}$，我们将其本质变量空间定义为：

$$V_{\mathrm{ess}}(\mathcal{C}) := \sum_{f\in\mathcal{C}} V_{\mathrm{ess}}(f).$$

若 $V_{\mathrm{ess}}(\mathcal{C}) = S_{n,1}(\mathbb{F})$，则称 $\mathcal{C}$ 为非退化；若它不是非退化的，则称其为退化。

非退化性的概念使我们能够在最小环境空间中工作。事实上，若一个$[(n,d)\ k,r]_{\mathbb{F}}$ 码 $\mathcal{C}$ 是退化的，且 $\dim(V_{\mathrm{ess}}(\mathcal{C})) = t$，则 $\mathcal{C}$ 可等距嵌入到 $S_{t,d}(\mathbb{F})$中。

我们来考察保持度量不变的环境空间的自然变换。换言之，我们考察 $(S_{n,d}(\mathbb{F}),\mathrm{d_{ess}})$ 的 $\mathbb{F}$-线性变换，即等距变换。对于任意 $A \in \mathrm{GL}(n,\mathbb{F})$ 和 $\lambda \in \mathbb{F}^*$，考虑诱导映射

$$\begin{array}{ccc} S_{n,d}(\mathbb{F}) & \longrightarrow & S_{n,d}(\mathbb{F}) \\ f(x) & \longmapsto & \lambda f \cdot A := \lambda f(x \cdot A). \end{array} \tag{3}$$

不难验证，这个 $\mathbb{F}$-线性映射是 $(S_{n,d}(\mathbb{F}),\mathrm{d_{ess}})$ 的等距映射。我们猜想，至少在某些自然条件下，每个等距映射都具有这种形式。

猜想 2.11。假设 $\mathrm{char}(\mathbb{F}) = 0$ 或 $\mathrm{char}(\mathbb{F}) > d$。那么 $(S_{n,d}(\mathbb{F}), \mathrm{d_{ess}})$ 的每个等距映射都具有以下形式：$f \mapsto \lambda f \cdot A$ 其中 $A \in \mathrm{GL}(n,\mathbb{F})$ 且 $\lambda \in \mathbb{F}^*$。

在本文中，我们将把注意力限制在这一已知的等距变换类上。

定义 2.12。若存在 $A \in \mathrm{GL}_n(\mathbb{F})$ 和 $\lambda \in \mathbb{F}^*$，使得两个 $[n, d)$ k、$r]_{\mathbb{F}}$ 本质秩度量码 $\mathcal{C}_1$ 与 $\mathcal{C}_2$ 等价，则称它们是等价的。

$$\mathcal{C}_2 = \lambda \mathcal{C}_1 \cdot A := \{\lambda f \cdot A \mid f \in \mathcal{C}_1\}.$$

在这种情形下，我们记作 $\mathcal{C}_1 \cong \mathcal{C}_2$。

3. Construction of Codes with Large Essential Rank

本节将推导一种构造本质秩度量码的方法，使其具有较大的最小距离。我们将利用 $\mathbb{F}$ 的一个次数为 n 的辅助循环伽罗瓦扩张，并推广 Delsarte-Gabidulin 码在秩度量下的构造。

设 $\mathbb{L}$ 是 $\mathbb{F}$ 的一个次数为 n 的循环伽罗瓦扩张。设 σ 是 $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ 的一个生成元。考虑相关的代数扩张

$$S_n(\mathbb{L}) = S_n(\mathbb{F}) \otimes_{\mathbb{F}} \mathbb{L} = \mathbb{L}[x_1, \dots, x_n], \qquad S_{n,d}(\mathbb{L}) = S_{n,d}(\mathbb{F}) \otimes_{\mathbb{F}} \mathbb{L} = \mathbb{L}[x_1, \dots, x_n]_d,$$

$$T_n(\mathbb{L}) = T_n(\mathbb{F}) \otimes_{\mathbb{F}} \mathbb{L} = \mathbb{L}[\partial_1, \dots, \partial_n], \qquad T_{n,d}(\mathbb{L}) = T_{n,d}(\mathbb{F}) \otimes_{\mathbb{F}} \mathbb{L} = \mathbb{L}[\partial_1, \dots, \partial_n]_d.$$

设 $\alpha^{(1)}$、……、$\alpha^{(d)} \in \mathbb{L}^n$ 是 $\mathbb{L}$ 的 $\mathbb{F}$-基，并设 $1 \le \rho \le n$。我们定义空间

$$\mathcal{C}_\rho^{n,d}(\alpha^{(1)}, \dots, \alpha^{(d)}) := \left\{ \alpha^{(1)}(\partial) \prod_{j=2}^{d} \sigma^{r_j}(\alpha^{(j)})(\partial) \;\middle|\; 0 \le r_2, \dots, r_d \le \rho - 2 \right\}^{\perp} \cap S_{n,d}(\mathbb{F}).$$

当 $d > 2$ 时，该空间是对称Delsarte-Gabidulin码的推广。我们将在第 5 节看到，对于 $d = 2$，我们的构造与[22]中给出的构造一致。本节其余部分将分析这些码的参数：最小本质秩距离和维数。

3.1. 最小距离。

本小节旨在证明最小本质秩距离的以下下界。

定理 3.1. 对于每个 $f \in \mathcal{C}^{n,}{}_{\rho}{}^{d}(\alpha^{(1)}, \dots, \alpha^{(d)}) \setminus \{0\}$，均有 $\mathrm{ess}(f) \ge \rho$。

为了证明定理3.1，我们需要一些辅助结果。我们从$d = 1$情形开始。

引理 3.2. 我们有 $\mathcal{C}^{n,}{}_{\rho}{}^{1}(\alpha) = \{0\}$。

证明. 令 $f \in \mathcal{C}^{n,}{}_{\rho}{}^{1}(\alpha)$，并将 $f = c(x)$ 写成某个 $c = (c_1, \dots, c_n) \in \mathbb{F}^n$。则

$$0 = \alpha(\partial) \circ c(x) = c(\alpha) = \sum_{i=1}^{n} c_i \alpha_i.$$

由于 $\alpha_1, \dots, \alpha_n$ 在 $\mathbb{F}$ 上线性相关，这意味着 $c_1, \dots, c_n = 0$。因此 $f = 0$。 □

以下引理给出了证明定理 3.1 的归纳步骤。

引理 3.3. 设 $d \ge 2$，$f \in \mathcal{C}^{n,}{}_{\rho}{}^{d}(\alpha^{(1)}, \dots, \alpha^{(d)})$，并假设对于某个 $g \in \mathbb{F}[y_1, \dots, y_{\rho-1}]_d$ 以及线性无关的 $\ell_1, \dots, \ell_{\rho-1} \in S_{n,1}(\mathbb{F})$，有 $f = g(\ell_1, \dots, \ell_{\rho-1})$。那么

$$\frac{\partial g}{\partial y_i}(\ell_1, \dots, \ell_{\rho-1}) \in \mathcal{C}_\rho^{n,d-1}(\alpha^{(1)}, \dots, \alpha^{(d-1)})$$

对所有 $i \in \{1, \dots, \rho - 1\}$。

证明。令 $r = (r_2, \dots, r_{d-1}) \in \{0, \dots, \rho - 2\}^{d-2}$，$r_d \in \{0, \dots, \rho - 2\}$ 并记

$$W_{d-1}^{r}(\partial) := \alpha^{(1)}(\partial) \sigma^{r_2}(\alpha^{(2)})(\partial) \cdots \sigma^{r_{d-1}}(\alpha^{(d-1)})(\partial).$$

我们有

$$\begin{aligned} 0 &= (W_{d-1}^r(\partial)\sigma^{r_d}(\alpha^{(d)})(\partial)) \circ f \\ &= (W_{d-1}^r(\partial)\sigma^{r_d}(\alpha^{(d)})(\partial)) \circ g(\ell_1, \ldots, \ell_{\rho-1}) \\ &= W_{d-1}^r(\partial) \circ (\sigma^{r_d}(\alpha^{(d)})(\partial) \circ g(\ell_1, \ldots, \ell_{\rho-1})) \\ &= W_{d-1}^r(\partial) \circ \sum_{i=1}^{\rho-1} \sigma^{r_d}(A_i) \cdot \frac{\partial g}{\partial y_i}(\ell_1, \ldots, \ell_{\rho-1}) \\ &= \sum_{i=1}^{\rho-1} \sigma^{r_d}(A_i) \cdot \Big(W_{d-1}^r(\partial) \circ \frac{\partial g}{\partial y_i}(\ell_1, \ldots, \ell_{\rho-1})\Big), \end{aligned}$$

其中 $A_i := \alpha^{(d)}(\partial) \circ \ell_i = \ell_i(\alpha^{(d)})$。因此我们看到

$$\begin{pmatrix} A_1 & \cdots & A_{\rho-1} \\ \vdots & & \vdots \\ \sigma^{\rho-2}(A_1) & \cdots & \sigma^{\rho-2}(A_{\rho-1}) \end{pmatrix} \begin{pmatrix} W_{d-1}^r(\partial) \circ \frac{\partial g}{\partial y_1}(\ell_1, \ldots, \ell_{\rho-1}) \\ \vdots \\ W_{d-1}^r(\partial) \circ \frac{\partial g}{\partial y_{\rho-1}}(\ell_1, \ldots, \ell_{\rho-1}) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \tag{4}$$

对所有 $r \in \{0, \ldots, \rho-2\}^{d-2}$。由 [17, 推论 4。13], 定义线性方程组（4）的矩阵是可逆的，从而得到

$$W_{d-1}^r(\partial) \circ \frac{\partial g}{\partial y_i}(\ell_1, \ldots, \ell_{\rho-1}) = 0$$

对所有 $r \in \{0, \ldots, \rho-2\}^{d-2}$ 和 $i \in \{1, \ldots, \rho-1\}$。因此，

$$\frac{\partial g}{\partial y_i}(\ell_1, \ldots, \ell_{\rho-1}) \in \mathcal{C}_\rho^{n,d-1}(\alpha^{(1)}, \ldots, \alpha^{(d-1)})$$

对所有 $i \in \{1, \ldots, \rho-1\}$。 □

现在我们可以给出定理 3.1 的证明。

定理 *3.1* 的证明。现在我们将证明，如果 $f \in \mathcal{C}^{n,\ \rho\ d}(\alpha^{(1)}, \ldots, \alpha^{(d)})$ 满足

$$f = g(\ell_1, \ldots, \ell_{\rho-1})$$

对于某个 $g \in \mathbb{F}[y_1, \ldots, y_{\rho-1}]_d$ 且线性无关的 ℓ_1，...，$\ell_{\rho-1} \in S_{n,\ 1}(\mathbb{F})$，则必然有 $f = 0$。我们对 d 采用归纳法。对于 $d = 1$，有 $f \in \mathcal{C}^{n,\ \rho\ 1}(\alpha) = \{0\}$，由引理 3.2 可知，因此 $f = 0$。对于 $d \geq 2$，由引理 3.3 我们知道

$$\frac{\partial g}{\partial y_i}(\ell_1, \ldots, \ell_{\rho-1}) \in \mathcal{C}_\rho^{n,d-1}(\alpha^{(1)}, \ldots, \alpha^{(d-1)})$$

对于所有 $i \in \{1, \ldots, \rho-1\}$。根据我们的归纳假设，可得

$$\frac{\partial g}{\partial y_i}(\ell_1, \ldots, \ell_{\rho-1}) = 0$$

对于所有 $i \in \{1, \ldots, \rho-1\}$。由于 ℓ_1、...、$\ell_{\rho-1}$ 线性无关，我们得到对所有 $i \in \{1, \ldots, \rho-1\}$均有 $\frac{\partial g}{\partial y_i} = 0$。因此

$$g = \frac{1}{d} \sum_{i=1}^{\rho-1} y_i \frac{\partial g}{\partial y_i} = 0$$

因此，$f = g(\ell_1, \ldots, \ell_{\rho-1}) = 0$。 □

例 3.4. 设 $(n, d, \rho) = (4, 3, 3)$。考虑域 $\mathbb{F} = \mathbb{F}_5$ 及其扩域 $\mathbb{L} = \mathbb{F}_{5^4} = \mathbb{F}_5(\gamma)$，其中 γ 是满足 $\gamma^4 = \gamma^2 + \gamma + 3$ 的 $\mathbb{L}$ 的本原元。取 $\alpha^{(1)} = \alpha^{(2)} = \alpha^{(3)} = (1, \gamma, \gamma^2, \gamma^3) =: \alpha$。设

$$\mathcal{B} = (x_1^3, x_1^2 x_2, \ldots, x_3 x_4^2, x_4^3)$$

为由所有按字典序排列的单项式组成的 $\mathbb{F}_5[x_1,x_2,x_3,x_4]_3$ 的基。那么 $\mathcal{C}^{4,\ 3\,3}(\alpha,\alpha,\alpha)$ 的生成矩阵为

$$\begin{pmatrix}
1&0&0&0&0&0&0&0&4&4&2&2&3&1&3&4&2&3&3&4\\
0&1&0&0&0&0&0&0&1&2&1&1&3&1&1&1&0&4&2&4\\
0&0&1&0&0&0&0&0&1&0&0&1&0&1&3&0&1&4&4&0\\
0&0&0&1&0&0&0&0&0&1&0&0&1&0&1&3&0&1&4&4\\
0&0&0&0&1&0&0&0&4&4&1&3&4&3&1&1&3&0&4&1\\
0&0&0&0&0&1&0&0&1&3&1&0&1&2&2&4&3&3&3&4\\
0&0&0&0&0&0&1&0&4&3&0&0&0&0&3&3&0&1&3&1\\
0&0&0&0&0&0&0&1&3&3&1&0&1&4&4&4&2&0&2&4
\end{pmatrix}$$

相对于基 $\mathcal{B}$。矩阵的第一行对应于多项式

$f := x_1^3-x_1x_3x_4-x_1x_4^2+2x_2^3+2x_2^2x_3-2x_2^2x_4+x_2x_3^2-2x_2x_3x_4-x_2x_4^2+2x_3^3-2x_3^2x_4-2x_3x_4^2-x_4^3$

含 $\mathrm{ess}(f) = 4$。

3.2. 维数。本小节中，我们给出关于所构造码的维数的估计。为简单起见，我们将范围限制为如下形式的码

$$\mathcal{C}_\rho^{n,d}(\alpha) := \mathcal{C}_\rho^{n,d}(\alpha,\dots,\alpha).$$

我们首先证明，$\mathcal{C}^{n,\ d}_{,\rho}(\alpha^{(1)},\dots,\alpha^{(d)})$ 的维数与 $\mathbb{F}$-基 $\alpha^{(1)},\dots,\alpha^{(d)}$ 的选取无关，因此这一限制并无影响。

命题 3.5. 设 $\alpha^{(1)},\dots,\alpha^{(d)},\beta$ 是 $\mathbb{F}$ 的 $\mathbb{L}$-基。则：

(1) We have $\mathcal{C}_\rho^{n,d}(\alpha^{(1)},\dots,\alpha^{(d)}) \cong \mathcal{C}_\rho^{n,d}(\beta,\alpha^{(2)},\dots,\alpha^{(d)})$.
(2) We have $\mathcal{C}_\rho^{n,d}(\alpha^{(1)},\dots,\alpha^{(d)}) = \mathcal{C}_\rho^{n,d}(\alpha^{(1)},\alpha^{(\pi(2))},\dots,\alpha^{(\pi(d))})$ for every permutation π of $\{2,\dots,d\}$.
(3) We have $\mathcal{C}_\rho^{n,d}(\alpha^{(1)},\dots,\alpha^{(d)}) \cong \mathcal{C}_\rho^{n,d}(\alpha^{(1)},\dots,\alpha^{(d-1)},\beta)$.

证明。（1）设 $A\in \mathrm{GL}_n(\mathbb{F})$ 满足 $A\alpha^{(1)} = \beta$，并设 $f \in \mathcal{C}^{n,\ \rho\ d}(\beta,\alpha^{(1)},\dots,\alpha^{(d)})$。那么，对于每个 $r = (r_2,\dots,r_d) \in \{0,\dots\rho-2\}^{d-1}$，我们有

$$\begin{aligned}
0 &= \beta(\partial)\circ(Z_{d-1}^r(\partial)\circ f)\\
&= \alpha^{(1)}(\partial\cdot A)\circ(Z_{d-1}^r(\partial)\circ f)\\
&= \alpha^{(1)}(\partial)\circ(Z_{d-1}^r(\partial)\circ f)(x\cdot A)\\
&= \alpha^{(1)}(\partial)Z_{d-1}^r(\partial)\circ(f(x\cdot A)).
\end{aligned}$$

其中 $Z_{d-1}^r(\partial) = \prod_{j=2}^d \sigma^{r_j}(\alpha^{(j)})(\partial)$。这表明

$$\mathcal{C}_\rho^{n,d}(\alpha^{(1)},\dots,\alpha^{(d)})\cdot A = \mathcal{C}_\rho^{n,d}(\beta,\alpha^{(2)},\dots,\alpha^{(d)}).$$

（2）根据 $T_n(\mathbb{L})$ 中的交换性，这一点显然成立。
（3）证明过程与（1）相同，只需利用 $A\in\mathrm{GL}(n,\mathbb{F})$ 中的矩阵在 σ 下保持不变这一附加性质。□

因此，从现在起，我们假设 $\alpha := \alpha^{(1)},\dots,\alpha^{(d)}$ 全部相等。在此情形下，我们首先给出 $\mathcal{C}^{n,\ \rho\ d}(\alpha)$ 的两种等价描述。

引理 3.6. 我们有

$$\begin{aligned}
\mathcal{C}_\rho^{n,d}(\alpha) &= \left\{\prod_{j=1}^d \sigma^{r_j}(\alpha)(\partial)\ \middle|\ 0\le r_1,\dots,r_d\le\rho-2\right\}^\perp \cap S_{n,d}(\mathbb{F})\\
&= \left\{\prod_{j=1}^d \sigma^{r_j}(\alpha)(\partial)\ \middle|\ 0=r_1\le r_2\le\cdots\le r_d\le\rho-2\right\}^\perp \cap S_{n,d}(\mathbb{F}).
\end{aligned}$$

证明。考虑第一个等式。显然，包含关系 $\supseteq$ 成立。令 $f \in \mathcal{C}^{n,}{}_{\rho}{}^{d}(\alpha)$。为证明等式成立，我们需要证明对于所有 $0 \leq r_1, \ldots\ldots, r_d \leq \rho - 2$, $\prod_{j=1}^{d} \sigma^{r_j}(\alpha)(\partial) \circ f = 0$。由于 $\sigma^{r_j}(\alpha)(\partial)$'s 彼此交换，我们已经知道当 $r := \min(r_1, \ldots\ldots, r_d) = 0$ 时该结论成立。一般地，我们注意到

$$\prod_{j=1}^{d} \sigma^{r_j}(\alpha)(\partial) \circ f = \sigma^{r} \left(\prod_{j=1}^{d} \sigma^{r_j - r}(\alpha)(\partial) \circ f \right) = \sigma^{r}(0) = 0$$

因为 $r_j - r = 0$，其中 $j \in \{1, \ldots, d\}$。因此，第一个等式成立。第二个等式显然可由以下事实得出：$\sigma^{r_j}(\alpha)(\partial)$彼此可交换。□

引理 3.6 给出了关于 $\mathcal{C}^{n,}{}_{\rho}{}^{d}(\alpha)$ 的余维的第一个上界。具体而言，子空间 $\mathcal{C}^{n,}{}_{\rho}{}^{d}(\alpha)$ 由以下方程定义

$$\begin{aligned} \binom{(d-1)+(\rho-2)}{d-1} &= \#\{(\delta_1, \ldots, \delta_d) \in \mathbb{Z}_{\geq 0}^{d} \mid \delta_1 + \ldots + \delta_d = \rho - 2\} \\ &= \#\{(r_2, \ldots, r_d) \in \mathbb{Z}_{\geq 0}^{d-1} \mid 0 = r_1 \leq r_2 \leq \cdots \leq r_d \leq r_{d+1} = \rho - 2\} \end{aligned}$$

$\mathbb{L}$上的方程，其中每个方程都可以解释为 $\mathbb{F}$上的 n 方程。这里第二个等式中我们使用了 $\delta_i = r_{i+1} - r_i$。由此得到以下结果。

命题 3.7。我们有

$$\dim \mathcal{C}_{\rho}^{n,d}(\alpha) \geq \binom{n+d-1}{d} - n\binom{d+\rho-3}{d-1}.$$

对于一个 m 关于 $\mathcal{C}^{n,}$ 维数的更精确下界 $_{\rho}{}^{d}(\alpha)$，我们必须更好地理解条件以及

$$\prod_{j=1}^{d} \sigma^{r_j}(\alpha)(\partial) \circ f = 0$$

它们之间的关系。

引理 3.8。设 $f \in \mathbb{F}[x_1, \ldots, x_n]_d$和 $r_1, \ldots\ldots, r_d, s_1, \ldots\ldots, s_d \in \mathbb{Z}$。假设存在一个 $x \in \mathbb{Z}$，使得对于所有 $j \in \{1, \ldots, d\}$, $r_j = x + s_j$模 n。则

$$\prod_{j=1}^{d} \sigma^{r_j}(\alpha)(\partial) \circ f = 0 \quad \text{if and only if} \quad \prod_{j=1}^{d} \sigma^{s_j}(\alpha)(\partial) \circ f = 0.$$

证明。我们有

$$\prod_{j=1}^{d} \sigma^{r_j}(\alpha)(\partial) \circ f = \prod_{j=1}^{d} \sigma^{x+s_j}(\alpha)(\partial) \circ f = \sigma^{x} \left(\prod_{j=1}^{d} \sigma^{s_j}(\alpha)(\partial) \circ f \right)$$

由于 $\sigma^{n} = \mathrm{id}$，因此所述等价关系成立。□

下面的例子表明，即使限制在情形 $r_1 = 0$ 且 $r_2 \leq \cdots \leq r_d$ 下，定义 $\mathcal{C}^{n,}{}_{\rho}{}^{d}(\alpha)$ 的条件也可能是冗余的。

例 3.9。设 $d = 3$, $f \in \mathbb{F}[x_1, \ldots, x_n]_d$，记 $x := \rho - 2$，并假设 $n = 2x$ 成立。那么

$$\alpha(\partial)\alpha(\partial)\sigma^{x}(\alpha)(\partial) \circ f = 0 \quad \text{if and only if} \quad \alpha(\partial)\sigma^{x}(\alpha)(\partial)\sigma^{x}(\alpha)(\partial) \circ f = 0$$

由于 $(x, x, 0) \equiv (0, 0, x) + (x, x, x)$ 模 n 可以重新排列为 $(0, x, x)$。

注 3.10。当 $0 < \mathrm{char}\,\mathbb{F} \leq d$ 时，还存在另一种冗余：我们有

$$\alpha(\partial)^{d} \circ f = d! f(\alpha) = 0$$

因此，条件 $\alpha(\partial)^{d} \circ f = 0$ 得以平凡地满足。

由于 r_j 是 σ 的指数，我们可以自然地将它们视为 $\mathbb{Z}/n\mathbb{Z}$ 的元素。又由于 r_j 的顺序并不重要，我们看到，定义 $\mathcal{C}^{n,\ \rho}{}^{d}(\alpha)$ 的条件可以由多重集 $S = \{\!\{r_1, \ldots, r_k\}\!\}$ 进行索引。对于这样的多重集 S 和一个整数 $x \in \mathbb{Z}$，我们定义

$$x + S = \{\!\{x + y \bmod n \mid y \in S\}\!\}.$$

该运算定义了 $\mathbb{Z}$ 在集合 $\mathcal{M}^{n}$上的作用, ^{d} 即由所有元素均属于 d的 元多重集组成的集合。引理 3.8 表明，处于同一 $\mathbb{Z}$-轨道中的两个多重集定义了等价条件。因此， $\mathcal{C}^{n,\ \rho}{}^{d}(\alpha)$ 的余维至多为包含形如 $\{\!\{r_1, \ldots, r_d\}\!\}$ 且满足 $0 \le r_1$、……、 $r_d \le \rho - 2$ 的多重集的轨道数乘以 n 。我们猜想等号成立。

猜想 3.11。设 $\operatorname{char}\mathbb{F} = 0$ 或 $\operatorname{char}\ \mathbb{F} > d$ 且 $1 \le \rho \le n$。则 $\mathcal{C}^{n,\ \rho}{}^{d}(\alpha)$ 在 $\mathbb{F}[x_1, \ldots, x_n]_d$ 中的余维等于 n 乘以 $\mathcal{M}^{n}$中包含形如 $\{\!\{r_1, \ldots, r_d\}\!\}$ 且满足 $0 \le r_1$、……、 $r_d \le \rho - 2$ 的多重集的 $\mathbb{Z}$-轨道数。

关于此类轨道数量的更多信息，请参见附录。

本节最后，我们将考察相对于命题 2.9 的类 Singleton 界而言，我们的码距离最优码还有多远。由命题 2.9 和 3.7，可得

$$s(n, d, \rho) \le \dim \mathcal{C}_{\rho}^{n,d}(\alpha) \le r(n, d, \rho).$$

for

$$\begin{aligned} s(n, d, \rho) &:= \binom{n + d - 1}{d} - n\binom{\rho + d - 3}{d - 1}, \\ r(n, d, \rho) &:= \binom{n + d - 1}{d} - \binom{\rho + d - 2}{d}. \end{aligned}$$

现在我们渐近地比较 $s(n, d, \rho)$ 和 $r(n, d, \rho)$ 的值，以确定我们的码与最优码有多接近。

首先，当 d、ρ 固定时，有

$$\begin{aligned} s(n, d, \rho) &\sim n^d/d! \\ r(n, d, \rho) &\sim n^d/d! \end{aligned}$$

当 n 趋于无穷大时。由此可见，按照类 Singleton 界，我们的码具有最大维数。当 d 固定且 $\rho = \tau n$ 对某个常数 $0 < \tau < 1$ 时，则有

$$\begin{aligned} s(n, d, \rho) &\sim (1 - d\tau^{d-1}) \cdot n^d/d! \\ r(n, d, \rho) &\sim (1 - \tau^d) \cdot n^d/d! \end{aligned}$$

在这种情形下，我们的码距离命题 $\frac{1-\tau^d}{1-d\tau^{d-1}}$的上界还差一个因子2.9。不过，这可能是由多种原因造成的。首先，通过进一步研究 $\mathcal{C}^{n,\ \rho}{}^{d}(n,\ d)$ 的 $\mathbb{Z}$-轨道，可以改进 $\mathcal{M}^{n,\ d}$ 维数的下界，如上文所述。另一方面，我们认为命题 2.9 的界也可以改进。事实上，我们将在第 5 节看到，对于 $d = 2$ 且当 $\mathbb{F}$ 为有限时，Schmidt [22]证明了一个更好的上界。

4. 解码算法

在本节中，为了简便起见，我们再次令 $\alpha := \alpha^{(1)}, \ldots, \alpha^{(d)}$ 相等，并将 $\mathcal{C}_{\rho}^{d}(\alpha) := \mathcal{C}^{n}{}_{,\rho}{}^{d}(\alpha, \ldots, \alpha)$ 记为。假设发送的是 $f \in \mathcal{C}_{\rho}^{d}(\alpha)$，接收到的是 $F = f + g'$，且 $\operatorname{ess}(g') = e \le (\rho - 1)/2$。因此，对于某个 $g \in S_{e,d}(\mathbb{F})$ 以及线性无关的 $\ell_1, \ldots, \ell_e \in S_{n,1}(\mathbb{F})$，有 $g' = g(\ell_1, \ldots, \ell_e)$。我们的目标是重构 f。为此，我们将解码分为两部分：首先重构 $V_{\mathrm{ess}}(g') = \langle \ell_1, \ldots, \ell_e \rangle_{\mathbb{F}}$，然后恢复 g'。显然，同时知道 F 和 g' 后，我们就能重构原始码字 f。

4.1. 恢复 $V_{\text{ess}}(g')$。对于多项式 $h \in S_n(\mathbb{L})$，我们将 $\text{coeff}_1(h) \ldots, \text{coeff}_n(h) \in S_n(\mathbb{F})$定义为满足以下条件的多项式

$$h = \alpha_1 \operatorname{coeff}_1(h) + \ldots + \alpha_n \operatorname{coeff}_n(h).$$

对于 $k \in \{1, \ldots, d\}$ 和 $r = (r_1, \ldots, r_k) \in \{0, \ldots, \rho - 2\}^k$，记作

$$Z_k^r(\partial) := \prod_{j=1}^{k} \sigma^{r_j}(\alpha)(\partial) \in T_{n,k}(\mathbb{L}).$$

我们有如下结果。

命题 4.1。空间 $V_{\text{ess}}(g')$ 由以下元素张成

$$\left\{ \operatorname{coeff}_i \left(Z_{d-1}^r(\partial) \circ g(\ell_1, \ldots, \ell_e) \right) \,\middle|\, i \in \{1, \ldots, n\}, r \in \{0, \ldots, \rho - 2\}^{d-1}, r_1 = 0 \right\}.$$

证明。通过坐标变换，不妨设对每个 $j \in \{1, \ldots, e\}$都有 $\ell_j = x_j$。现在，对于 $k \geq 1$，定义 $F_k \subseteq T_{e,k}(\mathbb{F})$ 为由所有元素张成的子空间

$$\left\{ \operatorname{coeff}_i \left(Z_k^r(\partial)|_{\partial_{e+1}, \ldots, \partial_n = 0} \right) \,\middle|\, i \in \{1, \ldots, n\}, r \in \{0, \ldots, \rho - 2\}^k, r_1 = 0 \right\}.$$

我们断言 $F_k = T_{e,k}(\mathbb{F})$。

回顾一下，映射$\Phi_{e,\,k}\colon S_{e,\,k}(\mathbb{F}) \times T_{e,\,k}(\mathbb{F}) \longrightarrow \mathbb{F}$ 定义于（2）是一个完美配对。若 $F_k \neq T_{e,\,k}(\mathbb{F})$，则 $F_k^{\perp}$包含一个非零多项式$h \in S_{e,\,k}(\mathbb{F})$。将 h 视为$S_{n,\,k}(\mathbb{F})$中的一个元素。于是 $h \in \mathcal{C}_\rho^k(\alpha)$。事实上，

$$\frac{\partial h}{\partial x_{e+1}} = \cdots = \frac{\partial h}{\partial x_n} = 0$$

我们看到

$$\begin{aligned} 0 &= \Phi_{e,k} \left(h, \operatorname{coeff}_i \left(Z_k^r(\partial)|_{\partial_{e+1}, \ldots, \partial_n = 0} \right) \right) \\ &= \operatorname{coeff}_i \left(Z_k^r(\partial)|_{\partial_{e+1}, \ldots, \partial_n = 0} \right) \circ h \\ &= \operatorname{coeff}_i \left((Z_k^r(\partial)|_{\partial_{e+1}, \ldots, \partial_n = 0}) \circ h \right) \\ &= \operatorname{coeff}_i \left(Z_k^r(\partial) \circ h \right) \end{aligned}$$

对所有的 $i \in \{1, \ldots, n\}$ 和 $r \in \{0, \ldots, \rho - 2\}^k$均成立。然而，$\text{ess}(h) \leq e \leq (\rho - 1)/2$，且 $\mathcal{C}_\rho^k(\alpha)$中的每个非零元素的本质秩均为 $\geq \rho$。这是一个矛盾，因此$F_k = T_{e,\,k}(\mathbb{F})$。

最后，我们注意到

$$V_{\text{ess}}(g') = \langle x_1, \ldots, x_e \rangle_{\mathbb{F}} = \Phi_{e,d,d-1}(g(x_1, \ldots, x_e), T_{e,d-1}(\mathbb{F})) = \Phi_{e,d,d-1}(g(x_1, \ldots, x_e), F_{d-1})$$

恰好由所述集合张成。 □

实际上，我们可以改进命题 4.1：注意到可以减少空间 $V_{\text{ess}}(g')$ 的生成元数量。事实上，由于对 r 的各个条目进行置换$Z_k^r(\partial)$ 后得到的结果相同，因此我们实际上只需考虑那些 r 条目按非递减顺序排列的情形。换句话说，定义

$$X_{k,\rho} := \{(0, r_2, \ldots, r_k) \in \{0, \ldots, \rho - 2\}^k \mid 0 \leq r_2 \leq \ldots \leq r_k\}.$$

推论 4.2. 空间 $V_{\text{ess}}(g')$ 由以下元素张成：

$$\left\{ \operatorname{coeff}_i \left(Z_{d-1}^r(\partial) \circ g(\ell_1, \ldots, \ell_e) \right) \,\middle|\, r \in X_{d-1,\rho} \right\}.$$

根据推论 4.2 ，我们知道，为了重构 $V_{\text{ess}}(g')$，只需高效地恢复

$$Z_{d-1}^r(\partial) \circ g(\ell_1, \ldots, \ell_e) =: h^r(x)$$

对于 $r \in X_{d-1,\,\rho}$。记 $h_i^r(x) :=$ 系数$_i(h^r)$，使得

$$h^r(x) = \alpha_1 \operatorname{coeff}_1(h^r) + \ldots + \alpha_n \operatorname{coeff}_n(h^r) = \alpha_1 h_1^r(x) + \ldots + \alpha_n h_n^r(x).$$

计算 $(h_1^r(x)\dots,h_n^r(x))$ 的问题可以转化为对 $\mathbb{L}^n\cong\mathbb{F}^{n\times n}$ 中某个具有最小距离 ρ 的 Gabidulin 码进行译码的问题。下面将解释这种联系。

4.1.1. 综合征译码。对于每个 $u\in X_{d,\ \rho}$，我们计算 F 的 u-综合征，其定义为

$$s_u:=Z_d^u(\partial)\circ F\in\mathbb{L}.$$

当 $v\in\{0,\dots,\rho-2\}^d$ 可以重排为 $u\in X_{d,\ \rho}$ 时，我们记作 $s_v=s_u$。取 $\beta:=\sigma^{-\rho+2}(\alpha)\in\mathbb{L}^n$，并定义 $\gamma=(\gamma_1,\dots,\gamma_n)\in\mathbb{L}^n$ 为下式的唯一解（相差一个 $\mathbb{L}$-标量倍数）：

$$\sum_{j=1}^{n}\sigma^i(\beta_j)\gamma_j=0,\qquad\text{for all } i\in\{0,\dots,n-1\}\setminus\{n-\rho+1\}. \tag{5}$$

我们考虑以下 Gabidulin 码

$$\mathcal{G}^{\sigma}_{\rho,n}(\gamma):=\{(\mathrm{ev}_{\gamma_1}(f),\dots,\mathrm{ev}_{\gamma_n}(f))\mid f\in\mathbb{L}[\sigma],\deg_\sigma(f)\le n-\rho\}\subseteq\mathbb{L}^n, \tag{6}$$

其中，对于 $f=\sum_i f_i\sigma^i\in\mathbb{L}[\sigma]$ 和 $\alpha\in\mathbb{L}$，我们定义 $\mathrm{ev}_\alpha(f):=\sum_i f_i\sigma^i(\alpha)$。

Gabidulin 码因其数学特性和高效的译码算法，构成了秩度量中最重要的一类码。它们最初由 Delsarte [9], 引入，后来又由 Gabidulin [11]重新发现。它们最显著的性质是，对于给定参数，其最小秩距离达到可能的最大值。更具体地说，我们可以在空间 $\mathbb{L}^n$ 上赋予一个权函数，即$\mathbb{F}$-秩权重，定义如下：

$$\mathrm{rk}_{\mathbb{F}}(v)=\dim_{\mathbb{F}}\langle v_1,\dots,v_n\rangle_{\mathbb{F}},\qquad\text{for any } v=(v_1,\dots,v_n)\in\mathbb{L}^n.$$

秩重量诱导出所谓的秩距离，定义在 $\mathbb{L}^n$上。这样的度量空间与度量空间 ($\mathbb{F}$-线性等距同构（$\mathbb{F}^{n\times n}$,$\mathrm{d_{rk}}$）；参见第 5 节。文献 [9, 11] 证明，对于任意$1\le\rho\le n$，Gabidulin 码中非零码字的最小秩重量为 $\mathcal{G}^{\sigma}_{\rho,\ n}(\gamma)$ 为 ρ。此外，$(\mathcal{G}^{\sigma}_{\rho,\ n}(\gamma)$ 的校验矩阵（见式 6）为

$$H^{\sigma}_{\rho,n}(\beta)=\begin{pmatrix}\beta_1 & \beta_2 & \cdots & \beta_n\\ \sigma(\beta_1) & \sigma(\beta_2) & \cdots & \sigma(\beta_n)\\ \vdots & \vdots & & \vdots\\ \sigma^{\rho-2}(\beta_1) & \sigma^{\rho-2}(\beta_2) & \cdots & \sigma^{\rho-2}(\beta_n)\end{pmatrix}. \tag{7}$$

据此，对于任意 $v\in\mathbb{L}^n$，我们将向量 $v(H^{\sigma}_{\rho,n}(\beta))^\top$ 称为其 H-综合。需要指出的是，有若干种 Gabidulin 码译码算法会用到 H-综合的计算。给定矩阵 $H^{\sigma}_{\rho,n}(\beta)$ 和向量 $s\in\mathbb{L}^{\rho-1}$，这些算法会返回秩重量不超过 $\frac{\rho-1}{2}$ 的唯一向量 $v\in\mathbb{L}^n$，使得$v(H^{\sigma}_{\rho,n}(\beta))^\top=s$；如果这样的向量存在的话。关于 Gabidulin 码的译码详情，感兴趣的读者可参阅 [3, 第 2 节8] 及其中的参考文献。

Pr命题 4.3。 令 r_2、……、$r_{d-1}\in\{0,\dots,\rho-2\}$，并取 $r=(0$、r_2、……、$r_{d-1})$。该 n

$$(h_1^r(\alpha),\dots,h_n^r(\alpha))$$

向量是其 H-综合为 $(\sigma^{t-\rho+2}(s_{(r,\rho-2-t)}))_{t=0}^{\rho-2}$ 在$\mathcal{G}^{\sigma}_{\rho,\ n}(\gamma)$ 的最小秩重量错误向量。

证明。注意到

$$s_u=Z_d^u(\partial)\circ F=Z_d^r(\partial)\circ(f+g')=Z_d^u(\partial)\circ f+Z_d^u(\partial)\circ g'=Z_d^u(\partial)\circ g'.$$

我们有

$s_{(r,r_d)}=\sigma^{r_d}(\alpha)\quad(\partial)\circ h^r=\sigma^{r_d}(h_1^r(\alpha))\,\alpha_1+\ldots+\sigma^{r_d}(h_n^r(\alpha))\,\alpha_n$，对所有 $r_d\in\{0,\dots,\rho-2\}$ 均成立；或者等价地，对每个方程应用 σ^{-r_d}，

$$\sigma^{-r_d}(s_{(r,r_d)})=h_1^r(\alpha)\sigma^{-r_d}(\alpha_1)+\ldots+h_n^r(\alpha)\sigma^{-r_d}(\alpha_n),\qquad\text{for all } r_d\in\{0,\dots,\rho-2\}.$$

令 $r_d = \rho - 2 - t$，后一个方程组也可以改写为

$$\sigma^{t-\rho+2}(s_{(r,\rho-2-t)}) = h_1^r(\alpha)\sigma^t(\beta_1) + \ldots + h_n^r(\alpha)\sigma^t(\beta_n), \qquad \text{for all } t \in \{0,\ldots,\rho-2\}. \tag{8}$$

根据命题 4.1 我们有 $\langle h_1^r, \ldots\ldots, h_n^r\rangle_{\mathbb{F}} \subseteq V_{\text{ess}}(g')$，因此可以推 deduce 得到

$$\dim_{\mathbb{F}}\langle h_1^r(\alpha),\ldots,h_n^r(\alpha)\rangle_{\mathbb{F}} = \dim_{\mathbb{F}}\langle h_1^r,\ldots,h_n^r\rangle_{\mathbb{F}} \leq \dim_{\mathbb{F}} V_{\text{ess}}(g') = e \leq \frac{\rho-1}{2}.$$

因此我们看到，$(h_1^r(\alpha)$ ....., $h_n^r(\alpha))$ 确实是最小秩重量的向量，其 H-综合为 $(\sigma^{t-\rho+2}($ $s_{(r,\rho-2-t)}))_{t=0}^{\rho-2}$。□

因此，对于码 $\mathcal{G}_{\rho,\ n}^{\sigma}(\gamma)$ 的任意译码算法 $\mathsf{Dec}(H_{\rho,\ n}^{\sigma}(\beta)\ \cdot)$，我们可以首先恢复向量 $(h_1^r(\alpha)$ ....., $h_n^r(\alpha))\ = \mathsf{Dec}(H_{\rho,\ n}^{\sigma}(\beta)\ s)$，其中 $s := (\sigma^{t-\rho+2}(s_{(r,\rho-2-t)}))_{t=0}^{\rho-2}$。由此，我们随后可以恢复向量 $(h_1^r$ (x) ....., $h_n^r(x))$，最后

$$h^r = Z_{d-1}^r(\partial)\circ g(\ell_1,\ldots,\ell_e),$$

正如最初计划的那样。

4.2. 恢复 g'。现在我们已经找到了空间 $V_{\text{ess}}(g')$，首先任选其一组 $\mathbb{F}$-基，即 $(\ell_1,\ldots,\ell_e)$，然后进行坐标变换，使得对于所有 $i \in \{1,\ldots,e\}$，都有 $\ell_i = x_i$。我们希望恢复 $g' = g(x_1,\ldots,x_e) \in S_{e,\ d}(\mathbb{F})$，已知

$$s_r = Z_d^r(\partial)\circ g, \quad r \in X_{d,\rho}. \tag{9}$$

引理 4.4. 方程组至多有一个解

$$Z_d^r(\partial)\circ g = s_r, \quad r \in X_{d,\rho}.$$

证明. 假设 g_1, g_2 都是这些方程的解。那么 $g_1 - g_2 \in \mathcal{C}_\rho^d(\alpha)$。由于 $\mathcal{C}_\rho^d(\alpha)$的最小距离为 ρ，且 $g_1 - g_2$ 的本质秩为 $\leq \rho - 1$，这意味着$g_1 - g_2 = 0$。因此，该方程组至多有一个解。□

根据引理 4.4，现在我们确实可以恢复 g。下面总结译码算法。

算法 1：码的译码算法 $\mathcal{C}^{n,\ \rho\ d}(\alpha)$
数据：$n, d, \rho \in \mathbb{N}$，含有 $d \geq 2$ 和 $2 \leq \rho \leq n$、一个 $\mathbb{F}$-基 $\alpha \in \mathbb{L}^n$ 以及一个接收字 $F \in S_{n,\ d}(\mathbb{F})$，使得存在一个 $f \in \mathcal{C}^{n,\ \rho\ d}(\alpha)$，且 $\mathsf{ess}(F-f) \leq \frac{\rho-1}{2}$
结果：原始码字 $f \in \mathcal{C}^{n,\ \rho\ d}(\alpha)$
$L := \emptyset$;
计算 $\sigma^i(\alpha)$，其中 $i \in \{1,\ldots,n-1\}$;
$\beta := \sigma^{-\rho+2}(\alpha)$;
当 $u \in X_{d,\rho}$ 时
$\quad s_u := Z_d^u(\partial)\ \circ F$;
end
当 $r \in X_{d-1,\rho}$ 时
$\quad s := (\sigma^{2-\rho}(s_{(r,\rho-2)})\ \sigma^{3-\rho}(s_{(r,\rho-3)}) \ldots, s_{(r,0)})$;
$\quad (h_1^r(\alpha)\ldots,h_n^r(\alpha)) := \mathsf{Dec}(H^{\sigma}{}_{\rho,n}(\beta)\ s)$;
$\quad L \leftarrow L \cup \{h_1^r(x)\ldots,h_n^r(x)\}$;
end
$(\ell_1,\ldots,\ell_e) :=$ 基(张成空间$_{\mathbb{F}}(L)\ \mathbb{F})$;
$g :=$求解((9));
$g' := g(\ell_1,\cdots\ \ell_e)$;
返回 $F - g'$

4.3. 算法 1 的复杂度。 我们将所有计算表示为在 $\mathbb{F}$ 和 $\mathbb{L}$上的运算，从而逐步分析算法 1 的计算成本。这是因为，根据 $\mathbb{L}$中元素表示方式的选择，某些运算可能更快或更慢。此外，还有一些针对有限域的扩域运算的更快算法。在本节的其余部分，令 ω 为矩阵乘法的指数，已证明其满足 $\omega \leq 2.37188$ [10]。

第一步是为 $i \in \{1, \ldots, n-1\}$ 计算 $\sigma^i(\alpha)$。如果相对于正规基表示 $\mathbb{L}$ 的元素，这可以在常数时间内完成（$\sigma^i(\alpha)$ 只是表示 α 的向量的第 i 次移位）；如果将 $\mathbb{L}$ 中的元素相对于任意 $\mathbb{F}$-基 $\beta_1, \ldots, \beta_n$ 表示，其中 $\sigma^i(\beta_j)$ 的值已知，则需要在 $\mathbb{F}$ 上进行 $\mathcal{O}(n^2)$ 次运算。无论采用哪种方式，这都不会是该算法中开销最大的步骤。

接下来，我们需要计算 F 对每个 $u \in X_{d,\ \rho}$ 的 u-综合征。实际上，我们对每个 $k \in \{1, \ldots, d\}$ 和 $u \in X_{k,\ \rho}$ 计算 $Z_k^u(\partial) \circ F$，以便利用以下事实：

$$Z_{k+1}^u(\partial) \circ F = \sigma^{u_{k+1}}(\alpha)(\partial) \circ (Z_k^{(0,u_2,\ldots,u_k)}(\partial) \circ F)$$

对于每个 $k \in \{1, \ldots, d-1\}$ 和 $u \in X_{k+1,\ \rho}$。因此，对于每个 $k \in \{1, \ldots, d\}$ 和 $u \in X_{k,\ \rho}$，我们需要计算 $L(\partial) \circ G$ 对于某个 $L \in \mathbb{L}^n$ 和 $G \in S_{n,\ d+1-k}(\mathbb{L})$，这需要在 $\mathbb{L}$ 上进行 $n\binom{n-1+d-k}{d-k}$ 次乘法和 $(n-1)\binom{n-1+d-k}{d-k}$ 次加法。由此得到的总数为

$$\sum_{k=1}^{d} \binom{\rho+k-3}{k-1}(2n-1)\binom{n-1+d-k}{d-k} = \mathcal{O}\left(n^d\right)$$

这一步在 $\mathbb{L}$ 上需要进行上述运算。

现在，对于每个 $r \in X_{d-1,\ \rho}$ 我们计算向量 s；如果相应元素采用正规基表示，则其代价可忽略不计，否则需要在 $\mathbb{F}$ 上进行 $\mathcal{O}(\rho n)$ 次运算。此外，我们求解译码实例 $\mathsf{Dec}(H_{\rho,\ n}^{\sigma}(\beta)\ s)$。当元素采用正规基表示时，这可以通过在 $\mathbb{L}$ 上进行 $\mathcal{O}(n^2)$ 次运算完成；例如参见 [3, 第 2 节8]。假设选择了正规基，这一步的总成本为在 $\mathbb{L}$ 上进行 $\mathcal{O}(n^2|X_{d-1,\ \rho}|) = \mathcal{O}(n^2\binom{d+\rho-4}{d-2})$ 次运算。

之后，我们需要从集合 L 中提取一个 $\mathbb{F}$-基，该集合张成空间为 $\mathsf{span}_{\mathbb{F}}(L)$，其大小为 $\leq n|X_{d-1,\ \rho}|$。由于元素 $h_i^j(x) \in L$ 是 $S_{n,1}(\mathbb{F})$ 的元素，因此它们是长度为 n 的向量。基的计算因此可以通过高斯消元完成，其在 $\mathbb{F}$ 上需要执行$\mathcal{O}(n^\omega|X_{d-1,\rho}|) = \mathcal{O}(n^\omega\binom{d+\rho-4}{d-2})$ 次运算；见 [5]。

最后，我们需要求解（9）。记

$$g = \sum_{t_1+\ldots+t_e=d} a_{t_1,\ldots,t_e} x_1^{t_1} \cdots x_e^{t_e},$$

我们看到，（9）变成了一个在 $\mathbb{L}$ 上、含有$|X_{d,\ \rho}|$ 个方程以及 $\binom{e+d-1}{d}$ 个变量$a_{t_1,\ \ldots,\ t_e}$ 的线性方程组。由于我们希望在 $\mathbb{F}$ 上求解，因此可以通过选取 $\mathbb{L}$ 的任意一个 $\mathbb{F}$-基，将每个方程转换为在 $\mathbb{F}$ 上的 n 个方程。这样总共得到

$$n|X_{d,\rho}| = n\binom{d+\rho-3}{d-1}$$

在 $\mathbb{F}$ 上的方程。这样的线性方程组可以使用高斯消元求解，其计算成本为 $\mathcal{O}(n|X_{d,\ \rho}|\binom{e+d-1}{d}^{\omega-1}) = \mathcal{O}(n\binom{d+\rho-3}{d-1}\binom{e+d-1}{d}^{\omega-1})$ 次在 $\mathbb{F}$ [5] 上的运算。

在采用非特定基表示 $\mathbb{L}$的元素时， $\mathbb{F}$上的乘法需要 $\mathbb{L}$ 成本 $\mathcal{O}$（n^2）次运算，而加法需要 $\mathcal{O}$（n）次运算。如果以更巧妙的方式表示$\mathbb{L}$ 的元素，则可以将乘法加速到在 $\mathbb{F}$上仅需$\mathcal{O}$（n）次运算。然而，这是否与拥有正规基相容并不总是显而易见。在有限域上，可以拥有 $\mathbb{L}$ 的 $\mathbb{F}$-基，这些基既是正规基，又具有 [18]的线性复杂度。当我们能够做到这一点时，就算法的

运算次数而言，其总计算成本为
$\mathbb{F}$

$$\mathcal{O}\left(n^3\binom{d+\rho-4}{d-2}+n\binom{d+\rho-3}{d-1}\binom{e+d-1}{d}^{\omega-1}+n^{d+1}\right).$$

假设 $e\simeq\frac{\rho}{2}$ 和 $\rho=\tau n$ 对于某个 $0<\tau<1$，则总成本为

$$\mathcal{O}(n^{d\omega})$$

在 $\mathbb{F}$ 上的运算。

注 4.5。 如果我们限制在 $d=2$ 的情形下，可以看出，我们的算法复杂度并非最优。我们可以直接使用包含 $\mathcal{C}^n$、$_\rho{}^2(\alpha)$ 且具有相同最小秩距离的经典 Gabidulin 码的译码器（这是由 Gabidulin 码的结构决定的），并以 $\mathcal{C}^n$、$_\rho{}^2(\alpha)$ 次 $\mathcal{O}(n^2)$ 在 $\mathbb{L}$ 上的运算进行译码，因而需要 $\mathcal{O}(n^3)$ 次 $\mathbb{F}$上的运算，而我们使用算法 $\mathcal{O}(n^{2\omega})$ 需要总计 $\mathbb{F}$ 上的运算。使用算法 1。这表明译码器的速度仍有改进空间。

5. Essential-rank-metric codes as rank-metric codes

本节旨在将本质秩度量码理论与秩距离赋予的、发展成熟的码理论联系起来。我们将借助 Carlini 的一个结果来实现这一点， [6], 该结果展示了如何将齐次多项式 f 的本质秩转换为与 f相关的特殊矩阵的秩，即其 第一催化矩阵。此外，我们还将把本质变量空间与矩阵的列支撑联系起来，即由其列生成的线性空间。

定义 5.1. 设 $z_1,\dots,z_m$ 是 $S_{n,d-1}(\mathbb{F})$ 的单项式基，并按字典序排列，其中 $m=\binom{n+d-2}{d-1}$。$f\in S_{n,d}(\mathbb{F})$ 的第一催化矩阵是矩阵 $C_f\in\mathbb{F}^{n\times m}$，其中

$$\partial_i\circ f=\sum_{j=1}^{m}(C_f)_{i,j}z_j.$$

下述定理是 Carlini 在 [6] 中证明的主要结果。它将齐次多项式的本质秩与其第一催化矩阵联系起来，并刻画本质变量空间。

定理 5.2（[6，命题 10]）。设 $f\in S_{n,d}(\mathbb{F})$，并假设 $\mathrm{char}(\mathbb{F})=0$ 或 $\mathrm{char}(\mathbb{F})>d$。则以下结论成立：

(1) $\mathrm{ess}(f)=\mathrm{rk}(C_f)$
(2) $V_{\mathrm{ess}}(f)=\{D\circ f\mid D\in T_{n,d-1}(\mathbb{F})\}$

我们通过展开例 2.5 来说明定理5.2。

例 5.3. 设

$$f=3x_1^3+8x_1^2x_2+5x_1^2x_3+12x_1x_2^2+4x_1x_2x_3+4x_1x_3^2+8x_2^3+2x_2x_3^2+x_3^3\in S_{3,3}(\mathbb{F})$$

如例 2.5 所示，并让我们计算 f的一阶和二阶偏导数：得到

$$\begin{aligned}\partial_1\circ f&=9x_1^2+16x_1x_2+10x_1x_3+12x_2^2+4x_2x_3+4x_3^2,\\ \partial_2\circ f&=8x_1^2+24x_1x_2+4x_1x_3+24x_2^2+2x_3^2,\\ \partial_3\circ f&=5x_1^2+4x_1x_2+8x_1x_3+4x_2x_3+3x_3^2\end{aligned}$$

and

$$\begin{aligned}\partial_1^2\circ f&=18x_1+16x_2+10x_3,\\ \partial_1\partial_2\circ f&=16x_1+24x_2+4x_3,\\ \partial_2^2\circ f&=24x_1+48x_2,\\ \partial_1\partial_3\circ f&=10x_1+4x_2+8x_3,\\ \partial_2\partial_3\circ f&=4x_1+4x_3,\\ \partial_3^2\circ f&=8x_1+4x_2+6x_3.\end{aligned}$$

因此， f 的第一催化矩阵为

$$C_f = \begin{pmatrix} 9 & 16 & 10 & 12 & 4 & 4 \\ 8 & 24 & 4 & 24 & 0 & 2 \\ 5 & 4 & 8 & 0 & 4 & 3 \end{pmatrix}.$$

根据定理 5.2，我们得到

$$\operatorname{ess}(f) = \operatorname{rk}(C_f) = 2$$

and

$$\begin{aligned} V_{\operatorname{ess}}(f) &= \langle \partial_1^2 \circ f, \partial_1\partial_2 \circ f, \partial_2^2 \circ f, \partial_1\partial_3 \circ f, \partial_2\partial_3 \circ f, \partial_3^2 \circ f \rangle_{\mathbb{F}} \\ &= \langle x_1 + 2x_2, x_1 + x_3 \rangle_{\mathbb{F}}. \end{aligned}$$

作为定理 5.2的推论，我们可以将度量空间 $(S_{n,d}(\mathbb{F}), \mathrm{d}_{\mathrm{ess}})$ 等距嵌入到由 $\mathbb{F}$ 上的 $n \times \binom{n+d-2}{d-1}$ 矩阵构成的空间中，其距离函数 d_{rk} 定义为

$$\mathrm{d}_{\mathrm{rk}}(A, B) = \operatorname{rk}(A - B), \quad A, B \in \mathbb{F}^{n \times \binom{n+d-2}{d-1}},$$

这称为秩距离。

推论 5.4. 假设 $\operatorname{char}(\mathbb{F}) = 0$ 或 $\operatorname{char}(\mathbb{F}) > d$。映射

$$\begin{array}{ccc} (S_{n,d}(\mathbb{F}), \mathrm{d}_{\mathrm{ess}}) & \longrightarrow & (\mathbb{F}^{n \times \binom{n+d-2}{d-1}}, \mathrm{d}_{\mathrm{rk}}) \\ f & \longmapsto & C_f \end{array}$$

是一个 $\mathbb{F}$-线性等距嵌入。

例 5.5。 设 $\mathcal{C}$ 是例 2.8中给出的本质秩度量码，即 $\mathcal{C} := \langle f_1, f_2 \rangle_F$，其中

$$\begin{aligned} f_1 &= 3x_1^3 + 8x_1^2x_2 + 5x_1^2x_3 + 12x_1x_2^2 + 4x_1x_2x_3 + 4x_1x_3^2 + 8x_2^3 + 2x_2x_3^2 + x_3^3, \\ f_2 &= x_1^3 + 2x_1x_2^2 + x_3^3. \end{aligned}$$

我们已经提到， $\mathcal{C}$ 是一个 $[(3,\ 3)2,\ 2]_{\mathbb{F}}$ 本质秩度量码。在此我们证明， $\mathcal{C}$ 的最小本质秩距离实际上为 2。利用推论5.4 中的嵌入可知， $\mathcal{C}$ 与秩度量码 $\mathcal{C}' := \langle C_{f_1},\ C_{f_2} \rangle_{\mathbb{F}} \subseteq \mathbb{F}^{3\times 6}$是等距的。矩阵 C_{f_1} 的第一催化矩阵 f_1 已在例 5.3中计算出，而矩阵 C_{f_2} 的第一催化矩阵 f_2 为

$$C_{f_2} = \begin{pmatrix} 3 & 0 & 0 & 2 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}.$$

显然可知 $\operatorname{rk}(C_{f_2}) = 3$。此外，任意形如 $C_{f_1} + \lambda C_{f_2}$ 且满足 $\lambda \in \mathbb{F}$ 的矩阵的第 3 列和第 5 列均线性无关。这表明，对于每个 $A \in \mathcal{C}'$，$\operatorname{rk}(A) \geq 2$，由此我们可以得出， $\mathcal{C}$ 的最小本质秩距离为 2。

注 5.6. 推论 5.4 使我们能够将 $S_{n,d}(\mathbb{F})$ 中的每个本质秩度量码与 $\mathbb{F}^{n\times\binom{n+d-2}{d-1}}$ 中的一个秩度量码对应起来。这些对应与等价相容：设 $\mathcal{C}_1$,$\mathcal{C}_2 \subseteq S_{n,d}(\mathbb{F})$ 是两个等价的本质秩度量码。这意味着存在 $A \in \mathrm{GL}(n, \mathbb{F})$ 和 $\lambda \in \mathbb{F}^*$，使得 $\mathcal{C}_2 = \lambda\mathcal{C}_1 \cdot A$。令 $S^{d-1}(A)$ 表示相对于单项式基、由式（3）中给出的线性映射 $S_{n,d-1}(\mathbb{F}) \to S_{n,d-1}(\mathbb{F})$ $g \mapsto g(x \cdot A)$ 所对应的矩阵。于是，对于所有 $f \in S_{n,d}(\mathbb{F})$，都有 $C_{\lambda f \cdot A} = \lambda A C_f S^{d-1}(A)^{-1}$，因此

$$\{C_f \mid f \in \mathcal{C}_2\} = \lambda A \cdot \{C_f \mid f \in \mathcal{C}_1\} \cdot S^{d-1}(A)^{-1} \text{ and } \{C_f \mid f \in \mathcal{C}_1\}$$

作为秩度量码等价；例如参见 [24,定义 9]。

推论 5.4 还使我们能够推导本质秩度量码参数的界。

推论 5.7. 假设 $\mathrm{char}(\mathbb{F}) = 0$ or $\mathrm{char}(\mathbb{F}) > d \geq 2$. 设 $\mathcal{C}$ 是一个 $[(n,d)\ k,r]_{\mathbb{F}}$本质秩度量码。那么

$$k \leq \binom{n+d-2}{d-1}(n-r+1).$$

证明。 由推论 5.4，我们知道 $\mathcal{C}$ 与秩度量码 $\mathcal{C}' \subseteq \mathbb{F}^{n\times\binom{n+d-2}{d-1}}$ 等距。因此，该推论可由秩度量码的 Singleton 界推出；例如参见 $\mathcal{C}'$ 。 [9]□

注 5.8。 推论 5.7 的界从不优于命题 2.9中的类 Singleton 界。事实上，对于固定的 n， d，考虑函数

$$\begin{aligned} F\colon \{1,\dots,n\} &\to \mathbb{Z} \\ r &\mapsto \binom{n+d-2}{d-1}(n-r+1) - \binom{n+d-1}{d} + \binom{r+d-2}{d}. \end{aligned}$$

我们有 $F(n) = 0$对于 $(a,b) = (n+d-2,d)$ 为 $\binom{a+1}{b} = \binom{a}{b} + \binom{a}{b-1}$。并且对于 $r \in \{1,\dots,n-1\}$，我们有

$$\begin{aligned} F(r) - F(r+1) &= \binom{n+d-2}{d-1} + \binom{r+d-2}{d} - \binom{r+d-1}{d} \\ &= \binom{n+d-2}{d-1} - \binom{r+d-2}{d-1} \geq 0 \end{aligned}$$

当 $\binom{a+1}{b} = \binom{a}{b} + \binom{a}{b-1}$ 对于 $(a,b) = (r+d-2,d)$ 且 $r \leq n$ 时。因此，对于所有 $r \leq n$， $F(r) \geq 0$。

现在我们分析这些码的参数 $\mathcal{C}^{n,\ \rho}{}^{d}(\alpha)$ 作为秩度量码。根据命题3.7 和推论5.7，我们知道

$$s(n,d,\rho) \leq \dim \mathcal{C}_{\rho}^{n,d}(\alpha) \leq t(n,d,\rho).$$

for

$$\begin{aligned} s(n,d,\rho) &:= \binom{n+d-1}{d} - n\binom{\rho+d-3}{d-1}, \\ t(n,d,\rho) &:= \binom{n+d-2}{d-1}(n-\rho+1). \end{aligned}$$

现在我们渐近地比较 $s(n,d,\rho)$ 和 $t(n,d,\rho)$。首先，当 d,ρ 固定时，我们有

$$\begin{aligned} s(n,d,\rho) &\sim n^d/d! \\ t(n,d,\rho) &\sim n^d/(d-1)! \end{aligned}$$

当 n 变大时。我们看到，我们的码（以及它们所在的环境空间）距离具有最大维数还差一个因子 d。当 d 固定且 $\rho = \tau n$ 对某个常数 $0 < \tau < 1$ 时，则

$$\begin{aligned} s(n,d,\rho) &\sim (1 - d\tau^{d-1}) \cdot n^d/d! \\ t(n,d,\rho) &\sim d(1-\tau) \cdot n^d/d! \end{aligned}$$

当 τ 相对于 d 较小时（更准确地说，当 $\tau^{-1} > d^{1/(d-2)}$ 时），我们有 $d\tau^{d-1} < \tau$，因此，我们的码距离达到上界仍相差一个因子 d 。

注 5.9。 码 $\mathcal{C}^{n}{}_{\rho}{}^{d}(\alpha)$ 不可能达到最优 （将其解释为秩度量码时），这一事实直接源于命题 2.9 中的界与推论 d中的界相差甚远，后者仅为前者的一个因子 5.7。此外，我们还怀疑命题2.9 中的界实际上并不紧。事实上，当 $d = 2$时，我们将在后面的推论 5.13 中看到，当 $\mathbb{F}$ 是有限域时，上界至少还可以得到改进。该结果在 [22] 中得到证明，其方法基于关联方案，并且高度依赖于该域 $\mathbb{F}$ 是有限的这一条件。当 $\mathbb{F}$ 不是有限域时，这个改进后的界是否仍然成立，依旧是一个开放问题。然而，在有限域上，研究类似的方法能否同样为 $d > 2$给出改进的上界，也将颇有意义。

Qu问题 5.10。 是否有可能改进命题 2.9中的类 Singleton 界?

最后，我们说明为何可以将多项式的本质变量空间解释为一种自然的支撑概念。在编码理论中，支撑理论为度量空间的元素提供了有用的组合视角，并使我们能够将线性码等具体对象与拟阵等更抽象的对象联系起来；例如参见 [2]。对于秩度量码的情形，也就是域 $n\times m$ 上的矩阵空间 $\mathbb{F}$，可以将研究与 $\mathbb{F}^n$的子空间格联系起来。具体而言，（列）支撑的 $A=(a^1\mid\cdots\mid a^m)\in\mathbb{F}^{n\times m}$是空间

$$\operatorname{supp}(A):=\langle a^1,\ldots,a^m\rangle\subseteq\mathbb{F}^n.$$

这一概念在近期的研究中已得到详细探讨；例如参见 [16]。

Pr命题 5.11. 假设 $\operatorname{char}(F)>d$ 或 $\operatorname{char}(\mathbb{F})=0$，并令 $f\in S_{n,\,d}(\mathbb{F})$。 n

$$V_{\mathrm{ess}}(f)=\operatorname{supp}(C_f)\cdot(x_1,\ldots,x_n):=\{v(x)\mid v\in\operatorname{supp}(C_f)\}.$$

证明。根据定理5.2， f 的本质变量空间由以下元素张成

$$\{(\partial_1^{a_1}\ldots\partial_n^{a_n})\circ f\mid a_1+\ldots+a_n=d-1\}=\{v_1(x),\ldots,v_m(x)\},$$

其中 $m=\binom{n+d-2}{d-1}$ 且这些元素按字典序排列。将向量v_1、.....、 v_m 作为行排列成一个 $m\times n$ 矩阵，得到第（$d-1$）个催化矩阵 $C_{f,\,d-1}$。观察可知 $(C_{f,\,d-1})^{\top}=DC_f$，其中 $D\in\mathbb{F}^{m\times m}$是某个可逆对角矩阵；例如参见 [15]。因此，$C_f$的行张成空间$_{d-1}$ 与 C_f的列张成空间重合，也就是 C_f的支撑。□

5.1. 二次多项式的情形。我们详细分析当 $d=2$且 $\operatorname{char}(\mathbb{F})\neq 2$ 时的情况。在这种情形下，本质秩度量码在秩度量下与对称矩阵空间等距。

命题 5.12. 对于每个 $f\in S_{n,\,2}(\mathbb{F})$，矩阵 C_f 是对称的。映射 $f\mapsto C_f$ 是配备本质秩度量的空间 $S_{n,\,2}(\mathbb{F})$ 与配备秩度量的 $n\times n$ 上的对称矩阵空间之间的等距映射。

证明。记

$$f=\sum_{1\le i\le j\le n}a_{ij}x_ix_j,$$

我们看到

$$C_f=\begin{pmatrix}2a_{1,1}&a_{1,2}&\cdots&a_{1,n}\\a_{1,2}&2a_{2,2}&\ddots&\vdots\\\vdots&\ddots&\ddots&a_{n-1,n}\\a_{1,n}&\cdots&a_{n-1,n}&2a_{n,n}\end{pmatrix}$$

是一个对称矩阵。映射 $f\mapsto C_f$ 显然是 $S_{n,\,2}(\mathbb{F})$ 与 $n\times n$ 上的对称矩阵空间之间的双射，其中 $\mathbb{F}$ 的特征为 $\mathbb{F})\neq 2$。根据定理 5.2，该双射实际上是一个等距映射。□

换言之，对于 $d=2$ 而言，本质秩度量码实际上是 对称秩度量码。已有多位作者对其进行研究；例如参见 [8, 22]。由此，本质秩度量码为对称秩度量码提供了一种推广。

当 $d=2$ 且域 $\mathbb{F}$ 为有限域时，我们实际上可以利用 n、d、k 和 r 之间更精细的界。这得益于 Schmidt 的工作，他采用了基于关联方案 [22] 的组合方法。

推论 5.13 （[22, 定理 3。3]）。 假设 $\mathbb{F}$ 是有限域，且 $\mathrm{char}(\mathbb{F}) > 2$。令 $\mathcal{C}$ 为一个$[(n, 2)\ k, r]_{\mathbb{F}}$本质秩度量码。则

$$k \le \begin{cases} \dfrac{n(n-r+2)}{2} & \text{if } n-r \text{ is even,} \\ \dfrac{(n+1)(n-r+1)}{2} & \text{if } n-r \text{ is odd.} \end{cases}$$

注 5.14. 推论 5.13 改进了命题 2.9中的类 Singleton 界。事实上，对于 $d = 2$, $[(n,2)\ k\ r]_{\mathbb{F}}$码的类 Singleton 界为

$$k \le \frac{(n+r)(n-r+1)}{2},$$

除 $r \in \{1, n\}$ 外，该界总是较差；在此处两个界相同。

接下来我们证明，利用命题 5.12中的对应关系，本文为 $d = 2$ 构造的本质秩度量码实际上是对称 Gabidulin 码。为此，我们需要确定一些 $\mathbb{F}$ 上向量空间之间的对应关系。

取 $\mathbb{L}$ 在 $\mathbb{F}$ 上的一组基 $\alpha_1, \dots, \alpha_n$。设 $\beta_1, \dots, \beta_n$ 是 $\alpha_1, \dots, \alpha_n$ 关于迹内积的对偶基，并设 $\gamma_1, \dots, \gamma_n$ 是 $\mathbb{L}$ 在 $\mathbb{F}$ 上的一组基，使得

$$(\gamma_1, \dots, \gamma_n) \perp (\sigma^i(\alpha_1), \dots, \sigma^i(\alpha_n))$$

对于 $i = 0, \dots, n-2$。考虑以下映射:

$$\begin{array}{ccc} \mathrm{End}_{\mathbb{F}}(\mathbb{L}) & \to & \mathbb{L}^n, \\ \varphi & \mapsto & (\varphi(\alpha_1), \dots, \varphi(\alpha_n)), \end{array} \qquad \begin{array}{ccc} \mathbb{L}^n & \to & \mathbb{F}^{n\times n}, \\ v & \mapsto & A_v, \end{array}$$

$$\begin{array}{ccc} \mathrm{End}_{\mathbb{F}}(\mathbb{L}) & \to & \mathrm{Bil}(\mathbb{L}\times\mathbb{L}, \mathbb{F}), \\ \varphi & \mapsto & ((x,y) \mapsto \mathrm{Tr}(\varphi(x)y)), \end{array} \qquad \begin{array}{ccc} \mathrm{Bil}(\mathbb{L}\times\mathbb{L}, \mathbb{F}) & \to & \mathbb{F}^{n\times n}, \\ f & \mapsto & B_f, \end{array}$$

其中，对于 $i = 1, \dots, n$， $v_i = \sum_{j=1}^n (A_v)_{ij}\beta_j$；对于 $i, j = 1, \dots, n$， $f(\alpha_i, \alpha_j) = (B_f)_{ij}$。这些映射都是 $\mathbb{F}$-线性同构，并且下图交换:

$$\begin{array}{ccc} \mathrm{End}_{\mathbb{F}}(\mathbb{L}) & \to & \mathbb{L}^n \\ \downarrow & & \downarrow \\ \mathrm{Bil}(\mathbb{L}\times\mathbb{L}, \mathbb{F}) & \to & \mathbb{F}^{n\times n} \end{array}$$

我们先回顾各个空间中（正规）Gabidulin 码的构造。设 σ 是 $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ 的一个生成元。那么，Gabidulin 码是如下形式的子空间

$$\left\{ \sum_{i=-k}^{\ell} \mu_i \sigma^i \,\middle|\, \mu_{-k}, \dots, \mu_\ell \in \mathbb{L} \right\} \subseteq \mathrm{End}_{\mathbb{F}}(\mathbb{L})$$

对于 $k, \ell \ge 0$，其中 $k + \ell \le n - 2$。在 $\mathrm{Bil}(\mathbb{L}\times\mathbb{L}, \mathbb{F})$ 中，它是

$$\left\{ (x,y) \mapsto \sum_{i=-k}^{\ell} \mathrm{Tr}(\mu_i \sigma^i(x) y) \,\middle|\, \mu_{-k}, \dots, \mu_\ell \in \mathbb{L} \right\}.$$

在 $\mathbb{L}^n$ 中，这对应于生成矩阵为以下矩阵的码

$$\begin{pmatrix} \sigma^{-k}(\alpha_1) & \cdots & \sigma^{-k}(\alpha_n) \\ \vdots & & \vdots \\ \sigma^{\ell}(\alpha_1) & \cdots & \sigma^{\ell}(\alpha_n) \end{pmatrix}$$

和校验矩阵

$$\begin{pmatrix} \sigma^{-k}(\gamma_1) & \cdots & \sigma^{-k}(\gamma_n) \\ \vdots & & \vdots \\ \sigma^{-(n-2-\ell)}(\gamma_1) & \cdots & \sigma^{-(n-2-\ell)}(\gamma_n) \end{pmatrix}$$

在 $\mathbb{L}$上，即码 $\sigma^{-k}(\mathcal{G}^{\sigma}_{n-\ell-k,\ n}(\alpha))$，如（6）所定义，其中 $\alpha=(\alpha_1、\ ...、\ \alpha_n)$。在 $\mathbb{F}^{n\times n}$内部，我们得到

$$\left\{M\in\mathbb{F}^{n\times n}\,\middle|\,\sigma^i(\gamma)M\beta^\top=0\text{ for }i=-(n-2-\ell),\dots,-k\right\},$$

其中 $\gamma=(\gamma_1,\dots,\gamma_n)$ 和 $\beta=(\beta_1,\dots,\beta_n)$。

对称 Gabidulin 码是由所有对称元素构成的（正则）Gabidulin 码的子空间：我们对 $\mathbb{F}^{n\times n}$ 中的元素定义了转置，这又导出了 $\mathrm{End}_{\mathbb{F}}(\mathbb{L})$、$\mathrm{Bil}(\mathbb{L}\times\mathbb{L},\mathbb{F})$ 和 $\mathbb{L}^n$ 中元素的转置概念。

引理5.15。对于 $\mu\in\mathbb{L}$ 和 $k\in\mathbb{Z}$，有

$$(\mu\sigma^k)^\top=\sigma^{-k}(\mu)\sigma^{-k}$$

证明。令 $A,B\in\mathbb{F}^{n\times n}$ 为满足以下条件的矩阵：对于 $i=1,\dots,n$，$\mu\sigma^k(\alpha_i)=\sum_{j=1}^n A_{ij}\beta_j$；对于 $j=1,\dots,n$，$\sigma^{-k}(\mu)\sigma^{-k}(\alpha_j)=\sum_{i=1}^n B_{ji}\beta_i$。于是我们看到

$$A_{ij}=\mathrm{Tr}(\mu\sigma^k(\alpha_i)\alpha_j)=\mathrm{Tr}(\sigma^{-k}(\mu)\alpha_i\sigma^{-k}(\alpha_j))=B_{ji}$$

对于 $i,j=1,\dots,n$，有。因此 $A^\top=B$，故引理得证。 □

因此，对称 Gabidulin 码是形如.....的子空间

$$\left\{\mu_0\sigma^0+\sum_{i=1}^{\ell}(\mu_i\sigma^i+\sigma^{-i}(\mu_i)\sigma^{-i})\,\middle|\,\mu_0,\dots,\mu_\ell\in\mathbb{L}\right\}\subseteq\mathrm{End}_{\mathbb{F}}(\mathbb{L})$$

此类码的元素在 $\mathrm{Bil}(\mathbb{L}\times\mathbb{L},\mathbb{F})$ 中对应于形如.....的双线性型

$$(x,y)\mapsto\mathrm{Tr}\left(\mu_0xy+\sum_{i=1}^{\ell}(\mu_i\sigma^i(x)y+\sigma^{-i}(\mu_i)\sigma^{-i}(x)y)\right)=\mathrm{Tr}\left(\mu_0xy+\sum_{i=1}^{\ell}\mu_i(\sigma^i(x)y+x\sigma^i(y))\right)$$

对于 μ_0，.....，$\mu_\ell\in\mathbb{L}$。因此，这些确实恰好是[22]中构造的对称 Gabidulin 码。在 $\mathbb{F}^{n\times n}$中，我们得到

$$\left\{M\in\mathbb{F}^{n\times n}\,\middle|\,M^\top=M,\sigma^i(\gamma)M\beta^\top=0\text{ for }i=-(n-2-\ell),\dots,-\ell\right\}.$$

下面的命题表明，这恰好是我们为 $d=2$ 构造的码 .

命题5.16。空间

$$\left\{M\in\mathbb{F}^{n\times n}\,\middle|\,M^\top=M,\sigma^i(\gamma)M\beta^\top=0\text{ for }i=-(n-2-\ell),\dots,-\ell\right\}.$$

等于 $\mathcal{C}^{n,\ 2}_{n-2\ell}(\sigma^{n-2-\ell}(\beta)\ \gamma)$ 在等距映射 $f\mapsto C_f$ 下的像。

证明。由于映射 $f\mapsto C_f$ 是 $S_{n,2}(\mathbb{F})$ 与对称矩阵空间之间的等距映射，因此只需验证，对于 $f\in S_{n,2}(\mathbb{F})$，以下条件

$$\sigma^{n-2-\ell}(\beta(\partial))\sigma^j(\gamma(\partial))\circ f=0,\qquad j=0,\dots,n-2\ell-2,$$

以及以下条件

$$\sigma^i(\gamma)C_f\beta^\top=0,\qquad i=-(n-2-\ell),\dots,-\ell,$$

是等价的。取 $j\in\{0,\dots,n-2\ell-2\}$ 和 $i=j-(n-2-\ell)$。我们证明

$$\sigma^{n-2-\ell}(\beta(\partial))\sigma^j(\gamma(\partial))f=0\iff\sigma^i(\gamma)C_f\beta^\top=0$$

对所有 $f\in S_{n,2}(\mathbb{F})$ 均成立。两个方程都是关于 f 的线性方程，而空间 $S_{n,2}(\mathbb{F})$ 由形如 $(v(x))^2$ 且满足 $v\in\mathbb{F}^n$ 的多项式张成。因此我们可以假设 $f=(v(x))^2$，并且

$C_f = 2v^\top v$。现在很容易验证

$$\begin{aligned}\sigma^{n-2-\ell}(\beta(\partial))\sigma^j(\gamma(\partial)) \circ f &= \sigma^{n-2-\ell}\left(\beta(\partial)\sigma^i(\gamma(\partial)) \circ f\right)\\ &= \sigma^{n-2-\ell}\left(2(\beta \cdot v)(\sigma^i(\gamma) \cdot v)\right)\\ &= \sigma^{n-2-\ell}\left(2\sigma^i(\gamma)v^\top v\beta^\top\right)\\ &= \sigma^{n-2-\ell}\left(\sigma^i(\gamma)C_f\beta^\top\right)\end{aligned}$$

对于所有 $v \in \mathbb{F}^n$，从而

$$\sigma^{n-2-\ell}(\beta(\partial))\sigma^j(\gamma(\partial)) \circ f = \sigma^{n-2-\ell}\left(\sigma^i(\gamma)C_f\beta^\top\right)$$

对于所有 $f \in S_{n,\,2}(\mathbb{F})$。这表明了所声称的等价性。 □

6. Other ranks of polynomials

齐次多项式的秩有多种自然定义。每一种秩都定义了多项式之间的一种距离度量，并且对于每一种秩，我们都可以寻求构造具有大最小距离的高维码。本节将考察下文定义的嵌套秩概念。我们的目标尤其是为研究一类新的码提供动机，我们称之为强度度量码。

定义 6.1。令 $f \in S_{n,\,d}(\mathbb{F})$。$f$ 的强度是整数

$$\mathrm{str}(f) \coloneqq \min\{r \in \mathbb{Z}_{\geq 0} \mid f = g_1h_1 + \ldots + g_rh_r,\ g_i, h_i \in S_n(\mathbb{F}), \deg(g_i), \deg(h_i) < d\}.$$

f 的切片秩是整数

$$\mathrm{sl}(f) \coloneqq \min\{r \in \mathbb{Z}_{\geq 0} \mid f = \ell_1g_1 + \ldots + \ell_rg_r,\ \ell_i \in S_{n,1}(\mathbb{F}), g_i \in S_{n,d-1}(\mathbb{F})\}.$$

f 的本质秩是整数

$$\mathrm{ess}(f) \coloneqq \min\{r \in \mathbb{Z}_{\geq 0} \mid f = g(\ell_1, \ldots, \ell_r),\ g \in S_{r,d}(\mathbb{F}), \ell_i \in S_{n,1}(\mathbb{F})\}.$$

f 的华林秩是整数

$$\mathrm{war}(f) \coloneqq \min\{r \in \mathbb{Z}_{\geq 0} \mid f = \lambda_1\ell_1^d + \ldots + \lambda_r\ell_r^d,\ \lambda_i \in \mathbb{F}, \ell_i \in S_{n,1}(\mathbb{F})\}.$$

命题 6.2. 设 $f \in S_{n,\,d}(\mathbb{F})$。则

$$\mathrm{str}(f) \leq \mathrm{sl}(f) \leq \mathrm{ess}(f) \leq \mathrm{war}(f).$$

证明。切片分解特别地也是一种强度分解。因此，$\mathrm{str}(f) \leq \mathrm{sl}(f)$。当 $f \in \mathbb{F}[\ell_1, \ldots, \ell_r]$ 时，f 具有一个包含 r 项的切片分解。因此，$\mathrm{sl}(f) \leq \mathrm{ess}(f)$。当 $f = \ell_1^d + \ldots + \ell_r^d$ 时，则有 $f \in \mathbb{F}[\ell_1, \ldots, \ell_r]$。因此，$\mathrm{ess}(f) \leq \mathrm{war}(f)$。□

命题 6.2 表明，具有较高最小强度距离的码，相对于切片秩、本质秩和华林秩，也具有较高的最小距离。下面的结果可以看作是这一陈述的推广。

定理 6.3 （[4, 定理 4]）。设 $\mathbb{F}$ 是一个完美域，且 $\mathrm{char}(\mathbb{F}) = 0$ 或 $\mathrm{char}(\mathbb{F}) > d$，并设 $\mathcal{P}$ 是域 $\mathbb{F}$上齐次 d 次多项式的一个性质。假设对于所有具有性质 $\mathcal{P}$、$m \in \mathbb{Z}_{\geq 0}$ 和 ℓ_1、……、$\ell_n \in S_{m,\,1}(\mathbb{F})$ 的 $f \in S_{n,\,d}(\mathbb{F})$，多项式 $f(\ell_1, \ldots\ldots, \ell_n) \in S_{m,\,d}(\mathbb{F})$ 也具有性质 $\mathcal{P}$。那么，要么所有多项式都具有 $\mathcal{P}$，要么存在一个常数 k，使得对于所有具有 $\mathcal{P}$的多项式 f，$\mathrm{str}(f) \leq k$。

令 $\mathcal{P}$ 表示秩为 $\leq \ell$ （其中 ℓ 为某个常数）的性质，并采用上述秩的某种定义，我们可以看出，具有高强度意味着其他秩也很高。该定理表明，具有较高最小强度距离的码，由于其元素不具有此类性质，可能拥有良好的解码性质。所有这些都促使我们关注以下问题。

Ques问题 6.4：能否显式构造具有高最小强度距离的码? ?

即使对于维数为 1 的码，也就是由单个多项式张成的码，这个问题也并不简单。在这种情形下，问题是要显式构造强度高的多项式。下面的引理给出了一种求多项式强度下界的方法。

引理 6.5。设 $f \in S_{n,d}(\mathbb{F})$，并设 Sing($f$) 为超曲面$\{f = 0\}$的奇异轨迹。那么 dim Sing($f$) $\geq n - 2\,\mathrm{str}(f)$。特别地，当 Sing($f$) $= \{0\}$时，我们有 str(f) $\geq n/2$。

证明。当 $f = g_1h_1 + \ldots + g_rh_r$且 deg g_i、deg $h_i < d$时，则 $\{g_1, h_1, \ldots, g_r, h_r = 0\}$ 包含于 $\{f = 0\}$的奇异轨迹中。这个子簇在 $\mathbb{F}^n$中的余维为 $\leq 2r$。□

利用引理 6.5，我们知道如何构造强度为 $\geq \lceil n/2 \rceil$的多项式。下面的定理表明，至少当 char($\mathbb{F}$) $= 0$ 时，这远未达到可能的最大强度。

定理 6.6 ([14, 定理 12.8])。假设 $\mathbb{F}$ 是代数闭域，且 char($\mathbb{F}$) $= 0$。那么，$S_{n,d}(\mathbb{F})$ 中多项式的一般切片秩在 $d = 2$ 时等于 $\lceil n/2 \rceil$，并且

$$\min\left\{ r \in \mathbb{Z}_{\geq 0} \,\middle|\, r(n+1-r) \geq \binom{n-r+d}{d} \right\}$$

当 $d \geq 3$时。

定理 6.7 ([1, 推论 1.9])。假设 $\mathbb{F}$ 是代数闭域，且 char($\mathbb{F}$) $= 0$。那么，$S_{n,d}(\mathbb{F})$ 中一般元素的强度与切片秩一致。

由于有界切片秩是扎里斯基闭条件，一般切片秩、最大切片秩以及强度都相同。因此我们看到，强度远高于$\lceil n/2 \rceil$ 的多项式确实存在。这一方向上已知的最佳结果是 Gesmundo-Ghosal- Ikenmeyer-Lysikov 的构造[13]，其中的多项式具有切片秩 $\geq \lceil n/2 \rceil + 1$。然而，引理 6.5 确实为研究具有强力度量的码提供了一个起点。

问题 6.8. 能否显式构造 $S_{n,\,d}(\mathbb{F})$ 中的高维码，使得每个非零元素都定义一个光滑射影超曲面?

References

[1] Edoardo Ballico、Arthur Bik、Alessandro Oneto、Emanuele Ventura, *Strength and slice rank of forms are generically equal* 2022 DOI:10.1007/s11856-022-2397-0 , 《以色列数学杂志》 () 。[2] Alexander Barg, *The matroid of supports of a linear code*, 《工程应用代数与计算》8（1997年），第165–172页。DOI:10.1007/s002000050060[3] Hannes Bartz、Lukas Holzbaur、Hedongliang Liu、Sven Puchinger、Julian Renner、Antonia Wachter-Zeh, *Rank-Metric Codes and Their Applications*, 《通信与信息理论基础与趋势》19（2022年），第3期，第390–546页。[4] Arthur Bik、Jan Draisma、Rob H. Eggermont, *Polynomials and tensors of bounded strength*, 《当代数学通讯》 **21** 2019 7, 1850062 DOI:10.1142/S0219199718500621 () ，第期。James [5] *Triangular factorization and inversion by fast matrix multiplication* R. Bunch、John E. Hopcroft, , 《计算数学》28（1974年），第125期，第231–236页。 DOI:10.2307/2005828[6] Enrico Carlini, *Reducing the number of variables of a polynomial*, 《代数几何与几何建模》, Springer, 2006, 237 247 DOI:10.1007/978-3-540-33275-6_15 第–页。Alain Couvreur, , 预印本。[7] *Improved decoding of symmetric rank metric errors* arXiv:2212.08713 [8] *Codes spanned by quadratic and Hermitian forms* Mario A. de Boer, , IEEE信息论汇刊42（1996年），第5期，第1600–1604页。 DOI:10.1109/18.532907[9] Philippe Delsarte, *Bilinear forms over a finite field, with applications to coding theory*, 《组合理论杂志A辑》 **25** 1978 3, 226 241 DOI:10.1016/0097-3165(78)90015-8 () ，第期，第–页。Ran [10] *Faster matrix multiplication via asymmetric hashing* Duan、Hongxun Wu、Renfei Zhou, , 预印本。arXiv:2210.10173[11] `Ernest M. Gabidulin, *Theory of Codes with Maximum Rank Distance*, 《信息传输问题》21（1985年），第1期，第3–16页。[12] `Ernest M. Gabidulin、Nina I. Pilipchuk, *Symmetric rank codes*, 《信息传输问题》40（2004年），第2期，第103–117页。DOI:10.1023/B:PRIT.0000043925.67309.c6[13] Fulvio Gesmundo、Purnata Ghosal、Christian Ikenmeyer、Vladimir Lysikov, *Degree-restricted strength decompositions and algebraic branching programs* arXiv:2205.02149 , 预印本。

[14] Joe Harris, *Algebraic Geometry: A First Course*。GTM 133，Springer-Verlag，1992年。[15] Anthony Iarrobino、Vassil Kanev, *Power sums, Gorenstein algebras, and determinantal loci*, 《数学讲义》。1721, 1999 DOI:10.1007/BFb0093426 Springer Verlag，柏林，。Relinde P.M.J. Jurrius、[16] *On defining generalized rank weights* Ruud Pellikaan，，《通信数学进展》11（2017年），第1期，第225–235页。 DOI:10.3934/amc.2017014[17] Tsit-Yuen Lam、Andr´e Leroy, *Vandermonde and Wronskian matrices over division rings*, 《代数杂志》 **119** 1988 2, 308 336 DOI:10.1016/0021-8693(88)90063-4 （），第期，第–页。Ronald C. Mullin、Ivan M. Onyszchuk、[18] Scott A. Vanstone、Richard M. Wilson, *Optimal normal bases in* GF(p^n **22** 1988 2, 149 161 DOI:10.1016/0166-218X(88)90090-X), 《离散应用数学》（），第期，[19] *Maximum-rank array codes and their application to crisscross error correction* 第–页。Ron M. Roth，，《IEEE信息论汇刊》 **37** 1991 2, 328 336 DOI:10.1109/18.75248 （），[20] *Tensor Codes for the Rank Metric* 第期，第–页。Ron M. Roth，，IEEE信息论汇刊42（1996年），第6期，第2146–2157页。 DOI:10.1109/18.556603[21] Kai-Uwe Schmidt, *Quadratic and symmetric bilinear forms over finite fields and their association schemes*, 《代数组合学》3（2020年），第1期，第161–189页。 DOI:10.5802/alco.88[22] Kai-Uwe Schmidt, *Symmetric bilinear forms over finite fields with applications to coding theory*, 《代数组合学杂志》 **42** 2015 2, 635 670 DOI:10.1007/s10801-015-0595-0 （），第期，第–页。Danilo [23] Silva、Frank R. Kschischang、Ralf Koetter, *A Rank-Metric Approach to Error Control in Random Network Coding* **54** 2008 9, 3951 3967 ，IEEE信息论汇刊（），第期，第–页。DOI:10.1109/TIT.2008.928291[24] John Sheekey, *MRD codes: Constructions and Connections*, 《组合学与有限域：差集、多项式、伪随机性及其应用》，Radon计算与应用数学丛书23，2019年。 DOI:10.1515/9783110642094-013

Appendix A. Orbits of small-width multisets modulo n

固定整数 $d \geq 2$ 和 $n > k \geq 0$。考虑由 d 个元素组成的多重集的集合 $\mathcal{M}$

$$S = \{\!\{x_1, \ldots, x_d\}\!\}$$

其元素 $x_1, \ldots, x_d$ 属于 $\mathbb{Z}/n\mathbb{Z}$，以及 $\mathbb{Z}$ 在 $\mathcal{M}$ 上的作用定义为

$$x + S = \{\!\{x + y \bmod n \mid y \in S\}\!\}$$

我们将 $\{0, \ldots, n-1\}$ 的元素与其在 $\mathbb{Z}/n\mathbb{Z}$ 中的像等同起来，并考虑 $\mathcal{M}$ 的子集$\mathcal{R}$，其中包含的多重集的所有元素都属于 $\{0, \ldots, k\}$，且至少包含一个 0。现在提出以下问题。

问题 A.1. 有多少个 $\mathbb{Z}$ 轨道与 $\mathcal{R}$ 相交?

本附录旨在回答当 $\frac{2}{3}n > k$ 时的这个问题。我们首先考虑 $n \gg k$ 的情形。

命题 A.2. 假设 $\frac{1}{2}n > k$。那么每个 $S \in \mathcal{R}$ 都属于 $\mathcal{M}$ 的一个不同的 $\mathbb{Z}$-轨道。

证明。设 S、$S' \in \mathcal{R}$ 是不同的多重集，并假设对于某个 $x \in \mathbb{Z}$，有 $S' = x + S$。不妨设 $x \in \{1, \ldots, n-1\}$。注意到 $x = x + 0 \in x + S = S'$，因此$x \in \{0, \ldots, k\}$。我们有 $S = (n-x) + S'$。由此可得 $n - x = (n-x) + 0 \in (n-x) + S' = S$，进而 $n - x \in \{0, \ldots, k\}$。所以 $n = x + (n-x) \leq k + k$。矛盾，因此 S、S' 必定属于不同的 $\mathbb{Z}$- 轨道。□

引理 A.3。 $\mathcal{R}$ 的元素数量等于

$$\binom{(d-1)+k}{d-1}.$$

证明。表示多重集 $S \in \mathcal{R}$ 的一种方法是将其编码为元组 $(n_0, \ldots, n_k)$，其中 n_i 等于 $i \in \{0, \ldots, k\}$ 在 S中的出现次数。由此可知，当且仅当 $n_0 \in \mathbb{N}, n_1, \ldots, n_k \in \mathbb{Z}_{\geq 0}$ 和 $n_0 + \ldots + n_k = d$时，这些元组表示 $\mathcal{R}$ 的一个元素；在这种情形下，多重集 S 由 $(n_0, \ldots, n_k)$ 唯一确定。这表明， $\mathcal{R}$ 的大小等于所有和为 $d-1$的非负整数 $(n_0 - 1, n_1, \ldots, n_k)$ 元组（$(k+1)$-元组）的数量。共有

$$\binom{(d-1)+k}{d-1}$$

这样的元组。 □

命题 A.4. 假设 $\frac{1}{2}n > k$。那么 $\mathcal{R}$ 与.....相交

$$\binom{(d-1)+k}{d-1}$$

$\mathbb{Z}$-轨道的 $\mathcal{M}$。

我们考虑的第二种情形是 n 较小。

命题 A.5. 假设 $\frac{2}{3}n > k \geq \frac{1}{2}n$。那么映射 π 将.....映到.....

$$((n_0,\dots,n_a),(m_0,\dots,m_b)) \mapsto \bigcup_{i=0}^{a}\bigcup_{j=1}^{n_i}\{\!\{i\}\!\} \cup \bigcup_{i=0}^{b}\bigcup_{j=1}^{m_i}\{\!\{k-b+i\}\!\}$$

是集合之间的一个双射

$$\left\{((n_0,\dots,n_a),(m_0,\dots,m_b)) \;\middle|\; \begin{array}{l} a,b\in\mathbb{Z}_{\geq 0}, n_0,m_0\in\mathbb{N}, n_1,\dots,n_a,m_1,\dots,m_b\in\mathbb{Z}_{\geq 0},\\ a+b=2k-n,\ n_0+\ldots+n_a+m_0+\ldots+m_b=d,\\ (n_0,\dots,n_a)\neq(m_0,\dots,m_b)\end{array}\right\}$$

且 $\{S\in\mathcal{R}\mid \#(\mathbb{Z}\cdot S)\cap\mathcal{R}>1\}$。此外，我们有 $\mathbb{Z}\cdot\pi((n_0,\dots,n_a),(m_0,\dots,m_b))\cap\mathcal{R}$等于

$$\{\pi((n_0,\dots,n_a),(m_0,\dots,m_b)),\pi((m_0,\dots,m_b),(n_0,\dots,n_a))\}$$

对于前一个集合中的所有元素。

证明。首先，将 π 视为到 $\mathcal{R}$的映射。我们先证明 π 是单射。显然，只需证明：若

$$S := \pi((n_0,\dots,n_a),(m_0,\dots,m_b)) = \pi((n'_0,\dots,n'_{a'}),(m'_0,\dots,m'_{b'})),$$

则 $(a',b')=(a,b)$。反设不然。不妨设 $a'>a$ 且 $b'<b$。由于 $k-b\in S$ 且$k-b<k-b'$，可知 $k-b\leq a'$。因此 $k\leq a'+b\leq(2k-n)+(2k-n)=4k-2n$，从而 $2n\leq 3k$。这与假设 $k<\frac{2}{3}n$矛盾。因此 $(a',b')=(a,b)$，且 π是单射。接下来，我们证明 π的像包含于所述陪域中。设 $((n_0,\dots,n_a),(m_0,\dots,m_b))$ 是定义域中的一个元素。我们证明，$\pi((n_0,\dots,n_a),(m_0,\dots,m_b))$ 的 $\mathbb{Z}$-轨道至少包含 $\mathcal{R}$中的两个元素。确实如此，因为

$$\pi((m_0,\dots,m_b),(n_0,\dots,n_a)) = n-k+b+\pi((n_0,\dots,n_a),(m_0,\dots,m_b))$$

也包含在这个轨道中，并且 $(n_0,\dots,n_a)\neq(m_0,\dots,m_b)$。

设 $S,S'\in\mathcal{R}$ 是不同的多重集，并假设对于某个 $x\in\mathbb{Z}$，$S'=x+S$。不妨设 $x\in\{1,\dots,n-1\}$。我们的目标是证明

$$S=\pi((n_0,\dots,n_a),(m_0,\dots,m_b)) \text{ and } S'=\pi((m_0,\dots,m_b),(n_0,\dots,n_a))$$

对于某些唯一的 $n_0,\dots,n_a,m_0,\dots,m_b$，它们具有所需性质。

第一步是从 S计算 x。我们有 $x=x+0\in x+S=S'$ 且 $n-x=(n-x)+0\in(n-x)+S'=S$，因此 $x,n-x\in\{0,\dots,k\}$。所以 $n-k\leq x\leq k$。由于 $0\in S'=x+S$且 $x\leq k$，我们有 $n-x\in S$和 $n-x\geq n-k$。所以 $n-x\geq\min\{y\mid y\in S,y\geq n-k\}$。我们声称等号成立。假设并非如此。那么存在一个 $y\in S$，使得 $n-k\leq y<n-x$。我们得到元素

$$z := x+y\in x+S=S'$$

其满足 $n-k+x\leq z<n$。由于 $z<n$和 $z\in S'$，我们得到 $z\leq k$。因此 $n-k+x\leq z\leq k$。由此可得 $x\leq 2k-n$，于是

$$\frac{1}{3}n < n-k\leq x\leq 2k-n < 2\cdot\frac{2}{3}n-n=\frac{1}{3}n.$$

矛盾，因此必须有 $n-x=\min\{y\mid y\in S,y\geq n-k\}$。我们得到

$$x=n-\min\{y\mid y\in S,y\geq n-k\}.$$

定义 $b := x - (n-k) \geq 0$ 和 $a := (2k-n) - b = k - x \geq 0$。我们确实有 a、$b \in \mathbb{Z}_{\geq 0}$ 和 $a + b = 2k - n$。接下来，我们证明

$$S = \pi((n_0, \ldots, n_a), (m_0, \ldots, m_b))$$

对于某些 $n_0, n_1, \ldots, n_a, m_0, m_1, \ldots, m_b \in \mathbb{Z}_{\geq 0}$。令 $z \in S$。那么我们需要证明 $z \leq a$ 或 $z \geq k - b$ 成立。如果 $z \geq n - k$，那么 $z \geq \min\{y \mid y \in S, y \geq n-k\} = n - x = k - b$。假设 $z < n - k$。那么 $x + z \in x + S = S'$ 和 $x + z < x + (n-k) \leq x + (n-x) = n$。因此 $x + z \leq k$ 必定成立。所以 $z \leq k - x = a$。由于 S 的每个元素都包含在$\{0, \ldots, a\} \cup \{k-b, \ldots, k\}$中，我们得到

$$S = \pi((n_0, \ldots, n_a), (m_0, \ldots, m_b))$$

其中 $n_i \in \mathbb{Z}_{\geq 0}$ 等于 i 在 S 中的出现次数，而 $m_j \in \mathbb{Z}_{\geq 0}$ 等于 $k - b + j$ 在 S中的出现次数。由于 $0, n - x = k - b \in S$，我们可知 $n_0, m_0 \in \mathbb{N}$。最后，我们有

$$\pi((n_0, \ldots, n_a), (m_0, \ldots, m_b)) = S \neq S' = \pi((m_0, \ldots, m_b), (n_0, \ldots, n_a))$$

因此 $(n_0, \ldots, n_a) \neq (m_0, \ldots, m_b)$。所以 $((n_0, \ldots, n_a), (m_0, \ldots, m_b))$ 具有所需性质，并且 S 包含于 π 的像中。因此 π 是满射。由于 x 由 S唯一确定，我们看到 $\mathbb{Z}$- S 轨道与 $\mathcal{R}$ 的交恰好为 $\{S, S'\}$。□

例 A.6。假设 $n = 2k$。那么 $\mathcal{R}$ 中其 $\mathbb{Z}$-轨道与 $\mathcal{R}$相交两次的多重集，均具有 $\{\!\{0, \ldots, 0, k \ldots, k\}\!\}$的形式，其中 0 的数量和 k的数量分别为 ≥ 1，二者不同且总和为 d。

现在我们可以计算在此范围内与 $\mathcal{R}$ 相交的轨道数。

定理 A.7。假设 $\frac{2}{3}n > k \geq \frac{1}{2}n$。则 $\mathcal{R}$ 相交于

$$\binom{(d-1)+k}{d-1} - \frac{1}{2}\left((2k-n+1)\binom{(d-2)+(2k-n+1)}{d-2} - \delta_{2|d}\delta_{2|n}\binom{(d/2-1)+(k-n/2)}{d/2-1}\right)$$

$\mathcal{M}$的轨道。

证明。该命题表明，$\mathcal{M}$ 的一个轨道与 $\mathcal{R}$ 相交时，所含元素数量只能是 0、1 或 2。因此，与 $\mathcal{R}$ 相交的 $\mathcal{M}$ 的轨道数量等于 $\mathcal{R}$ 的大小减去 $\mathcal{R}$ 的子集大小的一半；该子集由所有满足 $\#(\mathbb{Z} \cdot S) \cap \mathcal{R} > 1$ 的元素 S 组成。这个 $\mathcal{R}$ 子集的大小等于

$$\sum_{a=0}^{2k-n} \#\left\{((n_0, \ldots, n_a), (m_0, \ldots, m_{2k-n-a})) \;\middle|\; \begin{array}{l} n_0, m_0 \in \mathbb{N}, n_1, \ldots, n_a, m_1, \ldots, m_{2k-n-a} \in \mathbb{Z}_{\geq 0}, \\ n_0 + \ldots + n_a + m_0 + \ldots + m_{2k-n-a} = d \end{array}\right\}$$

减去

$$\#\left\{((n_0, \ldots, n_a), (m_0, \ldots, m_b)) \;\middle|\; \begin{array}{l} a, b \in \mathbb{Z}_{\geq 0}, n_0, m_0 \in \mathbb{N}, n_1, \ldots, n_a, m_1, \ldots, m_b \in \mathbb{Z}_{\geq 0}, \\ a + b = 2k - n,\ n_0 + \ldots + n_a + m_0 + \ldots + m_b = d, \\ (n_0, \ldots, n_a) = (m_0, \ldots, m_b) \end{array}\right\}.$$

我们有

$$\begin{aligned} & \#\left\{((n_0, \ldots, n_a), (m_0, \ldots, m_{2k-n-a})) \;\middle|\; \begin{array}{l} n_0, m_0 \in \mathbb{N}, n_1, \ldots, n_a, m_1, \ldots, m_{2k-n-a} \in \mathbb{Z}_{\geq 0}, \\ n_0 + \ldots + n_a + m_0 + \ldots + m_{2k-n-a} = d \end{array}\right\} \\ = & \#\left\{((p_0+1, p_1, \ldots, p_a), (p_{a+1}+1, p_{a+2}, \ldots, p_{2k-n+1})) \;\middle|\; \begin{array}{l} p_0, \ldots, p_{2k-n+1} \in \mathbb{Z}_{\geq 0}, \\ p_0 + \ldots + p_{2k-n+1} = d-2 \end{array}\right\} \\ = & \binom{(d-2)+(2k-n+1)}{d-2} \end{aligned}$$

对于所有 $a \in \{0, \dots, 2k-n\}$ 以及

$$\begin{aligned}
& \#\left\{ ((n_0,\dots,n_a),(m_0,\dots,m_b)) \;\middle|\; \begin{array}{l} a,b \in \mathbb{Z}_{\geq 0}, n_0, m_0 \in \mathbb{N}, n_1,\dots,n_a,m_1,\dots,m_b \in \mathbb{Z}_{\geq 0}, \\ a+b = 2k-n,\ n_0+\ldots+n_a+m_0+\ldots+m_b = d, \\ (n_0,\dots,n_a) = (m_0,\dots,m_b) \end{array} \right\} \\
= \;& \delta_{2|n} \cdot \#\left\{ ((n_0,\dots,n_{k-n/2}),(n_0,\dots,n_{k-n/2})) \;\middle|\; \begin{array}{l} n_0 \in \mathbb{N}, n_1,\dots,n_{k-n/2} \in \mathbb{Z}_{\geq 0}, \\ 2(n_0+\ldots+n_{k-n/2}) = d \end{array} \right\} \\
= \;& \delta_{2|d}\delta_{2|n} \cdot \#\left\{ (n_0'+1, n_1,\dots,n_{k-n/2}) \;\middle|\; \begin{array}{l} n_0', n_1,\dots,n_{k-n/2} \in \mathbb{Z}_{\geq 0}, \\ n_0'+\ldots+n_{k-n/2} = d/2-1 \end{array} \right\} \\
= \;& \delta_{2|d}\delta_{2|n} \binom{(d/2-1)+(k-n/2)}{d/2-1}.
\end{aligned}$$

这就得到了所述等式。 □

Arthur Bik，高等研究院，美国新泽西州普林斯顿 Einstein Drive 1 号，邮编 08540；以及马克斯·普朗克数学科学研究所，德国莱比锡因塞尔大街 22 号，邮编 04103*Email address*：mabik@ias.edu

Alessandro Neri，数学系：分析、逻辑与离散数学，根特大学，比利时根特克赖赫斯大道 281 号，邮编 9000；以及马克斯·普朗克数学科学研究所，德国莱比锡因塞尔大街 22 号，邮编 04103

Email address：alessandro.neri@ugent.be