广义低秩校验码

Ermes Franch[1],Philippe Gaborit[2],Chunlei Li[1]

[1] 挪威卑尔根大学{
ermes.franch, chunlei.li}@uib.no[2]
法国利摩日大学 gaborit@unilim.fr

arXiv:2305.02053v1 [cs.IT] 3 May 2023

摘要。本文通过在 $\mathbb{F}_q^m$ 上引入基于$\mathbb{F}_q^{m\times m\times m}$中的一般三阶张量的双线性乘积，推广了低秩校验（LRPC）码的概念，其中 $\mathbb{F}_q$ 是含有 q 个元素的有限域。广义 LRPC 码一般是 $\mathbb{F}_q$-线性码，而对三阶张量的特定选择则对应于原始的 $\mathbb{F}_{q^m}$-线性 LRPC 码。对于广义 LRPC 码，我们通过调整 LRPC 码的译码方法，提出了两种概率多项式时间译码算法，并证明所提出算法的译码失败率与 LRPC 码的译码失败率相近。

1 引言

秩度量码由 Delsarte 于 1978 [8]，提出，随后 Gabidulin [10] 和 Roth [26] 也分别独立地对其进行了研究。Gabidulin [10] 深入研究了一类最大秩距离码，这类码后来被称为 Gabidulin 码。Gabidulin 码可视为 Reed-Solomon 码在秩度量下的对应形式。因此，若干用于 Reed-Solomon 码的高效确定性译码算法（例如 [10, 20, 27], 中的算法）经改造后可用于 Gabudilin 码。凭借最优的秩距离和高效的译码，Gabidulin 码在随机网络编码 [18],、交叉错误纠正 [26], 、密码学 [11], 等领域得到了广泛应用，同时也推动了秩度量码的其他研究方向。过去四十年间，秩度量码取得了显著进展，其在编码理论中的重要性也日益提升 [5, 9]。

在密码学应用中，与汉明度量下的码相比，秩度量码在达到相同安全级别时可以使用更短的密钥，

例如 McEliece 密码系统中的 Goppa 码。此外，随机 $\mathbb{F}_q$-线性秩度量码的译码问题可以归约为已证明为 NP 完全的 MinRank 问题 [6]。对于 $\mathbb{F}_{q^m}$-线性秩度量码，则存在一种归约到 NP 完全问题的概率归约方法 [14]。译码问题的困难性以及秩度量码密钥较短这一优势，奠定了基于秩的密码学的基础。近年来，研究人员提出了各种基于秩的密码方案，包括 RankSign [13], 基于身份的加密 [12], ROLLO [21], 签名方案 Durandal [1], 等。另一方面，$\mathbb{F}_{q^m}$-秩度量码似乎具有很强的代数结构，难以通过非平凡的方式对其进行安全掩蔽。基于 Gabidulin 码的 GPT 密码系统 [11] 及其变体容易受到 Overbeck 提出的代数攻击 [23]。针对 $\mathbb{F}_{q^m}$-线性秩度量码的译码问题，Ourivsky 和 Johansson [22] 利用了$\mathbb{F}_{q^m}$-线性结构来降低译码复杂度。最近，一系列论文提出了采用相同模型的改进攻击 [2] [4] [3]，尽管低秩校验（LRPC）码 [24]的结构较弱，这些攻击仍对若干基于此类码的方案的安全参数提出了挑战。

受针对 $\mathbb{F}_{q^m}$ 线性秩度量码的译码问题及相关密码方案的代数攻击 [2,3] 近期进展的启发，本文提出了一种生成 $\mathbb{F}_q$ 线性秩度量码的方法，这类码不具有显著的代数结构，同时支持高效译码。具体而言，我们提出了一种扩展方法，通过在 $\mathbb{F}_q^m$ 上引入基于 $\mathbb{F}_q^{m\times m\times m}$ 中一个一般三阶张量 T 的双线性乘积 $\cdot_T$，将维数为 k 的 $\mathbb{F}_q$ 线性码扩展为维数为 km 的新 $\mathbb{F}_q$ 线性码。当将该扩展方法应用于具有低秩校验矩阵 H_1、.....、$H_{n-k} \in \mathbb{F}_q^{m\times n}$ 的 $\mathbb{F}_q$ 线性码时，我们得到了一大类 $\mathbb{F}_q$ 线性矩阵码，称为广义 LRPC 码。对于 $T \in\mathbb{F}_q^{m\times m\times m}$ 的特定选择，这些码对应于 $\mathbb{F}_{q^m}$ 线性 LRPC 码。在继续讨论广义 LRPC 码的译码之前，我们证明双线性乘积

$\cdot_T$ 满足以下性质：对于 $\mathbb{F}_q^m$ 中两个维数较小的子空间 r、d，它们的乘积空间的维数存在一个不超过 rd 的上界。讨论由不同张量得到的广义 LRPC 码之间的关系，并研究双线性乘积 $\cdot_T$ 关于 $\mathcal{B}$ 中基元素的可逆性。

从中选取 H_1、...、H_{n-k} 中的列。最后，我们通过调整 $\mathbb{F}_{q^m}$-线性 LRPC 码的译码方法，提出了两种用于广义 LRPC 码译码的概率多项式时间错误支撑恢复算法。我们还分析了各个译码步骤中的错误概率，并表明这些译码算法具有与 LRPC 码相似的译码失败率。

本文结构如下。第2节介绍 $\mathbb{F}_{q^m}$-线性和 $\mathbb{F}_q$-线性秩度量码的必要符号和基础知识，并简要回顾 LRPC 码及其译码过程。在第3节中，我们从 $\mathbb{F}_q^{m\times m\times m}$ 中三阶张量的一些辅助知识、三阶张量与向量之间的乘法入手，然后介绍一种基于三阶张量的 $\mathbb{F}_q^m$ 上的双线性乘积，并讨论该双线性乘积的一些性质。第4节和第5节专门讨论广义 LRPC 码以及这一新码族的译码：第4节提出广义 LRPC 码，讨论其与 $\mathbb{F}_{q^m}$-线性 LRPC 码的关系，并研究由不同三阶张量得到的广义 LRPC 码之间的关系；第5节针对三阶张量的可逆性提出两种广义 LRPC 码的译码算法，并分析这些算法的译码失败率。

2 预备知识

在本节中，我们将介绍后续各节所需的基本符号和辅助结果。

为避免使用繁琐的记号，我们用 $[n]$ 表示集合 $\{1,\dots,n\}$。我们用 $\mathbb{F}_q$ 表示含有 q 个元素的有限域，其中 q 是一个素数幂。向量空间 $\mathbb{F}_q^n$ 是由 $\mathbb{F}_q$ 上的所有 n元组构成的集合，而 $\mathbb{F}_q^{m\times n}$是由 $\mathbb{F}_q$. 上的所有 $m\times n$矩阵构成的集合。向量将用小写粗体字母表示。给定一个向量 $\mathbf{v}$，其第 i个分量记为 v_i。矩阵将用大写字母表示。给定一个矩阵 A，其第 i行、第 j列的元素记为 $a_{i,\ j}$。

2.1 秩度量码

在本小节中，我们回顾向量和矩阵中秩度量码的一些基础知识及相关性质。

设 $\mathbb{F}_{q^m}$ 是含有 q^m 个元素的有限域。设 $B = \{\beta_1, \ldots \beta_m\}$ 是 $\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$ 上的一组基。基 B 诱导出 $\mathbb{F}_{q^m}$ 与 $\mathbb{F}_q^m$ 之间的同构，具体如下：元素 $a = \sum_{i=1}^{m} a_i\beta_i \in \mathbb{F}_{q^m}$ 映射为 $\phi_B(a) = (a_1, \ldots, a_m)^\intercal \in \mathbb{F}_q^m$。利用同构 ϕ_B，我们可以将行向量 $\mathbf{v} \in \mathbb{F}_{q^m}^n$ 与矩阵 $V = (\phi_B(v_1) \ldots, \phi_B(v_n)) \in \mathbb{F}_q^{m\times n}$ 对应，其中每个 $\phi_B(v_i)$ 都是大小为 m 的列向量。滥用记号，定义 $\phi_B(\mathbf{v}) = V$。

秩度量码可以用向量或矩阵的形式表示。我们从向量表示下秩度量码的一些基础知识开始。

定义 1（支撑——向量）。给定子集 $S \subseteq \mathbb{F}_{q^m}$，由 S 的元素生成的 $\mathbb{F}_q$-向量子空间称为 S 的支撑，记作 $\langle S\rangle_{\mathbb{F}_q}$。类似地，向量 $\mathbf{v} \in \mathbb{F}_{q^m}^n$ 的支撑记作 $\langle \mathbf{v}\rangle_{\mathbb{F}_q}$，它是由其坐标生成的向量空间；矩阵 $H \in \mathbb{F}_{q^m}^{n_1\times n_2}$ 的支撑记作 $\langle H\rangle_{\mathbb{F}_q}$，它是由矩阵 H 的所有元素生成的向量空间。

定义 2（秩度量码——向量）。向量秩度量码$\mathcal{C}$ 是 $\mathbb{F}_{q^m}^n$ 的一个子集，其最小（秩）距离定义为 $d_R(\mathcal{C}) = \min\{d_R(\mathbf{u},\mathbf{v}) \mid \mathbf{u} \neq \mathbf{v} \in \mathcal{C}\}$，其中 $\mathbf{u}$ 和 $\mathbf{v}$ 之间的秩距离定义为

$$d_R(\mathbf{u}, \mathbf{v}) := \mathrm{Rank}(\phi_B(\mathbf{u}) - \phi_B(\mathbf{v})) = \dim(\langle \mathbf{u} - \mathbf{v}\rangle_{\mathbb{F}_q}),$$

特别地，$d_R(\mathbf{u}, 0) = \dim(\langle \mathbf{u}\rangle_{\mathbb{F}_q})$ 是 $\mathbf{u}$ 的秩权重。

如果秩度量码 $\mathcal{C}$ 是 $\mathbb{F}_q$-线性的（分别为 $\mathbb{F}_{q^m}$-线性的），即它是 $\mathbb{F}_q$-线性（分别为 $\mathbb{F}_{q^m}$-线性）子空间 $\mathbb{F}_{q^m}^n$，则称其为 $\mathbb{F}_{q^m}$-线性码 $\mathcal{C}$。维数为 k的码存在生成矩阵 $G \in \mathbb{F}_{q^m}^{k\times n}$，使得 $\mathcal{C} = \{\mathbf{x}G \mid \mathbf{x} \in \mathbb{F}_{q^m}^k\}$.。研究码的对偶码可以提供有关该码本身的一些信息。

定义 3（向量对偶性）。对于向量码 $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$，其对偶码 $\mathcal{C}$定义为

$$\mathcal{C}^\perp = \{\mathbf{x} \in \mathbb{F}_{q^m}^n \mid \mathbf{c} \cdot \mathbf{x}^\intercal = \sum_{i=1}^{n} c_i x_i = 0, \forall \mathbf{c} \in \mathcal{C}\}.$$

若 $\mathcal{C}$ 是维数为 k的 $\mathbb{F}_{q^m}$-线性码，则其对偶码 $\mathcal{C}^\perp$ 是维数为 $n-k$的线性码。设 $\mathcal{C}$ 是一个 $\mathbb{F}_{q^m}$-线性向量码，其生成

矩阵为 $G \in \mathbb{F}_{q^m}^{k\times n}$. 。容易看出，其对偶码 $\mathcal{C}^{\perp}$的生成矩阵 H 是 $\mathcal{C}$的校验矩阵，即 $HG^{\perp} = \mathbf{0}$。校验矩阵是纠错码中的重要工具。设 $\mathcal{C}$ 是一个带有校验矩阵 $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ 的 $\mathbb{F}_{q^m}$-线性码。若考虑 $\mathsf{y} \in \mathbb{F}_{q^m}^{n}$，则有：$\mathsf{y} \in \mathcal{C}$ 当且仅当 $H\mathsf{y}^{\intercal} = \mathbf{0}$。一般而言，我们有 $H\mathsf{y}^{\intercal} = \mathsf{s} \in \mathbb{F}_{q}^{n-k}$，这称为 y 的伴随式。基于秩的密码学中的一个重要问题是秩伴随式译码问题（RSD）。

定义 4（RSD 问题——向量形式）。给定一个 $\mathbb{F}_{q^m}$-线性向量码 $\mathcal{C} \subseteq \mathbb{F}_{q^m}^{n}$ 的校验矩阵 $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ 、伴随式 $\mathsf{s} \in \mathbb{F}_{q^m}^{n-k}$以及一个较小的整数 r，求一个向量 $\mathsf{y} \in \mathbb{F}_{q^m}^{n}$，使得 $H\mathsf{y}^{\intercal} = \mathsf{s}$ 且 $w_R(\mathsf{y}) \leq r$.

矩阵秩度量码与向量形式的秩度量码密切相关。下面我们将介绍矩阵秩度量码的一些基本概念。在 $\mathbb{F}_{q}^{m}$与 $\mathbb{F}_{q^m}$之间存在同构的条件下，可以类似地定义向量秩度量码的相应概念。

类似地，我们在 $\mathbb{F}_{q}^{m\times n}$中的矩阵空间上定义支撑和距离。

定义 5（支撑）。给定一个矩阵 $U \in \mathbb{F}_{q}^{m\times n}$，其列支撑记为 Colsp($U$)，是由其所有列的张成空间所生成的 $\mathbb{F}_{q}^{m}$ 向量空间。

定义 6（秩度量码——矩阵形式）。矩阵秩度量码$\mathcal{C}$ 是 $\mathbb{F}_{q}^{m\times n}$ 的子集。若集合 $\mathcal{C} \subseteq \mathbb{F}_{q}^{m\times n}$是 $\mathbb{F}_{q}^{m\times n}$ 的 $\mathbb{F}_{q}$-线性子空间，则称其为线性矩阵秩度量码。矩阵码 $\mathcal{C}$ 的最小距离定义为

$$d_R(\mathcal{C}) = \min\{d_R(U,V) \mid U \neq V \in \mathcal{C}\},$$

其中 $d_R(U,V) :=$ 秩($U - V$) $=$ 维数(列空间($U - V$))。

类 Singleton 界将秩度量码的最大可能大小与其最小距离联系起来。

定义 7（最大秩距离码）。设 $m \geq n$。所有矩阵秩度量码 $\mathcal{C} \subseteq \mathbb{F}_{q}^{m\times n}$均满足以下类 Singleton 界。

$$|\mathcal{C}| \leq q^{m(n-d+1)}. \tag{1}$$

如果一个码 $\mathcal{C}$ 达到了类 Singleton 界，则称其为最大秩距离（MRD）码。

设 $\mathcal{C}$ 是一个维数为 k 的 $\mathbb{F}_q$-线性矩阵秩度量码。这意味着存在 $G_1, \ldots, G_k \in \mathbb{F}_q^{m\times n}$ 个线性无关矩阵，它们生成该码。我们可以类似地定义一个生成矩阵，将这些矩阵收集成一个三维数组 $G = (G_1, \ldots, G_k) \in \mathbb{F}_q^{m\times n\times k}$。这类三维数组简称三阶张量，将在下一节中介绍并详细讨论。设 $\mathcal{C}$ 是由 G 生成的码，其中任意元素 $C \in \mathcal{C}$ 都可以表示为 $C = \sum_{i=1}^{k} x_i G_i$，其中 $\mathbf{x} = (x_1, \ldots, x_k) \in \mathbb{F}_q^k$。对于矩阵码，对偶性是通过迹内积来定义的。

定义 8（对偶性——矩阵）。对于矩阵码 $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$，其对偶码 $\mathcal{C}$ 定义为

$$\mathcal{C}^{\perp} = \{X \in \mathbb{F}_q^{m\times n} \mid \mathrm{Tr}(CX^{\intercal}) = \sum_{i=1}^{m}\sum_{j=1}^{n} c_{i,j}x_{i,j} = 0, \forall C \in \mathcal{C}\}.$$

若 $\mathcal{C}$ 是维数为 k的线性矩阵码，则其对偶码 $\mathcal{C}^{\perp}$ 也是维数为 $mn-k$的线性矩阵码。对于维数为 k的线性矩阵码，其 3-张量生成元 $H = (H_1, H_2, \ldots, H_{nm-k})$ 是其 $\mathcal{C}^{\perp}$ 的 3- 张量校验矩阵 $\in \mathbb{F}_q^{m\times n\times(mn-k)}$ $\mathcal{C}$。

码 $\mathcal{C}$ 的 3-张量校验矩阵 H 可以像校验矩阵一样，用于检验矩阵 $C \in \mathbb{F}_q^{m\times n}$ 是否属于码 $\mathcal{C}$。根据构造，$H_1, \ldots, H_{nm-k}$ 是 $\mathcal{C}^{\perp}$的一组基，这意味着 $\mathrm{Tr}(CH_i^{\intercal}) = 0, \forall i \in [nm-k]$。对于给定的 $C \in \mathbb{F}_q^{m\times n}$，当且仅当对所有 H_i 都有 $\mathrm{Tr}(CH_i^{\intercal}) = 0$时，$C \in \mathcal{C}$ 成立。与 $\mathbb{F}_{q^m}$-线性情形类似，对于给定的矩阵 $Y \in \mathbb{F}_q^{m\times n}$，我们可以将其伴随式定义为 $\mathbf{s} = (\mathrm{Tr}(YH_1^{\intercal}) \ldots, \mathrm{Tr}(YH_{nm-k}^{\intercal})) \in \mathbb{F}_q^{nm-k}$。借助这一伴随式概念，我们可以表述矩阵码的（RSD）问题。

定义 9（秩综合译码问题 - 矩阵）。给定一个 $\mathbb{F}_q$ 线性矩阵码 $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ 的校验矩阵 $H \in \mathbb{F}_q^{m\times n\times(nm-k)}$、一个伴随式 $\mathbf{s} \in \mathbb{F}_q^{nm-k}$ 和一个较小的整数 r，求一个矩阵 $Y \in \mathbb{F}_q^{m\times n}$，使得 $(\mathrm{Tr}(YH_1^{\intercal}) \ldots, \mathrm{Tr}(YH_{nm-k}^{\intercal})) = \mathbf{s}$ 且 $\mathrm{Rank}(Y) \leq r$.

现在我们讨论秩度量码的矩阵表示与向量表示之间的联系。回顾一下，ϕ_B 是从基 B诱导出的从$\mathbb{F}_{q^m}$ 到 $\mathbb{F}_q^m$的一个同构。设 $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ 是一个向量秩度量码。码 $\phi_B(\mathcal{C}) = \{\phi_B(\mathrm{c}) \mid \mathrm{c} \in \mathcal{C}\}$ 是一个矩阵秩度量码，其码字是 $\mathbb{F}_q^{m\times n}$的元素。注意， ϕ_B 保持秩距离，即对于 $\mathbb{F}_{q^m}$中的任意 u、v，都有d_R(u, v) $= d_R(\phi_B(\mathrm{u})\ \phi_B(\mathrm{v}))$。此外，显然有$\phi_B(\langle \mathrm{v}\rangle_{\mathbb{F}_q}) = \{\phi_B(x) \mid x \in \langle \mathrm{v}\rangle_{\mathbb{F}_q}\}$ =列空间(ϕ_B(v))。因此， ϕ_B也在 $\mathbb{F}_{q^m}$ 的 $\mathbb{F}_q$-线性子空间与$\mathbb{F}_q^m$的 $\mathbb{F}_q$-线性子空间之间诱导出一个同构。

根据目前所见，无论采用向量形式还是矩阵形式来考察秩度量码，似乎都一样。通常，采用向量形式处理 $\mathbb{F}_{q^m}$-线性秩度量码，采用矩阵形式处理 $\mathbb{F}_q$-线性秩度量码会比较方便。

这两种表示方式的一个重要区别在于对偶性的概念。回顾一下，向量形式的秩度量码的对偶性是根据 $\mathbb{F}_{q^m}^n$ 上的内积定义的，而矩阵秩度量码的对偶性则是根据 $\mathbb{F}_q^{m\times n}$ 上的迹内积定义的。 $\mathbb{F}_{q^m}^n$ 中两个向量的内积属于 $\mathbb{F}_{q^m}$，而 $\mathbb{F}_q^{m\times n}$ 中两个矩阵的迹内积属于 $\mathbb{F}_q$。因此， $\phi_B(\mathcal{C}^\perp) \neq \phi_B(\mathcal{C})^\perp$ 通常并不令人意外。Gorla和Ravagnani讨论并明确展示了这种关系 [15]。尽管一个 $\mathbb{F}_{q^m}$-线性向量码的对偶码与其矩阵表示的对偶码是两个不同的码，但它们实际上是同构的。

定理 1. *[15]* 令 $\mathcal{C} \in \mathbb{F}_{q^m}^n$ 为一个 $\mathbb{F}_{q^m}$-线性向量码。考虑 $\mathbb{F}_{q^m}$ 的一组基 $B = \{\beta_1, \ldots, \beta_m\}$ 及其正交基 $B' = \{\beta'_1, \ldots, \beta'_m\}$，满足 $\mathrm{Tr}_q^{q^m}(\beta_i\beta'_j) = \delta_{i,\ j}$, $\forall\, i, j \in [m]$。则有

$$\phi_B(\mathcal{C})^\perp = \phi_{B'}(\mathcal{C}^\perp).$$

2.2 LRPC 码

本节将简要介绍低秩奇偶校验（LRPC）码及其译码算法。LRPC 码由 Gaborit、Murat、Ruatta 和 Z´emor [24] 于 2013年 提出。此后，它们已被用于许多

密码方案 $[1, 12, 13, 21]$ owing to 其较弱的代数结构和高效的译码。

定义 10（LRPC 码）。若一个 $\mathbb{F}_{q^m}$-线性向量码 $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$的维数为 $\mathbb{F}_{q^m}$- 维数 k，且存在一个校验矩阵 $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$，使其支撑的维数为 dim($\langle H\rangle_{\mathbb{F}_q}$) $= d$，则称其为密度为 d 的 LRPC 码。

给定一个维数为 d、秩为 $n-k$ 的 $\mathbb{F}_q$-线性子空间 $\mathcal{H} \subseteq \mathbb{F}_{q^m}$ 和 $H \in \mathcal{H}^{(n-k)\times n}$。在大多数情况下，我们有 $\langle H\rangle_{\mathbb{F}_q} = \mathcal{H}$，而以 H 为校验矩阵的码 $\mathcal{C}$ 是一个密度为 d 的 LRPC 码。

LRPC 码的译码算法基于以下观察。

观察 1 设 $\mathcal{A} = \langle\alpha_1、\ \ldots、\ \alpha_r\rangle_{\mathbb{F}_q}$、$\mathcal{B} = \langle\beta_1、\ \ldots、\ \beta_d\rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}$ 是两个维数为 r 和 d 的 $\mathbb{F}_q$-线性子空间，使得 $rd \le m$。设乘积空间 $\mathcal{A}.\mathcal{B} = \langle\mathcal{AB}\rangle_{\mathbb{F}_q}$ 是包含 $\mathcal{AB} = \{ab \mid a \in \mathcal{A}、\ b \in \mathcal{B}\}$ 的最小 $\mathbb{F}_q$-线性子空间。注意，如果 $a = \sum_{j=1}^{r} a_j\alpha_j \in \mathcal{A}$ 和 $b = \sum_{k=1}^{d} b_k\beta_k \in \mathcal{B}$，那么

$$ab = \sum_{j=1}^{r}\sum_{k=1}^{d} a_j b_k(\alpha_j\beta_k),$$

因此，$\mathcal{A}.\mathcal{B}$ 由 $\{\alpha_j\beta_k \mid (j,k) \in [r] \times [d]\}$ 生成，其维数的上界为 rd。上述内容也可以用一种等价的方式表示：考虑一个 =($\alpha_1, \ldots, \alpha_r$)和一个 =($\beta_1, \ldots, \beta_d$)，则 $\mathcal{A} = \langle\mathsf{a}\rangle_{\mathbb{F}_q}$、$\mathcal{B} = \langle\mathsf{b}\rangle_{\mathbb{F}_q}$ 以及 $\mathcal{A}.\mathcal{B} = \langle\mathsf{a} \otimes \mathsf{b}\rangle_{\mathbb{F}_q}$。

设 $\mathcal{C}$ 是一个 LRPC 码，其校验矩阵为 H，并具有较小的支撑 $\mathcal{H} = \langle h_1, \ldots, h_d\rangle_{\mathbb{F}_q}$，其中 $\mathbb{F}_q$ 线性无关。假设收到向量 $\mathsf{y} = \mathsf{x} + \mathsf{e}$，其中 $\mathsf{x} \in \mathcal{C}$，而 $\mathsf{e} \in \mathbb{F}_{q^m}^n$ 是一个秩重量较小的错误 r。我们有 $\langle\mathsf{e}\rangle_{\mathbb{F}_q} = \mathcal{E}$，且 dim($\mathcal{E}$) $= r$。若考虑伴随式 $\mathsf{s} = H\mathsf{y}^\intercal = H\mathsf{e}^\intercal$，则有 $s_i = \sum_{j=1}^{n} h_{i,\ j}e_{j}$。注意，根据观察 1，每个乘积 $h_{i,\ j}e_j$ 都属于 $\mathcal{H}.\mathcal{E}$，因此 $\langle\mathsf{s}\rangle_{\mathbb{F}_q} \subseteq \mathcal{H}.\mathcal{E}$。由于 dim($\mathcal{H}.\mathcal{E}$) $\le rd$，若将每个 $s_i, i \in [n-k]$ 视为 $\mathcal{H}.\mathcal{E}$ 中均匀分布的随机元素，则对于 $n-k \ge rd$，以较高概率有 $\langle\mathsf{s}\rangle_{\mathbb{F}_q} = \mathcal{H}.\mathcal{E}$。该概率的估计量级为 $1 - q^{rd-(n-k)}$ [21]。对于一个固定元素 $h \in \mathbb{F}_{q^m}$ 和 $\mathbb{F}_q$ 线性子空间 $\mathcal{E} \subseteq \mathbb{F}_{q^m}$，我们用

$\mathcal{E}h = \{eh \mid e \in \mathcal{E}\}$ 表示将每个元素 $e \in \mathcal{E}$ 乘以 h 后得到的 $\mathbb{F}_q$ 线性子空间。注意，对于 $\mathcal{H} = \langle h_1, \ldots, h_d \rangle_{\mathbb{F}_q}$，$\mathcal{H}.\mathcal{E}$ 的一种等价写法是

$$\mathcal{H}.\mathcal{E} = \mathcal{E}h_1 + \cdots + \mathcal{E}h_d.$$

考虑

$$\mathcal{H}.\mathcal{E}h_i^{-1} = \mathcal{E}h_1h_i^{-1} + \cdots + \mathcal{E}h_ih_i^{-1} + \cdots + \mathcal{E}h_dh_i^{-1}$$

显然，$\mathcal{E} \subseteq \mathcal{H}.\mathcal{E}h_i^{-1}$。如果我们考虑所有这些子空间的交集，那么得到 $\mathcal{E} = \bigcap_{i\in[d]} \mathcal{H}.\mathcal{E}h_i^{-1}$，其概率至少估计为$1 - q^{-(d-1)(m-rd-r)}$ [21]。

根据错误支撑的信息，展开由 $\mathbb{F}_q$ 上伴随式的 $n-k$ 个元素给出的、定义在 $\mathbb{F}_{q^m}$ 上的线性系统相对容易。通常，这会得到 nr 个变量关于$\mathbb{F}_q$ 的 $(n-k)rd$ 个线性无关方程，当 $(n-k)d \geq n$ 时，可以唯一求解。

我们看到，LRPC 码可以定义为 $\mathbb{F}_{q^m}$-线性秩度量向量码。在下一节中，我们将讨论 $\mathbb{F}_q^m$ 上的双线性乘积，并以此为基础，将 LRPC 码的构造推广到仅为 $\mathbb{F}_q$-线性的矩阵码。

3 $\mathbb{F}_q^m$ 上的双线性乘积

本文将推广基于 $\mathbb{F}_q^{m\times m\times m}$ 上三阶张量的双线性乘积构造 LRPC 码的方法，其中 $\mathbb{F}_q^m$basisd。为此，我们首先介绍 $\mathbb{F}_q$ 上三阶张量的一些基础知识。

3.1 三阶张量

在本文中，$\mathbb{F}_q^{n_1\times n_2\times n_3}$中的元素称为三阶张量，并将用大写字母表示。给定一个三阶张量 T，我们将用 $t_{i,j,k}$表示其第 i、j、k 个元素。从代数角度看，一个三阶张量 $T \in \mathbb{F}_q^{n_1\times n_2\times n_3}$可以表示为由 n_3 个大小为 $n_1 \times n_2$的矩阵 T_i 组成的向量，即 $T =(T_1, \ldots, T_{n_3})$。从几何角度看，我们可以将三阶张量视为一个大小为$n_1 \times n_2 \times n_3$ 的平行六面体，置于三个坐标组成的系统中，如图 1 (a) 所示，其中

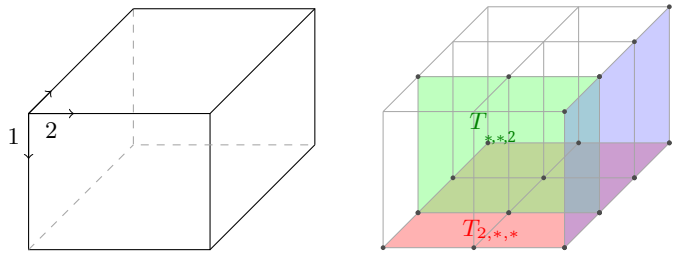
第一个指标表示垂直轴，第二个指标表示水平轴，第三个指标表示垂直于纸面的轴。给定一个 3-张量 T，当将 T 的第一个指标固定为某个值 i（对于 $1 \le i \le n_1$）时，可以得到一个大小为 $n_2 \times n_3$ 的矩阵。同样，固定第二个指标时可以得到一个大小为 $n_1 \times n_3$ 的矩阵，固定第三个指标时可以得到一个大小为 $n_1 \times n_2$ 的矩阵。我们将通过分别将 T 的第一个、第二个和第三个指标固定为 i、j 和 k 所得到的矩阵记为 $T_{i,*,*}$,$T_{*,j,*}$,$T_{*,*,k}$，其中通配符 $*$ 表示相应指标可以自由选择。

例 1。考虑一个张量

$$T = \left(\begin{array}{c|c|c|c} 1\,2\,0 & 1\,1\,1 & 1\,0\,4 & 1\,0\,1 \\ 0\,2\,0 & 0\,3\,0 & 1\,0\,0 & 1\,1\,5 \end{array}\right) \in \mathbb{F}_7^{2\times 3\times 4}.$$

图 1 (b) 展示了张量 T 的 3 个这种记法示例。具体来说，分别将 T 的第 1 个指标固定为 2、将 T 的第 2 个指标固定为 3，以及将 T 的第 3 个指标固定为 2，可得到以下三个矩阵

$$T_{2,*,*} = \begin{pmatrix} 0\,0\,1\,1 \\ 2\,3\,0\,1 \\ 0\,0\,0\,5 \end{pmatrix}, T_{*,3,*} = \begin{pmatrix} 0\,1\,4\,1 \\ 0\,0\,0\,5 \end{pmatrix}, T_{*,*,2} = \begin{pmatrix} 1\,1\,1 \\ 0\,3\,0 \end{pmatrix}.$$



(a) (b)

图 1：三阶张量的可视化与切片

与三阶张量相关的乘法将是所提出的广义 LRPC 码的一项核心特性。下面我们将介绍三阶张量与向量之间相对于指标 1、2 和 3 的乘法，

从可视化的角度来看，这些乘法可以解释为方向性乘法。我们先回顾矩阵与向量之间的类似乘法。二维矩阵 $M \in \mathbb{F}_q^{m\times n}$可以视为二阶张量，其中第 1 个指标表示垂直轴，第 2 个指标表示水平轴。给定两个向量 $\mathbf{x} \in \mathbb{F}_q^m$、$\mathbf{y} \in \mathbb{F}_q^n$，乘积 $\mathbf{x}M$ 是以 $\mathbf{x}$ 为权重、沿垂直方向对 M 的各行作线性组合；乘积 $M\mathbf{y}^\intercal$ 则是以 $\mathbf{y}$ 为权重、沿水平方向对 M 的各列作线性组合。我们可以分别将这两个乘积视为垂直乘法和水平乘法。三阶张量与向量之间以下的方向性乘法也以类似方式定义。

定义 11. 给定一个三阶张量 $T \in \mathbb{F}_q^{n_1\times n_2\times n_3}$、向量 $\mathbf{x} \in \mathbb{F}_q^{n_1}$、$\mathbf{y} \in \mathbb{F}_q^{n_2}$、$\mathbf{z} \in \mathbb{F}_q^{n_3}$，我们将 T 与 $\mathbf{x}$ 之间的垂直乘法记作 $T_{\mathbf{x},\,*,\,*}$，并将其定义为沿垂直方向对 T 关于 $\mathbf{x}$ 的线性组合，即

$$T_{\mathbf{x},*,*} := x_1 T_{1,*,*} + \cdots + x_{n_1} T_{n_1,*,*} = \sum_{i=1}^{n_1} x_i T_{i,*,*},$$

其中，$T_{\mathbf{x},\,*,\,*}$ 的第 j、k 个元素为 $\sum_{i=1}^{n_1} x_i t_{i,\,j,\,k}$。类似地，$T$ 与 $\mathbf{y}$ 之间的水平乘法定义了矩阵

$$T_{*,\mathbf{y},*} := \sum_{j=1}^{n_2} y_j T_{*,j,*},$$

而 T 与 $\mathbf{z}$ 之间的垂直乘法定义了矩阵

$$T_{*,*,\mathbf{z}} := \sum_{k=1}^{n_3} z_k T_{*,*,k}.$$

下面的示例展示了方向乘法。

例 2. 设 T 为例 1 中给出的三阶张量，设 $\mathbf{x} = (1, 1) \in \mathbb{F}_7^2$，$\mathbf{y} = (1, 0, 2) \in \mathbb{F}_7^3$，$\mathbf{z} = (1, 0, 0, 1) \in \mathbb{F}_7^4$。根据定义 11，$T$ 与 $\mathbf{x}$ 之间的垂直乘法定义为

$$T_{\mathbf{x},*,*} = T_{1,*,*} + T_{2,*,*} = \begin{pmatrix} 1&1&1&1 \\ 2&1&0&0 \\ 0&1&4&1 \end{pmatrix} + \begin{pmatrix} 0&0&1&1 \\ 2&3&0&1 \\ 0&0&0&5 \end{pmatrix} = \begin{pmatrix} 1&1&2&2 \\ 4&4&0&1 \\ 0&1&4&6 \end{pmatrix}$$

类似地， T 与 $\mathbf{y}$ 之间的水平乘法以及 T 与 $\mathbf{z}$ 之间的垂直乘法分别如下:

$$T_{*,\mathbf{y},*} = T_{*,1,*} + 2T_{*,3,*} = \begin{pmatrix} 1\,1\,1\,1 \\ 0\,0\,1\,1 \end{pmatrix} + 2\begin{pmatrix} 0\,1\,4\,1 \\ 0\,0\,0\,5 \end{pmatrix} = \begin{pmatrix} 1\,3\,2\,3 \\ 0\,0\,1\,4 \end{pmatrix}$$

and

$$T_{*,*,\mathbf{z}} = T_{*,*,1} + T_{*,*,4} = \begin{pmatrix} 1\,2\,0 \\ 0\,2\,0 \end{pmatrix} + \begin{pmatrix} 1\,0\,1 \\ 1\,1\,5 \end{pmatrix} = \begin{pmatrix} 2\,2\,1 \\ 1\,3\,5 \end{pmatrix}.$$

令 $\mathbf{e}_i \in \mathbb{F}_q^{n_1}$表示 $\mathbb{F}_q^{n_1}$的标准基中的第 i个元素（即一个长度为 n_1 的向量，其第 j 个位置上的值为 1，其余位置上的值均为 0）。 T 与 $\mathbf{e}_i$ 之间的垂直乘法为$T_{\mathbf{e}_i,\ *,\ *} = T_{i,\ *,\ *}$。类似地，与长度为 n_2 的标准向量 $\mathbf{e}j$ 和长度为 n_3 的标准向量 $\mathbf{e}_k$ 进行的水平乘法和垂直乘法分别为$T_{*,\ \mathbf{e}_j,\ *} = T_{*,\ j,\ *}$ 和$T_{*,\ *,\ \mathbf{e}_k} = T_{*,\ *,\ k}$。

注意，相同的记法也可以轻松地推广到矩阵。考虑$M \in \mathbb{F}_q^{m\times n}$,$\mathbf{x} \in \mathbb{F}_q^m$, $\mathbf{y} \in \mathbb{F}_q^n$，我们可以使用相同的记法来表示

$$\mathbf{x}M = M_{\mathbf{x},*} \quad M\mathbf{y}^\intercal = M_{*,\mathbf{y}}.$$

假设我们希望沿第一个指标将矩阵 $T_{*,\mathbf{y},*}$ 与向量 $\mathbf{x}$ 相乘。我们可以将上述引入的记号扩展为

$$(\mathbf{x}T_{*,\mathbf{y},*})_k = (T_{\mathbf{x},\mathbf{y},*})_k = \sum_{i=1}^{n_1}\sum_{j=1}^{n_2} t_{i,j,k}x_iy_j,$$

其中 $(T_{\mathbf{x},\mathbf{y},*})_k$ 表示 k向量的第 $T_{\mathbf{x},\mathbf{y},*}$.

利用定义 11 中引入的乘法，我们可以用 $G = (G_1, G_2, \ldots, G_k)$ 这一 3-张量生成元，在 $\mathbb{F}_q^{m\times n\times k}$ 中以紧凑形式表示 $\mathbb{F}_q^{m\times n}$ 中的一个 $\mathbb{F}_q$-线性矩阵码 $\mathcal{C}$，即

$$\mathcal{C} = \{G_{*,*,\mathbf{z}} \mid \mathbf{z} \in \mathbb{F}_q^k\}.$$

类似地， $\mathcal{C}$ 的对偶码可以写成 $\mathcal{C}^\perp = \{H_{*,*,\mathbf{z}} \mid \mathbf{z} \in \mathbb{F}_q^{n-k}\}$，其中 $H \in \mathbb{F}_q^{m\times n\times(n-k)}$ 是 $\mathcal{C}$ 的 3-张量校验矩阵。

在第2.1节中，我们看到了在同构 ϕ_B 下， $\mathbb{F}_{q^m}$-线性向量码及其矩阵码在对偶性中的不同内积。下面我们

将仔细考察这种差异如何影响矩阵形式下的 $\mathbb{F}_{q^m}$-线性秩度量码的译码，这表明下一小节需要在 $\mathbb{F}_q^m$ 上使用 T-乘积。

给定 $\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$上的一组基 B，直观地说，$\mathbb{F}_{q^m}$-线性码 $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ 的校验矩阵 $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ 可以转换为一个三阶张量 $\phi_B(H) \in \mathbb{F}_q^{m\times n\times(n-k)}$。$H$ 的每一行都会经由 ϕ_B 转换为 $\mathbb{F}_q^{m\times n}$中的一个矩阵。三阶张量 $\phi_B(H)$由与 H 的 $n-k$ 行对应的 $n-k$ 矩阵沿垂直于纸面的方向排列而成。对于矩阵 H，支撑较小意味着所有条目 $h_{i,j}$ 都属于一个较小的支撑 $\langle H\rangle_{\mathbb{F}_q} = \langle\beta_1, \ldots\ldots, \beta_d\rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}$ 的维数为 $d < m$。条目 $h_{i,j}$ 对应于 H的第 i 行中的第 j 个元素。在 $\phi_B(H)$ 中，它对应于第 i 个矩阵的第 j 列，因此 $\phi_B(h_{i,j}) = \phi_B(H)_{*,j,i}$。由于每个 $h_{i,j} \in \langle\beta_1,\ldots\ldots,\beta_d\rangle_{\mathbb{F}_q}$，每个向量 $\phi_B(H)_{*,j,i}$都属于 $\phi_B(\langle\beta_1,\ldots\ldots,\beta_d\rangle_{\mathbb{F}_q}) \subseteq \mathbb{F}_{q^m}$，而它是一个维数为 $d < m$ 的子空间。一个维数为 km 的 $\mathbb{F}_q$-维 $\mathbb{F}_q$-线性矩阵码 $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ 有一个校验张量 $H \in \mathbb{F}_q^{m\times n\times(nm-km)}$。遵循上述直观理解，我们可以将张量 H 的支撑定义为所有向量 $H_{*,i,j}$ 的张成空间。低密度校验张量是指支撑较小的张量。

矩阵码的问题在于伴随式的推广。设 $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ 是一个维数为 k 的 $\mathbb{F}_{q^m}$-线性码。设 $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$ 是 $\mathcal{C}$ 的校验矩阵，且 $\mathsf{e} \in \mathbb{F}_{q^m}^n$ 是一个错误。我们可以将 e 的伴随式计算为 $\mathsf{s} = \mathsf{e}H^\intercal \in \mathbb{F}_{q^m}^{n-k}$。由于伴随式是 $\mathbb{F}_{q^m}^{n-k}$ 的向量，其支撑可以是 $\mathbb{F}_{q^m}$ 中维数至多为 $n-k$ 的任意 $\mathbb{F}_q$-线性子空间。与 LRPC 码的情形一样，已知伴随式的支撑或许能让我们获知错误支撑的一些信息。对于矩阵码，伴随式仅有两种可能的支撑：$\{\mathbf{0}\}$ 和 $\mathbb{F}_q$。考虑码 $\mathcal{C}' = \phi_B(\mathcal{C}) \subseteq \mathbb{F}_q^{m\times n}$ 以及矩阵 $E = \phi_B(\mathsf{e}) \in \mathbb{F}_q^{m\times n}$。码 $\mathcal{C}'$ 在 $\mathbb{F}_q$ 上的维数为 km，并且存在一个校验张量 $H' \in \mathbb{F}_q^{m\times n\times m(n-k)}$。在此情形下，$E$ 的伴随式 $\mathsf{s}' \in \mathbb{F}_q^{m(n-k)}$ 可表示为 $s'_i = \mathrm{Tr}(H_{*,\,*,\,i}E^\intercal) \in \mathbb{F}_q$。若 E 不属于码，则 s' 的支撑为子空间 $\mathbb{F}_q$；否则为 $\{\mathbf{0}\}$。

请注意，s 和 s'都可以描述为 $n-km$ 个 $\mathbb{F}_q$元素。s 和 s' 之间的区别在于这些元素的分组方式。对于 s,

将这些元素按每组 m 个元素划分为子数组是很自然的，这些元素对应于 $\phi_B(s_i)$。另一方面，第二个伴随式 s′缺乏结构，这导致在矩阵码背景下对 LRPC 码进行译码时出现问题。为了解决这一问题，我们基于三阶张量引入了 $\mathbb{F}_q^m$中的向量乘积，从而得到结构更规整的伴随式。

3.2 $\mathbb{F}_q^m$ 上的 T-乘积

给定 $\mathbb{F}_q$上的 $\mathbb{F}_{q^m}$ 的一组基 B，同构 $\phi_B : \mathbb{F}_{q^m} \to \mathbb{F}_q^m$保持了 $\mathbb{F}_q$上的向量空间结构。在一个域中，我们有两个二元运算 $+, \cdot : \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$. 二元运算 $+$ 以及标量乘法 $\lambda \in \mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ 都由 ϕ_B 自然保持。也就是说，$\phi_B(\lambda_1 \mathbf{x} + \lambda_2 \mathbf{y}) = \lambda_1 \phi_B(\mathbf{x}) + \lambda_2 \phi_B(\mathbf{y})$。由于我们没有标准方法来定义 $\mathbb{F}_q^m$中两个元素之间的乘积，应用同构 ϕ_B 后，我们失去了域结构。

$\mathbb{F}_{q^m}$ 上的乘积具有两个对于 LRPC 码的译码算法至关重要的性质。正如观察 1 所指出的，给定两个维数分别为 r和 d的子空间 $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_{q^m}$，集合 $\mathcal{AB} = \{ab \mid a \in \mathcal{A}, b \in \mathcal{B}\}$ 包含于一个维数上界为 rd的空间 $\mathcal{A}.\mathcal{B}$ 中。得益于这一性质，我们可以将伴随式的支撑与校验矩阵的支撑以及错误的支撑联系起来。仅凭这一性质还不足以恢复错误的支撑。域 $\mathbb{F}_{q^m}$ 中乘积的第二个基本性质是，当 $b \neq 0$时，方程 $xb = c$ 恰好有一个解 $x = cb^{-1}$。借助以下事实，可以根据 $\mathcal{A}.\mathcal{B} = \langle \mathcal{AB} \rangle_{\mathbb{F}_q}$ 和 $\mathcal{B}$ 恢复 $\mathcal{A}$：对于任意 $0 \neq b \in \mathcal{B}$，都有 $\mathcal{A} \subseteq (\mathcal{A}.\mathcal{B})b^{-1} = \{sb^{-1} \mid s \in \mathcal{A}.\mathcal{B}\}$。对这些集合取交集后，就有可能以较高概率恢复 $\mathcal{A}$。牢记这两个性质，我们首先考虑一种满足这两个性质的 $\mathbb{F}_q^m$上的乘积。

我们简要介绍预半域的概念，它是一种满足 3 个性质的重要代数结构 [17，第 2 节。3]。

定义 12（有限预半域）。三元组 $S, +, \star$，其中 S 是有限集合，且两个二元运算 $+, \star$ 是定义在 $+, \star$ 上的二元运算：$S \times S \to S$，若满足以下 3 个性质，则称为有限预半域：

1. $S,+$ 构成阿贝尔群。2. 对任意 $a,b,c \in S$，有 $(a+b) \star c = ac + bc$ 且 $a \star (b+c) = ab + ac$。3. 对所有 $a,b \in S$，有 $a \star b = 0$ 当且仅当 $a = 0$ 或 $b = 0$。

请注意，当 S 是有限集时，第三个条件等价于要求 $a \star x = b$ 和 $y \star a = c$ 始终存在唯一解。

我们需要一种稍微更专门化的结构。

定义 13（$\mathbb{F}_q$-线性预半域）。设 $\star$： $\mathbb{F}_q^m \times \mathbb{F}_q^m \to \mathbb{F}_q^m$是定义在 $\mathbb{F}_q^m$上的二元运算。若 $\mathbb{F}_q^m$、$+$、$\star$满足以下三个性质，则称其为一个 $\mathbb{F}_q$-线性预半域。对于任意 a、b、c $\in \mathbb{F}_q^m$,

– S、$+$ 构成一个阿贝尔群。–（双线性）(μa+νb)$\star$c $= \mu$(a$\star$c)+ν(b$\star$c), 且 a$\star$(μb+νc) $= \mu$(a$\star$b)+ν(a$\star$c)，对任意 μ、$\nu \in \mathbb{F}_q$.均成立。–（可逆）给定方程 x $\star$b $=$ c，对于所有 b $\neq$ 0，都存在唯一解 x。换言之，右乘映射 R_b(x) $=$ x $\star$b 是可逆的。由于 $\mathbb{F}_q^m$的元素个数有限，我们还可知 R_b 是双射。

定义 13 中的第二个条件要求乘积 $\star$ 具有分配性和 $\mathbb{F}_q$-线性。当 q 为素数时，它与定义 12 的第二个性质一致。此外，定义 12 和定义 13 中的第三个条件是等价的。注意，如果 a′$\star$b $=$ a$\star$b $=$ c，那么 (a′−a)$\star$b $=$ 0因此 a $=$ a′ 或 b 具有一个非零零因子。在本文的其余部分，我们将满足第三个条件的乘积称为可逆乘积。

由 $\mathbb{F}_q$-线性预半域在集合 $\mathbb{F}_q^m$上定义的一个例子，可以通过将 $\mathbb{F}_{q^m}$ 上的标准乘积与 ϕ_B进行复合得到。明确地说，定义的乘积为 $\star$ a $= \phi_B$(ab), 其中 $a = \phi_B^{-1}$ (a)$b = \phi_B^{-1}$ (b) $\in \mathbb{F}_{q^m}$，而$+$ 表示两个向量的分量逐项相加。对于第一个性质，我们显然有 $\mathbb{F}_q^m$，$+$ 是一个阿贝尔群。第二个性质源于域中乘法的双线性。考虑右乘法 R_b(x) $=$ x $\star$ b $= \phi_B(xb)$，其逆 $R_b^{-1}(x)$恰好是函数 $R_{b^{-1}}$(x) $=$x$\star$b$^{-1} = \phi_B(xb^{-1})$。我们有 $R_b(R_{b^{-1}}(x)) = x$，这只是以一种烦琐的方式表达：对于 $0 \neq b \in \mathbb{F}_{q^m}$，我们有 $(xb)b^{-1} = x$，对所有 $x \in \mathbb{F}_{q^m}$.均成立。

在本小节的其余部分，我们将展示有限 $\mathbb{F}_q$-线性预半域 $(\mathbb{F}_q^m, +, \star)$ 的结构如何保留允许在域 $\mathbb{F}_{q^m}$上对 LRPC 码进行译码的两个基本性质。随后，我们将引入 $\mathbb{F}_q^m$ 上的双线性乘法；在 Knuth 已于 [17], 研究的某些特殊条件下，该乘法产生一个 $\mathbb{F}_q$-线性预半域。最后，我们将展示如何放宽这些条件，同时仍能对更大一类的部分可逆乘积进行译码；这类乘积将在后文定义。

定理 2. 设 $(\mathbb{F}_q^m, +, \star)$ 是一个 $\mathbb{F}_q$-线性预半域。设 $\mathcal{A} = \langle \boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_r \rangle_{\mathbb{F}_q}$,$\mathcal{B} = \langle \boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_d \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_q^m$ 是维数分别为 r 和 d 的两个线性子空间，且 $rd \leq m$。考虑 $\mathcal{A} \star \mathcal{B} = \{\mathsf{a} \star \mathsf{b} \mid \mathsf{a} \in \mathcal{A}, \mathsf{b} \in \mathcal{B}\}$，并设 $\langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q}$ 是包含 $\mathcal{A} \star \mathcal{B}$. 的 $\mathbb{F}_q^m$ 的最小子空间。我们有以下两个性质：

1. $\dim(\langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q}) \leq rd$
2. $\mathcal{A} \subseteq \mathrm{R}_{\mathbf{b}}^{-1}(\langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q}) = \{\mathrm{R}_{\mathbf{b}}^{-1}(\mathbf{c}) \mid \mathbf{c} \in \langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q}\}, \forall 0 \neq \mathbf{b} \in \mathcal{B}.$

证明。考虑集合 $\langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q}$。我们要证明其维数 $\dim(\langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q}) = k$ 的上界为 rd。根据定义，子空间 $\langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q}$ 由集合 $\mathcal{A} \star \mathcal{B} = \{\mathsf{a} \star \mathsf{b} \mid \mathsf{a} \in \mathcal{A}, \mathsf{b} \in \mathcal{B}\}$ 生成。一个一般元素 $\mathsf{a} \star \mathsf{b} \in \mathcal{A} \star \mathcal{B}$ 可表示为

$$\mathbf{a} \star \mathbf{b} = \Big(\sum_{i \in [r]} a_i \boldsymbol{\alpha}_i \Big) \star \Big(\sum_{j \in [d]} b_j \boldsymbol{\beta}_j \Big) = \sum_{(i,j) \in [r] \times [d]} \lambda_{j,i} \mu_{j,j} (\boldsymbol{\alpha}_i \star \boldsymbol{\beta}_j).$$

这意味着 $\{(\boldsymbol{\alpha}_i \star \boldsymbol{\beta}_j)\}_{(i,j) \in [r] \times [d]}$ 是 $\langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q}$ 的一组生成元，其大小至多为 rd, 也就是说，$\langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q}$ 的维数至多为rd。

对于证明的第二部分，考虑集合 $\mathcal{A} \star \mathsf{b} = \{\mathsf{a} \star \mathsf{b} \mid \mathsf{a} \in \mathcal{A}\}$。由于 $\star$对第一个自变量具有线性性，它是 $\mathbb{F}_q^m$的一个线性子空间。我们可以将空间 $\langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q}$ 分解为

$$\langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q} = \mathcal{A} \star \boldsymbol{\beta}_1 + \cdots + \mathcal{A} \star \boldsymbol{\beta}_d,$$

其中 $\mathcal{A} \star \boldsymbol{\beta}_j = \langle \boldsymbol{\alpha}_1 \star \boldsymbol{\beta}_j$、.....、$\boldsymbol{\alpha}_r \star \boldsymbol{\beta}_j \rangle_{\mathbb{F}_q}$.。注意，每个子空间 $\mathcal{A} \star \boldsymbol{\beta}_j$ 都包含于 $\langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q}$ 中，并且所有子空间的并集覆盖了$\langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q}$. 的一组基。

由于 $\star$ 可逆，若 $\mathbf{b} \neq 0$，则有 $\mathrm{R}^{-1}{}_{\mathbf{b}}(\mathcal{A} \star \mathbf{b}) = \mathcal{A}$。特别地，$\mathrm{R}^{-1}_{\beta_i}(\mathcal{A} \star \beta_i) = \mathcal{A}$，因此 $\mathcal{A} \subseteq \mathrm{R}^{-1}_{\beta_i}(\langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q})$。对于任意的 $0 \neq \mathbf{b} \in \mathcal{B}$，我们总可以写出一个包含 $\mathbf{b}$ 的 $\mathcal{B}$ 的基。即 $\mathcal{B} = \langle \mathbf{b}\ \beta'_2, \ldots, \beta'_d \rangle_{\mathbb{F}_q}$。通过这一基变换，我们可以考虑如下分解

$$\langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q} = \mathcal{A} \star \mathbf{b} + \mathcal{A} \star \beta'_2 + \cdots + \mathcal{A} \star \beta'_d$$

并得出 $\mathcal{A} = \mathrm{R}^{-1}{}_{\mathbf{b}}(\mathcal{A} \star \mathbf{b}) \subseteq \mathrm{R}^{-1}{}_{\mathbf{b}}(\langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q})$】【。 □

请注意，证明定理 2 中的第一个性质并不需要可逆性。对于非可逆的双线性乘积 $\star$，仍然有 $\dim(\langle \mathcal{A} \star \mathcal{B} \rangle_{\mathbb{F}_q}) \leq \dim(\mathcal{A})\ \dim(\mathcal{B})$。

我们已经看到，将向量空间 $\mathbb{F}_q^m$ 配备由 $\mathbb{F}_{q^m}$ 上的标准乘积与同构 $\phi_B : \mathbb{F}_{q^m} \to \mathbb{F}_q^m$ 复合而成的乘积后，便构成一个 $\mathbb{F}_q$- 线性预半域。毫不意外，这种构造与有限域 $\mathbb{F}_{q^m}$ 同构；如果我们决定采用这种乘积，就会得到我们已经熟知的 LRPC 码。

下面我们介绍一种基于三阶张量T的更通用的双线性乘积基。Knuth 在 [17] 中提出了一种非常相似的构造。关于张量记号的详细说明，请参阅第 3.1 节。

定义 14（T-乘积）。设 T 是 $\mathbb{F}_q^{m \times m \times m}$ 中的一个三阶张量。对于 $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^m$，我们将 $\mathbf{a}$ 和 $\mathbf{b}$ 之间的 T-乘积定义为

$$\mathbf{a} \cdot_T \mathbf{b} = \mathbf{a} T_{*,\mathbf{b},*} = T_{\mathbf{a},\mathbf{b},*}.$$

更具体地，对于 $\mathbf{a} = (a_1, \ldots, a_m)$ 和 $\mathbf{b} = (b_1, \ldots, b_m)$，我们定义$T$-乘积 $\mathbf{c} = \mathbf{a} \cdot_T \mathbf{b} = T_{\mathbf{a},\ \mathbf{b},\ *}$ 为

$$c_k = \sum_{i=1}^{m} \sum_{j=1}^{m} a_i b_j t_{i,j,k}, \quad k \in [m].$$

将 T-乘积定义为 $\mathbf{a} \cdot_T \mathbf{b} = \mathbf{b} T_{\mathbf{a},\ *,\ *}$ 是等价的。为阐明该乘积的用法，我们在此举一个例子。

例3。考虑以下三阶张量 $T \in \mathbb{F}_7^{3\times3\times3}$

$$T = (T_{*,*,1}, T_{*,*,2}, T_{*,*,3}) = \left(\begin{array}{ccc|ccc|ccc} 1&0&3&2&2&2&1&5&6\\ 3&4&0&1&3&3&3&2&2\\ 0&1&0&0&2&1&1&2&2 \end{array}\right).$$

考虑两个向量 $\mathbf{a} = \begin{pmatrix}2&0&2\end{pmatrix}$ 和 $\mathbf{b} = \begin{pmatrix}1&1&1\end{pmatrix}$，根据定义 14，我们有

$$\mathbf{a} \cdot_T \mathbf{b} = \mathbf{a}T_{*,\mathbf{b},*} = (2,0,2)\begin{pmatrix}4&6&5\\0&0&0\\1&3&5\end{pmatrix} = (3,4,6),$$

等价地，我们可以计算相同的乘积:

$$\mathbf{a} \cdot_T \mathbf{b} = \mathbf{b}T_{\mathbf{a},*,*} = (1,1,1)\begin{pmatrix}2&4&4\\2&1&0\\6&6&2\end{pmatrix} = (3,4,6).$$

注意，矩阵 $T_{*,\ \mathbf{b},\ *}$ 不是满秩的。这意味着存在多个 $\mathbf{a}$ 的取值，使得 $\mathbf{a} \cdot_T \mathbf{b} = (3,4,6)$。例如，我们有 $(2,0,2) \cdot_T (1,1,1) = (2,1,2) \cdot_T (1,1,1) = (3,4,6)$。对于这一选择 T，T-乘积不可逆，因此在这种情况下，$(\mathbb{F}_q^m, +, \cdot_T)$ 不是一个 $\mathbb{F}_q$- 线性预半域。

正如我们刚才在例3中看到的，对于任意张量 $T \in \mathbb{F}_q^{m\times m\times m}$，$T$-乘积都是双线性的；但一般而言，它不一定可逆。

在第 3.1 节中，我们讨论如何将三阶张量解释为矩阵线性码的生成元。研究由张量 T 生成的码，将为我们提供一个充要条件，以判断给定张量 T 的关联 T- 积是否可逆。[7, 定理 3] 探讨了类似背景下的这一联系，[17, 定理 4.4.1] 中也曾对此进行研究。

命题 1. 对于给定的三阶张量 $T \in \mathbb{F}_q^{m\times m\times m}$，三元组 $(\mathbb{F}_q^m, +, \cdot_T)$ 是一个 Fq-线性预半域，当且仅当 $\{T_{*,i,*} \in \mathbb{F}_q^{m\times m}\}$ 是一个维数为 m 的最大秩距离码的基。等价地，当且仅当

$$\mathrm{Rank}(T_{*,\mathbf{b},*}) = m,\ \forall \mathbf{b} \in \mathbb{F}_q^m \setminus \{\mathbf{0}\}.$$

得益于这一结果，所有已知的维数为 m 的 $\mathbb{F}_q$-线性最大秩距离码（MRD 码）都可以用来生成可逆的 T-乘积。此外，我们还报告了一项重要结果，该结果与命题 1 中给出的预半域构造有关。具体而言，以下结果给出了一种构造新预半域的方法：对另一个预半域乘积所定义的三阶张量进行处理。

命题 2. *[17, 定理 4.3.1]* 设 $T \in \mathbb{F}_q^{m\times m\times m}$是一个可导出 $\mathbb{F}_q$-线性预半域的三阶张量。如果 U 是一个定义为 $u_{i,j,k} = t_{\sigma(i,j,k)}$ 的张量，其中 σ 是 (i, j, k) 的一个置换，那么 U定义了另一个 $\mathbb{F}_q$-线性预半域。

利用这一结果，可以使用命题 1，通过对一个已知的最大秩距离码进行变换来构造一个新的$[m \times m, m]$ 最大秩距离码。

推论 1. 设 $T \in \mathbb{F}_q^{m\times m\times m}$是一个可导出 $\mathbb{F}_q$-线性预半域的三阶张量，则以下各码：

$$\mathcal{T}_1 = \langle T_{i,*,*} \mid i \in [m]\rangle_{\mathbb{F}_q}, \mathcal{T}_2 = \langle T_{*,i,*} \mid i \in [m]\rangle_{\mathbb{F}_q}, \mathcal{T}_3 = \langle T_{*,*,i} \mid i \in [m]\rangle_{\mathbb{F}_q}$$

都是 $\mathbb{F}_q^{m\times m\times m}$中的最大秩距离码，其维数为 m ，最小距离为 m。

证明. 根据命题 1，我们已经知道 $\mathcal{T}_2$ 是一个最大秩距离码，其维数为 m ，最小距离为 m。

应用命题 2，令 $U = T^\sigma$ 为对定义另一个预半域的张量的指标应用置换 σ 后得到的张量。令 $\mathcal{U}_2 = \langle U_{*,\ i,\ *} \mid i \in [m]\rangle_{\mathbb{F}_q}$，对于 $\sigma = (1, 3, 2)$，我们得到 $\mathcal{U}_2 = \mathcal{T}_1$；对于 $\sigma = (2, 3)$，我们得到 $\mathcal{U}_2 = \mathcal{T}_3$。

由命题 2，张量 U 定义了一个 $\mathbb{F}_q$-线性预半域，应用命题 1 可得所需结果。□

利用 T-积在 $\mathbb{F}_{q^m}$ 上，我们可以在 $\mathbb{F}_q^{m\times n}$ 上定义一个内积。

定义 15（T-内积）。对于两个矩阵 A、$B \in \mathbb{F}_q^{m\times n}$，我们用 $\mathbf{a}_j$ 表示 A 的第 j 列，用 $\mathbf{b}_j$ 表示 B的第 j 列。A 和 B 的 T-内积定义为

$$A \cdot_T B = \sum_{j\in[n]} \mathbf{a}_j^\intercal \cdot_T \mathbf{b}_j^\intercal \in \mathbb{F}_q^m.$$

向量 $A \cdot_T B \in \mathbb{F}_q^m$ 可以用迹函数改写为

$$(A \cdot_T B)_k = \mathrm{Tr}(A^\intercal T_{*,*,k} B) = \mathrm{Tr}(T_{*,*,k} B A^\intercal),$$

其中，Tr(M)表示 M中对角元素的和。

为了解定义 15 中两个公式的等价性，考虑$C = A^\intercal T_{*,*,k} B$，特别是

$$\begin{aligned} c_{j,j} &= \sum_{i=1}^{m} A^\intercal[j,i](T_{*,*,k}B)[i,j] = \sum_{i=1}^{m} A^\intercal[j,i] \sum_{l=1}^{m} (T_{*,*,k})[i,l]B[l,j] \\ &= \sum_{i=1}^{m}\sum_{l=1}^{m} a_{i,j} t_{i,l,k} b_{l,j} = T_{\mathbf{a}_j^\intercal, \mathbf{b}_j^\intercal, k}. \end{aligned}$$

代入第二个公式可得

$$(A \cdot_T B)_k = \sum_{j\in[n]} c_{j,j} = \sum_{j\in[n]} T_{\mathbf{a}_j^\intercal, \mathbf{b}_j^\intercal, k} = \sum_{j\in[n]} \mathbf{a}_j^\intercal \cdot_T \mathbf{b}_j^\intercal.$$

值得注意的是，$\mathbb{F}_q^{m\times n}$上的 T-内积可以转换为 $\mathbb{F}_{q^m}^n$上的标准内积。固定 $\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$上的一组基 B 后，我们可以证明，两个向量 $\mathbf{x}$、$\mathbf{y} \in \mathbb{F}_{q^m}^n$ 之间的标准内积可以表示为由 T的特定选择所诱导的对应两个矩阵X_B、Y_B之间的 T-内积。回忆一下，迹算子 $\mathrm{Tr}^{q^m/q}$：$\mathbb{F}_{q^m} \to \mathbb{F}_q$定义为 $\mathrm{Tr}^{q^m/q}(a) = a + a^q + \cdots + a^{q^{m-1}} = \sum_{i=0}^{m-1} a^{q^i}$。给定 $\mathbb{F}_{q^m}$在 $\mathbb{F}_q$上的一组基 $B = (\alpha_1, \ldots, \alpha_m)$，矩阵 Δ_B 定义为 $(\Delta_B)_{i,j} = \mathrm{Tr}^{q^m/q}(\alpha_i\alpha_j)$，它总是可逆的（参见 [19, 定理 2.37]）。注意，对于 $x = \sum_{i=1}^m x_i\alpha_i$，我们有

$$\mathrm{Tr}_{q^m/q}(\alpha_j x) = \sum_{i=1}^{m} x_i \,\mathrm{Tr}_{q^m/q}(\alpha_i\alpha_j).$$

因此 $(\mathrm{Tr}^{q^m/q}(\alpha_1 x), \ldots, \mathrm{Tr}^{q^m/q}(\alpha_m x)) = \phi_B(x)\Delta_B$，并且由于 Δ_B 可逆，我们还有 $\phi_B(x) = (\mathrm{Tr}^{q^m/q}(\alpha_1 x), \ldots, \mathrm{Tr}^{q^m/q}(\alpha_m x))\Delta_B^{-1}$。以下引理说明了 $\mathbb{F}_{q^m}^n$ 上的内积与和三阶张量相关联的 $\mathbb{F}_q^{m\times n}$ 上的新内积之间的联系。

引理 1. 设 $\mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^m}^n$，且 $B = (1, \alpha, \ldots, \alpha^{m-1})$ 是 $\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$ 上的一组基，其中 α 是 $\mathbb{F}_{q^m}$ 的本原元，其伴随矩阵为 A_B，并设 $B' = (\beta_1, \ldots, \beta_m)$ 为其标准正交基。设 $T \in \mathbb{F}_q^{m \times m \times m}$ 是如下定义的三阶张量：$T_{*,*,k} = (A_B^{k-1})^\intercal M^{-1}$，其中 M 是基变换 $BM = B'$。若定义三阶张量 U，使得 $U_{*,*,l} = \sum_{k=1}^m T_{*,*,k} (\Delta_B^{-1})_{k,l}$，则有

$$\phi_B(\mathbf{x}\mathbf{y}^\intercal) = \phi_B(\mathbf{x}) \cdot_U \phi_B(\mathbf{y}).$$

注意，对于 $n = 1$，这意味着 $(\mathbb{F}_{q^m}, +, \cdot) \cong (\mathbb{F}_q^m, +, \cdot_U)$。

证明。考虑 $X_{B'} = \phi_{B'}(\mathbf{x})$ 和 $Y_B = \phi_B(\mathbf{y})$，我们有 $B' X_{B'} = \mathbf{x}$ 和 $BY_B = \mathbf{y}$，此外 $B' M^{-1} M X_{B'} = BMX_{B'} = \mathbf{x}$，因此 $X_B = MX_{B'}$。内积 $\mathbf{x}\mathbf{y}^\intercal = \sum_{i=1}^n x_i y_i$ 的迹可计算为

$$\mathrm{Tr}_{q^m/q}(\mathbf{x}\mathbf{y}^\intercal) = \sum_{i=1}^n \sum_{j=1}^m \sum_{k=1}^m x_{i,j} y_{i,k} \, \mathrm{Tr}_{q^m/q}(\alpha^{k-1} \beta_j) = \sum_{i=1}^n \sum_{j=1}^m x_{i,j} y_{i,j},$$

注意，最后一项等于 $\mathrm{Tr}(X_{B'} Y_B^\intercal)$。

类似地，我们可以计算 $\mathrm{Tr}_{q^m/q}(\alpha^t \mathbf{x}\mathbf{y}^\intercal)$。注意，$\phi_B(\alpha^t \mathbf{y}) = A_B^t Y_B$，于是 $\mathrm{Tr}_{q^m/q}(\alpha^t \mathbf{x}\mathbf{y}^\intercal) = \mathrm{Tr}(X_{B'} (A_B^t Y_B)^\intercal)$。在基 B 中写出所有项，并利用迹的性质，可将其改写为 $\mathrm{Tr}(Y_B^\intercal (A_B^t)^\intercal M^{-1} X_B)$。考虑由 $T_{*,*,k} = (A_B^{k-1})^\intercal M^{-1}$ 给出的三阶张量 T，根据定义 15，我们有

$$(X_B \cdot_T Y_B)_k = \mathrm{Tr}(Y_B^\intercal (A_B^k)^\intercal M^{-1} X_B).$$

最后，我们可以应用定理 2.3。7 [19]从而得到

$$\phi_B(\mathbf{x}\mathbf{y}^\intercal) = (\phi_B(\mathbf{x}) \cdot_T \phi_B(\mathbf{y})) \Delta_B^{-1} = \phi_B(\mathbf{x}) \cdot_U \phi_B(\mathbf{y}).$$

□

4 广义 LRPC 码

在本节中，我们将介绍 $\mathbb{F}_q$ 上的广义低秩奇偶校验矩阵码，并讨论它们的一些性质。下面首先讨论如何利用 $\mathbb{F}_q^{m \times m \times m}$ 中的张量扩展 $\mathbb{F}_q$-线性秩度量码。

假设 $\mathbf{g}_1$、. . .、$\mathbf{g}_k \in \mathbb{F}_{q^m}^n$ 是 $\mathbb{F}_q$-线性无关向量。$\mathbb{F}_q$-线性码 $\mathcal{C} = \langle \mathbf{g}_1$、. . .、$\mathbf{g}_k \rangle_{\mathbb{F}_q}$ 的 $\mathbb{F}_q$-维数为 k，可以通过考虑 $\mathbf{g}_1$、. . .、$\mathbf{g}_k$ 的所有 $\mathbb{F}_{q^m}$-线性组合来展开。这样，我们得到 $\mathbb{F}_{q^m}$-线性码 $\mathcal{C}_{\mathbb{F}_{q^m}} = \langle \mathbf{g}_1$、. . .、$\mathbf{g}_k \rangle_{\mathbb{F}_{q^m}}$。码 $\mathcal{C}_{\mathbb{F}_{q^m}}$ 的 $\mathbb{F}_q$-维数至多为mk。设 $\alpha \in \mathbb{F}_{q^m}$ 是 $\mathbb{F}_{q^m}$ 的一个本原元，则刚才考虑的展开可以改写为

$$\mathcal{C}_{\mathbb{F}_{q^m}} = \langle \alpha^{i-1}\mathbf{g}_j \rangle_{\mathbb{F}_q}, \quad i \in [m], j \in [k].$$

$\mathcal{C}$ 与 $\mathcal{C}_{\mathbb{F}_{q^m}}$ 之间的关系可以表示为

$$\mathcal{C}_{\mathbb{F}_{q^m}} = \mathcal{C} + \alpha\mathcal{C} + \cdots + \alpha^{m-1}\mathcal{C},$$

其中 $\alpha^i\mathcal{C} = \{\alpha^i\mathbf{c} \mid \mathbf{c} \in \mathcal{C}\}$。将 $x \in \mathbb{F}_{q^m}$ 映射到 αx 的函数是 $\mathbb{F}_q$-线性的。一旦我们固定了 $\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$ 上的一组基 B，就可以将乘以 α 表示为乘以矩阵 A_B，该矩阵由以下关系定义：对于所有 $x \in \mathbb{F}_{q^m}$，$A_B\phi_B(x) = \phi_B(\alpha x)$。

码 $\mathcal{C}$ 具有矩阵表示。

$$\phi_B(\mathcal{C}) = \langle \phi_B(\mathbf{g}_j) \mid j \in [k] \rangle_{\mathbb{F}_q}$$

而码 $\mathcal{C}_{\mathbb{F}_{q^m}}$ 具有如下矩阵表示 马会

$$\phi_B(\mathcal{C}_{\mathbb{F}_{q^m}}) = \langle \phi_B(\alpha^{i-1}\mathbf{g}_j) \rangle_{\mathbb{F}_q} = \langle A_B^{i-1}\phi_B(\mathbf{g}_j) \mid (i,j) \in [m] \times [k] \rangle_{\mathbb{F}_q}$$

其中 $A_B^0 = I_m$。这两种矩阵表示之间的关系可以表示为

$$\phi_B(\mathcal{C}_{\mathbb{F}_{q^m}}) = \phi_B(\mathcal{C}) + A_B\phi_B(\mathcal{C}) + \cdots + A_B^{m-1}\phi_B(\mathcal{C}),$$

其中 $A_B^i\phi_B(\mathcal{C}) = \{A_B^i C \mid C \in \phi_B(\mathcal{C})\}$.

上述展开中的矩阵 $A_B^i, i = 0, \ldots, m-1$ 可视为 $\mathbb{F}_q^{m\times m\times m}$ 中张量的切片。类似地，我们可以通过一个一般的张量 T，将维数为 k 的 $\mathbb{F}_q$-线性矩阵码扩展到更高维数，且维数至多为 mk。

定义 16（T-扩展）。设 $\mathcal{C} = \langle G_j \mid j \in [k] \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_q^{m \times n}$ 是一个维数为 k 的矩阵码，且 $T \in \mathbb{F}_q^{m \times m \times m}$ 是一个三阶张量。$\mathcal{C}$ 的 T-扩展码定义为

$$\mathcal{C}_T = \langle T_{*,*,i} G_j \mid (i,j) \in [m] \times [k] \rangle_{\mathbb{F}_q}.$$

$\mathcal{C}_T$ 的维数最多为 km。

4.1 主要构造

现在我们可以介绍本文的主要构造了。

定义 17（广义 LRPC 码）。设 T 是 $\mathbb{F}_q^{m \times m \times m}$ 中的一个三阶张量，且 H_1，...，H_{n-k} 是 $\mathbb{F}_q^{m \times n}$ 中线性无关的 $n-k$ 矩阵。设 $\mathcal{B} \subseteq \mathbb{F}_q^m$ 是一个向量子空间，使得 Colsp(H_i) $\subseteq \mathcal{B}$，$\forall i \in [n-k]$ 且 dim($\mathcal{B}$) $= d < m$。考虑码 $\mathcal{H} = \langle H_1, ..., H_{n-k} \rangle_{\mathbb{F}_q}$ 及其 T-展开 $\mathcal{H}_T = \langle T_{*,\ *,\ i} H_j \mid (i,j) \in [m] \times [n-k] \rangle_{\mathbb{F}_q}$。码 $\mathcal{C} =$($\mathcal{H}_T$)$^{\perp}$ 称为广义 LRPC 码，可明确表示为

$$\mathcal{C} = \{C \in \mathbb{F}_q^{m \times n} \mid \mathrm{Tr}(T_{*,*,i} H_j C^{\intercal}) = 0, \forall (i,j) \in [m] \times [n-k]\}.$$

作为广义 LRPC 码的第一个示例，我们可以证明经典 LRPC 码是广义 LRPC 码的一种特殊情况。我们用 $\mathbf{h}_1$、.....、$\mathbf{h}_{n-k}$ 表示矩阵 $H \in \mathbb{F}_{q^m}^{(n-k) \times n}$ 的各行，使得 dim($\langle H \rangle_{\mathbb{F}_q}$) $= d <$$m$。矩阵 H 是向量形式下 LRPC 码 $\mathcal{C}$ 的校验矩阵。

我们要证明，码 $\mathcal{C}$ 的矩阵形式与一个广义 LRPC 码同构。为此，我们需要选择一个合适的 $\mathbb{F}_q$ 上的 $\mathbb{F}_{q^m}$基，以及一个合适的三阶张量 T。设 α 是 $\mathbb{F}_{q^m}$ 的一个本原元，且设 $B = \{1, \alpha, \ldots, \alpha^{m-1}\}$ 是 $\mathbb{F}_q$. 上的 $\mathbb{F}_{q^m}$ 基。取 $H_i = \phi_B$($\mathbf{h}_i$)，其中 $i = 1$ 为 2, . . . , $n-k$。码 $\mathcal{H} = \langle H_1, \ldots, H_{n-k} \rangle_{\mathbb{F}_q}$ 是 ϕ_B ($\mathcal{C}^{\perp}$)的一个 $\mathbb{F}_q$-线性子空间，其维数为 $n-k$。滥用记号，我们将 ϕ_B($\langle H \rangle_{\mathbb{F}_q}$) =$\langle \phi_B(h_{i,j}) \mid (i,j) \in [n-k] \times [n] \rangle_{\mathbb{F}_q}$，注意，对于所有$i \in [n-k]$.，列空间($H_i$) $\subseteq \phi_B$($\langle H \rangle_{\mathbb{F}_q}$)。此外，由于 dim($\langle H \rangle_{\mathbb{F}_q}$) $= d < m$，因此 dim(ϕ_B($\langle H \rangle_{\mathbb{F}_q}$)) $= d < m$.。

为了证明 ϕ_B($\mathcal{C}$) 是广义 LRPC 码，我们需要找到一个适当的三阶张量 T，使得展开式 $\mathcal{H}_T = \phi_B$($\mathcal{C}^{\perp}$)。码 $\mathcal{C}^{\perp} = \langle \mathbf{h}_j \mid j \in$

$[n-k]\rangle_{\mathbb{F}_{q^m}}$是 H的行所张成的 $\mathbb{F}_{q^m}$。我们还有 $\mathcal{C}^{\perp} = \langle \alpha^{i-1}\mathbf{h}_j \mid (i,j) \in [m] \times [n-k]\rangle_{\mathbb{F}_q}$。正如我们上面所见，乘以 α是一个线性函数。我们将与该函数相关联的矩阵记为 A_B，其所依据的基为 B。现在很明显，

$$\phi_B(\mathcal{C}^{\perp}) = \langle A_B^{i-1} H_j \mid (i,j) \in [m] \times [n-k]\rangle_{\mathbb{F}_q},$$

这是使用三阶张量 T 对码 $\mathcal{H}$ 进行展开，其中$T_{*,\ *,\ i} = A_B^{i-1}$ 对于 $i \in [m]$，其中 $A_B^0 = I_m$。注意，集合 I_m、A_B、.....、A_B^{m-1} 构成一个最大秩距离码的基。由命题 2可知，由 T 诱导的乘积是可逆的。

到目前为止，我们已经证明了 $\mathcal{H}_T = \phi_B(\mathcal{C}^{\perp})$。根据定义 17，码 $(\mathcal{H}_T)^{\perp}$是一个广义 LRPC 码。我们有 $(\mathcal{H}_T)^{\perp} = \phi_B(\mathcal{C}^{\perp})^{\perp}$。回顾定理 1 [15]，我们还得到 $\phi_B(\mathcal{C}^{\perp})^{\perp} = \phi_{B'}(\mathcal{C})$，由此得到同构

$$(\mathcal{H}_T)^{\perp} = \phi_{B'}(\mathcal{C}) \cong \phi_B(\mathcal{C}).$$

4.2 广义 LRPC 码之间的关系

为了定义广义 LRPC 码，我们需要一个由矩阵H_1、.....、$H_{n-k} \in \mathbb{F}_q^{m\times n}$生成的码 $\mathcal{H}$，这些矩阵的列空间包含于一个较小的子空间$\mathcal{B} \subseteq \mathbb{F}_q^m$中，还需要一个三阶张量 T。这里自然会产生一个问题：由不同矩阵码和张量导出的两个广义 LRPC 码之间是否存在某种关系？本小节研究矩阵码由两个同位张量展开时的这一问题。

我们首先回顾 Knuth 的研究中关于预半域的一些观察 [17]，这些观察与我们的讨论密切相关。Knuth 指出，所有预半域都与非奇异三阶张量 T 相关，其乘法的定义方式大致与我们定义 T-乘积的方式相同。采用本文引入的记号，他对非奇异三阶张量的定义对应于如下性质：切片 $T_{*,\ *,\ k}$ 的任意非零线性组合都是可逆的（见命题 2）。若存在 3 个可逆线性映射 A、B、C，从 S到 S'，使得对于 S、$+$、$\cdot_T$以及 S'、$+$、$\cdot_U$，

$$(x \cdot_T y)C = (xA) \cdot_U (yB)$$

对所有 x、$y \in S$ 均成立。

每个三阶张量 $T \in \mathbb{F}_q^{m\times m\times m}$都可以与一个三线性映射 $\mathbb{F}_q^m \times \mathbb{F}_q^m \times \mathbb{F}_q^m \to \mathbb{F}_q$ 相关联，而每个三线性映射也可以解释为一个三阶张量。考虑 $\mathbb{F}_q^m$ 的标准基 $\mathbf{e}_1$、$\ldots$、$\mathbf{e}_m$，则有 $T(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k) = t_{i,j,k}$。

设 $U(\mathbf{x}, \mathbf{y}, \mathbf{z}) = T(\mathbf{x}A, \mathbf{y}B, \mathbf{z}C)$，其中 A、B、$C \in \mathbb{F}_q^{m\times n}$ 是可逆线性映射。我们得到 U 与 T 的各项之间的如下关系。

$$u_{i,j,k} = \sum_{u=1}^{m}\sum_{v=1}^{m}\sum_{w=1}^{m} a_{i,u}b_{j,v}c_{k,w}t_{u,v,w}. \tag{2}$$

我们将证明，$\mathbf{x} \cdot_T \mathbf{y}$ 与 $\mathbf{x} \cdot_U \mathbf{y}$ 之间的关系为

$$(\mathbf{x} \cdot_U \mathbf{y})(C^{\intercal})^{-1} = (\mathbf{x}A) \cdot_T (\mathbf{y}B), \tag{3}$$

这表明张量 U 与 T 同位。当 $C = I_m$ 时，这一关系显而易见。为了理解 $C \neq I_m$ 时的情况，并避免繁杂的记号，考虑较简单的情形：$U(\mathbf{x}, \mathbf{y}, \mathbf{z}) = T(\mathbf{x}, \mathbf{y}, \mathbf{z}C)$。定义 $\mathbf{v} = \mathbf{x}\cdot_T\mathbf{y} = \sum_{i,j,k=1}^{m} x_i y_j t_{i,j,k}\mathbf{e}_k$。现在考虑 $\mathbf{x}\cdot_U\mathbf{y} = \sum_{i,j,k=1}^{m} x_i y_j u_{i,j,k}\mathbf{e}_k$，我们可以利用（2）代入 $u_{i,j,k}$，得到

$$\begin{aligned}\mathbf{x} \cdot_U \mathbf{y} &= \sum_{k=1}^{m}\sum_{i=1}^{m}\sum_{j=1}^{m}\sum_{w=1}^{m} c_{k,w}x_i y_j t_{i,j,w} = \sum_{w=1}^{m}\left(\sum_{i,j,k=1}^{m} x_i y_j t_{i,j,w}\right) c_{k,w} \\ &= \sum_{w=1}^{m}\left(\sum_{i,j,k=1}^{m} x_i y_j t_{i,j,k}\mathbf{e}_k\right) c_{k,w} = \mathbf{v}C^{\intercal} = (\mathbf{x} \cdot_T \mathbf{y})C^{\intercal}.\end{aligned}$$

接下来，我们将分析两个同位的三阶张量 U 和 T 所对应的 $\mathcal{C} = \mathcal{H}_T^{\perp}$ 与 $\mathcal{D} = \mathcal{H}_U^{\perp}$ 之间的关系。我们从展开码 $\mathcal{H}_T = \langle T_{*,\,*,\,j}H_i \mid (i,j) \in [n-k]\times[m]\rangle_{\mathbb{F}_q}$ 和 $\mathcal{H}_U = \langle U_{*,\,*,\,j}H_i \mid (i,j) \in [n-k]\times[m]\rangle_{\mathbb{F}_q}$ 入手。我们希望研究当 $U(\mathbf{x}, \mathbf{y}, \mathbf{z}) = T(\mathbf{x}A, \mathbf{y}B, \mathbf{z}C)$ 时，这两个码之间的关系。

在较简单的情况下，U 与 T 之间的关系属于$U(\mathbf{x}, \mathbf{y}, \mathbf{z}) = T(\mathbf{x}, \mathbf{y}, \mathbf{z}C)$ 这一类型，方程 (2) 变为

$$u_{i,j,k} = \sum_{w=1}^{m} t_{i,j,w}c_{k,w}.$$

这意味着 $U_{*,*,k} = \sum_{w=1}^{m} T_{*,*,w} c_{k,w}$，基本上我们可以将每个切片$U_{*,*,k}$ 表示为$T_{*,*,w}$的线性组合。由于根据假设 C 是可逆的，我们有

$$\mathcal{U}_3 = \langle U_{*,*,k} \mid k \in [m] \rangle_{\mathbb{F}_q} = \langle T_{*,*,k} \mid k \in [m] \rangle_{\mathbb{F}_q} = \mathcal{T}_3.$$

因此我们有 $\mathcal{H}_T = \mathcal{H}_U$，这意味着 $\mathcal{C} = \mathcal{D}.$。由于任意选择的可逆 C 都会得到相同的码，因此一般情况下我们总可以考虑 $C = I_m$。接下来只需考察当 $U(\mathrm{x}, \mathrm{y}, \mathrm{z}) = T(\mathrm{x}A, \mathrm{y}B, \mathrm{z})$ 时会发生什么。在这种情况下，我们有 $U_{*,\ *,\ k} = AT_{*,\ *,\ k}B^{\intercal}$，于是 $\mathcal{H}_U = A(B^{\intercal}\mathcal{H})_T$。由于 A 可逆，我们可以得出结论：

$$\mathcal{H}_U \cong (B^{\intercal}\mathcal{H})_T \tag{4}$$

对于两个张量 $U(\mathrm{x}, \mathrm{y}, \mathrm{z}) = T(\mathrm{x}A, B\mathrm{y}B, \mathrm{z}C)$。

注意，对于一个可逆矩阵 B，$\mathcal{H} \cong B^{\intercal}\mathcal{H}$。很容易由（4）得出结论：$\mathcal{H}_T \cong (B^{\intercal}\mathcal{H})_T \cong \mathcal{H}_U$。然而，第一个合同关系通常不成立。

注 1 使用相同三阶张量$T \in \mathbb{F}_q^{m \times m \times m}$对两个同构码进行扩展，通常并不同构。

例如，考虑 $H \in \mathbb{F}_q^{m \times n}$一个矩阵，使其所有列都属于 $T_{*,\ *,\ k}$ 的核，则 $T_{*,\ *,\ k}H = 0$ 但我们可以构造 $H' = AH$，使得 A 是一个可逆矩阵，并且 $T_{*,\ *,\ k}AH \neq 0.$ 码 $\mathcal{H} = \langle H \rangle_{\mathbb{F}_q}$ 和 $A\mathcal{H}$ 同构，但 $\mathcal{H}_T$ 的维数至多为 $m-1$，而 $(A\mathcal{H})_T$ 的维数最多可达 m。

作为本节的总结，在某些情况下，对于某些可逆矩阵 B，两个同位张量$U(\mathrm{x}, \mathrm{y}, \mathrm{z}) = T(\mathrm{x}A, \mathrm{y}B, \mathrm{z}C)$对应的码 $\mathcal{C} = \mathcal{H}_T^{\perp}$和 $\mathcal{D} = \mathcal{H}_U^{\perp}$是同构的。这里给出这类可逆矩阵 B的两种选择。若 $B^{\intercal}$ 与所有 $T_{*,*,k}$都可交换，则有 $U_{*,*,\ k} = AB^{\intercal}T_{*,*,k}$，于是 $\mathcal{H}_U = AB^{\intercal}\mathcal{H}_T$；由于 $AB^{\intercal}$ 可逆，我们可以得出 $\mathcal{C} \cong \mathcal{D}$。使这两个码保持同构的第二种 B 选择是 $B^{\intercal}\mathcal{H} = \mathcal{H}$（对于 $B = I_m$，这是一个平凡情形）；在这种情况下，显然有 $\mathcal{H}_U \cong (B^{\intercal}\mathcal{H})_T = (I_m\mathcal{H})_T = \mathcal{H}_T.$。这同样意味着 $\mathcal{C} \cong \mathcal{D}.$

5 广义 LRPC 码的译码

本节将讨论广义 LRPC 码的译码。在特定条件下，LRPC 码所用的译码算法可以推广到广义版本。回顾一下，LRPC 码的译码算法可分为两个步骤。第一步旨在利用 $\langle H\mathbf{e}^{\intercal}\rangle_{\mathbb{F}_q} \subseteq \mathcal{H}.\mathcal{E}$ 这一事实来恢复乘积空间 $\mathcal{H}.\mathcal{E}$。第二步旨在从 $\mathcal{H}.\mathcal{E}$ 恢复错误支撑 $\mathcal{E}$，其形式为

$$\mathcal{E} \subseteq \bigcap_{i\in[d]} h_i^{-1}\mathcal{H}.\mathcal{E}$$

其中，h_1、……、h_d 是校验矩阵 $\mathcal{H}$ 的支撑的一组基。请注意，标准乘积在 $\mathbb{F}_{q^m}$ 上的可逆性仅用于 $\mathcal{H}$ 的基 h_1、h_2、……、h_d。

对于维数为 mk 的广义 LRPC 码 $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$，根据定义 17，存在一个码 $\mathcal{H} = \langle H_1、\ldots\ldots、 H_{n-k}\rangle_{\mathbb{F}_q}$，其中 $\mathrm{Colsp}(H_i) \subseteq \mathcal{B} = \langle \beta_1、\ldots\ldots、 \beta_d\rangle_{\mathbb{F}_q}$、$\forall i \in [n-k]$，以及一个三阶张量 $T \in \mathbb{F}_q^{m\times m\times m}$，使得 $(\mathcal{H}_T)^{\perp} = \mathcal{C}$。正如我们将看到的，广义 LRPC 码 $\mathcal{C}$ 的译码涉及讨论 $T_{*,\ \mathbf{b},\ *}$ 关于子空间 $\mathcal{B}$ 中元素 $\mathbf{b}$ 的可逆性。

下面我们首先讨论码 $\mathcal{C}$ 的一种基本译码方法，该方法要求$T_{*,\ \mathbf{b},\ *}$ 对某个 $\mathbf{b} \in \mathcal{B}$可逆。此方法直接受到 LRPC 码译码的启发。然后，我们研究一种不受此条件限制的改进译码方法。

5.1 基本译码

对于如上由子空间 $\mathcal{B}$ 和三阶张量 $T \in \mathbb{F}_q^{m\times m\times m}$构造的广义 LRPC 码 $\mathcal{C} = (\mathcal{H}_T)^{\perp}$，本小节将讨论在 $\mathcal{B}$ 和 T 满足以下条件时对 $\mathcal{C}$ 的译码：

条件 1 如果存在 $\mathcal{B}$ 的一个基 $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$，使得对于每个元素 $\mathbf{b}_j$，矩阵 $T_{*,\mathbf{b}_j,*} \in \mathbb{F}_q^{m\times m}$ 都可逆，则称子空间 $\mathcal{B}$ 与三阶张量 T 相容。

由命题 1 可知，当一个三阶张量 T 在 $\mathbb{F}_{q^m}$上定义了一个预半域结构时，换言之，当矩阵码 $\mathcal{T}_2$ 是一个维数为 m的最大秩距离码时，对于任意非零的 $\mathbf{b} \in \mathcal{B}$，矩阵 $T_{*,\mathbf{b},*}$ 都是可逆的。因此，$\mathbb{F}_q^{m\times m}$中任何维数为 $\mathbb{F}_q$的 m 维最大秩距离矩阵码都满足条件 1。显然，给定一个子空间 $\mathcal{B}$，满足条件 1 的张量集合 T 远大于维数为 m的 $\mathbb{F}_q^{m\times m}$中的最大秩距离码集合。

现在我们讨论译码过程。假设我们接收到消息$Y = C+E$，其中 $C \in \mathcal{C}$，且 $E \in \mathbb{F}_q^{m\times n}$是一个秩为低秩 r的矩阵。我们可以将译码过程分为两个步骤。在第一步中，我们将恢复 E的列支撑。一旦列支撑已知，我们就能够写出 $E = FX$，其中 $F \in \mathbb{F}_q^{m\times r}$满足 $\mathsf{Colsp}(F) = \mathsf{Colsp}(E) = \langle \mathbf{f}_1, \ldots\ldots, \mathbf{f}_r\rangle_{\mathbb{F}_q}$，且$X \in \mathbb{F}_q^{r\times n}$是一个包含 nr 个未知数的矩阵。在第二步中，我们将求解一个线性系统，以确定这些 nr 个未知数。

步骤 1 对于 $C \in \mathcal{C}$，根据定义可知 $C \cdot_T H_i = \mathbf{0}, \forall i \in [n-k]$。因此 $Y \cdot_T H_i = (C + E) \cdot_T H_i = E \cdot_T H_i = \mathbf{s}_i$。$E$ 的每一列都属于子空间 $\mathcal{E} = \langle \mathbf{f}_1, \ldots\ldots, \mathbf{f}_r\rangle_{\mathbb{F}_q}$，而 H_i 的每一列 $\mathbf{h}_{i,j}$ 都属于 $\mathcal{B} = \langle \mathbf{b}_1, \ldots\ldots, \mathbf{b}_d\rangle_{\mathbb{F}_q}$。我们用 $\mathbf{e}_j$ 表示 E 的第 j 列，用 $\mathbf{h}_{i,j}$ 表示 H_i 的第 j 列。由于 T-乘积是双线性的，根据定理 2 可得

$$\mathbf{s}_i = E \cdot_T H_i = \sum_{j\in[n]} \mathbf{e}_j \cdot_T \mathbf{h}_{i,j} \in \langle \mathcal{E} \cdot_T \mathcal{B}\rangle_{\mathbb{F}_q}, \forall i \in [n-k] \tag{5}$$

其中 $\dim(\langle \mathcal{E} \cdot_T \mathcal{B}\rangle_{\mathbb{F}_q}) \leq rd$. 令 $S = (\mathbf{s}_1, \ldots, \mathbf{s}_{n-k})$，我们将得到 $\mathsf{Colsp}(S) \subseteq \langle \mathcal{E} \cdot_T \mathcal{B}\rangle_{\mathbb{F}_q}$，当 $(n-k) \geq rd$ 时，该等式以较高的概率成立。

为了恢复 $\mathcal{E} = \mathsf{Colsp}(E)$，我们将利用条件 1，即存在一个 $\mathcal{B}$ 的基 $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$，使得其上的 T-乘积是可逆的。空间 $\langle \mathcal{E} \cdot_T \mathcal{B}\rangle_{\mathbb{F}_q}$ 可以表示为

$$\langle \mathcal{E} \cdot_T \mathcal{B}\rangle_{\mathbb{F}_q} = \langle \mathbf{f}_i \cdot_T \mathbf{b}_j\rangle_{\mathbb{F}_q} = \langle \mathbf{f}_i T_{*,\mathbf{b}_j,*} \mid (i,j) \in [r] \times [d]\rangle_{\mathbb{F}_q}.$$

在条件 1 下，对于所有 $\mathbf{b}$，我们有 $\mathcal{E} \subseteq \langle \mathcal{E} \cdot_T \mathcal{B}\rangle_{\mathbb{F}_q} (T_{*,\mathbf{b}_j,*})^{-1}$。利用这一事实，我们得到

$$\mathcal{E} \subseteq \bigcap_{j\in[d]} \langle \mathcal{E} \cdot_T \mathcal{B}\rangle_{\mathbb{F}_q} (T_{*,\mathbf{b}_j,*})^{-1}. \tag{6}$$

等式很可能成立，这样我们就能够恢复$\mathcal{E}$。我们在算法 1 中总结了上述过程。

算法 1：广义 LRPC 码的错误支撑恢复

输入：一个广义 LRPC 码 $\mathcal{C} = \mathcal{H}_T^{\perp}$，其张量为 $T \in \mathbb{F}_q^{m\times m\times m}$，并且
$\mathcal{H} = \langle H_1, \ldots, H_{n-k}\rangle_{\mathbb{F}_q}$，其中列空间$(H_i) \subseteq \mathcal{B} = \langle \mathbf{b}_1, \ldots, \mathbf{b}_d\rangle_{\mathbb{F}_q}, \forall i$。
一个矩阵 $Y = X + E \in \mathbb{F}_q^{m\times n}$ 与 $X \in \mathcal{C}$ 和 $E \in \mathbb{F}^{m\times n}$搭配 秩为 r。
输出：维数为 r 的支撑 $\mathcal{E}$ =列空间(E)。
// 假设：维数$(\mathcal{E}.\mathcal{B}) = rd$
// 条件：$T_{*,\ \mathbf{b}_j,\ *}$ 对于所有 $j \in [d]$ 均可逆
// 计算伴随式
$S = []$;
对 $i \in [n-k]$ 执行
  S.追加$(Y \cdot_T H[i])$;
结束
// 计算伴随式空间
$\mathcal{S} = \langle S\rangle_{\mathbb{F}_q}$;
如果 dim$(\mathcal{S}) == rd$ 那么
  // 计算交集
  $\mathcal{E} = \mathcal{S}(T_{*,\ \mathbf{b}_1,\ *})^{-1}$;
  对于 $\mathbf{b}_i \in \{\mathbf{b}_2 \ldots \mathbf{b}_d\}$，执行
    $\mathcal{E} = \mathcal{E} \cap \mathcal{S}(T_{*,\mathbf{b}_i,*})^{-1}$;
  end
  返回 $\mathcal{E}$;
// $\mathcal{S}$ 的维数太低
否则
  错误支撑恢复失败;
结束

步骤 2 假设第一步成功，我们得到了 $\mathbf{f}_1, \ldots, \mathbf{f}_r$，它们生成 $\mathcal{E}$。我们可以将它们收集在矩阵 $F = (\mathbf{f}_1, \ldots, \mathbf{f}_r) \in \mathbb{F}_q^{m\times r}$中，并将错误表示为 $E = FX$，其中 $X \in \mathbb{F}_q^{r\times n}$. 考虑 $\mathbf{s}_i = E \cdot_T H_i$，根据定义 15，其 j 个分量 $\mathbf{s}_{i,j} = \mathrm{Tr}(T_{*,*,}{}_j H_i E^{\intercal}) = \mathrm{Tr}(T_{*,*,j} H_i X^{\intercal} F^{\intercal})$。对于每个 $\mathbf{s}_{i,j}$，我们都会得到一个关于 X 中所含 nr 个变量的线性方程。总共有 $(n-k)m$ 个这样的线性方程，涉及 nr 个变量。事实证明，这些方程并非线性无关。与经典 LRPC 码一样，我们至多能得到 $(n-k)rd$ 个线性无关方程。该空间

$\langle \mathcal{E} \cdot_T \mathcal{B} \rangle_{\mathbb{F}_q}$ 由向量 $\mathbf{z}_{k,\ l} = \mathbf{f}_k \cdot_T \mathbf{b}_l = \mathbf{f}_k T_{*,\ \mathbf{b}_l,\ *} \in \mathbb{F}_q^m$生成，令 $Z = \{\mathbf{z}_{k,\ l} \mid (k,l) \in [r] \times [d]\}$ 表示该生成元集合。每个向量 $\mathbf{s}_i = E \cdot_T H_i \in \langle \mathcal{E} \cdot_T \mathcal{B} \rangle_{\mathbb{F}_q}$ 都可以表示为

$$\mathbf{s}_i = \sum_{k=1}^{r} \sum_{l=1}^{d} \eta_{i,k,l} \mathbf{z}_{k,l}, \tag{7}$$

其中 $\eta_{i,\ k,\ l} \in \mathbb{F}_q$ 是 $\mathbf{s}_i$ 相对于生成元集合Z的坐标。$\mathbf{s}_i$ 的另一种表示方式由校验方程给出:

$$\mathbf{s}_i = E \cdot_T H_i = \sum_{j=1}^{n} \mathbf{e}_j \cdot_T \mathbf{h}_{i,j} = \sum_{j=1}^{n} \mathbf{e}_j T_{*,\mathbf{h}_{i,j},*}, \tag{8}$$

其中 $\mathbf{e}_j$ 是 j列，$\mathbf{h}_{i,\ j}$ 是矩阵 H_i的 j列。我们有 $\mathbf{e}_j = \sum_{k=1}^{r} x_{k,\ j} \mathbf{f}_k$ 和 $\mathbf{h}_{i,\ j} = \sum_{l=1}^{d} \mu_{i,\ j,\ l} \mathbf{b}_l$，注意到 $T_{*,\ \mathbf{h}_{i,\ j,\ *},\ *} = \sum_{l=1}^{d} \mu_{i,\ j,\ l} T_{*,\ \mathbf{b}_l,\ *}$，将其代入式 (8) 得到

$$\mathbf{s}_i = \sum_{j=1}^{n} \sum_{k=1}^{r} \sum_{l=1}^{d} x_{k,j} \mu_{i,j,l} (\mathbf{f}_k T_{*,\mathbf{b}_l,*}) = \sum_{j=1}^{n} \sum_{k=1}^{r} \sum_{l=1}^{d} x_{k,j} \mu_{i,j,l} \mathbf{z}_{k,l}. \tag{9}$$

由 (7) 和 (9) 可得包含 $(n-k)rd$ 个方程的方程组

$$\sum_{j=1}^{n} x_{k,j} \mu_{i,j,l} = \eta_{i,k,l}, \quad (i,k,l) \in [n-k] \times [r] \times [d]. \tag{10}$$

最后，与经典 LRPC 码的情况一样，我们有 nr 个未知数和 $(n-k)rd$ 个方程。对于 $n \leq (n-k)d$，如果 (10) 中至少有 nr 个方程线性无关，那么该方程组有唯一解。如果方程组 (10) 只有 $nr - a$ 个线性无关的方程，该算法将给出一个包含 q^a 个可能解的列表。

5.2 成功概率

与经典 LRPC 码类似，广义 LRPC 码的译码算法不是确定性的。在步骤 1 中，我们有 $\mathrm{Colsp}(S) \subseteq \langle \mathcal{E} \cdot_T \mathcal{B} \rangle_{\mathbb{F}_q}$。空间 $\langle \mathcal{E} \cdot_T \mathcal{B} \rangle_{\mathbb{F}_q}$ 的维数上限为 rd。这种情况有可能发生

即使 $n-k \geq rd$，空间 Colsp(S) 也严格包含于 $\langle \mathcal{E} \cdot_T \mathcal{B} \rangle_{\mathbb{F}_q}$。从直观上看，我们可以假设 S 的列是从 $\langle \mathcal{E} \cdot_T \mathcal{B} \rangle_{\mathbb{F}_q}$ 中均匀采样得到的向量。在此假设下，均匀地从维数为 rd 的空间 $\langle \mathcal{E} \cdot_T \mathcal{B} \rangle_{\mathbb{F}_q}$ 中抽取元素组成大小为 $n-k \geq rd$ 的集合，该集合张成整个空间 $\langle \mathcal{E} \cdot_T \mathcal{B} \rangle_{\mathbb{F}_q}$ 的概率为 [24]。

$$P(\mathrm{Colsp}(S) = \langle \mathcal{E} \cdot_T \mathcal{B} \rangle_{\mathbb{F}_q}) = 1 - q^{rd-(n-k)}.$$

注意，在 dim($\langle \mathcal{E} \cdot_T \mathcal{B} \rangle_{\mathbb{F}_q}$) $= s < rd$ 的情况下，该概率会提高至 $1-q^{s-(n-k)}$。假设 dim($\langle \mathcal{E} \cdot_T \mathcal{B} \rangle_{\mathbb{F}_q}$) $= rd$ 是最坏情况。

与经典 LRPC 码类似，步骤 1 失败的第二个原因由 $\langle \mathcal{E} \cdot_T \mathcal{B} \rangle_{\mathbb{F}_q}(T_{*,\mathbf{b}_i,*})^{-1}$ 不等于 $\mathcal{E}$ 时交集的概率给出。这个概率可以近似为以下概率：d 个维数为 rd 的子空间 $\mathcal{R}_1$、...、$\mathcal{R}_d \subseteq \mathbb{F}_q^m$，每个都包含同一个维数为 r 的子空间 $\mathcal{E}$，其交集大于 $\mathcal{E}$。假设$\mathcal{R}_1$、...、$\mathcal{R}_d$是独立随机选取的，则它们的交集大于 $\mathcal{E}$ 的概率为 $q^{-(d-1)(m-rd-r)}$ [21]。考虑到这两个可能的失败原因，步骤 1 的成功概率下界为 $1-(q^{rd-(n-k)} + q^{-(d-1)(m-rd-r)})$。注意，在 $\mathcal{E} \subsetneq \bigcap_{i\in[d]} \langle \mathcal{E} \cdot_T \mathcal{B} \rangle_{\mathbb{F}_q}(T_{*,\mathbf{b}_i,*})^{-1}$的情况下，在某些情形下仍有可能唯一纠正错误。设 $r < r' = \dim\left(\bigcap_{i\in[d]} \langle \mathcal{E} \cdot_T \mathcal{B} \rangle_{\mathbb{F}_q}(T_{*,\mathbf{b}_i,*})^{-1}\right)$，步骤 2 中的线性系统将具有 nr' 个未知数和 $(n-k)rd$ 个方程。如果$nr' \leq (n-k)rd$，仍有可能唯一恢复正确的错误。

5.3 改进译码

在第 5.1 节中，我们讨论了子空间 $\mathcal{B}$ 和三阶张量 T 相容时广义 LRPC 码的译码，其译码过程与 LRPC 码的类似。事实上，即使 $\mathcal{B}$ 和 T 不相容，广义 LRPC 码仍然可以高效译码。下面我们将研究这种情况下广义 LRPC 码的译码。这使我们能够随机选择子空间 $\mathcal{B}$ 和三阶张量T。为了保持大致相同的译码成功概率，我们可能需要付出一定代价，即略微增大 m 至 $m+3$。

假设广义 LRPC 码 $\mathcal{C} = (\mathcal{H}_T)^{\perp}$ 由定义 17 中的维数为 d 的子空间$\mathcal{B}$ 和三阶张量 $T \in \mathbb{F}_q^{m\times m\times m}$构造，其中 $\mathcal{B}$ 和T 不相容；并假设 E 是一个错误矩阵，其列支撑为低维的$\mathcal{E} = \mathsf{Colsp}(E)$ r。在错误支撑恢复过程中，维数上界仍为rd的 $\mathsf{s}_i = E \cdot_T H_i \in \langle \mathcal{E} \cdot_T \mathcal{B}\rangle_{\mathbb{F}_q}$。令 $S = (\mathsf{s}1, \ldots, \mathsf{s}_{n-k})$，则有 $\mathcal{S} = \mathsf{Colsp}(S) \subseteq \langle \mathcal{E} \cdot_T \mathcal{B}\rangle_{\mathbb{F}_q}$. 如果 $(n-k) \geq rd$，那么以较高概率有 $\mathcal{S} = \langle \mathcal{E} \cdot_T \mathcal{B}\rangle_{\mathbb{F}_q}$。接下来，我们要利用 $\mathcal{B}$ 和 $\langle \mathcal{E} \cdot_T \mathcal{B}\rangle_{\mathbb{F}_q}$恢复 $\mathcal{E}$。我们知道，如果存在一个元素 $\mathsf{b} \in \mathcal{B}$ 使得 $T_{*,\mathbf{b},*}$ 可逆，那么 $\mathcal{E} \subseteq \langle \mathcal{E} \cdot_T \mathcal{B}\rangle_{\mathbb{F}_q}(T_{*,\mathbf{b},*})^{-1}$。然而，当子空间 $\mathcal{B}$ 和三阶张量不相容时，$T_{*,\mathcal{B},*}$中可能没有足够多的可逆元素。因此，使用第 5.1 节所述的基本译码，我们将无法恢复 $\mathcal{E}$。

在进行译码之前，我们需要介绍一些线性代数的结果。

引理 2. 设 T: $\mathbb{F}_q^m \to \mathbb{F}_q^m$是一个线性映射，令 $\mathsf{Im}(T)$、$\mathsf{ker}(T)$分别表示 T 的像和核。给定 $\mathbb{F}_q^m$的一个子空间 $\mathcal{A}$，其关于 T 的原像的维数为

$$\dim(T^{-1}(\mathcal{A})) = \dim(\ker(T)) + \dim(\mathcal{A} \cap \mathrm{Im}(T)).$$

证明. 首先注意到 $T^{-1}(\mathcal{A})) = T^{-1}(\mathcal{A} \cap \mathsf{Im}(T))$。根据第一同构定理，存在一个线性双射 T'，它在 $\mathbb{F}_q^m/\,\mathsf{ker}(T)$ 与 $\mathsf{Im}(T)$ 之间，其中 $\mathbb{F}_q^m/\,\mathsf{ker}(T)$ 是由等价关系 $\mathsf{v} \sim \mathsf{v} + \mathsf{z}$（其中 $\mathsf{z} \in \mathsf{ker}(T)$）得到的商空间。

$$\begin{array}{ccc} \mathbb{F}_q^m & \xrightarrow{\ T\ } & \mathrm{Im}(T) \\ {\scriptstyle \pi}\downarrow & \nearrow_{T'} & \\ \mathbb{F}_q^m/\ker(T) & & \end{array}$$

设 $[\mathcal{V}]$ 是 $\mathbb{F}_q^m/\,\mathsf{ker}(T)$ 中维数为 $\mathsf{dim}(\mathcal{A} \cap \mathsf{Im}(T))$ 的唯一子空间，使得 $T'([\mathcal{V}]) = \mathcal{A} \cap \mathsf{Im}(T)$。其唯一性由 T' 是双射这一事实保证。空间 $[\mathcal{V}]$ 对应于等价类 $\mathcal{V} + \mathsf{ker}(T)$,

特别地，我们有 $T(\mathcal{V}+\ker(T)) = T'\circ\pi(\mathcal{V}+\ker(T)) = T'([\mathcal{V}]) = \mathcal{A}\cap \mathrm{Im}(T)$。$T^{-1}(\mathcal{A})$ 中没有其他元素。设 $\mathbf{x}\notin\mathcal{V}+\ker(T)$，则 $T(\mathbf{x}) = T'(\pi(\mathbf{x})) = T'([\mathbf{x}])\notin\mathcal{A}\cap\mathrm{Im}(T)$。□

引理3. 设 $\mathcal{V}=\langle \mathbf{v}_1,\ldots,\mathbf{v}_k\rangle_{\mathbb{F}_q}\subseteq\mathbb{F}_q^m$，并令 T 为线性映射。我们有 $T^{-1}(T(\mathcal{V})) = \mathcal{V}+$ 核 (T) 】【。

证明。在不失一般性的情况下，我们有 $\mathcal{V}=\mathcal{V}'\oplus(\mathcal{V}\cap$ 核$(T))$，其中$\oplus$ 表示直和。根据第一同构定理，我们有 $T(\mathcal{V})$ 与 $[\mathcal{V}]=[\mathcal{V}']\in\mathbb{F}_q^m/$ 核(T) 通过同构T'同构。按照引理 2 的证明，我们有 $T'^{-1}(T(\mathcal{V})) = [\mathcal{V}']$。由此可得 $T^{-1}(T(\mathcal{V})) = \mathcal{V}'+$ 核$(T) = \mathcal{V}+$ 核(T). □

假设 $\mathcal{S}=$列空间$(S) = \langle\mathcal{E}\cdot_T\mathcal{B}\rangle_{\mathbb{F}_q}$，并考虑 Rank$(T_{*,\mathbf{b},*}) = m-a$ 对某个 $\mathbf{b}\in\mathcal{B}$ 的情况。由于 $T_{*,\mathbf{b},*}$ 不可逆，我们无法直接计算空间 $\mathcal{S}(T_{*,\mathbf{b},*})^{-1}$。克服这一问题的一种方法是考虑函数$T_{\mathbf{b}}(\mathbf{x}) = \mathbf{x}T_{*,\mathbf{b},*}$。根据引理 2 的证明，逆像

$$T_{\mathbf{b}}^{-1}(\mathcal{S}) = \{\mathbf{x}\in\mathbb{F}_q^m \mid \mathbf{x}T_{*,\mathbf{b},*}\in\mathcal{S}\} = \mathcal{V}+\ker(T)$$

是一个维数为 $\dim(T^{-1}{}_{\mathbf{b}}(\mathcal{S})) = \dim(\mathcal{S}\cap T_{\mathbf{b}}(\mathbb{F}_q^m)) + \ker(T_{\mathbf{b}}) \le rd+a.$ 的空间

注意，$T_{\mathbf{b}}(\mathcal{E})\subseteq\mathcal{S}$那么 $T^{-1}{}_{\mathbf{b}}(T_{\mathbf{b}}(\mathcal{E}))\subseteq T^{-1}{}_{\mathbf{b}}(\mathcal{S})$。由引理3可知，$T^{-1}{}_{\mathbf{b}}(T_{\mathbf{b}}(\mathcal{E})) = \mathcal{E}+\ker(T_{\mathbf{b}})$，特别是 $\mathcal{E}\subseteq\mathcal{E}+\ker(T_{\mathbf{b}})\subseteq T^{-1}{}_{\mathbf{b}}(\mathcal{S})$。以较高概率对不同的 $\mathbf{b}_i$ 对应的 $T^{-1}{}_{\mathbf{b}_i}(\mathcal{S})$ 求交，将恰好得到空间 $\mathcal{E}$，或一个包含 $\mathcal{E}$ 的较小子空间。

恢复错误支撑后，我们可以像使用前一个算法那样继续进行。

要实现这个新算法，我们需要求出 $T^{-1}\ \mathbf{b}_i\ (\mathcal{S})$。考虑函数 $T_{\mathbf{b}_i}(\mathbf{x}) = \mathbf{x}T_{*,\mathbf{b}_i,*}$，首先计算核 $\ker(T_{\mathbf{b}_i})$ 和像 $\hat{}\ \mathrm{Im}(T_{\mathbf{b}_i})$。设 $\dim(\ker(T_{\mathbf{b}_i})) = a$，并令 $\mathcal{S} = \mathcal{S}\cap\mathrm{Im}(T_{\mathbf{b}_i})$，根据引理 2，我们知道 $\dim(T^{-1}\,\mathbf{b}_i\,(\mathcal{S})) \le \dim(\hat{}\mathcal{S}) + a.$ 对于 $\hat{}$ 的所有基元素 $\mathbf{s}1,\ldots,\mathbf{s}_k$，都可以找到 $\mathbf{x}j$，使得 $T_{\mathbf{b}_i}(\mathbf{x}j) = \mathbf{s}j\cdot$。根据 $\hat{}$ 的构造，我们有 T 是 $\langle\mathbf{x}1,\ldots,\mathbf{x}_k\rangle_{\mathbb{F}_q}$ 与 $\mathcal{S}$ 之间的一个同构，而 $T^{-1}\ \mathbf{b}_i(\mathcal{S}) = \langle\mathbf{x}1,\ldots,\mathbf{x}_k\rangle_{\mathbb{F}_q}+\ker(T_{\mathbf{b}_i})$。

算法 2：广义 LRPC 的改进错误支撑恢复码

一个广义 LRPC 码 $\mathcal{C} = \mathcal{H}_T^{\perp}$，带有张量 $T \in \mathbb{F}_q^{m \times m \times m}$和
$\mathcal{H} = \langle H_1$、……、$H_{n-k} \rangle_{\mathbb{F}_q}$，其中列空间$(H_i) \subseteq \mathcal{B} = \langle \mathbf{b}_1$、……、$\mathbf{b}_d \rangle_{\mathbb{F}_q}$、$\forall i$。
一个矩阵 $Y = X + E \in \mathbb{F}_q^{m \times n}$ 与 $X \in \mathcal{C}$ 和 $E \in \mathbb{F}^{m \times n}_q$ 秩为 r。
输出：维数为 r的支撑 $\mathcal{E}$ =列空间(E)。
// 假设：dim$(\mathcal{E}.\mathcal{B}) = rd$
// 计算伴随式
$S = []$;
对于 $i \in [n-k]$ 执行
  S.append$(Y \cdot_T H[i])$;
结束
// 计算伴随式空间
$\mathcal{S} = \langle S \rangle_{\mathbb{F}_q}$;
若 dim$(\mathcal{S}) == rd$ 则
  // 计算待求交的子空间
  $Z = \{\}$;
  适用于 $i \in \{1, \ldots, d\}$ do
    $\mathcal{A} =$ Im$(T_{*,\ \mathbf{b}_i,\ *}) \cap \mathcal{S}$;
    // 计算 $\mathcal{A}$的逆像
    $Z_i = \{\mathbf{0}\}$;
    对于 $\mathbf{a}_j \in$基$(\mathcal{A})$，执行 do
      $Z_i = Z_i + \langle$Solve$(\mathbf{a}j)\rangle_{\mathbb{F}_q}$;
    end
    $Z_i = Z_i +$核$(T_{*,\mathbf{b}_d,*})$;
    Z.append(Z_i);
  end
  // 计算交集
  $\mathcal{E} = Z[1]$;
  for $i \in \{2 \ldots d\}$ do
    $\mathcal{E} = \mathcal{E} \cap Z[i]$;
  end
  返回 $\mathcal{E}$;
// $\mathcal{S}$ 的维数太低
否则
  错误支撑恢复失败;
结束

错误概率 $\mathcal{S} = \langle \mathcal{E} \cdot_T \mathcal{B} \rangle_{\mathbb{F}_q}$ 其中 $\mathcal{S} = \langle \mathbf{s}_1, \ldots \mathbf{s}_{n-k} \rangle_{\mathbb{F}_q}$ 的概率可估计为 $1 - q^{rd-(n-k)}$。为了恢复正确的错误支撑，我们需要满足的第二个条件是，子空间 $d$spaces $T^{-1}{}_{\mathbf{b}_i}(\mathcal{S})$ 的交集恰好为 $\mathcal{E}$。我们知道 $\mathcal{E} \subseteq T^{-1}{}_{\mathbf{b}_i}(\mathcal{S})$，更准确地说，我们有 $\mathcal{E} + \ker(T_{*,\mathbf{b}_i,*}) \subseteq T^{-1}{}_{\mathbf{b}_i}(\mathcal{S})$，因此

$$\mathcal{E} + \bigcap_{i=1}^{d} \ker(T_{*,\mathbf{b}_i,*}) \subseteq \bigcap_{i=1}^{d} T_{\mathbf{b}_i}^{-1}(\mathcal{S}).$$

如果我们以相互独立的方式从均匀分布中选取矩阵 $T_{*,\mathbf{b}_i,*}$，那么 $\cap_{i=1}^{d} \ker(T_{*,\mathbf{b}_i,*}) = 0$ 的可能性很大。与之前的算法相比，真正的变化在于，子空间 $T^{-1}{}_{\mathbf{b}_i}(\mathcal{S})$ 的维数 rd 并不都相同。以下命题估计了 $\dim(T^{-1}{}_{\mathbf{b}_i}(\mathcal{S}))$ 的取值分布。

命题3。假设 $\dim(\mathrm{Im}(T_{\mathbf{b}_i})) = a \geq rd$。那么我们有

$$\mathrm{P}(\dim(T_{\mathbf{b}_i}^{-1}(\mathcal{S})) = rd + \epsilon) = q^{-rd\epsilon} \begin{bmatrix} m-a \\ \epsilon \end{bmatrix}_q \alpha$$

其中 $\max\{0, m-a-rd\} \leq \epsilon \leq m-a$ 和 $\alpha = \prod_{i=0}^{t-1} \frac{1-q^{i-rd}}{1-q^{i-m}} \prod_{i=t}^{rd-1} \frac{1-q^{i-(a+t)}}{1-q^{i-m}}$ 趋近于 $H_q = \lim_{m\to\infty} \prod_{i=1}^{m}(1-q^{-i})$。

证明。从引理3可知，存在一个子空间 $\mathcal{A}$ 使得$T^{-1}{}_{\mathbf{b}_i}(\mathcal{S}) = \mathcal{A} +$ 核$(T_{*,\mathbf{b}_i,*})$，其中该和为直和。特别地，我们有 $\mathcal{A} \cong \mathcal{S} \cap \mathrm{Im}(T_{\mathbf{b}_i})$，于是

$$\dim(T_{\mathbf{b}_i}^{-1}(\mathcal{S})) = \dim(\mathcal{S} \cap \mathrm{Im}(T_{\mathbf{b}_i})) + \dim(\ker(T_{\mathbf{b}_i})). \tag{11}$$

注意，$\dim(\mathcal{S} \cap \mathrm{Im}(T_{\mathbf{b}_i})) = \dim(\mathcal{S}) + \dim(\mathrm{Im}(T_{\mathbf{b}_i})) - \dim(\mathcal{S} + \mathrm{Im}(T_{\mathbf{b}_i}))$。将此等式代入（11），得到

$$\begin{aligned} \dim(T_{\mathbf{b}_i}^{-1}(\mathcal{S})) &= \dim(\mathcal{S}) + \dim(\mathrm{Im}(T_{\mathbf{b}_i})) + \dim(\ker(T_{\mathbf{b}_i})) - \dim(\mathcal{S} + \mathrm{Im}(T_{\mathbf{b}_i})) \\ &= rd + m - \dim(\mathcal{S} + \mathrm{Im}(T_{\mathbf{b}_i})). \end{aligned}$$

对于子空间 $\mathcal{S}$ 和 $\mathrm{Im}(T_{\mathbf{b}_i})$，我们知道 $a = \dim(\mathrm{Im}(T_{\mathbf{b}_i})) \leq \dim(\mathcal{S} + \mathrm{Im}(T_{\mathbf{b}_i})) \leq m$。此外，$\dim(\mathcal{S} + \mathrm{Im}(T_{\mathbf{b}_i})) = a + t$ 的概率为，其中

$0 \le t \le m-a$，其形式如下（证明见附录中的命题 4）：

$$\frac{\prod_{i=0}^{t-1}(q^m - q^{a+i}) \prod_{i=0}^{rd-t-1}(q^a - q^i)}{\prod_{i=0}^{rd-1}(q^m - q^i)} \begin{bmatrix} rd \\ t \end{bmatrix}_q . \tag{12}$$

记为 $\epsilon = m-a-t$。那么，$\dim(T^{-1}{}_{\mathbf{b}_i}(\mathcal{S})) = rd+m-a-t = rd+\epsilon$ 的概率由式 (12) 给出，可改写为

$$q^{-rd(m-a-t)} \begin{bmatrix} m-a \\ t \end{bmatrix}_q \alpha\beta \tag{13}$$

其中 $\alpha = \prod_{i=0}^{t-1} \frac{q^m - q^{i+m-rd}}{q^m - q^i} = \prod_{i=0}^{t-1} \frac{1-q^{i-rd}}{1-q^{i-m}}$ 且 $\beta = \prod_{i=t}^{rd-1} \frac{q^m - q^{i+(m-a)-t}}{q^m - q^i} = \prod_{i=t}^{rd-1} \frac{1-q^{i-(a+t)}}{1-q^{i-m}}$.

□

注意，对于随机三阶张量 $T \in \mathbb{F}_q^{m\times m\times m}$，以高概率，$\mathrm{Im}(T_{\mathbf{b}_i})$ 的维数 a 接近 m，这表明在大多数情况下，对于 $d \ge 2$， $a + rd \ge m$。根据命题3，我们有

$$\begin{aligned} \mathrm{P}(\dim(T_{\mathbf{b}_i}^{-1}(\mathcal{S})) = rd) &\approx 1 - q^{-(a+rd-m)}/(q-1) \\ \mathrm{P}(\dim(T_{\mathbf{b}_i}^{-1}(\mathcal{S})) = rd+1) &\approx (1 - q^{-(a+rd+2-m)})q^{-(a+rd-m)}/(q-1) \end{aligned}$$

这些是 $T^{-1}{}_{\mathbf{b}_i}(\mathcal{S})$ 的维数所有可能取值中的主导情形。因此，即使 $\ker(T_{\mathbf{b}_i})$ 的维数 $m-a$ 非零，我们也可以假设 $T^{-1}{}_{\mathbf{b}_i}(\mathcal{S})$ 的维数为 rd 或甚至为 $rd+1$。

基于这一考虑，对于随机三阶张量 T，认为所有原像 $T^{-1}{}_{\mathbf{b}_i}(\mathcal{S})$ 的维数都是 $rd+1$，几乎是最坏的情况。一些矩阵 $T_{\mathbf{b}_i}$ 可逆，这意味着 $T^{-1}{}_{\mathbf{b}_i}(\mathcal{S})$ 的维数为 rd。当 $T_{\mathbf{b}_i}$ 不可逆时，正如上文所述， $T^{-1}{}_{\mathbf{b}_i}(\mathcal{S})$ 的维数为 rd 或 $rd+1$ 的情况将占主导，尤其是在 $rd - \dim(\ker(T_{\mathbf{b}_i})) = rd-(m-a) \gg 0$ 或 q取较大值时。

文献 [21] 表明， d 个都包含同一维数为 r的子空间的独立子空间，其交集的维数严格大于 r 的概率估计为 $q^{-(d-1)(m-rd-r)}$。将同样的估计用于维数为 $rd+t$的 d个子空间，而非 rd，可得估计值 $q^{-(d-1)(m-rd-r)+dt}$，其中 $t=0$，1。为了获得与算法 1 中大致相同的概率，在算法 2 中，我们需要将 m 的值增至 $m+1$ 或 $m+2$ （对于 $d=2$）；这样做的好处是，我们可以去掉子空间 $\mathcal{B}$ 与三阶张量 T 必须兼容的限制。

6 结论

这项工作的贡献有两方面。首先，我们提出了一种基于 $\mathbb{F}_q^{m\times m\times m}$ 中三阶张量、定义在 $\mathbb{F}_q^m$ 上的双线性乘积，并利用它将维数从 k 扩展到 km 的 $\mathbb{F}_q$ 线性矩阵秩度量码。这种扩展是传统 $\mathbb{F}_{q^m}$ 线性码生成方式的一种推广；传统方式是取 $\mathbb{F}_{q^m}$ 上满秩生成矩阵各行的 $\mathbb{F}_{q^m}$ 线性张成。其次，我们利用扩展的思想推导出 $\mathbb{F}_q$ 线性广义 LRPC 码，这类码支持概率多项式时间译码。由于与 MiniRank 问题有着密切联系，所提出的 $\mathbb{F}_q$ 线性 LRPC 码在密码学应用中具有重要意义，值得进行谨慎而全面的研究，这也将是我们未来工作的重点。

参考文献

1. N. Aragon、O. Blazy、P. Gaborit、A. Hauteville 和 G. Z´emor。 *Durandal: A Rank Metric BasedSignature Scheme*，第 728–758 页。施普林格，2019 年 04 月。2. M. Bardet、P. Briaud、M. Bros、P. Gaborit、V. Neiger、O. Ruatta 和 J.-P. Tillich。针对基于秩度量码的密码系统的代数攻击，2019 年 10 月。3. M. Bardet、M. Bros、D. Cabarcas、P. Gaborit、R. Perlner、D. Smith、J.-P. Tillich 和 J. Verbel。 *Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank Problems*，第 507–536 页。施普林格，2020 年 12 月。4. M. Bardet、M. Bros、D. Cabarcas、P. Gaborit、R. Perlner、D. Smith-Tone、J.-P. Tillich 和 J. Verbel。无需 Gröbner 基即可求解秩译码和 MinRank 问题的代数攻击。 *arXiv preprint arXiv:2002.08322*，2020 年。5. H. Bartz、L. Holzbaur、H. Liu、S. Puchinger、J. Renner 和 A. Wachter-Zeh。秩度量码及其应用，2022 年。

6. N. T. Courtois. 基于线性代数问题 minrank 的高效零知识身份认证。载于 C. Boyd（编），*Advances in Cryptology — ASIACRYPT 2001*，第 402–421 页，柏林、海德堡，2001 年。施普林格柏林海德堡出版社。 7. J. Cruz、M. Kiermaier、A. Wassermann 和 W. Willems。最大秩距离码的代数结构。*Advances in Mathematics of Communications*，10，2015 年 1 月。 8. P. Delsarte。有限域上的双线性形式及其在编码理论中的应用。 *Journal ofCombinatorial Theory*， *Series A*，25(3):226–241，1978 年。 9. E. Gabidulin。 *Rank Codes*。TUM 大学出版社，2021 年。 10. E. M. Gabidulin。最大秩距离码理论。 *Problemy Peredachi Infor-matsii*，21(1):3–16，1985 年。 11. E. M. Gabidulin、A. V. Paramonov 和 O. V. Tretjakov。非交换环上的理想及其在密码学中的应用。载于 D. W. Davies（编）， *Advances in Cryptology –EUROCRYPT'91*，第 482–489 页。施普林格，1991 年。 12. P. Gaborit、A. Hauteville、D. H. Phan 和 J.-P. Tillich。基于秩度量码的基于身份的加密。载于 J. Katz 和 H. Shacham（编）， *Advances in Cryptology – CRYPTO*2017，第 194–224 页。施普林格国际出版公司，2017 年。 13. P. Gaborit、O. Ruatta、J. Schrek 和 G. Z´emor。RankSign：一种基于秩度量的高效签名算法。载于 M. Mosca（编），*Post-Quantum Cryptography*，第 88–107 页。施普林格国际出版公司，2014 年。 14. P. Gaborit 和 G. Z´emor。秩码译码问题和最小距离问题的困难性。 *IEEE Transactions on Information Theory*，62(12):7245–7252，2016 年。 15. E. Gorla 和 A. Ravagnani。赋有秩度量的码。 *CoRR*，abs/1710.02067，2017 年。 16. A. Hauteville。基于 LRPC 码的加密系统的秩度量译码及攻击。技术报告，INRIA，2014 年 3 月。inria-01755842。 17. D. E. Knuth。有限半域与射影平面。*Journal of Algebra*，2(2):182–217，1965 年。 18. R. Koetter 和 F. R. Kschischang。随机网络编码中的错误与擦除纠正编码。*IEEE Transactions on Information Theory*，54(8):3579–3591，2008 年。 19. R. Lidl 和 H. Niederreiter。 *Finite Fields*。剑桥大学出版社，1997 年。 20. P. Loidreau。一种用于 Gabidulin 码译码的 Welch–Berlekamp 类算法。载于 Ø. Ytrehus（编），*International Workshop on Coding and Cryptography (WCC)*，第 36–45 页，柏林、海德堡，2006 年。施普林格。 21. C. A. Melchor、N. Aragon、M. Bardet、S. Bettaieb、L. Bidoux、O. Blazy、J.-C. Deneuville、P. Gaborit、A. Hauteville、A. Otmani、O. Ruatta、J.-P. Tillich 和 G. Z´emor。ROLLO（Rank-Ouroboros、LAKE 和 LOCKER 的合并项目）。载于 *Second round submission to the NIST post-quantum cryptography call*，2020 年 4 月。 22. A. V. Ourivski 和 T. Johansson。秩度量码译码的新技术及其在密码学中的应用。 *Probl. Inf. Transm.*，38(3):237–246，2002 年。 23. R. Overbeck。基于 Gabidulin 码的公钥密码系统的结构性攻击。*Journalof Cryptology*，21:280–301，2008 年 4 月。 24. Philippe Gaborit、Ga´etan Murat、Olivier Ruatta 和 Gilles Z´emor。低秩奇偶校验码及其在密码学中的应用。载于 2013 年编码与密码学研讨会（WCC'2013）论文集，挪威卑尔根，2013 年。可在 www.selmer.uib.no/wcc2013/pdfs/gaborit.pdf 获取。

25. G. P´olya. 关于某些格点多边形的数量。 *Journal of Combinatorial Theory*, 6(1):102–105, 1969年。26. R. M. Roth. 最大秩阵列码及其在交叉错误纠正中的应用。
IEEE Transactions on Information Theory, 37(2):328–336, 1991年。27. A. Wachter-Zeh、V. Afanassiev 和 V. Sidorenko. Gabidulin 码的快速译码。 *Designs, Codes and Cryptography*, 66(1-3):57–73, 2013年。

A 附录

我们将展示如何计算两个子空间之和的维数的概率。若考虑两个子空间 $\mathcal{A}$, $\mathcal{B} \subseteq \mathbb{F}_q^m$, 则

$$\dim(\mathcal{A}+\mathcal{B}) = \dim(\mathcal{A}) + \dim(\mathcal{B}) - \dim(\mathcal{A}\cap\mathcal{B}).$$

假设 $\dim(\mathcal{A}) = a$, $\dim(\mathcal{B}) = b$ 且 $\dim(\mathcal{A}\cap\mathcal{B}) = t'$, 若定义 $t = b - t'$, 则有

$$P(\dim(\mathcal{A}+\mathcal{B}) = a+t) = P(\dim(\mathcal{A}\cap\mathcal{B}) = t' = b-t).$$

已有一个公式 [16] 可以计算第二个概率。我们将给出另一种证明，并由此得到一个等价公式。在继续之前，我们需要一个关于高斯系数另一种解释的预备结果。以下引理的证明参见 [25]。

引理4. 高斯系数定义如下

$$\begin{bmatrix} m \\ r \end{bmatrix}_q = \prod_{i=0}^{r-1} \frac{q^m - q^i}{q^r - q^i} = \sum_{\alpha=0}^{r(m-r)} N_{m,r,\alpha} q^\alpha.$$

考虑一个由 m 条竖线和 r 条横线构成的 $m \times r$ 网格有向图，见图 2。将这些线的交点视为顶点，将连接它们且方向从左到右或从下到上的线段视为边。我们可以用 (i, j) 标记第 i 条竖线与第 j 条横线交点处的顶点，该顶点与 $(i+1, j)$ 和 $(i, j+1)$ 相连。从顶点 $(1, 1)$ 到顶点 (m, r)，且路径下方的面积（路径下方方格的数量）为 α 的可能路径数对应于 $N_{m,\ r,\ \alpha}$。

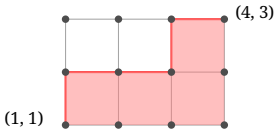


图 2：路径面积

命题 4。设 $\mathcal{A}$、$\mathcal{B} \subseteq \mathbb{F}_q^m$ 是两个子空间，其维数分别为 $\dim(\mathcal{A}) = a$ 和 $\dim(\mathcal{B}) = b$。考虑 $a \geq b$，则概率 $P(\dim(\mathcal{A}+\mathcal{B}) = a+t)$ 可表示为

$$\frac{\prod_{i=0}^{t-1}(q^m - q^{a+i}) \prod_{i=0}^{b-t-1}(q^a - q^i)}{\prod_{i=0}^{b-1}(q^m - q^i)} \begin{bmatrix} b \\ t \end{bmatrix}_q . \tag{14}$$

证明。设 $(\boldsymbol{\alpha}_1, \ldots \boldsymbol{\alpha}_a)$ 是 $\mathcal{A}$ 的一组基，$(\boldsymbol{\beta}_1, \ldots \boldsymbol{\beta}_b)$ 是 $\mathcal{B}$ 的一组基，并考虑矩阵 $A = (\boldsymbol{\alpha}_1^\intercal, \ldots \boldsymbol{\alpha}_a^\intercal)$ 和 $B = (\boldsymbol{\beta}_1^\intercal, \ldots \boldsymbol{\beta}_b^\intercal)$。我们有 $\dim(\mathcal{A}+\mathcal{B}) = \mathrm{w_R}(A \mid B)$。估计 $\mathrm{w_R}(A \mid B)$ 的一种方法如下。考虑矩阵序列 $A_0, \ldots, A_b$，其中 $A_0 = A$ 和 A_i 递归定义为 $A_i = (A_{i-1} \mid \boldsymbol{\beta}_i^\intercal)$。我们有 $A_b = \mathrm{w_R}(A \mid B)$，并且对于序列中的所有 i，$\mathrm{w_R}(A_i) \leq \mathrm{w_R}(A_{i+1}) \leq \mathrm{w_R}(A_i) + 1$。为简化记号，我们将 $\mathrm{Colsp}(A_i)$ 记为 $\mathcal{A}_i$。每次我们从 B 向 A 添加一列时，维数要么增加 1，要么保持与上一步相同。图 3 展示了这种情况，其中坐标为 (i, j) 的节点对应于数对 $(\mathcal{A}_i, j)$，而节点之间的线段表示可能的转移。具体来说，我们用红线表示一条从 $(\mathcal{A}_0, a)$ 到 $(\mathcal{A}_4, a+2)$ 的路径，该路径经过 $(\mathcal{A}_1, a+1)$、$(\mathcal{A}_2, a+1)$ 和 $(\mathcal{A}_3, a+2)$。

我们将 $P_{(a+v)\,i+1}$ 称为概率 $P(\dim(\mathcal{A}_{i+1}) = \dim(\mathcal{A}_i) \mid \dim(\mathcal{A}_i) = a+v)$，即已知 $\dim(\mathcal{A}_i) = a+v$ 的条件下，$\dim(\mathcal{A}_{i+1}) = \dim(\mathcal{A}_i) + 1$ 的概率，该概率由 $1 - P_i^{(a+v)}$ 给出。维数不会增加的概率，等于 $\boldsymbol{\beta}_{i+1}^\intercal \in \mathcal{A}_i$ 的概率。由于 $\boldsymbol{\beta}_1$、……、$\boldsymbol{\beta}_b$ 线性无关，且 $\langle \boldsymbol{\beta}_1$、……、$\boldsymbol{\beta}_i \rangle_{\mathbb{F}_q} \subseteq \mathcal{A}_i$，因此有 $q^{a+t} - q^i$ 种可能的

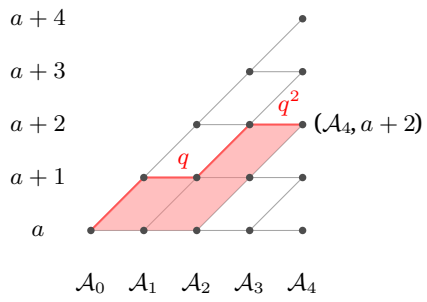


图 3： $\mathcal{A}_i$的维数

$\boldsymbol{\beta}_{i+1}$使得 $\boldsymbol{\beta}_{i+1} \in \mathcal{A}_i$且 $\boldsymbol{\beta}_{i+1} \notin \langle \boldsymbol{\beta}_1$、……、$\boldsymbol{\beta}_i \rangle_{\mathbb{F}_q}$。而满足 $\boldsymbol{\beta}_{i+1} \notin \langle \boldsymbol{\beta}_1$、……、$\boldsymbol{\beta}_i \rangle_{\mathbb{F}_q}$的 $\boldsymbol{\beta}_{i+1} \in Fq^m$的数量为 $q^m - q^i$.。由此得到转移概率

$$P_{i+1}^{(a+v)} = \frac{q^{a+v} - q^i}{q^m - q^i}, \quad 1 - P_{i+1}^{(a+v)} = \frac{q^m - q^{a+v}}{q^m - q^i}. \tag{15}$$

请注意， $P_{a+1}^{(a)} = 0$反映了这样一个事实：在维数为 a的空间中，我们已经添加了 a个线性无关向量后，如果维数仍为 a，再添加一个线性无关向量必然会使总维数增加 1。我们还知道， $1 - P_i^{(m)} = 0$ 反映了这样一个事实：一旦 $\mathcal{A}_{i-1}$ 达到满维数 m， $\mathcal{A}_i$ 的维数就无法继续增长。

在图 3 中，节点表示每个 $\mathcal{A}_i$可能的维数。例如，我们知道 $\dim(\mathcal{A}_0)$ 必须为 a ，而 $\dim(\mathcal{A}_i)$ 可以是 a 到 $\min(a+i, m)$ 之间的任意值。要计算在维数为 a 的空间中添加 b 个线性无关向量后，得到维数为 $a+t$的空间的概率，可以将从节点 $(\mathcal{A}_0, a)$ 到 $(\mathcal{A}_b, a+t)$ 的所有可能路径按其概率加权后求和。

我们可以将式（15）中的转移概率改写为

$$P_{i+1}^{(a+v)} = \frac{x_{a+v,i}}{z_i}, \quad 1 - P_{i+1}^{(a+v)} = \frac{y_{a+v}}{z_i} \tag{16}$$

其中 $x_{a+v,i} = q^{a+v} - q^i$、 $y_{a+v} = q^m - q^{a+v}$ 和 $z_i = q^m - q^i$。特定路径的概率将由各次转移概率的乘积给出。所有路径

将具有相同的长度 b，无论我们选择哪条路径，始终都会有$\prod_{i=0}^{b-1} z_i$ 作为分母。每条路径都包含 t 个维数增加的步骤，以及 $b-t$ 个维数保持不变的步骤。由于概率 y_{a+v} 不依赖于 i，因此每条路径的概率都会包含一个因子 $\prod_{v=0}^{t-1} y_{a+v}$。最后，注意到 $x_{a+v,i} = qx_{a+v+1,i+1}$，因此每条路径都会具有相同的因子 $\prod_{i=0}^{b-t-1} x_{a,i}$，以及另一个因子$q^{f_p}$，其中 f_p 是一个取决于路径的整数。总而言之，任何一条从 $(\mathcal{A}_0, a)$ 到 $(\mathcal{A}_b, a+t)$ 的路径 p，其概率都可以表示为

$$P(p) = \frac{\prod_{v=0}^{t-1} y_{a+v} \prod_{i=0}^{b-t-1} x_{a,i}}{\prod_{i=0}^{b-1} z_i} q^{f_p} = Q(a,b,t) q^{f_p}. \tag{17}$$

指数 f_p 是唯一取决于路径的参数，因为 $x_{a+v,i} = qx_{a+v+1,i+1}$ 我们知道，每当维数增加时，之后的所有水平步都会使 f_p 增加一。基本上，f_p 对应于路径 p 下方的面积。例如，在图 3 中可以看到 $f_p = 3$，而路径的权重确实是 $Q(a,b,t)q^3$。随后，我们可以结合 (17) 和引理4，并注意到

$$P(\dim(\mathcal{A}+\mathcal{B}) = a+t) = Q(a,b,t) \sum_{p \in P_{a,b,t}} q^{f_p} = Q(a,b,t) \begin{bmatrix} b \\ t \end{bmatrix}_q, \tag{18}$$

其中 $P_{a,b,t}$ 表示所有长度为 b、起始维数为 a且终止维数为 $a+t$的路径的集合。□

注 1. 经过一些代数变形，命题 4 中的公式 (14) 可改写为

$$q^{b(t-(m-a))} \begin{bmatrix} m-a \\ t \end{bmatrix}_q \alpha\beta \tag{19}$$

其中 $\alpha = \prod_{i=0}^{t-1} \frac{q^m - q^{i+m-b}}{q^m - q^i}$和 $\beta = \prod_{i=t}^{b-1} \frac{q^m - q^{i+(m-a)-t}}{q^m - q^i}$.。回想一下，$0 \le t \le \min(b, m-a)$，当 $t = m-a$对应于 $\mathcal{A}+\mathcal{B} = \mathbb{F}_q^m$的情况时，如果我们

将此值代入（19）后，除 Q_{m-a-1} 之外的所有项都将趋近于 1。这样我们就得到了一个简单得多的公式 $\prod_{i=0}^{m-a-1} \frac{q^m - q^{i+m-b}}{q^m - q^i}$，可近似为 $1 - q^{m-a-b-1}$.

对于较低的 t 值，主导部分由前两项决定，从而得到 $q^{(t-b)(m-a-t)}$ 的近似值。

在实际中，这意味着以较大的概率， $t = m-a$ 或 $t = m-a-\epsilon$，其中 ϵ 的值较小。等价地， $\mathcal{A} + \mathcal{B}$ 的维数等于 m 或 $m - \epsilon$，其中 ϵ的值较小。