arXiv:2304.00627v1 [cs.IT] 2 Apr 2023

广义线性化 Reed–Solomon 码的区分与恢复

Felicitas H¨ormann[1,2], Hannes Bartz[1],和 Anna-Lena Horlemann[2]

[1] 德国航空航天中心（DLR）通信与导航研究所，德国{felicitas.hoermann, hannes.bartz}@dlr.de

[2] 瑞士圣加仑大学计算机科学学院
anna-lena.horlemann@unisg.ch

摘要。我们研究线性化 Reed–Solomon（LRS）码的可区分性，定义并分析了经典 Reed–Solomon 码和 Gabidulin 码中平方码区分器与 Overbeck 区分器的对应形式。我们的主要结果表明，对于使用平凡自同构定义的广义线性化 Reed–Solomon（GLRS）码，平方码区分器有效；而 Overbeck 型区分器则适用于一般情形下的 LRS 码。我们进一步展示了在零导子情形下，如何从此类码的任意生成矩阵中恢复码定义参数。对于其他自同构和导子的选择，模拟结果表明这些区分器和恢复算法并不奏效。因此，相应的 LRS 码和 GLRS 码可能适用于基于编码的密码学。

1 引言

过去几十年间，研究人员在量子计算机的设计与实现方面取得了巨大进展。正如研究所示，量子计算机能够在多项式时间内解决质因数分解和离散对数问题，因此，如果攻击者拥有功能强大的量子计算机，就可以破解当今大多数公钥密码系统（例如 RSA 和 ECC）。抗量子密码学的迫切需求显而易见，尤其是因为现在存储，日后窃取 攻击允许人们现在保存加密数据，并在资源可用后立即将其解密。这一点也反映在 NIST 于 2016年启动的后量子密码学标准化进程中。经过三轮竞赛后，首批密钥封装机制（KEM）于 2022年7月实现标准化，其中一些提交方案被推进至第四轮，以便进一步研究[1]。第四轮剩余的四个 KEM 候选方案中，有三个是基于编码的。此外，第四个候选方案（即 SIKE）最近已被攻破 [7]。这也解释了为什么尽管迄今尚未有基于编码的候选方案被选中进行标准化，相关领域仍对编码相关原语寄予厚望并充满信心。

基于编码的密码学主要依赖于 McEliece 类方案，这些方案的灵感源自奠基性论文 [17]。其主要思想是选择一个秘密码的生成矩阵

并通过应用某些通常为等距或近等距的变换来掩盖其代数结构，使攻击者无法仅凭混淆矩阵的公开信息推导出已知的（或任何其他）高效译码器。

随着时间推移，人们提出了基于多种码族以及汉明度量和秩度量下伪装函数的类 McEliece 实例。例如，[4,25] 基于汉明度量下的 Reed–Solomon（RS）码；GPT 系统及其变体（例如，参见 [8,9,23]）则使用秩度量下的 Gabidulin 码。然而，在这两种情况下，都有人提出了多项式时间攻击，并攻破了若干系统：利用[25, 28] 中引入的平方码方法，可以区分 RS 码与随机码；而类 Overbeck 策略 [10,11,19–21] 则为 Gabidulin 码提供了区分器。这些研究还说明了如何恢复等价秘密密钥，使攻击者能够针对公有码进行解密。

和秩度量最早在 2005 [13, 第 III 节] 中确立，并推广了汉明度量和秩度量。因此，研究基于和秩度量码的类 McEliece 密码系统能否确保安全通信，是很自然的。文献 [22] 研究了和秩度量码的通用译码，因此为基于和秩度量的密码学的安全级别估计提供了指导。Mart´ınez-Pe˜nas [14] 提出了线性化 Reed–Solomon（LRS）码，这是 RS 码和 Gabidulin 码的和秩度量类比码，因此可作为类 McEliece 系统中秘密码的初步朴素选择。

我们着重研究如何区分 LRS 码与随机码，并提出了两种区分器，分别受到平方码思路和 Overbeck 方法的启发。我们的结果可用于区分广义线性化 Reed–Solomon 码（GLRS 码），我们将其定义为具有非零块乘子的 LRS 码。由于这一更一般的码族在半线性等价下封闭，这些方法也适用于经过等距伪装的 GLRS 码。最后，我们着重研究零导子情形，并展示如何从经过半线性等距变换伪装的 GLRS 生成矩阵中恢复高效的译码算法。

2 预备知识

首先，我们整理一些后文将用到的概念和结果。特别地，设 q 为一个素数幂，并用 $\mathbb{F}_q$表示阶为 q 的有限域。对于 $m \geq 1$，我们还考虑阶为 q^m的扩域 $\mathbb{F}_{q^m} \supseteq \mathbb{F}_q$。给定矩阵 $\boldsymbol{M} \in \mathbb{F}_{q^m}^{k\times n}$，令 $\langle M\rangle$ 表示由 $\boldsymbol{M}$的各行张成的 $\mathbb{F}_{q^m}$-线性向量空间。

2.1 和秩度量

$n \in \mathbb{N}^*$ 到 $\ell \in \mathbb{N}^*$ 的一个（整数）组合（简称 ℓ-组合）是一个向量 $\boldsymbol{n} = (n_1, \ldots, n_\ell) \in \mathbb{N}^\ell$，满足对所有 $1 \leq i \leq \ell$都有 $n_i > 0$，且符合 $n = \sum_{i=1}^{\ell} n_i$。如果 $\boldsymbol{n}$ 包含 k 个互不相同的元素 $\tilde{n}_1, \ldots, \tilde{n}_k$，记 λ_j 表示

对每个 $j = 1, \ldots, k$， $\tilde{n}_j$ 在 $\boldsymbol{n}$ 中出现的次数，并记作 $\lambda(\boldsymbol{n}) := (\lambda_1, \ldots, \lambda_k) \in \mathbb{N}^k$。

在全文中， $n \in \mathbb{N}^*$ 通常表示所讨论码的长度，我们将固定采用 n的某个特定 ℓ-组合 $\boldsymbol{n} = (n_1, \ldots, n_\ell)$。我们经常按照 $\boldsymbol{n}$将向量$\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ 或矩阵$\boldsymbol{M} \in \mathbb{F}_{q^m}^{k \times n}$（其中 $k \in \mathbb{N}^*$）分块。具体而言，对于所有 $1 \le i \le \ell$，我们分别记 $\boldsymbol{x} = (\boldsymbol{x}^{(1)} \mid \cdots \mid \boldsymbol{x}^{(\ell)})$，其中$\boldsymbol{x}^{(i)} \in \mathbb{F}_{q^m}^{n_i}$；以及 $\boldsymbol{M} = (\boldsymbol{M}^{(1)} \mid \cdots \mid \boldsymbol{M}^{(\ell)})$，其中 $\boldsymbol{M}^{(i)} \in \mathbb{F}_{q^m}^{k \times n_i}$，对于所有 $1 \le i \le \ell$。

向量$\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ 相对于 $\boldsymbol{n}$的和秩重量定义为 $\mathrm{wt}_{\Sigma R}^{\boldsymbol{n}}(\boldsymbol{x}) = \sum_{i=1}^{\ell} \mathrm{rk}_q(\boldsymbol{x}^{(i)})$，其中 $\mathrm{rk}_q(\boldsymbol{x}^{(i)})$ 是 $\boldsymbol{x}^{(i)}$ 中 $\mathbb{F}_q$-线性无关元素的最大数目， $i = 1, \ldots, \ell$。由此诱导的和秩度量定义为 $d_{\Sigma R}^{\boldsymbol{n}}(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{wt}_{\Sigma R}^{\boldsymbol{n}}(\boldsymbol{x} - \boldsymbol{y})$，其中 $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$。由于我们始终采用相同的 ℓ-组合 $\boldsymbol{n}$，为简便起见，记作 $\mathrm{wt}_{\Sigma R}$ 和 $d_{\Sigma R}$。

$\mathbb{F}_{q^m}$线性和秩度量码 $\mathcal{C}$ 是 $\mathbb{F}_{q^m}^n$的一个 $\mathbb{F}_{q^m}$子空间。其长度为 n，维数为 $k := \dim(\mathcal{C})$。我们进一步将其最小（和秩）距离定义为

$$d(\mathcal{C}) := \{d_{\Sigma R}(\boldsymbol{c}_1, \boldsymbol{c}_2) : \boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathcal{C}, \boldsymbol{c}_1 \neq \boldsymbol{c}_2\} = \{\mathrm{wt}_{\Sigma R}(\boldsymbol{c}) : \boldsymbol{c} \in \mathcal{C}, \boldsymbol{c} \neq \boldsymbol{0}\},$$

其中，最后一个等式由码的线性性得出。若矩阵 $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$满足 $\mathcal{C} = \langle \boldsymbol{G} \rangle$，则称其为 $\mathcal{C}$ 的生成矩阵。若 $\mathcal{C}$ 是矩阵 $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$ 的核，则称 $\boldsymbol{H}$ 为 $\mathcal{C}$的校验矩阵。由 $\mathcal{C}$ 的任意校验矩阵 $\boldsymbol{H}$ 生成的码是 $\mathcal{C}$ 的对偶码，记作 $\mathcal{C}^\perp$。

2.2 自同构、导子与共轭

$\mathbb{F}_{q^m}$ 上的自同构 θ 是一个映射 $\theta : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$，满足性质 $\theta(a+b) = \theta(a) + \theta(b)$，以及 $\theta(a \cdot b) = \theta(a) \cdot \theta(b)$，其中对任意 a、$b \in \mathbb{F}_{q^m}$均成立。我们将所有 $\mathbb{F}_{q^m}$-自同构组成的群记为 $\mathrm{Aut}(\mathbb{F}_{q^m})$。注意，每个自同构都逐点固定 $\mathbb{F}_{q^m}$ 的某个子域。$\mathrm{Aut}(\mathbb{F}_{q^m})$ 中其元素至少逐点固定 $\mathbb{F}_q$ 的循环子群，称为域扩张 $\mathbb{F}_{q^m}/\mathbb{F}_q$的伽罗瓦群，记作 $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$。每个 $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ 都是 Frobenius 自同构的幂（相对于 q），其定义为

$$\varphi : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}, \quad a \mapsto a^q.$$

也就是说， $\sigma \in \{\varphi^0, \ldots, \varphi^{m-1}\}$。$\sigma = \varphi^l$的不变域为$\mathbb{F}_q^{\gcd(l,m)}$，其中 $l \in \{0, \ldots, m-1\}$。为简单起见，以下假设 $\sigma = \varphi^l$ 且 $\gcd(l, m) = 1$，即令 σ 的不变域为 $\mathbb{F}_q$。

σ-导子是一个映射 $\delta : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$，满足以下两个条件：对所有 $a, b \in \mathbb{F}_{q^m}$， $\delta(a + b) = \delta(a) + \delta(b)$，且 $\delta(a \cdot b) = \delta(a) \cdot b + \sigma(a) \cdot \delta(b)$。在我们的有限域情形中，每个 σ-导子都是内导子，也就是说，对于某个$\gamma \in \mathbb{F}_{q^m}$，它等于 $\delta = \gamma(\mathrm{Id} - \sigma)$，其中 Id 是 $\mathbb{F}_{q^m}$上的恒等映射。当自同构 σ 可由上下文明确时，我们常用 δ_γ 指代与 $\gamma \in \mathbb{F}_{q^m}$对应的导子。

对于固定的一对 (σ, δ)，我们可以根据一种称为 (σ, δ)-共轭的等价关系对 $\mathbb{F}_{q^m}$ 的元素进行分组：

定义 1. 如果存在一个 $c \in \mathbb{F}_{q^m}^*$ 满足以下条件，则称两个元素 $a, b \in \mathbb{F}_{q^m}$ 为 (σ, δ)-共轭

$$a^c := \sigma(c)ac^{-1} + \delta(c)c^{-1} = b.$$

$a \in \mathbb{F}_{q^m}$ 的所有共轭元都归入相应的共轭类

$$\mathcal{K}(a) := \{a^c : c \in \mathbb{F}_{q^m}^*\} \subseteq \mathbb{F}_{q^m}.$$

对于带有 $\gamma \in \mathbb{F}_{q^m}$ 的 $\delta = \delta_\gamma$，类 $\mathcal{K}(\gamma)$ 称为平凡共轭类。

2.3 和秩度量中的等距变换

由于大多数基于编码的密码系统都采用等距伪装，我们在此简要回顾和秩等距变换的刻画。请注意，我们需要区分 $\mathbb{F}_q$-线性等距变换与 $\mathbb{F}_{q^m}$-线性等距变换。前者已在 [18,命题 426], 中研究，而后者则见于 [2, 15]。具体而言，块长度相等的特殊情形（即 $\boldsymbol{n} = (\frac{n}{\ell}, \ldots\ldots, \frac{n}{\ell})$）见于 [15, 定理 2]；任意块长度的推广以及对半线性等距变换的扩展则归功于 [2, 第 3 节3]。鉴于我们对基于编码的密码学的研究动机，我们重点关注 $\mathbb{F}_{q^m}$-(半)线性等距变换。具体而言，我们考虑如下问题：

定义 2. 双射 $\iota\colon \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^n$ 是 $\mathbb{F}_{q^m}^n$上的一个（和秩）等距变换，当且仅当它保持和秩，即对于所有 $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$，均有 $d_{\Sigma R}(\boldsymbol{x}) = d_{\Sigma R}(\iota(\boldsymbol{x}))$。当一个等距变换是 $\mathbb{F}_{q^m}$-线性的时，我们称其为线性等距变换。半线性等距变换 ι 是可加的，并且存在一个 $\mathbb{F}_{q^m}$-自同构 θ，使得对于所有 $a \in \mathbb{F}_{q^m}$ 和所有 $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$，$\iota$ 满足 $\iota(a\boldsymbol{x}) = \theta(a)\iota(\boldsymbol{x})$。

回顾一下，一般线性群 $\mathsf{GL}(n, \mathbb{F}_q)$ 包含 $\mathbb{F}_q$ 上大小为 $n \times n$ 的所有满秩矩阵，而对称群 Sym_n 由 n 个元素的所有置换组成。我们引入以下记号

$$\begin{aligned} \mathrm{GL}(\boldsymbol{n}, \mathbb{F}_q) &:= \mathrm{GL}(n_1, \mathbb{F}_q) \times \cdots \times \mathrm{GL}(n_\ell, \mathbb{F}_q) \\ \text{and} \quad \mathrm{Sym}_{\lambda(\boldsymbol{n})} &:= \mathrm{Sym}_{\lambda_1} \times \cdots \times \mathrm{Sym}_{\lambda_k}, \end{aligned}$$

其中 $\lambda(\boldsymbol{n})$ 计算 $\boldsymbol{n}$ (见 第 2.1 小节）中不同条目的出现次数。注意，$\mathsf{Sym}^{\lambda(\boldsymbol{n})}$ 是 $\mathsf{Sym}^{\sum_j \lambda_j} = \mathrm{Sym}_\ell$的子群。

定理 1（和秩等距变换 [2,15]）。$\mathbb{F}_{q^m}^n$ 上的 $\mathbb{F}_{q^m}$-线性等距变换群为

$$\mathrm{LI}(\mathbb{F}_{q^m}^n) := \left((\mathbb{F}_{q^m}^*)^\ell \times \mathrm{GL}(\boldsymbol{n}, \mathbb{F}_q)\right) \rtimes \mathrm{Sym}_{\lambda(\boldsymbol{n})}.$$

其作用 $\mathsf{act}_{\mathrm{LI}}$：$\mathsf{LI}(\mathbb{F}_{q^m}^n) \times \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^n$ 定义为

$$\mathrm{act}_{\mathrm{LI}}(\iota, \boldsymbol{x}) := \left(c_1 \boldsymbol{x}^{(\pi^{-1}(1))} \boldsymbol{M}_1 \mid \cdots \mid c_\ell \boldsymbol{x}^{(\pi^{-1}(\ell))} \boldsymbol{M}_\ell\right)$$

对于 $\iota = ((c_1, \ldots, c_\ell), (\boldsymbol{M}_1, \ldots, \boldsymbol{M}_\ell)\ \pi)$ 和 $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$。类似地，$\mathbb{F}_{q^m}^n$ 上的$\mathbb{F}_{q^m}$-半线性等距变换群为

$$\mathrm{SI}(\mathbb{F}_{q^m}^n) := \mathrm{LI}(\mathbb{F}_{q^m}^n) \rtimes \mathrm{Aut}(\mathbb{F}_{q^m})$$

其作用 $\mathrm{act}_{\mathrm{SI}} : \mathrm{SI}(\mathbb{F}_{q^m}^n) \times \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^n$ 由下式给出

$$\mathrm{act}_{\mathrm{SI}}((\iota, \theta), \boldsymbol{x}) := \theta(\mathrm{act}_{\mathrm{LI}}(\iota, \boldsymbol{x}))$$

对于 $(\iota, \theta) \in \mathrm{SI}(\mathbb{F}_{q^m}^n)$ 和 $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$。

由于 MacWilliams 扩张定理在这一一般情形下并不成立（秩度量情形下的反例见 [3, 例 2.9 (a)] ），和秩度量下的码等价性是通过整个空间的等距变换来定义的（参见 [2,定义 3。9]）。

定义 3. 若存在一个线性等距变换 $\iota \in \mathrm{LI}(\mathbb{F}_{q^m}^n)$，使得下式成立，则称两个和秩度量码 $\mathcal{C}, \mathcal{D} \subseteq \mathbb{F}_{q^m}^n$ 线性等价

$$\mathrm{act}_{\mathrm{LI}}(\iota, \mathcal{C}) := \{\mathrm{act}_{\mathrm{LI}}(\iota, \boldsymbol{c}) : \boldsymbol{c} \in \mathcal{C}\} = \mathcal{D}.$$

若存在 $(\iota, \theta) \in \mathrm{SI}(\mathbb{F}_{q^m}^n)$，使得下式成立，则称它们半线性等价

$$\mathrm{act}_{\mathrm{SI}}((\iota, \theta), \mathcal{C}) := \{\mathrm{act}_{\mathrm{SI}}((\iota, \theta), \boldsymbol{c}) : \boldsymbol{c} \in \mathcal{C}\} = \mathcal{D}.$$

2.4 斜多项式

斜多项式环 $\mathbb{F}_{q^m}[x; \sigma, \delta]$ 定义为多项式 $f(x) = \sum_i f_i x^i$ 的集合，其中只有有限个非零系数 $f_i \in \mathbb{F}_{q^m}$。它采用传统的多项式加法，但乘法由规则 $xa = \sigma(a)x + \delta(a)$确定。与传统多项式环类似，我们将非零斜多项式 $f(x) = \sum_i f_i x^i \in \mathbb{F}_{q^m}[x; \sigma, \delta]$ 的次数定义为 $\deg(f) := \max\{i : f_i \neq 0\}$，并将零多项式的次数设为 $-\infty$。

请注意，尽管它与 $\mathbb{F}_{q^m}[x]$有许多相似之处，但相同的求值策略（即，对于 $c \in \mathbb{F}_{q^m}$，使用 $f(c) = \sum_i f_i c^i$）在此情形下并不适用。相反，文献中提供了两种适用于斜多项式的求值方法：余式求值和广义算子求值。本文将重点讨论后者。

对于 a、$b \in \mathbb{F}_{q^m}$，定义算子

$$\mathcal{D}_a(b) := \sigma(b)a + \delta(b)$$

及其幂 $\mathcal{D}_a^i(b) := \mathcal{D}_a(\mathcal{D}_a^{i-1}(b))$，其中 $i \geq 0$ （满足 $\mathcal{D}_a^0(b) = b$ 且 $\mathcal{D}_a^1(b) = \mathcal{D}_a(b)$）。对于 $\boldsymbol{a} = (a_1, \ldots, a_\ell) \in \mathbb{F}_{q^m}^\ell$和 $\boldsymbol{B} \in \mathbb{F}_{q^m}^{k \times n}$，我们记作 $\mathcal{D}_{\boldsymbol{a}}(\boldsymbol{B}) := (\mathcal{D}_{a_1}(\boldsymbol{B}^{(1)}) \mid \cdots \mid \mathcal{D}_{a_\ell}(\boldsymbol{B}^{(\ell)}))$，其中 $\mathcal{D}_{a_i}(\boldsymbol{B}^{(i)})$ 表示将 $\mathcal{D}_{a_i}(\cdot)$ 逐元素应用于 $\boldsymbol{B}^{(i)}$ 的各项（$1 \leq i \leq \ell$）。此记法也适用于向量 $\boldsymbol{b} \in \mathbb{F}_{q^m}^n$，并可扩展至算子的幂。

在零导子情形下，上述定义的算子的 i 重复应用可表示为

$$\mathcal{D}_a^i(b) = \sigma^i(b) \cdot \mathcal{N}_i(a)$$

对于任意 a、$b \in \mathbb{F}_{q^m}$ 和 $i \in \mathbb{N}^*$。这里，$\mathcal{N}_i(a) := \prod_{j=0}^{i-1} \sigma^j(a) = \sigma^{i-1}(a) \ldots \sigma(a) \cdot a$ 表示广义幂函数。

引理 1. 对于任意 a、b 和 $c \in \mathbb{F}_{q^m}$，等式 $\mathcal{D}_a(bc) = \sigma(b)\mathcal{D}_a(c) + \delta(b)c$ 成立。

证明。根据 $\mathcal{D}_a(\cdot)$ 的定义和导子的乘积法则，可得

$$\begin{aligned}\mathcal{D}_a(bc) &= \sigma(bc)a + \delta(bc) = \sigma(bc)a + \delta(b)c + \sigma(b)\delta(c) \\ &= \sigma(b)(\sigma(c)a + \delta(c)) + \delta(b)c = \sigma(b)\mathcal{D}_a(c) + \delta(b)c.\end{aligned}$$

□

现在定义斜多项式的广义算子求值：

定义 4. 斜多项式 $f(x) = \sum_i f_i x^i \in \mathbb{F}_{q^m}[x;\ \sigma、\ \delta]$ 关于求值参数 $a \in \mathbb{F}_{q^m}$ 在点 $b \in \mathbb{F}_{q^m}$ 处的广义算子求值定义为

$$f(b)_a := \sum_i f_i \mathcal{D}_a^i(b).$$

对于向量 $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$、向量 $\boldsymbol{a} = (a_1, \ldots, a_\ell) \in \mathbb{F}_{q^m}^\ell$ 以及参数 $d \in \mathbb{N}^*$，广义 Moore 矩阵 $\mathfrak{M}_d(\boldsymbol{x})_{\boldsymbol{a}}$ 定义为

$$\mathfrak{M}_d(\boldsymbol{x})_{\boldsymbol{a}} := \left(\boldsymbol{V}_d(\boldsymbol{x}^{(1)})_{a_1}, \ldots, \boldsymbol{V}_d(\boldsymbol{x}^{(\ell)})_{a_\ell}\right) \in \mathbb{F}_{q^m}^{d \times n},$$

$$\text{where } \boldsymbol{V}_d(\boldsymbol{x}^{(i)})_{a_i} := \begin{pmatrix} x_1^{(i)} & \cdots & x_{n_i}^{(i)} \\ \mathcal{D}_{a_i}(x_1^{(i)}) & \cdots & \mathcal{D}_{a_i}(x_{n_i}^{(i)}) \\ \vdots & \ddots & \vdots \\ \mathcal{D}_{a_i}^{d-1}(x_1^{(i)}) & \cdots & \mathcal{D}_{a_i}^{d-1}(x_{n_i}^{(i)}) \end{pmatrix} \quad \text{for } 1 \le i \le \ell.$$

若 $\boldsymbol{a}$ 包含来自两两不同的非平凡共轭类的代表元 $\mathbb{F}_{q^m}$ 且 $\mathbf{rk}_q\left(\boldsymbol{x}^{(i)}\right) = n_i$ 对所有 $1 \le i \le \ell$，根据 [14, 定理 2] 和 [12,定理 4。5] 有 $\mathbf{rk}_{q^m}\left(\mathfrak{M}_d(\boldsymbol{x})_{\boldsymbol{a}}\right) = \min(d, n)$。

2.5 （广义）线性化 Reed–Solomon 码

我们回顾 LRS 码的定义，这类码同时推广了 RS 码和 Gabidulin 码。LRS 码是基于斜多项式的求值码；在汉明度量和秩度量情形下，斜多项式分别特化为常规多项式和线性化多项式。

定义 5（线性化 Reed–Solomon 码 [14, 定义 31]）。令 $\boldsymbol{a}=(a_1,\ldots,a_\ell)\in \mathbb{F}_{q^m}^{\ell}$ 由 $\mathbb{F}_{q^m}$中互不相同的非平凡共轭类的代表元组成。取向量 $\boldsymbol{\beta}\in\mathbb{F}_{q^m}^{n}$，其各个块 $\boldsymbol{\beta}^{(i)}=\left(\beta_1^{(i)},\ldots,\beta_{n_i}^{(i)}\right)$包含 $\mathbb{F}_q$-线性无关的元素，对所有 $i=1,\ldots,\ell$均成立。则长度为 线性化 Reed–Solomon（LRS）码，其长度为 n，维数为 k，定义如下

$$\mathrm{LRS}[\boldsymbol{\beta},\boldsymbol{a};\boldsymbol{n},k]:=\left\{\left(\boldsymbol{c}^{(1)}(f)\mid\cdots\mid\boldsymbol{c}^{(\ell)}(f)\right):f\in\mathbb{F}_{q^m}[x;\sigma,\delta]_{<k}\right\}\subseteq\mathbb{F}_{q^m}^{n}$$

where $\boldsymbol{c}^{(i)}(f):=\left(f(\beta_1^{(i)})_{a_i},\ldots,f(\beta_{n_i}^{(i)})_{a_i}\right)$.

注意，LRS 码以等号达到 $d\le n-k+1$ 由 [14,命题 34] 给出的 Singleton 类界，其中 d 表示该码的最小和秩距离。因此，它们是最大和秩距离（MSRD）码。

广义 Moore 矩阵 $\mathfrak{M}_k(\boldsymbol{\beta})_{\boldsymbol{a}}$ 是码 LRS$[\boldsymbol{\beta},\boldsymbol{a}$的生成矩阵； $\boldsymbol{n},k]$。由于这种形式的生成矩阵很有用，例如它可导出已知的高效译码算法，因此我们称其为 LRS$[\boldsymbol{\beta},\boldsymbol{a}$的典范生成矩阵； $\boldsymbol{n},k]$。注意，典范生成矩阵的参数 $\boldsymbol{\beta}$和 $\boldsymbol{a}$通常并不唯一，即使固定一个特定的 $\boldsymbol{a}$，也不能保证 $\boldsymbol{\beta}$唯一。

在零导子情形下，LRS 码的对偶码可描述为

$$\mathrm{LRS}[\boldsymbol{\beta},\boldsymbol{a};\boldsymbol{n},k]^{\perp}=\mathrm{LRS}[\boldsymbol{\alpha},\sigma^{-1}(\boldsymbol{a});\boldsymbol{n},n-k]_{\sigma^{-1}},\tag{1}$$

其中，右侧的下标 σ^{-1} 表示这是一个相对于逆自同构 σ^{-1} 的 LRS 码（见 [5,6]）。向量$\boldsymbol{\alpha}=(\boldsymbol{\alpha}^{(1)}\mid\cdots\mid\boldsymbol{\alpha}^{(\ell)})\in\mathbb{F}_{q^m}^{n}$ 满足

$$\sum_{i=1}^{\ell}\sum_{j=1}^{n_i}\alpha_j^{(i)}\mathcal{D}_{a_i}^{h-1}(\beta_j^{(i)})=0\quad\text{for all } h=1,\ldots,n-1\tag{2}$$

并且根据 [16, 定理 4]，其和秩重量为 $\mathrm{wt}_{\Sigma R}(\boldsymbol{\alpha})=n$。特别地，零导子 LRS 码的对偶码仍然是 LRS 码。允许非零导子时，LRS 码的对偶码是线性化 Goppa 码，它们与 LRS 码（非规范地）同构 [5,6]。

正如定理 2 的证明所示，与 LRS 码（半）线性等价的码不一定本身就是 LRS 码。不过，对于通过允许非零块乘子而得到的更一般码族，这一结论成立。我们将 GLRS 码定义如下：

定义 6（广义线性化 Reed–Solomon 码）。设 $\mathcal{C}:=\mathrm{LRS}[\boldsymbol{\beta},\boldsymbol{a};\ \boldsymbol{n},\ k]$ 是定义 5 中的 LRS 码。此外，设 $\boldsymbol{v}=(v_1,\ \ldots,\ v_\ell)\in\mathbb{F}_{q^m}^{\ell}$ 是一个由非零 $\mathbb{F}_{q^m}$ 元素组成的向量。我们将广义线性化 Reed–Solomon 码 GLRS$[\boldsymbol{\beta},\boldsymbol{a},\boldsymbol{v};\ \boldsymbol{n},\ k]$ 定义为

$$\mathrm{GLRS}[\boldsymbol{\beta},\boldsymbol{a},\boldsymbol{v};\boldsymbol{n},k]:=\left\{\left(v_1\boldsymbol{c}^{(1)}\mid\cdots\mid v_\ell\boldsymbol{c}^{(\ell)}\right):\boldsymbol{c}\in\mathcal{C}\right\}\subseteq\mathbb{F}_{q^m}^{n}.$$

注意，当 $\boldsymbol{v}$ 为全一向量时，我们可以从 GLRS 码中恢复 LRS 码。由于根据 $\mathbb{F}_{q^m}$，用不同的非零 定理1，对块进行乘法是一个和秩等距变换，因此可得以下推论：

推论 1. 码 GLRS$[\boldsymbol{\beta}, \boldsymbol{a}, \boldsymbol{v};\ \boldsymbol{n}, k]$ 的最小和秩距离为 $d = n - k + 1$。因此，GLRS 码是最大和秩距离的。

码 GLRS$[\boldsymbol{\beta}, \boldsymbol{a}, \boldsymbol{v};\ \boldsymbol{n}, k]$ 的生成矩阵具有如下形式

$$\boldsymbol{G} = \left(v_1 \boldsymbol{V}_k(\boldsymbol{\beta}^{(1)})_{a_1} \mid \cdots \mid v_\ell \boldsymbol{V}_k(\boldsymbol{\beta}^{(\ell)})_{a_\ell}\right).$$

与 LRS 情形类似，我们将任何这种形式的生成矩阵称为 GLRS$[\boldsymbol{\beta}, \boldsymbol{a}, \boldsymbol{v};\ \boldsymbol{n}, k]$ 的典范生成矩阵。注意，GLRS 码的典范生成矩阵不仅取决于参数 $\boldsymbol{\beta}$ 和 $\boldsymbol{a}$，还取决于块乘子 $\boldsymbol{v}$。

3 问题陈述

我们要解决的主要问题是：将经由 $\mathbb{F}_{q^m}$-半线性等距变换伪装的 GLRS 码，与长度和维数相同的随机和秩度量码区分开来。形式化地说，我们将这一任务表述如下：

问题 1（半线性等价意义下的 GLRS 码判别）。给定一个满秩矩阵 $\boldsymbol{M} \in \mathbb{F}_{q^m}^{k\times n}$，判断是否存在参数 $\boldsymbol{\beta} \in \mathbb{F}_{q^m}^n$, $\boldsymbol{a} \in \mathbb{F}_{q^m}^\ell$, $\boldsymbol{v} \in \mathbb{F}_{q^m}^\ell$, $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$，以及一个作为 σ-导子的 δ，使得 $\langle \boldsymbol{M} \rangle$ 与 GLRS$[\boldsymbol{\beta}, \boldsymbol{a}, \boldsymbol{v};\ \boldsymbol{n}, k]$ 半线性等价。

我们现在研究 $\mathbb{F}_{q^m}$-半线性变换如何影响 GLRS 码，以便更好地理解这一问题。 定理 2 表明，每个半线性等距变换（参见 定理 1）都会将一个 GLRS 码变换为另一个参数可能不同的 GLRS 码：

定理 2. 设 $\mathcal{C} = \mathrm{GLRS}[\boldsymbol{\beta}, \boldsymbol{a}, \boldsymbol{v};\ \boldsymbol{n}, k]$ 是关于 σ和 $\delta := \delta_\gamma$的 GLRS 码。进一步设 $\iota \in \mathrm{LI}(\mathbb{F}_{q^m}^n)$ 表示一个 $\mathbb{F}_{q^m}$-线性等距变换，满足 $\iota = \hat{} ((c_1, \ldots, c_\ell), (\boldsymbol{M}_1, \ldots, \boldsymbol{M}_\ell)\ \pi)$。那么，线性等价码 $\mathcal{C} := \mathrm{act}_{\mathrm{LI}}(\iota, \mathcal{C})$ 也是关于 σ 和 δ 的 GLRS 码。也就是说，$\hat{}\mathcal{C} = \mathrm{GLRS}[\hat{}\boldsymbol{\beta}, \hat{}\boldsymbol{a}, \hat{}\boldsymbol{v};\ \boldsymbol{n}, k]$，其中 $\hat{}\ \boldsymbol{\beta} = (\boldsymbol{\beta}^{(\pi^{-1}(1))}\boldsymbol{M}_1 \mid \cdots \mid \boldsymbol{\beta}^{(\pi^{-1}(\ell))}\boldsymbol{M}_\ell)$，$\hat{}\boldsymbol{a} = (a_{\pi^{-1}(1)} \cdots, a_{\pi^{-1}(\ell)})$，且 $\hat{}\boldsymbol{v} = (c_1 v_{\pi^{-1}(1)} \cdots, c_\ell v_{\pi^{-1}(\ell)})$。

对于半线性等距变换 $(\iota, \theta) \in \mathrm{SI}(\mathbb{F}_{q^m}^n)$，其中 ι如上所述，且 $\theta \in \mathrm{Aut}(\mathbb{F}_{q^m})$，码 $\mathrm{act}_{\mathrm{SI}}((\iota, \theta)\ \mathcal{C})$ 是相对于自同构 σ和可能不同的导子 $\delta_{\theta(\gamma)} := \theta(\gamma)(\mathrm{Id} - \sigma)$ 的 GLRS 码。其参数为 $\theta(\boldsymbol{\beta})$,$\theta(\hat{}\boldsymbol{a})$, 和 $\theta(\hat{}\boldsymbol{v})$，其中 θ 逐元素作用于向量。

证明。整个证明中，我们使用简写记号 $v_{\pi_i} := v_{\pi^{-1}(i)}$、 $a_{\pi_i} := a_{\pi^{-1}(i)}$以及$\boldsymbol{\beta}^{(\pi_i)} := \boldsymbol{\beta}^{(\pi^{-1}(i))}$。 $\mathcal{C}$ 具有如下形式的生成矩阵

$\boldsymbol{G} := \left(v_1 \boldsymbol{V}_k(\boldsymbol{\beta}^{(1)})_{a_1},\ \ldots,\ v_\ell \boldsymbol{V}_k(\boldsymbol{\beta}^{(\ell)})_{a_\ell}\right)$。若 ι 作用于 $\boldsymbol{G}$ 的第 j 行，其中 $j \in \{1, \ldots, k\}$，则得到

$$\left(c_1 v_{\pi_1} \mathcal{D}^{j-1}_{a_{\pi_1}}(\boldsymbol{\beta}^{(\pi_1)})\boldsymbol{M}_1 \mid \cdots \mid c_\ell v_{\pi_\ell} \mathcal{D}^{j-1}_{a_{\pi_\ell}}(\boldsymbol{\beta}^{(\pi_\ell)})\boldsymbol{M}_\ell\right). \tag{3}$$

由于广义算子求值是 $\mathbb{F}_q$-线性的，因此有 $\mathcal{D}^{j-1}_{a_{\pi_i}}(\boldsymbol{\beta}^{(\pi_i)})\boldsymbol{M}_i = \mathcal{D}^{j-1}_{a_{\pi_i}}(\boldsymbol{\beta}^{(\pi_i)}\boldsymbol{M}_i)$ 对所有 $i = 1$、……、ℓ 成立，因此，(3) 正好是 j的第 j 行

$$\hat{\boldsymbol{G}} := \left(c_1 v_{\pi_1} \boldsymbol{V}_k(\boldsymbol{\beta}^{(\pi_1)}\boldsymbol{M}_1)_{a_{\pi_1}}, \ldots, c_\ell v_{\pi_\ell} \boldsymbol{V}_k(\boldsymbol{\beta}^{(\pi_\ell)}\boldsymbol{M}_\ell)_{a_{\pi_\ell}}\right).$$

^^由于 $\boldsymbol{G}$ 生成了 $\mathcal{C}$，这就证明了定理的第一部分。第二部分由以下观察得出

$$\theta(v\mathcal{D}^{j-1}_a(\beta)) = \theta(v)\left(\mathcal{D}^{\sigma,\delta_{\theta(\gamma)}}_{\theta(a)}\right)^{j-1}(\theta(\beta)) \tag{4}$$

对于任意 v、a、$\beta \in \mathbb{F}^*_{q^m}$ 以及 $j \in \mathbb{N}^*$ 满足 $\mathcal{D}^{\sigma}$、. $^{\delta_{\theta(\gamma)}}(\cdot)$ 表示关于自同构 σ 和导子$\delta_{\theta(\gamma)}$ 的广义算子求值: $= \theta(\gamma)(\mathrm{Id} - \sigma)$。(4) 可通过对 j进行归纳验证。 □

事实上，这表明，关于固定自同构和固定导子的 GLRS 码在线性等价下封闭。如果允许固定自同构对应不同的导子，则 GLRS 码甚至在半线性等价下也封闭。直观地说，这意味着 问题 1 归结为区分 GLRS 码。因此，我们提出并聚焦于 问题 2:

问题 2（区分 GLRS 码）。给定一个满秩矩阵 $\boldsymbol{M} \in \mathbb{F}^{k\times n}_{q^m}$，判断是否存在参数 $\boldsymbol{\beta} \in \mathbb{F}^n_{q^m}$, $\boldsymbol{a} \in \mathbb{F}^\ell_{q^m}$, $\boldsymbol{v} \in \mathbb{F}^\ell_{q^m}$, $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$，以及作为 σ-导子的 δ，使得 $\langle \boldsymbol{M} \rangle = \mathrm{GLRS}[\boldsymbol{\beta}, \boldsymbol{a}, \boldsymbol{v};\ \boldsymbol{n}, k]$。

下面更准确地说明，在已知自同构 σ 和导子 $\delta := \delta_\gamma$的情况下，上述两个问题之间的关系。若仅考虑线性等价，则问题 1 等价于问题 2，因为每个与关于 σ 和 δ 的 GLRS 码线性等价的码，本身也是关于相同自同构和导子的 GLRS 码。在更一般的半线性情形下，我们可以通过求解问题 2 的多个实例来解决问题 1。具体而言，根据定理 2，我们需要针对所有满足 $\theta \in \mathrm{Aut}(\mathbb{F}_{q^m})$ 的导子 $\delta_{\theta(\gamma)} := \theta(\gamma)(\mathrm{Id} - \sigma)$ 考虑问题 2。由于当 s 为 $\mathbb{F}_q$ 关于其素域的扩张次数时，$|\mathrm{Aut}(\mathbb{F}_{q^m})| = sm$，因此问题 1 等价于求解 sm 个问题 2 的实例。

我们提出了两种多项式时间区分器，可部分解决 问题 2，条件是 σ 和 δ 已知，详见 第 4 节。然而，仅仅知道一个矩阵是否生成 GLRS 码，并不足以攻破一种基于 GLRS 码的假想 McEliece 类密码系统。我们更希望为公开已知的码恢复一种高效的译码算法，例如，通过找出一个典范生成矩阵。因此，以下问题备受关注:

问题 3（恢复典范 GLRS 生成矩阵）。给定 GLRS 码 $\mathcal{C}$ 的任意生成矩阵 $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k\times n}$，求参数 $\boldsymbol{\beta} \in \mathbb{F}_{q^m}^{n}$,$\boldsymbol{a} \in \mathbb{F}_{q^m}^{\ell}$, $\boldsymbol{v} \in \mathbb{F}_{q^m}^{\ell}$, $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$，以及一个 σ-导子 δ，使得$\left(v_1 \boldsymbol{V}_k(\boldsymbol{\beta}^{(1)})_{a_1} \mid \cdots \mid v_\ell \boldsymbol{V}_k(\boldsymbol{\beta}^{(\ell)})_{a_\ell}\right)$ 是 $\mathcal{C}$ 的典范生成矩阵。

我们研究问题 3，并在第 5 节中展示两种技术，用于在已知自同构 σ的零导子情形下，部分解决 GLRS 码中的该问题。

4 GLRS 码的区分器

本节介绍两种能够在许多实例中解决问题 2的方法，即将 GLRS 码与随机码区分开的任务。在这两种方法中，我们都假设已知自同构 σ 以及相对于其进行码区分的导子 δ。

在第 4.1 小节中，我们重点讨论一种平方码区分器，该区分器受 RS 码区分器启发。它适用于通过恒等自同构和零导子构造的 GLRS 码。

随后，我们在第 4.2 小节中介绍一种受秩度量情形启发的 Overbeck 类区分器。该方法能够处理自同构和导子的任意有效组合，但要求已知求值参数向量 $\boldsymbol{a}$。此外，Overbeck 型区分器无法处理块乘子，因此仅适用于 LRS 码。不过，通过最多应用该区分器（q^m-1）$^\ell$ 次，仍然可以处理 GLRS 码（有关更多细节，请参见第 4.2 小节）。

我们使用 SageMath 的实现 [26]，针对不同的参数集对本节中介绍的所有结果进行了实验验证。

4.1 平方码区分器

针对基于广义 Reed–Solomon（GRS）码的 McEliece/Niederreiter 变体，Sidelnikov 和 Shestakov 在 [25] 中提出了第一个多项式时间攻击。随后，Wieschebrink 对该攻击进行了改进，用于攻击改进后的 Berger–Loidreau 密码系统 [27], ，该密码系统基于 GRS 子码。 [27] 中的方法在 [28] 中得到进一步改进，使其能够处理更小的子码，从而攻破采用大多数实际参数的密码系统。 [28] 中的攻击基于码的逐元素乘积（或 Schur 平方码）的性质。对于任意向量 $\boldsymbol{x}$、$\boldsymbol{y} \in \mathbb{F}_{q^m}^{n}$，我们将 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的逐元素乘积（也称为 Schur 乘积或星乘积）定义为

$$\boldsymbol{x} \star \boldsymbol{y} := (x_1y_1, x_2y_2 \ldots, x_ny_n).$$

$\mathbb{F}_{q^m}$-线性码 $\mathcal{C} \subseteq \mathbb{F}_{q^m}^{n}$ 的平方码定义为

$$\mathcal{C} \star \mathcal{C} := \{\boldsymbol{c}_1 \star \boldsymbol{c}_2 : \boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathcal{C}\}.$$

区分$\mathbb{F}_{q^m}^{n}$ 中的随机线性码与 $\mathcal{C}$ 广义 Reed–Solomon 码$\mathcal{C} \star \mathcal{C}$的主要观察是，平方广义 Reed–Solomon 码的维数为 $\dim(\mathcal{C} \star \mathcal{C}) \quad =$

$\min(n,\ 2k-1)$，与平方随机线性码的预期维数相比很小。请注意，类似的技术曾用于超出唯一解码半径的 RS 码幂解码（参见 [24, 引理 1]）。

现在，我们将为由恒等自同构 $\sigma = \mathrm{Id}$ 的斜多项式环构造的 GLRS 码推导一个类似的区分器。注意，在这种情况下，唯一可能的导子是零导子。引理 2 给出了推导 GLRS 码平方码区分器所需的一些基本结果：

引理 2. 对于 $\sigma = \mathrm{Id}$，设 $\mathcal{C} = \mathrm{GLRS}[\boldsymbol{\beta}, \boldsymbol{a}, \boldsymbol{v};\ \boldsymbol{n}, k]$ 是由 $\mathbb{F}_{q^m}[x;\ \sigma]_{<k} = \mathbb{F}_{q^m}[x]_{<k}$ 中的多项式构造的 GLRS 码。那么我们有

$$\mathcal{C} = \Big\{ \big(f(a_1), \ldots, f(a_1) \mid \cdots \mid f(a_\ell), \ldots, f(a_\ell)\big) \cdot \mathrm{diag}\big((v_1\boldsymbol{\beta}^{(1)} \mid \cdots \mid v_\ell \boldsymbol{\beta}^{(\ell)})\big) \\ : f \in \mathbb{F}_{q^m}[x]_{<k} \Big\},$$

其中 $f(\cdot)$ 表示普通多项式求值。

证明。由于 σ 是恒等自同构，因此 $f \in \mathbb{F}_{q^m}[x;\ \sigma]$ 在元素 $\beta_j^{(i)} \in \mathbb{F}_{q^m}$ 处关于求值参数 $a_i \in \mathbb{F}_{q^m}$ 的广义算子求值为

$$f(\beta_j^{(i)})_{a_i} = \sum_{l=0}^{k-1} f_l \mathcal{D}^l_{a_i}(\beta_j^{(i)}) = \sum_{l=0}^{k-1} f_l \sigma^l(\beta_j^{(i)}) \mathcal{N}_l(a_i) = \beta_j^{(i)} \sum_{l=0}^{k-1} f_l a_i^l = \beta_j^{(i)} f(a_i),$$

其中 $f(\cdot)$ 表示普通多项式求值。因此，任意 $\boldsymbol{c} \in \mathcal{C}$ 都可以写成

$$\begin{aligned} \boldsymbol{c} &= (v_1 f(\beta_1^{(1)})_{a_1}, \ldots, v_1 f(\beta_{n_1}^{(1)})_{a_1} \mid \cdots \mid v_\ell f(\beta_1^{(\ell)})_{a_\ell}, \ldots, v_\ell f(\beta_{n_\ell}^{(\ell)})_{a_\ell}) \\ &= (v_1\beta_1^{(1)} f(a_1), \ldots, v_1\beta_{n_1}^{(1)} f(a_1) \mid \cdots \mid v_\ell \beta_1^{(\ell)} f(a_\ell), \ldots, v_\ell \beta_{n_\ell}^{(\ell)} f(a_\ell)). \end{aligned}$$

□

这使我们能够推导出引理 3该引理给出了 GLRS 码的平方码维数，以及与之形成对比的随机线性码平方码维数的结果。

引理 3. 1. 设 $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ 是一个维数为 k 、相对于 $\sigma = \mathrm{Id}$ 的 GLRS 码。则

$$\dim(\mathcal{C} \star \mathcal{C}) = \min(\ell, 2k-1).$$

2. 设 $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ 是一个维数为 k 、均匀随机选取的线性码。则

$$\Pr\left(\dim(\mathcal{C} \star \mathcal{C}) < \min\left(n, \frac{k(k+1)}{2}\right)\right) \xrightarrow{k\to\infty} 0,$$

其中，$\Pr(\cdot)$ 表示括号中事件发生的概率。

证明。 1. 设 $\boldsymbol{c}$、$\boldsymbol{c}'$ 是来自 $\mathcal{C}\star\mathcal{C}$ 的两个码字，它们由多项式 f、$g\in\mathbb{F}_{q^m}[x$的求值构造而成；其中 σ]的次数 $\deg(f)$ $=\deg(g)$ $=k-1$最大。于是，根据 引理 2，可得 $\boldsymbol{c}\star\boldsymbol{c}'$ 具有如下形式

$$\boldsymbol{c}\star\boldsymbol{c}'=((f\cdot g)(a_1),\ldots,(f\cdot g)(a_1)\mid\cdots\mid(f\cdot g)(a_\ell),\ldots,(f\cdot g)(a_\ell))\cdot\operatorname{diag}\left(\left(v_1^2\left(\boldsymbol{\beta}^{(1)}\right)^2\mid\cdots\mid v_\ell^2\left(\boldsymbol{\beta}^{(\ell)}\right)^2\right)\right),$$

其中，对各块 $\boldsymbol{\beta}^{(i)}$ for $i=1$、.....、ℓ 的平方按元素进行理解。由于 $\boldsymbol{a}$ 包含 $\mathbb{F}_{q^m}$的不同共轭类的代表元， $\boldsymbol{a}$ 中的元素两两不同。由于 $\boldsymbol{\beta}$ 包含按块 $\mathbb{F}_q$-线性无关的元素， $\boldsymbol{\beta}$ 中的所有元素均非零。结合 $\boldsymbol{v}$ 仅包含非零元素这一事实可知，该对角矩阵具有满秩 n。因此，只考虑每个块的第一列，我们得到一个长度为 ℓ、维数为 $\deg(f\cdot g)$ $+1=2k-1$的广义 Reed–Solomon 码。相应生成矩阵的大小为 $(2k-1)$ $\times\ell$，从而得到该结论。

2. 这直接由 [27] 得出。

□

定理 3 总结了恒等自同构情形下，针对 GLRS 码的 Wieschebrink 类平方码区分器的结果。

定理 3（平方码区分器）。设 $2<k\leq\frac{n}{2}$，并令 σ 为恒等自同构。给定 $\mathbb{F}_{q^m}^n$ 中一个 k-维码的生成矩阵，我们可以在 $\mathbb{F}_{q^m}$ 中通过 $\mathcal{O}(n^5)$ 次运算，以高概率 [1] 将 GLRS 码与随机码区分开来。

证明。 利用 引理 3 通过考察平方码的维数，我们可以高概率地区分 GLRS 码与随机线性码。其复杂度约为

$$\mathcal{O}(k^4n+k^2n+k^2(n-k)^2n)\subseteq\mathcal{O}(n^5)$$

次运算，依据 [28]可得。 □

4.2 一个 Overbeck 类区分器

Overbeck 在[19–21]中针对 Gabidulin 码提出了一种区分器。其主要思想是反复对公生成矩阵应用 Frobenius 自同构，并将所得结果垂直堆叠起来。由于 Gabidulin 码存在一个生成矩阵，使得其第 i行是对生成向量应用（$i-1$）次 Frobenius 自同构得到的结果，因此，堆叠矩阵的秩对于每个新的矩阵块仅增加一。但随机满秩矩阵的表现不同，堆叠矩阵通常具有高得多的秩。

[1] 事实上，该区分器能够以概率 1 识别 GLRS 码。但在小概率情况下，它可能会错误地将非 GLRS 码判定为 GLRS 码。

Horlemann-Trautmann、Marshall 和 Rosenthal [11] 采用了一种略有不同的方法，我们简称为 HMR 方法，用于恢复 Gabidulin码的秘密参数。我们提及他们的技术，是因为它由此产生了一种区分器，而且与 Overbeck方法类似：它同样利用了 Frobenius 自同构对公生成矩阵的反复作用。但 HMR 方法不考虑相应码的和，而是关注这些码的交，并表明每次迭代后，其维数仅减少一。随机码在这一操作下则表现不同。

现在，我们介绍 Overbeck 方法在和秩度量下对 LRS 码的一种推广。与平方码区分器不同，Overbeck 类区分器适用于具有任意自同构 σ 以及任意有效 σ 导子 δ 的一般情形。由于它不支持块乘子，即 GLRS 码，下面简要说明如何将用于 LRS 码的区分器一般性地应用于 GLRS 码。因此，回顾一下，GLRS 码 GLRS$[\boldsymbol{\beta}, \boldsymbol{a}, \boldsymbol{v};\ \boldsymbol{n}, k]$ 的生成矩阵具有形式 $(v_1\boldsymbol{G}^{(1)} \mid \cdots \mid v_\ell \boldsymbol{G}^{(\ell)})$，其中 $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k\times n}$ 是 LRS$[\boldsymbol{\beta}, \boldsymbol{a};\ \boldsymbol{n}, k]$ 的生成矩阵。但这意味着，如果我们将 Overbeck 类区分器应用于矩阵 $(v_1^{-1}\boldsymbol{M}^{(1)} \mid \cdots \mid v_\ell^{-1}\boldsymbol{M}^{(\ell)})$，$\boldsymbol{M} \in \mathbb{F}_{q^m}^{k\times n}$ 它至少会成功一次，其中 表示 GLRS 码的公生成矩阵。因此，我们可以针对不同的 $\boldsymbol{v}^{-1} \in \mathbb{F}_{q^m}^{\ell}$ 运行 Overbeck 类区分器，直到其成功，或者在最坏情况下检查所有可能的 $(q^m-1)^\ell$ （逆）块乘子。

引理4。取 $k < n$，令 $\boldsymbol{a} \in \mathbb{F}_{q^m}^{\ell}$ 的元素属于 $\mathbb{F}_{q^m}$ 的互不相同的非平凡共轭类，并令 $\boldsymbol{x} \in \mathbb{F}_{q^m}^{n}$ 为一个满足 $\mathrm{wt}_{\Sigma R}(\boldsymbol{x}) = n$ 的向量。那么，广义 Moore 矩阵 $\mathfrak{M}_k(\boldsymbol{x})_{\boldsymbol{a}}$ 满足：

1. 加法码 $\mathcal{A} := \langle \mathfrak{M}_k(\boldsymbol{x})_{\boldsymbol{a}} \rangle + \langle \mathcal{D}_{\boldsymbol{a}}(\mathfrak{M}_k(\boldsymbol{x})_{\boldsymbol{a}}) \rangle$ 等于 $\langle \mathfrak{M}_{k+1}(\boldsymbol{x})_{\boldsymbol{a}} \rangle$，因此 $\dim(\mathcal{A}) = k+1$。2. 交码 $\mathcal{I} := \langle \mathfrak{M}_k(\boldsymbol{x})_{\boldsymbol{a}} \rangle \cap \langle \mathcal{D}_{\boldsymbol{a}}(\mathfrak{M}_k(\boldsymbol{x})_{\boldsymbol{a}}) \rangle$ 由矩阵 $\mathfrak{M}_{k-1}(\mathcal{D}_{\boldsymbol{a}}(\boldsymbol{x}))_{\boldsymbol{a}}$ 生成，因此 $\dim(\mathcal{I}) = k-1$。

证明。1. 令 $\boldsymbol{A} \in \mathbb{F}_{q^m}^{2k\times n}$ 表示将 $\mathfrak{M}_k(\boldsymbol{x})_{\boldsymbol{a}}$ 与 $\mathcal{D}_{\boldsymbol{a}}(\mathfrak{M}_k(\boldsymbol{x})_{\boldsymbol{a}})$ 纵向堆叠后得到的矩阵。由于 Moore 矩阵结构，$\mathcal{D}_{\boldsymbol{a}}(\mathfrak{M}_k(\boldsymbol{x})_{\boldsymbol{a}})$ 的前 $k-1$ 行与 $\mathfrak{M}_k(\boldsymbol{x})_{\boldsymbol{a}}$ 的最后 $k-1$ 行相同，因此我们得到

$$\mathcal{A} = \langle \boldsymbol{A} \rangle = \left\langle \begin{pmatrix} \mathfrak{M}_k(\boldsymbol{x})_{\boldsymbol{a}} \\ \mathcal{D}^k_{\boldsymbol{a}}(\boldsymbol{x}) \end{pmatrix} \right\rangle = \langle \mathfrak{M}_{k+1}(\boldsymbol{x})_{\boldsymbol{a}} \rangle.$$

此外，$k+1 \le n$ 成立，且 $\boldsymbol{a}$ 和 $\boldsymbol{x}$ 的必要条件适用，因此我们得到 $\dim(\mathcal{A}) = \mathrm{rk}_{q^m}(\mathfrak{M}_{k+1}(\boldsymbol{x})_{\boldsymbol{a}}) = \min(k+1, n) = k+1$。

2. 由于 $\mathfrak{M}_k(\boldsymbol{x})_{\boldsymbol{a}}$ 的最后 $k-1$ 行与 $\mathcal{D}_{\boldsymbol{a}}(\mathfrak{M}_k(\boldsymbol{x})_{\boldsymbol{a}})$ 的前 $k-1$ 行重合，因此它们的线性包 $\langle \mathfrak{M}_{k-1}(\mathcal{D}_{\boldsymbol{a}}(\boldsymbol{x}))_{\boldsymbol{a}} \rangle$ 必然包含于 $\mathcal{I}$ 中。注意，由于 $\mathcal{D}_a(\cdot)$ 的 $\mathbb{F}_q$ 线性，有 $\mathrm{wt}_{\Sigma R}(\mathcal{D}_{\boldsymbol{a}}(\boldsymbol{x})) = \mathrm{wt}_{\Sigma R}(\boldsymbol{x}) = n$ 成立，这意味着 $\mathrm{rk}_{q^m}(\mathfrak{M}_{k-1}(\mathcal{D}_{\boldsymbol{a}}(\boldsymbol{x}))_{\boldsymbol{a}}) = k-1$。因此，

$$\begin{aligned} \dim(\mathcal{I}) &= \mathrm{rk}_{q^m}(\mathfrak{M}_k(\boldsymbol{x})_{\boldsymbol{a}}) + \mathrm{rk}_{q^m}(\mathcal{D}_{\boldsymbol{a}}(\mathfrak{M}_k(\boldsymbol{x})_{\boldsymbol{a}})) - \dim(\mathcal{A}) \\ &= 2k - k - 1 = k - 1 \end{aligned}$$

并且 $\mathcal{I} = \langle \mathfrak{M}_{k-1}(\mathcal{D}_{\boldsymbol{a}}(\boldsymbol{x}))_{\boldsymbol{a}} \rangle$ 由维数相等性可得。

□

定义算子

$$\Gamma_{\boldsymbol{a}}^{j}: \quad \mathbb{F}_{q^m}^{k\times n} \to \mathbb{F}_{q^m}^{(j+1)k\times n}, \qquad \boldsymbol{M} \mapsto \begin{pmatrix} \boldsymbol{M} \\ \mathcal{D}_{\boldsymbol{a}}(\boldsymbol{M}) \\ \vdots \\ \mathcal{D}_{\boldsymbol{a}}^{j}(\boldsymbol{M}) \end{pmatrix}$$

对于固定的求值参数向量 $\boldsymbol{a} \in \mathbb{F}_{q^m}^{\ell}$ 和自然数 $j \in \mathbb{N}$。

推论 2。设 $\boldsymbol{G}$ 是 $\mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{a}$码的任意生成矩阵；$\boldsymbol{n}$，$k]$。那么，$\Gamma_{\boldsymbol{a}}^{j}(\boldsymbol{G})$生成 $\mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{a}$码；$\boldsymbol{n}$，$k+j]$ 并且对所有 $0 \le j \le n-k$，$\mathrm{rk}_{q^m}(\Gamma_{\boldsymbol{a}}^{j}(\boldsymbol{G})) = k+j$成立。

证明。 如果 $\boldsymbol{G} = \mathfrak{M}_k(\boldsymbol{\beta})_{\boldsymbol{a}}$，则这些结论由对引理4的迭代应用得到。在其他情况下，存在一个矩阵 $\boldsymbol{S} = (S_{i,\ j})_{i,\ j} \in \mathrm{GL}_k(\mathbb{F}_{q^m})$，使得 $\boldsymbol{G} = \boldsymbol{S} \cdot \mathfrak{M}_k(\boldsymbol{\beta})_{\boldsymbol{a}}$。

我们首先关注 j的最小非平凡取值，即 $j = 1$。$\mathcal{D}_{\boldsymbol{a}}(\boldsymbol{G})$ 的第 l 行 $= \mathcal{D}_{\boldsymbol{a}}(\boldsymbol{S} \cdot \mathfrak{M}_k(\boldsymbol{\beta})_{\boldsymbol{a}})$ 为

$$\begin{aligned} \mathcal{D}_{\boldsymbol{a}}\Big(\sum_{i=1}^{k} S_{l,i}\mathcal{D}_{\boldsymbol{a}}^{i-1}(\boldsymbol{\beta})\Big) &= \sum_{i=1}^{k} \mathcal{D}_{\boldsymbol{a}}(S_{l,i}\mathcal{D}_{\boldsymbol{a}}^{i-1}(\boldsymbol{\beta})) \\ &\overset{(*)}{=} \sum_{i=1}^{k} \sigma(S_{l,i})\mathcal{D}_{\boldsymbol{a}}^{i}(\boldsymbol{\beta}) + \delta(S_{l,i})\mathcal{D}_{\boldsymbol{a}}^{i-1}(\boldsymbol{\beta}), \end{aligned} \tag{5}$$

其中，$*$由引理 1 得出。但这是元素 $\boldsymbol{\beta}, \mathcal{D}_{\boldsymbol{a}}(\boldsymbol{\beta}) \ldots, \mathcal{D}_{\boldsymbol{a}}^{k}(\boldsymbol{\beta})$ 的 $\mathbb{F}_{q^m}$-线性组合，即 $\mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{a}; \boldsymbol{n}, k+1]$ 的一个基。因此，包含关系 $\langle \mathcal{D}_{\boldsymbol{a}}(\boldsymbol{G}) \rangle \subseteq \mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{a}; \boldsymbol{n}, k+1]$ 适用。由于 $\boldsymbol{G}$ 生成 $\mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{a}; \boldsymbol{n}, k] \subseteq \mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{a}; \boldsymbol{n}, k+1]$，进一步可得 $\langle \Gamma_{\boldsymbol{a}}(\boldsymbol{G}) \rangle \subseteq \mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{a}; \boldsymbol{n}, k+1]$。

我们来证明另一个包含关系 $\langle \Gamma_{\boldsymbol{a}}(\boldsymbol{G}) \rangle \supseteq \mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{a}; \boldsymbol{n}, k+1]$。首先注意到，$\langle \Gamma_{\boldsymbol{a}}(\boldsymbol{G}) \rangle \supseteq \langle \boldsymbol{G} \rangle = \mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{a}; \boldsymbol{n}, k]$ 以及 $\mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{a}; \boldsymbol{n}, k+1] = \mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{a}; \boldsymbol{n}, k] + \langle \mathcal{D}_{\boldsymbol{a}}^{k}(\boldsymbol{\beta}) \rangle$ 成立。因此，只需证明 $\langle \Gamma_{\boldsymbol{a}}(\boldsymbol{G}) \rangle$中存在一个元素，其 $\mathbb{F}_{q^m}$-线性组合包含 $\mathcal{D}_{\boldsymbol{a}}^{k}(\boldsymbol{\beta})$ 的非零倍数。但由于 $\boldsymbol{S}$ 满秩，其第 k 列中存在一个非零元素，记为 $S_{l^*,k}$。现在，由 (5) 可知，$\mathcal{D}_{\boldsymbol{a}}(\boldsymbol{G})$ 的第 l^* 行具有如下形式

$$\sigma(S_{l^*,k})\mathcal{D}_{\boldsymbol{a}}^{k}(\boldsymbol{\beta}) + \sum_{i=1}^{k-1} \sigma(S_{l,i})\mathcal{D}_{\boldsymbol{a}}^{i}(\boldsymbol{\beta}) + \delta(S_{l,i})\mathcal{D}_{\boldsymbol{a}}^{i-1}(\boldsymbol{\beta}),$$

其中右侧显然包含于 $\mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{a}; \boldsymbol{n}, k]$。由于当且仅当 $S_{l^*,k} \neq 0$ 时，$\sigma(S_{l^*,k})$ 非零，这表明 $\langle \mathcal{D}_{\boldsymbol{a}}(\boldsymbol{G}) \rangle \supseteq \langle \mathcal{D}_{\boldsymbol{a}}^{k}(\boldsymbol{\beta}) \rangle$，因此 $\langle \Gamma_{\boldsymbol{a}}(\boldsymbol{G}) \rangle \supseteq \mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{a}; \boldsymbol{n}, k+1]$。

综上，我们得到 $\langle \Gamma_{\boldsymbol{a}}(\boldsymbol{G}) \rangle = \mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{a}; \boldsymbol{n}, k+1]$，这直接推出 $\mathrm{rk}_{q^m}(\Gamma_{\boldsymbol{a}}(\boldsymbol{G})) = k+1$。

对于 $j > 1$，这些结果由以下事实归纳得出：

$$\langle \Gamma_{\boldsymbol{a}}^{j}(\boldsymbol{G})\rangle = \left\langle \begin{pmatrix} \Gamma_{\boldsymbol{a}}^{j-1}(\boldsymbol{G}) \\ \mathcal{D}_{\boldsymbol{a}}^{j}(\boldsymbol{G}) \end{pmatrix} \right\rangle \overset{(\circ)}{=} \langle \Gamma_{\boldsymbol{a}}(\Gamma_{\boldsymbol{a}}^{j-1}(\boldsymbol{G}))\rangle,$$

因为在步骤（$\circ$）中添加的所有行都已包含在 $\Gamma_{\boldsymbol{a}}^{j-1}(\boldsymbol{G})$ 的行空间中。由已知 $\langle \Gamma_{\boldsymbol{a}}^{j}(\boldsymbol{G})\rangle = \mathsf{LRS}[\boldsymbol{\beta}, \boldsymbol{a};\ \boldsymbol{n},\ k+j]$ 可得陈述 $_{q^m}(\Gamma_{\boldsymbol{a}}^{j}(\boldsymbol{G})) = k+j$；结合已知 $\Gamma_{\boldsymbol{a}}^{j-1}(\boldsymbol{G}) = \mathsf{LRS}[\boldsymbol{\beta}, \boldsymbol{a};\ \boldsymbol{n},\ k+j-1]$，即可得到 $j = 1$ 的证明。□

相比之下，在 $\mathbb{F}_{q^m}$ 上随机选取的满秩矩阵在应用 $\Gamma_{\boldsymbol{a}}$ 时往往表现得截然不同。这类似于 [20, 假设 2]。

猜想 1。设 $\boldsymbol{M} \in \mathbb{F}_{q^m}^{k\times n}$ 是一个随机选取的矩阵，具有满 $\mathbb{F}_{q^m}$-秩，并且对于 $i = 1, \ldots, \ell$，每个分块 $\boldsymbol{M}^{(i)}$ 在 $\mathbb{F}_q$ 上具有满列秩。假设 $\boldsymbol{a} \in \mathbb{F}_{q^m}^{\ell}$ 由 $\mathbb{F}_{q^m}$ 的不同非平凡共轭类的随机选取代表元组成，并固定参数 $j \in \{1, \ldots, n-k\}$。则，$\mathsf{rk}_{q^m}(\Gamma_{\boldsymbol{a}}^{j}(\boldsymbol{M})) = \min((j+1)k, n)$ 以高概率成立。

借助这些结果，如果已知 问题 2，那么当 σ、δ以及 $\boldsymbol{a}$ 已知时，我们可以在多项式时间内求解 LRS 码的问题。我们将其总结为 定理 4：

定理 4（Overbeck 类区分器）。设 $\boldsymbol{M} \in \mathbb{F}_{q^m}^{k\times n}$ 为任意满秩矩阵。在 $\mathbb{F}_{q^m}$ 中进行 $\mathcal{O}(n^5)$ 次运算，我们可以以高概率[2] 判定 $\boldsymbol{M}$ 是否生成关于 σ、δ 和 $\boldsymbol{a}$ 的 LRS 码。

证明。首先，选择一个 $0 \le j \le n-k$，使得 $k + j < \min((j+1)k, n)$ 成立。我们在 $\mathbb{F}_{q^m}$ 中通过 $\mathcal{O}(jkn) \subseteq \mathcal{O}(n^3)$ 次运算构造矩阵 $\Gamma_{\boldsymbol{a}}^{j}(\boldsymbol{M}) \in \mathbb{F}_{q^m}^{(j+1)k\times n}$。接下来，我们在 $\mathcal{O}(n^5)$ $\mathbb{F}_{q^m}$ 次运算中计算其秩。根据推论 2 和猜想 1，我们知道，如果 $\mathsf{rk}_{q^m}(\Gamma_{\boldsymbol{a}}^{j}(\boldsymbol{M})) = k+j$ 成立，则以高概率 $\boldsymbol{M}$ 生成关于给定参数的 LRS 码。然而，如果 $\mathsf{rk}_{q^m}(\Gamma_{\boldsymbol{a}}^{j}(\boldsymbol{M})) > k+j$，我们可以确定 $\boldsymbol{M}$ 不是关于给定参数的 LRS 码的生成矩阵。□

注 1. 我们通过模拟进行了实证验证：如果区分器针对另一组求值参数运行，那么在大多数情况下，它无法识别 LRS 码。即使已知求值参数 $\boldsymbol{a} = (a_1, \ldots, a_\ell)$ 的共轭类，而区分器使用的是其他代表元 $\hat{\boldsymbol{a}} := (a_1{}^{c_1}, \ldots, a_\ell{}^{c_\ell})$，其中 $c_1, \ldots, c_\ell \in \mathbb{F}_{q^m}^{*}$，情况仍然如此。

这意味着，即使掌握所选共轭类的旁信息，也无助于区分过程；要实现区分，必须知道确切的求值参数。如果无法获取这些信息，最坏情况下就必须尝试指数级数量的可能性。

[2] 事实上，区分器以概率 1 识别 GLRS 码。但它也可能以较小的概率错误地将非 GLRS 码判定为 GLRS 码。

本节余下部分将简要概述如何把采用 HMR 方法的区分器推广到 LRS 情形。给定一个满秩矩阵 $\boldsymbol{M} \in \mathbb{F}_{q^m}^{k\times n}$和参数 σ, δ以及 $\boldsymbol{a}$，我们将考察交码，而非如前文所述考察加法码。类似于 推论 2，我们可以得到 推论 3，为简洁起见，此处省略其证明。

推论 3。设 $\boldsymbol{G}$ 是 LRS$[\boldsymbol{\beta}, \boldsymbol{a}$ 的任意生成矩阵；$\boldsymbol{n}, k]$。那么，j 重交码 $\bigcap_{i=0}^{j}\langle \mathcal{D}_{\boldsymbol{a}}^{i}(\boldsymbol{M})\rangle$ 等于 LRS$[\mathcal{D}_{\boldsymbol{a}}^{j}(\boldsymbol{\beta})$ $\boldsymbol{a}$；$\boldsymbol{n}, k-j]$，因此对于所有 $0 \le j \le k-1$，其维数为 $\mathbb{F}_{q^m}$- $k-j$。

从启发式角度看，将 $\mathcal{D}_{\boldsymbol{a}}(\cdot)$作用于随机满秩矩阵，会产生另一个本质上随机的码。对于较小的维数 k，因此可以合理地假设，j重交码（来自推论 3）的维数要低得多。这说明为什么推论 3可以用作 LRS 码的区分器；当然，正如本节开头所述，它也可以用于 GLRS 码。

5 恢复典范生成矩阵

如果已知的只是 GLRS 码经过置乱、且可能进一步伪装的生成矩阵，那么恢复同一码的典范生成矩阵就是一项关键任务。典范生成矩阵揭示的秘密码结构（截至目前）与高效译码算法的知识直接相关。本节部分解决问题 3，并展示在自同构 σ 已知的情况下，如何恢复具有零导子的 GLRS 码。与区分器一样，以下结果也已在 SageMath 中实现，并针对多个参数集进行了检验。

第一种方法要求使用恒等自同构，并求出合适的求值参数 $\boldsymbol{a}$ 和块乘子 $\boldsymbol{v}$；第二种方法则假设已知 $\boldsymbol{a}$，并允许在自同构任意但已知的情况下恢复 $\boldsymbol{\beta}$。因此，若考虑相对于恒等自同构的 GLRS 码，我们便可结合这两种区分器，先恢复 $\boldsymbol{a}$ 和 $\boldsymbol{v}$，再恢复 $\boldsymbol{\beta}$。

5.1 平方码方法

对于这种方法，我们聚焦于仅允许零导子的恒等自同构。恢复策略基于这样一个事实：如第 4.1 小节所述，我们可以从 GLRS 码的任意生成矩阵中提取一个广义 Reed–Solomon 码。随后，我们恢复该广义 Reed–Solomon 码的参数，继而恢复 GLRS 码的参数。

定理 5. 设 $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k\times n}$ 表示一个 GLRS 码 $\mathcal{C}$ 的生成矩阵，其对应于恒等自同构和零导子。我们可以在 $\mathbb{F}_{q^m}$ 中通过 $\mathcal{O}$ 次 $k^2 n$ 运算恢复参数 $\boldsymbol{a}$、$\boldsymbol{v} \in \mathbb{F}_{q^m}^{\ell}$，使得 $\mathcal{C}$ 存在典范生成矩阵。

证明。回顾引理 3 可知，由生成矩阵 $\boldsymbol{G}$ 的每个分块中各取一列所组成的矩阵 $\boldsymbol{G}^{(i)}$ 生成一个长度为 ℓ 、维数为 k的广义 Reed–Solomon 码。若 $\ell > k$ ，则这是一个非平凡的广义 Reed–Solomon 码；而若 $\ell \leq k$ ，则该码为整个空间 $\mathbb{F}_{q^m}^{\ell}$。为描述恢复过程，我们将区分以下两种情况：

1. 在 $\ell \geq k$ 成立的情况下，我们可以直接选择求值点为 $\boldsymbol{a} = (1, \alpha, \alpha^2, \ldots, \alpha^{\ell})$，其中 $\alpha \in \mathbb{F}_{q^m}$为本原元。显然，具有这些参数的范德蒙矩阵是满秩的，因此其线性包为整个空间，即它是平凡 RS 码的生成矩阵。此外，$1, \alpha, \alpha^2, \ldots, \alpha^{\ell}$ 代表不同的共轭类（因为我们考虑的是零导子），因此是 LRS 码的一组有效选择。注意，在这种情形下，我们不需要考虑列乘子，即可以假设$\boldsymbol{v}$ 为全一向量。2. 在另一种情况下，即当 $\ell < k$时，所得的广义 Reed–Solomon 码及其对偶码均为非平凡码，即它们的最小距离都大于一。此时，我们可以对该广义 Reed–Solomon 码的校验矩阵应用 [25] 中的 Sidelnikov–Shestakov 算法，以找到合适的 $\boldsymbol{a}$ 和 $\boldsymbol{v} \in \mathbb{F}_{q^m}^{\ell}$。这需要在 $\mathbb{F}_{q^m}$中进行 $\mathcal{O}(k^2 n)$ 次运算。

□

根据代码在潜在密码系统中的伪装方式，攻击者可以利用 引理 3 中关于平方码余维的事实，来寻找公有码的合适子码。随后，可以将 定理 5 中的参数恢复算法应用于所获得的子码。

5.2 类 Overbeck 方法

在相关文献中，有三种不同的方法基于类似于 Overbeck 区分器的思想来恢复 Gabidulin 码的秘密参数：

1. Overbeck [20] 通过反复应用 Frobenius 自同构，计算所得各码的和，直至得到一个余维为一的码。随后，从一维对偶码的生成元中恢复秘密参数。
2. Horlemann-Trautmann、Marshall 和 Rosenthal [11] 计算通过反复应用 Frobenius 自同构得到的各码的交集，直至结果为一维码。后者的一个生成元即可给出该码的秘密参数。 3. Horlemann-Trautmann、Marshall 和 Rosenthal [10]提出的另一种方法，将该任务转化为：在由公钥矩阵和一个受损码字生成的码中寻找秩一码字。

我们介绍零导子情形下针对 LRS 码的前两种方法，此时自同构 σ 和求值参数 $\boldsymbol{a} \in \mathbb{F}_{q^m}^{\ell}$ 已知。请注意，第三种技术同样适用于我们的情形，但为简洁起见，此处略去。此外，通过先猜测块乘子，再执行这些恢复方法，也可将其扩展至 GLRS 码，这与 第 4.2 小节中介绍的区分策略类似。

定理 6. 设 $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k\times n}$为 LRS 码 $\mathcal{C} :=\mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{a};\ \boldsymbol{n}, k]$ 关于已知自同构 σ 和零导子的生成矩阵。若求值参数 $\boldsymbol{a} \in \mathbb{F}_{q^m}^{\ell}$ 已知，则我们可以恢复码定位元$\tilde{\boldsymbol{\beta}} \in \mathbb{F}_{q^m}^{n}$，使得 $\mathfrak{M}_k(\tilde{\boldsymbol{\beta}})_{\boldsymbol{a}}$ 在 $\mathbb{F}_{q^m}$中经 $\mathcal{O}(n^5)$ 次运算即可生成 $\mathcal{C}$。

˜证明。首先注意，任意 $\mathbb{F}_{q^m}^*$倍的 $\boldsymbol{\beta}$ $\boldsymbol{\beta}$ 都足够，因为

$$\mathfrak{M}_k(\tilde{\boldsymbol{\beta}})_a = \operatorname{diag}\left((c, \sigma(c), \ldots, \sigma^{k-1}(c))\right) \cdot \mathfrak{M}_k(\boldsymbol{\beta})_{\boldsymbol{a}}$$

˜对 $\boldsymbol{\beta}$: $= c \cdot \boldsymbol{\beta}$，其中 $c \in \mathbb{F}_{q^m}^*$，上述结论成立。由于对角矩阵满秩，˜ $\mathfrak{M}_k$ $(\boldsymbol{\beta})_{\boldsymbol{a}}$ 和 $\mathfrak{M}_k(\boldsymbol{\beta})_{\boldsymbol{a}}$ 的行空间均等于 $\mathcal{C}$。下面说明如何用上述三种方法中的前两种恢复这样的 ˜$\boldsymbol{\beta} \in \mathbb{F}_{q^m}^{n}$:

1. 由 推论 2，可得等式 $\langle \Gamma_{\boldsymbol{a}}^{n-k-1}(\boldsymbol{G})\rangle = \mathrm{LRS}[\boldsymbol{\beta}, \boldsymbol{a};\ \boldsymbol{n},\ n-1]$而该码的对偶码 $\mathcal{D}$ 的维数为一。方程组 $\boldsymbol{H} \in \mathbb{F}_{q^m}^{n}$ 的解 $\Gamma_{\boldsymbol{a}}^{n-k-1}(\boldsymbol{G}) \cdot \boldsymbol{H}^{\top} = \boldsymbol{0}$ 是 $\mathcal{D}$的生成矩阵（更确切地说，是生成向量）。由于我们处于零导子情形，可以利用关于 LRS 码对偶码的结果（1）˜，并通过（ $\boldsymbol{\beta}$ ）从 $\boldsymbol{H}$ 恢复合适的对象（2）。
2. 我们首先计算交空间 $\bigcap_{i=0}^{k-1}\langle \mathcal{D}_{\boldsymbol{a}}^{i}(\boldsymbol{G})\rangle$ ，根据$[\mathcal{D}_{\boldsymbol{a}}^{k-1}(\boldsymbol{\beta})\ \boldsymbol{a},\ \boldsymbol{n},\ 1]$ 它等于 LRS推论 3。因此，该空间的每个生成元$\boldsymbol{g} \in \mathbb{F}_{q^m}^{n}$ （尤其是我们计算得到的那个）都具有以下形式 $c \cdot \mathcal{D}_{\boldsymbol{a}}^{k-1}(\boldsymbol{\beta})$，其中 $c \in \mathbb{F}_{q^m}^*$。注意，在零导子情形下，对于固定的 $\mathcal{D}_a^i(\cdot$，算子 $a \in \mathbb{F}_{q^m}$ 和 $i \geq 0$ 的逆为

$$\left(\mathcal{D}_a^i\right)^{-1}(b) := \sigma^{-i}\left(\frac{b}{\mathcal{N}_i(a)}\right) \quad \text{for all } b \in \mathbb{F}_{q^m}.$$

我们利用这一事实，从 $\boldsymbol{g} = c \cdot \mathcal{D}_{\boldsymbol{a}}^{k-1}(\boldsymbol{\beta})$ 推导出以下方程:

$$\sigma^{-k+1}\left(\left(\frac{\boldsymbol{g}^{(1)}}{\mathcal{N}_{k-1}(a_1)} \mid \cdots \mid \frac{\boldsymbol{g}^{(\ell)}}{\mathcal{N}_{k-1}(a_\ell)}\right)\right) = \sigma^{-k+1}(c) \cdot \boldsymbol{\beta}.$$

˜求解得到的线性方程组，即可恢复一个合适的 $\boldsymbol{\beta}$。

在这两种情况下，复杂度都主要取决于分别计算 $\Gamma_{\boldsymbol{a}}^{n-k-1}(\boldsymbol{G})$ 和 $\Gamma_{\boldsymbol{a}}^{k-1}(\boldsymbol{G})$ 的简化行阶梯形。这可以在 $\mathbb{F}_{q^m}$ 中用 $\mathcal{O}(n^5)$ 次运算完成。□

6 结论

我们将 GLRS 码定义为具有非零块乘子的 LRS 码，并针对这一码族提出了两种区分器，其灵感来自汉明度量和秩度量中的类似技术。对于恒等自同构和零导子，平方码区分器可以发挥作用；而 Overbeck 式区分器则能够处理任意自同构和导子。当自同构 σ、导子 δ 以及在

后一种情况下额外已知求值参数 a 和块乘子 v时，两种区分器的运行时间均为多项式级。

由于许多 McEliece 类密码系统采用等距伪装，我们进一步研究了与 GLRS 码半线性等价的码。我们证明，对于固定的自同构以及导子的某些可能取值，GLRS 码在半线性等价下封闭。

最后，我们部分解决了在零导子情形下，如何从 GLRS 码的任意生成矩阵恢复其典范生成矩阵（从而找到高效译码器）的问题。如果已知 σ =Id 或 σ、v 和 a，则复杂度仍为多项式级。更具体地说，我们证明，在恒等自同构情形下，平方码方法能够恢复 GLRS 码的适当求值参数 a 和块乘子 v；对于任意自同构和零导子，如果已知 a 和 v，类似 Overbeck 的策略能够恢复 GLRS 码的适当码定位元 β。

这项工作是朝着构建基于和秩度量的抗量子密码系统迈出的第一步。自然，这一领域还引出了许多其他研究问题：正如模拟所示，若使用了错误的求值参数，类似 Overbeck 的区分器似乎不起作用。即使参数选自正确的共轭类，情况依然如此，因此值得对此进行研究。另一个思路是寻找一种新的运算，使平方码区分器在任意自同构下也能发挥作用。

我们还希望进一步研究其他区分方法，例如扩展生成矩阵或应用近等距变换，并考察 GLRS 码及其区分器如何推广到斜度量中。

参考文献。

1 Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D.：《NIST 后量子密码标准化进程第三轮状态报告》（2022）2. Alfarano, G.N., Lobillo, F.J., Neri, A., Wachter-Zeh, A.：和秩乘积码及最小距离界。《有限域及其应用》80, 102013（2022）3. Barra, A., Gluesing-Luerssen, H.：Frobenius 环上码的 MacWilliams 延拓定理与局部-全局性质。《纯粹与应用代数杂志》219(4)，703–728（2015）4. Berger, T.P., Loidreau, P.：如何掩盖用于密码学的码的结构。《设计、编码与密码学》35(1)，63–79（2005）5. Caruso, X.：斜有理函数的留数与线性化 Goppa 码。arXiv 预印本 arXiv:1908.08430v1（2019）6. Caruso, X., Durand, A.：线性化 Reed–Solomon 码的对偶码。《设计、编码与密码学》（2022）7. Castryck, W., Decru, T.：针对 SIDH 的高效密钥恢复攻击（预备版本）。密码学电子印刷档案 ia.cr/2022/975（2022）8. Gabidulin, E.M., Paramonov, A.V., Tretjakov, O.V.：非交换环上的理想及其在密码学中的应用。载于：密码学进展——EUROCRYPT ’91。第 482–489页（1991）

9. Gabidulin, E.M.：针对 GPT 公钥密码系统的攻击与反攻击。《设计、编码与密码学》48(2)，171–177（2008）10. Horlemann-Trautmann, A.L., Marshall, K., Rosenthal, J.：基于秩的密码系统的若干考量。载于：2016年 IEEE 国际信息论研讨会。第2544–2548页（2016）11. Horlemann-Trautmann, A.L., Marshall, K., Rosenthal, J.：针对基于 Gabidulin 码的密码系统的 Overbeck 攻击扩展。《设计、编码与密码学》86(2)，319–340（2018）12. Lam, T.Y., Leroy, A.：除环上的 Vandermonde 矩阵与朗斯基矩阵。《代数学杂志》119(2)，308–336（1988）13. Lu, H.f., Kumar, P.V.：具有最优速率-分集权衡的空时码统一构造。《IEEE 信息论汇刊》51(5)，1709–1730（2005）14. Mart´ınez-Pe˜nas, U.：任意除环上的斜码与线性化 Reed–Solomon 码及最大和秩距离码。《代数学杂志》504，587–612（2018）15. Mart´ınez-Pe˜nas, U.：和秩度量的汉明码与单纯形码。《设计、编码与密码学》88(8)，1521–1539（2020）16. Mart´ınez-Pe˜nas, U., Kschischang, F.R.：使用线性化 Reed–Solomon 码实现可靠且安全的多轮网络编码。《IEEE 信息论汇刊》65(8)，4785–4803（2019）17. McEliece, R.J.：基于代数编码理论的公钥密码系统。《深空网络进展报告》42-44，114–116（1978）18. Neri, A.：扭曲线性化 Reed-Solomon 码：斜多项式框架。《代数学杂志》609，792–839（2022）19. Overbeck, R.：基于 Gabidulin 码的公钥密码系统的结构攻击。《密码学杂志》21(2)，280–301（2007）20. Overbeck, R.：针对 GPT 及其变体的一种新型结构攻击。载于：密码学进展——Mycrypt 2005。第50–63页（2005）21. Overbeck, R.：基于编码理论的公钥密码学。博士论文，达姆施塔特工业大学（2007）22. Puchinger, S., Renner, J., Rosenkilde, J.：和秩度量中的通用译码。载于：2020年 IEEE 国际信息论研讨会。第54–59页（2020）23. Rashwan, H., Gabidulin, E.M., Honary, B.：一种基于秩码的 GPT 密码系统的巧妙方法。载于：2010年 IEEE 国际信息论研讨会。第2463–2467页（2010）24. Schmidt, G., Sidorenko, V., Bossert, M.：使用移位寄存器综合译码超出最小距离一半的 Reed–Solomon 码。载于：2006年 IEEE 国际信息论研讨会。第459–463页（2006）25. Sidelnikov, V.M., Shestakov, S.O.：论基于广义 Reed–Solomon 码的密码系统的不安全性。《离散数学及其应用》2(4)（1992）26. Stein, W.A., 等：Sage 数学软件（9.7 版）。Sage 开发团队（2022），http://www.sagemath.org 27. Wieschebrink, C.：对一种修改后的 Niederreiter 加密方案的攻击。载于：公钥密码学国际研讨会。第14–26页（2006）28. Wieschebrink, C.：基于 GRS 子码的 Niederreiter 公钥方案的密码分析。载于：后量子密码学国际研讨会。第61–72页（2010）