arXiv:2602.01464v1 [math.AG] 1 Feb 2026

曲面上的分层局部可恢复码

CAROLINA ARAUJO[1],LUANA COSTA[1], BETH MALMSKOG[2], JORGE MELLO[3], ELIZA MENEZES[1],CEC´ILIA SALGADO[4], 和 LARA VICINO[4]

Abstract. 我们构造了由 $\mathbb{A}^3$ 上的曲面得到的具有层次结构的局部可恢复码，这些曲面允许由阿廷-施赖埃尔型或库默尔型曲线构成的纤维化。我们利用纤维化的几何与算术性质推导出这些码的参数；该纤维化通过投影到其中一个坐标上得到。作为附带结果，我们估计了某些曲面族中有理点的数量，并在一种情况下给出了明确计数。

关键词：局部可恢复码、层次结构、纤维化曲面、阿廷-施赖埃尔曲线、库默尔曲线数学主题分类代码：11G20, 14G50, 94B27

1. Introduction

纠错码提供了一种方法，可以将精心设计的冗余融入需要存储或通过可能存在噪声的信道传输的信息中，从而纠正错误或恢复丢失的信息。不同的用途需要具备不同能力的码。云存储应用面临着独特的挑战：服务器可能经常整体发生故障或无法使用，因此，完全存储在单台服务器上的信息有彻底消失的风险，无论单个码字中加入了多少冗余。仅为每台服务器备份，就会使存储开销至少翻倍，因此，更理想的做法是找到一种更高效的方式，将每条信息分散存储到多台服务器上，以便从其他服务器恢复任何丢失的数据。局部可恢复码 （LRC）是一类纠错码，具有这样的性质：如果码字中的任意一个符号被擦除，就可以利用另一组规模相对较小的码符号来恢复丢失的值。这组符号称为该擦除位置的恢复集 。LRC 于 [10] 年提出，近年来得到了广泛研究。具有层次结构 的 LRC（有时简称为 HLRC）为每个位置提供第二个规模更大的恢复集，这可能有助于恢复更多的擦除。HLRC 首次于 [13], 年提出，是为局部恢复制定“备用方案”的一种方式，因此，即使少数位置被擦除，也无需访问码字中的大多数符号即可修复。

有限域上曲线和高维簇丰富的几何与代数结构，自然可以导出具有局部性和层次结构等结构的代数簇上的求值码。代数曲线一直是若干有趣构造中的关键组成部分，包括局部可恢复码（例如见 [15, 16, 17]）、分层局部可恢复码（例如见 [3] 和 [9]），以及具有可用性的局部可恢复码（例如见 [8]）。尽管曲面上的码已得到广泛研究，其中也包括一些关于由曲面构造局部可恢复码的工作（例如见 [2, 11, 1, 12]），但曲面的潜力，尤其是那些允许沿含有许多 $\mathbb{F}_q$-点的曲线纤维化的曲面，自然生成分层局部可恢复码的潜力，直到最近才在文献中显现，并由 [5] 开创。曲线的直积是自然的例子

[1]IMPA, Estrada Dona Castorina 110, 22460-320 Rio de Janeiro, Brazil
[2]Colorado College Department of Mathematics and Computer Science, Colorado Springs, Colorado USA
[3]Department of Mathematics and Statistics, Oakland University, Michigan, USA
[4]Faculty of Science and Engineering - Bernoulli Institute, University of Groningen, Groningen 9747AG, TheNetherlands

E-mail addresses: caraujo@impa.br, luana.costa@impa.br, bmalmskog@colroadocollege.edu, jorgedemellojr@oakland.edu, elizabeth.menezes@impa.br, c.salgado@rug.nl, l.vicino@rug.nl.

，它们是允许纤维化的曲面；考虑更一般的纤维化，则会拓宽可能性范围，并提供更多例子。

我们的出发点是形如 $\mathcal{S}$：$h(y) = f(x, z) \subset \mathbb{A}^3_{(x,y,z)}$ 的仿射曲面，其中对某个变量进行特殊化（例如取 z），可得到一族曲线 $\mathcal{Z}_\gamma$：$h(y) = f(x, \gamma)$，且这些曲线上有许多 $\mathbb{F}_q$ 点。码的求值点由 T 的一个精心选取的子集给出，该子集取自 S 的 $\mathbb{F}_q$ 有理点集。接着，我们考虑由多项式 $g(x, y, z)$ 构成的向量空间 V，并对 x、y 和 z 中的次数施加适当的界，以及求值映射 $V \to \mathbb{F}_q^n$，其中 $n = |T|$。虽然求值集的选择和向量空间的构造自然是在仿射情形下进行的，但为了在每条曲线 $\mathcal{Z}_\gamma$ 上应用贝祖定理并估计最小距离，我们使用了 $\mathcal{S}$ 在 $\mathbb{P}^2_{(x:y:w)} \times \mathbb{A}^1_z$ 中的（部分）紧化。

更具体地说，我们考虑 $\mathcal{S}$ 的如下形式的方程

- $y^p - y = f(x, z)$，其中 p 是素数，q 是 p 的幂，而 $f(x, z)$ 是一个多项式；或者
- $y^m = f(x, z)$，其中 $\gcd(q, m) = 1$，$\mathbb{F}_q$ 含有一个本原 $m-$ 次单位根，并且 $f(x, z)$ 是一个多项式。

在第一种情形下，由某个 $\gamma \in \mathbb{F}_q$ 的 $y^p - y = f(x, \gamma)$ 定义的曲线 $\mathcal{Z}_\gamma$ 通常是一条阿廷-施赖埃尔曲线，其射影闭包是射影直线的一个次数为 p 的伽罗瓦覆盖。在第二种情形下，由 $y^m = f(x, \gamma)$ 定义的曲线 $\mathcal{Z}_\gamma$ 通常是一条库默尔曲线，其射影闭包是射影直线的一个循环次数为 m 的伽罗瓦覆盖。对于我们的应用而言，这些都是极佳的曲线族，因为这些曲线族中曲线的结构使我们能够合理地计数其 $\mathbb{F}_q$-有理点。

本文将详细讨论这两类曲面，并分别给出一个具有明确方程的具体例子（见第 4 节和第 6 节）。我们注意到，这两个具体例子都呈现出特殊的几何特征。在第 4 节讨论的特殊阿廷-施赖尔构造中，相应曲面的射影化包含无穷远直线，即 $\{x = w = 0\}$ 和 $\{z = w = 0\}$。上文所述的纤维化，即关于变量 z 的特殊化，对应于从直线 $\{z = w = 0\}$ 出发的投影所给出的有理映射 $\mathbb{P}^3 \dashrightarrow \mathbb{P}^1$。也可以从另一条无穷远直线 $\{x = w = 0\}$ 投影，从而在同一曲面上得到另一个由阿廷-施赖尔曲线构成的纤维化。在第二个例子（第 6 节）中，该曲面是某条由厄米特曲线覆盖的曲线上的仿射锥，其方程关于 x 和 z 对称。关于变量 x 的特殊化会在同一曲面上给出另一个由库默尔曲线构成的纤维化。

1.1. **文章概要**。 在第2节中，我们介绍求值码和分层局部可恢复码的相关背景，以及本文将用到的代数几何与函数域理论中的基本概念。在第3节中，我们介绍一种在具有阿廷–施赖尔纤维的曲面上构造分层局部可恢复码的一般方法，并明确给出其参数的界。在第 4 节中，我们在本文框架下讨论一个来自 [5] 的具体例子。类似地，在第 5 节中，我们介绍一种在具有 Kummer 纤维的曲面上构造分层局部可恢复码的一般方法，并在第 6 节中研究一个具体例子。由于我们运用有趣的几何论证，对一类新的曲面进行了点数统计，因此这项工作本身也具有独立的研究价值。

2. Notations and background

在本文中，设 p 是素数，$q = p^h$，其中整数 $h > 0$，且 $\mathbb{F}_q$ 是含有 q 个元素的有限域。用 $\mathbb{F}_q^*$ 表示其乘法群。对于正整数 $n \in \mathbb{Z}_{>0}$，记 $[n] := \{1, ..., n\}$。

2.1. **码**。 首先，我们回顾编码理论中的一些概念。

定义 2.1. 若 $x = (x_1, x_2, \ldots, x_n)$ 和 $y = (y_1, y_2, \ldots, y_n)$ 是 $\mathbb{F}_q^n$ 中的向量，则它们的汉明距离是整数 $d(x, y) := |\{i : x_i \neq y_i\}|$，等于它们不同分量的数量。向量 $x \in \mathbb{F}_q^n$ 的汉明重量 $w(x)$ 是其非零分量的数量，即 $w(x) := d(x, 0)$，而子集 $S \subseteq \mathbb{F}_q^n$ 的最小距离为 $d(S) := \min\{d(x, y) : x \neq y \text{ in } S\}$.

定义 2.2。设 $n, k, d \in \mathbb{Z}_{>0}$，满足 $k, d \leq n$。域 $\mathbb{F}_q$ 上长度为 n、维数为 k、最小距离为 d 的线性码 C，是 $\mathbb{F}_q^n$ 的一个 $\mathbb{F}_q$-线性子空间，其维数 $C = k$，且 $d(C) = d$。我们称 C 为一个 $[n, k, d]$-码，其元素称为码字。

注意，作为向量空间，C 的最小距离等于其最小汉明重量，即 $d = \min\{d(x, 0) : 0 \neq x \in C\}$. 此外，我们可以通过将 C 限制到码位置的一个子集，得到一个新的码。

定义 2.3。若 $I = \{a_1, a_2, \ldots, a_{n_1}\} \subseteq [n]$，其中 $n_1 \leq n$ 且对所有 $i \in [n_1]$均有 $a_i < a_{i+1}$，则定义码字 x 在 I 上的删 *puncture* 为 $x_I = (x_{a_1}, x_{a_2}, \ldots, x_{a_{n_1}})$，并定义 C 在 I 上的删 *puncture* 为 $C_I = \{x_I : \ x \in C\}$。我们称$I$为 C_I相对于 C 的支撑集，并记作Supp C_I。

在文献中，术语“删 puncture”有时意味着所得的码与原码具有相同的维数。这里我们不作此假设。不难看出，C_I 对$[n, k, d]$-码 C进行删 puncture 后仍是线性码，并且 C_I是一个 $[n_1, k_1, d_1]$-码，具有 $n_1 \leq n$、$k_1 \leq k$和 $d_1 \leq d$。删 punct 码的概念是局部可恢复码的核心。

定义 2.4 ([10]). 设 $n, r, \rho \in \mathbb{Z}_{>0}$。一个长度为 n、定义在 $\mathbb{F}_q$ 上的线性码 C，若对于每个 $i \in [n]$，都存在一个长度至多为 $r + \rho - 1$、最小距离至少为ρ的删 *punct* 码 C_i，使得 C_i 的支撑集包含 i，则称其为(r, ρ)局部可恢复码。C_i 的支撑集和Supp $C_i \setminus \{i\}$ 分别称为位置 i 的修复组和恢复集。有时我们称 C 具有(r, ρ)局部性。

注意，对于所有 $j \in$，Supp C_i 都是 C_i 的修复组；删 punct 码的维数至多为 r，因为只需知道 r 个坐标，就足以确定其余坐标。这个局部可恢复码的定义推广了引言中的思路，允许在任意修复组内恢复 $\rho - 1$ 个擦除。单擦除的情形由 $\rho = 2$ 覆盖。这里要注意，r 是下层码 C_i 的维数，而 ρ 是其最小距离。

具有层次结构的局部可恢复码最早在 [13]中得到研究。我们在此给出那里引入的HLRC码的定义，并略作修改。

定义*2.5*（[13]）。设 $n, n_1, n_2, k, k_1, k_2, d, d_1, d_2 \in \mathbb{Z}_{>0}$满足 $n_2 < n_1 \leq n$, $k_2 \leq k_1 \leq k$且 $d_2 < d_1 \leq d$。线性 $[n, k, d]$-码 C称为具有局部参数$((n_1, k_1, d_1), (n_2, k_2, d_2))$的分层局部性，如果对每个 $i \in [n]$，存在一个删 *punct* 码$C_{1,i}$，其长度至多为 n_1，维数$C_{1,i} \leq k_1$ 且最小距离 $d(C_{1,i}) \geq d_1$，并满足 $i \in$ *Supp*$C_{1,i}$，使得$C_{1,i}$具有(k_2, d_2)-局部性，其修复组的大小至多为 n_2。我们用$C_{2,i}$ 表示$C_{1,i}$ 在其关于位置 i的修复组上的删 *puncture*，从而$C_{2,i}$ 的长度至多为 n_2，维数$C_{2,i} \leq k_2$, $d(C_{2,i}) \geq d_2$ 且 $i \in$ *Supp* $C_{2,i}$。

具有分层局部性的局部可恢复码称为HLRC码。

注 2.6. 我们将 n_1 和 n_2 列为相应码长度的上界，以涵盖不同位置具有不同大小恢复组的情形。对于任意位置，较小恢复组的最大大小为 n_2，而删 *punct* 码$C_{1,i}$对任意 i 的最大长度为 n_1。

注 2.7. 在全文中，我们将定理 *2.5* 中的码 $C_{1,i}$（分别是 $C_{2,i}$）称为位置 i的中间（分别是较低）码 。我们选择这一术语，虽然它不同于 [13], ，但更便于在文中进行讨论；这一点在本文后续各节中将会明了。

我们在本小节末回顾簇 $\mathcal{S}$ 上 $\mathbb{F}_q$的求值码定义，因为本文讨论的正是这类码。

定义 2.8. 设 $\mathcal{S}$ 是 $\mathbb{F}_q$ 上的一个拟射影簇。考虑 $\mathcal{S}(\mathbb{F}_q)$ 中由点组成的集合 $T = \{P_1, \ldots, P_n\}$，以及函数域 $\mathbb{F}_q(\mathcal{S})$ 中的一个 $\mathbb{F}_q$-向量空间，其函数在 T 中没有极点。V 在 T 上的求值码 是 $\mathbb{F}_q$-向量空间

$$C(T, V) \coloneqq \{(f(P_1), \ldots, f(P_n)) : f \in V\} \subseteq \mathbb{F}_q^n.$$

换言之， $C(T,V)$ 定义为求值映射 $ev_T\colon V \to \mathbb{F}_q^n$ 的像，其中对每个 $f \in V$，$ev_T(f) := (f(P_1)\ldots, f(P_n))$。

请注意，定理 2.8 中定义的码属于代数几何（AG）码，因为它们是通过在代数簇的点上对该簇函数域中的函数求值而得到的。

2.2. **代数几何工具**。 本文中，定义我们所构造的码的求值集由仿射空间 $\mathbb{A}^3_{(x,y,z)}$ 中的曲面上的点组成，其坐标为 (x, y, z)。然而，本研究的一个重要目的是使用射影空间，并在无穷远点处对函数求值，以改进码参数。对于 $\gamma \in \mathbb{F}_q$，我们将 $\mathbb{A}^3_{(x,y,z)}$ 中的平面 $z = \gamma$ 视为二维仿射空间 $\mathbb{A}^2_{(x,y)}$，并称其为 $\mathbb{A}^2_\gamma$。随后，我们取 $\mathbb{A}^2_\gamma$ 的射影闭包，记为 $\mathbb{P}^2_\gamma$，并使用齐次坐标 $(x\colon y\colon w)$。另一项基本工具是考察投影映射的纤维。为表示这些映射，我们使用 π，下标表示其投影到的坐标。例如，定义

$$\pi_x : \mathbb{A}^3_{(x,y,z)} \to \mathbb{A}^1_x \qquad\qquad \pi_{x,z} : \mathbb{A}^3_{(x,y,z)} \to \mathbb{A}^2_{(x,z)}$$
$$(\alpha,\beta,\gamma) \mapsto \alpha \qquad\qquad (\alpha,\beta,\gamma) \mapsto (\alpha,\gamma)$$

研究 $\mathbb{P}^2_\gamma$ 时，一些基础的交理论会很有用。以下定义和定理均出自 [6,第 5 节。14]。

定义 *2.9.* 设 K 为任意域。考虑两条平面曲线 $C, D \subset \mathbb{P}^2(K)$，其交 $X = C \cap D$ 的维数为 0。令 $\Gamma(X, \mathcal{O}_X)$ 表示 X 上结构层 $\mathcal{O}_X$ 的整体截面空间。则称 $i(C, D) := \dim_K \Gamma(X, \mathcal{O}_X)$ 为 C 与 D 的相交数。对于 $P \in X$，称 $i_P(C, D) := \dim_K \mathcal{O}_{X,P}$ 为 C 与 D 在 P 处的相交数，其中 $\mathcal{O}_{X,P}$ 表示 X 在 P 处的局部环。

备注 2.10. 注意，$\dim X = 0$ 当且仅当 C 和 D 由没有公因子的齐次多项式给出。在这种情况下，我们有

$$i(C, D) = \sum_{P \in X} i_P(C, D).$$

定理 2.11 (B´ezout)。 若 C 和 D 是 $\mathbb{P}^2(K)$中的平面曲线，分别由齐次多项式 g 和h 定义，且没有公因子，则 $i(C, D) =$(次数 g)(次数 h)。

2.3. **阿廷-施赖埃尔与库默尔覆盖**。 本小节简要回顾单变量函数域中的一些概念，因为本文大量使用两类特殊的伽罗瓦函数域扩张。关于单变量函数域理论的全面阐述，请参阅 [14]。

设 K 是任意完全域， x是 K上的一个超越元。 K上的单变量代数函数域 F/K 通常简称为函数域，是 $K(x)$的有限扩张。域 K 称为 F的常数域；当其含义明确时，我们通常用 F 代替 F/K。现在设 Φ 是一个包含 F的固定代数闭域，并设 F'/K'是另一个满足 $\Phi \supseteq F'$的函数域。

若 F'/K'是 F/K的代数扩张，则称函数域 F'/K'为 F/K的代数扩张，其中 $F' \supseteq F$是代数域扩张，且 $K' \supseteq K$。与 [14], 中一样，我们采用 F'/F 这一记号表示函数域扩张。

函数域 F/K 的一个基本不变量是其亏格 g，它等于 F的正则微分空间作为 K上向量空间的维数。注意，这也正是 F的任意典范除子所对应的黎曼-罗赫空间的维数。

相对于其亏格而言拥有大量有理位的函数域一直以来都是文献中广泛研究的对象，这不仅因为它们是特别有趣的极值对象，也因为它们可用于构造参数良好的求值码（代数几何码）。著名的 Hasse-Weil 界给出了有限域 $\mathbb{F}_q$ 上函数域有理位数量的下界和上界。

定理 2.12（Hasse-Weil 界）。设 $F/\mathbb{F}_q$ 是有限域 $\mathbb{F}_q$ 上亏格为 g 的函数域。F 的 $\mathbb{F}_q$-有理位数量 $N(F)$ 满足不等式

$$|N(F)-(q+1)| \leq 2g\sqrt{q}.$$

亏格为 g 的函数域 $F/\mathbb{F}_q$ 若满足 $N(F) = q+1+2g\sqrt{q}$，则称为极大。与极大函数域相关联的（非奇异）代数曲线也称为极大曲线。

例 2.13。极大函数域中最著名的例子之一是厄米特函数域，即厄米特曲线的 $\mathbb{F}_{q^2}$-有理函数域。

考虑由仿射方程 $y^{q+1} = x^q + x$ 在 $\mathbb{F}_{q^2}$ 上给出的厄米特曲线 $\mathcal{H} \subseteq \mathbb{A}^2_{(x,y)}$ 的仿射模型。$\mathcal{H}$ 的 $\mathbb{F}_{q^2}$-有理函数域为 $H := \mathbb{F}_{q^2}(x,y)$，其中 $y^{q+1} = x^q + x$；它是亏格为 $g = q(q-1)/2$ 的极大函数域，定义在 $\mathbb{F}_{q^2}$ 上。

现在我们回顾两种特殊类型的伽罗瓦函数域扩张的定义，并引入库默尔型和阿廷-施赖埃尔曲面的术语，全文均使用这两个术语。

定义 2.14。设 λ 为自然数。设 F/K 为代数函数域，其中 K 包含一个本原 λ 次单位根（且 $n>1$ 和 n 与 K的特征互素）。假设 $u \in F$是满足以下条件的元素：对于所有 $w \in F$和 $d|\lambda$， $u \neq w^d$， $d>1$。设 $F' = F(y)$，其中 $y^\lambda = u$。则称 F'/F为 F的库默尔扩张。

定理 2.15 ([14 ，命题 3.7。3])。沿用上述记号，设 F'/F是 F的库默尔扩张。

- 扩张 F'/F是伽罗瓦扩张，其次数为 n，最小多项式为 $T^\lambda - u$。伽罗瓦群是循环群， F'/F 的自同构由 $\sigma(y) = \zeta y$给出，其中 $\zeta \in K$ 是一个 λ 次单位根。
- 设 P 是 F 的一个位，且 P' 是位于 P 上方的 F' 的一个位。那么 P' 的分歧指数为 $e(P'|P) = \frac{\lambda}{r_P}$，不同指数为 $d(P|P') = \frac{\lambda}{r_P} - 1$，其中 $r_P := \gcd(\lambda, v_P(u))$。

若 F 的特征与 λ 互素，且 F 包含一个本原 λ 次单位根，则 F 的所有循环伽罗瓦 λ 次扩张都是库默尔扩张。

若 $F = K(x)$ 是有理函数域，且 $u = f(x) \in F$ 满足上述条件，则具有仿射模型 $y^\lambda = f(x)$ 的曲线 C 称为库默尔曲线，相应诱导的覆盖映射 $C \to \mathbb{P}^1_x$ 称为 *Kummer* 覆盖。

注意， C 上方恰有 λ 个不同的点位于 $\mathbb{P}^1_x$ 的任意一个非分歧点之上；并且，考虑到 $\zeta \in K$，若这些点中任意一个定义在 K 的某个给定扩张上，则它们全部都定义在该扩张上。

若 $F = K(x, z)$ 是 $\mathbb{P}^2_{x,\,z}$的函数域，且 $u = f(x, z)$ 满足上述条件，则函数域为 F'、仿射模型为 $y^\lambda = f(x, z)$ 的曲面S称为 *Kummer*型曲面。

定义 2.16. 设 F/K 是特征为 $p>0$ 的代数函数域。假设 $u \in F$ 是一个满足以下条件的元素：对所有 $w \in F$，都有 $u \neq w^p - w$，且 $F' = F(y)$，其中 $y^p - y = u$。那么 F'/F 称为 F 的 *Artin-Schreier*扩张。

定理 2.17 ([14, 命题 3.7.8]). 沿用上述记号，设 F'/F 是一个 *Artin-Schreier*扩张。对 F 的每一个位 P，定义 $m_P := m$，若存在某个 $z \in F$ 满足 $v_P(u-(z^p-z)) = -m < 0$，且 $m \not\equiv 0 \pmod p$；否则定义为 $m_P := -1$，也就是说，若对某个 $z \in F$ 有 $v_P(u-(z^p-z)) \geq 0$。

- 扩张 F'/F是次数为 p 的伽罗瓦扩张。 F'/F的自同构由 $\sigma(y) = y+\nu$给出，其中 $\nu = 0$、1、.....、$p-1$。

F的位 P在该扩张中非分歧，当且仅当对于某个 $z \in F$，有 $v_P(u-(z^p-z)) \geq 0$。

位 P完全分歧，当且仅当存在满足 $v_P(u-(z^p-z)) < 0$ 的 $z \in F$

若 F 的特征为 p，则任何次数为 p 的循环域扩张都是 Artin-Schreier扩张。

当 $F = K(x)$ 是有理函数域，且 $u = f(x) \in F$ 满足上述条件时，具有仿射模型 $y^p - y = f(x)$ 的曲线 C 称为 阿廷-施赖埃尔曲线，其诱导的覆盖映射 $C \to \mathbb{P}^1_x$ 称为 阿廷-施赖埃尔覆盖。

注意，考虑到阿廷-施赖尔自同构，在覆盖中， $\mathbb{P}_x^1$ 的任一非分歧点上方恰有 p 个 C 的点；如果这些点中任意一个定义在 $\mathbb{F}_p$ 的某个给定扩域上，那么所有这些点都定义在该扩域上。

若 $F = K(x,z)$ 是 $\mathbb{P}^2_{x,z}$ 的函数域，且 $u = f(x,z) \in F$ 满足上述条件，那么函数域为 $F' = F(y)$、仿射模型为 $y^p - y = f(x,z)$ 的曲面 S 称为阿廷-施赖尔曲面。

我们的研究对象是具有阿廷-施赖埃尔曲线和库默尔曲线纤维化的曲面。由阿廷-施赖埃尔曲线和库默尔曲线构造的码已得到广泛研究，但其高维类似物的研究仍相对不足。在 [5], 中，作者提出了一种新颖的方法，利用几何以及曲面到曲线的纤维化，为码赋予局部性和层次结构。他们的框架允许我们在拟射影框架下研究曲面，从而改进 HLRC 码的最小距离。

3. Codes on Artin-Schreier surfaces

本节介绍一种从阿廷-施赖埃尔曲面构造分层局部可恢复码的方法。我们采用的方法重新审视了 [5], 中的方法，并为所得码的最小距离给出了一个非平凡下界；在某些假设下，该下界优于 [5] 中的界。当我们的界不更优时，我们仍能得到 [5] 中的界。

3.1. 码构造：一种拟射影方法。 令 $q := p^h$ 为某个素数 p 的正幂。考虑由下式定义的 $\mathbb{A}^3_{(x,y,z)}$ 中的曲面

$$\mathcal{S}_f : y^p - y - f(x,z) = 0, \tag{3.1}$$

其中 $f \in \mathbb{F}_q[x,z]$ 是一个满足 $\deg_x f \geq p+1$ 的多项式，并且对于任意 $g(x,z) \in \mathbb{F}_q(x,z)$，均有 $f(x,z) \neq \overline{g}(x,z)^p - g(x,z)$。此外，对于 $\gamma \in \mathbb{F}_q$，定义簇

$$\mathcal{Z}_\gamma := \begin{cases} y^p - y - f(x,z) = 0 \\ z - \gamma = 0 \end{cases}, \tag{3.2}$$

它是 $\mathcal{S}_f$ 与平面 $\mathbb{A}^2_\gamma$ 在 $\mathbb{A}^3_{(x,y,z)}$ 中的交，该平面由 $z = \gamma$ 给出，见第 2.2 节。换言之，一般而言， $\mathcal{Z}_\gamma$ 是 $\mathbb{A}^2_\gamma$ 中由 $y^p - y - f(x,\gamma) = 0$ 定义的曲线。注意，在某些情况下，该交并不可约，但我们所用的纤维是几何不可约曲线。如第 2.2 节所述，我们将 $\mathbb{A}^2_\gamma$ 的射影闭包记为 $\mathbb{P}^2_\gamma$，其齐次坐标为 $(x : y : w)$。此外，令 $s := \deg_x f$，并将 $F_\gamma(x,w)$ 记为 $f(x,\gamma) \in \mathbb{F}_q[x]$ 关于变量 w 的齐次化。那么，由下式定义的曲线

$$\overline{\mathcal{Z}}_\gamma : y^p w^{s-p} - y w^{s-1} - F_\gamma(x,w) = 0 \tag{3.3}$$

是 $\mathcal{Z}_\gamma$ 在 $\mathbb{P}^2_\gamma$中的射影闭包。注意， $\mathcal{Z}_\gamma$ 有唯一的无穷远点 $P_\gamma := (0:1:0)$ 位于 $\mathbb{P}^2_\gamma$中，该点对应于 $[(0:1:0), (\gamma, 1)]$，位于 $\mathbb{P}^2_{(x:y:w)} \times \mathbb{A}^1_z$中的 S_f的部分紧化内。

在以下引理中，我们计算 P_γ 在 $\mathcal{Z}_\gamma$上的重数，以及 $\mathcal{Z}_\gamma$ 与直线 $w = 0$ 和 $x = 0$ 在 P_γ处的交重数。

引理 3.1。 若 $s \geq p+1$，则 P_γ 是 $\mathcal{Z}_\gamma$ 中的一个重数为 $s-p$的点。此外，直线 $w = 0$ 是 $\mathcal{Z}_\gamma$ 在该点处唯一的切线，并以重数 s与其相交，而直线 $x = 0$ 与 $\mathcal{Z}_\gamma$ 在 P_γ 处以重数 $s-p$相交。

证明。 令 $h(x,y,w) = y^p w^{s-p} - y w^{s-1} - F_\gamma(x,w)$ 为定义 $\mathcal{Z}_\gamma$在 $\mathbb{P}^2_\gamma$中的齐次多项式。注意， $\overline{F_\gamma}(x,w)$ 是若干单项式（关于 x 和 w）之和，且每项次数均为 s。由于点 P_γ 是仿射图 $y = 1$中的原点，要计算它在 $\mathcal{Z}_\gamma$ 上的重数，我们将 $h(x,y,w)$ 关于 y去齐次化，得到 $w^{s-p} - w^{s-1} - F_\gamma(x,w)$，并考察此表达式中的最低次项。由于 $F_\gamma(x,w)$ 中出现的所有单项式次数均为 s，因此最低次项为 w^{s-p}，这表明

P_γ 是 $\mathcal{Z}_\gamma$ 上的一个 $s-p$ 重数点，并且 $\mathcal{Z}_\gamma$ 在 P_γ 处唯一的切线是直线 $w=0$。特别地，注意，如果 $s=p+1$，那么 P_γ 是 $\mathcal{Z}_\gamma$ 上的非奇异点，其切线为直线 $w=0$；而如果 $s>p+1$，那么 P_γ 是奇异点，但其切线仍只有 $w=0$。

由定义 $\mathcal{Z}_\gamma$ 的方程可知，$\overline{P_\gamma}$ 是 $\mathcal{Z}_\gamma$ 与直线 $w=0$ 的交点中唯一的点。根据贝祖定理，$w=0$ 与 $\mathcal{Z}_\gamma$ 在 P_γ 处的交数恰为 s，即 $\mathcal{Z}_\gamma$ 的次数。另一方面，对于任意一条经过 P_γ 的其他直线 ℓ，由于 ℓ 在 P_γ 处不是 $\mathcal{Z}_\gamma$ 的切线，ℓ 与 $\mathcal{Z}_\gamma$ 在 P_γ 处的交数为 $s-p$，即 P_γ 作为 $\mathcal{Z}_\gamma$ 上一点的重数。□

现在，我们将定义一个由曲面 $\mathcal{S}_f$ 上的求值码构成的分层局部可恢复码族。

定义 3.2。设 $f\in\mathbb{F}_q[x,z]$ 满足 次数$_x(f(x,z))=s$，其中 s 是一个 $s\geq p+1$ 整数。设 $\mathcal{S}_f$ 为由式 (x,z) 定义的曲面，如式 (3.1) 所示，并设 $\mathcal{Z}_\gamma$ 按式 (3.2) 定义。设 η 为一个正整数，满足

$$0\leq\eta\leq\max\{|\pi_x(\mathcal{Z}_\gamma(\mathbb{F}_q))|:\gamma\in\mathbb{F}_q,\deg_x(f(x,\gamma))=s\}$$

并令 $\Gamma\subseteq\mathbb{F}_q$ 表示该子集

$$\Gamma:=\{\gamma\in\mathbb{F}_q:\pi_x(\mathcal{Z}_\gamma(\mathbb{F}_q))\geq\eta\ and\ \deg_x(f(x,\gamma))=s\}. \tag{3.4}$$

设 $\rho_1\in[\eta]$、$\rho_2\in[p]$和 $\rho_3\in[|\Gamma|]$ 为正整数，使得

(1) $\rho_1\geq 2$、$\rho_2\geq 2$和 $\rho_3\geq 1$；*(2)*

$$p\eta\geq s(\eta-\rho_1+p-\rho_2)-(s-p)(\eta-\rho_1)+1=s(p-\rho_2)+p(\eta-\rho_1)+1。$$

定义一个求值码（见定理 *2.8*）$C^f:=C(T,V)$，其求值集为

$$T:=\{(x,y,z)\in\mathcal{S}(\mathbb{F}_q):z\in\Gamma\}=\bigcup_{\gamma\in\Gamma}\mathcal{Z}_\gamma(\mathbb{F}_q), \tag{3.5}$$

以及求值多项式的向量空间

$$V=V_{\rho_1,\rho_2,\rho_3}:=\langle x^iy^jz^k:0\leq i\leq\eta-\rho_1,0\leq j\leq p-\rho_2,0\leq k\leq|\Gamma|-\rho_3\rangle. \tag{3.6}$$

在下面的小节中，我们证明码 C^f 具有局部性和层次结构，并讨论其维数、最小距离和码率。

注 3.3。根据构造，定理 *3.2* 中的码 C^f 的长度为 $n:=|T|\geq p\eta|\Gamma|$。事实上，设η 满足每个 $\mathcal{Z}_\gamma$ 至少有 ηp 个仿射点。由于 $\mathcal{Z}_\gamma$ 是阿廷-施赖埃尔曲线，这等价于其仿射点的 $\mathcal{Z}_\gamma$具有 η 个或更多不同的 x-坐标值。因此，$|T|\geq p\eta|\Gamma|$，因为$|\pi_x(\mathcal{Z}_\gamma)|\geq\eta$ 且 $\pi_z(T)=\Gamma$。

注 3.4。正如第 *3.2* 节中的讨论将会说明的，定理 *3.2* 中的条件(2) 是确保C^f 的最小距离 d 的某个下界为正所必需的。不过需要指出的是，即使去掉该条件，最小距离仍有一个非平凡（正）的下界。更确切地说，在定理 *3.10* 的证明中，我们证明下界 $d\geq\rho_1\rho_2\rho_3$ 始终成立；由定理 *3.7* 可推知，若 $\rho_1\geq s$，则定理 *3.8* 中证明的界大于或等于 $\rho_1\rho_2\rho_3$。

3.2. **最小距离的维数、局部性与下界**。在本小节中，我们讨论定理 3.2 中的码 C^f 的参数。首先，对每个纤维 $\mathcal{Z}_\gamma$ 应用贝祖定理，计算 C^f 的最小距离d 的一个界′，并减去函数在 P_γ 处的最小消失重数，再对所有 $\gamma\in\Gamma$ 取值。

设 $M:=\eta+p-\rho_1-\rho_2$，并考虑由 $\mathbb{F}_q$ 构成的（齐次）形式向量空间

$$V_H=\langle x^iy^jw^\ell:0\leq i\leq\eta-\rho_1,0\leq j\leq p-\rho_2,i+j+\ell=M\rangle. \tag{3.7}$$

注意，当 $g\in V$限制在 $\mathbb{A}^2_\gamma$上时，它给出一个函数 $g_\gamma(x,y):=g(x,y,\gamma)$，可以写成$g_\gamma=G_\gamma(x,y,1)$，其中 $G_\gamma\in V_H$是 g_γ关于某个变量 w的齐次化。由此显然可知

G_γ 在 $w=1$ 满足条件的 $\mathcal{Z}_\gamma$ 的仿射点上的消失，与 g_γ 在 $\mathcal{Z}_\gamma$上的消失相同。此外， $g \in V$ 在 P_γ 处的消失重数，也可用 G_γ 在 P_γ处的消失重数来描述；这恰好是由 G_γ 和 $\mathcal{Z}_\gamma$定义的曲线在原点处的交数，其中取 $\mathbb{P}^2_\gamma$的仿射图 $y=1$ 。据此，以下引理计算了对于任意 $\gamma \in \Gamma$， V 中任意函数在 P_γ处的最小消失重数。

引理 3.5。 设 $\mathcal{Z}_\gamma$和 P_γ 如上所定义，并设 V_H 为式 (3.7)中定义的（齐次） $\mathbb{F}_q$-向量空间形式。令 $\mathcal{G}$ 表示 $\mathbb{P}^2_\gamma$ 中由形式 $G \in V_H \setminus \{0\}$的零点定义的曲线。那么

$$\min_{G \in V_H \setminus \{0\}} \{i_{P_\gamma}(\mathcal{G}, \overline{\mathcal{Z}}_\gamma)\} = (s-p)(\eta - \rho_1).$$

证明。设

$$G(x,y,w) = \sum_{i=0}^{\eta-\rho_1} \sum_{j=0}^{p-\rho_2} a_{i,j} x^i y^j w^{M-i-j},$$

其中 $a_{i,j} \in \mathbb{F}_q$，且至少有一个 $a_{i,j} \neq 0$。

我们首先注意到，根据定理 3.1，一次形式 x（它定义了 $\mathbb{P}^2_\gamma$ 中的直线 $x=0$ ）在 $\mathcal{Z}_\gamma$ 的点 P_γ 处以重数 $s-p$ 为零，且一次形式 w 在 $\mathcal{Z}_\gamma$ 的点 P_γ 处以重数 s 为零。因此，若 $a_{i,j} \neq 0$，则单项式 $a_{i,j} x^i y^j w^{M-i-j}$ 以重数 $i(s-p)+(M-i-j)s$ 为零，而次数为 M 的形式 G 为零的重数至少为

$$\min\{i(s-p) + (M-i-j)s : 0 \leq i \leq \eta - \rho_1, 0 \leq j \leq p - \rho_2\}$$

在 P_γ 处。由于 $s-p<s$，该最小值将为 $(s-p)(\eta-\rho_1)$。 □

推论 3.6. V_H 中的每个非零函数除 P_γ 外，至多在 $\mathcal{Z}_\gamma$ 的 $Ms-(s-p)(\eta-\rho_1)$ 个点上为零。

证明。 这是 Bez´out 定理的直接应用。 □

注 *3.7.* 设 $c \in C^f$ 为任意非零码字，并考虑由 C^f 通过保留与集合 $\{P \in T \mid \pi_z(P) = \gamma\}$中的点相对应的码字位置而得到的删 ***punct*** 码，这些点恰好是 $\mathcal{Z}_\gamma$上的 $\mathbb{F}_q$-点。特别地，由定理 *3.6* 可知，这种删 ***punct*** 码的最小距离至少为 $\eta p - Ms + (s-p)(\eta-\rho_1)$。然而，在定理 *3.10* 的证明中，我们证明另一个下界为 $\rho_1\rho_2$。根据 ρ_1 和 s，我们可以确定这两个下界中哪一个更大。事实上，注意到 $\eta p - Ms + (s-p)(\eta-\rho_1) = \rho_1 p - s(p-\rho_2)$，且 $\rho_1 p - s(p-\rho_2) \geq \rho_1\rho_2$ 当且仅当 $(p-\rho_2)(\rho_1 - s) \geq 0$，因而当且仅当 $\rho_1 \geq s$，因为由定理 *3.2* 的假设， $p-\rho_2 \geq 0$ 总是成立。

推论 3.8. C^f 的最小距离至少为 $\rho_3\left(\eta p - Ms + (s-p)(\eta-\rho_1)\right) = \rho_3(\rho_1 p - s(p-\rho_2))$。

证明。 设 $g(x,y,z) \in V \setminus \{0\}$。由于求值集 T 中的点有 $|\Gamma|$ 个不同的 z 值，且 g 在 z 中的最高次数为 $|\Gamma| - \rho_3$，因此至少有 ρ_3 个 $\gamma \in \Gamma$ 值使得 $g(x,y,\gamma)$ 不恒等于 0。对于这些 γ 值中的每一个， g 在 $\mathcal{Z}_\gamma$ 上的消失情况与相应的 $G_\gamma \in V_H$ 在 $\mathcal{Z}_\gamma$ 的仿射点上的消失情况相同。由于定理 3.6 表明， G_γ 在 $\mathcal{Z}_\gamma$ 的仿射点上至多有 $Ms-(s-p)(\eta-\rho_1)$ 个零点，特别地， G_γ 在 $\mathcal{Z}_\gamma$ 的点上也至多有这么多个零点。因此， $\mathcal{Z}_\gamma$ 中至少有 $\eta p - Ms + (s-p)(\eta-\rho_1)$ 个求值点处 g 不为零。根据定理 3.2 中的条件 (2)，这个数量至少为 1。□

注 3.9. 注意，在 $j = p-\rho_2$ 和 $\eta = \rho_1$的情形下，函数 $y^{p-\rho_2}$ 在 P_γ处不为零，因此定理 *3.5* 给出的交数为零。在这种情况下，定理 *3.6* 仅得出 ***Bézout*** 定理的结论，结果仍然成立。此时最小距离的界为 $\rho_3(\eta p - Ms)$。由定理 *3.2*， $\eta p - Ms \geq 1$且 $\rho_3 \geq 1$，因此在这种情况下最小距离也为正。

定理 3.8 给出了定理 3.2 中码 C^f 的下界 $d \geq \rho_3(\eta p - Ms + (s-p)(\eta - \rho_1))$。现在我们证明，任何这样的码都是一个分层局部可恢复码，其下层码支撑在 $\pi_{x,z}$: $\mathcal{S}_f \to \mathbb{A}^2_{x,z}$的纤维上，而中间码支撑在曲线 $\mathcal{Z}_\gamma$上，参见定理 2.5 和定理 2.7。

定理 3.10。 设 $f \in \mathbb{F}_q[x,z]$ 满足 次数$_x(f(x,z)) = s$，其中 $s \in \mathbb{Z}_{\geq p+1}$，并令 $\mathcal{S}_f$和 $\mathcal{Z}_\gamma$如式 (3.1) 及式 (3.2)所示。设 C^f 为来自 $\mathcal{S}_f$ 的求值码，如定理 *3.2* 所示，采用对参数 η、ρ_1、ρ_2、ρ_3的任意适当选择而得。

码 C^f 具有分层局部性，其下层码支撑集位于 $\pi_{x、z}$: $\mathcal{S}_f \to \mathbb{A}^2_{(x,z)}$ 的纤维上，中层码支撑集位于曲线 $\mathcal{Z}_\gamma$上。更确切地说， C^f 是一个 $[n,k,d]$-码，满足

$$n = |T| \geq \eta p|\Gamma|, \quad k = (\eta - \rho_1 + 1)(p - \rho_2 + 1)(|\Gamma| - \rho_3 + 1),$$
$$d \geq \rho_3 \max\{\rho_1\rho_2,\ \rho_1 p - s(p-\rho_2)\}.$$

此外，采用定理 *2.5* 中的记号， C^f 具有局部参数

$$((n_1,k_1,d_1),(n_2,k_2,d_2)),$$

其中

$$n_1 \geq \eta p, \qquad k_1 = (\eta - \rho_1 + 1)(p - \rho_2 + 1), \qquad d_1 = \max\{\rho_1\rho_2,\ \rho_1 p - s(p-\rho_2)\}$$
$$n_2 = p, \qquad k_2 = p - \rho_2 + 1, \qquad d_2 = \rho_2.$$

证明。 考虑码字 $c \in C^f$中索引为 i 的位置。 c 在位置 i 上的坐标，由多项式 V在某个固定点 P_i处的求值给出：$=(\alpha,\ \beta,\ \gamma) \in T$。将 $C^f_{2,i}$记为从 C^f 得到的删 punct 码：保留求值集 T中与 P_i具有相同 x 坐标和 z 坐标的点所对应的码字位置，即满足 $x = \alpha$ 和 $z = \gamma$ 的点。这些点恰好是纤维

$$F_{2,i} \coloneqq (\pi_{x,z}|_{\mathcal{S}_f})^{-1}(\pi_{x,z}(P_i)) = \{(\pi_x(P_i), \pi_y(P_i) + \delta, \pi_z(P_i)) : \delta \in \mathbb{F}_p\},$$

这尤其表明 $n_2 = p$。现在令 $g \in V$，并注意到 $g|_{F_{2,i}} = g(\alpha,y,\gamma)$ 是关于 y 的单变量多项式，其次数至多为 $p - \rho_2$。这意味着，已知 g 在 F_2 中 $p - \rho_2 + 1$ 个点处的求值后，我们可以使用拉格朗日插值，在整个 $F_{2,i}$ 上插值得到 $g(\alpha,y,\gamma)$。因此，我们具有 $(p-(\rho_2-1)\ \rho_2)$ 局部性，并且在低层可以恢复对应于 $F_{2,i}$ 中的点的任意 $\rho_2 - 1$ 个坐标擦除。这意味着低层码 $C^f_{2,i}$ 是一个维数至多为 $k_2 = p - \rho_2 + 1$ 、最小距离至少为 $d_2 = \rho_2$ 的 (k_2,d_2) 局部可恢复码。

现在用 $C^f_{1,i}$ 表示由 C^f 得到的删 punct 码，该码保留了与 $F_{1,i}$中的点相对应的码字位置，其中我们定义

$$F_{1,i} \coloneqq \{P \in T \mid \pi_z(P) = \gamma\}.$$

注意 这些点恰好是 $\mathcal{Z}_\gamma$ 上的 $\mathbb{F}_q$-点，由此可得 $n_1 \geq \eta p$.

$C^f_{1,i}$的维数至多为 $k_1 = (\eta - \rho_1 + 1)(p - \rho_2 + 1)$，这直接由定理 3.2 中多项式空间 V 的定义得出。另一方面，为了证明 $C^f_{1,i}$ 的最小距离至少为 $d_1 = \rho_1\rho_2$，我们先计算码中唯一确定一个向量所需坐标数的下界。令

$$g_\gamma(x,y) \coloneqq g(x,y,\gamma) = g_0(x) + g_1(x)y + \ldots g_{p-\rho_2}(x)y^{p-\rho_2}, \tag{3.8}$$

其中 $g_j \in \mathbb{F}_q[x]$，且对每个 $0 \leq j \leq p - \rho_2$ 都有 $\deg(g_j) \leq \eta - \rho_1$。现在考虑在这个多元多项式 g 的情形下进行多项式插值，可得如下结论。

对于 $a \in \mathbb{F}_q$，我们定义 T 的以下子集：

$$W_a \coloneqq \{(a,y) \in \mathcal{Z}_\gamma(\mathbb{F}_q) : y^p - y = f(a,\gamma)\}.$$

注意，根据求值集 T 和集合 Γ 的定义，至少存在 η 个不同的非空集合W_a，因为对于 T 中的任意点，特别是对于 $F_{1,i}$中的任意点，其 z 坐标都是集合 Γ 的元素。此外，如果 $W_a \neq \emptyset$，那么根据 Artin-Schreier 理论， $|W_a| = p$。

与定理 3.1]，的证明类似， [5, 现在的主要思路是通过拉格朗日单变量多项式插值求出方程 (3.8) 中的每个 $g_j(x)$，这需要在至少 $\eta - (\rho_1 - 1)$ 个 a 值下求出 $g_j(a)$，其中$W_a \neq \emptyset$。为此，注意到

$$g_\gamma(a, y) = g_0(a) + g_1(a)y + \dots g_{p-\rho_2}(a)y^{p-\rho_2}$$

是一个单变量多项式，因此，只要在 W_a 中至少 $p - (\rho_2 - 1)$ 个不同点上给出 $g_\gamma(\{v4, y)$ 的值，就可以插值得到它的系数 $g_j(a)$。

要使 $g_\gamma(x, y)$ 上的这一分层插值过程成功，我们需要 $\eta - (\rho_1 - 1)$ 个集合 $W_a \neq \emptyset$，使得在 W_a 中至少 $p - (\rho_2 - 1)$ 个点上的 $g_\gamma(a, y)$ 求值已知。

注意，对于固定的 $W_a \neq \emptyset$，只有当与 W_a 中的点对应的指标处至少有 ρ_2 个擦除时，才能确定所有 j 的 $g_j(a)$。此外，对于每个 j，只有当存在至少 ρ_1 个 $a \in \mathbb{F}_q$ 值满足 $W_a \neq \emptyset$，而我们未能取回 $g_j(a)$ 时，下一步确定 $g_j(x)$ 的系数才会失败。因此，若要导致恢复失败，$F_{1,i}$ 中的 $g_\gamma(x, y)$ 求值缺失数必须至少为 $\rho_1\rho_2$，这进而保证中间码 $C_{1,i}^f$ 的最小距离至少为 $\rho_1\rho_2$。如定理 3.7 中所述，由定理 3.6 可知，$C_{1,i}^f$ 的最小距离也有下界 $\rho_1 p - s(p - \rho_2)$，由此可得 $d_1 = \max\{\rho_1\rho_2, \rho_1 p - s(p - \rho_2)\}$。

为完成证明，我们现在考虑完整码 C^f，并证明当 V 和 T 时，求值映射是单射的，从而证明 C 的维数恰好等于 V 作为 $\mathbb{F}_q$-向量空间的维数。此外，结合证明的前一部分与定理 3.8，我们还证明界 $d \geq \rho_3\max\{\rho_1\rho_2, \rho_1 p - s(p - \rho_2)\}$ 成立。

为证明当 V 和 T 时求值映射的单射性，令 $g \in V \setminus \{0\}$。如定理 3.8 的证明中所述，至少存在 ρ_3 个 $\gamma \in \Gamma$ 的取值，使得 $g(x, y, \gamma)$ 在 $\mathcal{Z}_\gamma$ 上不恒为零。此外，对于每个 g 不恒为零的 $\mathcal{Z}_\gamma$，定理 3.6 保证 g 除了 P_γ 外，至多在 $\mathcal{Z}_\gamma$ 的 $Ms - (s - p)(\eta - \rho_1)$ 个点上取零，因此特别地，它在 T 中至多在 $\rho_3(Ms - (s - p)(\eta - \rho_1))$ 个点上取零。由于根据定理 3.2 的条件（2）， $|T| \geq \rho_3\eta p > \rho_3(Ms - (s - p)(\eta - \rho_1))$，因此可知， V 中任何非零函数都不可能在 T 的所有点上取零，从而特别地， T 中点上的求值映射是单射的。

总之，注意到至少存在 ρ_3 个 $\gamma \in \Gamma$ 值，使得任意 $g \in V \setminus \{0\}$ 在 $\mathcal{Z}_\gamma$ 上都不恒为零；结合 $C_{1,i}^f$ 的最小距离下界 $\rho_1\rho_2$，特别可知 $\rho_1\rho_2\rho_3$ 是 d 的一个下界。另一方面，根据定理 3.8，我们已经知道 $\rho_3(\rho_1 p - s(p - \rho_2)$ 也是 d 的一个下界，因此得到界 $d \geq \rho_3\max\{\rho_1\rho_2, \rho_1 p - s(p - \rho_2)\}$。根据定理 3.7，我们还已经知道，当 $\rho_1 < s$ 时，$\max\{\rho_1\rho_2, \rho_1 p - s(p - \rho_2)\} = \rho_1\rho_2$；而当 $\rho_1 \geq s$ 时，$\max\{\rho_1\rho_2, \rho_1 p - s(p - \rho_2)\} = \rho_1 p - s(p - \rho_2)$。□

注 3.11。与证明 [5, 定理3.1], 中的情况一样，我们注意到，定理 *3.10* 的证明给出了下层码和中间码层级上的显式恢复过程。

4. Examples of HLRCs from Artin-Schreier surfaces

本节将重新考察 [5, 第 4],节中讨论的阿廷-施赖尔曲面上的分层局部可恢复码示例，展示如何通过我们的方法改进其最小距离界，并对其渐近参数给出更精确的估计。

在本节中，我们始终令 p 为一个奇素数。沿用第3节中的记号， [5, 第 4] 节所讨论的例子中的阿廷-施赖尔曲面为

$$\mathcal{S}_f : y^p - y = x^{p+1}z^2 + x^2z^{p+1} \tag{4.1}$$

在 $\mathbb{F}_{p^2}$上，其纤维为

$$\mathcal{Z}_\gamma : y^p - y = x^{p+1}\gamma^2 + x^2\gamma^{p+1}, \tag{4.2}$$

其中 $\gamma \in \mathbb{F}_{p^2}^*$。

我们根据定理 3.2，考虑任意来自 S_f 的 HLRC C^f，其中 $\eta = 2p-1$。注意到，这给出了仍满足 [5, 定理 3.1], 假设的码，但不同于 [5, 定理 4.4], 中描述的例子，在后者中 η 被设为等于 p。特别地，选择 $\eta = 2p-1$ 会产生码 C^f；对于 ρ_1， ρ_2， ρ_3的任意适当选择，这些码都比 [5, 定理 4.4]中所考虑的码更短。事实上，根据 [5, 引理 4.3], ，这意味着求值集 T 的基数为 $|T| = \eta p|\Gamma|$，严格小于 [5, 定理 4.4]中定义的码的求值集基数。这是因为，此类码的求值集还包含纤维 $\mathcal{Z}_\gamma$ 上的所有 $\mathbb{F}_{p^2}$-有理点，其中 $\gamma^{p-1} = \gamma^{1-p}$；而在我们的构造中，这些点因 $\eta = 2p-1$ 而被排除。

采用这样的求值点后，我们现在选择参数 ρ_1, ρ_2, ρ_3，使得 $p+1 \le \rho_1 \le \eta,\ 2 \le \rho_2 \le p,\ 1 \le \rho_3 \le |\Gamma|$. 。这样，对于上述任意选择的 ρ_1, ρ_2, ρ_3 ，相应的 C^f 的求值多项式空间为

$$V := V_{\rho_1,\rho_2,\rho_3} := \langle x^i y^j z^k : 0 \le i \le 2p-1-\rho_1, 0 \le j \le p-\rho_2, 0 \le k \le |\Gamma| - \rho_3 \rangle. \tag{4.3}$$

特别是在 上述指标 $\eta, \rho_1, \rho_2, \rho_3$ 满足定理 3.2 中的条件 (1) 和 (2)。

尽管采用了较小的求值点集，但按照我们的定理 3.2 构造的码 C^f 仍满足定理 3.1] 的假设（尤其参见定理 4.4], 的证明中 [5, 式 (4.12)]之后的讨论）。因此不难看出， C^f 的层次结构以及较低层码和中间码的局部参数，本质上与定理 4.4] 中描述的相同。另一方面，采用我们的选择后，完整码的长度更短，但我们仍能给出中间码和完整码的最小距离界，且优于定理 4.4] 中给出的界。

事实上，由定理 3.7可知，对于 $\rho_1 = p+1$，我们得到与 [5, 定理 4.4], 中相同的界；而对于 $\rho_1 > p+1$，我们得到更大的下界，即中层码的最小距离为 $\rho_1 p - (p+1)(p-\rho_2)$，而 C^f 的最小距离为 $\rho_3(\rho_1 p - (p+1)(p-\rho_2))$。

注 4.1。 根据关于 η、 ρ_1、 ρ_2 的假设，特别可知 $\eta p - M(p+1) + (\eta - \rho_1) \ge 2p+2$，因此，由定理 *3.8* 可知， C^f 的最小距离 d 满足 $d \ge \rho_3(2p+2)$。另一方面，由 [5, 定理 4.4] 得到的 d 的一般下界为 $d \ge p+4$，并且对于任意 $p \ge 2$ 以及如定理 *3.2* 中所述的 ρ_3 的任意选择，均有 $\rho_3(2p+2) \ge p+4$ 。

我们通过考察若干码的例子来结束本节，这些例子采用了指标 ρ_1、 ρ_2 和 ρ_3 的显式选择，并讨论这些选择如何影响码的最小距离、信息率和相对距离。

例 4.2. 具有最大维数的码 C^f 是具有最小指标的码，即 $\rho_1 = p+1 \rho_2 = 2$ 和 $\rho_3 = 1$。显然，在这种情况下，我们得到一个参数为

$$n = (2p^2-p)(p-1)^2, \qquad k_{\max} = (p-1)^4, \qquad d \ge 2p+2.$$

注意，信息率的阶为 $1/2$。

*Wh*取 $\rho_1 = p+1$、 $\rho_2 = 2$ 和 $\rho_3 = p+1$ 时，我们得到一个参数为

$$n = (2p^2-p)(p-1)^2, \qquad k = (p^2-3p+1)(p-1)^2, \qquad d \ge (p+1)(2p+2),$$

其信息率的阶也为 $1/2$。注意，这使最小距离相比例 *4.2* 提高了 $p+1$ 倍，同时保持码率的阶不变。

此外，我们也希望随着 p 增加，码率和相对距离都保持远离 *0*。比如，选择参数为 $\rho_1 = p+1$、 $\rho_2 = \frac{p-1}{2}$ 和 $\rho_3 = (p-1)_2^{\ 2}$, , 即可达到这一点，并得到

一个 $[n,k,d]$-码，其

$$n=(2p^2-p)(p-1)^2, \qquad k=(p+1)\left(\frac{p+3}{2}\right)\left(\frac{p^2+3}{2}-p\right), \qquad d\geq\frac{(p-1)^2(p^2-1)}{4}.$$

请注意，对于信息率和相对最小距离，渐近参数分别为 $1/8$ 和 $1/2$ 的数量级。

5. Codes on Kummer-type surfaces

本节沿用第 3 节的思路，构造一种一般方法，将具有纤维化且纤维为库默尔曲线的曲面转化为 HLRC 代数几何码。

与前面一样，设 $q:=p^h$ 是某个素数 p 的正整数次幂，并设 $\lambda\in\mathbb{Z}_{>0}$ 满足 $\gcd(p,\ \lambda)=1$。此外，假设 $\mathbb{F}_q$ 含有一个本原 λ 次单位根。考虑由下式定义的 $\mathbb{A}^3_{(x,y,z)}$ 中的曲面：

$$\mathcal{S}_f: y^\lambda - f(x,z)=0, \tag{5.1}$$

其中

$$f(x,z):=c\cdot x^h\cdot z^\nu\cdot\prod_{i=1}^{\mu-h}(x-a_iz)\in\mathbb{F}_q[x,z], \tag{5.2}$$

其中 $c\in\mathbb{F}_q^*$、$\mu\in\mathbb{Z}_{>0}$、$h,\ \nu\in\mathbb{Z}_{\geq 0}$、$0\leq h\leq\mu-1$、$\mu,\ \nu<\lambda$，且 $a_i\in\mathbb{F}_q^*$ 满足：对于任意 $i\neq j$，都有 $a_i\neq a_j$。现在令$\gamma\in\mathbb{F}_q^*$，并定义

$$\mathcal{Z}_\gamma:=\begin{cases}y^\lambda-f(x,z)=0\\ z-\gamma=0\end{cases}, \tag{5.3}$$

也就是说，这是在 $\mathbb{A}^3_{(x,y,z)}$ 中由平面 $z=\gamma$ 与 $\mathcal{S}_f$ 相交得到的曲线。现在令 $\mathbb{A}^2_\gamma$ 如第 2.2 节所定义。由于 $\mathcal{Z}_\gamma$ 位于平面 $z-\gamma=0$ 上，略微滥用记号，如第 3.1 节所示，我们也用 $\mathcal{Z}_\gamma$ 表示由 $y^\lambda-f(x,\ \gamma)=0$ 定义的 $\mathbb{A}^2_\gamma$ 中的平面曲线。

注 5.1。请注意，根据我们的假设以及在式 (5.2) 中对任意$i\neq j$选取 $a_i\neq a_j$ 这一事实，可知曲线 $\mathcal{Z}_\gamma$是库默尔型的，并且多项式 $f(x,\gamma)$ 是$\mu-h+1$ 个互不相同因子的乘积，其中 $\mu-h$ 个因子不是 x的倍数。事实上，

$$f(x,\gamma)=c\cdot x^h\cdot\gamma^\nu\cdot\prod_{i=1}^{\mu-h}(x-a_i\gamma)$$

对任意 $i\neq j$，也有 $a_i\gamma\neq a_j\gamma$，因为 $\gamma\in\mathbb{F}_q^*$，且乘以 γ 是域 $\mathbb{F}_q$上的一个自同构。

仍采用第 2.2 节中引入的记号，我们用 $\mathbb{P}^2_\gamma$表示 $\mathbb{A}^2_\gamma$ 的射影闭包，其齐次坐标为（$x:\ y:w$），并令

$$\overline{\mathcal{Z}}_\gamma: y^\lambda - F_\gamma(x,w)=0, \tag{5.4}$$

其中，$F_\gamma(x,w)$ 是 $f(x,\gamma)\in\mathbb{F}_q[x]$ 关于变量 w的齐次化。由于我们假设$\mu<\lambda$，多项式 $F_\gamma(x,w)$ 是次数为 λ 的齐次多项式，而 λ 是 w的倍数。更准确地说，

$$F_\gamma(x,w)=c\cdot w^{\lambda-\mu}\cdot x^h\cdot\gamma^\nu\cdot\prod_{i=1}^{\mu-h}(x-a_i\gamma\ w). \tag{5.5}$$

公式（5.4）中定义的曲线 $\mathcal{Z}_\gamma$ 是 $\mathbb{P}^2_\gamma$ 中 $\mathcal{Z}_\gamma$ 的射影闭包。注意，这条曲线有唯一的无穷远点，即 $P_\gamma:=(1:0:0)$，它对应于 $\mathbb{P}^2_{(x:y:w)}\times\mathbb{A}^1_z$ 中 S_f 的部分紧化中的点 $[(1:0:0),\ (\gamma,\ 1)]$。与第 3.1 节中一样，我们先观察点 P_γ 在 $\mathcal{Z}_\gamma$ 上的重数。

引理 5.2。点 P_γ 是 $\mathcal{Z}_\gamma$ 上的一个重数为 $\lambda-\mu$ 的点。此外，直线 $w=0$ 是在该点处与 $\mathcal{Z}_\gamma$ 相切的唯一切线，与其相交的重数为 λ；而直线 $y=0$ 与 $\mathcal{Z}_\gamma$ 在 P_γ 处相交，重数为 $\lambda-\mu$。

证明。令 $h(x,y,w):=y^\lambda-c\cdot w^{\lambda-\mu}\cdot x^h\cdot\gamma^\nu\cdot\prod_{i=1}^{\mu-h}(x-a_i\gamma\, w)$ 为在 $\mathbb{P}^2_\gamma$ 中定义 $\mathcal{Z}_\gamma$ 的齐次多项式，见公式（5.4）和公式（5.5）。由于点 P_γ 是 $\mathbb{P}^2_\gamma$ 的仿射图中满足 $x=1$ 的原点，要计算其在 $\mathcal{Z}_\gamma$ 中的重数，我们将 $h(x,y,w)$ 关于 x 去齐次化，得到 $y^\lambda-c\cdot w^{\lambda-\mu}\,\gamma^\nu\cdot\prod_{i=1}^{\mu-h}(1-a_i\gamma\, w)$。从这里开始，证明与定理 3.1 的证明完全类似。□

5.1. **码　　构造**。仿照定理 3.2，现在令 $\eta\in\mathbb{Z}_{>0}$ 为一个正整数，　　h

$$0\le\eta\le\max\{|\pi_x(\mathcal{Z}_\gamma(\mathbb{F}_q))|\ :\ \gamma\in\mathbb{F}_q\},\tag{5.6}$$

并令 $\Gamma\subseteq\mathbb{F}_q$ 表示该子集

$$\Gamma:=\{\gamma\in\mathbb{F}_q\ :\ |\pi_x(\mathcal{Z}_\gamma(\mathbb{F}_q))|\ge\eta\}.\tag{5.7}$$

对于任意 $\gamma\in\Gamma$，我们定义 $\mathcal{S}_f$的 $\mathbb{F}_q$-有理点的以下子集：

$$T_\gamma:=\{(x,y,\gamma)\in\mathcal{S}_f(\mathbb{F}_q)\mid(x,y)\in\mathcal{Z}_\gamma(\mathbb{F}_q)\}\setminus\{(\bar{x},0,\gamma)\mid\bar{x}\in\mathbb{F}_q,\ f(\bar{x},\gamma)=0\}.\tag{5.8}$$

在我们的 记号中，该子集可与 $\mathbb{P}^2_\gamma$ 中 $\mathcal{Z}_\gamma$ 的点的子集对应，即

$$\overline{\mathcal{Z}}_\gamma(\mathbb{F}_{q^2})\setminus(\{(1:0:0)\}\cup\{(\bar{x}:0:1)\mid\bar{x}\in\mathbb{F}_q,\ f(\bar{x},\gamma)=0\})\,.\tag{5.9}$$

注 5.3。注意，根据我们对集合 Γ的选择，对于任意 $\gamma\in\Gamma$，都有 $|T_\gamma|\ge\eta\lambda$ 。事实上，根据我们对 $f(x,z)$ 的定义（见式 (5.2)）以及库默尔理论，对于任意 $\bar{x}$——它是点$P:=(\bar{x}:\ \bar{y}:\ \bar{w})\in T_\gamma$的 x-坐标——方程 $y^\lambda-f(\bar{x},\gamma)=0$在 $\mathbb{F}_{q^2}$ 中恰有 λ 个不同的解，这意味着在 T_γ 中恰有 λ 个不同的点，其 x-坐标等于 $\bar{x}$。

定义 5.4. 设 $\mathcal{S}_f$ 为式 (5.1)定义的曲面。另设 $\mathcal{Z}_\gamma$ 如式 (5.3) 所示，且 T_γ 如式 (5.8)所示，其中 η 和 Γ 分别如上文式(5.6) 和式 (5.7)所定义。定义集合

$$T:=\bigcup_{\gamma\in\Gamma}T_\gamma.\tag{5.10}$$

此外，设 $\rho_1\in[\eta]$、$\rho_2\in[\lambda]$ 和 $\rho_3\in[|\Gamma|]$ 为正整数，使得 $\rho_1\ge\lambda$ 和 $\rho_2\ge2$。定义 $\mathbb{F}_q$-向量空间

$$V:=V_{\rho_1,\rho_2,\rho_3}:=\langle x^iy^jz^l\mid0\le i\le\eta-\rho_1,\,0\le j\le\lambda-\rho_2,\,0\le l\le|\Gamma|-\rho_3\rangle.\tag{5.11}$$

我们定义一个求值码（见定理 *2.8*）$C^f:=C(T,\ V)$，其求值集为 T，多项式向量空间为 V。

注 5.5. 由定理 *5.3* 可直接得出，定理 *5.4* 中的码的长度为 $n:=|T|\ge\eta\lambda|\Gamma|$。事实上，由定理 *5.3* 可知 $|T_\gamma|\ge\eta\lambda$，且任意两个不同的集合 $T_\gamma\subseteq T$ 互不相交。

5.2. **最小距离的维数、局部性和下界**。在本小节中，我们讨论如定理 5.4 所述的码 C^f 的参数，这也是第 3.2 节的对应部分。我们首先计算 C^f 的最小距离 d 的一个界：该界通过对每个纤维 $\mathcal{Z}_\gamma$ 应用 Bézout 定理，并减去 V 中函数在 P_γ 处的最小消失重数（对所有 $\gamma\in\Gamma$）得到。

令 $M:=\eta+\lambda-\rho_1-\rho_2$，并仿照公式 (3.7)，定义由（齐次）形式构成的 $\mathbb{F}_q$-维向量空间

$$V_H:=\langle x^iy^jw^\ell:0\le i\le\eta-\rho_1,\ 0\le j\le\lambda-\rho_2,\ i+j+\ell=M\rangle.\tag{5.12}$$

如第 3.2 节中公式 (3.7) 后的讨论所述，任意函数 $g(x,\ y,\ z)\in V$都可限制为 $\mathcal{Z}_\gamma$上的函数 $g_\gamma(x,\ y)=g(x,\ y,\ \gamma)$，且每个这样的函数都可写成 $g_\gamma=G_\gamma(x,\ y,\ 1)$ 的形式，其中 $G_\gamma\in V_H$ 是 g_γ 关于某个变量 w的齐次化。G_γ在 $\mathcal{Z}_\gamma$ 上满足 $w=1$ 的仿射点处的消失情况，与其在 $\mathcal{Z}_\gamma$上的消失情况相同。此外，$g\in V$ 在 P_γ

处的消失重数也可由 G_γ 在 P_γ处的消失重数来描述，而这恰好是由 G_γ 和 $\mathcal{Z}_\gamma$ 定义的曲线在原点处的交数，且该原点位于 $\mathbb{P}^2_\gamma$中满足 $x = 1$ 的仿射图上。因此，我们得到以下引理和推论，它们分别对应于定理3.5和定理 3.6。

引理5.6。 令 $\mathcal{Z}_\gamma$ 和 $P_\gamma := (1 : 0 : 0)$ 如上所定义，并令 V_H 为式 (5.12)中定义的形式的 $\mathbb{F}_q$-向量空间。令 $\mathcal{G}$ 表示由形式 $G \in V_H \setminus \{0\}$ 的消失所定义的 $\mathbb{P}^2_\gamma$ 中的曲线。那么

$$\min_{G\in V_H\setminus\{0\}}\{i_{P_\gamma}(\mathcal{G}, \overline{\mathcal{Z}}_\gamma)\} = (\lambda - \mu)(\lambda - \rho_2).$$

证明。令

$$G(x, y, w) = \sum_{i=0}^{\eta-\rho_1}\sum_{j=0}^{\lambda-\rho_2} b_{i,j}x^i y^j w^{M-i-j},$$

其中$b_{i,j} \in \mathbb{F}_q$ 且至少有一个$b_{i,j} \neq 0$。

注意到，由定理5.2，一次形式 y在 $\mathcal{Z}_\gamma$的点 P_γ处以重数 $\lambda-\mu$为零，且一次形式 w 在 $\mathcal{Z}_\gamma$的点 P_γ 处以重数 λ 为零。因此，若$b_{i,j} \neq 0$，则单项式$b_{i,j}x^i y^j w^{M-i-j}$ 以重数 $j(\lambda - \mu) +(M - i - j)\lambda$ 为零，且M次形式 G 为零的重数至少为

$$\min\{j(\lambda - \mu) + (M - i - j)\lambda : 0 \le i \le \eta - \rho_1, 0 \le j \le \lambda - \rho_2\}$$

在 P_γ处。该最小值为$(\lambda - \mu)(\lambda - \rho_2)$，因为 $\lambda - \mu < \lambda$。 □

推论 5.7. V_H中的每个非零函数在$\mathcal{Z}_\gamma$上除 P_γ之外至多在 $M\lambda - (\lambda - \mu)(\lambda - \rho_2)$ 个点处为零。

证明. 由B´ezout定理直接得出。 □

由此，我们得到定理 3.8 对定理 5.4 中的码 C^f 的对应结论。

推论 5.8。 C^f 的最小距离至少为 $\rho_3 (\eta\lambda - M\lambda + (\lambda - \mu)(\lambda - \rho_2)) = \rho_3(\lambda\rho_1 - \mu(\lambda -\rho_2))$。

证明。设 $g(x, y, z) \in V$。由于求值集 T 中的点对应 z 值互不相同，共有 $|\Gamma|$ 个，且 g 在 z 中的最高次数为 $|\Gamma| - \rho_3$，因此至少有 ρ_3 个 $\gamma \in \Gamma$ 值使得 $g(x, y, \gamma)$ 不恒为 0。对于这些 γ 值中的每一个， g 在 $\mathcal{Z}_\gamma$ 上的消失情形与相应的 $G_\gamma \in V_H$ 在 $\mathcal{Z}_\gamma$ 的仿射点上的消失情形相同。由推论 5.7 可知， G_γ 在 $\mathcal{Z}_\gamma$ 的仿射点上至多于 $M\lambda - (\lambda - \mu)(\lambda - \rho_2)$ 个点处消失，因此在 $\mathcal{Z}_\gamma$ 中至多于这么多个点处消失。因此， $\mathcal{Z}_\gamma$ 中必有 $\eta\lambda - M\lambda + (\lambda - \mu)(\lambda - \rho_2) = \lambda\rho_1 - \mu(\lambda - \rho_2)$ 个求值点使得 g 不消失，所需结论即得。□

注记 5.9。 当 $\rho_2 = \lambda$ 时，定理*5.6* 中计算得到的最小值为零，因为在 V 中存在一些函数（因此在 V_H 中也有相应的形式）在 P_γ 处不为零。这意味着，定理*5.8* 中得到的最小距离界仍为正值，它实际上只是由纤维 $\mathcal{Z}_\gamma$上的 ***Bézout*** 定理给出的估计。

注记 5.10。 定理*5.8* 中给出的码 C^f 的最小距离 d 下界始终为正。更确切地说，我们有

$$\begin{aligned}\eta\lambda - M\lambda + (\lambda - \mu)(\lambda - \rho_2) &= \eta\lambda - (\eta + \lambda - \rho_1 - \rho_2)\lambda + (\lambda - \mu)(\lambda - \rho_2)\\ &= -\lambda^2 + (\rho_1 + \rho_2)\lambda + (\lambda - \mu)(\lambda - \rho_2)\\ &= \mu\rho_2 + \rho_1\lambda - \mu\lambda\end{aligned}$$

并且，由于 $\mu\rho_2 \ge \mu$ 因为 $\rho_2 \ge 2$，且 $\rho_1\lambda - \mu\lambda \ge 0$ 因为 $\rho_1 \ge \lambda$，因此我们有

$$\eta\lambda - M\lambda + (\lambda - \mu)(\lambda - \rho_2) \ge \lambda^2 - \mu\lambda + \mu > 0. \tag{5.13}$$

注意，式 (5.13) 特别意味着，对于定理 *5.4* 中定义的码 C^f，无论参数 ρ_1, ρ_2, ρ_3 如何选择，其最小距离始终至少具有下界 $\lambda^2 - \mu\lambda + \mu$。

注记5.11. 按照我们对式(5.8)中集合 T_γ 的选取，对任意 $\gamma \in \Gamma$，我们并不把 $\{(\bar{x}, 0, \gamma) \mid \bar{x} \in \mathbb{F}_{q^2},\ f(\bar{x}, \gamma) = 0\}$中的所有点都纳入求值点集合$T$。注意，这些点恰好是投影映射$\pi_{x,z}$的$\mathbb{F}_q$-有理分歧点，而我们的恢复过程对它们并不适用。事实上，对任意满足 $f(\bar{x}, \gamma) = 0$的 $\bar{x} \in \mathbb{F}_q$，$(\bar{x}, \gamma)$ 在$\pi_{x,z}$ 下的原像的基数严格小于 λ。

相对于定理*5.6*中所用的方法，考虑这些点并不能改进最小距离的界。事实上，V中可能存在函数，它在 $\{(\bar{x}, 0, \gamma) \mid \bar{x} \in \mathbb{F}_{q^2},\ f(\bar{x}, \gamma) = 0\}$中的任何点上都不为零。事实上，$V$中所有函数都在所有这些点上为零的仅有情形，是 $\rho_1 = \eta$、$\rho_3 = |\Gamma|$ 和 $\rho_2 \le \lambda - 1$的情形；这些情形并不特别有意义，因为此时求值函数空间将仅仅是 $V := \langle y^j \mid 0 \le j \le \lambda - \rho_2 \rangle$。

定理 5.8 给出码 C^f 的下界 $d \ge \rho_3(\eta\lambda - M\lambda + (\lambda - \mu)(\lambda - \rho_2))$，其中该码如定理 5.4 所述。在下面的定理中，我们证明，任何这样的码都是分层局部可恢复码，其下层码支撑在 $\pi_{x,\,z}\colon \mathcal{S}_f \to \mathbb{A}^2_{x,\,z}$ 的纤维上，而中层码支撑在曲线 $\mathcal{Z}_\gamma$ 上（参见定理 2.5 和定理 2.7）。

定理 5.12。设 $\mathcal{S}_f$ 和 $\mathcal{Z}_\gamma$ 分别如式 (5.1) 和式 (5.3) 所示。设 C^f 是来自 $\mathcal{S}_f$ 的求值码，如定理 *5.4* 所述，选取参数 η、ρ_1、ρ_2、ρ_3 的任意合适取值构造而成。

码 C^f 具有分层恢复性质，其下层码支撑在 $\pi_{x,\,z}\colon\ \mathcal{S}_f \to \mathbb{A}^2_{x,\,z}$ 的纤维上，而中层码支撑在曲线 $\mathcal{Z}_\gamma$ 上。更准确地说，C^f 是一个 $[n, k, d]$- 码，且

$$n = |T| \ge \eta\lambda|\Gamma|, \quad k = (\eta - \rho_1 + 1)(\lambda - \rho_2 + 1)(|\Gamma| - \rho_3 + 1), \quad d \ge \rho_3 \max\{\rho_1\rho_2,\ \lambda\rho_1 - \mu(\lambda - \rho_2)\}.$$

此外，采用定理 *2.5* 中的记号，C^f 具有局部参数

$$((n_1, k_1, d_1), (n_2, k_2, d_2)),$$

其中

$$\begin{aligned} &n_1 \ge \eta\lambda, && k_1 = (\eta - \rho_1 + 1)(\lambda - \rho_2 + 1), && d_1 = \max\{\rho_1\rho_2,\ \lambda\rho_1 - \mu(\lambda - \rho_2)\},\\ &n_2 = \lambda, && k_2 = \lambda - \rho_2 + 1, && d_2 = \rho_2. \end{aligned}$$

证明。这个定理的证明与定理 3.10 的证明完全类似，只需作相应调整，因此为简洁起见，我们省略证明。□

6. Examples of HLRCs from Kummer-type surfaces

本节将给出一些来自具有 Kummer 纤维的曲面的 HLRC码的具体例子。这些例子的灵感来自 [18] 和 [4], ，其中研究了曲线 $\mathcal{Z}_1$（见式 (6.2)）在所有点处的魏尔斯特拉斯半群以及其自同构群。关于本节中使用的单变量函数域的记号和术语，参见第 2.3 节。

设 $q \equiv 2$（模 3）且 $m := (q+1)/3$。采用第 5 节中的记号，令

$$f(x, z) := -z^m x^{2m} - x^m z^{2m} = -x^m z^m (x^m + z^m)$$

并考虑代数曲面

$$\mathcal{S}_f : y^{q+1} - f(x, z) = y^{q+1} + z^m x^{2m} + x^m z^{2m} = 0. \tag{6.1}$$

在 $\mathbb{F}_{q^2}$ in $\mathbb{A}^3_{(x,y,z)}$ 上。

为了构造定理 5.4 中的 $\mathcal{S}_f$ 上的求值码，我们按如下方式进行。为了选择求值点集 T，我们考虑 $\mathcal{S}_f(\mathbb{F}_{q^2})$ 中位于曲线上的点

$$\mathcal{Z}_\gamma : y^{q+1} + \gamma^m x^{2m} + x^m \gamma^{2m} = 0, \tag{6.2}$$

上。采用第 2.2 节引入的记号，令 $\mathcal{Z}_\gamma$ 表示 $\mathcal{Z}_\gamma$ 在 $\mathbb{P}^2_\gamma$ 中的射影化，并令 $\mathcal{Y}_\gamma$ 表示 $\mathcal{Z}_\gamma$ 的正规化。在下面的引理中，我们计算 $\mathcal{Z}_\gamma$ 和 $\mathcal{Y}_\gamma$ 上的 $\mathbb{F}_{q^2}$-有理点的数量。

引理 6.1。 设 $\gamma \in \mathbb{F}_{q^2} \setminus \{0\}$。曲线 $\mathcal{Z}_\gamma$ 具有 $(q^3 + 2q^2 + 2q + 7)/3$ $\mathbb{F}_{q^2}$个点，其正规化$\mathcal{Y}_\gamma$ 具有 $(q^3 + 2q^2 + 4q + 3)/3$ $\mathbb{F}_{q^2}$个点。

证明。 我们断言，$\mathcal{Z}_\gamma$ 通过一个 $\mathbb{F}_{q^2}$-有理覆盖映射被厄米特曲线覆盖。根据 [7, 定理 10，2], 这意味着 $\mathcal{Z}_\gamma$ 是极大的。因此， $\mathcal{Y}_\gamma$ 在 $\mathbb{F}_{q^2}$上也极大，因为它与 $\mathcal{Z}_\gamma$双有理等价。考虑 $\mathcal{H}_q$： $U^{q+1} + V^{q+1} + W^{q+1} = 0$。作为厄米特曲线的一个模型， $\mathcal{H}_q$在 $\mathbb{F}_{q^2}$上是极大的。此外，映射 φ_γ： $\mathcal{H}_q \to \mathcal{Z}_\gamma$ 定义为

$$U \mapsto U^3 = x,\ V \mapsto UVW = y,\ W \mapsto \frac{1}{\gamma}W^3 = w$$

是一个三重覆盖，这证明了我们最初的断言。

现在我们希望计算 $\mathcal{Z}_\gamma$ 和 $\mathcal{Y}_\gamma$上的 $\mathbb{F}_{q^2}$有理点数。我们先利用哈塞-韦伊定理计算 $\mathcal{Y}_\gamma$ 上的$\mathbb{F}_{q^2}$有理点数，然后推导出 $\mathcal{Z}_\gamma(\mathbb{F}_{q^2})$的基数。为此，我们首先计算 $\mathcal{Y}_\gamma$的（几何）亏格 $g(\mathcal{Y}_\gamma)$，也就是函数域 $\overline{\mathbb{F}}_{q^2}(\mathcal{Y}_\gamma)$的亏格。注意， $g(\mathcal{Y}_\gamma)$等于 $\mathcal{Z}_\gamma$的亏格 $g(\mathcal{Z}_\gamma)$，因为曲线 $\mathcal{Y}_\gamma$和 $\mathcal{Z}_\gamma$ 双有理等价，因此它们的函数域 $\mathbb{F}_{q^2}(\mathcal{Y}_\gamma)$和 $\mathbb{F}_{q^2}(\mathcal{Z}_\gamma)$同构。图1对此进行了图示总结。

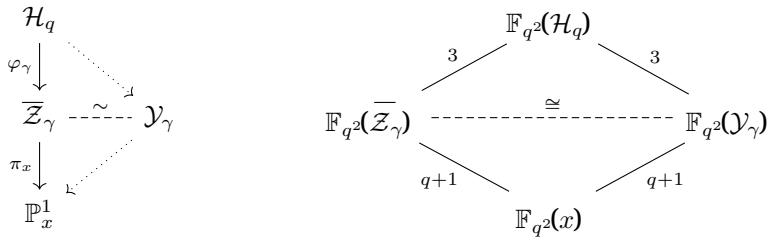

FIGURE 1. 最左侧的图概述了曲线 $\mathcal{H}_q$、 $\mathcal{Z}_\gamma$和 $\mathcal{Y}_\gamma$之间的有理映射。映射 π_x 是到 x坐标的投影，映射φ_γ 是上文定义的三重覆盖，水平虚线箭头表示 $\mathcal{Z}_\gamma$与 $\mathcal{Y}_\gamma$的双有理等价。点状箭头表示交换图中诱导的有理映射。最右侧的图是在函数域语境下对最左侧图的“翻译”。

为计算亏格 $g(\mathcal{Z}_\gamma)$（也就是说，如前所见，即函数域 $\mathbb{F}_{q^2}(\mathcal{Z}_\gamma)$的亏格），我们对函数域扩张 $\mathbb{F}_{q^2}(\mathcal{Z}_\gamma)/\mathbb{F}_{q^2}(x)$应用黎曼–赫尔维茨公式（参见 [14, 定理 3.4.13]）。这是一个次数为 $q+1$的库默尔扩张。根据库默尔理论，可以证明（例如参见 [18, 第3节1]），该扩张中唯一的分歧处是 x 的零点 Q_0 和极点 Q_∞，以及 $x^m + \gamma^m$ 的 m 个不同零点 $Q_1, \ldots, Q_m$。更确切地说， Q_0 和 Q_∞ 各有 m 个不同的扩张，分歧指数均为 3，而 $Q_1, \ldots, Q_m$ 完全分歧。因此， $\mathbb{F}_{q^2}(\mathcal{Z}_\gamma)/\mathbb{F}_{q^2}(x)$的黎曼–赫尔维茨公式给出

$$2(g(\overline{\mathcal{Z}}_\gamma) - 1) = -2(q+1) + 2m + 2m + qm = \frac{q^2 - q - 2}{3},$$

因此我们有 $g(\mathcal{Y}_\gamma) = g(\mathcal{Z}_\gamma) = (q^2 - q + 4)/6$.

我们现在可以计算 $\mathcal{Y}_\gamma$的 $\mathbb{F}_{q^2}$-有理点的个数，根据 Hasse-Weil，该个数为

$$\begin{aligned}|\mathcal{Y}_\gamma(\mathbb{F}_{q^2})| &= q^2+1+2\cdot g(\mathcal{Y}_\gamma)\cdot q = q^2+1+2\cdot\frac{q^2-q+4}{6}\cdot q\\ &= \frac{q^3+2q^2+4q+3}{3}.\end{aligned}$$

为了计算 $\mathbb{F}_{q^2}$ 上的有理点，只需注意，除奇点 (1 : 0 : 0) 和 (0 : 0 : 1) 外， $\mathcal{Z}_\gamma$ 上其余所有 $\mathbb{F}_{q^2}$ 有理点都是非奇异的，因此与 $\mathcal{Y}_\gamma$ 上的 $\mathbb{F}_{q^2}$ 有理点一一对应。

如前所述，根据 [18, 第3节。1] 中的讨论可知，以点 (0 : 0 : 1) 为中心的 $\mathcal{Z}_\gamma$ 恰有 m 个分支，以 (1 : 0 : 0) 为中心的分支有 m 个。因此，$\mathcal{Y}_\gamma$ 上有 m 个点位于 (0 : 0 : 1) 上方，而 $\mathcal{Y}_\gamma$ 上有 m 个点位于 (1 : 0 : 0) 上方。事实上，以 (0 : 0 : 1)（分别以 (1 : 0 : 0)）为中心的 $\mathcal{Z}_\gamma$ 的分支，与 x 在 $\mathbb{F}_{q^2}(\mathcal{Z}_\gamma)/\mathbb{F}_{q^2}(x)$ 中的零点 Q_0 （分别是极点 Q_∞）上方的 m 个不同赋值点一一对应。因此， $\mathcal{Z}_\gamma$（$\mathbb{F}_{q^2}$）的基数为

$$|\overline{\mathcal{Z}}_\gamma(\mathbb{F}_{q^2})| = |\mathcal{Y}_\gamma(\mathbb{F}_{q^2})| - 2(m-1) = \frac{q^3+2q^2+2q+7}{3}.$$

□

为从本例中的曲面 $\mathcal{S}_f$ 构造定理 5.4 中的码，我们考虑以下集合T_γ （见式 (5.8)），其中 $\gamma\in\mathbb{F}_{q^2}\setminus\{0\}$,

$$T_\gamma := \{(x,y,\gamma)\in\mathcal{S}(\mathbb{F}_{q^2}) : (x,y)\in\mathcal{Z}_\gamma(\mathbb{F}_{q^2})\}\setminus(\{(0,0,\gamma)\}\cup\{(a,0,\gamma) : a^m+\gamma^m=0\}).$$

注意，每个这样的集合 T_γ 都可以视为 $\mathcal{Z}_\gamma$ 的子集，其定义如下:

$$\overline{\mathcal{Z}}_\gamma(\mathbb{F}_{q^2})\setminus(\{(0:0:1),(1:0:0)\}\cup\{(a:0:1) : a^m+\gamma^m=0\}),$$

这恰好是本节所讨论的特定情形下式 (5.9) 中所描述的集合。此外，根据定理 6.1，我们实际上可以计算本例中集合 T_γ 的基数。事实上，根据我们对 q的假设，方程 $x^m+\gamma^m=0$ 在 $\mathbb{F}_{q^2}$上总有 m 个互异解，因此集合$\{(a:0:1):\ a^m+\gamma^m=0\}$ 包含 m 个 $\mathcal{Z}_\gamma$上的互异点。根据库默尔理论（参见定理 6.1 证明中的讨论以及 [18, 第 3 节。1]），可以看出，这些点中的每一个都是 $\mathbb{F}_{q^2}(\mathcal{Z}_\gamma)/\mathbb{F}_{q^2}(x)$中一个全分歧赋值点的中心。于是，我们可以利用定理 6.1计算 T_γ 的基数:

$$|T_\gamma| = |\overline{\mathcal{Z}}_\gamma(\mathbb{F}_{q^2})| - 2 - m = \frac{q^3+2q^2+q}{3} = \frac{q(q+1)^2}{3} = q(q+1)m.$$

给定 $a\neq 0$ 于 $\mathbb{F}_{q^2}$ 中，且有 $a^m+\gamma^m\neq 0$，存在 $q+1$ 个 y 的值，使得 $y^{q+1}+a^m\gamma^m(a^m+\gamma^m)=0$。换言之，

$$|\{x\in\mathbb{F}_{q^2} : (x,y,\gamma)\in T_\gamma,\ \exists\, y\in\mathbb{F}_{q^2}\}| = \frac{|T_\gamma|}{q+1} = mq.$$

在定理 5.4 的记号下，这意味着我们令 $\eta := mq$，相应的集合 Γ 为$\Gamma=\mathbb{F}_{q^2}\setminus\{0\}$。记 $|T_\gamma|=\eta(q+1)$，于是对于参数 ρ_1、ρ_2、ρ_3 的任意选择，由 $\mathcal{S}_f$ 构造的码 C^f 的长度等于 $|T|=|T_\gamma|\cdot|\Gamma|=\eta(q+1)(q^2-1)$。

令 $q\neq 2$，并考虑定理 5.4 中的由 $\mathcal{S}_f$ 得到的码，其中 η、Γ 和 T 如上所述，并取参数 ρ_1、ρ_2、ρ_3，使得 $q+1\leq\rho_1\leq\eta$、$2\leq\rho_2\leq q+1$、$1\leq\rho_3\leq q^2-1$.。这样，给定上述 ρ_1、ρ_2、ρ_3 的任意选择，相应码 C^f 的求值多项式空间为

$$V := V_{\rho_1,\rho_2,\rho_3} := \langle x^iy^jz^k : 0\leq i\leq\eta-\rho_1, 0\leq j\leq q+1-\rho_2, 0\leq k\leq q^2-1-\rho_3\rangle. \tag{6.3}$$

注意，我们假设 $q\neq 2$，只是为了确保 $\eta\geq q+1$，从而能够在范围 $q+1\leq\rho_1\leq\eta$ 内选取 ρ_1。

这些码的参数 C^f 可由定理 5.12 得出。不过，与第 4 节中的做法类似，我们现在讨论一些参数取特定值 ρ_1， ρ_2， ρ_3 时的例子，这些取值会带来特别有趣的结果。

例 6.2. 对于本节所讨论的码，定理*5.8*中的界为 $d \geq (3\rho_1 + 2\rho_2 - 6m)m\rho_3$。令 $\rho_1 = \eta$、 $\rho_2 = q+1$ 和 $\rho_3 = q^2 - 2$，于是有 $d \geq \eta(q+1)(q^2-2)$。

注意，采用这一组 ρ_1、 ρ_2、 ρ_3，我们得到一个维数为 $k = 2$ 的码 C^f，其求值函数空间 V 就是 $V = \langle 1, z\rangle$。这或许并不是求值函数空间的理想选择，尤其是因为 z 在集合 T_γ 上为常数。然而，这个例子表明，定理*5.8*给出的 d 下界是紧的。事实上，考虑多项式 $1 - z \in V$，并注意到它在 $(\alpha, \beta, \gamma) \in T$ 处为零，当且仅当 $\gamma = 1$，也就是说，恰好在 $T_1 \subseteq T$ 中的那些点处为零。与 $1 - z$ 的求值相关联的码字重量因此为 $n - |T_1| = \eta(q+1)(q^2-1) - \eta(q+1) = \eta(q+1)(q^2-2)$，这恰好就是此情形下定理*5.8*给出的界。

例 6.3. 为了获得最大维数，从而获得最大码率，应当改为为指标 $\rho_1 = q+1$、 $\rho_2 = 2$、 $\rho_3 = 1$ 选择尽可能小的值。这得到一个 $[n, k, d]$-码，其

$$n = \eta(q+1)(q^2-1), \qquad k_{\max} = (\eta - q)(q+1)(q^2-1), \qquad d \geq (q+1)^2 - m(q-1),$$

其中信息率约为 1。

此外，由于 $\rho_3 = 1$，在这种情况下，完整码的最小距离界与中层码的最小距离界一致；事实上，中层码的最小距离也与完整码的最小距离一致。确实，设 $P(x, y) \in V$ 是一个多项式，它在纤维 $\tilde{\gamma}$ 上给出一个重量最小的码字 c_P。由于 $\rho_3 = 1$，多项式 V 中的多项式在 z 中的最高次数为 $q^2 - 2$，因此我们可以考虑多项式 $\tilde{P}(x, y, z) := (z - \gamma_1) \cdot \cdots \cdot (z - \gamma_{q^2-2}) \cdot P(x, y) \in V$，其中，对于任意 $i \neq j$， $\gamma_i \neq \gamma_j$，且对于所有 i， $\gamma_i \neq \tilde{\gamma}$。注意，这样的多项式在 $q^2 - 2$ 个纤维上恒等于零，也就是说，在除 $\mathcal{Z}_{\tilde{\gamma}}$ 以外的所有纤维上恒等于零。由于我们知道，在 $\mathcal{Z}_{\tilde{\gamma}}$ 上， P 的限制给出一个重量最小的码字 $\tilde{}$，这意味着完整码中与 P 对应的码字实际上具有相同的重量。

例6.4。 还存在一些 ρ_i 的选择，使得当 q 增大时，码率和相对最小距离都与0 保持有界距离。

如果 q 为偶数，选择 $\rho_1 = mq/2$、 $\rho_2 = 1$、 $\rho_3 = q^2/2$，即可得到一个 $[n, k, d]$-码，其满足

$$n = \eta(q+1)(q^2-1) \approx \frac{q^5}{3}, \qquad k = \frac{q^2}{2}\left(\frac{mq}{2} + 1\right)(q+1) \approx \frac{q^5}{12}, \qquad d \geq m(q^2 - 3q)\frac{q^2}{4} \approx \frac{q^5}{12}.$$

如果 q 为奇数，选择 $\rho_1 = m\left(q-1\right)/2$、 $\rho_2 = 1$、 $\rho_3 = \left(q^2-1\right)/2$，即可得到一个 $[n, k, d]$-码，其满足

$$n = \eta(q+1)(q^2-1) \approx \frac{q^5}{3}, \quad k = \frac{q^2+1}{2}\left(\frac{3m^2}{2} + 1\right)(q+1) \approx \frac{q^5}{12},$$
$$d \geq m(q^2 - 4q - 1)\frac{q^2-1}{4} \approx \frac{q^5}{12}.$$

对于较大的 q，这将使信息率和相对距离都渐近地趋于 $1/4$ 。

7. Observations、 Generalizations、 and Next Steps

本文所采用的一般方法，是在一个曲面 $\mathbb{A}^3$ 上构造求值码，并使其纤维化为曲线 $\mathcal{Z}_\gamma$；每条曲线都具有一定的结构正则性，并配有一个自然覆盖 $\phi_\gamma : \mathcal{Z}_\gamma \to \mathbb{A}^1$，而对于许多 $y \in \mathbb{A}^1$ ，在我们关注的域上，各曲线中的纤维 $\phi_\gamma^{-1}(y)$具有相同的基数。与点 P 对应的位置的小恢复组，是与纤维$\phi_\gamma^{-1}(\phi_\gamma(P))$上的点对应的位置集合；该位置的较大恢复组

则对应于 $\mathcal{Z}_\gamma$上的求值点集合。码的函数必须经过构造，使得将任意函数限制在嵌套纤维上时，删 punct 码的维数足够小，从而能够恢复所需数量的位置。本文阐述了如何将每条曲线 $\mathcal{Z}_\gamma$ 射影化，以改善最小距离界和相应曲线的维数；并说明在我们的例子中，射影曲面上的一条直线如何产生具有所需性质的纤维化。具有阿廷-施赖埃尔纤维化和库默尔纤维化的曲面，是探索我们获取分层码这一一般方法的绝佳起点。不过，这种一般方法的适用范围要广泛得多，而且还可以就这一背景下哪些因素有助于构造优良的码提出一些观察。

我们的第一个观察是，在这一构造中，当曲线 $\mathcal{Z}_\gamma$ 相对于曲线的次数具有较多求值点（即需要许多点）时，最小距离界和维数最大。这是因为，如果一个求值函数 f 限制为 $\mathcal{Z}_\gamma$ 上的次数为 e 的函数，而曲线 $\mathcal{Z}_\gamma$ 的次数为 s，那么该函数在 $\mathcal{Z}_\gamma$ 上至多有 se 个零点（减去无穷远处交点的数量）。如果 $\mathcal{Z}_\gamma$ 上的求值点数量相对于 s 较大，我们就可以使用次数更高的求值函数，同时仍能保证函数值非零，从而得到维数更大的码。或者， se 与 $\mathcal{Z}_\gamma$ 上求值点数量之间的差距越大，最小距离界就越大。

然而，我们仍须考虑这与码的长度 n 如何相互作用；如下所述，点数较多且亏格较大的曲线可以得到良好的码率。定理 2.12 中的 Hasse-Weil 界指出，亏格为 g 的曲线在 $\mathbb{F}_q$ 上的（射影）点数至多为 $q+1+2g\sqrt{q}$。对于满足 $g \geq 2\sqrt{q}$ 的极大曲线 $\mathcal{Z}_\gamma$，最后一项占主导，因此 $\mathcal{Z}_\gamma$ 上的点数约为 $2g\sqrt{q}$。对于次数为 s 的光滑平面曲线 C，Pl¨ucker 公式给出 $g = {}_{(s-1)(s-2)\ 2}$。因此，我们采用亏格大致按 $s^2/2$ 增长这一启发式估计。在这种情况下， $\mathcal{Z}_\gamma$ 上约有 $s^2\sqrt{q}$ 个点。因此我们需要 $se \leq s^2\sqrt{q}$。若要追求最大的码率，我们会尽可能增大 e，使其约为 $s\sqrt{q}$。我们假设 $\mathcal{Z}_\gamma \in \mathbb{A}^3_{x,\ y}$，并且投影映射的形式为 $\phi_\gamma(x,\ y) = \bar{y}$，该映射的次数为 t，其中 $t \ll e$。这是合理的，因为最小恢复集的大小为 t，而我们希望这个集合相当小。于是，函数 f 在 x 中的次数界约为 e。综合以上假设，完整码的码率约为 $\frac{et|\Gamma|}{s^2\sqrt{q}|\Gamma|} = \frac{s\sqrt{q}t}{s^2\sqrt{q}} = \frac{t}{s}$。当 t 接近 s 时，我们可以达到接近 1 的码率。

第二个观察是，如果 C 是 $\mathbb{A}^2_{(x,y)}$ 中的一条曲线，我们的框架可以很容易地应用于 $\mathbb{A}^3_{(x,y,z)}$ 中 C 上的锥。这意味着，如果 C 是一条亏格较高、相对于其亏格有许多点，并且在所需的域上有正则纤维覆盖 $\mathbb{A}^1$ 的曲线，我们的构造就能轻松构造出具有分层恢复且参数良好的码。厄米特曲线是 $\mathbb{F}_{q^2}$ 上亏格最大的极大曲线，因此将其作为例子是顺理成章的。

例 7.1. 如定理 *2.13* 所示，令 $\mathcal{H}_q$ 为由仿射方程 $y^q + y = x^{q+1}$ 定义在 $\mathbb{F}_{q^2}$ 上的厄米特曲线。我们考虑由同一方程定义在 $\mathbb{A}^3$ 中的曲面 $\mathcal{S}_q$，即厄米特曲线上的锥。

Let

$$T = \{(x, y, z) : x, y, z \in \mathbb{F}_{q^2}, y^q + y = x^{q+1}\}$$

作为该码的求值点集合，并令

$$V = V_{\rho_1,\rho_2,\rho_3} = \langle x^i y^j z^k : 0 \leq i \leq q^2 - \rho_1, 0 \leq j \leq q - \rho_2, 0 \leq k \leq q^2 - \rho_3 \rangle,$$

其中 $\rho_1 \geq 2$、 $\rho_2 \geq 2$、 $\rho_3 \geq 1$ 和 $(q+1)\ \rho_2 + q\rho_1 > q^2 + q$。

对于每个 $\gamma \in \mathbb{F}_{q^2}$， $\mathcal{Z}_\gamma$ 都是 $\mathcal{H}_q$， $\mathcal{Z}_\gamma\ (\mathbb{F}_{q^2}) = q^3$的一个副本。注意， $\mathcal{Z}_\gamma$ 的射影化与无穷远直线相切，并以重数 $q+1$ 与其交于点 $[0 : 1 : 0]$。映射 $\phi_\gamma : \mathcal{Z}_\gamma \to \mathbb{A}^1$ 由 $(x,\ y) \mapsto y$ 给出。通过与阿廷 - 施赖尔情形中几乎完全相同的论证，我们得到长度为 $n = q^5$， $k = (q^2 - \rho_1 + 1)\ (q - \rho_2 + 1)\ (q^2 - \rho_3 + 1)$ 的分层码，其中 $d \geq \rho_3 \mathit{max}\{\rho_1\rho_2, \rho_1 q - (q+1)\ (q - \rho_2)\}$。局部参数也与定理 *3.10* 中相同，只是用 q 代替 p， $s = q + 1$ 和 $\eta = q^2$。

请注意 因此，我们可以选择 $\rho_1 = q$、 $\rho_2 = 2$ 和 $\rho_3 = 1$，从而得到码率为常数阶的码。

注 7.2。 此外，将厄米特曲线视为 *Kummer* 曲线，并讨论通过定理 *5.4* 中的构造，从厄米特曲线 $\mathcal{H}_q$ 上方的锥体中借助映射 $\phi_\gamma(x、\ y) = x$得到的码 C^f 的参数，也很有意思。

为了使集合 Γ 尽可能大，我们令 $\eta：= q（q-1）$。事实上，通过这种方式 $\Gamma = \mathbb{F}_{q^2}$，因为对于任意 $\gamma \in \mathbb{F}_{q^2}$，纤维 $\mathcal{H}_q \times \{z = \gamma\}$ 上如式 （5.8） 中的集合 T_γ 恰好由 $\mathcal{S}_q$ 的所有仿射有理点组成，其中到 x 坐标的投影映射是非分歧的。这尤其意味着 $|T_\gamma| = q^3 - q = q（q-1）（q+1）$。

此外，按照式 （5.1） 中的记号，我们有 $\lambda = q+1$ 和 $\mu = q$。选择参数 $\rho_1 = \lambda = q+1$、$\rho_2 = 2$、$\rho_3 = 1$（这一选择给出了最小距离的最大界），我们得到一个码 C^f，其长度为 $n = q^2（q^3 - q）$，维数为 $k = （q^2 - 2q）（q-1）（q^2-1）$，最小距离为 $d \geq （q+1）^2 - q（q-1） = 3q+1$。

请注意，该码比第 *6* 节中用相同参数 ρ_1、ρ_2、ρ_3 得到的码更长。事实上，尽管第 *6* 节示例中所考虑曲面的方程与此处具有相同的 λ 和 μ，但每个集合 T_γ 的基数都更小，集合 Γ 的基数也更小。因此，比较由此处考虑的厄米锥得到的码与第 *6* 节中的码并非显而易见。

此处描述的锥构造有望产生良好的分层码，但缺乏更一般的曲面框架所具备的灵活性。例如，我们在第 4 节和第 6 节示例族中的曲面关于 x 和 z 对称，因此可以纤维化为两条正交的曲线纤维化，而这两条纤维化都将具有固定 y 的纤维划分开来。这些曲线可以产生具有多种中间码选择的分层码，即在中间层具有局部恢复和可用性的码。探索由这些代数几何码及其相关码所能获得的恢复结构，是未来研究的一片沃土。

Acknowledgments

本研究源于由 B. Malmskog、C. Salgado 和 L. Vicino 在 2024年7月7日至12日于巴西里约热内卢 IMPA 举办的研讨会“有限域与编码理论多样性”期间主持的项目“来自高维簇的局部可恢复码”。我们谨此感谢 IMPA 的热情接待。

C. Araujo 的部分经费由 CNPq 和 FAPERJ 提供。L. Costa 的部分经费由 CAPES 提供。B. Malmskog 的部分经费由美国国家科学基金会资助，项目编号为 DMS-2137661。C. Salgado 和 L. Vicino 的部分经费由 NWO 开放竞争 ENW – XL 资助项目（项目“有理点：新维度” - OCENW.XL21.XL21.011）。

本研究的部分工作是在 B. Malmskog 访问普林斯顿高等研究院（IAS）并拜访 C. Salgado 期间完成的。他们感谢该研究院的热情接待。C. Salgado 在高等研究院访问期间，部分经费由 James D. Wolfensohn基金和美国国家科学基金会依据资助编号 DMS-1926686 共同提供。

References

[1] K. Aguilar、A. Alvarez、R. Ardila、P.S. Ocal、C. Rodriguez Avila 和 A. V´ arilly-Alvarado, *Locally recoverable algebro-geometric codes with multiple recovery sets from projective bundles*，《设计、编码与密码学》，即将发表。[2] A. Barg、K. Haymaker、E. W. Howe 和 G. Matthews，A. V´ arilly-Alvarado, *Locally recoverable codes from algebraic curves and surfaces*，《编码理论与密码学的代数几何》（E. Howe、K. Lauter 和 J. Walker 编），女性数学家协会第 9 卷，（2017），95–127。[3] S. Ballentine、A. Barg、S. Vl˘ adut., *Codes with hierarchical locality from covering maps of curves*，《IEEE信息论汇刊》65.10（2019），6056-6071。[4] P. Beelen、M. Montanucci、L. Vicino, *Weierstrass semigroups and automorphism group of a maximal curve with the third largest genus* **92** 2023 102300，《有限域及其应用》（），。[5] J. Berg、B. Malmskog、W. West, *Codes with Hierarchical Locality on Artin-Schreier Surfaces*，arXiv 预印本 arXiv:2405.19533（2024）。[6] U. G¨ortz、T. Wedhorn, *Algebraic geometry I: schemes*，Springer Fachmedien Wiesbaden（2020）。[7] J.W.P. Hirschfeld、G. Korchm´aros、F. Torres, *Algebraic curves over a finite field*，普林斯顿大学出版社（2008）。

[8] K. Haymaker、B. Malmskog、G.L. Matthews, *Locally recoverable codes with availability $t \geq 2$ from fiber products of curves*, 《通信数学进展》**12**，第 2 期，（2018），317–336。[9] K. Haymaker、B. Malmskog、G.L. Matthews, *Algebraic hierarchical locally recoverable codes with nested affine subspace recovery* **93 1**，2025 111 132 ，《设计、编码与密码学》。（），–。[10] N. Prakash、G.M. Kamath、V. Lalitha、P.V. Kumar, *Optimal linear codes with a local-error-correction property*，2012年IEEE国际信息论研讨会论文集（2012），2776–2780。[11] C. Salgado、A. V´arilly-Alvarado 和 J. F. Voloch, *Locally Recoverable Codes on Surfaces*，《IEEE信息论汇刊》，第 67 卷，第 9 期，（2021），第 5765–5777 页。[12] C. Salgado、L. Vicino *Locally recoverable codes with availability from a family of fibered surfaces* arXiv 预印本 arXiv:2512.08100（2025）。[13] B. Sasidharan、G.K. Agarwal、P. Vijay Kumar, *Codes with hierarchical locality*，2015年IEEE国际信息论研讨会论文集（2015），1257–1261。[14] H. Stichtenoth, *Algebraic function fields and codes*，Springer《数学研究生教材》，柏林、海德堡（2009）。[15] I. Tamo、A. Barg, *A family of optimal locally recoverable codes*，《IEEE信息论汇刊》**60.8**（2014），4661–4676。[16] I. Tamo、A. Barg、S.G. Vl˘adut., *Locally recoverable codes on algebraic curves* 《IEEE信息论汇刊》，**63**，8，2017 4928 4939 期（）–[17] S. Tafazolian、J. Top *Locally recoverable codes with multiple recovering sets from maximal curves* arXiv 预印本 arXiv:2509.15163（2025）。[18] L. Vicino, *Weierstrass semigroups of maximal function fields with applications to AG codes*，博士论文，DTU Compute，丹麦技术大学（2023）。