关于准循环与广义准循环代数几何码

Matteo Bonini[1], Arianna Dionigi[2], 和 Francesco Ghiandoni[3]

[1]奥尔堡大学数学科学系。mabo@math.aau.dk[2]佛罗伦萨大学数学与计算机科学系。arianna.dionigi@unifi.it[3]普里莫斯卡大学数学系。francesco.ghiandoni@famnit.upr.si

arXiv:2602.05097v1 [cs.IT] 4 Feb 2026

摘要

我们介绍了由代数曲线构造拟循环（QC）码和广义准循环（GQC）码的新方法。与以往基于椭圆曲线的方法不同，我们的方法适用于作为有理函数域的库默尔扩张的曲线，包括超椭圆曲线、范数—迹曲线和厄米特曲线。这使得构造具有灵活余指标的准循环码成为可能。我们利用已知的自同构群分类推导出明确的参数公式。

关键词：准循环码、代数几何码、代数曲线。**数学主题分类代码：**14G50 - 11T71 - 94B27 - 08A35

引言

纠错码是数字通信中的基础工具，通过引入冗余来保护经噪声信道传输的信息，从而实现错误检测与纠正。自 20 世纪 40 年代末 Golay、Hamming 和 Shannon 的开创性工作以来，编码理论为满足通信系统日益增长的需求并适应数学方法的进步而迅速发展。在研究最广泛的码族中，循环码和拟循环码（QC）因其强大的代数结构、紧凑的生成矩阵以及高效的编码和译码算法而备受重视 [18]。尽管循环码历史悠久且已得到广泛研究，但其是否渐近良好仍是未知问题，这一问题已悬而未决五十余年 [21]。相比之下，四十多年前就已证明，拟循环码能够达到渐近良好的参数 [9]。

近年来，准循环码因其在后量子密码学中的重要性而重新受到关注。在后量子密码学中，具有结构的线性码在设计安全且高效的密码学原语方面发挥着重要作用 [22]。这种日益增长的关注促使研究者寻求兼具优良参数和结构灵活性的新构造。

准循环码通过要求在多个位置的移位下保持不变来推广循环码，这些位置的数量称为余指标。这种对称性带来了高度结构化的生成矩阵，因此只需存储少量行即可，大幅降低内存需求，并加快编码和译码过程。更一般地说，广义准循环码可视为一组生成多项式，是对循环码范式的扩展。

传统上，基于代数曲线构造准循环码主要聚焦于椭圆曲线 [28], ，利用其自同构群来定义码的结构。然而，这种方法存在内在局限：椭圆曲线的自同构的阶至多为 6，因此可实现的余指标和由此带来的设计灵活性都受到限制。相比之下，具有较大循环自同构群的曲线天然适用于构造准循环码，其余指标可取群阶的任意除数，从而为实际应用提供了宝贵的自由度。

本文基于自同构群在适当代数曲线的有理点集上的作用，提出了在$\mathbb{F}_{q^r}$ （ $r \geq 1$）上构造代数几何准循环码和广义准循环码的一般方法。我们给出了由若干类曲线得到的显式构造，并特别

着重讨论由有理函数域的库默尔扩张得到的构造。我们的框架还给出了具体实例，展示了如何构造具有多种余指标的准循环码。

我们的方法尤其适用于一大类曲线，其中包括超椭圆曲线、范数迹曲线、厄米特曲线以及后者的一些著名商曲线。与椭圆情形不同，这些曲线通常具有阶显著更高的自同构，且这些自同构往往构成循环群。因此，余指标等于群阶任意一个除子的准循环码都存在。此外，当群作用仅使用一个轨道时，循环码本身便作为一种特殊情形出现，这凸显了循环对称性与几何构造之间微妙而重要的联系。

所考虑的若干曲线在 $\mathbb{F}_{q^2}$上是极大曲线，因此可得到码率和相对最小距离渐近良好的准循环码。更一般地，增大亏格往往会改善Singleton缺陷，从而进一步提升性能。在超椭圆情形下，具有循环自同构群的极大曲线实例同样能提供优良参数，并且在亏格和余指标的选择上具有灵活性。

1 预备知识

除非另有说明，我们将考虑 $q = p^h$ ，其中 p 为素数， $h > 0$为整数，并用 $\mathbb{F}_q$表示含有 q 个元素的有限域。

在某些情况下，我们还会考虑定义在基域的域扩张 $\mathbb{F}_{q^r}$ 上的代数曲线，例如研究极大曲线、德利涅–卢斯蒂格曲线，或其他自然定义在比 $\mathbb{F}_q$更大的域上的曲线族时。出现这种情况时，曲线及其函数域相应的标量扩张均视为隐含存在。

1.1 代数曲线

令 $\mathbb{K}$ 为 $\mathbb{F}_q$的代数闭包。我们用 $\mathbb{P}^n$ （分别用 $\mathbb{A}^n$）表示定义在 $\mathbb{K}$上的 n维射影（分别为仿射）空间，并用 PG(n, q)（分别用 AG(n, q) 或 $\mathbb{F}_q^n$）表示 $\mathbb{P}^n$ （分别为 $\mathbb{A}^n$）的 $\mathbb{F}_q$-有理点集合。

设 $F(X, Y) \in \mathbb{F}_q[X, Y]$ 是定义仿射几何不可约平面代数曲线 $\mathcal{X}$的多项式，该曲线由方程 $F(X, Y) = 0$定义在 $\mathbb{F}_q$上。 $\mathcal{X}$的次数定义为 deg($\mathcal{X}$) = deg(F)。它在 $\mathbb{K}$上的函数域记为 $\mathbb{K}(\mathcal{X})$，其 $\mathbb{F}_q$-有理函数子域记为 $\mathbb{F}_q(\mathcal{X})$。我们用 Div$_q$($\mathcal{X}$) 表示定义在 $\mathbb{F}_q$上的 $\mathcal{X}$的除子群；用 Aut$_{\mathbb{K}}$($\mathcal{X}$)（分别用 Aut($\mathcal{X}$)）表示 $\mathcal{X}$的 $\mathbb{K}$-自同构群（分别为 $\mathbb{F}_q$-自同构群）。设 $P = (u, v) \in \mathbb{A}^2(\mathbb{K})$ 是仿射平面上的一个点，并考虑其展开式

$$F(X + u, Y + v) = F_0(X, Y) + F_1(X, Y) + F_2(X, Y) + \cdots + F_n(X, Y),$$

其中每个 F_i 要么为零，要么是次数为 i的齐次多项式，而 n 是 F的次数。 P在 $\mathcal{X}$上的重数 记作 $m_P(\mathcal{X})$ 或 $m_P(F)$，定义为满足$F_m \neq 0$的最小整数 m。由方程 $F_m = 0$ 给出的平面曲线称为 P处 $\mathcal{X}$ 的切锥 ，切锥的任一线性分支称为 P处 $\mathcal{X}$ 的切线 。

点 P位于曲线 $\mathcal{X}$上，当且仅当 $m_P(\mathcal{X}) \geq 1$。若此条件成立，当 $m_P(\mathcal{X}) = 1$时，称 P为 $\mathcal{X}$上的简单 点（或非奇点）；而当 $m_P(\mathcal{X}) > 1$时，则称其为奇异 点。无穷远点的定义类似，即指射影闭包中位于无穷远直线上的 $\mathcal{X}$ 的点。我们用 Sing($\mathcal{X}$) 表示 $\mathcal{X}$的所有奇异点的集合，包括仿射平面内的点和无穷远点。

令 $H \leq \mathrm{Aut}_{\mathbb{K}}(\mathcal{X})$，并考虑不变域

$$\mathbb{K}(\mathcal{X})^H = \{f \in \mathbb{K}(\mathcal{X}) \mid \sigma(f) = f \text{ for all } \sigma \in H\}.$$

令 $\mathcal{X}/H$ 表示函数域为 $\mathbb{K}(\mathcal{X})^H$ 的非奇异射影曲线。域扩张 $\mathbb{K}(\mathcal{X})$:$\mathbb{K}(\mathcal{X})^H$ 是伽罗瓦扩张，其群为 H，并记

$$\pi \colon \mathcal{X} \longrightarrow \mathcal{X}/H$$

对于相应的商态射。

对于点 $P \in \mathcal{X}$，稳定子 H_P是固定 P的 H的子群，而 P处的分歧指数为 $e_P = |H_P|$。具有 $e_P > 1$ 的点是分歧点，它们在 π 下的像是支点。

群 H 作用于 $\mathcal{X}$ 的点集，并将其划分为若干轨道

$$\mathcal{O}(P) = \{\sigma(P) \mid \sigma \in H\}.$$

根据轨道-稳定子定理，

$$|\mathcal{O}(P)| \cdot |H_P| = |H|.$$

若 $|\mathcal{O}(P)| = |H|$，则称一个轨道为长轨道；否则称为短轨道。点 $Q \in \mathcal{X}/H$是分支点，当且仅当位于其上方的轨道是短轨道。已知 H 只有有限多个短轨道，并且覆盖 π 是非分歧的，当且仅当每个轨道都是长轨道。

若亏格 $g(\mathcal{X}) \geq 2$，则 $\mathrm{Aut}_{\mathbb{K}}(\mathcal{X})$ 是有限群（例如参见 [15, 第 11]章）。经典的 Hurwitz 界，

$$|\mathrm{Aut}_{\mathbb{K}}(\mathcal{X})| \leq 84(g(\mathcal{X}) - 1),$$

当 p 整除 $|\mathrm{Aut}_{\mathbb{K}}(\mathcal{X})|$时，在正特征下通常不成立。尽管如此，在附加假设下仍有更强的界。特别地，下述结果适用于阿贝尔子群。

定理 1.1 ([15, 定理 11。79])。 设 H 是 $\mathrm{Aut}_{\mathbb{K}}(\mathcal{X})$的阿贝尔子群。则

$$|H| \leq \begin{cases} 4g(\mathcal{X}) + 4, & \text{if } p \neq 2, \\ 4g(\mathcal{X}) + 2, & \text{if } p = 2. \end{cases}$$

1.2 线性码

这里回顾编码理论中的一些基本定义（关于这些概念的完整介绍，请参阅 [16]）。

设 k, n 是两个正整数，满足 $k \leq n$。维数为 k、长度为 n 的 q 元线性码（或称定义在 $\mathbb{F}_q$ 上的 $[n, k]$ 码）是一个 k 维向量子空间 $\mathcal{C} \subseteq \mathbb{F}_q^n$。 $\mathcal{C}$ 中的元素称为码字。 $\mathcal{C}$ 的生成矩阵是任意一个 $k \times n$ 矩阵 G，其各行构成 $\mathcal{C}$ 在 $\mathbb{F}_q$ 上的一组基。

通常，线性码配备汉明度量。

对于 $x \in \mathbb{F}_q^n$， x 的汉明重量是 x 的非零坐标个数，即，

$$\mathrm{wt}(x) = |\mathrm{supp}(x)|,$$

其中 $\mathrm{supp}(x) = \{i : x_i \neq 0\}$。 $v, w \in \mathbb{F}_q^n$ 之间的汉明距离 定义为

$$d(v, w) = \mathrm{wt}(v - w).$$

线性码 $\mathcal{C}$ 的最小（汉明）距离定义为

$$d(\mathcal{C}) = \min\{\mathrm{wt}(c) \mid c \in \mathcal{C},\, c \neq 0\}.$$

编码理论中最基本的界之一是 Singleton界。

命题 1.2 (Singleton界). 设 $\mathcal{C}$ 是一个最小距离为 d的 $[n, k]$ 线性码。那么

$$d \leq n - k + 1.$$

$[n, k, d]$ 码 $\mathcal{C}$ 的 Singleton缺陷定义为

$$s(C) = n - k + 1 - d.$$

满足 $s(\mathcal{C}) = 0$ 的码称为最大距离可分（MDS）码；等价地， $\mathcal{C}$ 以等号达到 Singleton界。

MDS码在经典和现代编码理论中都发挥着核心作用，例如出现在 Reed–Solomon码以及若干分布式存储构造中。若码 $\mathcal{C}$ 的 Singleton缺陷为 $s(\mathcal{C}) = 1$，则称其为近最大距离可分（AMDS）码。若码 $\mathcal{C}$ 满足 $\mathcal{C}$ 和$\mathcal{C}^{\perp}$ 均为 AMDS码，则称其为近最大距离可分码。

MDS码和 AMDS码都满足非常严格的组合约束：例如，它们的参数对 $\mathcal{C}$ 和 $\mathcal{C}^{\perp}$的最小距离施加了紧密关系，而且只有非常受限的长度 n 和字母表大小 q 族能够支撑此类码。由代数曲线上构造的代数几何（AG）码也形成了值得关注的相关码族，其中 Singleton缺陷的上界由曲线的亏格给出；这提供了大量码类，其参数同样受几何或组合限制支配，并在 MDS/AMDS 特性与更一般的情形之间起到衔接作用。

1.3 代数几何码

设 $\mathcal{X}$ 是定义在有限域 $\mathbb{F}_q$ 上的射影、光滑、几何不可约代数曲线，记 $\mathbb{F}_q(\mathcal{X})$ 为其函数域。对于一个除子

$$G = \sum_{P \in \mathcal{X}} n_P P \in \mathrm{Div}_q(\mathcal{X}),$$

相应的 *Riemann–Roch*空间 定义为

$$\mathscr{L}(G) = \{ f \in \mathbb{F}_q(\mathcal{X})^{\times} \mid (f) + G \geq 0 \} \cup \{0\},$$

其中（f）是 f 的主除子。这是一个有限维的 $\mathbb{F}_q$-向量空间，其维数记为 $\ell(G)$。

设 P_1、……、P_n 是 $\mathcal{X}$ 上的 n 个互不相同的 $\mathbb{F}_q$-有理点，并设 $G \in \mathrm{Div}_q(\mathcal{X})$ 是一个除子，使得对于每个 $i = 1$、……、n，都有 $v_{P_i}(G) = 0$，从而 $\mathrm{Supp}(G)$ 与 $\{P_1, \ldots, P_n\}$ 不相交。考虑求值映射

$$\begin{aligned} \mathrm{ev} = \mathrm{ev}_{P_1,\ldots,P_n} : \mathscr{L}(G) &\longrightarrow \mathbb{F}_q^n, \\ f &\longmapsto \left(f(P_1), \ldots, f(P_n)\right). \end{aligned}$$

如果定义

$$D := P_1 + \cdots + P_n,$$

the与 D 和 G相关联的代数几何码（*AG*码）is

$$\mathcal{C}(D, G) := \mathrm{ev}(\mathscr{L}(G)) \subseteq \mathbb{F}_q^n.$$

AG码的标准性质（参见 [25,第II.2]节）给出以下参数：

$$n = \deg(D), \qquad k = \ell(G) - \ell(G - D), \qquad d \geq n - \deg(G).$$

此外，根据Riemann–Roch定理，若

$$n > \deg(G) > 2g - 2,$$

则 G 是非特殊的，因此

$$k = \deg(G) - g + 1.$$

2 广义准循环代数几何码的构造

准循环码是指在一种具有特定结构的分块循环移位下保持不变的线性码。下面对其进行形式化定义。

定义 2.1。设 q为素数幂，且设 $\ell, m \in \mathbb{Z}_{>0}$。若线性码 $\mathcal{C} \subseteq \mathbb{F}_q^{\ell m}$在长度为 m的分块循环移位下保持不变，则称其为指标为 ℓ(余指标为 m）的拟循环码。更确切地说，将每个码字 $c \in \mathbb{F}_q^{\ell m}$写为

$$c = (c_0, c_1, \ldots, c_{\ell-1}), \qquad c_j = (c_{0,j}, c_{1,j}, \ldots, c_{m-1,j}) \in \mathbb{F}_q^m,$$

因此，将 $\mathbb{F}_q^{\ell m}$视为由 ℓ 个区块的直积，每个区块的长度为 m。

令 τ： $\mathbb{F}_q^m \to \mathbb{F}_q^m$表示循环移位

$$\tau(c_{0,j}, c_{1,j}, \ldots, c_{m-1,j}) = (c_{m-1,j}, c_{0,j}, \ldots, c_{m-2,j}),$$

并定义算子 T： $\mathbb{F}_q^{\ell m} \to \mathbb{F}_q^{\ell m}$为

$$T(c_0, c_1, \ldots, c_{\ell-1}) = (\tau(c_0), \tau(c_1), \ldots, \tau(c_{\ell-1})).$$

若 $\mathcal{C}$ 满足

$$T(\mathcal{C}) = \mathcal{C} \quad \textit{(equivalently, } T^k(\mathcal{C}) = \mathcal{C} \textit{ for all } k \in \mathbb{Z}\textit{).}$$

下面的定义通过允许分块长度发生变化，推广了这一概念 y.

定义 *2.2*。*</style}*令 q为一个素数幂，并令 m_0、 m_1、…、 $m_{\ell-1} \in \mathbb{Z}_{>0}$。一个线性码

$$\mathcal{C} \subseteq \mathbb{F}_q^{m_0} \times \mathbb{F}_q^{m_1} \times \cdots \times \mathbb{F}_q^{m_{\ell-1}}$$

称为分块长度为（m_0、 m_1、 . . . 、 $m_{\ell-1}$）的广义准循环码（GQC），如果它在分块循环移位下保持不变。

明确地，将每个码字写成

$$c = (c_0, c_1, \ldots, c_{\ell-1}), \qquad c_j = (c_{0,j}, c_{1,j}, \ldots, c_{m_j-1,j}) \in \mathbb{F}_q^{m_j}.$$

对于每个 j，令τ_j： $\mathbb{F}_q^{m_j} \to \mathbb{F}_q^{m_j}$表示循环移位

$$\tau_j(c_{0,j}, c_{1,j}, \ldots, c_{m_j-1,j}) = (c_{m_j-1,j}, c_{0,j}, \ldots, c_{m_j-2,j}),$$

并定义

$$T(c_0, c_1, \ldots, c_{\ell-1}) = (\tau_0(c_0), \tau_1(c_1), \ldots, \tau_{\ell-1}(c_{\ell-1})).$$

那么，如果满足以下条件， $\mathcal{C}$ 就是一个广义准循环码

$$T(\mathcal{C}) = \mathcal{C} \quad \textit{(equivalently, } T^k(\mathcal{C}) = \mathcal{C} \textit{ for all } k \in \mathbb{Z}\textit{).}$$

注 2.3. 注意，若 $\mathcal{C}$是一个长度为 $(m_1, \ldots, m_s)$ 且满足 $m_1 = \cdots = m_s$ 的广义准循环码，那么 $\mathcal{C}$就是一个长度为 $s \cdot m_1$的准循环码。

从现在起，我们将重点研究没有仿射奇点且有唯一无穷远点的代数曲线，该点记作 P_∞。

定理 2.4. 设 $\mathcal{X}$ 是有限域 $\mathbb{F}_q$上的一条亏格为 g 的曲线。设 $\sigma \in \mathrm{Aut}(\mathcal{X})$ 是 $\mathcal{X}$的一个自同构，且固定 P_∞。设 $\mathcal{O}_1, \ldots, \mathcal{O}_m$是 $\mathcal{X}(\mathbb{F}_q)$ 在 σ作用下的 m 个互异长轨道，并设除子 D_1 和 D_2 定义如下

$$D_1 = \sum_{i=1}^{m} \sum_{P_i \in \mathcal{O}_i} P_i,$$

$$D_2 = tP_\infty$$

其中 $2g - 2 < t < m \cdot ord(\sigma)$。代数几何码

$$\mathcal{C}(D_1, D_2) = (f(P_1), f(\sigma(P_1)), \ldots, f(\sigma^{ord(\sigma)-1}(P_1)), \ldots, f(P_m), f(\sigma(P_m)), \ldots, f(\sigma^{ord(\sigma)-1}(P_m)))$$

其中 $f \in \mathscr{L}(D_2)$是一个 $[m \cdot ord(\sigma)\ t + 1 - g, d \geq n - t]_q$准循环码，其余指标为 $ord(\sigma\ \ )$.

证明。 由 [25,推论 2.2.3] 可知，若

$$2g - 2 < t < m \cdot \mathrm{ord}(\sigma),$$

那么 $k = t + 1 - g$和 $d \geq n - t$。由于 σ固定了 P_∞，我们有 $\sigma^{-1}(P_\infty) = P_\infty$。对于每个 $f \in \mathscr{L}(D_2)$,

$$v_{P_\infty}(\sigma(f)) = v_{\sigma^{-1}(P_\infty)}(f) \geq t,$$

且对于每个 $P \in \mathcal{X} \setminus \{P_\infty\}$,

$$v_P(\sigma(f)) = v_{\sigma^{-1}(P)}(f) \geq 0.$$

因此 $\sigma(f) \in \mathscr{L}(D_2)$。

设 $\mathrm{ord}(\sigma) = r$，并设 $\{f_1, \ldots, f_k\}$ 是 $\mathscr{L}(D_2)$ 的一组基。码 $\mathcal{C}(D_1, D_2)$ 的生成矩阵 G 为

$$G = \begin{pmatrix} f_1(P_1) & \cdots & f_1(\sigma^{r-1}(P_1)) & f_1(P_2) & \cdots & f_1(\sigma^{r-1}(P_2)) & \cdots & f_1(P_m) & \cdots & f_1(\sigma^{r-1}(P_m)) \\ f_2(P_1) & \cdots & f_2(\sigma^{r-1}(P_1)) & f_2(P_2) & \cdots & f_2(\sigma^{r-1}(P_2)) & \cdots & f_2(P_m) & \cdots & f_2(\sigma^{r-1}(P_m)) \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ f_k(P_1) & \cdots & f_k(\sigma^{r-1}(P_1)) & f_k(P_2) & \cdots & f_k(\sigma^{r-1}(P_2)) & \cdots & f_k(P_m) & \cdots & f_k(\sigma^{r-1}(P_m)) \end{pmatrix}$$

$$= (ev(f_1), \ldots, ev(f_k))^T.$$

为了证明 $\mathcal{C}(D_1, D_2)$ 是拟循环的，我们必须证明：如果

$$\gamma = (\gamma_1, \ldots, \gamma_n) = \sum_{i=1}^{k} c_i \, ev(f_i)$$

属于 $\mathcal{C}(D_1, D_2)$，那么向量

$$\gamma' = (\gamma_r, \gamma_1, \ldots, \gamma_{r-1}, \gamma_{2r}, \gamma_{r+1}, \ldots, \gamma_{2r-1}, \ldots, \gamma_n, \gamma_{n-r+1}, \ldots, \gamma_{n-1})$$

也属于 $\mathcal{C}(D_1, D_2)$。

我们知道，当且仅当 $\gamma' \in \mathcal{C}(D_1, \ D_2)$

$$\gamma' = (g(P_1), g(\sigma(P_1)), \ldots, g(\sigma^{r-1}(P_1)), g(P_2), \ldots, g(\sigma^{r-1}(P_2)), \ldots, g(P_m), \ldots, g(\sigma^{r-1}(P_m)))$$

对某个 $g \in \mathscr{L}(D_2)$。等价地，对每个 $i \in \{1, \ldots, r\}$,

$$\gamma_i = g(\sigma^i(P_1)),$$

并且对每个长度为 r 的块同样如此。

事实上，对每个 $i \in \{1, \ldots, r\}$ 以及每个 $\ell \in \{0, \ldots, m-1\}$,

$$\gamma_{i+\ell r} = \sum_{j=1}^{k} c_j f_j(\sigma^{\,i-1}(P_{\ell+1})) = \sum_{j=1}^{k} c_j f_j(\sigma^{-1}(\sigma^i(P_{\ell+1}))) = \sum_{j=1}^{k} c_j \sigma(f_j)(\sigma^i(P_{\ell+1})).$$

该结论可通过选取

$$g = \sum_{j=1}^{k} c_j \sigma(f_j),$$

根据证明的第一部分，它属于 $\mathscr{L}(D_2)$。 □

定理 2.5. 设 $\mathcal{X}$ 是定义在有限域 $\mathbb{F}_q$上、亏格为 g 的曲线。设 σ 是 $\mathcal{X}$的一个自同构，且它固定 P_∞。设 $\mathcal{O}_1$，...，$\mathcal{O}_s$ 是 $\mathcal{X}$在 σ作用下的 s 条互不相同的非平凡轨道，其长度分别为 m_1，.....，m_s，$m_i \,|\, \mathrm{ord}(\sigma)$。考虑由下式定义的除子 D_1 与 D_2

$$D_1 = \sum_{i=1}^{s} \sum_{P_i \in \mathcal{O}_i} P_i, \ D_2 = t\overline{P}$$

与 $2g - 2 < t < m_1 + \cdots + m_s$。那么代数几何码

$$\mathcal{C}(D_1, D_2) = (f(P_1), f(\sigma(P_1)), \ldots, f(\sigma^{ord(\sigma)-1}(P_1)), \ldots, f(P_m), f(\sigma(P_m)), \ldots, f(\sigma^{ord(\sigma)-1}(P_m))),$$

其中 $f \in \mathscr{L}(D_2)$ 是一个余指标为 $(m_1, \ldots, m_s)$ 的 $[n, k, d]_q$广义准循环码，$n = m_1 + \cdots + m_s$、$k = t + 1 - g$ 和 $d \geq n - t$。

证明。 证明是对定理 2.4 的证明的直接推广。 □

3 由分离多项式定义的曲线

本节将展示如何利用定理 2.4 构造一大类明确的准循环代数几何码。在某些情况下，我们还将讨论相应自同构群的结构。

假设 char($\mathbb{F}_q$) $\neq 2$。设 $\mathcal{X}$ 为定义在 $\mathbb{F}_{q^r}$ 上的射影平面曲线，其中 q 是素数 p 的幂，其仿射形式为

$$X^m = B(Y), \tag{1}$$

其中 $B(Y) \in \mathbb{F}_{q^r}[Y]$ 是次数为 d 的可分多项式， $m \geq 2$, $d \geq 1$, $m \not\equiv 0 \pmod{p}$，且 gcd(m, d) $= 1$。此外，我们假设 deg($\mathcal{X}$) ≥ 3。

这类曲线通常称为有理函数域的循环、超椭圆或库默尔扩张。它们具有一个阶为 m 的自同构 $\tau \in$ Aut($\mathcal{X}$)，定义为

$$(x, y) \longmapsto (\xi x,\, y), \qquad \xi^m = 1,$$

使得 t 循环群 $\langle\tau\rangle$ 是 Aut($\mathcal{X}$) 的正规子群，且商曲线 $\mathcal{X}/\langle\tau\rangle$ 的亏格为零。

定理总结了 $\mathcal{X}$ 的一些相关性质；参见 [25, 命题 3.73]，其中给出了函数域方面的等价表述。其他特殊情形包括 $B(Y)$为线性化多项式的情形，见 [15, 第 12 节1] 和 [2, 引理 21], ；以及$d = \deg(B(Y)) > m$的情形，见 [20, 第 5 节1]。

定理 3.1。曲线 $\mathcal{X}$： $X^m - B(Y) = 0$ 是绝对不可约曲线，且没有仿射奇点。

(i) 若 $|m - d| = 1$，则 $\mathcal{X}$ 是非奇异的。

(ii) (a) 若 $m > d + 1$，则 $P_\infty = (0 : 0 : 1)$ 是$m - d$)重奇点，属于曲线 $\mathcal{X}$。*(b)* 若 $m < d + 1$，则 $P_\infty = (0 : 1 : 0)$ 是$d - m$)重奇点，属于曲线 $\mathcal{X}$。*(c)* 在这两种情形下， P_∞ 是 $\mathcal{X}$唯一分支的中心；此外， P_∞ 是$\mathcal{X}$.的唯一无穷远点

(iii) 自然投影 $\pi\colon \mathcal{X} \to \mathcal{X}/\langle\tau\rangle \cong \mathbb{P}^1$, $\pi(x, y) = y$ 的次数为 m.。此覆盖恰好在 $B(Y)$ 的根 $\alpha_1, \ldots,$ α_d 处分支。特别地， $\mathcal{X}$ 的亏格为 $g = (m-1(d-1)\,2$。

(iv) 设 $\mathbb{K} = \overline{\mathbb{F}_q}$, 并令 $\mathbb{K}(x, y) = \mathbb{K}(\mathcal{X})$，其中 $x^m = B(y)$ 表示 $\mathcal{X}$. 的函数域。那么，$\mathbb{K}(y) \subset \mathbb{K}(x, y)$ 是一个次数为 m 的循环伽罗瓦扩张，并且 $\mathrm{Gal}(\mathbb{K}(x, y)/\mathbb{K}(y)) = \langle\tau\rangle$.

(v) 设 $G := \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}(x, y))$。则商群 $G := G/\langle\tau\rangle$ 同构于$\overline{\mathrm{P}}\mathrm{GL}(2, \mathbb{K})$ 的一个子群，该子群保持 $\mathcal{X}$ 的所有魏尔斯特拉斯点构成的集合 $\{P_1, \ldots, P_d, P_\infty\}$，其中 $P_i = (0, \alpha_i)$ 对于 $i = 1, \ldots, d$.

G群和 $\mathbb{K}(\mathcal{X})$ 的子域 $\mathbb{K}(\mathcal{X})^G$分别称为 $\mathcal{X}$ 的约化自同构群 和 G 在 $\mathbb{K}(\mathcal{X})$ 中的不变量 （或 G-不变量）。根据伽罗瓦理论和定理 3.1(iii)，域扩张 $\mathbb{K}(\mathcal{X})^G \subseteq \mathbb{K}(y)$ 是有理的。特别地， $\mathbb{K}(\mathcal{X})^G$的任意生成元都是一个 G-不变量。因此， $\mathbb{K}(\mathcal{X})^G = \mathbb{K}(z)$，其中不变量 z 可选为 y 中的一个次数为 $|G|$的有理函数。

对于由仿射方程 $F(X, Y) = 0$定义的一般平面曲线，要将显式的 G-不变量确定为 x 和 y 中的有理函数，通常是一项困难的工作；当定义多项式 $F(X, Y)$ 过于复杂，或者 G 的生成元作用并非由线性变换给出时，这在计算上可能难以实现。

相比之下，对于由形如 (1) 的方程定义的平面曲线，更容易得到 $z = \phi(y)$ 的显式表达式。关于 $d = \deg(B(Y)) > m$的情形，参见 [20, 引理 12]；而关于 $\mathcal{X}$ 为厄米特曲线的情形，参见 [13]。

注 3.2. 由于 $\mathcal{X}/\langle\tau\rangle$ 的亏格为零，且 $G = \mathrm{Aut}(\mathcal{X}/\langle\tau\rangle)$ 在射影直线上的作用是 $\mathrm{PGL}(2, \mathbb{K})$的一个子群，因此 G 同构于以下群之一： C_n、 D_n、 A_4、 S_4、 A_5、初等阿贝尔群与循环群的半直积、$PSL(2, q^r)$ 和 $PGL(2, q^r)$，其中

- $C_n = \langle\sigma\rangle$，其中 $\sigma(y) = \zeta y$，且 ζ 是一个本原 n次单位根。
- $D_{2n} = \langle\sigma, \lambda\rangle$，其中 $\sigma(y) = \xi y$、 $\lambda(y) = \frac{1}{y}$，且 ξ 是一个本原 n 次单位根。

- $A_4 = \langle \sigma, \mu \rangle$，其中 $\sigma(y) = -y$ 和 $\mu(y) = i\frac{y+1}{y-1}$，且 $i^2 = -1$。
- $S_4 = \langle \sigma, \mu \rangle$，其中 $\sigma(y) = iy$ 和 $\mu(y) = i\frac{y+1}{y-1}$，$i^2 = -1$。
- $A_5 = \langle \sigma, \rho \rangle$，其中 $\sigma(y) = \xi y$，$\rho(y) = -\frac{y+b}{by-1}$，$\xi$ 是本原五次单位根，且 $b = -i(\xi + \xi^4)$ 满足 $i^2 = -1$。

见 *[19]*。此外，在 *[23]* 中，确定了定义在特征为 $p \neq 2$ 的有限域上的亏格为 $g \geq 2$ 的循环曲线的所有可能自同构群（详情亦见 *[20,* 定理 *17]*）。

注 *3.3*。令 $m \mid q^r - 1$ 和 $\ell := \#\{v \in \mathbb{F}_{q^r} : B(v) = 0\} \leq d$. 那么容易看出，$\tau$ 定义在 $\mathbb{F}_{q^r}$ 上，并在 $\mathcal{X}(\mathbb{F}_{q^r})$ 上诱导出 $\ell + 1$ 个短轨道 $\{P_1\}, \ldots, \{P_\ell\}, \{P_\infty\}$，即 τ 固定了 $\mathcal{X}$ 的 $\ell + 1\mathbb{F}_{q^r}$-有理点。因此，由定理 *2.4* 可知存在一个余指标为 m 的 $[n, t-(m-1)(d-1)_2 \quad +1, \geq n-t]$ 准循环码，其中 $n = {}^{\mathcal{X}(\mathbb{F}_{q^r})}{}_m{}^{-\ell-1}$，且 $(m-1)(d-1) - 2 < t < n$.

下文将详细分析若干由形如 (1) 的分离多项式定义的著名平面曲线族。对于每个曲线族，我们都确定其自同构群，并特别考察群中元素对曲线有理点的作用。在此分析的基础上，我们推导出若干具有优良参数的准循环码和广义准循环码的存在性。本节最后给出一个例子，说明如何从自同构群为循环群的曲线出发，构造余指标参数具有高度灵活性的准循环码。

例 3.4. 令 $r = 1$ 并假设 $q \equiv 1$ (模 21)。考虑定义在 $\mathbb{F}_q$ 上的曲线 $\mathcal{X}: \quad x^3 = y^8 - y$，其亏格为 $g = 7$。容易验证，$\mathcal{X}$ 具有一个阶为21 的循环自同构群 G，使得 $G = G_{P_\infty} = \langle \sigma \rangle$，其中自同构 σ 由 $(x, y) \mapsto (\epsilon x, \xi y)$ 给出，ϵ、$\xi \in \mathbb{F}_q^*$ 是满足 $\epsilon^3 = \xi^7 = 1$ 的非平凡元素。由定理 *1.1*，群 G 是 $\mathcal{X}$ 的最大循环自同构群。

直接计算表明，σ 在 $\mathcal{X}(\mathbb{F}_q) \setminus \{P_\infty\}$ 上诱导出两个短轨道，其长度分别为1 和7，以及 $\#\mathcal{X}(\mathbb{F}_q)_{21} - 9$ 个长轨道。

对于 $q = 127$，通过 MAGMA *[5]* 计算可知，自同构 $\sigma(x, y) = (19x, 2y)$ 生成了七个长度为21的轨道，记为 $\mathcal{O}_1$，……，$\mathcal{O}_7$。因此，根据定理 *2.4*，代数几何码 $\mathcal{C}(D_1, D_2)$ 是一个余指标为21 的 $[147, t-6, \geq 147-t]_{127}$ 准循环码，其中 $D_1 = \sum_{i=1}^{7} \sum_{P_i \in \mathcal{O}_i} P_i$ 且 $D_2 = tP_\infty$，适用于 $12 < t < 147$。

此外，考虑自同构 $\sigma^3(x, y) = (x, \xi y)$，也可以构造余指标为7的准循环码。在这种情况下，对域大小的条件可放宽为 $q \equiv 1$ (模 7)。

4 超椭圆曲线

函数域的库默尔扩张及其相关的超椭圆曲线族，构成了我们构造中所研究曲线的基础对象。由此类扩张得到的几何曲线自然地融入一个更广泛的框架，其中超椭圆曲线或许是最经典的例子，因为它们提供了一种能够明确描述若干结构特征的情形。

当（1）中的指数等于 $m = 2$ 时，得到的就是超椭圆曲线这一类曲线，可将其视为最简单的非平凡超椭圆曲线。在本节中，我们假设 $\mathrm{char}(\mathbb{F}_q) \neq 2$。

超椭圆曲线作为由特定对合定义的射影直线二重覆盖，在代数几何中发挥着核心作用。这种对称性通常会带来丰富且往往可计算的自同构群，从而使人们能够详细理解其几何性质与算术性质。除了理论上的重要性之外，其雅可比簇高效的算术运算也使超椭圆曲线在应用中颇具价值，尤其是在密码学领域，因为紧凑的表示和快速的群运算都十分可取。

超椭圆曲线 $\mathcal{H}$ 定义在特征不为 2 的域 K 上，具有如下形式的仿射模型

$$\mathcal{H}: \quad x^2 = f(y),$$

其中 $f(y) \in K[y]$ 是一个次数为 $d \geq 5$ 的可分多项式。$f(y)$ 的可分性确保该曲线没有仿射奇点。

从定理 3.1 中的 (iii) 可以看出，投影 $(x,y) \mapsto y$ 定义了一个从 $\mathcal{H}$ 到 $\mathbb{P}^1$ 的次数为 2 的态射；因此，超椭圆曲线是射影直线的二重覆盖，且分支恰好位于 $f(y)$ 的根处（根据 d 的奇偶性，也可能在无穷远点处分支）。这类曲线具有一个特定对合，称为超椭圆对合，其定义为

$$(x,y) \longmapsto (-x,y),$$

它生成了 $\mathrm{Aut}(\mathcal{H})$ 的一个中心子群。

由于这种明确的结构，超椭圆曲线为具体描述许多几何和算术性质提供了天然的框架；它们也常被用作在有限域上进行构造的试验场，包括代数几何码以及自同构群的研究。

注 *4.1.* 考虑 $m=2$，设 $\mathcal{X}: x^2 - f(y) = 0$ 是一条亏格为 g 的超椭圆曲线，其定义多项式 $f \in \mathbb{F}_{q^r}[Y]$ 是次数为 $2g+1.$ 的无平方因子多项式。众所周知，$\mathcal{X}$ 没有仿射奇点，且唯一的无穷远点 P_∞ 的重数为 $2g-1$。此外，根据定理 *3.1*，以该点为中心的分支只有一个。现在，$\mathcal{X}$ 的自同构 τ 由 $(x,y) \mapsto (-x,y)$ 给出，称为超椭圆对合。由此，根据注 *3.3*，可知存在余指标为 *2* 的 $[n,k,d]_{q^r}$ 准循环码，其中 $n \le \#\mathcal{Y}(\mathbb{F}_{q^r}) - 2(g+1)$ $k = n-t+1$，且 $d \ge n-t$，其中 $2g-2 < t < n.$

从超椭圆曲线出发，可以构造具有相关参数的准循环码，既包括渐近情形（随着基域规模的增大），也包括在固定域上的情形。当基域固定且需要长码时，考虑高亏格的超椭圆曲线是有利的，因为它们可以具有许多有理点（回顾 Hasse–Weil 上界 $\#\mathcal{X}(\mathbb{F}_q) \le q+1+2g\sqrt{q}$）。另一方面，若需要较强的纠错能力，则低亏格曲线往往更为可取，因为它们通常能给出具有更大最小距离的码，如第 1.2 小节所讨论的。

特别地，借助定理 2.4，亏格2曲线可用于构造参数为$[n,k,d]_{q^r}$、最小距离为 $d=n-k-1$、且在某些情形下为 $d=n-k$（见例 4.8）的准循环码，同时对码长（余指标）的选择也相当灵活。这些方面将在下一节中更详细地加以考察。

本节最后，我们给出若干由亏格为 4 的超椭圆曲线构造的准循环码示例。根据定理 1.1，对于固定的亏格，这类曲线具有可能的最大循环自同构群；从准循环码的角度来看，这为相应余指标的选择提供了更大的灵活性。

例4.2。令 $r=1$ 和 $q \equiv 1$ 模 18，考虑曲线 $\mathcal{X}$： $x^2 = y^9 + a$ 在 $\mathbb{F}_q$上，其中 a是 $\mathbb{F}_q$中的一个 9 次幂。容易验证，$\mathcal{X}$ 在$\mathbb{F}_q$ 上具有一个阶为 18 的循环自同构群，该群由自同构 $\sigma(x,y) = (-x,\xi y)$生成，其中 $\xi \in \mathbb{F}_q$ 是一个本原 9 次单位根。此外，σ 在 $\mathcal{X}(\mathbb{F}_q) \setminus \{P_\infty\}$ 上的作用包含两个短轨道，其长度分别为 2 和 9，以及 $\frac{\#\mathcal{X}(\mathbb{F}_q) - 12}{18}$ 个长轨道。

特别地，对于 $q=73$ 曲线 $\mathcal{X}$具有 66 $\mathbb{F}_q$-有理点，而自同构 $\sigma\colon (x,y) \mapsto (-x,2y)$ 在 $\mathcal{X}(\mathbb{F}_q)$ 上诱导出三个长度为 18 的轨道。通过以与例 *3.4* 完全类似的方式选取除子 D_1 和 D_2，利用定理 *2.4* 可以构造余指标为 18 的准循环码，对每个 $6 < t < 66$均如此。

最后，由于对于 $i \in \{2,3,6\}$ 有 $\mathrm{ord}(\sigma^i) = \frac{18}{i}$，且 σ^i 在 $\mathcal{X}(\mathbb{F}_q)$ 上的作用与 σ的作用等价，因此该构造还可得到余指标为 3、6和 9的准循环码。

4.1 2属

对于亏格为2的曲线 $\mathcal{X}$，Cardona、Duursma、Gonzalez、Gutierrez、Kiyavash、Lario、Quer、Rio、Shaska 和 V¨olklein 通过一系列研究对其自同构群进行了全面分类；参见 $[6,7,10,24]$。这项研究由多位学者历经多年共同完成，如今已完整描述了 2 属曲线中可能出现的自同构群。

在特征2以外的情形下，亏格为2的曲线的自同构群分类表明，可能出现的自同构群为

$$\mathbb{Z}_2,\ \mathbb{Z}_{10},\ \mathbb{Z}_2 \times \mathbb{Z}_2,\ D_8,\ D_{12},\ \mathbb{Z}_3 \rtimes D_8,\ \mathrm{GL}(2,3),$$

以及由超椭圆对合给出的 S_5 的扩张。

由于在我们的设定中，我们尤其关注包含各种可能阶的元素的自同构群，以便让相应拟循环码的余指标具有更大的灵活性，因此我们重点关注以下情形

$$\mathrm{Aut}(\mathcal{X}) \in \{\mathbb{Z}_3 \rtimes D_8,\ \mathrm{GL}(2,3),\ \mathbb{Z}_{10}\}.$$

对于 $p \neq 2$，自同构群 G属于此列表的亏格为2的曲线已被完全确定。它们与形如

$$x^2 = f(y),$$

其中

$$f(y) = \begin{cases} y^6 - 1, & \text{if } G \cong \mathbb{Z}_3 \rtimes D_8, \\ y^5 - y, & \text{if } G \cong \mathrm{GL}(2,3), \\ y^5 + 1, & \text{if } G \cong \mathbb{Z}_{10}. \end{cases}$$

然而，在第一种情形中，稳定子 G_{P_∞} 不包含除 1、2、3、4和6 以外的其他阶元素。因此，定理 2.4 只能得到余指标为 2 、 3 、 4 或 6 的拟循环码。这类码已经在 [28], 中通过椭圆曲线上的代数几何码得到；事实上，固定无穷远点的椭圆曲线的任意自同构的阶至多为 6，参见 [28, 定理 1]和 [15, 定理 11.94]。

另一方面，曲线

$$\mathcal{X}\colon x^2 = y^5 + 1 \qquad \text{and} \qquad \mathcal{Y}\colon x^2 = y^5 - y$$

分别产生余指标为 10 和 8 的拟循环码。

注*4.3.* 令 $p \neq 2$, *5*， $q^r \equiv 1$ （模 *8*）和 $\mathcal{Y}\colon\ x^2 = y^5 - y$. 。那么，自同构 $\sigma \in G_{P_\infty}$ 由 $\sigma(x,y) = (ax, a^2y)$ 给出，其中 $a \in \mathbb{F}_{q^r}$ 是 *8* 次本原单位根。特别地，*ord(σ)* $= 8$，其在 $\mathcal{Y}(\mathbb{F}_{q^r}) \setminus \{P_\infty\}$ 上的作用诱导出两个大小分别为 *1* 和 *4* 的短轨道，即 $\{O\} = \{(0,0)\}$ 和$\{(0,1), (0,a^2), (0,-1), (0,-a^2)\}$，以及 $\#\mathcal{Y}(\mathbb{F}_q)_8$ 个长轨道。

以下命题直接由前述注记和定理 2.4 得出。

命题*4.4.* 设 $\mathcal{Y}\colon\ x^2 = y^5 - y$，并设 σ 如注*4.3* 所述。设 $\mathcal{O}_1, \ldots, \mathcal{O}_m$, $m = \#\mathcal{Y}(\mathbb{F}_{q^r})_8$ 为由 σ. 定义的所有可能的长轨道。考虑除子 $D_1 = \sum_{i=1}^m \sum_{P_i \in \mathcal{O}_i} P_i$ 和 $D_2 = tP_\infty$.。那么，对于 $2 < t < \#\mathcal{Y}(\mathbb{F}_{q^r}) - 6$，代数几何码 $\mathcal{C}(D_1, D_2)$ 是一个余指标为 *8* 的 $[\#\mathcal{Y}(\mathbb{F}_{q^r}) - 6, t-1, \geq \#\mathcal{Y}(\mathbb{F}_{q^r}) - 6 - t]_{q^r}$ 拟循环码。

对于曲线 $\mathcal{X}\colon\ x^2 = y^5 + 1$，构造基本类似，但还需要补充一些细节。下面给出具体构造。

注记 *4.5.* 设 $p \neq 2$,*5* 和 $q^r \equiv 1$ *(*模 *5)*。则 $G = G_{P_\infty} = \mathbb{Z}_2 \times Z_5 = \langle\sigma\rangle$，其中 $\sigma(x,y) = (-x, \xi y)$，且 $\xi \in \mathbb{F}_{q^r}$ 是本原五次单位根。特别地，*ord(σ)* $= 10$，其在 $\mathcal{X}(\mathbb{F}_q)$ 上的作用 $\setminus \{P_\infty\}$ 诱导出两个大小分别为 *2* 和 *5* 的短轨道，即 $\{R_1, R_2\} = \{(1,0), (-1,0)\}$ 和$\{Q_1, Q_2, Q_3, Q_4, Q_5\}$，其中 $Q_i = (0, -\xi^i)$，以及 $\#\mathcal{X}(\mathbb{F}_{q^r})_{10}$ 个长轨道。

命题 *4.6.* 设 σ 如注记 *4.5* 所述。设 $\mathcal{O}_1, \ldots, \mathcal{O}_m$, $m = \#\mathcal{X}(\mathbb{F}_{q^r})_{10}$ 是由 σ. 定义的所有可能的长轨道。考虑除子 $D_1 = \sum_{i=1}^m \sum_{P_i \in \mathcal{O}_i} P_i$, $D_2 = D_1 + \sum_{i=1}^5 Q_i + R_1 + R_2$ 和$D_3 = tP_\infty$.。那么对于 $2 < t < \#\mathcal{X}(\mathbb{F}_{q^r}) - 8$，代数几何码 $\mathcal{C}(D_1, D_3)$ 是一个余指标为 *10* 的 $[\#\mathcal{X}(\mathbb{F}_{q^r}) - 8, t-1, \geq \#\mathcal{X}(\mathbb{F}_{q^r}) - 8 - t]_{q^r}$拟循环码。此外，对于 $2 < t < \#\mathcal{X}(\mathbb{F}_q) - 1$，代数几何码 $\mathcal{C}(D_2, D_3)$ 是一个余指标为 *(2, 5, 10, . . . , 10)* 的 $[\#\mathcal{X}(\mathbb{F}_{q^r}) - 1, t-1, \geq \#\mathcal{X}(\mathbb{F}_{q^r}) - 1 - t]_{q^r}$广义准循环码。

此外，我们注意到，只需考虑 $\sigma^2(x,y) = (x, \xi^2 y)$ 及其在 $\mathcal{X}$ 的有理点上的作用，便可再次应用定理 2.4，从而得到余指标为 5 的准循环码。这里我们给出一些例子，它们可以用 Magma [5] 直接计算并验证。

例4.7. 设 $r=1$ 与 $q=41.$，则对于具有 54 $\mathbb{F}_q$-有理点的曲线 $\mathcal{Y}$: $x^2=y^5-y$，存在一个阶为 8 且固定 P_∞ 的自同构，由 $\sigma(x,y)=(3x,9y)$ 给出。通过直接计算可得，σ 生成 6 条长轨道 $\mathcal{O}_1$，.....，$\mathcal{O}_6$，由

$$\begin{aligned}
\mathcal{O}_1 &= \{(7,19),(21,7),(22,22),(25,34),(34,19),(20,7),(19,22),(16,34)\},\\
\mathcal{O}_2 &= \{(34,30),(20,24),(19,11),(16,17),(7,30),(21,24),(22,11),(25,17)\},\\
\mathcal{O}_3 &= \{(15,35),(4,28),(12,6),(36,13),(26,35),(37,28),(29,6),(5,13)\},\\
\mathcal{O}_4 &= \{(39,5),(35,4),(23,36),(28,37),(2,5),(6,4),(18,36),(13,37)\},\\
\mathcal{O}_5 &= \{(27,10),(40,8),(38,31),(32,33),(14,10),(1,8),(3,31),(9,33)\},\\
\mathcal{O}_6 &= \{(40,26),(38,29),(32,15),(14,12),(1,26),(3,29),(9,15),(27,12)\}.
\end{aligned}$$

现在，命题*4.4*中定义的代数几何码 $\mathcal{C}(D_1,D_2)$ 是一个余指标为8的 $[48,\,t-1,\,\geq 48-t]_{41}$ 准循环码，其中 $3\leq t\leq 47$。

例 *4.8.* 设 $r=1$ 和 $q=31.$ 那么 $\#\mathcal{X}(\mathbb{F}_q)=28$，且自同构 $\sigma(x,y)=(-x,2y)$ 在 $\mathcal{X}(\mathbb{F}_q)\backslash\{P_\infty\}$ 上诱导出两个短轨道，即 $\{(1,0),(-1,0)\}$ 和 $\{(0,15),(0,23),(0,27),(0,29),(0,30)\}$，以及两个长轨道，具体如下:

$$\mathcal{O}_1=\{(21,11),(10,26),(21,22),(10,21),(21,13),(10,11),(21,26),(10,22),(21,21),(10,13)\}$$

and

$$\mathcal{O}_2=\{(23,8),(8,2),(23,16),(8,4),(23,1),(8,8),(23,2),(8,16),(23,4),(8,1)\}.$$

那么，对于 $3\leq t\leq 19$，代数几何码 $\mathcal{C}(D_1,D_3)$ 是一个余指标为10的 $[20,\,t-1,\,\geq 20-t]_{31}$ 准循环码，其最小距离满足 $d=20-t+1$（即，$\mathcal{C}(D_1,D_3)$ 是一个 *NMDS*码），其中 $t\in\{3,17,19\}$；而在其余情况下，$d=20-t$。此外，仅利用上述定义的两个短轨道和自同构 σ^2，即可得到 $[27,\,t-1,\,\geq 27-t]_{31}$ 个余指标分别为$(2$、5、10、$10)$ 的广义准循环码，以及$[20,\,t-1,\,\geq 20-t]_{31}$ 个余指标为5的准循环码。

在下一小节中，我们将通过考虑一族 $\mathbb{F}_{q^2}$-极大超椭圆曲线，重点讨论情形 $r=2$。特别地，我们将研究亏格为 g的曲线 $\mathcal{X}_g$: $y^2=x^{2g+1}+1$，它与上文在情形 $g=2$中所描述的曲线 $\mathcal{X}$ 一致。

4.2 $\mathbb{F}_{q^2}$-极大曲线 $x^2=y^{2g+1}+1$

在 $[27,$定理 $6\,]$中，作者对曲线 $\mathcal{X}_g$: $x^2-y^{2g+1}-1=0$成为 $\mathbb{F}_{q^2}$-极大给出了完全刻画（另见 $[26,$ 定理 $1]$）。具体而言，$\mathcal{X}_g$ 为 $\mathbb{F}_{q^2}$-极大当且仅当 $2g+1$整除 $q+1.$

注 4.9. 考虑 $G:=\{(x,y)\mapsto(\epsilon x,\xi y):\ \epsilon^2=\xi^{2g+1}=1\}.$ 容易看出，G 是 $\mathcal{X}_g$ 的一个自同构群，且固定 P_∞ 和 $G\cong\mathbb{Z}_2\times\mathbb{Z}_{2g+1}.$。此外，由定理 *1.1* 可知，群 G 不被 $\mathcal{X}$的任何阿贝尔自同构群真包含。这意味着，结合定理 *2.4* 和 *2.5*，从由曲线 $\mathcal{X}_g$产生的代数几何码出发，可以构造余指标为ℓ的准循环码，其中 ℓ 是 $|G|=4g+2$的任意除子。

事实上，考虑域 $\mathbb{F}_{q^2}$，其中 q 是奇素数幂。设 $g\in\mathbb{N}$ 使得 $2g+1\mid(q+1)$。那么，$\#\mathcal{X}_g(\mathbb{F}_{q^2})=q^2+2gq+1$ 和 $G=\langle\sigma\rangle$，其中 $\sigma(x,y)=(-x,\xi y)$，且 $ord(\sigma)=2(2g+1)$。此外，σ 固定 P_∞，并在 $\mathcal{X}_1(\mathbb{F}_{q^2})\setminus\{P_\infty\}$ 个大小为 *2* 和 $2g+1$ 的短轨道，以及 $\frac{q-1}{2}+\frac{(q-2)(q+1)}{4g+2}$ 个长轨道。因此，由定理 *2.4* 和 *2.5* 可知，存在参数为

$$[q^2+2g(q-1)-3,\,t_1-g+1,\,\geq q^2+2g(q-1)-3-t_1]_{q^2}\quad and\quad [q^2+2gq,\,t_2-g+1,\,\geq q^2+2gq-t_2]_{q^2},$$

对于 $2g-2<t_1<q^2-2$ 和 $2g-2<t_2<q^2+2g$，其余指标分别为 $4g+2$ 和 $(2,2g+1,4g+2,\ldots,4g+2)$。

最后，由于 σ 的任意幂的阶都整除 $4g+2$，且此类幂在 $\mathcal{X}_g(\mathbb{F}_{q^2})$ 上的作用与 σ类似，因此可以构造具有上述参数且余指标分别为 2ℓ 和 $(2,\ell,2\ell,\ldots,2\ell)$的准循环码和广义准循环码，其中 ℓ 是 $2g+1$的任意除子。

5 范数-迹曲线

Let

$$\mathcal{N}_{q,r}: x^{\frac{q^r-1}{q-1}} = y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y \tag{2}$$

设其为范数-迹曲线。范数-迹曲线在文献中颇有名气 [14], ，近年来又因其在构造优良代数几何码及研究其参数方面的应用 [3, 4, 8]而重新受到关注。众所周知，$\mathcal{N}_{q,r}$ 有 $q^{2r-1}+1$ $\mathbb{F}_{q^r}$个有理点，其中唯一的无穷远点为 $P_\infty = (0:0:1)$。此外，在 [2, 定理 3.1] 中，作者证明了对于 $r \geq 3$，$\mathrm{Aut}(\mathcal{N}_{q,r}) = \mathrm{Aut}(\mathcal{N}_{q,r})_{P_\infty}$ 的阶为 $q^{r-1}(q^r-1)$，且是一个半直积 $G \rtimes C$，其中

$$G = \left\{(x,y) \mapsto (x, y+a) \mid \mathrm{Tr}_{q^r|q}(a) = 0\right\} \quad \text{and} \quad C = \left\{(x,y) \mapsto (bx, b^{\frac{q^r-1}{q-1}} y) \mid b \in \mathbb{F}_{q^r}^*\right\}.$$

以下命题是 [2, 定理 3.1] 的直接推论。记 $\Omega = \{(0, y): \mathrm{Tr}^{q^r|q}(y) = 0\}$ 为 q^{r-1} $\mathbb{F}_{q^r}$-有理点中满足 x. 为零的 $\mathcal{N}_{q,\ r}$ 的集合

命题 5.1. 设 $\sigma \in \mathrm{Aut}(\mathcal{N}_{q,\ r}) = G \rtimes C$. 则有以下几种情况。

- 若 $\sigma \in G$，则 σ 在 $\mathcal{N}_{q,\ r}(\mathbb{F}_{q^r}) \setminus \{P_\infty\}$ 上半正则地作用，其轨道长度为 p.
- 若 $\sigma \in C$，令 $\sigma(x,y) = (bx, b^{\frac{q^r-1}{q-1}} y)$，其中 $b \in \mathbb{F}_{q^r}^*$.。则 σ 固定点 $(0,0)$，$ord(\sigma) = ord(b) \mid q^r-1$，且 σ 在 $\Omega \setminus \{(0,0)\}$ 上恰好诱导出 $q^{r-1}-1$ $ord(\gamma)$ 个短轨道，每个轨道的长度为 $ord(\gamma)$，其中 $\gamma = b^{\frac{q^r-1}{q-1}}$。此外，$\sigma$ 在 $\mathcal{N}_{q,r}(\mathbb{F}_{q^r}) \setminus (\{P_\infty\} \cup \Omega)$上半正则地作用。
- 若 $\sigma \notin G \cup C$，令 $\sigma(x,y) = (bx, b^{\frac{q^r-1}{q-1}} y + a)$，其中 $a \neq 0$ 且 $b \neq 1$.(a) 若 $\gamma = b^{\frac{q^r-1}{q-1}} \neq 1$，则 $ord(\sigma) = ord(b)$，并且 σ 固定点 $P = (0, \frac{a}{\gamma-1}) \in \Omega$，且在 Ω 上作用 $\setminus \{P\}$，具有 $q^{r-1}-1$ 个长度为 $ord(\gamma)$ 的短轨道。进一步，σ 在$\mathcal{N}_q$上半正则地作用，$_r(\mathbb{F}_{q^r}) \setminus (\{P_\infty\} \cup \Omega)$。(b) 若 $\gamma = 1$，则 $ord(\sigma) = p \cdot ord(b)$，且 σ 在 Ω 上作用，具有 q^{r-1} 个长度为 p 的短轨道。进一步，σ 在 $\mathcal{N}_q$ 上半正则地作用，$_r(\mathbb{F}_{q^r}) \setminus (\{P_\infty\} \cup \Omega)$。

接下来的两个推论是定理 2.4 和 2.5、命题 5.1 以及以下等式的直接推论

$$\{\mathrm{ord}(b) : b \in \mathbb{F}_{q^r}^*\} = \{\ell \in \mathbb{N} : \ell \mid q^r - 1\}, \qquad \mathrm{ord}(\gamma) = \mathrm{ord}\left(b^{\frac{q^r-1}{q-1}}\right) = \gcd(\mathrm{ord}(b), q-1).$$

推论 5.2. 设 $r \geq 3$. 则存在 $[n, t - {}^{q}{}_{(q^{r-1}-1\ ^2)(q-1)+1, \geq n-t}]_{q^r}$ 个余指标为m的准循环线性码，其中 $q_{(q^{r-1}-1)_{q-1}}{}^{2} - 2 < t < n$ 和 n, m 如下。

- $n = q^{2r-1}$ *and* $m = p$; *or*
- $n = q^{2r-1} - q^{r-1}$ *and* $m \in \{p^\nu \ell : \nu \in \{0,1\}$ and $\ell \mid q^r - 1\}$.

推论 5.3。 设 $r \geq 3$. 则存在 $[n, t - {}^{q}{}_{(q^{r-1}-1\ ^2)\ q-1)\ +1, \geq\ n-t}]_{q^r}$ 余指标为 $(m_1, \ldots, m_s)$ 的广义准循环线性码，其中 ${}^{q}{}_{(q^{r-1}-1)\ q-1}{}^{2\ 2} - 2 < t < n$ 以及 n、m_1、$\ldots$、m_s 如下所示。

- $n = q^{2r-1} - 1$,
  - $\ell \mid q^r - 1$,
  - $s = s_1 + s_2$, *where* $s_1 := \frac{q^{r-1}-1}{\gcd(\ell, q-1)}$ *and* $s_2 := \frac{q^{2r-1}-q^{r-1}}{\ell}$,
  - $m_1 = \cdots = m_{s_1} = \gcd(\ell, q-1)$ *and* $m_{s_1+1} = \cdots = m_s = \ell$.
- $n = q^{2r-1}$

- $\ell \mid \frac{q^r-1}{q-1}$,
- $s = s_1 + s_2$, *where* $s_1 := \frac{q^{r-1}}{p}$ *and* $s_2 := \frac{q^{2r-1}-q^{r-1}}{p\cdot\ell}$,
- $m_1 = \cdots = m_{s_1} = p$ *and* $m_{s_1+1} = \cdots = m_s = p \cdot \ell$.

在下一节中，我们将重点讨论 $r = 2$ 的情形，此时方程（2）中定义的范数迹曲线与众所周知的厄米特曲线重合。

6 厄米特曲线

令 $\mathcal{H}_q$： $Y^q + Y = X^{q+1}$ 为定义在 $\mathbb{F}_{q^2}$ 上的厄米特曲线。回忆一下， $\mathcal{H}_q$ 是 $\mathbb{F}_{q^2}$-极大的；也就是说，它达到了 Hasse–Weil 上界，并且有

$$q^2 + 1 + 2g(\mathcal{H}_q)\, q = q^3 + 1$$

$\mathbb{F}_{q^2}$个有理点，其中

$$g(\mathcal{H}_q) = \frac{q(q-1)}{2}.$$

此外， $\mathcal{H}_q$ 是对应于域扩张 $\mathbb{F}_{q^2}/\mathbb{F}_q$的范数迹曲线；特别地，当 $r = 2$时，它对应于范数迹曲线。众所周知（见 [11, 第 4] 节）， Aut($\mathcal{H}_q$) 中 P_∞ 的稳定子 G 为

$$G = S_p \rtimes C, \quad S_p = \{\psi_{1,b,c}\} \text{ and } C = \{\psi_{a,0,0}\}$$

其中

$$\psi_{a,b,c} : (x, y) \longmapsto (ax + b, ab^q x + a^{q+1} y + c) \tag{3}$$

with

$$b, c \in \mathbb{F}_{q^2}, a \in \mathbb{F}_{q^2}^* \text{ and } c^q + c = b^{q+1}.$$

[11], 中给出的以下结果描述了 G 的每个元素在 $\mathcal{H}_q$的 $\mathbb{F}_{q^2}$-有理点上的完整作用。为方便读者，我们也在下文附上证明。

定理 6.1. 设 $\psi_{a,b,c}$ 如方程 (3) 所示。若 $\psi_{a,b,c} \in S_p$，则 $\psi_{a,b,c}$ 在 $\mathcal{H}_q$ 的仿射点上半正则地作用。若 $\psi_{a,b,c} \notin S_P$，则以下情况之一成立：

(1) 若 $p \mid ord(\psi_{a,b,c})$，则存在 $\frac{q}{p}$ 个长度为 p 的短轨道，且 $\psi_{a,b,c}$ 在 $\mathcal{H}_q$ 的其余$q^3 - q$ 个仿射点上半正则地作用。*(2)* 若 $ord(\psi_{a,b,c}) \mid q + 1$ $\psi_{a,b,c}$，则其固定 q 个 $\mathcal{H}_q$ 仿射点，并在其余点上半正则地作用。*(3)* 否则，$\psi_{a,b,c}$ 固定 $\mathcal{H}_q$的一个仿射点，存在 $\frac{q-1}{}$ 个长度为 $ord(a^{q+1})$ 的 $ord(a^{q+1})$ 短轨道，且 $\psi_{a,b,c}$ 在 $\mathcal{H}_q$ 的其余 $q^3 - q$ 个点上半正则地作用。

证明。若 $\psi_{a,b,c}$ 属于 S_p，则 ord($\psi_{a,b,c}$) $= p$；并且，由于 $\mathcal{H}_q$ 的 p-秩为零（ [12, 推论 2.5]），$\psi_{a,b,c}$ 在 $\mathcal{H}_q$ 的仿射点上半正则地作用（参见 [15,定理 11.133]）。因此，存在 $\frac{q^3}{p}$ 个长度为 p的轨道。否则， $a \neq 1$，那么，根据 [11, 引理 4.1]的证明， $\tau^{-1} \circ \psi_{a,b,c} \circ \tau = \psi_{a,0,c^*}$，其中 $c^{*q} + c^* = 0$ 且 $\tau = \psi_{1,e,f}$，并且 $e = \frac{b}{a-1}$ 和 $f^q + f = e^{q+1}$。因此，当 $a \neq 1$时，我们可以在共轭意义下假设 $b = 0$，特别是 ord$a$ |ord$\psi_{a,b,c}$。对于 $a \neq 1$，我们像 [11, 引理 4.2]中那样，将证明分为三种情形。

(1) p |ord($\psi_{a,b,c}$)。根据 [11, 引理 4.2], 在这种情况下，没有被$\psi_{a,b,c}$固定的仿射点。根据 [11, 引理4.1], 由于 p |ord$\psi_{a,b,c}$，唯一的可能性是 $a^{q+1} = 1$，且 ord$\psi_{a,b,c} = p \cdot$ ord(a)，因此，在共轭意义下，$\psi_{a,b,c}(x, y) = (ax, y + c^*)$，其中 $c^{*q} + c^* = 0$。考虑满足 $\psi^i_{a,b,c}(x, y) = (a^i x, y + ip) = (x, y)$ 的 $i \in \{0, \ldots,$ord($\psi_{a,b,c}$)$\}$ 和 $P = (x, y)$。注意，$\mathcal{H}_q$中有 q 个点满足 $x = 0$ 和 y，使得 $y^q + y = 0$；在这些点上，$\psi_{a,b,c}$的作用产生 rase个长度为 p 的轨道。对于$\mathcal{H}_q$ ψ_a的其余 $q^3 - q$ 个点，$_{b,c}$ 半正则地作用，因此有q^3-q ord($\psi_{a,b,c}$)个长轨道。

---

(2) $p \nmid \mathrm{ord}(\psi_{a,b,c})$ 和 $\mathrm{ord}(\psi_{a,b,c}) \mid q+1$.
由于 $a^{q+1}=1$，根据 [11, 引理 4.1 (ii)]，在共轭意义下，我们可以假设$\psi_{a,b,c}(x,y)=(ax,y)$，由此可得 $\mathrm{ord}(\psi_{a,b,c})=\mathrm{ord}(a)$。根据 [11, 引理 4.2]，在这种情况下存在 q 个不动点，即满足 $x=0$ 的 q 点（对于所有这些点，y 满足$y^q+y=0$）。在$\mathcal{H}_q$ ψ_a的其余 q^3-q 仿射点上，$_{b,c}$ 半正则地作用。因此存在$_{q^3-q}$ 个长度为 $\mathrm{ord}(_{\psi_a,b,c})$ 的长轨道。

(3) $\mathrm{ord}(\psi_{a,\ b,\ c}) \mid q+1$.
根据 [11, 引理 4.1 的证明，(ii)], 在这种情况下，在共轭意义下，$\psi_{a,b,c}(x,y)=(ax,a^{q+1}y)$，因此 $\mathrm{ord}(\psi_{a,b,c})=\mathrm{ord}(a)$。根据这里的 [11, 引理 4.2]，只有一个不动点，即 (0, 0)。存在 $\mathcal{H}_q$的 $q-1$ 个点满足 $x=0$ 且不同于 (0, 0)；在这些点上，$\psi_{a,b,c}$ 的作用产生$^{q-1}$ 个长度为 $\mathrm{ord}(a^{q+1})$ 的轨道，其中 $\mathrm{ord}(_{a^{q+1}})=\mathrm{ord}(a)\ \gcd(\mathrm{ord}(a)\ _{q+1})$。在 $\mathcal{H}_q$ 中满足$x\neq 0$ $\psi_{a,b}$的其余仿射点上，$_c$ 半正则地作用，因此存在 $^{q^3-q}$ 个长度为 $\mathrm{ord}(a)$ 的轨道，其中长度为 $\mathrm{ord}(a)$。

□

定理 6.2。 设 $\psi_{a,b,c}$ 是厄米特曲线 $\mathcal{H}_q$ 的一个自同构，且属于 P_∞的稳定子。设 $\mathcal{O}_1,\ldots,\mathcal{O}_m$ 是 $\psi_{a,b,c}$的长轨道。定义除子

$$D_1=\sum_{i=1}^{m}\sum_{P\in\mathcal{O}_i}P,$$

$$D_2=tP_\infty,$$

其中

$$q(q-1)-2<t<m\cdot\mathrm{ord}(\psi_{a,b,c}).$$

那么，代数几何码 $\mathcal{C}(D_1,D_2)$ 是余指标为 $\mathrm{ord}(\psi_{a,b,c})$的拟循环码。此外：

- 若 $\psi_{a,b,c}\in S_p$，则 $\mathcal{C}(D_1,D_2)$ 是一个

$$[q^3,\ t-\frac{q(q-1)}{2}+1,\ \geq n-t]_{q^2}$$

准循环码。

- 若 $\psi_{a,b,c}\notin S_p$，则以下情形之一成立：

(1) 如果 $p\mid\mathrm{ord}(\psi_{a,b,c})$，那么 $\mathcal{C}(D_1,D_2)$ 是一个

$$[q^3-q,\ t-\frac{q(q-1)}{2}+1,\ \geq n-t]_{q^2}$$

拟循环码。

(2) 如果 $\mathrm{ord}(\psi_{a,b,c})\mid(q+1)$，那么 $\mathcal{C}(D_1,D_2)$ 是一个

$$[q^3-q,\ t-\frac{q(q-1)}{2}+1,\ \geq n-t]_{q^2}$$

拟循环码。

(3) 否则，$\mathcal{C}(D_1,D_2)$ 也是一个

$$[q^3-q,\ t-\frac{q(q-1)}{2}+1,\ \geq n-t]_{q^2}$$

拟循环码。

证明。 该证明是定理 2.4 和定理 6.1 的直接推论。 □

6.1 具有大循环自同构群的厄米特曲线的一个商

在本小节中，我们考虑一族具有较大循环自同构群的厄米特曲线商曲线。

这类曲线由方程 $\mathcal{C}_m$ 定义

$$y^q - y = x^m$$

在 $\mathbb{F}_{q^2}$，其中 $m > 1$，$\gcd(q, m) = 1$，$p \neq 3$ 且 $m \mid (q+1)$。曲线 $\mathcal{C}_m$ 可由 $\mathbb{F}_{q^2}$ 上的厄米特曲线 $\mathcal{H}_q$ 关于 PGU(3，q) 的循环子群取商得到，该子群由自同构 $(x, y) \mapsto (\lambda x, y)$，组成，其中 $\lambda^m = 1$。。更多详情见 [11]。

Th这些曲线具有阶为 $N = pm$ 的循环自同构群，即 $G = \langle \eta \rangle$，其中

$$\eta(x) = \zeta_m x, \ \eta(y) = y + 1$$

其中 ζ_m 是一个本原 m 次单位根；此外，这些曲线的亏格为

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

此外，根据 Serre 的一项结果（引自 [17, 命题 6]，并在 [1, 命题5]中证明），$\mathcal{C}_m$ 是一条 $\mathbb{F}_{q^2}$-极大曲线，即 $\#\mathcal{C}_m(\mathbb{F}_{q^2}) = q^2 + 1 + (q-1)(m-1)q = mq(q-1) + (q+1)$。

不难看出，η 固定点 P_∞，并且在集合上作用时有 q/p 个长度为 p 的短轨道

$$\Omega := \{(0, y) : y \in \mathbb{F}_q\},$$

并在剩余的 $mq(q-1)$个 $\mathbb{F}_{q^2}$-有理点上半正则地作用。因此，以下结果是定理 2.4 和 2.5 的直接推论。

定理 6.3. 设 $q, m > 1$，其中 q 是素数 p的幂，且 $p \neq 3$，$\gcd(p, m) = 1$ 且 $m \mid (q+1)$。那么存在 $[mq(q-1) \ t - \frac{(q-1)(m-1)}{2} + 1、 \geq mq(q-1)$ 个余指标为 pm 的准循环线性码，其中 $t \geq \frac{q(q^{r-1}-1)}{q-1}^2 - 2 < t < n.$

此外，还存在 $[mq(q-1) + q、 t - \frac{(q-1)(m-1)}{2} + 1、 \geq mq(q-1) - t]_{q^2}$ 个余指标为 $(m_1, \ldots, m_s)$ 的广义准循环线性码，其中 $s = \frac{q}{p} + \frac{(q-1)}{p} = \frac{q^2}{p}$、$m_1 = \cdots = m_{\frac{q}{p}} = p$ 和 $m_{\frac{q}{p}+1} = \cdots = m_{\frac{q^2}{p}} = pm.$

参考文献

[1] Y. Aubry 和 M. Perret. 覆盖中的曲线 ζ 函数的整除性。数学档案，82(3):205–213，2004。[2] M. Bonini、M. Montanucci 和 G. Zini. 关于由分离多项式定义的平面曲线及其自同构。几何学进展，20(1):61–70，2020。[3] M. Bonini 和 M. Sala. 范数-迹曲线与某些低次曲线之间的交。有限域及其应用，67:101715，2020。[4] M. Bonini、M. Sala 和 L. Vicino. 三次曲面上的有理点以及来自范数迹曲线的代数几何码。纯数学与应用数学年刊（*1923-*），202(1):185–208，2023。[5] J. Cannon、A. Steel 等. Magma计算机代数系统。在线软件（*magma. maths. usyd. edu. au*），2005。[6] G. Cardona、J. Gonz´alez、J.-C. Lario 和 A. Rio. 关于雅可比簇为 GL2型的亏格2曲线。数学手稿，98(1):37–54，1999。[7] G. Cardona 和 J. Quer. 自同构群同构于 d_8 或d_{12} 的亏格2曲线。美国数学会汇刊，359(6):2831–2849，2007。[8] C. Carvalho、H. L´opez 和 G. Matthews. 递减范数-迹码。设计、编码与密码学，92(5):1143–1161，2024。

[9] C. Chen、W. W. Peterson 和 E. Weldon Jr. 关于准循环码的一些结果。《信息与控制》，15(5):407–423，1969。[10] I. Duursma. 椭圆曲线和超椭圆曲线的向量分解问题。《J. Ramanujan数学学会杂志》，20(1):59–76，2005。[11] A. Garcia、H. Stichtenoth 和 C.-P. Xing. 关于埃尔米特函数域的子域。《组合数学》，120(2):137–170，2000。[12] A. Garcia 和 S. Tafazolian. 某些极大曲线与卡蒂埃算子。《下萨克森州立与大学图书馆》，2007。[13] B. Gatti、F. Ghiandoni 和 G. Korchm´aros. 埃尔米特函数域中 PGU(3, q) 的不变量。《艺术与离散应用数学》，8(1):论文编号 1.09，8，2025。[14] O. Geil. 关于范数迹曲线上的码。《有限域及其应用》，9(3):351–371，2003。[15] J. W. P. Hirschfeld、G. Korchm´aros、F. Torres 和 F. Torres. 有限域上的代数曲线，第20卷。普林斯顿大学出版社，2008。[16] W. C. Huffman 和 V. Pless. 纠错码基础。剑桥大学出版社，2010。[17] G. Lachaud. 艾森斯坦和与有限域上某些代数曲线的点数。《巴黎科学院报告》，305(01)，1987。[18] S. Ling 和 P. Sol´e. 关于准循环码的代数结构。I. 有限域。《IEEE信息论汇刊》，47(7):2751–2760，2001。[19] M. L. Madan 和 R. C. Valentini. Le Dickson 与阿廷-施赖埃尔扩张的主定理。《纯粹与应用数学杂志》，1980。[20] A. Malmendier 和 T. Shaska. 从超椭圆曲线到超椭圆曲线。《阿尔巴尼亚数学杂志》，13(1):107–200，2019。[21] C. Mart´ınez-P´erez 和 W. Willems. 循环码类是否渐近良好? 《IEEE信息论汇刊》，52(2):696–700，2006。[22] C. A. Melchor、N. Aragon、S. Bettaieb、L. Bidoux、O. Blazy、J.-C. Deneuville、P. Gaborit、E. Per- sichetti、G. Z´emor 和 I. Bourges. 汉明准循环码（HQC）。美国国家标准与技术研究院后量子密码轮次，2(4):13，2018。[23] R. Sanjeewa. 任意特征有限域上定义的循环曲线的自同构群。《阿尔巴尼亚数学杂志》，3(4):131–160，2009。[24] T. Shaska 和 H. V¨olklein. 亏格2函数域的椭圆子域与自同构。载于《应用中的代数、算术与几何：Shreeram S. Abhyankar 70岁生日会议论文集》，第703–723页。施普林格，2004。[25] H. Stichtenoth. 关于几何戈帕码的自同构。《代数杂志》，130(1):113–121，1990。[26] S. Tafazolian. 一族极大超椭圆曲线。《纯粹与应用代数杂志》，216(7):1528–1532，2012。[27]S. Tafazolian. 关于某些极大超椭圆曲线的一则注记。《有限域及其应用》，18(5):1013–1016，2012。[28] H. Tong 和 Y. Ding. 拟循环 NMDS码。《有限域及其应用》，24:45–54，2013。