arXiv:2603.04049v1 [math.AG] 4 Mar 2026

微分 Goppa 码

D. GONZÁLEZGONZÁLEZ、A. L. MUÑOZ CASTAÑEDA 和 L. M. NAVAS VICENTE

摘要。Rosenbloom 和 Tsfasman 在关于 m 度量的奠基性研究中，引入了由光滑射影曲线 X 上的多重点定义的代数几何码。这一构造涉及一个除子 G 和另一个除子 $D = \sum np_i$，其中 p_i 是互异的有理点，且满足 $p_i \notin$supp(G) 和 $n \in \mathbb{N}$。尽管这些码意义重大，但文献中对任意亏格情形的系统发展仍不完整，因为大多数研究都集中在亏格零情形。

我们对这类码进行了严谨的研究。给定一条光滑射影曲线 X、一个可逆层 L以及一个有效除子 $D = \sum n_i p_i$ （其中 n_i 不一定相等），再给定点集 D 上的局部参数组 t_D，以及局部化 L_{p_i} 的平凡化 γ_D，即可定义相应的微分 Goppa 码。这种码源于曲线上可逆层的 n-喷射理论，该理论使得能够利用 L 截面的 Hasse-Schmidt 导数来描述码字。

研究了数据变化（t_D, γ_D）对码的影响，并描述了作用于这些参数的群。分析了此类变化对最小汉明距离的影响，并给出了亏格0和1的曲线的具体示例。建立了一个涉及亚纯微分形式主部的对偶定理。结果表明，Goppa 码构成微分 Goppa 码的真子类，而且每个线性码都能在 $\mathbb{P}^1$ 上利用两个有理点赋予微分 Goppa 码结构。

目录

1. 引言 2主要结果与组织结构 3关于预备知识与附录的说明 42. 背景 42.1. 曲线 42.2. 微分与留数 52.3. 除子与可逆层 52.4. 喷射层 6

2020年 数学主题分类。11T71, 14G50, 94B27, 14F10, 13N10。关键词和短语。代数几何码；喷射丛；Hasse-Schmidt 导数；代数微分演算。第一作者获得了一项博士前期合同资助，该合同由卡斯蒂利亚-莱昂自治区政府教育委员会资助，并由欧洲社会基金+（FSE+）共同资助。三位作者均获得项目 PID2023-150787NB-I00 资助，该项目由 MICIU /AEI /10.13039/501100011033 /FEDER、欧盟资助。

3. 微分 Goppa 码 I. 构造与性质 6 3.1. 有效除子处的泰勒级数映射 6 3.2. 微分 Goppa 码的定义 8 3.3. 关于局部参数与平凡化的依赖 9 3.4. 泰勒群 11 3.5. 若干注记 17 4. 例子 17 4.1. 射影直线 17 4.2. 椭圆曲线 20 5. 微分 Goppa 码 II. 对偶性 23 5.1. 重数双线性型与对偶码 23 5.2. 对偶泰勒平凡化 24 5.3. 对偶定理 26 6. 块距离与汉明距离。借助局部参数的设计 28 6.1. 块距离的定义与基本性质 28 6.2. d_{blk} 的可达性与一个显式构造 30 6.3. 具有 $d_H \geq d$ 31的参数的存在性 7. 两个基本结果 33 7.1. 每个线性分组码都是微分 Goppa 码 34 7.2. 强几何 Goppa 码构成一个真子类 35 附录 A. 射流、高阶导子与微分学 36 A.1. 平凡情形。有理函数 36 A.2. 一般情形。亚纯截面 39 参考文献 42

1. 引言

有限域上的经典代数几何码，是通过在一条光滑射影曲线上的一组互异有理点处对可逆层的整体截面求值而构造的。这一构造产生几何 Goppa 码，并构成代数几何与编码理论之间最富有成果的联系之一；例如，参见 [8, 29, 27]。在此框架中，每个求值点的重数为一，因此所编码的信息仅由截面在这些固定点处的取值来描述。

然而，从几何的观点来看，考虑具有任意重数的有效除子是自然的。当一个点以大于一的重数出现时，曲线的局部结构表明，相关信息不应再仅限于截面的取值，还应纳入其高阶数据。这直接导向射流、主部层以及 Hasse–Schmidt 导数的语言（参见 [10, 18, 19, 20, 23, 24]）。由此观点，经典评价码的推广在于用一种无穷小求值取代简单的逐点求值，其阶由除子的重数所控制。

编码理论中这类思想的出现可以追溯到 Rosenbloom 和 Tsfasman 关于 m-度量 [25]，的研究，其中有序块的存在恰恰体现了高阶局部

信息的重要性。不过，文献中已有的明确发展基本上都集中在亏格零情形，也就是射影直线上的构造。据作者所知，唯一的例外是 [3], ，其中研究了任意亏格曲线上的 Bottleneck度量。在这一背景下，多重求值通过导数或超导数恢复并拓展 Reed–Solomon型码族，从而产生所谓的重数码及其仿射变体 [1, 2]。

亏格零情形表明，这些构造兼具结构与算法方面的研究价值。具体而言，它们为带重数的一元码带来了参数近乎最优的列表译码结果 [16, 11, 9]；催生了具有局部性且支持次线性译码的高码率码族 [17, 31]；并推动了高效系统编码算法的发展 [4]。近来，人们还研究了基于超导数和差商的扩展，这些扩展基本上仍在与 $\mathbb{P}^1$[1, 2]对应的一元框架内开展。这一发展表明，在求值点考虑重数并非无关紧要的细微改进，而是具有鲜明性质的新码族的来源。

本文旨在将这些构造推广到任意亏格的光滑射影曲线，并对其几何推广进行研究。给定一条定义在$\mathbb{F}_q$上的几何不可约光滑射影曲线 X 、一个定义在 X上的可逆层 L 以及一个有效除子 $D = \sum_{i=1}^{s} n_i p_i$。我们定义一个线性码，它与沿 D对 L 的全局截面进行射流求值相关。该构造明确依赖于在 D 支撑中的各点处所选的局部一致化参数 t_D ，以及这些点处对 L 所作的适当平凡化 γ_D 。具体而言，与这些数据相关的码$C(X,\ L,\ D,\ t_D,\ \gamma_D)$的码字由截面相对于这些局部参数的 Hasse–Schmidt 导数描述。当所有重数均为一时，便恢复了几何 Goppa 码的经典情形。此外，虽然 Rosenbloom–Tsfasman 度量和秩度量下的最小距离不随局部数据$(t_D,\ \gamma_D)$的变化而改变，但最小汉明距离通常取决于这些选择。理解这种依赖关系，以及如何利用局部参数控制所得的汉明距离，将是本文的核心。

主要结果与文章结构。 第 2 节介绍全文所使用的记号和基本概念。第 3 节建立任意亏格光滑射影曲线上微分 Goppa 码的内禀几何表述（定义 3.4），用 Hasse–Schmidt 导数描述其码字（注 3.5），并确定其维数（引理 3.6）。我们分析构造对局部一致化参数和平凡化的依赖性，确定支配这些变化的群（称为泰勒群）（定义 3.11）。我们描述码字系数所满足的诱导变换法则（定理 3.10），并证明 Taylor 型平凡化在所有可能的平凡化空间中构成一个单独且严格真子的轨道（命题 3.20 和引理 3.22）。第 4 节给出亏格 0 和 1的具体例子。第 5 节介绍用于定义对偶性的自然分块双线性

形式，构造相应的对偶泰勒平凡化（引理5.5和引理 5.7），建立局部留数–Hasse 导数卷积恒等式（命题 5.9），并证明微分 Goppa 码的对偶性定理（定理5.10）。第 6 节研究最小距离对局部数据选择的依赖性。我们引入内禀块距离（定义 6.1 和定义 6.3），将其与汉明距离进行比较（引理 6.5），并证明块距离恰好等于改变泰勒平凡化后所能达到的最小汉明距离（定理 6.9）。随后，我们为基域的大小建立一个界，以确保存在具有预设汉明距离下界的参数（定理6.15）。最后，在第 7 节中，我们得到两个结构性结果。一方面，我们证明每个线性分组码都可以实现为 $\mathbb{P}^1$ （定理 7.1）。另一方面，我们证明强几何 Goppa 码构成强微分 Goppa 码的一个真子类（命题7.3和定理 7.4）。

我们还在附录中汇集了全文所用的代数曲线上射流丛的基本概念和基本性质。

关于预备知识与附录的说明。尽管本文的总体背景涉及代数几何码，但本文的论证系统地依赖于局部性质和无穷小性质，例如喷射层、截断泰勒态射和 Hasse–Schmidt 导数；这些内容通常不属于该领域标准论述的范畴（见 [10, 18, 19, 20, 23, 24]）。预备知识部分自成一体地阐述了全文所用的几何与微分概念。附录汇集了定义微分 Goppa 码、考察其对局部数据的依赖性并建立对偶定理所需的关键射流丛结果。

2. 背景

关于代数几何所需的背景知识，请读者参阅 [13, 27]。不过，为使本文内容自成一体，本节将简要回顾全文中使用的基本概念。

2.1. 曲线。 在本文中， X 表示定义在有限域 $\mathbb{F}_q$上的光滑射影几何不可约曲线，其亏格为 g 。我们用O_X 表示 X的结构层。若 $x \in X$ 是一个点，我们用 O_x 表示 O_X 在 x 处的局部化，用 $\mathfrak{m}x$ 表示 O_x的极大理想。我们用μ 表示其泛点，用 K_X或简称 K表示其函数域 $O\mu$。 X 的有理函数是 K的一个元素 f ，它定义了一个概形态射$f:\ X \to \mathbb{P}^1$。反过来，任意概形态射 $f:\ X \to \mathbb{P}^1$ 都确定一个有理函数 $f \in K$。回顾一下，给定一个有理函数 $f \in K$ 和一个闭点 $x \in X$，要么 $f \in O_x$ ，要么 $f^{-1} \in O_x$。有理函数 $f \in K$在 $x \in X$ 处正则，当且仅当 $f \in O_x$。

给定一个有理点 $x \in X$ ，存在一个典范同构 $\gamma_x : O_x/\mathfrak{m}x \simeq \mathbb{F}q$。若 $f \in K$ 是一个在 x处正则的有理函数，则 f在 x处的值为 $f(x) := \gamma_x(f(\mathrm{mod}\ \mathfrak{m}x)) \in \mathbb{F}q$。从几何上看， $f(x) = [\gamma_x(f$

(mod $\mathfrak{m}_x$))；1]。若闭点 x 是 f 的一个重数为 $n \in \mathbb{N}$ 的零点，即 $f \in \mathfrak{m}_x^n \setminus \mathfrak{m}x^{n+1}$，且是 f 的一个阶为 $-n \in \mathbb{Z}<0$ 的极点，即 $f^{-1} \in \mathfrak{m}_x^n \setminus \mathfrak{m}_x^{n+1}$，则称之为如此。 f 的零点或极点的阶记为 $\mathrm{ord}_x(f)$。

2.2. **微分形式与留数**。我们用 ω_X 表示 X 的典范层，可将其识别为 $\Delta($ $I/I^2)$，其中 $\Delta: X \hookrightarrow X \times X$ 是对角闭浸入，而 I 是 $\Delta(X)$ 的理想层。这是一个可逆层。我们将 Ω_X^1 的局部化记为 $\omega_{X,\ \mu}$。一维K-向量空间 Ω_X^1 的元素称为 X 的亚纯微分。我们将 $d: O_X \to \omega_X \subseteq \pi_1(O_X \otimes O_X)/I^2$ 记为层的典范 $\mathbb{F}q$-线性态射，

$$f \mapsto df = (f \otimes 1 - 1 \otimes f) \pmod{I^2},$$

它称为泛微分。这里， $\pi i: X \times X \to X$， $i = 1,\ 2$ 是到第 i 个因子的投影。对于点 x 处的局部化映射 $d{:}O_x \to \omega_{X,\ x}$，我们也使用相同的记号 d。

闭点 $x \in X$ 的局部参数是一个在 x处正则的 X 的有理函数 $t_x \in O_x \subset K$，使得 dt_x 生成 $\omega_{X,\ x}$。给定局部参数 t_x和有理函数 $f \in K$，我们用 $f(t_x)$ 表示 f 在 x 处相对于 t_x 的 Laurent 展开（见 A.3）。若 f 在 x 处正则，我们用 $D_{t_x}^n(f)$ 表示 f 在 x 处相对于 t_x 的第 n 阶导数（见 A.4）。

给定一个亚纯微分形式 $\eta \in K$ 和一个闭点 $x \in X$，我们可以选取一个局部参数 t_x 以及一种表示 $\eta = fdg$，其中 f 和 g 是有理函数。η 在 x 处的留数定义为（见 [28]）

$$\mathrm{Res}_x(\eta) := \left[\begin{array}{l} \text{degree } -1 \text{ coefficient in the Laurent} \\ \text{expansion of } f(t_x) \cdot g'(t_x) \end{array} \right] \tag{2.1}$$

其中 $g'(t_x)$ 表示 $D_{t_x}^1(g)$。留数与表示方式及局部参数的选取无关，并且满足

$$\sum_{x \in X} \mathrm{Res}_x(\eta) = 0,\ \forall \eta \in \Omega_X^1. \tag{2.2}$$

2.3. **除子与可逆层**。给定 X 上的一个除子 $G = \sum_{x \in X} n_x x$，我们用 $\mathrm{mult}x(G)$ 表示 G 在 x处的重数；即 $n_{x\circ}$ 将 G 限制到开子集 $U \subset X$ 上，得到的就是 $G_U{:=}\sum x \in U n_x x_\circ$ 给定一个有理函数 $f \in X$，我们分别用 $(f)0$ 和 $(f)\infty$ 表示其零点与极点除子，并用 $(f)\ =(f)0 - (f)\infty$ 表示其总除子。我们用 $O_X(G)$ 表示与之对应的可逆层。回顾

$$O_X(G)(U) := f \in K|\ (f)U + GU \geq 0 \cup 0. \tag{2.3}$$

如果 L 是 X 上的可逆层，我们用 $L(G)$ 表示 $L \otimes O_X(G)$。另请回忆，

$$\omega_X(G)(U) = \eta \in \Omega_X^1|\ (\eta)U + G_U \geq 0, \tag{2.4}$$

给定一个有理点 $x \in X$、 X 上的可逆层 L 以及一个满足 $x \in U \subset X$ 的局部截面 $s \in L(U)$，限制映射 $L(U)\ \to L_x/\mathfrak{m}xL_x$ 与平凡化 $\phi: L_x/\mathfrak{m}xL_x \simeq \mathbb{F}q$ 的复合导出一个 $\mathbb{F}q$-线性映射

$$ev_\phi : L(U) \to \mathbb{F}q,$$

而 $ev\phi(s)$ 称为 s在 x处相对于 ϕ的取值。若 ϕ' 是另一个平凡化，则对于某个 $\lambda \in \mathbb{F}_q^\times$，有 $ev'_\phi = \lambda \cdot ev_\phi$。

2.4. **喷射层**。给定一个可逆层 L，L 的 i-射流层定义为

$$J^i_X(L) := \pi_{1*}\left(\pi_2 L \otimes_{O_{X\times X}} O_{X\times X}/I^{i+1}\right).$$

粗略地说，$J^i_X(L)$ 是这样的 O_X-模：其在点 $p \in X$ 处的纤维为

$$J^i_p(L) := J^i_X(L)|_p \simeq L_p/\mathfrak{m}p^{i+1}L_p = L|(i+1)p. \tag{2.5}$$

层 $J^iX(L)$ 配备了一个典范映射 d^i_L：$L \to J^iX(L)$。固定一个局部平凡化 γ：$L|_U \simeq O_U$，并选取一个生成元 $z\in \omega_X$（必要时缩小 U），则 d^i_L 将局部截面 s 映射为其关于 z 的 i 阶泰勒展开。

$J^i_X(L)$ 的构造具有函子性，即给定一个模态射 γ：$L \to L'$，便有一个诱导态射

$$J^i(\gamma) : J^i_X(L) \to J^i_X(L')$$

它与典范映射 d^i_L 和 $d^i_{L'}$相容。

可逆层的喷射在本文中起着关键作用，我们已在附录 A中汇总了其基本性质。

3. 微分 Goppa 码 I. 构造与性质

在本节余下部分，我们固定一个亏格为 g、定义在有限域 $\mathbb{F}_q$ 上的光滑射影曲线 X、一个可逆层 L 和一个有效除子 X。

3.1. **有效除子处的泰勒级数映射**。令 n：=最大$_i\{n_i\}$为 D的最大重数，并令 n为元组 $(n_1, \dots, n_s)$。对于每个自然数 i，我们有 L的次数为 i的喷射层，$J^i_X(L)$。由基本短正合列A.8可知，对每个 n_i，都存在一个满射

$$\psi_i : J^{n-1}_X(L) \to J^{n_i-1}_X(L)$$

此外，与点 $p_i \in X$ 处的求值映射复合，$J^{n_i-1}_X(L) \to J^{n_i-1}_p(L)$，我们得到一个满射态射

$$\psi_i(p) := J^{n-1}_X(L) \to J^{n_i-1}_p(L).$$

结合这一点和初始设定，我们得到一个满态射$\oplus_i\psi_i(p_i)$，记作 Ψ_D，

$$\Psi_D : J^{n-1}_X(L) \to \oplus^s_{i=1} J^{n_i-1}_{p_i}(L).$$

另一方面，我们有典范映射 d^{n-1}_L：$L \to J^{n-1}_X(L)$ (定义 A.4)。取整体截面，将其拉回到 X 并与求值映射复合，我们得到一个 O_X-模的态射

$$(ev \circ H^0(d^{n-1}_L) \otimes 1 =)\ \partial^{n-1}_L : H^0(X, L) \otimes O_X \to J^{n-1}(L).$$

因此，我们得到如下图表

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Ker}(\Psi_D) & \longrightarrow & J_X^{n-1}(L) & \xrightarrow{\Psi_D} & \oplus_{i=1}^{s} J_{p_i}^{n_i-1}(L) & \longrightarrow & 0 \\ & & & & \uparrow{\scriptstyle \partial_L^{n-1}} & \nearrow{\scriptstyle \Theta_D:=\Psi_D\circ\partial_L^{n-1}} & & & \\ & & & & H^0(X,L)\otimes O_X & & & & \end{array}$$

定义 3.1。 L在有效除子 D 处的泰勒级数映射定义为态射

$$\Theta_D : H^0(X,L)\otimes O_X \to \oplus_{i=1}^{s} J_{p_i}^{n_i-1}(L)$$

引理 *3.2*。设 $U = Spec(A) \subset X$ 是一个将L平凡化的仿射开子集。固定一个平凡化 $\gamma\colon L|_U \simeq O_U$以及一个 $\omega_X|_U$的生成元 $z \in A$。令$\xi := \delta_U(z) \in J_U^{n-1}$，并令 $\xi^j := J^{n-1}(\gamma)^{-1}(\xi^j) \in J_X^{n-1}(L)(U)$。那么对于元素 $\sum_{\ell=1}^{r} s_\ell \otimes a_\ell \in H^0(X,L) \otimes O_X(U)$ $s_\ell \in H^0(X,L)$ $a_\ell \in O_X(U)$，有

1. $\partial_L^{n-1}(U)\left(\sum_{\ell=1}^{r} s_\ell \otimes a_\ell\right) = \sum_{j=0}^{n-1} \left(\sum_{\ell=1}^{r} a_\ell D_{U,\gamma,z}^{j}(s_\ell)\right) \overline{\xi^j}$.
2. $\Theta_D(U)\left(\sum_{\ell=1}^{r} s_\ell \otimes a_\ell\right) = \bigoplus_{p_i\in U} \sum_{j=0}^{n_i-1} \left(\sum_{\ell=1}^{r} a_\ell(p_i)\, D_{t_i}^{j}(\gamma(s_\ell))\right) \xi_{p_i}^{j}$

其中，对于 $p_i \in U$，我们用 $\xi_{p_i}^{j} \in J_{p_i}^{n_i-1}(L)$ 表示ξ^j在$\psi_i(p_i)$ 下的像，而 t_i 是 z 在 p_i处的局部化。

3. $H^0(\Theta_D)(s) = \bigoplus_{i=1}^{s} \sum_{j=0}^{n_i-1} D_{t_{p_i}}^{j}(\gamma_i(s)\overline{)}\xi_{p_i}^{j}$，其中 t_i 是p_i 处的局部参数，且 γ_i 是 L_{p_i}的平凡化。

注记 3.3. 给定局部平凡化 γ： $L_p \simeq O_p$ 以及整体截面$s \in H^0(X,L)$， $\gamma(s)$ 应理解为 s 在复合$H^0(X,L) \to L_p \simeq O_p$下的像。

证明。 1）由构造，对每个开子集 $V \subset X$ 以及每个元素$\sum_{\ell=1}^{r} s_\ell \otimes a_\ell \in H^0(X, L) \otimes O_X(V)$，有

$$\partial_{n-1}^{L}(V)\left(\sum_{\ell=1}^{r} s_\ell \otimes a_\ell\right) = \sum_{\ell=1}^{r} a_\ell \cdot \left(d_{n-1}^{L}(s_\ell)\right)|_V, \tag{3.1}$$

其中 $d_{n-1}^{L}(s_\ell) \in \Gamma(V, J_X^{n-1}(L))$ 表示由 $s_\ell \in H^0(X, L)$ 诱导的 $J_X^{n-1}(L)$ 的截面到 V的限制。现在我们对$V = U$应用（3.1），并在基 $\{\xi^j\}_{j=0}^{n-1}$中计算每个 $\left(d_{n-1}^{L}(s_\ell)\right)|_U$。由交换方图A.9，我们有 $J^{n-1}(\gamma)\left(d_{n-1}^{L}(s_\ell)|_U\right) = d_U^{n-1}(\gamma(s_\ell)) \in J_U^{n-1}$。将 $d_U^{n-1}(\gamma(s_\ell))$ 按基 $\{1, \xi, \ldots, \xi^{n-1}\}$写出，其系数恰好是高阶导子$D_{U,z}^{j}(\gamma(s_\ell))$（见A.2），因此 $d_U^{n-1}(\gamma(s_\ell)) = \sum_{j=0}^{n-1} D_{U,z}^{j}(\gamma(s_\ell))\,\xi^j$. 由定义 A.5， $D_{U,\gamma,z}^{j}(s_\ell) := D_{U,z}^{j}(\gamma(s_\ell)) \in A$。经 $(J^{n-1}(\gamma))^{-1}$ 拉回，得到

$$d_{n-1}^{L}(s_\ell)|_U = \sum_{j=0}^{n-1} D_{U,\gamma,z}^{j}(s_\ell)\,\overline{\xi^j}.$$

最后，将此表达式代入（3.1）（其中 $V = U$），并利用 O_U-模结构 $J_X^{n-1}(L)|_U$，即可得到所需公式。

2）由 1）和 Θ_D 的定义可知，$\Theta_D(U)(\sum_{\ell=1}^{r} s_\ell \otimes a_\ell) = \bigoplus_{p_i \in U} \sum_{j=0}^{n_i-1} \left(\sum_{\ell=1}^{r} a_\ell(p_i)\, D^j_{U,\ \gamma,\ z(s_\ell)}(p_i)\right) \overline{\xi^j_{p_i}}$。现在由 A.14 即得该公式。

3) 由 2) 可知 $H^0(\Theta_D)(s) = \bigoplus_{i=1}^{s} \sum_{j=0}^{n_i-1} D^j_{U_i,\gamma_i,z_i}(s)(p_i)\overline{\xi^j_{p_i}}$，其中每个三元组 (U_i, γ_i, z_i) 都满足额外条件 $p_i \in U_i$。最终公式再次由A.14得到。□

3.2. 微分 Goppa 码的定义。 现在我们给出本文的核心概念。

设 X 是一条光滑射影曲线，L 是 X 上的一个可逆层，$D = n_1 p_1 + \cdots + n_s p_s$ 是一个有效除子。对于每个 $i = 1, \ldots, s$，我们固定 t_i 作为 p_i 的一个局部参数，并固定一个平凡化 $\gamma_i : L_{p_i} \simeq O_{p_i}$。我们用 $\overline{\gamma_i}$ 表示诱导同构 $J^{n_i-1}_{p_i}(L) \simeq \mathbb{F}_q^{n_i}$，并用 γ 表示同构 $\oplus_{i=1}^{s}\gamma_i$。我们将使用如下记号

$$t_D = (t_{p_1}, \ldots, t_{p_n}),$$
$$\gamma_D = (\gamma_1, \ldots, \gamma_n),$$

在本文余下部分中。同样，我们用 ev_{t_D,γ_D} 表示复合线性映射

$$ev_{t_D,\gamma_D} : H^0(X, L) \xrightarrow{H^0(\Theta_D)} \oplus_{i=1}^{s} J^{n_i-1}_{p_i}(L) \xrightarrow{\overline{\gamma}} \mathbb{F}_q^M.$$

定义 3.4。 设 $\Gamma \subset H^0(X, L)$ 是一个线性子空间。我们将与数据 $X, L, D, \Gamma, t_D, \gamma_D$ 相关联的微分 Goppa 码定义为长度为 M 的线性码：$= \sum_{i=1}^{s} n_i$ 其定义如下：

$$C(X, L, D, \Gamma, t_D, \gamma_D) := \mathrm{Im}\,(ev_{t_D,\gamma_D}|_\Gamma)$$

如果 $C(X, L, D, \Gamma, t_D, \gamma_D)$ 是一致微分 Goppa 码，则称

$$n_1 = \cdots = n_s$$

在除子 D 中。如果 Γ 是完全线性系，

$$\Gamma = H^0(X, L),$$

我们用 $C(X, L, D, t_D, \gamma_D)$ 代替 $C(X, L, D, H^0(X, L)\ t_D, \gamma_D)$。

注 3.5. **1.**由引理 3.2, 3) 可知，任意一个$C(X, L, D, \Gamma, t_D, \gamma_D)$ 中的字都具有如下形式

$$ev_{t_D,\gamma_D}(s) := \Big(D^0_{t_{p_1}}(\gamma_1(s)), D^1_{t_{p_1}}(\gamma_1(s)), \ldots, D^{n_1-1}_{t_{p_1}}(\gamma_1(s)),$$
$$\vdots \tag{3.2}$$
$$D^0_{t_{p_s}}(\gamma_s(s)), D^1_{t_{p_s}}(\gamma_s(s)), \ldots, D^{n_s-1}_{t_{p_s}}(\gamma_s(s))\Big)$$

对于 $s \in \Gamma$。回顾一下，$D^0_{t_{p_i}}(\gamma_i(s)) = \gamma_i(s)(p_i)$。

2. 若 $n_1 = \ldots$、$n_s = 1$，则码 $C(X, L, D, \Gamma, t_D, \gamma_D)$ 仅依赖于类 $\gamma_i := \gamma_i \mod \mathfrak{m}_i$，而不依赖于局部参数。因此，$C(X, L, D, \Gamma, t_D, \gamma_D) = C(X, L, D, \Gamma, \gamma_D)$ 是 Tsfasman–Vlăduţ [29, §3.1.1] 意义下的几何 Goppa 码。此外，若 $L = O_X(G)$ 且 $\mathrm{supp}(G) \cap \mathrm{supp}(D) = \emptyset$，则 $L_{p_i} = O_{p_i}$，并且我们可以选取 $id_D := (id_{O_{p_1}}, \ldots, id_{O_{p_s}})$ 作为 γ_D。事实上，$C(X, L, D, \Gamma, id_D) = C(X, \cancel{G,} D, \Gamma)$ 是一个

几何 Goppa 码（在经典意义下 [8]），由线性级数Γ定义。

引理 3.6。 在上述情形下，成立

$$\mathrm{Ker}(H^0(\Theta_D)) = H^0(X, L(-D)).$$

因此，

$$\dim\ C(X, L, D, t_D, \gamma_D) = \dim\ H^0(X, L) - \dim\ H^0(X, L(-D)).$$

特别地，若 $\sum_{i=1}^{s} n_i > \deg(L)$，则

$$\dim\ C(X, L, D, t_D, \gamma_D) = \dim\ H^0(X, L).$$

证明。由引理 3.2(2)，且由于元素 $\xi_{p_i}^j$ 线性无关，我们有 $H^0(\Theta_D)(s) = 0$ 当且仅当 $D_{t_i}^j\big(\gamma_i(s)\big) = 0$ 对所有 $i = 1, \ldots, s$ 和 $j = 0, \ldots, n_i - 1$ 均成立。固定一个指标 i。由于 s 在 p_i 处正则，其在完备局部环 $O_{X,p_i} \simeq k[[t_i]]$ 中的局部表达式可写为

$$\gamma_i(s)(t_i) = \sum_{m \geq 0} a_m t_i^m.$$

根据微分算子 $D_{t_i}^j$ 的定义，我们有 $D_{t_i}^j(\gamma_i(s)) = a_j$。因此，$D_{t_i}^j(\gamma_i(s)) = 0$ 对所有 $j < n_i$ 成立，当且仅当 $\gamma_i(s) \in (t_i^{n_i}) = \mathfrak{m}_{p_i}^{n_i}$。撤销平凡化后，这一条件等价于 $s \in \mathfrak{m}_{p_i}^{n_i} L_{p_i}$。综合以上所有结果，我们得到

$$s \in \mathrm{Ker}\left(H^0(\Theta_D)\right) \iff s \in \mathfrak{m}_{p_i}^{n_i} L_{p_i} \text{ for all } i = 1, \ldots, s. \tag{3.3}$$

另一方面，截面 $s \in H^0(X, L)$ 属于 $H^0(X, L(-D))$ 当且仅当 $s_{p_i} \in \mathfrak{m}_{p_i}^{n_i} L_{p_i}$ 对所有 i 均成立。与 3.3 对比可得

$$\mathrm{Ker}\left(H^0(\Theta_D)\right) = H^0\big(X, L(-D)\big),$$

正如所声称的那样。第二部分显然成立。 □

注 3.7。由定义 3.4、引理 3.2 和引理 3.6可知，定义微分 Goppa 码的“求值映射”正是线性映射$H^0(X, L) \to L|_D$，它是对典范满射 $L \to L|_D$取整体截面后得到的。因此，一致微分 Goppa 码就是 Rosenbloom 和 Tsfasman 在 m中定义的 [25, §3]-度量下的代数几何码。

3.3. **关于局部参数与平凡化的依赖。** 现在我们的目标是研究当 $C(X, L, D, \Gamma, t_D, \gamma_D)$ 变化时，码 t_D 或 γ_D 变化而保持 X，L，D 不变。导子的乘积公式和法阿·迪布鲁诺公式（见 A.2.2）在此发挥重要作用。

引理 3.8. 设 X 和 D 如上所述，$p \in X$ 为有理点，$\gamma\colon L_p \simeq O_p$ 为平凡化，t 和 u 为 p 处的局部参数。定义 $T_p \in \mathrm{GL}_n(\mathbb{F}_q)$ 为以下元素构成的下三角矩阵

$$(T_p)_{m,j} := \begin{cases} \sum\limits_{\substack{(n_1,\ldots,n_m)\in\mathbb{N}^m \\ \sum_{r=1}^m r\, n_r = m \\ \sum_{r=1}^m n_r = j}} \binom{j}{n_1, n_2, \ldots, n_m} \prod_{r=1}^m D_u^r(t)^{n_r}, & 0 \leq j \leq m \leq n-1, \\ 0, & j > m. \end{cases}$$

那么，对于任意整体截面 $s \in H^0(X, L)$，有

$$(D_u^0(\gamma(s)), \dots, D_u^{n-1}(\gamma(s))) = (D_t^0(\gamma(s)), \dots, D_t^{n-1}(\gamma(s)))\, T_p.$$

证明。由于 $\gamma\colon L_p \simeq O_p$ 是 O_p–模的同构，我们可以选取一个仿射邻域 $U = \operatorname{Spec}(A) \subset X$ of p，使 L 平凡化，并配备一个平凡化 $\gamma_U\colon L|_U \simeq O_U$，其在 p 处的局部化 $(\gamma_U)_p$ 与 γ 一致。如有必要，进一步缩小 U，我们还可以选取 $\omega_X|_U$ 的生成元 $z, w \in A$，使得

$$t = \frac{z}{1} \in O_p, \qquad u = \frac{w}{1} \in O_p$$

是给定的局部参数。于是，对每个 $j \geq 0$ 以及每个 $s \in H^0(X, L)$，$D_t^j(\gamma(s)) = D^j_{U,\gamma_U,z}(s)(p)$ 和 $D_u^j(\gamma(s)) = D^j_{U,\gamma_U,w}(s)(p)$，由 (A.14) 可得。现在，在 U 上应用 Faà di Bruno 公式 A.12（将参数从 z 改为 w），在 p 处取值并再次利用 (A.14)，我们得到

$$D_u^m(\gamma(s)) = \sum_{j=0}^{m} D_t^j(\gamma(s)) \left(\sum_{\substack{(n_1,\dots,n_m)\in\mathbb{N}^m \\ \sum_{r=1}^m r n_r = m \\ \sum_{r=1}^m n_r = j}} \binom{j}{n_1, \dots, n_m} \prod_{r=1}^{m} \left(D_u^r(t)\right)^{n_r} \right),$$

对每个 $m = 0, \dots, n-1$。根据矩阵 T_p 的定义，内层括号为 $(T_p)_{m,j}$，因此上述等式等价于所声称的矩阵关系。□

引理 3.9。设 X 和 D 如上，设 $p \in X$ 为一个有理点，并设 t 为 p 处的局部参数。设 γ、$\gamma'\colon L_p \simeq O_p$ 为两个平凡化，并设 $f \in O_p^\times$ 满足 $\gamma' = f\,\gamma$。固定 $n \geq 1$，并将 $S_p \in \mathrm{GL}_n(\mathbb{F}_q)$ 定义为以下项构成的下三角矩阵

$$(S_p)_{m,j} := \begin{cases} D_t^{m-j}(f), & 0 \leq j \leq m \leq n-1, \\ 0, & j > m. \end{cases}$$

那么，对任意整体截面 $s \in H^0(X, L)$，有

$$\left(D_t^0(\gamma'(s)), \dots, D_t^{n-1}(\gamma'(s))\right) = \left(D_t^0(\gamma(s)), \dots, D_t^{n-1}(\gamma(s))\right) S_p.$$

证明。由于 $\gamma, \gamma'\colon L_p \simeq O_p$ 是 O_p–模的同构，我们可以选取 p 的一个仿射邻域 $U = \operatorname{Spec}(A) \subset X$，使 L 平凡化，并选取平凡化（仍记作）$\gamma, \gamma'\colon L|_U \simeq O_U$，它们在 p 处的局部化是给定的映射 $\gamma, \gamma'\colon L_p \simeq O_p$。于是，对唯一的 $f \in O_p^\times$，有 $\gamma' = f\,\gamma$；再次缩小 U 后，我们可以用元素 $f \in A^\times$ 表示它，该元素在 O_p 中的局部化是联系 γ' 和 γ 的给定单位元。

设 $z \in A$ 满足 dz 生成 $\omega_X|_U$，且其局部化 $t = z/1$是 p处选定的局部参数。根据（A.13）和（A.14），对于每个 $m \geq 0$ 以及每个 $s \in H^0(X, L)$，都有

$$D_t^m(\gamma(s)) = D^m_{U,\gamma,z}(s)(p), \qquad D_t^m(\gamma'(s)) = D^m_{U,\gamma',z}(s)(p). \tag{3.4}$$

现在将（A.11）应用于 $\gamma' = f\gamma$，然后应用（3.4）可得

$$D_t^m(\gamma'(s)) = \sum_{j=0}^{m} D_{U,z}^{m-j}(f)(p)\, D_t^j(\gamma(s)). \tag{3.5}$$

最后，利用相同的识别（A.14）（以 f 替代 $\gamma(s)$），可得 $D^r_{U,z}(f)(p) = D^r_t(f)$，其中 $r \geq 0$。代入（3.5），对于$m = 0, \ldots, n-1$，可得 $D^m_t(\gamma'(s))$ $= \sum_{j=0}^{m} D^{m-j}_t(f)\ D^j_t(\gamma(s))$。根据$S_p$的定义，前一个恒等式等价于所述矩阵关系。□

定理 3.10. 设 X 和 D 如上，且 $p \in X$ 是一个有理点。设t, t' 分别是 p 和 $\gamma, \gamma' \colon L_p \simeq O_p$ 的两个平凡化。设 $f \in O_p^{\times}$满足 $\gamma' = f\,\gamma$。固定 $n \geq 1$。对于任意整体截面 $s \in H^0(X, L)$，有

$$\big(D^0_{t'}(\gamma'(s)), \ldots, D^{n-1}_{t'}(\gamma'(s))\big) = \big(D^0_t(\gamma(s)), \ldots, D^{n-1}_t(\gamma(s))\big)\, S_p T_p.$$

证明。 直接先应用引理 3.9 再应用引理 3.8即可得出。剩下只需说明为何反向执行这些步骤不会得到 $T_p S_p$。若先在固定 γ 的情况下更换局部参数，引理3.8 给出

$$\big(D^0_{t'}(\gamma(s)), \ldots, D^{n-1}_{t'}(\gamma(s))\big) = \big(D^0_t(\gamma(s)), \ldots, D^{n-1}_t(\gamma(s))\big) T_p.$$

要在参数 t'处从 γ 变为 $\gamma' = f\gamma$，接着必须使用局部参数 t'应用引理3.9，由此得到一个矩阵

$$S'_p := \big(D^{m-j}_{t'}(f)\big)_{0 \leq j \leq m \leq n-1},$$

而不是矩阵 S_p（其元素为 $D^{m-j}_t(f)$）。因此，反向操作得到

$$\big(D'^0_t(\gamma'(s)), \ldots, D'^{n-1}_t(\gamma'(s))\big) = \big(D^0_t(\gamma(s)), \ldots, D^{n-1}_t(\gamma(s))\big) T_p\, S'_p.$$

这两个矩阵 S_p 和 S'_p 通过共轭相关：事实上，将引理3.8 应用于函数 f 本身可得

$$\big(D^0_{t'}(f), \ldots, D^{n-1}_{t'}(f)\big) = \big(D^0_t(f), \ldots, D^{n-1}_t(f)\big)\, T_p,$$

这等价于

$$S'_p = T_p^{-1}\, S_p\, T_p.$$

因此，$T_p\, S'_p = T_p\,(T_p^{-1} S_p T_p) = S_p T_p$，所以反向进行这些步骤会得到相同的最终矩阵 $S_p T_p$。□

3.4. 泰勒群。受上述引理启发，我们现在定义作用于数据 t_D, γ_D 的抽象群，这些数据定义了一个微分 Goppa 码。此处陈述的概念和结果后文还会再次出现。

设 X 是有限域 $\mathbb{F}_q$上的一条光滑曲线，$p \in X$ 是一个有理点，且 L 是 X上的一个可逆层。固定一个整数 $n \geq 1$，并回顾 $J^n_p = O_p/\mathfrak{m}_p^{n+1}$和 $J^n_p(L) = L_p/\mathfrak{m}_p^{n+1} L_p$。

定义 3.11。在 p 处、阶为 n的泰勒群是半直积

$$G_n(p) := (J^n_p)^{\times} \rtimes \mathrm{Aut}_{\mathbb{F}_q - alg}(J^n_p),$$

其中群运算 $\varphi \colon G_n(p) \times G_n(p) \to G_n(p)$ 定义为

$$(a_1, \sigma_1) \cdot (a_2, \sigma_2) \mapsto (a_1 \cdot \sigma_1(a_2), \sigma_1 \circ \sigma_2)$$

注记 3.12。 注意，$G_n(p)$ 是定义在 $\mathbb{F}_q$ 上的仿射代数群。

定义 3.13。 泰勒群 $G_n(p)$ 的基本作用是对 J_p^n 的作用，其定义规则为

$$\begin{aligned} \Xi : G_n(p) \times J_p^n &\to J_p^n \\ ((a,\sigma),r) &\mapsto a \cdot \sigma(r) \end{aligned} \tag{3.6}$$

引理 3.14. 基本作用是忠实的。

证明。 我们需要证明，若对所有 $r \in J$，都有 $a_1\sigma_1(r) = a_2\sigma_2(r)$，其中 $a_i \in J^\times$ 和 $\sigma_i \in \mathrm{Aut}_{\mathbb{F}_q\text{-alg}}(J)$，则 $a_1 = a_2$ 和 $\sigma_1 = \sigma_2$。由于 $\sigma_i(1) = 1$，在 $r = 1$ 处求值可得 $a_1 = a_2$。两边乘以 a_1^{-1}，得到对所有 r 都有 $\sigma_1(r) = \sigma_2(r)$，因此 $\sigma_1 = \sigma_2$。□

3.4.1. 基本表示。 取 p 处的一个局部参数 t_p。利用 J_p^n 的基 $\{1, t_p, \dots, t_p^{n-1}\}$，我们得到一个 $\mathbb{F}_q$-向量空间的同构u_{t_p}: $J_p^n \xrightarrow{\sim} \mathbb{F}_q^n$。

定义 3.15. 泰勒群$G_n(p)$的基本线性表示是由和诱导的线性表示

$$\rho_{t_p} : G_n(p) \longrightarrow \mathrm{Gl}_n(\mathbb{F}_q).$$

$J_p^n \xrightarrow{\sim} \mathbb{F}_q^n$。

我们的目标是明确描述ρ_{t_p}。为此，我们先引入一些记号。设$(a,\sigma) \in G_n(p)$，其中 $a \in (J_p^n)^\times$ 且 $\sigma \in \mathrm{Aut}^{\mathbb{F}_q-alg}(J_p^n)$。设 $f \in O_p^\times$ 满足

$$a = \overline{f} := f \pmod{\mathfrak{m}_p^n}. \tag{3.7}$$

那么， $a \mapsto f(t_p)$（模 t_p^n）给出了 $\mathbb{F}_q$-代数 $J_p^n \simeq \mathbb{F}_q[t_p]/t_p^n$的一个同构。在此同构下， $\sigma(t_p)$可写为

$$\sigma(t_p) = \sum_{r=1}^{n-1} c_r t_p^r, \quad c_1 \neq 0, \tag{3.8}$$

由于 t_p 生成 J_p^n，这个表达式完全确定了 σ。

引理 3.16. 矩阵$\rho_{t_p}(a,\sigma)$ 是以下乘积

$$\rho_{t_p}(a,\sigma) := S_p(a)\, T_p(\sigma),$$

其中 $S_p(a)$ 和 $T_p(\sigma)$ 是如下定义的下三角矩阵

$$(S_p(a))_{m,j} = D_{t_p}^{m-j}(f),$$

$$(T_p(\sigma))_{m,j} = \sum_{\substack{(k_1,\dots,k_m)\in\mathbb{N}^m \\ k_1+\cdots+k_{m-j+1}=j \\ \sum_{i=1}^{m-j+1} i k_i = m}} \binom{j}{k_1,\dots,k_{m-j+1}} \prod_{i=1}^{m-j+1} c_i^{k_i},$$

其中 $0 \le j \le m \le n-1$。

备注 3.17。 这些正是描述微分 Goppa 码定义中平凡化变换和局部参数变换的矩阵。

证明。 考虑 $\{1, t_p, \ldots, t_p^{n-1}\}$ 的 $\mathbb{F}_q$-向量空间 J_p^n。记$r = \sum_{j=0}^{n-1} r_j t_p^j$。根据线性表示 ρ_{t_p}的定义，3.7 和3.8，我们有：

$$\rho_{t_p}(a,\sigma)(r) = a \cdot \sigma(r) = f(t_p) \cdot \sigma\left(\sum_{j=0}^{n-1} r_j t_p^j\right) \pmod{t_p^n}.$$

由于 σ 是一个 $\mathbb{F}_q$-代数同态，我们有

$$\rho_{t_p}(a,\sigma)(r) = f(t_p) \cdot \sum_{j=0}^{n-1} r_j (\sigma(t_p))^j \pmod{t_p^n}.$$

设 $h = \rho_{t_p}(a,\sigma)(r) = \sum_{m=0}^{n-1} h_m t_p^m$。矩阵 ρ_{t_p} 必须满足关系$h_m = \sum_j (\rho_{t_p})_{m,j} r_j$。展开前面的表达式并利用 A.3 和A.4，我们得到

$$\sum_{m=0}^{n-1} h_m t_p^m = \left(\sum_{l=0}^{n-1} D_{t_p}^l(f) t_p^l\right) \sum_{j=0}^{n-1} r_j \left(\sum_{r=1}^{n-1} c_r t_p^r\right)^j \pmod{t_p^n}.$$

设$T_{s,j}$ 表示 $\sigma(t_p)^j$的第 s个系数。利用为多项式的 j次幂导出的多项展开公式，我们得到

$$T_{s,j} = \sum_{\substack{(k_1,\ldots,k_m)\in\mathbb{N}^m \\ k_1+\cdots+k_{s-j+1}=j \\ \sum_{i=1}^{s-j+1} i k_i = s}} \binom{j}{k_1,\ldots,k_{s-j+1}} \prod_{i=1}^{s-j+1} c_i^{k_i}.$$

将此代入该和式并重新排列求和次序，我们得到

$$\sum_{m=0}^{n-1} h_m t_p^m = \sum_{l=0}^{n-1} D_{t_p}^l(f) t_p^l \sum_{j=0}^{n-1} r_j \left(\sum_{s=j}^{n-1} T_{s,j} t_p^s\right) = \\ = \sum_{j=0}^{n-1} \left(\sum_{l=0}^{n-1}\sum_{s=j}^{n-1} D_{t_p}^l(f) T_{s,j} t_p^{l+s}\right) r_j.$$

取次数为 m 的项（其中 $m = l + s$），我们求得

$$h_m = \sum_{j=0}^{m} \left(\sum_{s=j}^{m} D_{t_p}^{m-s}(f) T_{s,j}\right) r_j.$$

这个和恰好符合下三角矩阵的矩阵乘法定义。特别是，

$$(\rho_{t_p})_{m,j} = \sum_{s=j}^{m} S_{m,s} T_{s,j},$$

其中 $S_{m,s} = D_{t_p}^{m-s}(f)$ 是下三角矩阵$S_p(a)$ 的第（m，s）项，而 $T_{s,j}$ 是表示自同构σ的矩阵的第（s，j）项。因此，$\rho_{t_p}(a,\sigma) = S_p(a) T_p(\sigma)$。□

注3.18。不难看出，基本表示表明，泰勒群为保持 Rosenbloom–Tsfasman 度量的线性自同构群中的一个三角子群提供了几何实现；关于该度量的深入研究见 [21]。也就是说，泰勒群可以视为源自形式局部几何的 Rosenbloom–Tsfasman 型自同构子群，即由局部参数的变换和局部平凡化的变换所产生的子群。

3.4.2. 平凡化空间上的作用。 固定一个平凡化 $\gamma_p : L_p \simeq O_p$ 以及 p 处的局部参数 t_p 。利用诱导同构 $\gamma_p : J_p^n(L) \simeq J_p^n$ 以及 J_p^n 的基 $\{1, t_p, \dots, t_p^{n-1}\}$，我们得到 $\mathbb{F}_q$-向量空间的一个同构

$$u_{t_p,\gamma_p} : J_p^n(L) \xrightarrow{\sim} \mathbb{F}_q^n. \tag{3.9}$$

令 $\mathrm{Iso}^{\mathbb{F}_q}(J_p^n(L)\ \mathbb{F}_q^n)$ 表示 $\mathbb{F}_q$–线性同构 $u\colon J_p^n(L) \to \mathbb{F}_q^n$ 的集合。令 $\mathrm{Iso}^{\mathrm{Tay}}(J_p^n(L)\ \mathbb{F}_q^n) \subset \mathrm{Iso}^{\mathbb{F}_q}(J_p^n(L)\ \mathbb{F}_q^n)$ 为由满足下述条件的那些同构 $u\colon J_p^n(L) \to \mathbb{F}_q^n$ 所组成的子集：存在 p 处的局部参数 t 以及平凡化 $\gamma\colon L_p \simeq O_p$，使得 $u = u_{t,\gamma}$。

固定一个平凡化 $\gamma_p : L_p \simeq O_p$。利用诱导同构 $\gamma_p : J_p^n(L) \simeq J_p^n$，我们得到一个作用

$$\Psi : G_n(p) \to \mathrm{Aut}(J_p^n(L))$$

如下：$g = (a, \sigma) \mapsto \Psi_g = (\gamma_p)^{-1} \circ \Xi_g \circ \gamma_p$，其中 $\Xi_g(r) = a \cdot \sigma(r)$（见 3.6）。因此，$G_n(p)$ 在平凡化集合 $\mathrm{Iso}^{\mathbb{F}_q}(J_p^n(L)\ \mathbb{F}_q^n)$ 上的作用由下式给出：

$$\begin{aligned} \widehat{\Psi} : G_n(p) \times \mathrm{Iso}_{\mathbb{F}_q}(J_p^n(L), \mathbb{F}_q^n) &\to \mathrm{Iso}_{\mathbb{F}_q}(J_p^n(L), \mathbb{F}_q^n) \\ (g, u) &\mapsto (g \cdot u) := u \circ \Psi_g^{-1} \end{aligned} \tag{3.10}$$

引理 3.19。设 $u \in \mathrm{Iso}^{\mathrm{Tay}}(J_p^n(L)\ \mathbb{F}_q^n)$ 且 $g \in G_n(p)$。则

$$g \cdot u := u \circ \Psi_g^{-1} \in \mathrm{Iso}_{\mathrm{Tay}}(J_p^n(L), \mathbb{F}_q^n).$$

$\widehat{\ }$等价地，$\mathrm{Iso}^{\mathrm{Tay}}(J_p^n(L)\ \mathbb{F}_q^n)$ 在作用 Ψ下是不变的。

证明。取 p 处的一个局部参数 t以及一个平凡化 $\gamma\colon L_p \simeq O_p$，使得$u = u_{t,\ \gamma}$（参见（3.9））。令 $g = (a,\ \sigma) \in G_n(p)$。回忆一下，$\gamma\colon J_p^n(L) \xrightarrow{\sim} J_p^n$是一个 J_p^n–模同构，并且 $\Psi_g = (\gamma)^{-1} \circ \Xi_g \circ \gamma$, $\Xi_g(r) = a \cdot \sigma(r)$。因此$g \cdot u = u_{t,\ \gamma} \circ \Psi_g^{-1} = u_{t,\ \gamma} \circ (\gamma)^{-1} \circ \Xi_g^{-1} \circ \gamma$。由于$u_{t,\ \gamma} = u_t \circ \gamma$，其中$u_t\colon J_p^n \xrightarrow{\sim} \mathbb{F}_q^n$是基 $\{1, t, \dots, t^n\}$下的系数映射，我们得到

$$g \cdot u = (u_t \circ \Xi_g^{-1}) \circ \overline{\gamma}. \tag{3.11}$$

现在我们逐步进行。

1. 由于 $\Xi_g(r) = a \cdot \sigma(r)$，我们有

$$\Xi_g^{-1}(r) = \sigma^{-1}(a^{-1} r), \tag{3.12}$$

对于每个 $(r \in J_p^n$。

2. 令 $\mathfrak{m} := \mathfrak{m}_p/\mathfrak{m}_p^{n+1}$ 为局部环 J_p^n 的极大理想。由于 $\sigma \in \mathrm{Aut}_{\mathbb{F}_q\text{-alg}}(J_p^n)$ 是环自同构，它保持 $\mathfrak{m}$（唯一的极大理想），因此也保持 $\mathfrak{m}^2$。所以 σ 诱导了 1 维向量空间 $\mathfrak{m}/\mathfrak{m}^2$上的一个 $\mathbb{F}_q$–线性自同构。特别地，若 t 表示一个

局部参数 t 在 J_p^n 中，则 $\sigma(\bar{t}) \in \mathfrak{m} \setminus \mathfrak{m}^2$。取 $t' \in \mathfrak{m}_p$，使其在 J_p^n 中的类等于 $\sigma(\bar{t})$。于是 $t' \notin \mathfrak{m}_p^2$，因此 t' 是 p 处的一个局部参数。根据构造，

$$\overline{t'} = \sigma(\bar{t}) \in J_p^n. \tag{3.13}$$

3. 考虑以下 $\mathbb{F}_q$–代数同构

$$\theta_t : \mathbb{F}_q[T]/(T^{n+1}) \xrightarrow{\sim} J_p^n, \quad T \mapsto \bar{t},$$
$$\theta_{t'} : \mathbb{F}_q[T]/(T^{n+1}) \xrightarrow{\sim} J_p^n, \quad T \mapsto \overline{t'}.$$

根据定义，u_t（分别为 $u_{t'}$）是以下映射的复合 θ_t^{-1}（分别为 $\theta_{t'}^{-1}$），并通过基 $\mathbb{F}_q[T]/(T^{n+1}) \simeq \mathbb{F}_q^{n+1}$ 给出的识别 $\{1, T, \dots, T^n\}$。等式（3.13）表明 $\sigma^{-1} \circ \theta_t' = \theta_t$。因此，

$$u_t \circ \sigma^{-1} = u_{t'}. \tag{3.14}$$

4. 由（3.12）和（3.14），可得 $u_t(\Xi_g^{-1}(r)) = u_t\big(\sigma^{-1}(a^{-1}r)\big) = u_{t'}(a^{-1} \cdot r)$，现在选取 $f \in O_p^\times$ 作为 $a^{-1} \in (J_p^n)^\times$ 的一个提升，并令 $\gamma' := f\,\gamma$。于是，诱导映射 $\gamma' \colon J_p^n(L) \to J_p^n$ 满足 $\gamma'(r)^- = a^{-1} \cdot \gamma(r)$。因此

$$(u_t \circ \Xi_g^{-1}) \circ \overline{\gamma} = u_{t'} \circ \overline{\gamma'} = u_{t',\gamma'}. \tag{3.15}$$

将（3.15）与（3.11）结合，即得 $g \cdot u = u_{t',\,\gamma'} \in \mathrm{Iso}^{\mathrm{Tay}}(J_p^n(L)\ \mathbb{F}_q^n)$，如所声称。□

命题 3.20。作用 Ψ 在 $\mathrm{Iso}^{\mathrm{Tay}}(J_p^n(L)\ \mathbb{F}_q^n)$ 上的限制是单纯传递的。也就是说，它是自由且传递的。

证明。我们需要证明该作用是传递且自由的。先证明该作用是自由的。固定 $u \in \mathrm{Iso}^{\mathrm{Tay}}(J_p^n(L)\ \mathbb{F}_q^n)$，并设对于某个 $g \in G_n(p)$ 有 $g \cdot u = u$。于是 $u \circ \Psi_g^{-1} = u$，这意味着 $\Psi_g = id$，因为 u 是一个同构。记 $g = (a, \sigma)$。在 $\gamma\colon J_p^n(L) \xrightarrow{\sim} J_p^n$ 下，条件 $\Psi_g = id$ 等价于 J_p^n 上的 $\Xi_g = id$，即对于所有 $r \in J_p^n$，都有 $a \cdot \sigma(r) = r$。取 $r = 1$，得到 $a = 1$。于是对于所有 r，都有 $\sigma(r) = r$，因此 $\sigma = id$，进而 $g = e$。所以 u 的稳定子群是平凡的。

还需证明该作用是传递的。固定 $u, v \in \mathrm{Iso}^{\mathrm{Tay}}(J_p^n(L)\ \mathbb{F}_q^n)$。选取一个局部参数 t 和一个平凡化 γ，使得 $u = u_{t,\gamma}$，并类似地选取 t', γ'，使得 $v = u_{t',\gamma'}$。考虑 $\mathbb{F}_q$– 线性自同构 $\phi := u^{-1} \circ v \in \mathrm{Aut}^{\mathbb{F}_q}(J_p^n(L))$。令 $\widetilde{\phi} := \gamma \circ \phi \circ (\gamma)^{-1} \in \mathrm{Aut}^{\mathbb{F}_q}(J_p^n)$。我们有 $\widetilde{\phi} = \gamma \circ \phi \circ \gamma^{-1} = u_t^{-1} \circ u_{t'} \circ (\gamma' \circ \gamma^{-1})$。由于 $\gamma' = \overline{f}\,\gamma$ 对唯一的 $f \in O_p^\times$ 成立，因此在 J_p^n 上有 $\gamma' \circ \gamma^{-1} = \times f$。定义

$$\sigma := u_t^{-1} \circ u_{t'} \in \mathrm{Aut}_{\mathbb{F}_q\text{-alg}}(J_p^n).$$

并令 $a := f \in (J_p^n)^\times$，我们得到

$$\widetilde{\phi}(r) = \sigma(a\,r) = \big(\sigma(a)\big) \cdot \sigma(r).$$

因此 $\phi = \Xi_{(a',\sigma)}$ 对于 $a' := \sigma(a) \in (J_p^n)^\times$。令 $g := (a', \sigma) \in G_n(p)$。那么 $\Psi_g = (\gamma)^{-1} \circ \Xi_g \circ \gamma = \phi$，因此 $g \cdot u = u \circ \Psi_g^{-1} = u \circ \phi^{-1} = v$。□

3.4.3. 关于泰勒平凡化的稠密性。 固定一个平凡化 $\gamma_p : L_p \simeq O_p$ 以及 p 处的一个局部参数 t_p。选择 (t_p, γ_p) 定义了一个双射

$$\begin{aligned} \Phi_{t_p,\gamma_p} : \mathrm{Iso}_{\mathbb{F}_q}(J_p^n(L), \mathbb{F}_q^n) &\xrightarrow{\sim} \mathrm{Gl}_n(\mathbb{F}_q) \\ u &\longmapsto u \circ u_{t_p,\gamma_p}^{-1}. \end{aligned} \tag{3.16}$$

其中$u_{t_p,\ \gamma_p}$ 的定义见3.9。另一方面，γ_p 诱导了一个作用

$$\Psi : G_n(p) \to \mathrm{Aut}(J_p^n(L))$$

通过基本作用定义如下： $g = (a,\ \sigma) \mapsto \Psi_g = (\gamma_p)^{-1} \circ \Xi_g \circ \gamma_p$其中 $\Xi_g(r) = a \cdot \sigma(r)$(见3.6)。回想一下， $G_n(p)$ 在平凡化集合$\mathrm{Iso}^{\mathbb{F}_q}(J_p^n(L)\ \mathbb{F}_q^n)$上的作用因此由下式给出

$$\begin{aligned} \widehat{\Psi} : G_n(p) \times \mathrm{Iso}_{\mathbb{F}_q}(J_p^n(L), \mathbb{F}_q^n) &\to \mathrm{Iso}_{\mathbb{F}_q}(J_p^n(L), \mathbb{F}_q^n) \\ (g, u) &\mapsto (g \cdot u) := u \circ \Psi_g^{-1} \end{aligned}$$

引理 3.21。映射 $\Phi_{t_p,\ \gamma_p}$ 是ρ_{t_p}-等变的，也就是说，

$$\Phi_{t_p,\gamma_p}(g \cdot u) = \Phi_{t_p,\gamma_p}(u) \cdot \rho_{t_p}(g)^{-1}$$

对所有 $g \in G_n$，$u \in \mathrm{Iso}^{\mathbb{F}_q}(J_p^n(L)\ \mathbb{F}_q^n)$，右侧表示标准矩阵乘法。

证明。 固定 $g = (a,\ \sigma) \in G_n(p)$。根据表示 ρ_{t_p} 的定义， Ξ_g 在基 $\{1, t_p, \ldots, t_p^{n-1}\}$ 中的表示矩阵恰好是 $\rho_{t_p}(g)$。就同构 $u_{t_p,\ \gamma_p}$ （定义于（3.9））而言，这等价于 $u_{t_p,\ \gamma_p} \circ \Psi_g \circ u_{t_p,\ \gamma_p}^{-1} = \rho_{t_p}(g)$。 $G_n(p)$ 在平凡化集合 $\mathrm{Iso}^{\mathbb{F}_q}(J_p^n(L)\ \mathbb{F}_q^n)$ 上的作用由规则 $(g \cdot u) := u \circ \Psi_g^{-1}$ 给出。将 $\Phi_{t_p,\ \gamma_p}$ 应用于此作用，我们得到

$$\begin{aligned} \Phi_{t_p,\gamma_p}(g \cdot u) &= (g \cdot u) \circ u_{t_p,\gamma_p}^{-1} \\ &= (u \circ \Psi_g^{-1}) \circ u_{t_p,\gamma_p}^{-1} \\ &= u \circ (\Psi_g^{-1} \circ u_{t_p,\gamma_p}^{-1}) \\ &= u \circ (u_{t_p,\gamma_p}^{-1} \circ u_{t_p,\gamma_p} \circ \Psi_g^{-1} \circ u_{t_p,\gamma_p}^{-1}) \\ &= (u \circ u_{t_p,\gamma_p}^{-1}) \circ (u_{t_p,\gamma_p} \circ \Psi_g^{-1} \circ u_{t_p,\gamma_p}^{-1}) \\ &= \Phi_{t_p,\gamma_p}(u) \circ \rho_{t_p}(g)^{-1} = \rho_{t_p}(g)\, \Phi_{t_p,\gamma_p}(u). \end{aligned}$$

□

引理 *3.22*。*Iso*$^{\mathrm{Tay}}(J_p^n(L)\ \mathbb{F}_q^n) = \Phi_{t_p,\gamma_p}^{-1}\left(\rho_{t_p}(G_n(p))\right)$ 成立。也就是说，*Iso*$^{\mathrm{Tay}}(J_p^n(L)\ \mathbb{F}_q^n)$ 是 *Iso*$^{\mathbb{F}_q}(J_p^n(L)\ \mathbb{F}_q^n)$ 中的单个 $G_n(p)$-轨道。特别地，*Iso*$^{\mathrm{Tay}}(J_p^n(L)\ \mathbb{F}_q^n) \subsetneq$ *Iso*$^{\mathbb{F}_q}(J_p^n(L)\ \mathbb{F}_q^n)$。此外，

$$\lim_{n\to\infty} \frac{|\,\mathrm{Iso}_{\mathrm{Tay}}(J_p^n(L), \mathbb{F}_q^n)|}{|\,\mathrm{Iso}_{\mathbb{F}_q}(J_p^n(L), \mathbb{F}_q^n)|} = 0$$

证明。第一部分由命题 3.20. 现在，由（3.16）可得

$$|\,\mathrm{Iso}_{\mathbb{F}_q}(J_p^n(L), \mathbb{F}_q^n)| = |\,\mathrm{Gl}_n(\mathbb{F}_q)| = \prod_{i=0}^{n-1}(q^n - q^i).$$

另一方面，$|(J_p^n)^\times| = (q-1)q^{n-1}$，$|\mathrm{Aut}^{\mathbb{F}_q-alg}(J_p^n)| = (q-1)q^{n-1}$，因此

$$|G_n| = (q-1)^2 q^{2n-2}.$$

因此 $|\mathrm{Iso}^{\mathrm{Tay}}(J_p^n(L)\ \mathbb{F}_q^n)| = |G_n| \ll |\mathrm{Gl}_n(\mathbb{F}_q)| = |\mathrm{Iso}^{\mathbb{F}_q}(J_p^n(L)\ \mathbb{F}_q^n)|$，显然如此。

$$\lim_{n\to\infty} \frac{|\mathrm{Iso}_{\mathrm{Tay}}(J_p^n(L), \mathbb{F}_q^n)|}{|\mathrm{Iso}_{\mathbb{F}_q}(J_p^n(L), \mathbb{F}_q^n)|} = \lim_{n\to\infty} \frac{(q-1)^2 q^{2n-2}}{\prod_{i=0}^{n-1}(q^n - q^i)} = 0$$

□

3.5. **一些备注**。

1. 请务必回顾备注 3.7。给定数据 X，D，L 其中$D = n_1 p_1 + \cdots + n_s p_s$，自然得到如下 $\mathbb{F}_q$-线性映射

$$H^0(X, L) \to L|_D = \oplus_{i=1}^s J_{p_i}^{n_i}(L).$$

通过固定平凡化 $\gamma_i \in \mathrm{Iso}^{\mathbb{F}_q}(J_{p_i}^{n_i}(L)\ \mathbb{F}_q^n)$，可得到一个 $\mathbb{F}_q$-线性映射

$$H^0(X, L) \to L|_D = \mathbb{F}_q^M,\ M := \sum_{i=1}^s n_i,$$

其像可视为与除子 D相关联的 Goppa 码，其重数不全为一；我们称之为重数 Goppa 码。迄今引入并研究的微分 Goppa 码构成重数 Goppa 码的一个子类，但这是一个相当特殊的子类。这正是引理3.22 所述的内容。重数 Goppa 码由任意平凡化（$\gamma_i \in \mathrm{Iso}^{\mathbb{F}_q}(J_{p_i}^{n_i}(L)\ \mathbb{F}_q^n)$）得到，而微分 Goppa 码则由泰勒平凡化（$\gamma_i \in \mathrm{Iso}^{\mathrm{Tay}}(J_{p_i}^{n_i}(L)\ \mathbb{F}_q^n)$）得到；与一般平凡化相比，泰勒平凡化极为特殊。

2. 容易证明，集合 $\mathrm{Iso}^t_{\mathrm{Tay}}(J_p^n(L)\ \mathbb{F}_q^n)$ 是一个仿射簇。事实上，它是由 Toeplitz 条件和非零常数项条件所定义的 $\mathrm{Mat}_{k\times M}(\mathbb{F}_q)$ 中某个仿射子空间的开子集。此外，泰勒群 $G_n(p)$（这是一个仿射代数群）在喷射空间上的作用是簇态射。因此，表示 ρ_{t_p}：$G_n(p) \to \mathrm{Gl}_n(\mathbb{F}_q)$ 是一个正则映射，也就是说，其矩阵项是群坐标的多项式函数。

4. 示例

4.1. 射影直线。取一个自然数 $k \geq 1$。令 $X = \mathbb{P}^1 := \mathrm{Proj}\mathbb{F}_q[x, y]$ 为射影直线，并取可逆层 $L = \mathcal{O}((k-1)p_\infty)$，其中 $p_\infty = [1; 0]$。令 $t := x/y$。众所周知，$H^0(\mathbb{P}^1, L)$ 的一组基为 $\{1, t, \ldots, t^{k-1}\}$。

4.1.1. 单点情形。 假设 $D = n \cdot p_\infty$。在此情形下，有理函数t 同时诱导出平凡化 γ：$L_{p_\infty} \to O_{p_\infty}$，$s \mapsto t^{-k+1}s$，以及在 p_∞，u 处的局部参数: $= t^{-1}$。对于任意 t^m，求值映射 $\mathrm{ev}_{t_D,\gamma_D}$:$H^0(\mathbb{P}^1, L) \to \mathbb{F}_q^n$ 由下式给出:

$$ev_{t_D,\gamma_D}(t^m) = \left(D_u^0(t^m)(p_\infty), D_u^1(t^m)(p_\infty), \ldots, D_u^{n-1}(t^m)(p_\infty)\right).$$

由于 $\gamma(t^m) = u^{k-m-1}$，因此有

$$D_u^j(\gamma(t^m))(p_\infty) = \delta_{j,k-m-1} := \begin{cases} 1, & \text{if } j = k-m-1, \\ 0, & \text{otherwise.} \end{cases}$$

因此，生成矩阵 $G(\infty) \in \mathbb{F}_q^{k\times n}$可由以下任一者给出

$$G(\infty) = \left[J_k \mid 0_{k\times(n-k)} \right], \text{ if } n \geq k$$

or

$$G(\infty) = \begin{pmatrix} 0_{(k-n)\times n} \\ J_n \end{pmatrix}, \text{ if } n \leq k,$$

其中 J_i 是 $i \times i$ 反对角矩阵

$$J_i = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

特别地，如果 $n = k$， $G(\infty)$ 是可逆的。等价地，$ev_{t_D,\ \gamma_D}$ 是一个同构。

4.1.2. 两点情形。 现在假设 $D = n \cdot p$，其中 $n \geq k$，并且 $p \neq p_\infty$是具有仿射坐标 $\alpha \in \mathbb{F}_q$的点。在此情形下， $L_p = O_p$ ，因此我们可以选择 id 作为 L_p的平凡化。另一方面，有理函数$u = t - \alpha$ 是 p处的局部参数。对于任意 t^m，我们已经知道求值映射 $ev_{t_D,\ \gamma_D}\colon H^0(\mathbb{P}^1,\ L) \to \mathbb{F}_q^n$ 由下式给出：

$$ev_{t_D,\gamma_D}(t^m) = \left(D_u^0(t^m)(\alpha), D_u^1(t^m)(\alpha), \ldots, D_u^{n-1}(t^m)(\alpha) \right).$$

利用二项式展开 $t^m = ((t-\alpha)+\alpha)^m$，我们得到：

$$D_u^j(t^m)(\alpha) = \binom{m}{j} \alpha^{m-j},$$

约定 $\binom{m}{j} = 0$ if $j > m$。生成矩阵的第 m 行（记作 $G(\alpha)$）对应于 t^m 的取值。因此，生成矩阵 $G(\alpha) \in \mathbb{F}_q^{k\times n}$的元素为

$$G(\alpha)_{m,j} = \binom{m}{j} \alpha^{m-j}, \qquad \text{with } \binom{m}{j} = 0 \text{ if } j > m,$$

并且可表示为以下任一种形式

$$G(\alpha) = \left[P_k(\alpha) \mid 0_{k\times(n-k)} \right], \text{ if } n \geq k,$$

or

$$G(\alpha) = \begin{pmatrix} P_n(\alpha) \\ R_{(k-n)\times n}(\alpha) \end{pmatrix}, \text{ if } n \leq k,$$

其中， $P_r(\alpha)$ 表示按 α 的幂进行缩放的 $r\times r$ 下三角帕斯卡矩阵，

$$P_r(\alpha) := \left(\binom{m}{j}\alpha^{m-j}\right)_{0\le m,j\le r-1} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \alpha & 1 & \cdots & 0 \\ \alpha^2 & \binom{2}{1}\alpha & \ddots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ \alpha^{r-1} & \binom{r-1}{1}\alpha^{r-2} & \cdots & 1 \end{pmatrix},$$

且 $R_{(k-n)\times n}(\alpha)$ 是由下式给出的 $(k-n)\times n$ 矩阵

$$R_{(k-n)\times n}(\alpha) := \left(\binom{m}{j}\alpha^{m-j}\right)_{n\le m\le k-1,\ 0\le j\le n-1}.$$

注意， $G(\alpha)$ 是满秩的。特别地，当 $k=n$ 时，求值映射是同构，且 $G(\alpha)$ 是可逆的。

4.1.3. 一般情形。 现在假设 $D=\sum_{i=1}^{s} n_i p_i$, $\sum_{i=1}^{s} n_i = n$ 其中 $p_1 = p_\infty$，并且对于 $i\ge 2$，点 p_i 的仿射坐标为 $\alpha_i\in\mathbb{F}_q$（因此 $p_i=[\alpha_i:\ 1]$）。我们按块排列 n 坐标，其中 $\mathbb{F}_q^n$ 的第 i 个块对应于导数 $D^j_{u_i}(\cdot)(p_i)$，对于 $j=0,\ \ldots\ldots,\ n_i-1$。

在 p_∞ 处，我们取局部参数 $u_1 := t^{-1}$ 以及平凡化 $\gamma_1 :\ L_{p_\infty}\to O_{p_\infty}$, $s\mapsto t^{-k+1}s$。对于 $i\ge 2$，我们取 p_i 处的局部参数 $u_i := t-\alpha_i$，并且由于 $p_i\neq p_\infty$，可以使用典范平凡化 $\gamma_i = \mathrm{id}$。于是，生成矩阵 G 分解为多个块

$$G = \big[\,G(\infty)\ \big|\ G(\alpha_2)\ \big|\ \cdots\ \big|\ G(\alpha_s)\,\big].$$

其中 $G(\infty)$ 和 $G(\alpha_i)$ 的计算方式见 §4.1.1 和 §4.1.2。

当然，我们也可以考虑对所有 i 都有 $p_i\neq p_\infty$ 的情形。在这种情况下，生成矩阵就是

$$G = \big[\,G(\alpha_1)\ \big|\ G(\alpha_2)\ \big|\ \cdots\ \big|\ G(\alpha_s)\,\big].$$

4.1.4. 亏格0 文献中的微分 *Goppa* 码。 现在我们的目标是展示所提出的框架与编码理论中已有构造之间的联系。

在文献 [32] 和 [33], 中，通过添加以下形式的标准基列向量来扩展经典 Reed–Solomon 码。

$$V_i = [0,\ldots,0,1,0,\ldots,0].$$

这些扩展得到近极大距离可分（NMDS）码，而这些码已无法再表示为亏格0或1的经典 Goppa 码。然而，对于微分 Goppa 码，情况则不再如此。在此背景下，相同的构造在射影直线 $\mathbb{P}^1$ 上具有如下微分 Goppa 结构。

令 $X=\mathbb{P}^1$，令 $L=\mathcal{O}_X((k-1)p_\infty)$，并定义除子

$$D = 2p_\infty + 2p_0 + \sum_{i=1}^{q-1} p_i.$$

对于 $k = 4$ 或 $k = 5$，它们分别对应于 [32], 中分析的两种情况，相关的生成矩阵具有以下显式形式。

$$G_4 = \begin{bmatrix} \alpha_1^3 & \cdots & \alpha_q^3 & 1 & 0 & 0 \\ \alpha_1^2 & \cdots & \alpha_q^2 & 0 & 1 & 0 \\ \alpha_1 & \cdots & \alpha_q & 0 & 0 & 1 \\ 1 & \cdots & 1 & 0 & 0 & 0 \end{bmatrix}, \qquad \alpha_i \neq \alpha_j \in \mathbb{F}_q.$$

因此，扩展 NMDS 码自然地源自 $\mathbb{P}^1$ 上喷射层的上同调描述，无需通过增加基曲线的亏格来构造。

在 [12] 中研究的 Roth–Lempel 码也呈现出类似的现象。这些码曾被作为无法通过射影直线或椭圆曲线上的经典 Goppa构造得到的例子。然而，在这一框架下，它们可以表示为 $\mathbb{P}^1$ 上的微分 Goppa 码。同样，设 $L = \mathcal{O}_X((k-1)p_\infty)$，并定义除子

$$D = 2p_\infty + \sum_{i=0}^{q-1} p_i,$$

由此诱导的态射 $H^0(\Theta_D)$ 得到如下形式的生成矩阵。

$$R_k = \begin{bmatrix} \alpha_1^{k-1} & \cdots & \alpha_q^{k-1} & 1 & 0 \\ \vdots & & \vdots & 0 & 1 \\ \vdots & & \vdots & 0 & 0 \\ \vdots & & \vdots & \vdots & \vdots \\ \alpha_1 & \cdots & \alpha_q & 0 & 0 \\ 1 & \cdots & 1 & 0 & 0 \end{bmatrix}, \qquad \alpha_i \neq \alpha_j \in \mathbb{F}_q. \tag{4.1}$$

这一表示表明，Roth–Lempel族也自然地符合微分Goppa形式体系。

尽管要完整验证其结构性质，需要进行与所引用文献中相当的详细分析，但本文提出的总体框架阐明了这些构造的几何起源。这种方法以 $\mathbb{P}^1$ 上的线丛和除子为基础进行统一描述，取代了逐案分析或计算论证。

4.2. 椭圆曲线。 为简单起见，假设 $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$。固定自然数 $1 \leq k \leq n$，令 $E \subset \mathbb{P}^2 = \mathrm{Proj}\ \mathbb{F}_q[X, Y, Z]$ 为魏尔斯特拉斯形式的椭圆曲线

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{F}_q,$$

其中，$x = X/Z$ 和 $y = Y/Z$ 是 $\mathbb{P}^2$ 的开子集 $Z \neq 0$ 上的仿射坐标。注意，无穷远点为 $e = [0;\ 1;\ 0]$。现在考虑可逆层 $L = O_E((k-1)e)$。众所周知，$H^0(E,\ L)$ 的一组基为

$$\mathcal{B}_k = \{1, x, \ldots, x^a,\ y, xy, \ldots, x^b y\},$$

其中

$$a := \left\lfloor \frac{k-1}{2} \right\rfloor, \qquad b := \left\lfloor \frac{k-4}{2} \right\rfloor.$$

4.2.1. 单点情形。 假设 $D = n \cdot e_\circ$ 有理函数 $u := -\frac{x}{y}$ 是 $e \in E$ 处的局部参数。另一方面，在 e 处， L 显然可以平凡化： $\gamma\colon\ L_e \to O_e,\ s \mapsto u^{k-1}s_\circ$ 因此，对于每个 $s \in H^0(E, L)$，我们有

$$ev_{t_D,\gamma_D}(s) = \big(D_u^0(\gamma(s))(e),\ D_u^1(\gamma(s))(e),\ \ldots,\ D_u^{n-1}(\gamma(s))(e)\big) \in \mathbb{F}_q^n.$$

由于 $\mathrm{ord}_e(x) = -2$ 且 $\mathrm{ord}_e(y) = -3$，我们在 e处关于 u得到 Laurent 展开

$$\begin{aligned} x &= u^{-2} + (\text{higher powers of } u),\\ y &= -u^{-3} + (\text{higher powers of } u), \end{aligned}$$

因此

$$\begin{aligned} \gamma(x^m) &= u^{k-1-2m}\big(1 + \cdots\big),\\ \gamma(x^m y) &= u^{k-1-(2m+3)}\big(-1 + \cdots\big). \end{aligned}$$

特别地，每个 $\gamma(b_r)$ 都有定义良好的最低次项 $\varepsilon_r\, u^{\rho_r}$，其中 $\varepsilon_r \in \{\pm 1\}$且 $\rho_r \geq 0$，因此

$$D_u^j(\gamma(b_r))(e) = 0 \ \text{ for } j < \rho_r, \qquad D_u^{\rho_r}(\gamma(b_r))(e) = \varepsilon_r \in \{\pm 1\}.$$

按照在 e处的阶递增顺序重新排列 $\mathcal{B}_k$ 的元素，我们可以假设 $\rho_1 \leq \rho_2 \leq \cdots \leq \rho_{k\circ}$ 若考虑由行 $j \in \{\rho_1, \ldots, \rho_k\}$构成的 G 的子矩阵 G'，则 G' 为上三角矩阵，其对角线元素为$\varepsilon_r \in \{\pm 1\}$，

$$G' = \begin{pmatrix} \varepsilon_1 & * & * & \cdots & * \\ 0 & \varepsilon_2 & * & \cdots & * \\ 0 & 0 & \varepsilon_3 & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \varepsilon_k \end{pmatrix},$$

其中 $*$ 表示可能非零的元素。特别地，子矩阵G' 具有满秩 k，这意味着原矩阵 G 的秩为 $k_\circ$ 因此，如果 $n = k$，矩阵 G 是可逆的。

4.2.2. 两点情形。 现在假设 $D = n \cdot p$，其中 $p = (\alpha, \beta) \in E$ 是一个满足 $p \neq e$ 的有理点。为简单起见，假设 $\beta \neq 0_\circ$ 那么

$$v := x - \alpha$$

是 p 处的局部参数，并且由于 $p \neq e$，我们可以使用恒等映射作为 L_p 的平凡化（即 $\gamma =$id）。求值映射为

$$ev_{t_D,\gamma_D}(f) = \big(D_v^0(f)(p),\ D_v^1(f)(p),\ \ldots,\ D_v^{n-1}(f)(p)\big) \in \mathbb{F}_q^n.$$

考虑 y 在 p 处关于 v 的泰勒展开，

$$y(v) = \beta + \sum_{r \geq 1} c_r v^r \in \mathbb{F}_q[[v]]$$

显然，展开式的系数由方程确定

$$\big(\beta + \sum_{r \geq 1} c_r v^r\big)^2 = (\alpha + v)^3 + A(\alpha + v) + B.$$

比较系数可得递推关系（其中 $c_0 := \beta$）

$$\begin{aligned} 2\beta\, c_1 &= 3\alpha^2 + A, \\ 2\beta\, c_2 + c_1^2 &= 3\alpha, \\ 2\beta\, c_3 + 2c_1c_2 &= 1, \\ 2\beta\, c_m + \sum_{r=1}^{m-1} c_r c_{m-r} &= 0, \qquad \text{for } m \geq 4. \end{aligned}$$

生成矩阵 $G \in \mathbb{F}_q^{k\times n}$定义为 $G_{r,\,j} = D_v^j(b_r)(p)$，其中 r =1、……、 k, $j = 0$、……、 $n-1$。其元素可明确写成如下形式。对于$m \geq 0$,

$$\begin{aligned} D_v^j(x^m)(p) &= \binom{m}{j}\,\alpha^{m-j} \\ D_v^j(x^m y)(p) &= D_v^j\big((\alpha+v)^m(\beta+\sum_{r\geq 1} c_r v^r)\big)(0) \\ &= \sum_{s=0}^{\min(j,m)} \binom{m}{s}\,\alpha^{m-s}\, c_{j-s}. \end{aligned} \tag{4.2}$$

特别地，前几行（对应于 1，x、…… ）构成一个缩放的帕斯卡型块：

$$\begin{pmatrix} 1 & 0 & 0 & \cdots \\ \alpha & 1 & 0 & \cdots \\ \alpha^2 & \binom{2}{1}\alpha & 1 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix},$$

而对应于 y 的行是

$$\big(\beta,\ c_1,\ c_2,\ \ldots,\ c_{n-1}\big),$$

对应于 xy 的行是

$$\big(\alpha\beta,\ \beta + \alpha c_1,\ c_1 + \alpha c_2,\ \ldots\big),$$

依此类推，根据公式（4.2）。

4.2.3. 多个点情形。 最后假设 $D = \sum_{i=1}^{s} n_i p_i$, $\sum_{i=1}^{s} n_i = n$ 是两两不同的有理点，并且允许 $p_1 = e$。若$p_i = e$，则取 $u_i = -x/y$ 为局部参数，并像单点情形那样通过 $\gamma_i(s) = u_i^{k-1}s$ 进行平凡化。若 $p_i \neq e$ 且 $p_i = (\alpha_i, \beta_i)$ 满足 $\beta_i \neq 0$，则取 $u_i = x - \alpha_i$为局部参数，并使用典范平凡化 $\gamma_i = id$。

与亏格零情形一样，生成矩阵可分解为若干块

$$G = \big[G^{(1)} \mid G^{(2)} \mid \cdots \mid G^{(s)}\big], \qquad G^{(i)} \in \mathbb{F}_q^{k\times n_i}.$$

若 $p_i = e$，块 $G^{(i)}$ 按 §4.2.1 计算。若 $p_i = (\alpha_i,\ \beta_i) \neq e$ （其中$\beta_i \neq 0$），块 $G^{(i)}$ 按 §4.2.2计算。与射影直线情形一样，将支撑 D 中各点对应的块依次拼接，即可得到完整的生成矩阵。

5. 微分 Goppa 码 II. 对偶性

几何 Goppa 码经典理论中的一个重要结果是，Goppa 码的对偶仍是 Goppa 码（见 [27, 29]）。这一重要结果建立在塞尔对偶、留数定理，以及亚纯微分的留数给出一个典范平凡化这一事实之上$\omega_X(p)|_p \simeq \mathbb{F}_q$（见 [29, §3.1.3，第 289] 页）。本节将证明一个类似的结果，即微分 Goppa 码的对偶也是微分 Goppa 码。为此，我们首先需要证明，一旦固定了 p 的一个局部参数，就存在一个 $\omega_X(np)${v27>的典范平凡化。

在本节中，X 是亏格为 g 的光滑射影曲线，定义在$\mathbb{F}_q$ 上，ω_X 是其典范层。

5.1. 重数双线性型与对偶码。 在陈述微分 Goppa 码的对偶定理之前，我们需要一个自然的双线性型，以便在重数 Goppa 码的背景下定义正交性。

考虑 $\mathbb{F}_q^M$，并固定 M、$H = \{n_1, \dots, n_s\}$ 的一个划分，其中 $\sum_{i=1}^s n_i = M$。我们用块坐标表示向量

$$c = (c_{1,0}, \dots, c_{1,n_1-1}\,;\ \dots\ ;\, c_{s,0}, \dots, c_{s,n_s-1}) \in \mathbb{F}_q^M,$$

对于 c'也类似。此处有一个标准的双线性型（见 [26, 5]）。

定义 5.1. $\mathbb{F}_q^M$上的 H-双线性型是如下映射

$$\langle \cdot, \cdot \rangle_H : \mathbb{F}_q^M \times \mathbb{F}_q^M \longrightarrow \mathbb{F}_q$$

定义为

$$\langle c, c' \rangle_H := \sum_{i=1}^{s} \sum_{j=0}^{n_i-1} c_{i,j}\, c'_{i,n_i-1-j}.$$

引理 5.2. 双线性型 $\langle \cdot, \cdot \rangle_H$ 是非退化的。

证明。显然，$\langle \cdot, \cdot \rangle_H$ 是 $\mathbb{F}_q$-双线性的。为证明非退化性，固定一个 $c \in V$，使得对所有 $c' \in V$，都有 $\langle c, c' \rangle_H = 0$。固定一个块指标 $i \in \{1, \dots, s\}$ 和一个坐标指标 $j \in \{0, \dots, n_i - 1\}$。令 $c' \in V$为一个向量，除 $c'_{i,n_i-1-j} = 1$外，其余坐标均为 0。于是，根据 $\langle \cdot, \cdot \rangle_H$的定义，双重求和中除指标为 (i, j) 的一项外，其余各项均为零，因此得到

$$0 = \langle c, c' \rangle_H = c_{i,j}.$$

由于 i 和 j 是任意的，c 的所有坐标都为零，因此 $c = 0$。所以 $\langle \cdot, \cdot \rangle_H$ 的左根基为零，因此 $\langle \cdot, \cdot \rangle_H$ 是非退化的。□

定义 5.3. 设 $C \subset \mathbb{F}_q^M$是一个线性子空间。C 的 H-对偶定义为

$$C^{\perp_H} := \{c' \in \mathbb{F}_q^M \mid \langle c, c' \rangle_H = 0 \ \forall c \in C\}$$

引理 5.4. 设 $C \subset V$ 是一个线性码。则有

1. 维数 $C^{\perp_H} = M -$ 维数 C。
2. $(C^{\perp_H})^{\perp_H} = C$。

证明。结论 (1) 和 (2) 由 $\langle \cdot, \cdot \rangle_H$ 的非退化性得出。 □

5.2. **对偶泰勒平凡化**。 已知经典 Goppa 码的对偶码也是 Goppa 码。这一基本结果建立在 Serre 对偶定理以及 $L|_p$ 的平凡化与 $(L^{-1} \otimes \omega_X(p))|_p$ 的平凡化之间的自然对应关系之上。本节将这一对应关系推广到多重点的情形。

引理 5.5. 设 $p \in X$ 是一个有理点， t 是 p处的一个局部参数。令$\mathrm{Triv}(L_p)$ 表示 O_p-线性同构 $\gamma\colon L_p \to O_p$的集合。

1. $\mathrm{Triv}(L_p)$ 是单位群 $O_p^\times$作用下的一个扭子。**2.** 对于任意 $\gamma \in \mathrm{Triv}(L_p)$，元素

$$\xi_{gen} := \gamma \otimes (t^{-n}dt) \tag{5.1}$$

是 O_p-模 $N_p = L_p^{-1} \otimes \omega_X(np)_p$的一个生成元

3. 映射

$$\Theta : \mathrm{Triv}(L_p) \longrightarrow \mathrm{Triv}(N_p),$$

其中 $\Theta(\gamma)$ 是将局部生成元 $\gamma \otimes t^{-n}dt$映至1的唯一平凡化；该映射相对于 $O_p^\times$的求逆自同构是等变的：

$$\Theta(u\gamma) = u^{-1}\Theta(\gamma).$$

特别地，它是一个双射。

证明。 1）这是一个众所周知的事实。

2）由于 L_p 是一个局部自由的 O_p-模，秩为 1，因此任意同构 γ 都是 L_p^{-1} 的一个基。同理， $t^{-n}dt$ 是 $\omega_X(np)_p$ 的一个基。两个秩 1 模的基的张量积是张量积模 N_p 的一个基，因此 ξ_{gen} 是一个生成元。

3）由 2）可知，$\mathrm{Triv}(L_p)$ 和 $\mathrm{Triv}(N_p)$ 都是单位群 $O_p^\times$ 作用下的扭子。现在，若我们将 γ 替换为 $\gamma' := u\gamma$，其中某个 $u \in O_p^\times$，则新的生成元为：

$$\xi'_{gen} = (u\gamma) \otimes (t^{-n}dt) = u(\gamma \otimes t^{-n}dt) = u\xi_{gen}.$$

由于 $\Theta(\gamma')(\xi'_{gen}) = 1$，我们必有 $\Theta(\gamma') = u^{-1}\Theta(\gamma)$。因此，映射 Θ 关于 $O_p^\times$ 的求逆自同构是等变的。回想一下，扭子之间的任何等变态射必定是一个双射。□

引理 5.6. 设 $p \in X$ 为一个有理点， t 为p处的一个局部参数。考虑与 t 相关联的 $J_p^n(L)$ 的泰勒平凡化集合，$\mathrm{Iso}^t_{\mathrm{Tay}}(J_p^n(L)\ \mathbb{F}_q^n)$。对偶映射 $\Theta\colon \mathrm{Triv}(L_p) \to \mathrm{Triv}(N_p)$ 可下降为泰勒平凡化空间之间一个良定义的映射：

$$\overline{\Theta} : \mathrm{Iso}^t_{\mathrm{Tay}}(J_p^n(L), \mathbb{F}_q^n) \longrightarrow \mathrm{Iso}^t_{\mathrm{Tay}}(J_p^n(N), \mathbb{F}_q^n).$$

此外，下图交换：

$$\begin{array}{ccc} \mathrm{Triv}(L_p) & \xrightarrow{\Theta} & \mathrm{Triv}(N_p) \\ \downarrow{\scriptstyle \pi_L} & & \downarrow{\scriptstyle \pi_N} \\ \mathrm{Iso}^t_{\mathrm{Tay}}(J_p^n(L), \mathbb{F}_q^n) & \xrightarrow{\overline{\Theta}} & \mathrm{Iso}^t_{\mathrm{Tay}}(J_p^n(N), \mathbb{F}_q^n) \end{array}$$

其中 π_L 和 π_N 是模 $\mathfrak{m}_p^n$的自然约化映射。

证明。设 $\gamma_1, \gamma_2 \in \mathrm{Triv}(L_p)$ 是两个定义相同模 $\mathfrak{m}_p^n$泰勒平凡化的平凡化。这意味着存在某个单位元 $u \in O_p^\times$，使得 $\gamma_2 = u\gamma_1 \mod \mathfrak{m}_p^n$。由引理 5.5 3)，我们有 $\Theta(\gamma_2) = \Theta(u\gamma_1) = u^{-1}\Theta(\gamma_1)$。由于 u 的形式为 $1 + m$，其中 $m \in \mathfrak{m}_p^n$，其在局部环 O_p中的逆元也满足 $u^{-1} \equiv 1 \mod \mathfrak{m}_p^n$。因此，$\pi_N(\Theta(\gamma_2)) = \pi_N(\Theta(\gamma_1))$，这证明了 Θ 定义良好。该图的交换性可直接由构造得出。□

引理 5.7。设 $p \in X$ 是一个有理点，t 是 p 处的局部参数。令$\gamma \in \mathrm{Triv}(L_p)$ 为一个局部平凡化，并令 $\Theta(\gamma) : N_p \xrightarrow{\sim} O_p$ 为对偶平凡化。对于任意截面 $\xi \in N_p$，在泰勒平凡化 $\Theta(\gamma)$ 下，$\xi := \xi \mod \mathfrak{m}_p^n \in \cancel{J_p^n(N)}$ 的坐标向量 $(g_0, \ldots, g_{n-1}) \in \mathbb{F}_q^n$为

$$g_k = \mathrm{Res}_p(t^{n-1-k}\eta_\xi), \quad for\ k = 0, \ldots, n-1,$$

其中 $\eta_\xi \in \omega_X(np)^p$ 是满足关系 $\xi = \gamma \otimes \eta_\xi$的微分形式。

证明。根据 N_p 作为秩为 1 O_p 的模的定义，截面 ξ 可以唯一表示为 $\xi = g \cdot \xi_{gen}$，其中 $g \in O_p$（见 5.1）。另一方面，$\Theta(\gamma)$ 由条件 $\Theta(\gamma)(\xi_{gen}) = 1$ 唯一确定（见引理 5.5）。应用平凡化 $\Theta(\gamma)$并利用其 O_p-线性性，得到 $\Theta(\gamma)(\xi) = \Theta(\gamma)(g \cdot \xi_{gen}) = g \cdot \Theta(\gamma)(\xi_{gen}) = g$。因此，$\Theta(\gamma)(\xi)$的像是向量 $(g_0, \ldots, g_{n-1})$，由函数 g 在 p 处关于局部参数 t的泰勒展开的前 n 个系数组成。为了将这些系数与 η_ξ的留数联系起来，我们比较 ξ的两种表示

$$\gamma \otimes \eta_\xi = g \cdot (\gamma \otimes t^{-n}dt) = \gamma \otimes (gt^{-n}dt). \tag{5.2}$$

这意味着亚纯微分的恒等映射 $\eta_\xi = gt^{-n}dt$。将泰勒展开 $g(t) = \sum_{j=0}^{\infty} g_j t^j$ 代入该表达式，得到

$$\eta_\xi = \left(\sum_{j=0}^{\infty} g_j t^j \right) t^{-n}dt = \sum_{j=0}^{\infty} g_j t^{j-n}dt.$$

另一方面，对于任意整数 $m \geq 0$，我们有

$$\mathrm{Res}_p(t^m \eta_\xi) = \mathrm{Res}_p \left(\sum_{j=0}^{\infty} g_j t^{j-n+m}dt \right).$$

根据留数的定义，只有 t 的指数为 -1 的项会产生贡献。这发生在 $j - n + m = -1$时，或者等价地，$j = n - 1 - m$。因此，$\mathrm{Res}_p(t^m\eta_\xi) = g_{n-1-m}$。令$k = n - 1 - m$，由此可得 $m = n - 1 - k$，于是得到：

$$g_k = \mathrm{Res}_p(t^{n-1-k}\eta_\xi).$$

□

5.3. **对偶定理**。 考虑如下几何数据 $(X,\ L,\ D)$ 如 §3.2中所示，并令 $M=\sum n_i$。 于是我们有短正合列

$$0\to L(-D)\to L\to L|_D\to 0$$

取整体截面后，我们得到

$$\cdots\to H^0(X,L)\to L|_D\to H^1(X,L(-D))\to\cdots$$

这里， $L|_D$ 就是 $\oplus_{i=1}^s J_{p_i}^{n_i-1}(L)$ (参见 (2.5))。令 $L|_D\simeq\mathbb{F}_q^M$为由数据 $(\{t_i\},\gamma_D)$给出的泰勒平凡化。那么，我们已经知道，

$$H^0(X,L)\to L|_D\simeq\mathbb{F}_q^M$$

恰好是微分 Goppa 码 $C(X,L,D,t_D,\gamma_D)$ (参见备注 3.7）。另一方面，我们可以考虑可逆层 $N=L^{-1}\otimes\omega_X(D)$所对应的上同调正合列:

$$\cdots\to H^0(X,L^{-1}\otimes\omega_X(D))\to(L^{-1}\otimes\omega_X(D))|_D\to H^1(X,L^{-1}\otimes\omega_X)\to\cdots$$

定义 5.8。 与数据 (X,L,D,t_D,γ_D) 相关联的对偶微分 Goppa 码定义为微分 Goppa 码

$$C(X,N,D,t_D,\Theta(\gamma_D))\ \text{ with } N=L^{-1}\otimes\omega_X(D).$$

其中 $\Theta(\gamma_D):=\{\Theta(\gamma_i)\}$ 我们将线性映射记为 $\mathrm{Res}_{t_D,\ \gamma_D}$

$$H^0(X,L^{-1}\otimes\omega_X(D))\to(L^{-1}\otimes\omega_X(D))|_D\simeq\mathbb{F}_q^M.$$

其像为 $C(X,\ N,\ D,\ t_D,\ \Theta(\gamma_D))$.

命题 5.9. 对于截面 $s\in H^0(X,L)$ 和 $\xi\in H^0(X,N)$，令 $\langle s,\xi\rangle\in H^0(X,\omega_X(D))$ 为由自然缩并 $L\otimes L^{-1}\to O_X$诱导的截面。固定一个指标 i、 p_i处的局部参数 t_i 以及局部平凡化 $\gamma_i: L_{p_i}\xrightarrow{\sim} O_{p_i}$。则:

$$\mathrm{Res}_{p_i}(\langle s,\xi\rangle)=\sum_{j=0}^{n_i-1}D_{t_i}^{(j)}\big(\gamma_i(s)\big)(p_i)\cdot\mathrm{Res}_{p_i}\Big(t_i^{n_i-1-j}\eta_i\Big).$$

其中 $\eta\in\omega_X(np)_{p_i}$ 是满足 $\xi=\gamma_i\otimes\eta_i$ 属于 O_{p_i}的微分形式。

证明。 给定 γ_i 和 t_i，我们有 $\Theta(\gamma_i)$。这些平凡化确定了 L_{p_i}和 N_{p_i}的局部基。具体而言， $e_i=\gamma_i^{-1}(1)$ 是 L_{p_i}的一个基，而 $\gamma_i\otimes t^{-n}dt$是 N_{p_i}的一个基。于是，我们可以在 p_i 处将 s 和 ξ 局部表示为： $s=f_ie_i$ 和$\xi=g_i\left(\gamma_i\otimes\frac{dt_i}{t_i^{n_i}}\right)$，其中 f_i，$g_i\in O_{p_i}$。 缩并 $\langle s,\ \xi\rangle$ 在 $\omega_X(D)_{p_i}$ 中由下式给出

$$\langle s,\xi\rangle=f_ig_i\frac{dt_i}{t_i^{n_i}}.$$

留数 $\mathrm{Res}_{p_i}(\langle s,\xi\rangle)$ 对应于 $f_ig_i/t_i^{n_i}$ 的 Laurent 展开中 t_i^{-1} 的系数，这等价于 $f_i(t_i)g_i(t_i)$ 的泰勒展开中的第 (n_i-1) 个系数。设 $f_i(t_i)=\sum_{a=0}^{\infty}f_{i,a}t_i^a$ 和 $g_i(t_i)=\sum_{b=0}^{\infty}g_{i,b}t_i^b$ 分别为相应的展开。根据柯西乘积，有:

$$\mathrm{Res}_{p_i}(\langle s,\xi\rangle)=\sum_{j=0}^{n_i-1}f_{i,j}g_{i,n_i-1-j}.\tag{5.3}$$

根据定义， f_i 的泰勒展开系数由哈斯导数 $f_{i,j} = D_{t_i}^{(j)}(f_i)(p_i) = D_{t_i}^{(j)}(\gamma_i(s))(p_i)$ 给出。由引理 5.7 可得 $g_{i,n_i-1-j} = \mathrm{Res}_{p_i}(g_i(t_i)\frac{dt_i}{t_i^{n_i-j}}) = \mathrm{Res}_{p_i}(t_i^{n_i-1-j}\eta_i)$。将这些恒等式代入 (5.3)，即完成证明。□

定理 5.10. 设 (X, L, D) 如上所述，且 (t_D, γ_D) 为选定的泰勒数据。设 $C = C(X, L, D, t_D, \gamma_D)$ 为相应的微分 *Goppa* 码。相对于 $\mathbb{F}_q^M$上的 H-双线性型， C 的对偶码恰为对偶微分 *Goppa* 码：

$$C^{\perp_H} = C(X, N, D, t_D, \Theta(\gamma_D)).$$

其中 $\Theta(\gamma_D) := \{\Theta(\gamma_1) \dots, \Theta(\gamma_s)\}$.

证明。设 $s \in H^0(X, L)$ 和 $\xi \in H^0(X, N)$。设 $c = ev_{t_D,\gamma_D}(s)$ 和 $c' = \mathrm{Res}_{t_D,\gamma_D}(\xi)$ 为相应的码字。根据 $\mathbb{F}_q^M$上的 H-双线性型的定义，我们有：

$$\langle c, c'\rangle_H = \sum_{i=1}^{s}\langle c_i, c_i'\rangle_{H,n_i},\ \langle c_i, c_i'\rangle_{H,n_i} := \sum_{j=0}^{n_i-1} c_{i,j}\, c'_{i,n_i-1-j}.$$

其中 $c_i = (c_{i,0}, \dots, c_{i,n_i-1})$ 和 $c_i' = (c_{i,0}, \dots, c_{i,n_i-1})$。根据引理 5.7，对偶截面的坐标满足 $c'_{i,n_i-1-j} = \mathrm{Res}_{p_i}(t_i^j\eta_{\xi,i})$，其中 $\eta_{\xi,i}$ 是 ξ 在 p_i 处的局部微分代表元，使得 $\xi = \gamma_i \otimes \eta_{\xi,i}$。另一方面，系数 c_i 由哈斯导数给出（参见注 3.5）：

$$c_{i,j} = D_{t_i}^{(j)}(f_i)(p_i) = D_{t_i}^{(j)}(\gamma_i(s))(p_i).$$

将这些代入局部 H-配对：

$$\langle c_i, c_i'\rangle_{H,n_i} = \sum_{j=0}^{n_i-1} c_{i,j}c'_{i,n_i-1-j} = \sum_{j=0}^{n_i-1} D_{t_i}^{(j)}(\gamma_i(s))(p_i)\,\mathrm{Res}_{p_i}(t_i^j\eta_{\xi,i})$$

由命题 5.9 可知，最后一项是在p_i处的 $\langle s, \xi\rangle$ 留数。因此 $\langle c, c'\rangle_H = \sum_{i=1}^{s}\mathrm{Res}_{p_i}(\langle s, \xi\rangle)$。根据留数定理 (2.2)，曲线 X 上全局亚纯微分在所有点处的留数之和为零。由于 $\langle s, \xi\rangle$ 在 D的支撑之外正则，我们有$\sum_{i=1}^{s}\mathrm{Res}_{p_i}(\langle s, \xi\rangle) = 0$，从而证明了 $C(X, N, D, t_D, \Theta(\gamma_D)) \subseteq C^{\perp_H}$。

为证明这个等式，我们比较维数。由上同调的长正合列、塞尔对偶以及引理 3.6 可知：

$$\begin{aligned}\dim C(X, L, D, t_D, \gamma_D) &= \dim H^0(X, L) - \dim H^0(X, L(-D))\\ \dim C(X, N, D, t_D, \Theta(\gamma_D)) &= \dim H^0(X, N) - \dim H^0(X, N(-D))\\ &= \dim H^1(X, L(-D)) - \dim H^1(X, L)\end{aligned}$$

因此，

$$\begin{aligned}\dim C(X, N, D, t_D, \Theta(\gamma_D)) =& M - \dim H^0(X, L) - \dim H^0(X, L(-D))\\ =& C^{\perp_H}.\end{aligned}$$

至此，证明完成。 □

6. 块与汉明距离。经由局部参数的设计

在本节其余部分，我们固定一条定义在有限域 $\mathbb{F}_q$ 上、亏格为 g 的光滑射影曲线 X，一个可逆层 L，以及一个属于 X的有效除子 $D = n_1p_1 + \cdots + n_sp_s$。考虑线性映射

$$H^0(\Theta_D) \;:=\; H^0(X, L) \to H^0(X, L|_D) = \bigoplus_{i=1}^{s} L_{p_i}/\mathfrak{m}_{p_i}^{n_i} L_{p_i}$$

由典范满射诱导的 $L \twoheadrightarrow L|_D$ （回顾定义 3.1）。对于局部参数与平凡化的一种选取 (t_D, γ_D)，我们有一个相伴的泰勒平凡化

$$\overline{\gamma} : H^0(X, L|_D) \simeq \mathbb{F}_q^M,$$

由此得到微分 Goppa 码（定义 3.4）

$$C(X, L, D, t_D, \gamma_D) = \mathrm{Im}(\mathrm{ev}_{t_D,\gamma_D}) \subseteq \mathbb{F}_q^M.$$

根据引理3.6，$\mathrm{ev}_{t_D,\gamma_D}$ 的核为 $H^0(X, L(-D))$，因此

$$k := \dim_{\mathbb{F}_q} C(X, L, D, t_D, \gamma_D) = \ell(L) - \ell(L(-D)),$$

与 (t_D, γ_D) 无关。虽然微分 Goppa 码的长度与维数不依赖于所选的 (t_D, γ_D)，但对最小汉明距离而言则不再如此。本节旨在阐明最小汉明距离对局部数据 (t_D, γ_D) 变化的依赖关系。

6.1. 块距离的定义与基本性质。 空间 $H^0(X,\ L|_D) \simeq \bigoplus_{i=1}^{s} L_{p_i}/\mathfrak{m}_{p_i}^{n_i} L_{p_i}$ 有一个自然分解，分解为s 个直和项，每一项对应 Supp(D) 中的一个点。这引出了“块支撑”的规范概念，它不依赖于任何坐标的选取。

定义 6.1。 设 $V := \bigoplus_{i=1}^{s} V_i$ 是 $\mathbb{F}_q$–向量空间的直和。对于$v = (v_1,\ \ldots,\ v_s) \in V$，我们将 v的块重量定义为

$$\mathrm{wt}_{\mathrm{blk}}(v) := \#\{\, i :\ v_i \neq 0 \,\}.$$

我们在 V 上定义块距离为

$$d_{\mathrm{blk}}(v, w) := \mathrm{wt}_{\mathrm{blk}}(v - w).$$

引理 6.2。 函数 d_{blk} 是 V上的度量。

证明。 对称性和正定性显然。此外，$d_{\mathrm{blk}}(v,\ w) = 0$ 当且仅当 $v - w = 0$，也就是说 $v = w$。为证明三角不等式，固定 $u,\ v,\ w \in V$。由于 $(u - w)_i = (u - v)_i + (v - w)_i$，条件 $(u - w)_i \neq 0$ 意味着 $(u - v)_i \neq 0$ 或 $(v - w)_i \neq 0$。因此，

$$\{i :\ (u - w)_i \neq 0\} \subseteq \{i :\ (u - v)_i \neq 0\} \cup \{i :\ (v - w)_i \neq 0\}.$$

取基数可得 $d_{\mathrm{blk}}(u, w) \leq d_{\mathrm{blk}}(u, v) + d_{\mathrm{blk}}(v, w)$。 □

定义 6.3。 设 $M \in \mathbb{N}$ 为一个自然数，$M = \sum_{i=1}^{s} n_i$ 为一个分解。考虑 $\mathbb{F}_q^M$上与分解 $\mathbb{F}_q^M = \oplus_{i=1}^{s} \mathbb{F}_q$相关联的块距离。线性码 $C \subset \mathbb{F}_q^M$的块距离定义为

$$d_{\mathrm{blk}}(C) \;:=\; \min\bigl\{\mathrm{wt}_{\mathrm{blk}}(c) :\ c \in C\bigr\}.$$

注 6.4。由定理 3.10，泰勒数据的变化通过可逆变换逐块作用。因此，给定一个微分 Goppa 码$C(X, L, D)$ $t_D, \gamma_D)$ $\subset \mathbb{F}_q^M$，量 $d_{\mathrm{blk}}(C(X, L, D)$ $t_D, \gamma_D))$ 仅取决于 (X, L, D)，即它与用于将 $H^0(X, L|_D)$ 识别为 $\mathbb{F}_q^M$ 的所有选择 $(t_D,$ $\gamma_D)$ 无关。因此，自然可以使用记号

$$d_{\mathrm{blk}}(X, L, D)$$

而不是 $d_{\mathrm{blk}}(C(X, L, D)$ $t_D, \gamma_D))$.

引理 6.5. 对于每一个选择 (t_D, γ_D)，$C(X, L, D, t_D, \gamma_D)$ 的汉明距离 d_H $\subseteq \mathbb{F}_q^M$满足

$$d_{\mathrm{blk}}(X, L, D) \le d_H\big(C(X, L, D, t_D, \gamma_D)\big) \le n\, d_{\mathrm{blk}}(X, L, D)$$

其中 $n{:=}\max_i\{n_i\}$。

证明。 固定 $0 \neq c \in C(X, L, D, t_D, \gamma_D)$，并令 $\tilde{c} := \overline{\gamma}^{-1}(c) \in H^0(X, L|_D)$。若 $\tilde{c}$ 有 r 个非零块，则在所选识别下，每一个这样的块都是 $\mathbb{F}_q^{n_i}$中的非零向量。因此，它对 c至少贡献一个非零坐标。故 $\mathrm{wt}_H(c) \ge r = \mathrm{wt}_{\mathrm{blk}}(\tilde{c})$，取最小值即得$d_H \ge d_{\mathrm{blk}}$。对于第二个不等式，若 $\tilde{c}$有 r 个非零块，则 c 的支撑包含于这些块的并集中，其总大小至多为$\sum_{j=1}^{r} n_{i_j} \le r\, n$。故 $\mathrm{wt}_H(c)$ $\le n\, \mathrm{wt}_{\mathrm{blk}}(\tilde{c})$，取最小值即得结论。□

注 6.6. 假设 $n_1 = \cdots = n_s = n$。赋予 $\mathbb{F}_q^{sn} = (\mathbb{F}_q^n)^s$ 块 Rosenbloom–Tsfasman 权重（见 [5, 7, 25, 26]）

$$\mathrm{wt}_{RT}\big((v^{(1)}, \ldots, v^{(s)})\big) := \sum_{i=1}^{s} \rho\big(v^{(i)}\big),$$

其中，对于任意 $w \in \mathbb{F}_q^n$，我们定义

$$\rho(w) = \begin{cases} 0, & w = 0, \\ \max\{j :\ w_j \neq 0\}, & w \neq 0. \end{cases}$$

于是，对于所有 $w \neq 0$，均有 $\rho(w) \ge 1$，因此对于所有 v，$\mathrm{wt}_{RT}(v) \ge \mathrm{wt}_{\mathrm{blk}}(v)$。特别地，

$$d_{RT}\big(C(X, L, D, t_D, \gamma_D)\big) \ \ge\ d_{\mathrm{blk}}(X, L, D),$$

对于每一种选择 (t_D, γ_D)，其中 d_{RT} 表示关于 Rosenbloom–Tsfasman 权重的距离。

注 6.7. 假设 $n_1 = \cdots = n_s = n$，并通过将每个点处的 n 个坐标分组为第i 行，将 $\mathbb{F}_q^{sn}$与矩阵空间 $\mathrm{Mat}_{s\times n}(\mathbb{F}_q)$ 等同。这样，任意 $c \in C(X, L, D, t_D,$ $\gamma_D)$ 都可以视为矩阵$A_c \in \mathrm{Mat}_{s\times n}(\mathbb{F}_q)$。于是秩权重定义如下（见 [6]）

$$\mathrm{wt}_{\mathrm{rk}}(c) = \mathrm{rank}(A_c).$$

由定理 3.10 可知，$\mathrm{wt}_{\mathrm{rk}}(c)$ 不依赖于 (t_D, γ_D) 的具体选择，因此我们将使用记号 $d_{rk}(X, L, D)$，而不是 $d_{rk}\big(C(X, L, D, t_D, \gamma_D)\big)$。另一方面，显然对于任意矩阵$A \in \mathrm{Mat}_{s\times n}(\mathbb{F}_q)$，我们有

$$\mathrm{wt}_{\mathrm{rk}}(A) \le \#\{\text{nonzero rows of } A\} = \mathrm{wt}_{\mathrm{blk}}(A).$$

因此，对于每一种选择 $(t_D,\ \gamma_D)$，都有

$$d_{rk}(X,L,D) \le\ d_{\mathrm{blk}}(X,L,D),$$
$$d_{rk}(X,L,D) \le \min\{s,n\},$$

其中 d_{rk} 是相对于秩权重的距离。

6.2. 可达性 d_{blk} 及其显式构造。本小节证明，通过改变 $L|_D$的泰勒平凡化，所能得到的最小汉明距离就是块距离。事实上，我们给出一种构造性方法，以求得产生块距离的局部数据（$t_D,\ \gamma_D$）。

引理 6.8。设 $p \in X$ 是一个有理点，t 是 p处的局部参数，$\gamma:\ L_p \simeq O_p$ 是一个平凡化。固定 $n \ge 1$，并设 $s \in H^0(X,L)$ 满足$\gamma(s)(t) \neq 0$模 t^n。令 $m:=$最小值 $\{l \in \{0,\dots,n-1\}|\ D_t^l(\gamma(s)) \neq 0\}$。那么，存在 $f \in O_p^\times$使得 $\gamma':=f\gamma$ 且满足

$$\gamma'(s)(t) = t^m \pmod{t^n}.$$

等价地，$\left(D_t^0(\gamma'(s)) \dots, D_t^{n-1}(\gamma'(s))\right) =(0,\dots,0,1,0,\dots,0)$，其中1 位于位置 m。

证明。令 $v:=\ \left(D_t^0(\gamma(s)) \dots, D_t^{n-1}(\gamma(s))\right) \in \mathbb{F}_q^n$，且 $m:=$最小值$\{\ell \in \{0,\dots,n-1\} \mid v_\ell \neq 0\}$。由引理 3.9，对于每个 $f \in O_p^\times$以及 $\gamma':=f\gamma$，有

$$\left(D_t^0(\gamma'(s)),\dots,D_t^{n-1}(\gamma'(s))\right) = v\,S_p(f), \tag{6.1}$$

其中 $S_p(f) \in \mathrm{Gl}_n(\mathbb{F}_q)$ 是下三角矩阵，其元素为 $(S_p(f))_{i,\ j} = D_t^{i-j}(f)$，其中 $j \le i$。现在，对于任意 $f \in O_p^\times$，我们可以写成 $f(t) = \sum_{r=0}^{n-1} b_r t^r$ (模 t^n)，其中 $b_0 \neq 0$。于是 $D_t^r(f) = b_r$对于 $0 \le r \le n-1$，因此 $S_p(f)$ 由 $b_0,\dots,b_{n-1}$确定。令 $w:=vS_p(f) =(w_0,\dots,w_{n-1})$。直接相乘可得，对于每个 k，$w_k = \sum_{i=k}^{n-1} v_i\, b_{i-k}$。由于 $v_0 = \cdots = v_{m-1} = 0$，我们有$w_k = 0$ 对于 $k < m$。因此，条件 $w = e_m$ 等价于以下方程组

$$w_m = 1, \qquad w_{m+1} = w_{m+2} = \cdots = w_{n-1} = 0. \tag{6.2}$$

令 $r:= n-1-m$，并考虑不定元 b_0、……、b_r（注意，w_k 仅涉及 b_0、……、b_{n-1-k}）。对于 $u = 0$、……、r（即 $k = m+u$），我们有 $w_{m+u} = \sum_{j=0}^{r-u} v_{m+u+j}\, b_j$。这给出了关于变量 b_0、……、b_r 的上三角线性方程组：

$$\begin{pmatrix} w_m \\ w_{m+1} \\ \vdots \\ w_{n-2} \\ w_{n-1} \end{pmatrix} = \begin{pmatrix} v_m & v_{m+1} & \cdots & v_{n-2} & v_{n-1} \\ 0 & v_m & \cdots & v_{n-3} & v_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & v_m & v_{m+1} \\ 0 & 0 & \cdots & 0 & v_m \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{r-1} \\ b_r \end{pmatrix},\ r = n-1-m.$$

由于 $v_m \neq 0$，该系统存在一个解 $(b_0,\dots,b_r) \in \mathbb{F}_q^{r+1}$，满足 $b_0 \neq 0$。现在，任取一个提升 $f \in O_p^\times$，使其在 p 处关于 t的泰勒展开与上述系数模 t^n 同余。于是，由 (6.1) 和 (6.2) 得到$vS_p(f) = e_m$，即 $\left(D_t^0(\gamma'(s)) \dots, D_t^{n-1}(\gamma'(s))\right) = e_m$。最后，根据 D_t^ℓ的定义，这等价于 $\gamma'(s)(t) = t^m$ (模 t^n)。□

定理 6.9。 存在平凡化 $\gamma'_D = (\gamma'_1, \dots, \gamma'_s)$（固定了一致化子），使得

$$d_H\big(C(X, L, D, t_D, \gamma'_D)\big) = d_{\mathrm{blk}}(X, L, D).$$

也就是说，通过改变(t_D, γ_D) 所能达到的最小汉明距离恰好为 $d_{\mathrm{blk}}(X, L, D)$。

证明。固定局部参数 t_D 以及截面 $s_0 \in H^0(X, L) \setminus H^0(X, L(-D))$，使得$\mathrm{wt}_{\mathrm{blk}}(\mathrm{ev}_{t_D,\gamma_D}(s_0)) = d_{\mathrm{blk}}(X, L, D)$。设 $S \subseteq \{1, \dots, s\}$ 为指标集 i，使得$\mathrm{ev}_{t_D,\gamma_D}(s_0)$ 的第 i块非零。于是$|S| = d_{\mathrm{blk}}(X, L, D)$，并且对 $i \notin S$我们有 $\gamma_i(s_0) \in \mathfrak{m}_{p_i}^{n_i}$。对每个 $i \in S$，在 p_i 处对 $n = n_i$ 应用引理 6.8，以找到单位元 $f_i \in O_p^\times$，使得新的平凡化$\gamma'_i := f_i \gamma_i$ 满足$(D_{t_i}^0(\gamma'_i(s_0)) \dots, D_{t_i}^{n_i-1}(\gamma'_i(s_0))) = e_{m_i}$，其中 e_{m_i} 是$\mathbb{F}_q^{n_i}$ 中的一个标准基向量。对 $i \notin S$，令$\gamma'_i := \gamma_i$。考虑该码

$$C' := C(X, L, D, t_D, \gamma'_D).$$

码字 $c'_0 := ev_{t_D,\gamma'_D}(s_0) \in C'$ 在由 S索引的每个块中恰好有一个非零坐标，且在块 $i \notin S$ 上为零。因此 $\mathrm{wt}_H(c'_0) = |S| = d_{\mathrm{blk}}(X, L, D)$，从而推出 $d_H(C') \le d_{\mathrm{blk}}(X, L, D)$。另一方面，引理 6.5 给出 $d_H(C') \ge d_{\mathrm{blk}}(X, L, D)$。故等式成立。 □

6.3. 满足 $d_H \ge d$ 的参数的存在性。 我们现在讨论如下设计问题：给定几何数据 (X, L, D) 与自然数 d，我们希望确定能保证存在泰勒平凡化 (t_D, γ_D) 的条件，使得所得微分 Goppa 码满足 $d_H \ge d$。

由辛格尔顿界，一个必要条件是 $d \le M - k + 1$。此外，引理 6.5 表明 $d \ge d_{\mathrm{blk}}(X, L, D)$ 是在此框架内可达到的最小距离的一个自然下界。因此，d必须满足

$$d_{\mathrm{blk}}(X, L, D) \le d \le M - k + 1.$$

回顾定义 3.11，泰勒群 $G_n(p)$作用于局部参数集合上。在本小节中，我们通过固定局部参数 $t_D = (t_1, \dots, t_s)$ 并仅允许平凡化变化，来简化搜索空间。这要求我们研究初始选择 γ_D 在局部重标度子群作用下的轨道：

$$\prod_{i=1}^{s} (J_{p_i}^{n_i})^\times \subset \prod_{i=1}^{s} G_{n_i}(p_i).$$

由于 $(J_p^n)^\times$ 通过下三角矩阵 $S_p(f)$ 在线性作用于喷射空间上（见引理 3.16），这一限制使我们能够将码参数视为仿射簇中的坐标。

定义 6.10. 对于每个点 $p_i \in \mathrm{Supp}(D)$，令 U_{n_i} 为参数化 n_i 阶喷射 $J_{p_i}^{n_i}$ 的单位群的簇：

$$U_{n_i} := \big\{ (b_{i,0}, \dots, b_{i,n_i-1}) \in \mathbb{F}_q^{n_i} : b_{i,0} \neq 0 \big\}. \tag{6.3}$$

我们将平凡化的参数空间定义为乘积簇：

$$\mathcal{P} := \prod_{i=1}^{s} U_{n_i}, \quad \dim \mathcal{P} = \sum_{i=1}^{s} n_i = M.$$

注 6.11. 注意，任意元素 $f_i \in U_{n_i}$ 定义一个单位元 $f_i(t_i) \equiv \sum_{j=0}^{n_i-1} b_{i,j} t_i^j \pmod{t_i^{n_i}}$。

给定初始平凡化 γ_D 与点 $f = (f_1, \ldots, f_s) \in \mathcal{P}$，我们用 $\gamma_D(f)$ 表示由单位元的作用得到的平凡化，即 $\gamma_i(f) := f_i \cdot \gamma_i$。下述引理表明，平凡化的所有变化均以这种方式产生。

引理 6.12. 固定局部参数 $t_D = (t_1, \ldots, t_s)$。设 T_D 为仿射簇 $\prod_{i=1}^{s} \mathrm{Iso}^{t_i}_{\mathrm{Tay}(J^{n_i}_{p_i}(L))\mathbb{F}_q^{n_i}}$。则对任意固定的 $\gamma_D \in T_D$，映射 $\widehat{\Psi}$ 由 Ψ 诱导（见 3.10）

$$\begin{aligned} \widehat{\Psi}_{\gamma_D} : \mathcal{P} &\longrightarrow T_D \\ f = (f_1, \ldots, f_s) &\longmapsto \gamma_D(f) = (f_1\gamma_1, \ldots, f_s\gamma_s) \end{aligned}$$

是仿射簇之间的同构。特别地，任意一组平凡化都由缩放子群对一组固定初始平凡化的作用唯一确定。

证明。双射性由命题 3.20（单传递群作用的轨道映射是双射）可知。另一方面，由注 3.12 和注 3.52）容易得出，该双射是仿射簇之间的同构。□

固定 $\mathrm{Im}(H^0(\Theta)) \subseteq H^0(X, L|_D)$ 的一组基 $s_1, \ldots, s_k$，并考虑使用固定局部参数 t_D和平凡化 γ_D, $C := C(X, L, D, t_D, \gamma_D) \subset \mathbb{F}_q^M$ 得到的相应微分 Goppa 码。现在，对每个 $f \in \mathcal{P}$，通过使用平凡化 $\gamma_D(f)$ 得到一个新码，我们将其记为$C(f)$。

引理 6.13。 若 G 是 C 的生成矩阵，则 $G(f) := GS(f)$ 是 $C(f)$ 的生成矩阵。这里，$S(f) \in \mathrm{Gl}_M(\mathbb{F}_q)$ 是分块对角矩阵

$$S(f) = \mathrm{diag}\left(S_{p_1}(\overline{f}_1), \ldots, S_{p_s}(\overline{f}_s)\right),$$

且每个块 $S_{p_i}(f_i)^- \in \mathrm{Gl}_{n_i}(\mathbb{F}_q)$ 都是引理 3.16中给出的下三角矩阵。特别地，生成矩阵 $G(f)$ 的每个元素都是参数空间中关于变量 $b_{i,j}$ 的正则函数（实际上是线性形式）。

证明。G 中的条目对应于 $\{s_1, \ldots, s_k\}$ 在初始平凡化 γ_D下的泰勒展开的系数。根据引理 6.12，新码 $C(f)$通过对$f = (f_1, \ldots, f_s) \in \mathcal{P}$, $\gamma_D(f) = (f_1\gamma_1, \ldots, f_s\gamma_s)$施加缩放作用得到。在 $\mathbb{F}_q^{n_i}$中，乘以 f_i 由 $S_{p_i}(f_i) \in \mathrm{GL}_{n_i}(\mathbb{F}_q)$ 表示。因此，新的生成矩阵为：

$$G(f) = G \cdot \mathrm{diag}\left(S_{p_1}(\overline{f}_1), \ldots, S_{p_s}(\overline{f}_s)\right) = GS(f).$$

最后，请注意，矩阵 $S_{p_i}(f_i)$的条目是系数$b_{i,j}$的线性组合。由于 $G(f) = GS(f)$， $G(f)$的每个条目也是系数$b_{i,j}$ 上的线性形式。□

引理 6.14. 设 $C(f) \subseteq \mathbb{F}_q^M$是由 $G(f)$生成的码。那么$d_H(C(f)) \geq d$当且仅当，对于每个满足$|J| = M - d + 1$的子集 $J \subseteq \{1, \ldots, M\}$，将列限制在 J上得到的子矩阵 $G(f)_J$的秩为 k。等价地，对于每个这样的 J，矩阵 $G(f)_J$ 至少存在一个非零的 $k \times k$ 子式。

证明。 这是经典的刻画 □

定理 6.15. 固定 (X, L, D) 以及满足 $1 \leq d \leq M - k + 1$ 的 $d \in \mathbb{N}$。那么存在一个常数 $\Delta = \Delta(M, k, d)$ ，使得若 $q > \Delta$ ，则以下结论成立：如果存在一个扩域 $\mathbb{F}_{q^m}$ 以及参数 $f^\star \in \mathcal{P}(\mathbb{F}_{q^m})$使得

$$d_H\big(C(X, L, D, t_D, \gamma_D(f^\star))\big) \geq d,$$

那么，存在满足条件的 $f \in \mathcal{P}(\mathbb{F}_q)$

$$d_H\big(C(X, L, D, t_D, \gamma_D(f))\big) \geq d.$$

证明。由引理 6.13， $G(f)$ 的每个元素都是参数空间 $\mathcal{P}$ 上的正则函数（实际上是线性形式）。由引理 6.14，条件 $d_H(C(f)) \geq d$ 等价于对每个满足 $|J| = M - d + 1$ 的子集 $J \subseteq \{1, \ldots, M\}$，都有 $\mathrm{wt}_{\mathrm{rk}}(G(f)_J) = k$。根据假设，存在$f^\star \in \mathcal{P}(\mathbb{F}_{q^m})$使得该条件成立。因此，对每个 J，至少存在一个 $G(f^\star)_J$ 的非零 $k \times k$ 子式。令 $P_J(f)$ 表示这样的子式；它是一个次数至多为 k 且含有 M 个变量的多项式。我们定义

$$P(f) := \prod_{J:\ |J| = M - d + 1} P_J(f) \in \mathbb{F}_q[b_{i,j}].$$

根据构造， $P(f^\star) \neq 0$，因此 $P \neq 0$。其总次数有如下界：

$$\deg(P) \leq k \cdot \binom{M}{M - d + 1} = k \cdot \binom{M}{d - 1} =: \Delta(M, k, d).$$

根据 Schwartz–Zippel 引理（应用于 P），$\mathbb{F}_q^M$中 P 的零点数至多为 Δq^{M-1}。若 $q > \Delta$，则 $\Delta q^{M-1} < q^M$，从而保证存在$f \in \mathbb{F}_q^M$使得 $P(f) \neq 0$。最后请注意，条件 $P(f) \neq 0$已经蕴含 $b_{i,\,0} \neq 0$对所有 i 都成立（否则，$G(f)$中对应的列将为零，这与子式的满秩相矛盾）。因此， f必然属于 $\mathcal{P}(\mathbb{F}_q)$，并且码 $C(f)$满足 $d_H(C(f)) \geq d$。□

注 6.16。 定理 6.15表明，由 $\mathcal{P}$ 中的 $d_H \geq d$ 定义的扎里斯基开子集，只要非空且基域足够大，就含有一个有理点。这里给出的界 $\Delta(M,\ k,\ d)$ 显然较为粗略；出于实际应用的考虑，进一步改进它将很有意义。

7. 两个基本结果

在最后一节中，我们给出两个突显微分 Goppa 码重要性的基本结果。首先，我们证明，任意线性分组码都可以在一条射影曲线上实现为微分 Goppa 码。

其次，我们证明，强几何 Goppa 码（文献中通常称为 SAG 码）构成强微分 Goppa 码的一个真子类。这些结果共同突显了我们方法的一项关键优势：即使所研究的曲线只有很少的点，也能够构造长度较大的类戈帕码，而且不受基域大小的限制。

7.1. **每个线性分组码都是微分 Goppa 码**。Pellikaan、Shen 和 van Wee 表明，每个线性码都可以通过戈帕构造从一条曲线上得到，从而将任意线性码纳入几何框架 [22]。另一方面，在卷积码的背景下也已给出了相关的实现结果[14]。下述定理可视为这一思想在 $\mathbb{P}^1$上的单点情形的微分形式对应版本。

定理 *7.1.* 每个线性码 C（定义在 $\mathbb{F}_q$ 上）都可以表示为微分 *Goppa* 码 $C = C(\mathbb{P}^1, L, D, \Gamma, t_D, \gamma_D)$，其中 $C(\mathbb{P}^1, L, D, t_D, \gamma_D)$ 如 *§4.1.1* 所述，且 $\Gamma \subset H^0(\mathbb{P}^1, L)$ 是一个合适的向量子空间。

证明。设 $C \subseteq \mathbb{F}_q^n$ 是维数为 k的线性码。设 $p_\infty \in \mathbb{P}^1$ 为无穷远点。令 $L := O_{\mathbb{P}^1}(n-1)$且 $D := n\,p_\infty$。选择p_∞ 处的局部参数 t 以及平凡化 γ，如 §4.1.1的单点构造中所述。如单点微分戈帕构造中所示，$\mathrm{ev}_{t_D,\gamma_D}\colon H^0(\mathbb{P}^1, L) \longrightarrow \mathbb{F}_q^n$ 是一个同构（ §4.1.1 ）。现在，定义

$$\Gamma := \mathrm{ev}_{t_D,\gamma_D}^{-1}(C) \subseteq H^0(\mathbb{P}^1, L).$$

我们得到 $C = C(\mathbb{P}^1, L, D, \Gamma, t_D, \gamma_D)$。 □

注 7.2。 **1.** 子空间 $\Gamma \subset H^0(\mathbb{P}^1, L)$可以根据矩阵 $G(p_\infty)$的表达式以及 $C \subset \mathbb{F}_q^n$的一组基（即生成矩阵）显式写出，记作 $\{c_1, \ldots, c_k\}$。经过简单计算可知，$\Gamma := G^{-1}(C) \subset V$的一组基由以下多项式给出

$$f_\ell(t) = \sum_{i=0}^{n-1} c_{\ell,n-i} t^i, \quad \ell = 1, \ldots, k.$$

其中 $c_i = (c_{i,1}, \ldots, c_{i,n})$ 对每个 $i = 1, \ldots, k$。

2. 我们可以用双点情形 §4.1.2中出现的零亏格微分戈帕码来表述上述定理。同样，我们可以明确描述子空间 Γ。容易看出 $G(\alpha)^{-1} = G(-\alpha)$。因此，若 $C \subset \mathbb{F}_q^n$的一个基（即生成矩阵）为 $\{c_1, \ldots, c_k\}$，则 $\Gamma := G^{-1}(C) \subset V$的一个基由下列多项式给出：

$$f_\ell(t) = \sum_{m=1}^{r} \left(\sum_{j=1}^{m} \binom{m-1}{j-1} (-\alpha)^{m-j} c_{\ell,j} \right) t^{m-1}, \quad \ell = 1, \ldots, k.$$

3. 选择 $\mathbb{P}^1$ 仅仅是为了简化。同样的结果也可以在单点情形下的椭圆曲线上表述（见 §4.2.1）。

7.2. **强几何 Goppa 码构成一个真子类。** 定理7.1 表明，若允许使用非完备的微分 Goppa 结构来表示线性码，那么底层几何数据便毫无用处。因此，为了使微分 Goppa 结构直接影响其所表示的码的参数和行为，必须限制所考虑的微分 Goppa 结构在选择时所允许的自由度。

如果微分形式（或几何）Goppa 码 $C := C(X,\ L,\ D,\ t_D,\ \gamma_D)$ 满足$g = g(X)$、 $d = \deg(L)$ 且 $n = \deg(D)$，则称其为强码。如果此时 $H^0(X,\ L(-D)) = H^1(X,\ L) = 0$，则黎曼-罗赫定理可用于计算该码的维数:

$$\dim C = 1 - g + d.$$

强几何 Goppa 码（也称 SAG 码 [22]）因诸多原因而格外引人关注。现在我们将看到，强几何 Goppa 码这一类构成了强微分 Goppa 码的一个真子类。也就是说，存在一些强微分 Goppa 码，无法表示为任意光滑射影曲线上的强几何 Goppa 码。

命题 7.3。 设 q 是一个素数幂，且 n、 $k \in \mathbb{N}$ 满足 $1 \leq k < n$。假设存在一个强几何 *Goppa* 码（按 *Tsfasman–Vlăduţ* 的定义） $C = C(X$、 L、 D、 $\gamma_D)$ 定义在 $\mathbb{F}_q$ 上，使得 X 是亏格为 g的光滑射影曲线， L是 X 上的可逆层，次数为$d := \deg(L)$， $D = p_1 + \cdots + p_n$ 是由 n 个互异有理点组成的和，且维数 $C = k$。令

$$t_q(n) := \max\left\{0,\ \left\lceil \frac{n-(q+1)}{2\sqrt{q}} \right\rceil\right\}.$$

那么必然有 $t_q(n) \leq k \leq n - t_q(n)$。

证明。 由于该码是强码，黎曼–罗赫定理给出 $k = d + 1 - g$，因此$d = k+g-1$。由 $2g-2 < d = k+g-1$ 可得 $g \leq k$。由于 $d = k+g-1 < n$，故有 $g < n-k+1$，因此 $g \leq n-k$。所以

$$g \leq \min(k, n-k).$$

另一方面，由于 D 支撑在 n 个不同的有理点上， $n \leq \#X(\mathbb{F}_q)$。根据哈斯–韦伊界（见 [30, 27, 15]） ，$\#X(\mathbb{F}_q) \leq q+1+2g\sqrt{q}$。因此 $n \leq q+1+2g\sqrt{q}$，所以 $g \geq \left\lceil \frac{n-(q+1)}{2\sqrt{q}} \right\rceil$。由于 g 是整数，

$$g \geq \left\lceil \frac{n-(q+1)}{2\sqrt{q}} \right\rceil.$$

如果这个下界为负，则它没有实际意义，因此有效下界为

$$g \geq t_q(n) := \max\left\{0,\ \left\lceil \frac{n-(q+1)}{2\sqrt{q}} \right\rceil\right\}.$$

将关于 g 的两个不等式结合起来，我们得到 $t_q(n) \leq \min(k, n-k)$，这等价于 $t_q(n) \leq k \leq n - t_q(n)$。 这就证明了该结论。 □

定理 7.4. 设 q 为素数幂，并设

$$t_q(n) := \max\left\{0,\ \left\lceil \frac{n-(q+1)}{2\sqrt{q}} \right\rceil\right\}.$$

设 n、k 为满足 $1 \leq k < n$ 的整数，并假设 $n \geq q + 2 + \lfloor 2\sqrt{q} \rfloor$。若

$$1 \leq k \leq t_q(n) - 1 \qquad or \qquad n - t_q(n) + 1 \leq k \leq n - 1.$$

那么，在 $\mathbb{F}_q$ 上存在一个长度为 n、维数为 k 的强微分 *Goppa* 码，但它不是 $\mathbb{F}_q$ 上的强几何 *Goppa* 码。

特别地，对于每个有限域 $\mathbb{F}_q$，强几何 *Goppa* 码类都是强微分 *Goppa* 码类的真子类。

证明。令 $X = \mathbb{P}^1_{\mathbb{F}_q}$，并令 $p_\infty \in X(\mathbb{F}_q)$ 为无穷远点。令 $d := k - 1$。由于 $1 \leq k < n$，我们有 $0 \leq d < n$。现在考虑由 $L = \mathcal{O}_{\mathbb{P}^1}(d)$ 和 $D = n\,p_\infty$ 定义的单点微分 Goppa 码 $C = C(X,\ L,\ D,\ t_D,\ \gamma_D)$。由于 $g(X) = 0$，强条件为 $-2 < d < n$，而该条件成立。因此，C 是一个强微分 Goppa 码。根据黎曼–罗赫定理，$\dim C = 1 - g + d = 1 + 0 + (k-1) = k$. 因此，$C$ 的长度为 n，维数为 k。

反设 C 是定义在 $\mathbb{F}_q$上的强几何 Goppa 码。由于 C 的长度为 n，维数为 k，命题 7.3 将推出$t_q(n) \leq k \leq n - t_q(n)$。这与关于 k的假设矛盾。因此，C 不是强几何 Goppa 码。

还需证明，对于每个有限域 $\mathbb{F}_q$，至少存在一对 (n, k)，使得定理的假设非空。选取整数 n，使得 $n \geq q + 2 + \lfloor 2\sqrt{q} \rfloor$。于是 $t_q(n) \geq 2$。特别地，$1 \leq t_q(n) - 1$，因此所选的 $k = 1$ 满足 $1 \leq k \leq t_q(n) - 1$。由此，数对 $(n, 1)$ 属于定理所涵盖的范围。现在将证明的第一部分应用于这个特定数对 $(n, 1)$。在 $\mathbb{P}^1_{\mathbb{F}_q}$ 上的构造给出一个长度为 n、维数为 1 的强微分 Goppa 码。根据命题 7.3 中的数值障碍，定义在 $\mathbb{F}_q$ 上的强几何 Goppa 码不可能具有这些参数。因此，这个码不是强几何 Goppa 码。由此可知，对于每个 $\mathbb{F}_q$，都存在一个不是强几何 Goppa 码的强微分 Goppa 码。□

附录 A. 射流、高阶导子与微分学

在本附录中，X 表示域 $\mathbb{F}_q$上的光滑射影曲线。这里给出的大多数构造和结果对一般的分离概形仍然成立，可能只需稍作修改。尽管关于射流丛的标准参考文献是 [10]，，但本附录中的所有结果都可以通过某种方式在 [18, 19, 20, 23, 24] 中找到。

设 X 是域 $\mathbb{F}_q$上的光滑射影曲线。对角线嵌入 $\Delta\colon X \hookrightarrow X \times X$ 是闭的，我们将 I 记为 $X \times X$中 X 的理想。令 $\pi_1,\ \pi_2\colon X \times X \to X$ 分别为到第一因子和第二因子的投影。

A.1. **平凡情形。有理函数。**

定义 A.1. 设 X 是域 $\mathbb{F}_q$上的光滑射影曲线。对于每个自然数 $i \in \mathbb{N}$，X 的 i 阶喷射层是环层

$$J^i_X = \pi_{1*}\left(O_{X\times X}/I^{i+1}\right).$$

层 J_X^i具有两种不同的 O_X-模（因此也是 O_X-代数）结构。回顾一下，对于 $l = 1, 2$，概形结构态射 π_l在 X上诱导出一个环层同态，记作 $\pi_l^\sharp$：$O_X \to \pi_{l*}O_{X\times X}$。

1. 考虑 $\pi_1^\sharp$ 与商映射 q 的推前的复合：$O_{X\times X} \to O_{X\times X}/I^{i+1}$:

$$\iota_X^i : O_X \xrightarrow{\pi_1^\sharp} \pi_{1*}O_{X\times X} \xrightarrow{\pi_{1*}(q)} \pi_{1*}(O_{X\times X}/I^{i+1}) = J_X^i.$$

这个环同态 ι_X^i 定义了第一个 O_X-模结构（标准向量丛结构）。局部而言，它将 $f \mapsto f \otimes 1$ 映射为（模 I^{i+1}）。

2. 类似地，我们有映射 $\pi_2^\sharp$： $O_X \to \pi_{2*}O_{X\times X}$。由于层$O_{X\times X}/I^{i+1}$ 支撑在对角线 $\Delta(X)$ 上，且 $\pi_1|_{\Delta(X)} = \pi_2|_{\Delta(X)}$，因此存在层环的典范同构 ϕ：$\pi_{2*}(O_{X\times X}/I^{i+1}) \xrightarrow{\sim} \pi_{1*}(O_{X\times X}/I^{i+1})$。我们将第二个映射 d^i 定义为以下复合:

$$d_X^i : O_X \xrightarrow{\pi_2^\sharp} \pi_{2*}O_{X\times X} \xrightarrow{\pi_{2*}(q)} \pi_{2*}(O_{X\times X}/I^{i+1}) \xrightarrow{\phi} J_X^i.$$

局部上，它将 $f \mapsto 1 \otimes f$（模 I^{i+1}）映射到.....，并定义第二个作用。映射 d_X^i 是 $\mathbb{F}_q$-代数的态射。
我们始终考虑由 ι_X^i给出的 J_X^i上的 O_X-代数结构。

A.1.1. 基本性质。 现在假设 X 是 $\mathbb{F}_q$上的光滑射影曲线。层 J_X^i 具有以下基本性质:

1. 对每个 $i \in \mathbb{N}$，都有一个 O_X-模的典范短正合列，

$$0 \to \omega_X^{\otimes i} \to J_X^i \to J_X^{i-1} \to 0.$$

2. 如果 $U \subset X$是一个开子集，那么 $J_X^i|_U \simeq J_U^i$典范地成立。
3. 如果 $x \in X$是一个有理点，那么 $J_X^i|_x \simeq O_{X,\,x}/\mathfrak{m}^{i+1}O_{X,\,x}$典范地成立。**4.** 如果 $U =$Spec(A) 是一个仿射开子集，那么

$$J_X^i|_U = (A \otimes_k A)/I_U^{i+1} \simeq O_U^{i+1}, \quad I_U := \mathrm{Ker}(A \otimes_k A \to A),$$

非典范地。 $J_X^i|_U$的一组基可按如下方式求得。令 $z \in A$为 $\omega_X|_U = I_U/I_U^2$ 的一个生成元。记作 $\delta_X^i = d_X^i - \iota_X^i$。定义

$$\xi := \delta_U^i(z) = (z \otimes 1 - 1 \otimes z) \pmod{I^{i+1}} \in J_X^i|_U.$$

那么， $\{1, \xi, \xi^2, \ldots, \xi^i\}$是 $J_X^i|_U$作为 O_X-模的一组基。

注 A.2。 对于一个有理点 $p \in U$，纤维 $J_p^n =$(J_X^n)_p \otimes_{O_{X,\,p}} k(p)是通过在 p 处对第一个因子求值得到的，因此 ξ 映射到 $z(p) - z =$–$(z - z(p))$ $\in \mathfrak{m}_p/\mathfrak{m}_p^{n+1}$。由于 $dz(p) \neq 0$，元素 $t := z - z(p)$ 是 p的一个局部参数，而基 $\{1, \xi, \xi^2, \ldots, \xi^i\}$ 特化为基$\{1, t, \ldots, t^n\}$（相差一个符号）的 J_p^n。

A.1.2. 通过射流得到有理函数的高阶导数与泰勒展开。设 $\mathbb{F}_q$ 为一个环，设 A 与 B $\mathbb{F}_q$-代数，以及 $m \in \mathbb{N} \cup \{\infty\}$。

定义 A.3. 从 A 到 B、关于 $\mathbb{F}_q$、阶为 m 的高阶导子是一个序列（$D_0, \ldots,$ D_m），其中 D_0: $A \to B$ 是一个 $\mathbb{F}_q$-代数同态

并且 $D_1, \ldots, D_m$: $A \to B$ 是 $\mathbb{F}_q$-模同态，使得对于所有 $x, y \in A$ 以及所有 $l = 0, \ldots, m$:

$$D_l(xy) = \sum_{i+j=l} D_i(x) D_j(y) \quad \text{(Leibniz rule)} . \tag{A.1}$$

我们用 $\mathbf{Der}_k^m(A, B)$ 表示从 A 到 B 的 m 阶高阶导子集合。

线性映射 d_X^i 与曲线上函数的高阶导子有着密切联系，具体如下。我们只考虑光滑射影曲线 X 的仿射开子集 $U = \mathbf{Spec}(A)$，并选取 $z \in A$，使得 $\xi := \delta_U^i(z)$ 生成 $\omega_X|_U$。那么，给定 $a \in A$，有

$$d_U^i(a) = D_{U,z}^0(a) + D_{U,z}^1(a)\xi + \cdots + D_{U,z}^i(a)\xi^i$$

其中

$$D_{U,z}^j(a) = \left[\begin{array}{l} j\text{-th coefficient of } d_U^i(a) \\ \text{in the basis } \{1, \xi, \ldots, \xi^i\} \end{array} \right]. \tag{A.2}$$

由于 d_U^i 是一个 $\mathbb{F}_q$-代数同态，因此每个 $D_{U,\,z}^j$ 都确定一个映射 $D_{U,\,z}^j$: $A \to A$，该映射是 $\mathbb{F}_q$-线性的，并且满足

$$D_{U,z}^j(ab) = \sum_{l=0}^{j} D_{U,z}^l(a)\, D_{U,z}^{j-l}(b), \qquad j = 0, \ldots, i.$$

也就是说，$(D_{U,\,z}^0, \ldots, D_{U,\,z}^i) \in \mathbf{Der}_k^i(A, A)$。有一个重要事实值得强调：上述每个 $D_{U,\,z}^j$ 都是 Grothendieck 意义下的微分算子；也就是说，每个 $D_{U,\,z}^j$: $A \to A$ 都等于 $pr_j \circ d_U^i$，其中 pr_j: $J_U^i \to A$ 是到第 j 个因子的投影。特别地，$D_{U,\,z}^1$ 是一个普通导子。

最后请注意，典范满射 $J_X^i \to J_X^{i-1}$确定了一个射影系统，因此我们可以定义

$$J_X^\infty := \varprojlim_i J_X^i.$$

典范映射 d_X^i 诱导出一个映射

$$d_X^\infty : O_X \to J_X^\infty$$

它可由完整的泰勒序列局部描述。更准确地说，给定一个仿射开子集 $U = \mathbf{Spec}(A)$ 和 $z \in A$，使得 $\xi := \delta_U^i(z)$ 生成$\omega_X|_U$，则

$$d_U^\infty(a) = D_{U,z}^0(a) + D_{U,z}^1(a)\xi + \cdots + D_{U,z}^i(a)\xi^i + \cdots$$

A.1.3. 与经典泰勒展开的比较。关于函数域中泰勒展开的详细论述，请参阅 [27, §4。2] 。

设 x: $K \to \mathbb{Z} \cup \{\infty\}$ 是一个离散 $\mathbb{F}_q$-赋值，而 $O_x \subset K$ 是相应的离散赋值环。$\mathfrak{m}_x$-进完备化定义为

$$\widehat{O}_x := \varprojlim_n O_x/\mathfrak{m}_x^n$$

$\widehat{}$显然， O_x-模的典范态射 $O_x \to O_x$ 是单射。因此，它们的分式域之间诱导的态射

$$\wr_{t_x} : K \hookrightarrow K_x$$

它也是单射。给定 x 处的一个参数 $t_x \in \mathfrak{m}_x \setminus \mathfrak{m}_x^2$，众所周知， $K_x \simeq \mathbb{F}_q((t_x))$。因此，给定 $f \in K$，我们将 f 在 x 处相对于 t_x 的 Laurent 展开定义为

$$f(t_x) := \wr_{t_x}(f) = \sum_{n \in \mathbb{Z}} f_n t_x^n \in \mathbb{F}_q((t_x)). \tag{A.3}$$

容易看出， f 在 x 处的阶满足：

$$\mathrm{ord}_x(f) = \min\{n \in \mathbb{N} |\ f_n \neq 0\}$$

若 f 在 x 处正则，即 $f \in O_x$，则

$$f(t_x) = \sum_{n=0}^{\infty} f_n t_x^n \in \mathbb{F}_q[[t_x]]^{1}$$

我们将 f 在 x 处相对于 t_x 的 n 阶导数定义为

$$D_{t_x}^n(f) := f_n. \tag{A.4}$$

为证明此定义的合理性，注意到 $\wr_{t_x}$ 是 $\mathbb{F}_q$-代数的态射，因此有

1. $D_{t_x}^0(f) = f(x)$ 对所有 $f \in O_x$[2] 均成立。**2.** $D_{t_x}^n(\lambda f + \mu g) = \lambda D_{t_x}^n(f) + \mu D_{t_x}^n(g)$ 对所有 λ， $\mu \in \mathbb{F}_q$ 和 f， $g \in O_x$ 均成立。**3. (Leibniz 法则)** $D_{t_x}^n(fg) = \sum_{i=0}^n D_{t_x}^i(f) D_{t_x}^{n-i}(g)$ 对所有 f， $g \in O_x$ 均成立。

正如我们在 A.1.2 中所见，每个截断元组 $(D_{t_x}^0, D_{t_x}^1, \ldots, D_{t_x}^n)$ 确定一个高阶导子。特别地， $D_{t_x}^1$ 是一个普通导子。我们还将使用经典记法

$$f'(t_x) = D_{t_x}^1(f). \tag{A.5}$$

最后，注意，若 f 在 x 处有一个 n 阶极点，则对于每个 $n \geq i > 0$，我们有

$$a_{-i} = D_{t_x}^{n-i}(t_x^n f) \tag{A.6}$$

A.2. 一般情形。亚纯截面。 设 X 是定义在域 $\mathbb{F}_q$ 上的一条光滑射影曲线。现在考虑 X 上的一个可逆层 L。那么， L 的 i 阶喷射层定义为

$$J_X^i(L) := \pi_{1*}\left(\pi_2^* L \otimes_{O_{X\times X}} O_{X\times X}/I^{i+1}\right). \tag{A.7}$$

这个层自然带有一个关于喷射代数$P_X^i := J_X^i(O_X)$的模结构。因此， P_X^i上的两个 O_X-模结构在 $J_X^i(L)$上诱导出两个相容结构。

---

[1]注意，固定 t_x后，存在典范同构 $\mathbb{F}_q[[t_x]]/t_x^{i+1} \simeq \bigoplus_{n=0}^i \mathfrak{m}_x^n/\mathfrak{m}_x^{n+1}$，因此存在典范同构 $\mathbb{F}_q[[t_x]] \simeq \lim_{\leftarrow i} \bigoplus_{n=0}^i \mathfrak{m}_x^n/\mathfrak{m}_x^{n+1}$。这可用于计算导数。[2]注意，

O_x $\mathbb{F}_q$ $\mathbb{F}_q$ $\subset$ 为离 O_x $\mathbb{F}_q \subset O_x \to O_x/\mathfrak{m}_x$ 散赋值环意味着，特别地，。因此，该复合对每一个有理点确定一个同构 $\mathbb{F}_q \simeq O_x/\mathfrak{m}_x$ $x \in X$ 。

除非另有说明，我们将在$J_X^i(L)$上考虑由左同态 $\iota^i\colon O_X \to P_X^i$导出的 O_X-模结构。

A.2.1. 基本性质：现假设 X 是 $\mathbb{F}_q$上的光滑射影曲线。层$J_X^i(L)$具有与J_X^i类似的基本性质：

1. 存在 O_X-模的典范短正合列，

$$0 \to \omega_X^{\otimes i} \otimes L \to J_X^i(L) \to J_X^{i-1}(L) \to 0. \tag{A.8}$$

2. 若 $U \subset X$是开子集，则典范地有$J_X^i(L)|_U \simeq J_U^i(L|_U)$。

3. 若 $x \in X$是有理点，则典范地有$J_X^i(L)|_x \simeq L_x/\mathfrak{m}^{i+1}L_x$。

4. 若 $U =$Spec(A)是使 L 平凡化的仿射开子集，且 $\gamma : L|_U \simeq O_X|_U$ 是一个平凡化，则

$$J_X^i(L)|_U \simeq J_X^i(L|_U) \overset{J^i(\gamma)}{\simeq} J_X^i|_U \simeq O_U^{i+1}$$

非典范地。这个同构也记作 $J^i(\gamma)$。

5. 典范满射 $\pi_2^*L \to \pi_2^*L \otimes O_{X\times X}/I^{i+1}$ 通过伴随诱导出一个 O_X-模态射 $L \to \pi_{2*}(\pi_2^*L \otimes O_{X\times X}/I^{i+1})$。由于 $\pi_2^*L \otimes O_{X\times X}/I^{i+1}$ 支撑在对角线上，存在一个典范的 $\mathbb{F}_q$-模同构 $\pi_{2*}(\pi_2^*L \otimes O_{X\times X}/I^{i+1}) \simeq \pi_{1*}(\pi_2^*L \otimes O_{X\times X}/I^{i+1})$。综上，得到一个 $\mathbb{F}_q$-线性映射

$$d_L^i := L \to J_X^i(L).$$

定义 A.4. L 的 i 阶截断泰勒序列映射是上文定义的 $\mathbb{F}_q$-线性映射 d_L^i。

需要特别强调的是，上文提到的典范同构，

$$J_X^i(L)\big|_x \simeq L_x/\mathfrak{m}_x^{i+1}L_x = L/L(-(i+1)x),$$

使截断泰勒序列映射 $d_L^i\colon L \to J_X^i(L)$ 与限制态射 $J_X^i(L) \to J_X^i(L)|_x$ 复合后与自然商映射一致

$$L \to L/L(-(i+1)x).$$

A.2.2. 可逆层的截面的导数。 截断泰勒序列映射的一项关键性质是，对于每个开子集 $U \subset X$，我们都有一个交换图

$$\begin{array}{ccccc} L|_U & \xrightarrow{d_L^i|_U} & J^i(L)|_U & \xrightarrow{\text{canonical}} & J^i(L|_U) \\ \downarrow{\scriptstyle \gamma} & & & & \downarrow{\scriptstyle J^i(\gamma)} \\ O_U & & \xrightarrow[d_U^i]{} & & J_U^i \end{array} \tag{A.9}$$

因此，给定一个局部截面 $s \in L|_U$ 和一个生成元 $z \in \omega_X|_U$，我们有

$$d_L^i|_U(s) = D_{U,z}^0(\gamma(s)) + D_{U,z}^1(\gamma(s))\overline{\xi} + \cdots + D_{U,z}^i(\gamma(s))\overline{\xi^i}$$

其中 $\overline{\xi^j} := J^i(\gamma)^{-1}(\xi^j)$。

定义 A.5. 我们将 s 关于平凡化 $(U,\ \gamma)$ 与参数 z 的第 j 阶导数定义为

$$D^j_{U,\gamma,z}(s) := D^j_{U,z}(\gamma(s)) \tag{A.10}$$

相对于 U、γ 和 z（假设 $U = \mathrm{Spec}(A)$），$D^j_{U,\gamma,z}$ 的依赖关系可描述如下：

1. 平凡化变换：设 $\gamma' : L|_U \simeq O_U$ 是另一个平凡化。则存在一个有理函数 $f \in O_U$，使得 $\gamma' = f\gamma$。因此，

$$D^j_{U,\gamma',z}(s) = D^j_{U,z}(\gamma'(s)) = D^j_{U,z}(f\gamma(s)) = \sum_{t=0}^{j} D^{j-t}_{U,z}(f) D^t_{U,z,\gamma}(s) \tag{A.11}$$

2. 参数变换（Faà di Bruno 公式）：现在固定 $\omega_X|_U$ 的另一个生成元 $w \in A$，并令 $\theta := \delta^i_U(w) \in J^i_U$。相对于基 $\{1, \theta, \ldots, \theta^i\}$，我们有

$$\xi = \sum_{l=0}^{i} D^l_{U,w}(z)\theta^l.$$

另一方面，$d^i_L|_U(s)$ 的两个不同表达式必须相等。也就是说，我们有等式

$$\sum_{j=0}^{i} D^j_{U,z,\gamma}(s)\xi^j = \sum_{j=0}^{i} D^j_{U,w,\gamma}(s)\theta^j$$

结合上述等式可得，对于 $m = 0, \ldots, i$，

(A.12)

$$D^m_{U,w,\gamma}(s) = \sum_{j=0}^{m} D^j_{U,z,\gamma}(s) \left(\sum_{\substack{l_1+\cdots+l_j=m \\ 1\le l_\alpha \le m}} \prod_{\alpha=1}^{j} D^{l_\alpha}_{U,w}(z) \right) =$$

$$= \sum_{j=0}^{m} D^j_{U,z,\gamma}(s) \left(\sum_{\substack{(n_1,\ldots,n_m)\in\mathbb{N}^m \\ \sum_{r=1}^m r n_r = m \\ \sum_{r=1}^m n_r = j}} \binom{j}{n_1, n_2, \ldots, n_m} \prod_{r=1}^{m} \left(D^r_{U,w}(z)\right)^{n_r} \right).$$

3. 开子集的变换：关于对 U 的依赖，值得指出的是 $D^j_{U,\ \gamma,\ z}(s) \in A$，而且如果 $V = \mathrm{Spec}(B) \subset U$（此处 $B = A_V$），那么 $D^j_{V,\ \gamma,\ z}(s|_U)$ 就只是局部化

$$D^j_{V,\gamma,z}(s|_U) = \frac{D^j_{U,\gamma,z}(s)}{1} \in B, \tag{A.13}$$

一个特别重要的推论是，给定一个有理点 $x \in U \subset X$，有理函数 $D^j_{U,\gamma,z}(s)$ 在 x 处的取值显然为

$$D^j_{U,\gamma,z}(s)(x) = \left[\begin{array}{l} \text{coefficient of order } j \text{ of the Taylor sequence of } \gamma(s) \\ \text{at } x \in X \text{ respect to the uniformizer } t_x := \dfrac{z}{1} \in O_x \end{array} \right].$$

也就是说，

$$D^{j}_{U,\gamma,z}(s)(x) = D^{n}_{t_x}(\gamma(s)) \tag{A.14}$$

如A.4中所定义

例 A.6。设 $\mathbb{F}_q$、K、X如上所述，$G = \sum_{x\in X} n_x \cdot x$是$X$ 的一个除子，而 $O_X(G)$ 是与 G相关联的可逆层。现在让我们看看如何在有理点 $x \in X$ 附近将 $O_X(G)$ 平凡化。我们区分两种情况：

1. 如果 $x \notin \operatorname{supp}(G)$，并令 $U_x := X \setminus \operatorname{supp}(G)$，则 $O_X(G)(U_x) = \{f \in K \mid (f)_{U_x} \geq 0\} \cup \{0\} = O_X(U_x)$。因此，$O_X(G)|_{U_x}$ 确实是平凡的。

2. 如果 $x \in \operatorname{supp}(G)$，令 $t_x \in K$ 为点 x 的一个局部参数。令 $U_x = X \setminus \{$为 $t_x\}$ 的极点。对于任意 $f \in O_X(G)(U_x)$，考虑元素$t_x^{n_x} \cdot f \in K$。注意到 $(t_x^{n_x} \cdot f) \geq 0$，所以 $t_x^{n_x} \cdot f \in O_X(U_x)$。该态射

$$\gamma : O_X(G)(U_x) \to O_X(U_x) \tag{A.15}$$

由 $f \mapsto t_x^{n_x} \cdot f$ 给出的是一个同构，即 U_x上的一个平凡化。假设我们处于第二种情形。令 $V_x :=U_x \setminus \{\ t_x\}$的零点。则$\gamma$：$O_X(G)(V_x) \simeq O_X(V_x)$是一个平凡化，且 dt_x生成 $\omega_X(V_x)$。于是，导数$D^{j}_{U,\gamma,z}(f)$在 x 处的值恰好是 $D^{n}_{t_x}(t_x^{n_x} f)$。

参考文献

1. S. Bhandari 等，《多项式、差商与码》，arXiv 预印本 arXiv:2412.01755 (2024)。2. M. B. Can 和 B. Horowitz，《广义高阶导数 Reed–Solomon 码》，arXiv 预印本 arXiv:2512.22948v1 (2025)。3. M. B. Can、D. Montero 和 F. Özbudak，《瓶颈度量下的评价码》，arXiv 预印本 arXiv:2509.17682v1 (2025)，研究瓶颈型度量下 Reed–Solomon 码的类似形式及其向代数几何码的扩展。4. N. Coxon，《重数码的快速系统编码》，符号计算杂志 **94** (2019)。5. S. T. Dougherty 和 M. M. Skriganov，《MacWilliams 对偶与 Rosenbloom–Tsfasman 度量》。6. E. M. Gabidulin，《秩码》，《密码学、安全与隐私百科全书》，2025。7. B. S. Gopinadh 和 V. Marka，《Rosenbloom–Tsfasman 度量下的码：综述》，《物理学杂志：会议系列》，第 1770 卷，2021。8. V. D. Goppa，《代数几何码》，《苏联消息报：数学》**21** (1983)，第 1 期，75–91。9. R. Goyal 等，《单变量重数码和折叠 Reed–Solomon 码的快速列表译码》，FOCS，2024。10. A. Grothendieck 和 J. Dieudonné，《代数几何基础：IV. 概形与概形态射的局部研究，第四部分》，IHÉS 数学出版物，第 32 卷，高等科学研究所，1967。11. V. Guruswami 和 C. Wang，《折叠 Reed–Solomon 码和重数码的线性代数列表译码》，IEEE 信息论汇刊 **59** (2013)，第 6 期，3493–3500。12. D. Han 和 C. Fan，《非椭圆曲线型 Roth–Lempel NMDS 码》，IEEE 信息论汇刊 **69** (2023)，第 9 期，5670–5675。13. R. Hartshorne，《代数几何》，数学研究生教材，第 52 卷，施普林格出版社，1977。14. J. I. Iglesias Curto、A. L. Muñoz Castañeda、J. M. Muñoz Porras 和 G. Serrano Sotelo，《每个卷积码都是 Goppa 码》，IEEE 信息论汇刊 **59** (2013)，第 10 期，6628–6641。

15. Y. Ihara, 《有限域上代数曲线有理点数的一些评注》, 东京大学理学部纪要 **28** (1981)。 16. S. Kopparty, 《关于重数码的列表译码》, STOC 会议录, 2012, 第 399–414 页。 17. S. Kopparty、S. Saraf 和 S. Yekhanin, 《具有亚线性时间译码和低带宽局部性的高码率码》, 美国计算机协会会刊 (JACM) **61** (2014), 第 3 期, 1–34。 18. D. Laksov, 《曲线上线性系的朗斯基行列式与普吕克公式》, 高等师范学院科学纪事 **17** (1984), 第 1 期, 45–66。 19. D. Laksov 和 A. Thorup, 《曲线族的 Brill–Segre 公式》, 第 123 卷, 美国数学学会, 普罗维登斯, 罗得岛州, 1991。 20. , 《曲线族的魏尔斯特拉斯点与间隙序列》, 《数学档案》**32** (1994), 第 2 期, 393–422。 21. K. Lee, 《具有 Rosenbloom–Tsfasman 度量的线性空间的自同构群》, 欧洲组合学杂志 **24** (2003), 第 6 期, 607。 22. R. Pellikan、B.-Z. Shen 和 G. J. M. van Wee, 《哪些线性码是代数几何码? 》, IEEE 信息论汇刊 **37** (1991), 第 3 期, 583–602。 23. D. Perkinson, 《格拉斯曼流形中的曲线》。 24. R. Piene, 《射影 n 维空间中曲线的数值特征》, 《实与复奇点》, Sijthoff and Noordhoff, 1977, 第 475–495 页。 25. M. Yu. Rosenbloom 和 M. A. Tsfasman, 《 m度量的码》, 《信息传输问题》*33* (1997), 第 1 期, 45–52。 26. A. K. Sharma 和 A. Sharma, 《关于 RT 度量下重量枚举式的麦克威廉斯恒等式》, 《离散数学、算法与应用》**06** (2014), 第 02 期。 27. H. Stichtenoth, 《代数函数域与码》, 第 2 版, 第 254 卷, 施普林格, 2009。 28. J. Tate, 《曲线上微分的留数》, 高等师范学院科学纪事 **第 4 辑, 1** (1968), 第 1 期, 149–159。 29. M. A. Tsfasman 和 S. G. Vlăduţ, 《代数几何码》, 《数学及其应用（苏联系列）》, 第 58 卷, 施普林格, 多德雷赫特, 1991。 30. A. Weil, 《有限域中方程解的数量》, 美国数学会通报 **55** 0029393 31 1949 5, 497 508 ( ), 第 – 期。 MR。L. Wu, 《重新审视重数码：一类新的高码率局部可纠错码》, 第 53 届 Allerton 会议, 2015。 32. L. Xu 和 C. Fan, 《由 Reed–Solomon 码构造的非椭圆曲线型近 MDS 码》, 《离散数学》**346**(2023), 第 9 期, 113490。 33. L. Xu、C. Fan 和 D. Han, 《由 PG(2, q) 中的极大弧构造的近 MDS 码》, 《有限域及其应用》**93** (2024), 102338。

萨拉曼卡大学数学系电子邮箱地址:
davidgonzalezgonzalez1.7@usal.es

莱昂大学数学系电子邮箱地址：amunc@unileon.es

萨拉曼卡大学数学系电子邮箱地址：navas@usal.es