arXiv:2602.03803v1 [math.NT] 3 Feb 2026

有限域上一般 Drinfeld 模的点子模计算

ANTOINE LEUDI`ERE 和 RENATE SCHEIDLE R

摘要。我们提出一种算法，用于计算有限域上 Drinfeld A-模的点模的任意子模的结构，其中A 是 $\mathbb{F}_q$上的函数环。当函数环为 $A = \mathbb{F}_q[T]$时，我们还计算该子模的 Frobenius 分解。我们的算法尤其适用于同源核和挠子模。我们在弗罗贝尼乌斯标准形、模的表示和 Fitting 理想的框架下介绍这些算法。它们主要依赖高效且经典的线性代数方法，并结合快速的 Ore 多项式运算。我们分析了算法的复杂度，探讨了优化方法，并在 SageMath 中提供了实现。最后，我们计算了一个与 Drinfeld $\mathbb{F}_q[T]$-模相关的简单不变量，它编码了 $\mathbb{F}_q[T]$ 中所有对应挠点为有理点的多项式。

1. 引言

Drinfeld 模是函数域算术中最重要的工具之一。秩二 Drinfeld 模与椭圆曲线及复乘理论有着密切的相似之处，秩一 Drinfeld 模类似于单位根和 Kronecker-Weber 定理，但高秩 Drinfeld 模在零特征中没有直接的对应物。Drinfeld 模于 1977年被引入，用于解决函数域中的 Langlands 猜想（针对 GL_r ）[Dri77；Laf01]，并取得了显著成功。在更具实际性的应用背景下，Drinfeld 模可用于有限域上多项式的先进因式分解 [DNS21] ，以及线性多项式的计算机代数 [BMZ25]。最近，人们发现 Drinfeld 模非常适合应用于编码理论 [BDM24；MP26]。鉴于函数域和代数曲线在编码理论中所发挥的重要技术与历史作用 [Gop83]，，Drinfeld 模为在代数几何和秩度量码领域大幅推进现有技术水平提供了一条很有前景的途径。

尽管 Drinfeld 模已成功应用于诸多领域，但关于其计算方面的研究远远落后于椭圆曲线的相关研究。Caranay、Greenberg 和 Scheidler 于 2018年发表的成果是最早明确探讨 Drinfeld 模算法问题的研究之一，且仅关注普通二秩 Drinfeld 模 [Car18; CGS20]。随后，Musleh 和 Schost 运用现代计算机代数技术，计算有限域上秩二 Drinfeld 模的 Frobenius 自同态的特征多项式[MS23]。秩二这一假设使得人们能够将椭圆曲线中的方法改用于 Drinfeld 模。直到 2023年，Musleh 和 Schost [MS23] 以及 Caruso 和 Leudi`ere [CL26] 引入全新技术，才解除这一相当严格的假设。值得注意的是，其中一些方法

和工具（例如为计算目的而使用的 Anderson 动机）在椭圆曲线领域没有直接对应且计算效率高的方案。本文的工作将沿着这一方向继续推进。

在 [CL26], Caruso 和 Leudi`ere 计算了同源的范数和自同态的特征多项式，这相当于椭圆曲线点计数在函数域上的对应问题。我们在此基础上，提出一种高效的通用算法，用于计算有限域上 Drinfeld 模态射的核的模结构，通过 其不变因子来表示。特别地，零态射这一特殊情形可恢复整个有理点模的结构。我们的方法采用了不同于以往工作的思路；尤其是，它并非建立在椭圆曲线理论的基础上。虽然使用了 Frobenius、史密斯标准形、模的表示和 Fitting 理想等经典工具，但我们也利用了 Drinfeld 模特有的性质以及计算机代数领域的先进技术。最重要的是，我们利用了 Drinfeld 模函数环 A 的有限生成$\mathbb{F}_q$-代数结构。这在椭圆曲线领域没有对应物；在椭圆曲线中，函数环所扮演的角色由整数 $\mathbb{Z}$承担。我们的算法适用于任意秩、定义在任意有限域上且对应任意函数环 A的 Drinfeld A-模。

在 $A = \mathbb{F}_q[T]$ 的情形下，我们进一步给出一种算法，用于计算点模子模的 Frobenius 分解（算法 4），并提供精确的渐近复杂度分析。固定 q 相对于其他参数不变时，该算法以 $O(dr + dn + d^{\omega})$ 的代价计算态射核的 不变因子和 Frobenius 分解，其中 n 是输入态射的 τ-次数， r 是其定义域 Drinfeld 模的秩，d 是基域的 $\mathbb{F}_q$-维数，而 $2 \leqslant \omega \leqslant 3$ 是矩阵乘法的一个可行指数（命题 4.2）。本文还给出了其他精确的复杂度结论。

最后，给定有限域上的一个 Drinfeld $\mathbb{F}_q[T]$-模，我们利用 Anderson 动机计算唯一的首一元素 $g \in \mathbb{F}_q[T]$ ，使得对于 $a \in \mathbb{F}_q[T]$， a-挠点是有理的，当且仅当 a 整除 g。不变量 g 是所有此类 a 的最小公倍式，我们无需预先知道有理点模的不变因子即可计算它。据我们所知，目前没有任何高效方法能够对椭圆曲线完成同样的任务。

我们的主要算法以 SageMath [The26; Ayo+23] 实现；代码可在 GitHub 上获取，并附有一个$Jupyter$ 笔记本，读者可在任何网络浏览器中轻松运行。所有代码和说明均可在`https://github.com/kryzar/research-drinfeld-submodules/`获取。

据我们所知，我们是首篇研究如何有效且高效地计算 Drinfeld 模的点模的子模的不变因子和 Frobenius 分解的工作。对于椭圆曲线，计算不变因子的最佳算法是通用阿贝尔群算法。例如，Sutherland 的方法 [Sut11] 通过在素数幂阶子群上求离散对数来计算一个基。虽然 Drinfeld 模的离散对数可以轻易求得 [Sca01], ，但将 Sutherland 的方法应用于这一情形，会得到一种通常比我们的方法慢得多的算法，无论从渐近复杂度分析还是从实现来看都是如此。此外，我们的方法具有确定性、易于实现且接近最优等优点。

本文组织如下。

(1) 第 2 节介绍必要的背景知识。我们简要介绍 Ore 多项式（§ 2.2）和 Drinfeld 模（§ 2.3）。我们回顾矩阵、多项式和 Ore 多项式的计算机代数，并着重讨论复杂度模型（§ 2.4）。最后，我们介绍一个通用框架，用于计算戴德金环上有限模的不变因子和 Frobenius 分解；这类有限模由有限个矩阵唯一确定（§ 2.5）。该框架可直接应用于 Drinfeld 模。具体而言，在 § 2.5.1 中，我们说明如何通过计算 Drinfeld 模在态射之核上的作用的弗罗贝尼乌斯标准形及其基变换矩阵，求得该核的不变因子和 Frobenius 分解。此方法无法推广到一般情形，此时我们需要借助 Fitting 理想来求得不变因子（§ 2.5.2）。(2) 第 3 节介绍最先进的多点求值方法（§ 3.1），并重新探讨与多项式整除链相关的算法（§ 3.2）。(3) 第 4 节介绍我们的主要算法。我们再次区分 $A = \mathbb{F}_q[T]$ 的情形（§ 4.1）和一般情形（§ 4.2）。在 $A = \mathbb{F}_q[T]$ 的情形下，我们还介绍计算挠子模的替代方法（§ 4.1.2），并讨论采用不同底层基本操作时算法的效率（§ 4.1.3）。(4) 第 5 节介绍一种简单方法：给定有限域上的 Drinfeld $\mathbb{F}_q[T]$-模，求出所有使 a-挠点有理的 $a \in \mathbb{F}_q[T]$ 。

2. 背景

2.1. **不变因子与 Frobenius 分解**。 我们首先定义用于刻画戴德金环上有限模结构的量。我们的目标是计算有限域上 Drinfeld 模点的子模的这些量。

定理 2.1。 设 A 为戴德金整环， W 为有限 A-模。存在理想 $\mathfrak{d}_1, \ldots, \mathfrak{d}_\ell \subset A$ 以及元素 $x_1, \ldots, x_\ell \in W$，使得以下结论成立。

(1) 这些元素生成该模： $W = Ax_1 \oplus \cdots \oplus Ax_\ell$；(2) 这些理想构成整除链： $\mathfrak{d}_1 \mid \cdots \mid \mathfrak{d}_\ell$；(3) 对于所有 i， x_i 的零化子为 $\mathfrak{d}_i$，即 $Ax_i \simeq A/\mathfrak{d}_i$；

特别地， $W \simeq \prod_{i=1}^{n} A/\mathfrak{d}_i$，且链 $(\mathfrak{d}_1, \ldots, \mathfrak{d}_\ell)$ 是唯一的。我们称这些理想 $\mathfrak{d}_1, \ldots, \mathfrak{d}_\ell$ 为 W 的不变因子，称这些元素 $x_1, \ldots, x_\ell$ 为 W 的Frobenius 分解 。

2.2. **Ore 多项式**。 Ore 多项式是定义 Drinfeld 模及其同源的主要组成部分。下文中，设 $\mathbb{F}_q$ 是含有q 个元素的有限域。设 K 是 $\mathbb{F}_q$的一个域扩张，且设 τ 是 K 上的 $\mathbb{F}_q$-线性 Frobenius 自同态，其定义为 $\tau(x) = x^q$。

定义 2.2. 集合

$$K\{\tau\} \coloneqq \left\{ \sum_{i=1}^{n} x_i \tau^i,\ n \in \mathbb{Z}_{\geqslant 0},\ x_1, \ldots, x_n \in K \right\}$$

在复合与加法运算下构成一个 $\mathbb{F}_q$-代数，称为*Ore* 多项式 的 $\mathbb{F}_q$-代数（相对于 $\mathbb{F}_q$ 和 K）。

尽管 Ore 多项式的乘法通常不可交换，但 Ore 多项式保留了经典多项式的许多重要特征。具体而言，我们有如下结论：

(1) 非零 Ore 多项式 $f = \sum_{i=1}^{n} x_i \tau^i \in K\{\tau\}$ 的 τ-次数记作 $\deg_\tau(f)$，它是满足 $x_i \neq 0$ 的最大 i。τ-赋值是满足 $x_i \neq 0$ 的最小 i。(2) $f \in K\{\tau\}$ 的核是一个 $\mathbb{F}_q$-向量空间，记作 $\ker f$。若 f 非零，则 $\dim_{\mathbb{F}_q}(\ker(f)) \leqslant \deg_\tau(f)$。$f$ 的根可能存在于 K 中，我们将其记作 $\ker_K(f) \coloneqq \ker(f) \cap K$。(3) 若 Ore 多项式 $f \in K\{\tau\}$ 满足 $\dim_{\mathbb{F}_q}(\ker(f)) = \deg_\tau(f)$，则称其为可分；若满足 $\dim_{\mathbb{F}_q}(\ker(f)) < \deg_\tau(f)$，则称其为不可分。(4) Ore 多项式代数 $K\{\tau\}$ 关于 τ-次数构成一个右欧几里得整环。对于任意 $f, g \in K\{\tau\}$，存在 $\alpha, \beta \in K\{\tau\}$ 使得 $f = \alpha g + \beta$ 且 $\deg_\tau(\beta) < \deg_\tau(g)$。因此，对于不全为零的任意 $f, g \in K\{\tau\}$，我们可以将 $\operatorname{rgcd}(f, g)$ 定义为满足 $K\{\tau\}f + K\{\tau\}g = K\{\tau\}\operatorname{rgcd}(f, g)$ 的唯一首一 Ore 多项式，并将 $\operatorname{llcm}(f, g)$ 定义为满足 $K\{\tau\}f \cap K\{\tau\}g = K\{\tau\}\operatorname{llcm}(f, g)$ 的唯一首一 Ore 多项式。

2.3. **Drinfeld 模**。现在我们转而定义 Drinfeld 模及相关对象，包括同源和点模。关于这一主题的一般介绍，请参阅 [Pap23] 或 [Arm+25] 。我们先确立记号和术语。以下，设 C 是定义在 $\mathbb{F}_q$ 上的光滑射影几何连通曲线，并带有一个几何闭点 ∞。设 A 为 $\mathbb{F}_q$（C）上在 ∞之外正则的函数所构成的环。那么 A 是一个戴德金整环，称为函数环。设 K 是 $\mathbb{F}_q$的一个域扩张，并配备一个 $\mathbb{F}_q$-代数态射 $\gamma: \ A \to K$。称对（K，γ）为一个 A-域。设 K 为 K的一个代数闭包。

定义 2.3。一个定义在（K，γ）上的*Drinfeld* A-模是一个 $\mathbb{F}_q$-代数态射

$$\begin{array}{rccc} \phi: & A & \to & K\{\tau\} \\ & a & \mapsto & \phi_a, \end{array}$$

使得 Im（ϕ）$\not\subset K$，并且对每个 $a \in A$，ϕ_a 的常数项为 γ（a）。

Drinfeld 模虽然名称中带有“模”，但并不是模，而是 $\mathbb{F}_q$-代数同态。不过，它们会在扩张 L/K 上诱导出模结构。

定义 2.4. 对于任意扩张 L/K，Drinfeld 模 ϕ 的 L-点模，记作 $\phi(L)$，是由下式定义的 A-模

$$\begin{array}{rcl} A \times L & \to & L \\ (a, z) & \mapsto & \phi_a(z). \end{array}$$

$\phi(K)$ 的元素称为有理点。

对于所有 Drinfeld 模，$\phi(L)$的底层集合相同，但作为 A-模，其结构取决于 ϕ。本文旨在当 K 为有限集时，计算 $\phi(K)$的任意 A-子模的不变因子。当 $A = \mathbb{F}_q[T]$时，我们还给出 $\phi(L)$任意子模的 Frobenius 分解（算法 4）。为了表示这些子模，我们引入态射和同源。

定义 2.5。 设 ϕ, ψ 是定义在(K, γ)上的两个 Drinfeld A-模。一个从态射ϕ 到 ψ 是满足以下条件的 Ore 多项式 $u \in K\{\tau\}$: 对每个 $a \in A$, $u\phi_a = \psi_a u$ 成立。同源 是非零态射。

态射 u 的核（其定义域为 ϕ ）是 $\phi(K)$ 的一个有限 A-子模。为避免歧义，当将 $\ker(u)$ 视为一个 A-模时，我们记作 $\phi(\ker(u))$。反过来， $\phi(K)$ 的每个有限 A-子模都是一个以 ϕ 为起点的同源的核，而该同源可通过 [Arm+25 命题 3.2] 有效计算。因此，我们的目标是计算态射的核的不变因子和 Frobenius 分解。

每个 Drinfeld 模都带有一个重要的不变量：其秩。

引理 2.6。 设 ϕ 是域 (K, γ) 上的一个 ***Drinfeld*** A-模。存在唯一的整数 $r \geqslant 1$, 使得对所有 $a \in A$, 都有 次数$_\tau(\phi_a) = r$维数$_{\mathbb{F}_q}(A/aA)$。整数 r 称为 ϕ的秩 。

注 2.7。 定义一个 Drinfeld A-模，等价于定义一个单射 $A \to K\{\tau\}$。如何构造这样的单射并不明确，而且这种单射可能根本不存在 [Pap23，注 4.3]。另一方面， $A = \mathbb{F}_q[T]$ （对应于 $C = \mathbb{P}^1_{\mathbb{F}_q}$）的情形则很简单：一个 Drinfeld $\mathbb{F}_q[T]$-模 ϕ 由 T 的像 ϕ_T唯一确定，其秩就是 $\deg_\tau(\phi)$。

最后，一个特别感兴趣的主题，例如计算 Tate 模、Weil 配对，以及近期的秩度量码 [BDM24; MP26]，是计算 $a \in A$ 上 ϕ_a 的核。

定义 2.8. 设 $a \in A$。 ϕ 的 a-挠点 是态射 ϕ_a 的核。它是 $\phi(K)$ 的一个 A-子模，记作 $\phi[a] := \phi(K)[a]$。包含于 L 中的 ϕ 的 a-挠点为 $\phi(L)[a] := \phi[a] \cap \phi(L)$。若 ϕ 的 a-挠点满足 $\phi(L)[a] = \phi[a]$, 则称其为 L-有理 。

2.4. **计算机代数**。 现在我们明确复杂度模型，并在 § 2.4.1 中回顾关于多项式和矩阵的经典计算机代数归约。我们特别强调 Ore 多项式的快速基本运算（§ 2.4.2、§ 2.4.3）。

2.4.1. 多项式和矩阵的代价函数。 我们先定义代价函数。设 F是一个域。 $F[T]$ 中次数为 $\leqslant n$ 的两个多项式可以相乘，代价为 $O(\mathbf{PM}(n))$ 次 F中的运算。我们假设 $\mathbf{PM}$ 是超可加的，即 $\mathbf{PM}(x+y) \leqslant \mathbf{PM}(x) + \mathbf{PM}(y)$ 对所有输入 x, y 都成立。当 F 是有限域时，我们可以取 $\mathbf{PM}(n) = n \log n \log\log n$ [GG13, § 8.3] （另见 [HHL17]，其复杂度略优）。此外:

- 在 $F[T]$ 中对两个次数分别为 m 和 n的多项式进行欧几里得除法， $m \geqslant n$，所需代价为 $O(\mathbf{PD}(m, n))$ 次 F中的运算。我们可以取 $\mathbf{PD}(m, n) = O(\mathbf{PM}(m-n) + \mathbf{PM}(n))$ [GG13, § 11]。
- 两个次数为 $\leqslant n$ 的多项式，其最大公因式可通过 F中的 $O(\mathbf{PG}(n))$次运算计算得出。我们可以选取$\mathbf{PG}(n) = \mathbf{PM}(n) \log n$ [GG13, § 11]，并假设$\mathbf{PG}(n) \in O(n^2)$。

接下来，我们为矩阵运算引入代价函数。在 $F^{d \times d}$ 中，两个矩阵的乘法可以通过在 F 中进行 $O(\mathbf{MM}(d))$ 次运算来完成。特别地，我们令 $2 \leqslant \omega \leqslant 3$ 满足 $\mathbf{MM}(d) = d^\omega$。

2.4.2. *Ore* 多项式。 我们的几乎所有算法都依赖于 Ore 多项式的底层基本操作：欧几里得除法、llcm 和 rgcd 的计算，以及多点求值。设 K 是 $\mathbb{F}_q$ 的有限扩张，且满足 $[K:\mathbb{F}_q]=d$。关于 $K\{\tau\}$ 中 Ore 多项式计算机代数的最新成果，归功于 Caruso 和 Le Borgne [CL17a]。他们的计算模型有一个问题，即假设 K 中的所有运算，包括 Frobenius 自同态的作用~(即计算 x^q，其中 $x\in K$)，都可以通过在 $\mathbb{F}_q$ 中进行 $O(d)$ 次运算来完成。但这一假设并非总是成立（关于此问题的讨论，参见 [MS23] ）。因此，我们分别统计算术运算和 Frobenius 自同态的作用。

定义2.9。令

$$\mathbf{SM}=(\mathbf{SM}_{\mathrm{A}},\mathbf{SM}_{\mathrm{F}}):\quad \mathbb{Z}_{>0}^2\quad\to\quad[1,\infty[$$

为一个函数，使得次数为 $\leqslant n$ 的两个 Ore 多项式可以进行乘法运算，其代价为 $O(\mathbf{SM}_{\mathrm{A}}(n))$ 次在 K 中的算术运算，以及 $O(\mathbf{SM}_{\mathrm{F}}(n))$ 次 Frobenius 运算。我们将该代价称为 $O(\mathbf{SM}(n))$ 次在 K中的算术运算和 *Frobenius* 运算。

2.4.3. 分治算法。稍后，我们将使用分治算法描述 Ore 多项式的快速多点求值算法（第 3.1 节）。下面回顾如何分析此类算法的代价。对于大小为 ℓ 的输入，分治算法的代价由如下形式的递归给出

$$T(\ell)\leqslant 2T\left(\frac{\ell}{2}\right)+\alpha\left(\left\lceil\frac{\ell}{2}\right\rceil\right), \tag{2.1}$$

如果 α 是超可加的，我们可以求解该递归：

$$T(\ell)=O(\alpha(\ell)\log\ell). \tag{2.2}$$

因此，引入以下记号会很方便：

命题 2.10. 对于 $\alpha:\ \mathbb{Z}_{>0}\to[1,\infty[$, 我们通过以下方式定义 $\alpha^{\geqslant 1}:\ \mathbb{Z}_{>0}\to[1,\infty[$:

$$\alpha^{\geqslant 1}(\ell):=\ell\sup_{1\leqslant\ell'\leqslant\ell}\frac{\alpha(\ell')}{\ell'}.$$

函数 $\alpha^{\geqslant 1}$ 是超可加的，并且是所有大于 α的此类函数中最小的。

在我们的情形中，我们不假设$\mathbf{SM}$ 是超可加的，因为 Caruso 和 Le Borgne 给出的$\mathbf{SM}$取值不满足这一性质 [CL17b，第 83] 页。遵循他们的方法，我们将改用$\mathbf{SM}^{\geqslant 1}:=(\mathbf{SM}_{\mathrm{A}}{}^{\geqslant 1},\ \mathbf{SM}_{\mathrm{F}}{}^{\geqslant 1})$来求解由分治算法产生的递归。

2.5. **由矩阵得到的模**。 现在我们介绍一条路线，用于计算有限域上 Drinfeld 模点的子模的不变因子和 Frobenius 分解。

2.5.1. 情形 $A=\mathbb{F}_q[T]$。 这是最简单的情形，因为对于 Drinfeld $\mathbb{F}_q[T]$-模ϕ， $\phi(K)$ 由 ϕ_T 的作用唯一确定。固定基域的一组 $\mathbb{F}_q$- 基后， ϕ_T 可表示为一个矩阵，其中包含关于 $\phi(K)$ 的全部信息。因此，任务就是从该矩阵中提取信息。为清晰起见，我们借助向量空间和矩阵描述一个通用框架，该框架可直接应用于 Drinfeld 模。

设 F 是一个域， V 是一个 F-向量空间，且 φ 是 V 的一个自同态（在我们的语境中， φ 的角色由 ϕ_T 承担）。这一设定自然地在 V 上赋予一个 F-模结构：

$$\begin{array}{ccc} F[T] \times V & \to & V \\ (a(\varphi), x) & \mapsto & a(\varphi)(x). \end{array}$$

这个新模记为 $V[\varphi]$。

注 2.11。对于有限域 K 上的 Drinfeld $\mathbb{F}_q[T]$-模 ϕ 以及定义域为 ϕ的态射 u，这种情况对应于取 $F = \mathbb{F}_q, V = \ker_K u, \varphi = \phi_T$和 $V[\varphi] = \phi(K)$。因此，目标是计算 $V[\varphi]$的不变因子和 Frobenius 分解。

若 V具有有限的 F-维数，我们可以为其赋予一个 F-基 $\mathcal{E} = (\varepsilon_1, \ldots, \varepsilon_d)$，而 φ 可由矩阵 $M \in F^{d\times d}$表示。通过计算矩阵 M的弗罗贝尼乌斯标准形，即可求得 $V[\varphi]$ 的不变因子：该标准形是如下形式的分块对角矩阵

$$\mathrm{F}_M = \begin{pmatrix} \boxed{C_{d_1}} & & \\ & \ddots & \\ & & \boxed{C_{d_\ell}} \end{pmatrix} \in F^{d\times d}$$

使得

(1) 每个 C_{d_i} 都是多项式 $d_i \in F[T]$的友矩阵；(2) 这些多项式构成整除链： $d_1 | \cdots | d_\ell$；(3) 矩阵 M 与 F_M 在 F上相似。

此外，若 S 是一个基变换矩阵，使得

$$\mathrm{F}_M = S^{-1} M S,$$

则可立即由 S^{-1} 得到 $V[\varphi]$ 的 Frobenius 分解。我们将 $S^{-1} \in F^{d\times d}$ 写成一个水平分块矩阵，其中第 i 个分块有 $\deg(d_i)$ 列，并将第 i 列标记为 x_i:

$$S^{-1} = \begin{pmatrix} \boxed{x_1 \cdots} & \cdots & \boxed{x_\ell \cdots} \end{pmatrix} \in F^{d\times d}$$

命题 2.12. 在上述记号下，理想 $(d_1), \ldots, (d_\ell)$ 是 $V[\varphi]$ 的不变因子，而元素 $x_1, \ldots, x_\ell$ 构成 $V[\varphi]$ 的一个 *Frobenius* 分解。

由命题 2.12 可知，要得到 $V[\varphi]$ 的不变因子和 Frobenius 分解，只需将 φ 表示为一个矩阵并计算其弗罗贝尼乌斯标准形。计算 Frobenius 标准形可以使用 Storjohann 的算法[Sto00，第 9] 章。

引理 2.13。设 $M \in F^{d\times d}$为一个矩阵。计算 M的弗罗贝尼乌斯标准形及其对应的幺模基变换矩阵，所需运算次数为 $O(\mathbf{MM}(d)(\log d)(\log\log d))$，运算在 F中进行。

设 ϕ 是有限域 K上的 Drinfeld $\mathbb{F}_q[T]$-模，且 u 是一个定义域为 ϕ的态射。因此，通过计算 ϕ_T 相对于 $\ker_K(u)$（一个 $\mathbb{F}_q$-向量空间）的 $\mathbb{F}_q$-基的矩阵，并按上述方法提取不变因子，就可以计算 $\phi(\ker_K(u))$（一个 $\mathbb{F}_q[T]$-模）的不变因子和 Frobenius 分解。在第 3.1 节中，我们将重新讨论 Ore 多项式的快速多点求值，以便高效计算 Ore 多项式的矩阵；随后给出我们的主要算法（算法 4）。

2.5.2. 一般情形。 一般情形的困难在于，不能假定函数环由一个元素生成。为了克服这一困难，我们使用模的表示。

定义 2.14。 设 A 是一个环， W 是一个 A-模。 W 的表示 是一个 A-模的正合序列

$$W' \xrightarrow{\alpha} W'' \xrightarrow{\beta} W \longrightarrow 0.$$

注 2.15。 这个定义的动机在于，映射 α 唯一确定了 W，且仅差一个同构，即 $W \simeq W''/\mathrm{Im}(\alpha)$。特别地，若 α 由一个对角矩阵表示，其元素为 $d_1, \dots, d_m$，则 $W \simeq A/(d_1) \times \cdots \times A/(d_\ell)$。

我们再次给出一个更一般的处理方法，它可以直接应用于 Drinfeld 模。与第 2.5.1 节一样，设 F 是一个域， V 是一个有限维 F-向量空间，维数为d。令 $\mathcal{E} = (\varepsilon_1, \dots, \varepsilon_d)$ 为 V的一组 F-基。这里，我们不假设 V带有一个指定的自同态，而是假设它扩张为一个 A-模，其中 A 是一个 F-代数，且有有限个生成元 $g_1, \dots, g_m \in A$。A-模结构记为 W。最后，记 $V_A := A \otimes_F V$。

注记 2.16。 上述设定适用于 $F = \mathbb{F}_q$, $V = \ker_K(u)$,$W = \phi(\ker_K(u))$，其中 ϕ 是定义在有限域 K 上的 Drinfeld A-模，其函数环为 A。注意，每个函数环 A都是在 $\mathbb{F}_q$上有限生成的。

我们有一个有限表示

$$(V_A)^n \xrightarrow{\chi} V_A \xrightarrow{\pi} W \longrightarrow 0,$$

其中我们定义

$$\begin{cases} \chi\left((a_k \otimes v_k)_{1 \leqslant k \leqslant n}\right) = \sum_{k=1}^n \left(a_k g_k \otimes v_k - a_k \otimes (g_k \cdot v_k)\right), \\ \pi(a \otimes v) = a \cdot v. \end{cases}$$

F基$\mathcal{E}$的基于 V规范地给出 V_A和 V_A^n的基，而 χ由矩阵 M_χ 表示，该矩阵是由伴随矩阵构成的分块矩阵

$$M_\chi = \begin{pmatrix} \boxed{g_1 \operatorname{Id} - M_1} \\ \vdots \\ \boxed{g_m \operatorname{Id} - M_m} \end{pmatrix} \in A^{d \times nd} \tag{2.3}$$

其中每个 M_i 都是 F-线性自同态 $x \mapsto g_i x$的矩阵。 g_i是什么？这些是 $\mathbb{F}_q$的 A生成元吗?

备注 2.17。 在 $A = \mathbb{F}_q[T]$ 的情况下，我们看到 M_χ 是特征矩阵 $T\mathrm{Id} - M$，因此 $V[\varphi] \simeq A^d/\mathrm{Im}(T\mathrm{Id} - M)$。所以， $V[\varphi]$ 的不变因子恰好是特征矩阵 $T\mathrm{Id} - M$ 的不变因子，即其史密斯标准形的非零对角元素。然而，计算多项式矩阵的史密斯标准形，远比计算同样大小且元素属于某个域的矩阵的弗罗贝尼乌斯标准形昂贵。

回到一般的模设定， W 的不变因子就是矩阵 M_χ 的不变因子，可以使用 Fitting 理想求得。[Fit36]:

引理 2.18。设

$$W' \xrightarrow{\alpha} W'' \xrightarrow{\beta} W \longrightarrow 0$$

是 W 的一个表示，并假设 α 在某个基下由矩阵 $M \in A^{r\times s}$ 给出，其中 r、 $s \in \mathbb{Z}_{\geqslant 0}$。对于 $1 \leqslant 0 \leqslant d$，令

$$\mathrm{Fitt}_i(W)$$

由 M 的 $(d-i)$ 阶子式生成的理想。$\mathrm{Fitt}_i(W)$ 的值不依赖于表示的选择。对于 $0 \leqslant i \leqslant d$，我们称 $\mathrm{Fitt}_i(W)$ 为 W 的第 i 个 Fitting 理想 。

经典结果 [Sta26, § 15.8] 指出，Fitting 理想构成一条整除链

$$\mathrm{Fitt}_d(W) \mid \cdots \mid \mathrm{Fitt}_0(W),$$

并且有以下有用的引理 [Sta26, Lemma 15.8.4]。

引理 2.19。 设 W 的不变因子为 $\mathfrak{d}_1, \ldots, \mathfrak{d}_\ell$。那么

$$\mathfrak{d}_i = \frac{\mathrm{Fitt}(d-i)}{\mathrm{Fitt}(d+1-i)}.$$

设 ϕ 是定义在有限域上的 Drinfeld A-模，其函数环为 A，并设 u 是一个定义域为 ϕ 的态射。设 $g_1, \ldots, g_m$ 是 A 作为 $\mathbb{F}_q$-代数的一组生成元。为了计算 $\phi(\ker_K(u))$（一个 A-模）的不变因子，只需计算 $\phi_{g_1}, \ldots, \phi_{g_m}$ 在 $\ker_K(u)$（一个 $\mathbb{F}_q$-向量空间）上的作用矩阵 $M_1, \ldots, M_m$，由这些矩阵计算矩阵 $g_i\,\mathrm{Id} - M_i$，并将它们堆叠成矩阵 M_χ，计算 M_χ 的 Fitting 理想，最后应用引理 2.19 得到 $\phi(\ker_K(u))$ 的不变因子。

3. 计算机代数

在第 2.5 节中，我们构建了在 K 为有限时，计算 A-子模 $\phi(K)$ 的不变因子所需的主要理论工具。接下来需要分析底层算法的计算复杂度。我们将重新讨论 Ore 多项式（第 3.1 节）和多项式整除链（第 3.2 节）。

3.1. **Ore 多项式的计算机代数。** 我们将提出一种高效的 Ore 多项式多点求值方法。首先，我们需要评估快速欧几里得除法、左最小公倍数和右最大公因式的计算成本。Caruso 和 Le Borgne 已经描述了经典方法在 Ore 多项式上的对应方法（参见 [CL17a，第 3.2.1] 节以及 [CL17b，第 3.2.2] 节）。我们陈述它们的复杂度，使之符合我们的复杂度模型。

引理 3.1. 设 f、$g \in K\{\tau\}$ 是两个次数为 $\leqslant n$ 的 *Ore* 多项式。对 f 除以 g 进行右 *Ore*欧几里得除法、求右最大公因式和左最小公倍数，所需的运算和 *Frobenius* 运算次数均为 $O(\mathbf{SM}^{\geqslant 1}(n)\log n)$ K。

接下来，我们讨论多点求值。设 f 是次数为 n 的 Ore 多项式，且 $X = (x_1, \ldots, x_\ell)$ 是 K 中的元素，其中 $n \leqslant \ell$。我们希望高效地计算 $f(x_1), \ldots, f(x_\ell)$。对于任意 $x \in K$，令 $L_x := \tau - {}^{\tau}(x)_x \in K\{\tau\}$。如果 $R_x \in K\{\tau\}$ 是 f 除以 L_x 时右除法所得的余式，那么 $f(x) = xR_x$。换句话说，$f(x)$ 是将 R_x 视为常数Ore多项式后，在 x 处的求值。对于元素 $x_{i_1}, \ldots, x_{i_{\ell'}} \in X$，我们令

$$L_{x_{i_1},\ldots,x_{i_{\ell'}}} := \operatorname{lclm}(L_{x_{i_1}}, \ldots, L_{x_{i_{\ell'}}}).$$

令 $R_{x_{i_1},\ldots,x_{i_{\ell'}}}$ 为 f 除以 $L_{x_{i_1},\ldots,x_{i_{\ell'}}}$所得的右除法余式。那么对于任意$x_{i_j}$ ，都有

$$f(x_{i_j}) = R_{x_{i_1},\ldots,x_{i_{\ell'}}}(x_{i_j}).$$

利用这些恒等式，我们可以如下分解多点求值问题。为便于表示，假设 ℓ 为偶数。我们将输入分成两半：$X_l = (x_1, \ldots, x_{\frac{\ell}{2}})$ 和 $X_r = (x_{\frac{\ell}{2}+1}, \ldots, x_\ell)$。已知 L_{X_l}和 L_{X_r} 后，通过计算 R_{X_l}和 R_{X_r}，即可得到 $f(x_1), \ldots, f(x_\ell)$，然后对所有$x_i \in X_l$ 计算 $R_{X_l}(x_i)$，并对所有 $x_i \in X_r$计算 $R_{X_r}(x_i)$。此步骤的代价是对次数为 $\leqslant \frac{\ell}{2}$ 的 Ore 多项式进行两次欧几里得除法，以及对大小为 $\leqslant \frac{\ell}{2}$ 的条目进行两次递归调用。

–

在算法 1 中，按照经典方法，我们将 X 的最小公倍式递归地预计算为一棵二叉树，称为的 *lclm*树。

算法 1： lclm树

输入： X'是以下集合族的子族：$X := (x_1, \ldots, x_\ell)$

输出： X'的lclm树

1 **如果** $X' = \{x_i\}$是单元素集合，**则**
2 　返回仅有的叶节点为 L_{x_i}的树。
3 **结束**
4 **否则**
5 　将 X' 拆分为两半：X'_l 和 X'_R。
6 　计算并设置 $T_l = \text{LclmTree}(X'_l)$。
7 　计算并设置 $T_r = \text{LclmTree}(X'_r)$。
8 　计算 L 和 T_l 的根的 lclm T_r。
9 　**返回**以 L 为根、以 T_l 和 T_r 为子树的二叉树。
10 **结束**

设 T_X 为算法 1 生成的树，我们假定其已预先计算。由此得到用于多点求值的算法 2。

算法 2： 多点求值

输入： 一个 Ore 多项式 f、元素 x_1、……、$x_\ell \in K$ 和树 T_X

输出： 求值结果 $f(x_1)$ ……，$f(x_\ell)$

若 若 $\ell = 1$ **则**
  返回 $f(x_1)$
结束
否则
  将 $x_1, \ldots, x_\ell$ 分成两半 X_l 和 X_r（必要时进行填充）。
  令 $\mathcal{T}_l$ 为 T_X 的左子树，并将 L_{X_l} 作为其根。
  令 $\mathcal{T}_r$ 为 T_X 的右子树，并将 L_{X_r} 作为其根。
  计算 R_{X_l}，作为 f 除以 L_{X_l} 的欧几里得除法。
  计算 R_{X_r}，作为 f 除以 L_{X_r} 的欧几里得除法。
  计算 $f(x_1) \ldots, f(x_{\ell/2}) =$ 多点求值$(R_{X_l}, X_l, \mathcal{T}_l)$。
  计算 $f(x_{\ell/2+1}) \ldots, f(x_\ell) =$ 多点求值$(R_{X_r}, X_r, \mathcal{T}_r)$。
  返回 $f(x_1) \ldots, f(x_\ell)$
结束

引理 3.2。 设 x_1，…，$x_\ell \in K$，且 f 是一个次数为 $\leqslant \ell$ 的 *Ore* 多项式。$f(x_1)$ …，$f(x_\ell)$ 中的各值可通过 $O(\mathbf{SM}^{\geqslant 1}(\ell)(\log \ell)^2)$ 次算术和 *Frobenius* 运算求得，其中 K。

证明。这项任务的成本是依次运行算法 1 和算法 2 的成本。对于这两个分治算法，规模为 ℓ 的输入，其成本由形式为 (2.1) 的递归式给出，其中 $\alpha(\ell) = \mathbf{SM}^{\geqslant 1}(\ell) \log \ell$（引理 3.1）。应用方程 (2.2) 以及 $x \mapsto \mathbf{SM}^{\geqslant 1}(x) \log x$（命题 2.10）的超可加性，即可完成证明。□

备注 3.3。Ore 多项式多点求值的成本为 $O(\mathbf{SM}^{\geqslant 1}(\ell)(\log \ell)^2)$ 次算术运算和 Frobenius 运算，而经典多点求值的成本为 $O(\mathbf{PM}(\ell)\log \ell)$ 次算术运算 [GG13，第 10 节。1]。额外的 $(\log \ell)$ 因子源于我们必须使用左最小公倍数，而不能使用乘积。

3.2. **整除链的计算机代数。** 现在我们转而讨论整除链相关的高效计算；当我们已知整个有理点模的这些量时，需要通过这些计算来求出扭子子模的不变因子和 Frobenius 分解（§ 4.1.2）。设 F 是一个域，$a \in F[T]$ 是一个多项式，$d_1 \mid \cdots \mid d_\ell$ 是 $F[T]$ 中多项式 ℓ 的一条整除链。算法 3 可高效计算多项式 $\gamma_i := \gcd(a, d_i)$ 和 $\rho_i := d_i/\gamma_i$，对所有 $1 \leqslant i \leqslant \ell$ 均如此。稍后，我们希望在向量和矩阵上计算这些多项式的值。设 $\delta := \deg(d_1) + \cdots + \deg(d_\ell)$。

引理 3.4。 算法 *3* 以 F 中 $\delta = \sum_{i=1}^{\ell} \deg(d_i)$ 次运算的代价，计算 $(\gamma_1, \ldots, \gamma_\ell)$ 和 $(\rho_1, \ldots, \rho_\ell)$，其代价为 $O(\mathbf{PM}(\deg(a)) + \mathbf{PM}(\delta)\log \delta)$。

证明。所有运算均为 F 中的算术运算。步骤 1 的代价为 $O(\mathbf{PM}(\deg(a) - \deg(d_\ell)) + \mathbf{PM}(\deg(a)))$ 次运算。接下来的两个步骤代价为 $O(\mathbf{PG}(\deg(a') + \deg(d_\ell)) + \mathbf{PD}(\deg(d_\ell) + \deg(\gamma_\ell)))$ 次运算，即 $O(\mathbf{PG}(\deg(d_\ell)))$。其余部分需要 $\sum_{i=1}^{\ell-1} O(\mathbf{PG}(\deg(d_{i+1})) + \mathbf{PD}(\deg(d_i)))$ 次运算，即 $O(\mathbf{PG}(d))$ 次运算。利用 $\mathbf{PG}(\delta) = \mathbf{PM}(\delta)\log \delta$ 这一事实，即可完成证明。□

算法 3： ChainGcd

输入： 多项式 a 和 d_1、…、d_ℓ。

输出： 列表 $(\gamma_1$、…、$\gamma_\ell)$ 和 $(\rho_1$、…、$\rho_\ell)$。

1 计算 $a' = a$ 对 d_ℓ 取模。
2 计算 $\gamma_\ell =$ 与 a'、d_ℓ 的最大公因式。
3 计算 $\rho_\ell = d_\ell/\gamma_\ell$。
4 **对于** i 从 $\ell - 1$ 递减至 1 **执行**
5 　计算 $\gamma_i =$ 最大公因式(γ_{i+1}, d_i)。
6 　计算 $\rho_i = d_i/\gamma_i$。
7 **结束**
8 **返回** (γ_i, ρ_i) 和 (γ_ℓ, ρ_ℓ)。

接下来，我们将说明如何在矩阵和向量上计算整除链。设 M 是一个元素属于 F 的 $d\times d$ 矩阵，并设 $x_1, \ldots, x_\ell$ 是 F^d 的向量。我们希望计算向量 $y_i = \rho_i(M)\, x_i$，其中 $1 \leqslant i \leqslant \ell$。一旦已知多项式 $(\rho_i)_{1\leqslant i\leqslant \ell}$（其计算代价见引理 3.4），计算 $(y_i)_{1\leqslant i\leqslant \ell}$ 有多种方法：

- 我们可以朴素地计算 $(y_i)_{1\leqslant i\leqslant \ell}$，耗费 $O(\delta d^2)$ 次运算，运算在 F 中进行。
- 在我们的应用中，我们有 $\delta \leqslant d$。因此，我们可以依次计算矩阵 $(\rho_i(M))_{1\leqslant i\leqslant \ell}$，总计耗费 $O(\ell \mathbf{MM}(d)(\log d)(\log\log d))$ 次运算，运算在 F 中进行，所用算法出自 Storjohann [Sto00，第 9] 章。然后，我们以相同的渐近成本计算 $(y_i)_{1\leqslant i\leqslant \ell}$。

为了考虑计算 $(y_i)_{1\leqslant i\leqslant \ell}$ 时的多种可能性，我们引入一个成本函数。

定义 3.5。设

$$\mathbf{EV}: \quad \mathbb{Z}_{>0} \quad \to \quad [1, \infty[$$

是一个函数，使得对于任意矩阵 $M \in F^{d'\times d'}$、任意一组向量 $x_1, \ldots, x_{\ell'} \in F^d$ 以及任意整除链 $d'_1 \mid \cdots \mid d'_\ell \in F[T]$，均可通过 F 中的 $O(\mathbf{EV}_d(\ell', \delta'))$ 次运算计算出量 $d'_1(M)x_1, \ldots, d'_{\ell'}(M)x_{\ell'}$，其中$\delta' = \sum_{i=1}^{\ell'} \deg(d'_i) \leqslant d'$。

4. 对 Drinfeld 模的应用

我们现在已具备计算有限域上 Drinfeld 模的点的子模结构所需的全部要素。更确切地说，设 (K, γ) 为一个A-域，且满足 $d = \dim_{\mathbb{F}_q}(K)$，并固定 K 的一个 $\mathbb{F}_q$-基 $\mathcal{E} = (\varepsilon_1, \ldots, \varepsilon_d)$。设 ϕ 为 (K, γ) 上秩为 r 的 Drinfeld A-模。我们的目标是，对任意定义域为 ϕ的态射 u，计算 $\phi(\ker_K(u))$ 的不变因子。注意，这包括 $\phi(K)$，因为它是零态射的核。在情形 $A = \mathbb{F}_q[T]$ 中，我们还计算 $\phi(K)$ 的任意 $\mathbb{F}_q[T]$-子模的 Frobenius 分解（将其表示为某个同源的核），并对我们的算法给出详细的复杂度分析。该问题是第 2.5 节所提出框架的一个直接实例。我们首先考虑情形 $A = \mathbb{F}_q[T]$（第 4.1 节），因为它可以利用非常高效的工具，具体而言是（元素属于某个域的矩阵的 Frobenius 标准形，而非多项式矩阵的 Fitting 理想。然后我们转向 A 为函数环时的一般 Drinfeld$A$-模情形。（第 4.2 节）。

4.1. 情形 $A = \mathbb{F}_q[T]$. 该情形属于第 2.5.1 节所提出的框架。沿用第 2.5.1 节中的相同记号，我们有 $F = \mathbb{F}_q$、 $\varphi = \phi_T$ 以及 $V = \ker_K(u)$。 $\phi(\ker_K(u))$（作为 $\mathbb{F}_q[T]$-模）的不变因子与 Frobenius 分解，可通过计算 ϕ_T 在 $\ker_K(u)$ 上作用（作为 $\mathbb{F}_q$-向量空间）的矩阵的弗罗贝尼乌斯标准形得到。因此我们需要两个要素：Ore 多项式的矩阵的快速计算，以及 Frobenius 标准形（引理 2.13）。

4.1.1. 计算同源的核。

引理 4.1. 设 $f \in K\{\tau\}$ 是一个 τ-次数为 n 的 *Ore* 多项式。设 x_1、.....、 x_ℓ 是 K 中的元素，其中 $\ell \leqslant d$。计算 $f(x_1)$ ..... 、 $f(x_\ell)$ 的代价为 $O(n)$ 次在 K 中的算术运算，以及 K 中 $O(\mathbf{SM}^{\geqslant 1}(d)(\log d)^2)$ 次算术和 *Frobenius* 运算。特别地，以相同代价可以计算相对于 E 的 f 的矩阵 $M_f \in {\mathbb{F}_q}^{d\times d}$ 。

证明。 首先，我们将 f 对 $\tau^d - 1$ 取模，这可以通过移位系数完成，代价为在 K 中进行 $O(n)$ 次算术运算。然后由引理 3.2 得出结论。□

设 u 是定义在 K 上、定义域为 ϕ 的 Drinfeld $\mathbb{F}_q[T]$-模态射。算法 4 计算 $\phi(\ker_K(u)$ 的不变因子和 Frobenius 分解。命题 4.2 给出了该算法的渐近复杂度。

命题 4.2. 设 u 是一个 *Drinfeld* $\mathbb{F}_q[T]$-模之间的态射，其定义域为 ϕ。算法 *4* 以 $\mathbb{F}_q$ 中 $O(\mathbf{MM}(d)(\log\ d)(\log\log\ d))$ 次算术运算、 $O(r + \deg_\tau(u))$ 次 K 中的算术运算，以及 $O(\mathbf{SM}^{\geqslant 1}(d)(\log d)^2)$ 次 K 中的 *Frobenius* 运算和算术运算，计算 核 u 的不变因子及 *Frobenius* 分解。

证明。 步骤 1 中计算 M_u 的代价为在 K 中进行 $O(\deg(u))$ 次算术运算，并在 K 中进行 $O(\mathbf{SM}^{\geqslant 1}(d)(\log d)^2)$ 次算术运算和 Frobenius 运算；这直接应用引理 4.1 即可。步骤 2 中计算 $\ker(M_u)$ 的一个 $\mathbb{F}_q$-基，代价为在 $\mathbb{F}_q$ 中进行 $O(\mathbf{MM}(d))$ 次运算。

下一个计算量较大的步骤，是计算 ϕ_T 作为 $\ker_K(u)$ 上 $\mathbb{F}_q$-线性自同态时的矩阵 X （步骤 9）。该矩阵的各列是 $\phi_T(b_1)\ldots,\phi_T(b_{d'})$ 相对于步骤 2 中计算得到的基 $\mathcal{B} = (b_1,\ldots,b_{d'})$ 的坐标。根据引理 4.1，计算 $\phi_T(b_1)\ldots,\phi_T(b_{d'})$ 需要在 K 中进行 $O(r)$ 次算术运算，并在 K 中进行 $O(\mathbf{SM}^{\geqslant 1}(d)(\log d)^2)$ 次算术运算和 Frobenius 运算。现在， X 可由方程 $NX = Y$ 唯一确定；该方程可使用标准线性代数方法求解，例如对 N 进行 LUP 分解，再进行前代和回代，代价为在 $\mathbb{F}_q$ [IMH82] 中进行 $O(\mathbf{MM}(d))$ 次算术运算。

下一个耗时较高的步骤是计算 X 的弗罗贝尼乌斯标准形 F_X ，以及幺模变换矩阵 S （§ 10）。根据引理 2.13，计算这些内容的运算成本为 $O(\mathbf{MM}(d')(\log d')(\log\log\ d'))$ 次 $\mathbb{F}_q$ 运算；这包含在 $\mathbb{F}_q$ 中的 $O(\mathbf{MM}(d)(\log\ d)(\log\log\ d))$ 次运算内。

最后，我们需要求出 $\phi(\ker_K(u))$ 的 Frobenius 分解。我们无法直接从 ${S^{-1}} \in {\mathbb{F}_q}^{d'\times d'}$ 中提取向量（如第 2.5.1 节所述），因为 S^{-1} 的列表示的是相对于基 $\mathcal{B}$ 的元素。相反，我们需要这些元素相对于原始基 $\mathcal{E}$ 的坐标。这些元素的坐标

算法 4： MorphismKernelInvariants

输入： 一个从有限域 K 上的 Drinfeld $\mathbb{F}_q[T]$-模 ϕ 出发的态射 u 配备有 $\mathbb{F}_q$-基 $\mathcal{E}$

输出： $\phi(\ker_K(u))$ 的不变因子及 Frobenius 分解

// Compute $\ker_K(u)$

1 计算 u 相对于$\mathcal{E}$的矩阵 $M_u \in \mathbb{F}_q^{d\times d}$。

2 计算 $\ker_K M_u$的一个 $\mathbb{F}_q$-基$\mathcal{B} = (b_1, \dots, b_{d'})$。

3 **如果**$\ker_K M_u = \{0\}$，**则**

4 　**返回**$(1 \in \mathbb{F}_q[T])$ 和 $(0 \in K)$

5 **结束**

6 将$\mathcal{B}$中的向量放入矩阵 $N_u = [b_1, \cdots \ b_{d'}] \in \mathbb{F}_q^{d\times d'}$.

// Compute the action of ϕ_T on 核$_K(u)$

7 求出 $\phi_T(b_i)$ 的坐标 y_i，$1 \leqslant i \leqslant d'$，相对于 $\mathcal{E}$。

8 将这些向量放入矩阵 $Y = [y_1, \dots, y_{d'}] \in \mathbb{F}_q^{d\times d'}$.

9 求出满足 $NX = Y$ 的唯一矩阵 X。

// Compute the Frobenius normal form of the action of ϕ_T

10 求出 X 的弗罗贝尼乌斯标准形 $\mathrm{F}_X \in \mathbb{F}_q^{d'\times d'}$，以及一个满足 $S\mathrm{F}_X S^{-1} = X$ 的基变换矩阵 $S \in \mathbb{F}_q^{d'\times d'}$。

// Convert the vectors to the basis E

11 计算 $S^{-1} \in \mathbb{F}_q^{d'\times d'}$。

12 将 F_X写成分块对角矩阵，其元素为 C_{d_1}、.....、C_{d_ℓ}。

13 计算矩阵 $S' := NS^{-1} \in \mathbb{F}_q^{d\times d'}$。

// Record and return the results

14 **对于** i，从 1 到 ℓ **执行**

15 　将 d_i 记作 $\mathbb{F}_q[T]$ 中与 C_{d_i} 对应的首一多项式。

16 　记 x_i 为 K 中的元素，其 F 坐标（相对于 $\mathcal{E}$）为索引为 $\deg(d_1) + \cdots + \deg(d_{i-1})$ 的列，在 S' 中。

17 **结束**

18 **返回** $(d_1, \dots, d_\ell)$ 和$(x_1, \dots, x_\ell)$。

为 S^{-1} 的列相对于 $\mathcal{E}$ 的坐标，恰好就是 S' 的列（步骤 13）。计算 S' 的成本也包含在 O 的 $\mathbf{MM}(d)$ 次运算中。$\mathbb{F}_q$。□

算法 5： ModuleOfPointsInvariants

输入： 有限域 K 上的 Drinfeld $\mathbb{F}_q[T]$-模 ϕ

输出： $\phi(K)$ 的不变因子和 Frobenius 分解

1 **返回** MorphismKernelInvariants(0_ϕ)，其中 0_ϕ 是零态射在 ϕ 上。

推论 4.3。算法 *5* 计算 ϕ(核$_K(u)$) 的不变因子和弗罗贝尼乌斯分解，其代价为：在 $\mathbb{F}_q$ 中进行 $O(\mathbf{MM}(d)(\log d)(\operatorname{loglog} d))$ 次算术运算，在 K 中进行 $r)$ 次算术运算，以及在 K 中进行 $O(\mathbf{SM}^{\geqslant 1}(d)(\log d)^2)$ 次 ***Frobenius*** 运算和算术运算。

注 4.4。若不使用算法 4（MorphismKernelInvariants）来实现算法 5（ModuleOfPointsInvariants），效率也只会略有提高。原因在于，在当前的描述中，由于 $\ker_K(u)$ 的基本身就是 $\mathcal{B}$，许多中间量都得以简化；于是我们计算的就是矩阵 ϕ_T 相对于 $\mathcal{E}$ 自身的弗罗贝尼乌斯标准形。矩阵 ϕ_T 可以预先计算，并用于其他运算，代价是在 K 中进行 $O(r)$ 次算术运算，并在 K 中进行 $O(\mathbf{SM}^{\geqslant 1}(d)(\log d)^2)$ 次算术运算和 Frobenius 运算（引理 4.1）。其余运算的代价是在 K 中进行 $O(\mathbf{MM}(d)(\log d)(\log\log d))$ 次算术运算（引理 2.13）。

4.1.2. 挠子子模。对于这个特殊情形，其中 $u=\phi_a$ 对某个 $a\in\mathbb{F}_q[T]$成立，w 可以直接重用 $\phi(K)$ 的不变因子 $(d_i)_{1\leqslant i\leqslant \ell}$ 和 Frobenius 分解 $(x_i)_{1\leqslant i\leqslant \ell}$，前提是它们已经计算出来（见算法 5 和推论 4.3）。假设对于每个 i，x_i 对应于 d_i，并沿用引理 3.4 之前给出的记号，我们记 $\gamma_i := \text{最大公因式}(a,\ d_i)$ 和 $\rho_i := d_i/g_i$，其中$1\leqslant i\leqslant \ell$。那么我们有一个 $\mathbb{F}_q[T]$-模的同构

$$\phi(K)[a]\simeq\prod_{i=1}^{\ell}\mathbb{F}_q[T]/(\gamma_i).$$

此外，元素 $x_{a,\ i}=\phi_{\rho_i}(x_i)$ 的阶为 γ_i。只考虑满足 $\gamma_i\neq 1$ 的指标集合 I_a，其中 i，我们有

$$\phi(K)[a]=\bigoplus_{i\in I_a}\mathbb{F}_q[T]x_{a,i}.$$

换言之，$(\gamma_i)_{i\in I_a}$ 和 $(x_{a,\ i})_{i\in I_a}$ 分别构成 $\phi(K)[a]$的不变因子和 Frobenius 分解。这将导出算法 6。

算法 6： TorsionFromModuleOfPoints

输入：多项式 $a\in A$、$\phi(K)$ 的不变因子 $(d_1,\dots,d_\ell)$ 和 Frobenius 分解 $(x_1,\dots,x_\ell)$，其中 ϕ 是有限域 K 上的 Drinfeld$\mathbb{F}_q[T]$-模输出：$\phi(K)[a]$ 的不变因子和 Frobenius 分解1 使用算法 3 计算 $\gamma_i := \gcd(a,d_i)$ 和 $\rho_i := d_i/\gamma_i$，其中 $1\leqslant i\leqslant \ell$ 取遍所有值。2 令 I_a 为满足 $\gamma_i\neq 1$ 的指标 $1\leqslant i\leqslant \ell$ 集合。3 对所有 $i\in I_a$，计算 $x_{a,i} := \phi_{\gamma_i}(x_i)$。4 返回 $(\gamma_i)_{i\in I_a}$ 和 $(x_{a,i})_{i\in I_a}$

为简洁起见，记 $d_a := \dim_{\mathbb{F}_q}\phi(K)[a]$，并记 $\ell_a :=\#I_a$ 为 $\phi(K)[a]$ 的不变因子个数。回顾定义 3.5 中对$\mathbf{EV}$的定义。

命题 4.5。给定$\phi(K)$的不变因子和 *Frobenius* 分解，算法 *6* 以 $O(\mathbf{PM}(\deg(a))+\mathbf{PM}(d)\log d+\mathbf{EV}_d(\ell_a,d_a))$ 次运算的代价，计算$\phi(K)[a]$ 的不变因子和 *Frobenius* 分解，其中 $\mathbb{F}_q$。

证明。根据引理 3.4，调用算法 3 需要在 $\mathbb{F}_q$ 中进行 $O(\mathrm{PM}(\deg(a))+\mathrm{PG}(d))$ 次运算。最后一步需要在 K 中进行 $O(\mathrm{EV}_d(\ell_a,d_a))$ 次运算，其中 $d_a=\dim_{\mathbb{F}_q}\phi(K)[a]$，且 $\ell_a=\#I_a$ 是不变因子的数量。渐近地，$\mathrm{PG}(d)\in O(d^2)$，而 $\mathrm{EV}_d(\ell_a,d_a)$ 至多为 $O(d^2)$，因此算法 6 的总成本为 $O(\mathrm{PM}(\deg(a))+\mathrm{EV}_d(\ell_a,d_a))$。□

4.1.3. 显式复杂度结果。我们根据 Ore 多项式的不同基本运算，确定若干算法的成本。我们从算法 5 开始。该算法主要包含两个步骤（注 4.4）：计算 K 的 $\mathbb{F}_q$-基 $\mathcal{E} = \{\varepsilon_1, \ldots\ldots, \varepsilon_d\}$ 下的 ϕ_T 矩阵 M_{ϕ_T}，以及计算其 Frobenius 分解。我们首先确定计算 M_{ϕ_T} 的成本。回顾一下，由于 K 是一个维数为 $\mathbb{F}_q$ 的有限域，在 K 中的一次算术运算可以通过 $\widetilde{\ }$ 次运算完成，成本为 $O(d\log\ q)$ 次位运算 [（GG13，第 2] 章）。

(1) 最朴素的方法是依次计算 $\phi_T(\varepsilon_1) \ldots, \phi_T(\varepsilon_d)$。计算一次求值需要 r Frobenius 运算，并使用平方乘法为一次 Frobenius 运算计算 $O(\log q)$ 次 K 中的运算，我们得到计算 ϕ_T的 $\sim O(rd^2(\log\ q)^2)$ 次位运算。(2) 如果我们使用多点求值（算法 2 和引理 4.1），结合 $\mathrm{SM_F}(d) = d^2$ 以及平方乘法，那么计算 M_{ϕ_T} 的代价为 $\widetilde{O}(r + d^3(\log q)^2)$。换言之，只有采用快速的 Ore 多项式乘法原语，才能实现快速多点求值。(3) 如果 $\widetilde{O}(\mathrm{SM}^{\geqslant 1}(d))$ 次 K 中的运算，如 [CL17b][1], 中所述，计为 $\widetilde{O}(d^{\frac{9-\omega}{5-\omega}}\log\ q)$ 次位运算，那么我们可以用 $\widetilde{O}(rd\log\ q + d^{\frac{9-\omega}{5-\omega}}(\log\ q)^2)$ 次位运算计算 M_{ϕ_T}。如果 r 属于 $O(d)$，这优于第 1 项中的朴素方法；但另一方面，如果 d 增长而 r 保持不变，则朴素方法在 d中具有更好的复杂度。(4) 如果我们在算法 1 和 2 中使用 [LS24 的欧几里得算法 3] ，那么计算 M_{ϕ_T} 的渐近速度并不比朴素方法快，因为仅第一次最小左公倍数计算就需要二次数量级的 Frobenius 运算和算术运算。(5) 在朴素方法（第 1 项）中使用 Kedlaya-Umans 算法 [KU11] 进行 Frobenius 运算，而不是使用平方乘法时，引理 4.1 给出的代价为 $\widetilde{O}(d(\log q)^2) + (rd^2\log\ q)^{1+o(1)}$ 次位运算。

这表明，计算 M_{ϕ_T} 最具优势的三种方法分别是朴素方法（项目 1）、使用 Caruso 和 Le Borgne 的快速乘法算法（以及复杂度模型）进行多点求值（项目 3），以及使用 Kedlaya-Umans 算法对 Frobenius 自同态进行应用时采用多点求值（项目 5）。

（1）如果我们使用朴素方法计算 M_{ϕ_T}（项目 1），那么算法 5 的$\widetilde{\ }$成本为 O（rd^2（$\log\ q$）$^2 + \mathbf{MM}$（d） $\log\ q$）次位运算。（3）如果我们使用多点求值（算法 2），并采用 Caruso 和 Le Borgne 用于计算 M_{ϕ_T}的模型及基本运算，则算法 5 的成本为$\widetilde{O}$（$rd\log\ q + d^{\frac{9-\omega}{5-\omega}}$（$\log\ q$）^{2}）次位运算。相对于变量 d而言，计算 M_{ϕ_T} 的成本因此占主导地位。（5）如果我们在引理 4.1 中使用 Kedlaya 和 Umans 的模型及基本运算（项目 5）进行多点求值（算法 2），则算法 5 的总成本为 $\widetilde{O}$（d（$\log\ q$）$^2 + \mathbf{MM}$（d） $\log\ q$） $+$（$rd^2\log\ q$）$^{1+o(1)}$ 次位运算。

更一般地，我们总可以假设 $\mathbf{SM_A}(d) \in \mathbf{MM}(d)$（直接相乘两个 Ore 多项式的朴素方法会得到 $\mathbf{SM_A}(d) = d^2$）。为清楚起见，固定 $\log q$ 并使用

$\sim$ $\sim O$，根据推论 4.3，算法 5 的总成本为 $O(r + \mathbf{MM}(d))\widetilde{\ }$ 次算术运算，以及 $O(\mathbf{SM_F}(d))$ 次 Frobenius 自同态的应用。

[1]原文中 $\mathbf{SM}^{\geqslant 1}$ 的值有一处笔误，已在 [CL26, § 1.2.3] 中更正。

在应用 Frobenius 的成本不高于~其他算术运算成本的模型中，这需要 $O(r + \mathrm{MM}(d))$ 次算术运算，而 Frobenius 标准形的计算占据主导地位。

接下来，我们研究计算 $\phi(K)[a]$, $a \in \mathbb{F}_q[T]$ 的不变因子与一个 Frobenius 分解的代价，其中已知 $\phi(K)$ 的不变因子与一个 Frobenius 分解。与之前一样，记 $d_a := \dim_{\mathbb{F}_q} \phi(K)[a]$，并记 $\ell_a := \#I_a$ 为 $\phi(K)[a]$ 的不变因子个数。如第 3.2 节所述，算法 6（见命题 4.5）的代价要么是使用直接方法在$\mathbb{F}_q$中进行 $O(\mathrm{PM}(\deg(a)) + \mathrm{PM}(d) \log d + d_a d^2)$ 次运算，要么是使用 Storjohann 的多项式矩阵求值原语 [Sto00] 在 $\mathbb{F}_q$ 中进行 $O(\mathrm{PM}(\deg(a)) + \mathrm{PM}(d) \log d + \ell_a \mathrm{MM}(d))$ 次运算。当 d_a 相对于 d较小时，优先采用第一种方法；否则应使用第二种方法。特别地，我们看到，若秩相对于 $\deg(a)$ 较大，或 d_a 相对于 d较小，则通过复用 $\phi(K)$ 的相应结果来计算 $\phi(K)[a]$ 的不变因子与 Frobenius 分解代价更低。

4.2. **一般情形**。对于一般情形，我们应用第 2.5.2 节的结果。设 A是一个函数环。那么 A 是一个有限生成的 $\mathbb{F}_q$-代数。曲线 C 和函数环 A 可以用多种方式表示。这里，我们假设 A 表示为商环 $\mathbb{F}_q[T_1, \ldots, T_m]/(P)$，其中 P是某个多项式，并记 $g_i := T_i$模 P, $1 \leqslant i \leqslant n$。设 ϕ 是定义在 (K, γ) 上的一个 Drinfeld A-模，且 u 是一个定义域为 ϕ的态射。我们的目标是计算 $\phi(\ker_K(u))$ 的不变因子。我们沿用第 2.5.2 节的方法，其中 $V = \ker_K(u)$。对每个 $1 \leqslant k \leqslant n$，令 M_i 为关于固定基 $\mathcal{E}$ 的矩阵，它表示作用于 $\ker_K(u)$ 上的 $\mathbb{F}_q$-线性自同态 ϕ_{g_i}。令$d_u := \dim_{\mathbb{F}_q}(\ker_K(u))$。于是我们有一个 A-模的同构

$$\phi(\ker_K(u)) \simeq A^{d_u}/\mathrm{Im}(M_\chi),$$

其中 M_χ 是由分块 $(g_k \,\mathrm{Id} - M_k)_{1 \leqslant k \leqslant n}$ 构成的纵向分块矩阵，如方程 (2.3) 所示。于是，计算 $\phi(\ker_K(u))$ 的不变因子可归结为如下简单步骤：

(1) 计算矩阵 $M_1, \ldots, M_m$，以及矩阵 M_χ；(2) 计算 Fitting 理想 $\mathrm{Fitt}_1(M), \ldots, \mathrm{Fitt}_d(M)$；(3) 计算理想 $\mathfrak{d}_i := \mathrm{Fitt}_{d-i}(M)/\mathrm{Fitt}_{d+i-1}(M)$，其中 $1 \leqslant i \leqslant d$。

由引理 2.19，理想 $(\mathfrak{d}_i)_{1 \leqslant i \leqslant d}$ 是 $\phi(\ker_K(u))$ 的不变因子。

5. 判定挠点何时为有理

我们最后讨论一个与有理挠子模的计算密切相关的问题，即确定所有使得 $\phi[a]$ 为有理的 $a \in \mathbb{F}_q[T]$，其中 ϕ是有限域 $K/\mathbb{F}_q$ 上 $\mathbb{F}_q$-维数为 d的 Drinfeld $\mathbb{F}_q[T]$-模。虽然 $\phi(K)$ 的所有点都是挠点（它们是 $\chi_\phi(1)$-挠点，其中 χ 是 *Frobenius* 自同态的特征多项式），但并不能保证存在非常值的 $a \in \mathbb{F}_q[T]$，使得 a- 挠点为有理。

5.1. **Anderson 动机**。首先，我们简要介绍$Anderson$ $\mathbb{F}_q[T]$-动机；一般性介绍请参见 [And86；Hei04；Pap23；Arm+25]。

定义 5.1。与 Drinfeld 模 ϕ关联的$Anderson$ $\mathbb{F}_q[T]$-动机，记作 $\mathbb{M}(\phi)$，是由下式定义的 $K[T]$-模：

$$\begin{array}{rcl} K[T] \times K\{\tau\} & \to & K\{\tau\} \\ \left(\sum_{i=0}^n \lambda_i T^i, f(\tau)\right) & \mapsto & \sum_{i=0}^n \lambda_i f(\tau) \phi_{T^i}. \end{array}$$

重要的是， $\mathbb{M}(\phi)$ 是一个自由的 $K[T]$-模，其典范基 为$\{1, \tau, \ldots, \tau^{r-1}\}$。此外， $\mathbb{M}$ 定义了一个反变函子：对于任意 Drinfeld 模的态射 $u\colon \phi \to \psi$，都存在一个 $K[T]$-模的态射 $\mathbb{M}(u)\colon \mathbb{M}(\psi) \to \mathbb{M}(\phi)$，其定义为 $\mathbb{M}(u)(f) = fu$。函子 $\mathbb{M}$是全忠实的，因此我们可以用 $K[T]$ 中的 r 个系数的元组来表示 Ore 多项式。这种表示可通过 CL26 的算法 1] 轻松计算得到。

5.2. **何时挠点是有理的**。 目前用于判定有理性的方法仅适用于固定的 $a \in \mathbb{F}_q[T]$。

- 对于任意 s，记 K_s 为 K的次数为 s 的扩张。要确定 a-挠点的最小定义域（即分裂域），可以使用 Anderson 动机（§ 5.1）。事实上， $\phi(K_s)$ $[a] = \phi[a]$ 当且仅当 K 的 Frobenius 自同态在 $\phi[a]$上是恒等映射。利用 Drinfeld 模与 Anderson 动机之间经由函子 $\mathbb{M}$建立的对应关系，这等价于 $\mathbb{M}(\tau^{sd})$在商模 $\mathbb{M}(\phi)/\mathbb{M}(\phi)\phi_a$ 上是恒等映射（详见 [Pap23, § 3.6] ）。我们可以有效地将 $\mathbb{M}(\tau^d)$写成矩阵 $M \in (\mathbb{F}_q[T]/(a))^{r\times r}$。于是，使$\phi(K_s)$ $[a] = \phi[a]$ 成立的最小 s，就是使 M^s 为恒等映射的最小 s。然而，计算 s 似乎在计算上十分困难。例如，当 $\mathbb{F}_q[T]/(a)$ 是一个域时，求矩阵的幂等阶需要求出 $\mathbb{F}_q[T]/(a)$中元素的乘法阶。目前，实现这一目标的最佳方法需要对某个 n对应的整数 $q^n - 1$ 进行因式分解。

- 若给定 a ，则很容易判断 a-挠点是否有理。若 h 是 ϕ_a的 τ-赋值，则 a-挠点有理当且仅当 ϕ_a 右整除$\tau^h(\tau^d - 1)$。

这两种方法可判定单个 $a \in \mathbb{F}_q[T]$的挠点有理性，但无法找出所有具有有理 a-挠点的 $a \in \mathbb{F}_q[T]$ 。我们介绍一种能完成此任务的方法，从可分情形开始。考虑安德森动机 $\mathbb{M}(\phi)$及其典范 $K[T]$-基$\{1, \ldots, \tau^{r-1}\}$。由于 K具有有限$\mathbb{F}_q$-维数 d，安德森动机 $\mathbb{M}(\phi)$在 $\mathbb{F}_q[T]$上是自由的。设 $p \in \mathbb{F}_q[T]$ 为 $\mathbb{F}_q$-代数态射 $\gamma\colon \mathbb{F}_q[T] \to K$ 的核的首一生成元。设 a 与 p互素，从而 ϕ_a 可分。则 a-挠点是 K-有理的，当且仅当 ϕ_a右整除 $\tau^d - 1$。由于 ϕ_a的 $\mathbb{F}_q[T]$-坐标就是$(a, 0, \ldots)$，我们有如下命题。

命题 5.2. 令 g_ϕ 为 $\tau^d - 1 \in \mathbb{M}(\phi)$ 的 $\mathbb{F}_q[T]$ 坐标的最大公因式。若 a 与 p 互素，则 ϕ 的 a 挠点是有理的，当且仅当 a 整除 g_ϕ。

换言之，元素 g_ϕ 是所有满足与 p 互素且使 a 挠点为有理点的 $a \in \mathbb{F}_q[T]$ 的最小公倍式。利用 $\phi(K)$ 的不变因子，以及 $\phi[a] \simeq (\mathbb{F}_q[T]/(a))^r$ 这一事实，也可以求得这个不变量；不过，我们将介绍一种更直接、高效的方法。

注意，若 a 是 p 的倍数，则命题 5.2 不成立。实际上，此时 ϕ_a 不可分，因此它的所有倍数也都不可分。然而， $\tau^d - 1$ 是可分的。要确定使 p^s 挠点为有理点的最大 s ，可以按以下方法进行。

(1) 计算 $\phi(K)$ 的不变因子的乘积 n_ϕ。可以直接从 Frobenius 自同态 χ_ϕ 的特征多项式n_ϕ 中得到 $n_\phi = \chi_\phi(1)$（有关方法的回顾，见 [CL26，附录 A]

用于计算 χ_ϕ）。事实上，任何使 $\phi[a]$ 成为有理数的 $a \in \mathbb{F}_q[T]$，都是 n_ϕ 的因子。(2) 计算 n_ϕ 的 p-进赋值 v。使用 分治 基数转换方法 [GG13，第 9.2] 节，可在 $\mathbb{F}_q$ 中以 $O(\mathbf{PM}(\deg(n_\phi))\log(\deg(n_\phi)/\deg(p)))$ 次运算完成。(3) 所求整数 s 满足 $s \leqslant v$。可以尝试所有可能性来求得它，也可以实现更复杂的搜索算法。

注记 5.3。计算 g_ϕ 的代价仅取决于输入的大小，而与输出的大小无关。该代价是多项式级的。相比之下，对于有限域上的椭圆曲线，我们尚不知道任何高效方法来计算其对应的 g_ϕ。

从 n_ϕ 计算不变量 g_ϕ，以及挠点有理性检验，也已在 SageMath 中实现，并在引言中提到的 *Jupyter* 笔记本中进行了演示。

结论

本文所介绍的所有算法均为确定性算法，并且在完全一般的情形下都能良好运行。尽管如此，仍有改进的空间。

(1) 鉴于算法 6，我们或许可以考虑：对于某个 Drinfeld 模 ϕ 和同源 u，是否可以复用 $\phi(K)$ 的不变因子和 Frobenius 分解，以计算 $\phi(\ker_K(u))$ 的不变因子和 Frobenius 分解。首先需要找到 u 的一个矩阵表示，使其成为 $\mathbb{F}_q[T]$-态射（例如 一个表示矩阵），而不仅仅是一个 $\mathbb{F}_q$-态射。构造此类表示的代价至少为 d 中的 $O(\mathbf{MM}(d))$ 次运算，这并不比（在 d 中）命题 4.5 的估计更好。总之，将同源表示为 Ore 多项式很直接，但这未必是最适合计算的表示方式。

(2) 在算法 6 中，我们计算形如 $P(M)x$ 的量，其中 P是关于 $\mathbb{F}_q[T]$ 的次数为 $n \leqslant d$的多项式， M 是一个元素属于 $\mathbb{F}_q$的 $d\times d$ 矩阵，而 x 是一个向量。假设 $n \leqslant d$ 对于获得更优的复杂度至关重要（使用 Storjohann 方法 [Sto00，第 9]章）；若不作此假设，计算 $P(M)$ 的最佳方法是 Paterson 和 Stockmeyer 提出的方法 [PS73],，其运算成本为 $O(\sqrt{n}\mathbf{MM}(d) + nd^2)$，运算在 $\mathbb{F}_q$中进行。Paterson-Stockmeyer 方法在一般情形下是最优的。这引出了一个问题：能否调整 Paterson-Stockmeyer 方法（其本身是对霍纳方法 [Hor19]的直接改编），以便计算 $P(M)x$而无需计算 $P(M)$。一个根本障碍似乎在于缺少相关的向量乘积。目前的替代方案需要大量预计算，导致其复杂度与 Storjohann 方法相同或更差。这引出了另一个问题：是否存在一种方法，能够计算 $P(M)x$（完全一般的情形），其成本为 $O(nd + \sqrt{nd^2})$，即在 d中达到成本最优，且仅需在 $\mathbb{F}_q$中进行运算。

(3) 算法 6 还需要进行与整除链相关的计算。具体来说，我们需要计算形如 $\phi_{\gamma_i}(x_i)$ 的元素，其中 γ_i 构成一条整除链。我们尚未找到一种能够利用这条整除链显著改善最坏情况复杂度的方法，例如

对于任意两个 i，j，若 $i<j$，已知 $\phi_{\gamma_i}(x_i)$、γ_j/γ_i 和 x_j，并非先验地有助于求出 $\phi_{\gamma_j}(x_j)$。无论这些问题是否应用于 Drinfeld 模，进一步研究都是必要的。特别是，在某些情况下，概率方法可能会有所帮助，例如不变因子较为光滑时。

（4）4.2 节的方法也留下了一些未解问题。假设 A给定为 $\mathbb{F}_q[T_1,\dots,T_m]$ 的商，使得能够使用 Gr¨obner 基技术来计算 $\ker_K(u)$ 的不变因子。探索并实现这一方向或许是有价值的。

最后，我们思考有限域的使用。这是大多数实际应用的场景，例如计算机代数 [DNS21； BMZ25] 以及编码理论 [BDM24； MP26]）。如果 ϕ 是有限域 K 上的 Drinfeld 模，那么无论在 $A=\mathbb{F}_q[T]$ 的情形下还是对于一般函数域，$\phi(K)$ 都是有限生成的。我们可以利用 A 作为有限生成 $\mathbb{F}_q$-代数的结构，并使用矩阵编码生成元的作用。对于椭圆曲线而言，这是不可能的，因为 A 所扮演的角色由 $\mathbb{Z}$ 承担。如果基域 K 是函数域，那么模$\phi(K)$ 不是有限生成的，其非挠点部分是秩为无限的自由模 $\aleph_0$[Poo95]。正如 Caruso 告知我们的那样，挠子部分已知是有限的[Pap23，《定理 6.4》3]。Anderson 动机很可能是计算这些挠点的重要工具。即使在无限情形下（但经过适当的变量变换），它们也能将同源表示为一个有限的方多项式矩阵，其余核同构于该同源的核。只需计算该矩阵的史密斯标准形，即可得到余核的不变因子。对于有限域，由于多项式矩阵的运算代价高昂，这一策略通常不如我们的方法高效。然而在一般情形下，Anderson 动机通过将问题化归为经典计算机代数而简化了问题。存在一个次数最小的首一可分同源，其核是 $\phi(K)$ 的挠子部分；寻找这一同源是未来的工作。

致谢

我们衷心感谢 Xavier Caruso 富有启发性的讨论。Antoine Leudi`ère 的部分研究经费由太平洋数学科学研究所提供。Renate Scheidler 获得加拿大自然科学与工程研究委员会（NSERC）资助，项目编号为 RGPIN-2025-03992。

参考文献

[And86] Greg W. Anderson. “t-动机”。载于：《杜克数学杂志》53.2 (1986年), 第 457–502 页。doi: 10.1215/S0012-7094-86-05328-7.[Arm+25] C´ecile Armana, Elena Berardini, Xavier Caruso, Antoine Leudi`ere,Jade Nardi, 和 Fabien Pazuki. “Drinfeld 模的计算方法”。2025年。url: https://hal.science/hal-05423892.[Ayo+23] David Ayotte, Xavier Caruso, Antoine Leudi`ere, 和 Joseph Musleh. “SageMath 中的 Drinfeld 模”。载于：*ACM* 计算与代数通讯57.2 (2023年), 第 65–71 页。doi: 10.1145/3614408.3614417.[BDM24] Luca Bastioni, Mohamed O. Darwish, 和 Giacomo Micheli. 基于 *Drinfeld* 模的最优秩度量码与秩局部性。2024年。doi: 10.48550/arXiv.2407.06081。

[BMZ25] Luca Bastioni, Giacomo Micheli, 和 Shujun Zhao. 线性化多项式的特征多项式。2025年。doi: 10.48550/arXiv.2506.16937.[Car18] Perlas Caranay. “秩二 Drinfeld 模的同源火山计算”。博士论文。卡尔加里大学，2018年。[CGS20] Perlas Caranay, Matthew Greenberg, 和 Renate Scheidler. “有限域上秩二 Drinfeld 模的模多项式与同源计算”。载于：《当代数学》754 (2020年)。编者：Susanne Brenner, Igor Shparlinski, Chi-Wang Shu, 和 Daniel Szyld, 第 283–313 页。doi: 10.1090/conm/754/15148.[CL17a] Xavier Caruso 和 J´er´emy Le Borgne. “有限域上斜多项式因式分解的一种更快新算法”。载于：《符号计算杂志》79 (2017年), 第 411–443 页。doi: 10.1016/j.jsc.2016.02.016.[CL17b] Xavier Caruso 和 J´er´emy Le Borgne. “斜多项式快速乘法”。载于：2017 年 ACM 符号与代数计算国际研讨会论文集。ISSAC ’17。计算机协会，2017年，第 77–84 页。doi: 10.1145/3087604.3087617.[CL26] Xavier Caruso 和 Antoine Leudi`ere. “一般 Drinfeld 模上范数与特征多项式的计算算法”。载于：《计算数学》95.357 (2026年)。doi: 10.1090/mcom/4052.[DNS21] Javad Doliskani, Anand Kumar Narayanan, 和 ´Eric Schost. “具有复乘的 Drinfeld 模、Hasse 不变量及有限域上的多项式因式分解”。载于：《符号计算杂志》。MICA 2016 105 (2021年), 第 199–213 页。doi: 10.1016/j.jsc.2020.06.007.[Dri77] Vladimir G. Drinfel’d. “某些非交换环的交换子环”。载于：《泛函分析及其应用》11.1 (1977年), 第 9–12 页。doi: 10.1007/BF01135527.[Fit36] Hans Fitting. “模的行列式理想”。载于：《德国数学家协会年报》46 (1936年), 第 195–228 页。url:http://eudml.org/doc/146122.[GG13] Joachim von zur Gathen 和 J¨urgen Gerhard. 《现代计算机代数》。第 3 版。剑桥大学出版社，2013年。doi: 10.1017/CBO9781139856065.[Gop83] Valerii Denisovich Goppa. “代数几何码”。载于：苏联数学—消息 21.1 (1983年), 第 75–91 页。doi: 10.1070/IM1983v021n01ABEH001641.[Hei04] Gert-Jan van der Heiden. “Drinfeld 模的 Weil 配对”。载于：数学月刊 143.2 (2004年), 第 115–143 页。doi: 10.1007/s00605-004-0261-4.[HHL17] David Harvey, Joris Van Der Hoeven, 和 Gr´egoire Lecerf. “有限域上的快速多项式乘法”。载于：《ACM 杂志》63.6 (2017年1月)。doi: 10.1145/3005344。

[Hor19] William George Horner. “用连续逼近求解各阶数值方程的新方法”. 载于: Philosophical Transactions of the Royal Society of London 109（1819年12月）, 第308–335页. doi:10.1098/rstl.1819.0023.[IMH82] Oscar H Ibarra、Shlomo Moran 与 Roger Hui. “快速 LUP 矩阵分解算法的推广及其应用”. 载于: 《算法杂志》3.1（1982年）, 第45–56页. doi: 10.1016/0196-6774(82)90007-4.[KU11] Kiran S. Kedlaya 与 Christopher Umans. “快速多项式因式分解与模复合”. 载于: 《SIAM 计算杂志》 40.6 （2011 年）, 第 1767–1802 页 . doi: 10.1137/08073408X.[Laf01] Laurent Lafforgue. “Drinfeld 的 chtoucas 与朗兰兹对应”. 载于: 《数学新进展》147（2001年）, 第1–241页. doi: 10.1007/s002220100174.[LS24] Antoine Leudi`ere 与 Pierre-Jean Spaenlehauer. “由虚超椭圆函数域的类域论计算群作用”. 载于: J. Symbolic Comput. 125（2024年）, 论文编号 102311, 19页. doi:10.1016/j.jsc.2024.102311.[MP26] Giacomo Micheli 与 MihranPapikian. 来自 Drinfeld 模的秩度量码. 2026年. url: https://arxiv.org/abs/2601.03653v1.[MS23] Yossef Musleh 与 ´Eric Schost. “利用晶体上同调计算有限 Drinfeld 模自同态的特征多项式”. 载于: 2023年国际符号与代数计算研讨会论文集. ISSAC ’23. 美国计算机协会, 2023年, 第461–469页. doi: 10.1145/3597066.3597080.[Pap23] Mihran Papikian. Drinfeld 模. 第296卷. 数学研究生教材. 施普林格国际出版公司, 2023年. doi: 10.1007/978-3-031-19707-9.[Poo95] Bjorn Poonen. “Drinfeld 模的局部高度函数与莫德尔-韦伊定理”. 载于: 《数学汇刊》97.3（1995年）, 第349–368页.[PS73] Michael S. Paterson 与 Larry J. Stockmeyer. “关于计算多项式所需的非标量乘法次数”. 载于: 《SIAM 计算杂志》（1973年）. 出版者: 工业与应用数学学会. doi: 10.1137/0202007.[Sca01] Thomas Scanlon. “基于 Drinfeld 模的公钥密码系统是不安全的”. 载于: 《密码学杂志》14.4（2001年）, 第225–230页. doi: 10.1007/s00145-001-0004-9.[Sta26] Stacks 项目作者. Stacks 项目. https://stacks.math.columbia.edu. 2026年.[Sto00] Arne Storjohann. “矩阵典范形的算法”. 博士论文. 苏黎世联邦理工学院, 2000年. url: https://doi.org/10.3929/ethz-a-004141007.[Sut11] Andrew Sutherland. “有限阿贝尔 p-群中的结构计算与离散对数”. 载于: 《计算数学》80.273（2011年）, 第477–500页. doi: 10.1090/S0025-5718-10-02356-2.[The26] Sage 开发团队. SageMath, Sage 数学软件系统（版本 10.8）. https://www.sagemath.org. 2026年.

卡尔加里大学电子邮箱地址:
antoine.leudiere@ucalgary.ca电子邮箱地址:
rscheidl@ucalgary.ca卡尔加里大学