# 利用晶体上同调计算有限 Drinfeld 模自同态的特征多项式

YOSSEF MUSLEH, Cheriton 计算机科学学院，滑铁卢大学，加拿大ÉRIC SCHOST, Cheriton 计算机科学学院，滑铁卢大学，加拿大

arXiv:2302.08611v1 [cs.SC] 16 Feb 2023

我们提出一种新算法，利用有限 Drinfeld 模所关联的晶体上同调，计算其任意自同态的特征多项式。我们的方法受到 Kedlaya 的 $p$-进算法的启发，该算法利用 Monsky-Washnitzer 上同调计算超椭圆曲线上 Frobenius 端同态的特征多项式。对于 Frobenius 端同态这一特定情形，我们采用大步小步算法对该方法进行专门化，并在此情形下给出复杂度分析，证明其渐近性能优于以往的方法。

CCS 概念： • **计算方法** → **符号与代数算法**。

补充关键词和短语：Drinfeld 模；算法；复杂度。

## 1 引言

Drinfeld 模最初由 Vladimir Drinfel'd 引入，用以证明全局函数域 [11] 上的 GL$_n$ 朗兹猜想。此后，由于椭圆曲线与秩二情形之间已有成熟的对应关系，Drinfeld 模受到了广泛关注。此外，秩一情形通常称为 *Carlitz* 模，它为分圆扩张提供了函数域类比；椭圆曲线上的复乘在数域类域论中所发挥的作用，与秩二 Drinfeld 模在函数域情形中的作用有着明显的相似之处。这促使人们尝试将椭圆曲线上的构造和算法推广过来，包括模多项式 [6], 、同源 [6], 以及自同态环 [13, 27]。

自然，人们也研究了 Drinfeld 模在密码学中的应用 [28], ，但长期以来，人们认为基于同源 [23, 36] 的公钥密码学容易受到攻击。Wesolowski 最终解决了这一问题，他证明了任意秩 Drinfeld 模之间的同源都可以在多项式时间内计算 [38]。

秩为 $r > 2$ 的 Drinfeld 模并没有如此明确的对应关系，尽管阿贝尔曲面与所谓的 $t$-模之间存在一种类比 [1]。由于这种差异，秩二 Drinfeld 模的研究远比一般秩的情形深入。

本文的主要目标是研究 Drinfeld 模中与 $p$-进方法类似的技术，例如 Kedlaya 的算法 [25] ，用于计算有限域上椭圆曲线或超椭圆曲线上 Frobenius 端同态的特征多项式。针对椭圆曲线的算法，会计算 Frobenius 在曲线的特征零提升的德拉姆上同调某个特定子空间的一组基上的作用，其系数取自 $\mathbb{Q}_p$。我们的方法遵循非常相似的思路，但事实证明，描述起来要简单得多；其关键在于采用 Gekeler 和 Anglès 提出的适用于 Drinfeld 模的晶体上同调版本 [2]。

更一般地，我们提出的方法可用于计算任意 Drinfeld 模的端同态的特征多项式。

## 2 背景与主要结果

### 2.1 基本预备知识

设 $R$ 为任意环，$r \in R$，且 $\sigma\colon R \to R$，为一个环同态。在本文中，我们始终遵循如下记号约定：写作 $\sigma(r) = \sigma r = r^{\sigma}$。若 $R$ 为多项式环，且 $\sigma$ 作用于其系数环，则 $r^{\sigma}$ 表示逐系数应用。

设 $q$ 为一个素数幂，并令 $\mathbb{F}_q$ 表示一个阶为 $q$ 的有限域，全文均固定此域。我们还固定一个 $\mathbb{F}_q$ 的域扩张 $\mathbb{L}$，使得 $[\mathbb{L}\colon \mathbb{F}_q] = n$。具体而言，对某个次数为 $n$ 的不可约 $\ell(t) \in \mathbb{F}_q[t]$，定义 $\mathbb{L} = \mathbb{L} = \mathbb{F}_q[t]/(\ell(t))$，因此 $\mathbb{L}$ 中的元素可表示为 $\mathbb{F}_q[t]$ 中次数小于 $n$ 的多项式。下文将讨论一种更适用于某些计算的替代表述。

### 2.2 Drinfeld 模

一般而言，Drinfeld 模可以定义在环 $A$ 上，该环由射影曲线上的函数构成，这些函数定义在 $\mathbb{F}_q$ 上，并且在无穷远处的一个固定点之外正则。就本文而言，我们仅考虑定义在 $\mathbb{P}^1 - \{\infty\}$ 的正则函数环上的 Drinfeld 模；也就是说，$A = \mathbb{F}_q[x]$。

我们固定一个环同态 $\gamma\colon A \to \mathbb{L}$，并令 $\mathfrak{p} \in A$ 为 $\ker\gamma$ 的首一不可约生成元。于是 $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_q[x]/(\mathfrak{p})$ 同构于 $\mathbb{L}$的一个子域；令 $m = \deg(\mathfrak{p})$，从而 $m$ 整除 $n$。这给出了一个同构$\mathbb{L} \simeq \mathbb{F}_q[x,t]/(\mathfrak{p}(x)\ g(x,\ t))$，其中 $g$是 $t$ 中次数为 $n/m$的首一多项式。有时，将 $\mathbb{L}$ 中的元素表示为 $t$ 上的一元多项式，切换为相应的 $x$，$t$二元表示会很方便；例如，此时 $\gamma_x$就是 $x$模 $(\mathfrak{p}(x)\ g(x,\ t))$ 的剩余类。我们假设 $\mathfrak{p}$和 $g$作为输入的一部分给出。

为了定义 Drinfeld 模，我们还必须引入斜多项式环 $\mathbb{L}\{\tau\}$，即

$$\mathbb{L}\{\tau\} = \{U = u_0 + u_1\tau + \cdots + u_s\tau^s \mid s \in \mathbb{N}, u_0, \ldots, u_s \in \mathbb{L}\},$$

其中乘法由关系 $\tau u = u^q\tau$诱导，对所有 $u \in \mathbb{L}$均成立。

定义 1. 一个秩为 $r$ 的Drinfeld $A$模 定义在 *over* $(\mathbb{L}, \gamma)$ 上，是一个环同态 $\phi\colon A \to \mathbb{L}\{\tau\}$，满足

$$\phi_x = \gamma_x + \Delta_1\tau^1 + \ldots + \Delta_r\tau^r$$

其中 $\Delta_i$ 属于 $\mathbb{L}$，对所有 $i$和 $\Delta_r \neq 0$均成立。

对于希望了解 Drinfeld 模通常定义时所处的更一般情形的读者，我们推荐阅读 Deligne 和 Husemöller 在 [9] 中撰写的综述。

当 $\mathbb{L} \cong \mathbb{F}_{\mathfrak{p}}$（即 $m = n$）时，Drinfeld 模定义在素域上。素域情形下 Drinfeld 模的算法往往在算法上更简单，我们也会经常强调它与更一般情形之间的区别。

例 1. 设 $\mathbb{F}_q = \mathbb{Z}/5\mathbb{Z}$且 $n = 4$。令 $\ell(t) = t^4 + tx^2 + 4t + 2$，并令 $\mathbb{L} = \mathbb{F}_5[t]/(\ell(t))$。令 $\gamma_x = t$模 $\ell(t)$，此时 $\mathbb{L} = \mathbb{F}_{\mathfrak{p}}$。一个二阶 *Drinfeld* 模由 $\phi_x = \tau^2 + \tau + t$ 给出。

我们也可以改为取 $\gamma_x = t^3 + t^2 + t + 3$模 $\ell(t)$，此时 $\mathfrak{p} = x^2 + 4x + 2$且 $\mathbb{F}_{\mathfrak{p}} \cong \mathbb{F}_{25}$。域 $\mathbb{L}$具有如下表示

$$\mathbb{L} = \mathbb{F}_5[t]/(\ell(t)) \simeq \mathbb{F}_5[x,t]/(\mathfrak{p}(x), g(x,t)),$$

其中 $g(x,t) = t^2 + 4tx + 3t + x$。给定一个三阶 *Drinfeld* 模 $\phi_x = \tau^3 + (t^3+1)\tau^2 + t\tau + t^3 + t^2 + t + 3$。

给定定义在（$\mathbb{L}$，$\gamma$）上的 Drinfeld $A$-模 $\phi$，$\psi$，$\mathbb{L}$-态射 $u\colon \phi \to \psi$ 是一个 $u \in \mathbb{L}\{\tau\}$，使得对所有 $a \in A$，$u\phi_a = \psi_a u$ 都成立。集合 $\mathrm{End}_{\mathbb{L}}(\phi)$ 是 $\mathbb{L}$-态射 $\phi \to \phi$ 的集合；因此，它是 $\mathbb{L}\{\tau\}$ 中 $\phi_x$ 的中心化子。它具有自然的环结构，并且包含 *Frobenius* 端同态 $\tau^n$。

### 2.3 特征多项式

特征 多项式 of an endomorphism $u \in \mathrm{End}_{\mathbb{L}}(\phi)$ can be defined through several points of view .

通过 $\phi$ 的作用，$A = \mathbb{F}_q[x]$ 及其分式域 $K = \mathbb{F}_q(x)$ 可分别视为斜分式域 $\mathbb{L}(\tau)$（$\mathbb{L}\{\tau\}$ 的斜分式域）中的子环和子域。于是，$\mathrm{End}^0_{\mathbb{L}}(\phi) = \mathrm{End}_{\mathbb{L}}(\phi) \otimes_A K$ 是 $\mathbb{L}(\tau)$ 中 $\phi_x$ 的中心化子；这是一个除环，其中心包含 $K$。

定义 2. $u$的特征多项式特征多项式($u$) 是相对于子域 $K$ 的约化特征多项式，其中 $u \in \mathrm{End}_{\mathbb{L}}(\phi)$ 见第 *9* 节 *[35,* 。

$u$的特征多项式的次数为 $r$，且系数属于 $A \subset K$，因此它属于 $A[Z]$。更准确地说，若 $\deg(u) = d$，则 CharPoly($u$) 的系数为 $a_0, \ldots, a_{r-1} \in A$，其中对所有 $i$ [27,，$\deg(a_i) \le d(r-i)/r$（命题 4.3]），并且满足

$$u^r + \sum_{i=0}^{r-1} \phi_{a_i} u^i = 0. \tag{1}$$

通过引入 $\phi$的*Tate* 模，可以得到 CharPoly($u$) 的另一种定义。Drinfeld 模 $\phi$在 $\mathbb{L}$ 的代数闭包 $\mathbb{L}$ 上诱导出一个 $A$-模结构，其定义为 $a * c = \phi_a(c)$，其中 $a \in A, c \in \mathbb{L}$（定义$\tau^i(c) = c^{q^i}$）。于是，对 $\mathfrak{I} \in A$，$\phi$的 $\mathfrak{I}$- 扭模定义为 $\phi[\mathfrak{I}] = \{c \in \overline{\mathbb{L}} \mid \mathfrak{I} * c = 0\}$。令 $\mathfrak{I}$ 为 $A$ 中异于 $\mathfrak{p}$ 的任一不可约元素，我们可以将 $\mathfrak{I}$- 进 Tate 模定义为 $T_{\mathfrak{I}}(\phi) = \varprojlim \phi[\mathfrak{I}^i]$。

令 $A_{\mathfrak{I}}$ 为 $A$ 的 $\mathfrak{I}$-进完备化，则 $T_{\mathfrak{I}}(\phi)$ 成为秩为 $r$ 的自由 $A_{\mathfrak{I}}$-模，而 $\mathrm{End}_{\mathbb{L}}(\phi)$ 中的元素会在 $T_{\mathfrak{I}}(\phi)$ 上诱导自同态。因此，对于 $u \in \mathrm{End}_{\mathbb{L}}(\phi)$，诱导自同态 $u \in \mathrm{End}_{A_{\mathfrak{I}}}(T_{\mathfrak{I}}(\phi))$ 的特征多项式 $\mathrm{CharPoly}^{A_{\mathfrak{I}}}(u)$ 与 CharPoly($u$) [2, 17] 一致。

例2. 设 $\mathbb{F}_q$、$\mathbb{L}$ 与例 *1* 的背景中所述相同，且 $\gamma_x = t^3 + 4t^2 + t + 1$模 $\ell(t)$。一个秩 *5 Drinfeld* 模由 $\phi_x = (4t^3 + t^2 + 2)\tau^5 + (t^3 + 3t^2 + t + 1)\tau^4 + (4t + 3)\tau^3 + (3t^2 + 4t + 4)\tau^2 + (4t^3 + 4t^2 + 4t)\tau + \gamma_x$ 给出。

$\tau^n$ 在 $\phi$ 上的特征多项式为 $Z^5 + 3Z^4 +$ （$x^3 + 4x^2 + x$）$Z^3 +$ （$2x^2 + 4x + 3$）$Z^2 +$ （$x^3 + 2x^2 + 4x + 2$）$Z$ $+2x^4 + 3x^2 + 4x + 2$

本文的结果基于对 CharPoly($u$) 的另一种诠释，即将其视为由 Gekeler 和 Anglès [2]提出的、由 $u$ 在某个晶体上同调 模上诱导的自同态的特征多项式。我们的第一个主要结果是一个计算 Frobenius 端同态特征多项式的算法。

这里，$\omega$是一个实数，使得环 $R$上的两个 $s \times s$矩阵可以在 $R$中通过 $O(s^\omega)$ 次环运算完成矩阵乘法；目前的最佳值为 $\omega \le 2.372$ [12]。我们还令 $\lambda$ 表示这样一个指数：环 $R$ 上的 $s \times s$ 矩阵的特征多项式可以在 $R$中通过 $O(s^\lambda)$ 次环运算计算得到。当 $R$ 为域时，其代价相当于矩阵乘法，因此为 $\lambda = \omega$ [32]。对于更一般的环，迄今已知的最佳值为$\lambda \approx 2.7$ [24]。

定理 1。 设 $\phi$ 是定义在 $(\mathbb{L}, \gamma)$ 上的秩为 $r$ 的 *Drinfeld* 模。存在一种确定性算法，可以计算 *Frobenius* 端同态 $\tau^n$ 的特征多项式，其比特复杂度为

- $(r^\omega n^{1.5}$对数 $q + n$对数$^2 q)^{1+o(1)}$针对素域情形 *($m = n$)*

- $((r^\lambda/m + r^\omega/\sqrt{m})n^2 \log q + n\log^2 q)^{1+o(1)}$ 对于一般情形 $m < n$。

当 $r$ 和 $q$ 固定时，定理中的运行时间本质上与 $n^2/\sqrt{m}$ 呈线性关系；在素域情形下为 $n^{1.5}$，并且随着 $m$ 减小，逐渐接近 $n^2$。此前最好的结果 [30] 仅适用于 $r = 2$ 的情形：在素域情形下，运行时间本质上与 $n^{1.5}$ 呈线性关系；其他情形下则与 $n^2$ 呈线性关系（$q$ 固定时）。

这一算法建立在源自 [10], 的线性递推技术之上，而这些技术迄今仅适用于 Frobenius 自同态这一特殊情形。

我们还得到了两种可应用于任意 $u \in \mathrm{End}_{\mathbb{L}}(\phi)$ 的算法。在这种情况下，复杂度部分取决于 $\mathbb{L}\{\tau\}$ 中乘法和欧几里得除法的复杂度，我们将其记为 $\mathrm{SM}(d,\ n,\ q)$，并将在第 3 节中更详细地讨论。

定理 2。 在定理 *1* 的假设下，存在确定性算法，可以计算次数为 $d$ 的自同态 $u$ 的特征多项式，其位复杂度为

- $\left(\min(dr^2,\ (d+r)r^{\omega-1})\, m\ (d+m)\ n\log q + r^\lambda n\ (d+m)\ /m\log\ q + n\log^2 q\right)^{1+o(1)}$
- $(r\mathrm{SM}(d+r,\ n,\ q)\ + r^\lambda n(d+m)/m\log\ q + n\log^2 q)^{1+o(1)}$。

同样，值得考虑固定 $r$ 和 $q$ 的情形。在这种情况下，我们得到的运行时间分别与 $d(d+m)n/m$ 和 $\mathrm{SM}(d,n,q)$ 基本呈线性关系。下一节中，我们将回顾SM的已知取值；对于 $\omega$ 的最佳已知取值，在固定 $q$ 时，当 $d \le n^{0.76}$ 时为 $(d^{1.69}n)^{1+o(1)}$，否则为 $(dn^{1.52})^{1+o(1)}$。因此，在 $d = \Theta(n)$ 的情况下，运行时间分别与 $n^3/m$ 和 $n^{2.53}$ 基本呈线性关系（所以哪种算法更优取决于 $m$ 的取值）。对于 $u = \tau^n$，前一定理中的算法显然更优。

## 3 计算预备知识

$\mathbb{L}$ 中复杂度分析的关键在于以下运算的成本：加法/减法、乘法、求逆以及（迭代的）Frobenius 映射。

我们在下文使用的一些算法（$\mathbb{L}\{\tau\}$ 中的乘法和欧几里得除法，来自 [7, 34]）假设所有这些运算都可以在 $\mathbb{F}_q$ 中使用 $\tilde{O}(n)$ 次运算完成。然而，对于我们所使用的 $\mathbb{L}$ 表示，目前尚不知晓是否如此；Couveignes 和 Lercier 证明了满足这些要求的“椭圆基”存在 [8],，但将其转换为我们的表示形式似乎并不简单。

这解释了为什么在我们的主要结果中，我们不计算 $\mathbb{F}_q$ 中的运算次数，而是计算位运算次数（我们的复杂度模型是标准的随机存取机）；下文将解释这如何使我们能够绕过上述限制。

利用基于快速傅里叶变换的算法，次数至多为 $n$ 且系数属于 $\mathbb{F}_q$ 的多项式可以在布尔时间 $(n\log q)^{1+o(1)}$ [5, 20] 内完成乘法。由此可知，在 $\mathbb{L} = \mathbb{F}_q[t]/(\ell(t))$ 中，基本域运算（加法、乘法、求逆）也可以以相同的渐近成本完成。

在 $\mathbb{L}$ 的元素的单变量表示与二元表示之间进行转换，渐近运行时间相同。记 $\alpha$ 为同构 $\mathbb{L} = \mathbb{F}_q[t]/(\ell(t)) \to \mathbb{F}_q[x,t]/(\mathfrak{p}(x)\ g(x,\ t))$；那么，给定 $\mathbb{F}_q[t]$ 中次数小于 $n$ 的 $f$，我们可以用 $(n\log q)^{1+o(1)}$ 次位运算计算其像 $\alpha(f \bmod \ell(t))$；$\alpha^{-1}$ [22, 33] 也同样如此。

最后一个重要操作是在 $\mathbb{L}$ 中应用 $q$-次 Frobenius。回顾一下，给定次数至多为 $n$ 的多项式 $f$、$g$、$h \in \mathbb{F}_q[x]$，模复合 是计算 $f(g) \bmod h$ 的操作。正如 [15], 中针对 $c \in \mathbb{L} = \mathbb{F}_q[t]/(\ell(t))$ 所展示的那样，$c^q$ 可以在与次数为 $n$ 的模复合相同的渐近时间内（忽略对数因子）计算得到，只需进行一次性预计算，该预计算需要 $(n\log^2 q)^{1+o(1)}$ 次位运算。由此可扩展至

Frobenius 的任意次幂（正次幂和负次幂）。需要指出的是，模复合技术也是上述在 $\mathbb{L}$ 中提到的两种元素表示法之间转换算法的基础。

在 [26], 中，Kedlaya 和 Umans 证明，对于次数为 $n$ 的情形，模复合可以在 $(n\log q)^{1+o}(1)$ 位运算中完成（另见 van der Hoeven 和 Lecerf 的改进结果 [22]），因此在 $\mathbb{L}$ 中计算 Frobenius（的迭代）也具有类似的成本。这里，采用布尔模型这一点至关重要：目前尚不清楚 Kedlaya 和 Umans 的算法能否用 $\mathbb{F}_q$ 运算来描述。

据此，我们可以直接将 [7, 34] 中的成本分析调整到布尔模型中。具体而言，遵循后者的参考文献（其采用的是代数成本模型），我们令 $\mathrm{SM}(d,n,q)$ 为一个满足以下条件的函数

- 次数为 $d$ 的乘法和右欧几里得除法，在 $\mathbb{L}\{\tau\}$ 中可通过 $O(\mathrm{SM}(d,n,q))$ 位运算完成
- 对于 $n,q$ 固定时，$\mathrm{SM}(d,n,q)/d$ 是非递减的。

后一条件类似于 [14], 中所用乘法函数的超线性，这将使我们能够简化一些复杂度分析。遗憾的是，$\mathrm{SM}(d,n,q)$ 没有简单的表达式：基于 [7, 34], 中的算法， [7] 中的分析给出了以下上界：

- 对于 $d \le n^{(5-\omega)/2}$，我们可以取 $\mathrm{SM}(d,n,q)$，其为 $(d^{(\omega+1)/2}n\log q)^{1+o}(1)$
- 否则，我们可以取 $\mathrm{SM}(d,n,q)$，其为 $(dn^{4/(5-\omega)}\log q)^{1+o}(1)$

例如，当 $d=n$ 时，这是 $(n^{(9-\omega)/(5-\omega)}\log q)^{1+o}(1)$。

对于 $\omega = 2.37$，当 $d \le n^{0.76}$ 时，代价为（$d^{1.69}n\log q$）$^{1+o}$（1），否则为（$dn^{1.52}\log q$）$^{1+o}$（1）；对于 $d=n$，指数为 2.53。为完整起见，我们指出，这些算法严重依赖 Frobenius 映射，因此需要承担此前提到的一次性代价（$n\log^2 q$）$^{1+o}$（1）。

还应注意，这些渐近代价分析并不能反映实际的运行时间。就作者所知，目前尚不存在达到其理论复杂度的 Kedlaya-Umans 算法软件实现，也不存在指数接近 2.37 的矩阵乘法软件实现。出于实际应用的目的，模复合的实现采用了 Brent 和 Kung 提出的算法 [4],，其代数复杂度为 $O(n^{(\omega+1)/2})$ 次运算，作用于 $\mathbb{F}_q$ 中。重新研究以这样的基为基础的斜多项式算法及其分析，是一项尚待完成的工作。

## 4 既有研究

仅针对秩二情形的特征多项式，尤其是 Frobenius 端同态的特征多项式的计算问题，已在 [18] 中得到详细研究。

最一般的方法是根据系数 $a_i = \sum_{j=0}^{n} {}^{r} a_{i_{(r-i)/,j}} x^j$ 的次数约束构造一个线性方程组。将特征多项式取值于弗罗贝尼乌斯元素，并比较各项系数，可得到一个基于

$$\tau^{nr} + \sum_{i=0}^{r-1} \sum_{j=0}^{\frac{n(r-i)}{r}} \sum_{k=0}^{n(r-i)} a_{i,j} f_{j,k} \tau^{k+ni} = 0, \tag{2}$$

其中 $f_{j,k}$ 是 $\phi_{x^j}$ 的系数。令 $\mathrm{MinPoly}(\tau^n)$ 表示 $\tau^n$（作为除环 $\mathrm{End}^0_{\mathbb{L}}(\phi)$ 中的元素，其中该除环定义在域 $K=\mathbb{F}_q(x)$ 上）的最小多项式，则当且仅当 $\mathrm{MinPoly}(\tau^n) = \mathrm{CharPoly}(\tau^n)$ 时，前述方程组的解唯一，并给出特征多项式。

Garai 和 Papikian 提出了一种计算特征多项式的算法 [13, §5.1] ，但仅适用于素域情形。与前一种方法一样，该算法依赖于对 $\phi_{x^i}$ 的显式计算，这是主要的

计算步骤。这可以通过 $O(n^2)$ 次递推关系求值来完成

$$f_{i+1,j} = \gamma_x^{q^j} f_{i,j} + \sum_{t=1}^{r} \Delta_t^{q^{j-t}} f_{i,j-t}.$$

因此，计算所有 $\phi_x$、$\phi_{x^2}$、……、$\phi_{x^n}$的比特复杂度为 $(rn^3\log(q))^{1+o(1)}$。

对秩为 $r = 2$ 时 Frobenius 端同态这一特定情形的算法进行了进一步研究，见 [31]和 [30]。后者重点研究了算法的复杂度，并采用了本文将使用的相同计算模型。正如我们在定理 1 之后所述，截至目前已知的最佳运行时间为关于 $n$的二次复杂度；例外情况是 $\mathrm{MinPoly}(\tau^n) = \mathrm{CharPoly}(\tau^n)$，或素域情形，此时可以达到 $(n^{1.5}\log q + n\log^2 q)^{1+o(1)}$的比特代价[10]。据我们所知，此前尚无针对任意自同态的分析 $u$。

在椭圆曲线的背景下，Kedlaya 算法 [25] 以有限精度计算 Frobenius 作用提升到 Monsky-Washnitzer 上同调某个子空间上的矩阵表示的特征多项式。我们的算法遵循相同的总体思路：我们计算自同态在晶体上同调上的作用矩阵，其系数取自一种与 Witt 向量相对应的幂级数环。事实证明，诱导的自同态可以通过斜多项式乘法相当简洁地描述，从而无需进行复杂的提升步骤。

## 5 晶体上同调

本节首先回顾 Drinfeld 模的晶体上同调的构造及其主要性质；相关内容可见于 [2],，其中该定义被归功于 Gekeler 未发表的工作。随后，我们引入这些对象的截断版本，将 Drinfeld 模的自同态的特征多项式计算，归约为截断幂级数环上矩阵的特征多项式计算。

### 5.1 定义

本小节的内容取自 [2, 16]。Drinfeld 模 $\phi$的导子 $D(\phi, \mathbb{L})$的集合，是满足如下关系的 $\mathbb{F}_q$-线性映射 $\eta$：$A \to \mathbb{L}\{\tau\}\tau$ 的集合：

$$\eta_{ab} = \gamma_a\eta_b + \eta_a\phi_b, \quad a, b \in A$$

令 $y$为一个新变量。集合 $D(\phi, \mathbb{L})$ 可以按如下方式构成一个 $\mathbb{L}[y]$-模。

定义 3。 *[2,*第 *2]* 节集合 $D(\phi, \mathbb{L})$ 在 $(cy^i * \eta)_a = c\eta_a\phi_{x^i}$作用下构成一个 $\mathbb{L}[y]$-模，其中 $\eta$属于 $D(\phi, \mathbb{L})$， $c$属于 $\mathbb{L}$、$i \geq 0$，且 $a$属于 $A$。

进一步令 $I$为由 $y - \gamma_x$生成的 $\mathbb{L}[y]$的理想；对于 $k \geq 1$，我们设

$$W_k = \mathbb{L}[y]/I^k$$

and

$$W = \varprojlim W_k \cong \mathbb{L}[[y - \gamma_x]].$$

因此 $W$附带投影 $\pi_k$： $W \to W_k$，它们通过截断一个幂级数得到；该幂级数表示为关于 $(y - \gamma_x)$ 的幂次之和，次数为 $k$。我们有典范环同态 $\iota_k$： $A \to W_k$，由 $\iota_k(x) = y \bmod I^k$ 给出。它们提升为包含映射 $\iota$： $A \to W$，并且同时与每个 $\pi_k$交换；后者通过$I$-进展开表示 $A$的元素。

$H^*$晶体上同调 crys($\phi$, $\mathbb{L}$) 是 $\phi$ 的 $W$-模 $W \otimes_{\mathbb{L}[y]} D(\phi, \mathbb{L})$，也就是 $\mathbb{L}[y]$ 在理想 $I = (y - \gamma_x)$ 处的 $D(\phi, \mathbb{L})$ 的完备化。

Gekeler 证明了 $D(\phi, \mathbb{L})$ 是一个射影因而也是自由的 $\mathbb{L}[y]$-模，其秩为 $r$ [16]，并且具有典范基 $\hat{\eta}_{(i)}$，满足 $\hat{\eta}_{(i)}(x) = \tau^i$，其中 $1 \le i \le r$。由此可知，正如 [2] 中所指出的，$H^*\mathrm{crys}(\phi, \mathbb{L})$ 也是一个秩为 $r$ 的自由 $W$-模。

注 1. 在该文献中，$A$ 不一定是多项式环，并且 $\mathbb{L}[y]$ 被 $A_{\mathbb{L}} := \mathbb{L} \otimes_{\mathbb{F}_q} \mathbb{A}$ 取代。在这种情况下，$D(\phi, \mathbb{L})$ 是一个秩为 $r$ 的射影 $A_{\mathbb{L}}$- 模，理想 $I$ 的定义有所变化，但它在 $A_{\mathbb{L}}$ 中仍为极大理想，因此 $A_{\mathbb{L}}$ 在 $I$ 处的完备化 $W$ 仍是一个局部环，而 $H^*\mathrm{crys}(\phi, \mathbb{L})$ 仍是一个在 $W$ 上秩为 $r$ 的自由模。

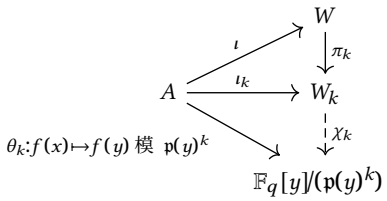
自同态 $u$ of $\phi$ 诱导出一个 $\mathbb{L}[y]$-自同态 $u^*$ of $D(\phi, \mathbb{L})$，定义为 $(u^*(\eta))_x = \eta_x u$，其中 $\eta$ 属于 $D(\phi, \mathbb{L})$；对于完备化 $H^*\mathrm{crys}(\phi, \mathbb{L})$，同样成立。根据 [2],，利用 $H^*\mathrm{crys}(\phi, \mathbb{L})$ 是 $W$ 上的自由模这一事实，可以按照通常方式定义特征多项式 $\mathrm{CharPoly}_W(u^*)$。

现在回顾一下，$\mathrm{CharPoly}(u)$ 表示 $u$ 的特征多项式，其定义见第 2.3 节。以下由 Anglès 提出的定理 [2, Thm. 3.2]，将该特征多项式与诱导自同态在 $H^*\mathrm{crys}(\phi, \mathbb{L})$ 上的特征多项式联系起来，其中 $\iota$ 在下文中逐系数作用。

定理 3. 对于 $u$ 属于 $\mathrm{End}_{\mathbb{L}}(\phi)$，$\mathrm{CharPoly}(u)^\iota = \mathrm{CharPoly}_W(u^*)$。

**5.2 截断上同调**

现在回忆一下，$\mathfrak{p} \in A$ 是 $\mathbb{F}_q$上的 $\gamma_x \in \mathbb{L}$ 的最小多项式。对于 $k \ge 1$，我们将定义一个 $\mathbb{F}_q$-线性同态 $\chi_k$，使得下图交换：




存在一个同构

$$T_k : \mathbb{F}_q[x, y]/(\mathfrak{p}(x), (y - x)^k) \to \mathbb{F}_q[y]/(\mathfrak{p}(y)^k);$$

例如参见 [29, 引理 13]。另一方面，回忆一下，$\mathbb{L} = \mathbb{F}_q[t]/(\ell(t))$同构于

$$\mathbb{F}_q[x, t]/(\mathfrak{p}(x), g(x, t)),$$

对于某个 $g$，它属于 $\mathbb{F}_q[x, t]$，且在 $t$ 中是次数为 $n/m$ 的首一元素；在 $\mathbb{L}$ 的这种表示中，$\gamma_x$ 就是 $x$（的剩余类）。由此，我们得到

$$\begin{aligned} W_k &= \mathbb{F}_q[t, y]/(\ell(t), (y - \gamma_x)^k) \\ &\simeq \mathbb{F}_q[x, t, y]/(\mathfrak{p}(x), g(x, t), (y - x)^k) \\ &\simeq \mathbb{F}_q[y, t]/(\mathfrak{p}(y)^k, G_k(y, t)), \end{aligned} \tag{3}$$

对于某个多项式 $G_k \in \mathbb{F}_q[y, t]$，它在 $t$ 中是次数为 $n/m$ 的首一多项式。

于是我们可以定义 $\chi_k$： $W_k \to \mathbb{F}_q[y]/(\mathfrak{p}(y)^k)$，定义如下：

$$\chi_k : \sum_{0 \le i < n/m} c_i t^i \mapsto c_0,$$

并且我们验证它满足我们的论断。第 6 节讨论了如何计算这个同态的具体细节。对于 $k \ge 1$，我们进一步将精度 $k$上同调空间 $H_k^*(\phi, \mathbb{L})$ 定义为 $W_k$-模

$$D(\phi,\mathbb{L})/I^k\, D(\phi,\mathbb{L}) \simeq H^*_{\mathrm{crys}}(\phi,\mathbb{L})/I^k\, H^*_{\mathrm{crys}}(\phi,\mathbb{L}).$$

I因此，t 是秩为 $r$ 的自由模，而 $u$ 的自同态会诱导 $H_k^*(\phi, \mathbb{L}$ 上的 $W_k$-线性自同态 $u_k^*$ ).

注2. 在 *[16],* 中，*Gekeler* 引入了 *Drinfeld* 模的 德拉姆上同调； 本构造中的 $k = 1$ 情形即为此例（此时 $W_k = \mathbb{L}$）。

在以下论断中，回顾一下，对于多项式 $P$ 以及作用于其系数环上的任意映射 $\chi$，我们用 $P^\chi$ 表示将 $\chi$ 逐系数应用于 $P$。

推论 4. 对于 $u$ 在 $\mathrm{End}_{\mathbb{L}}(\phi)$ 以及 $k \ge 1$， 特征多项式$(u)^{\theta_k}$ =特征多项式$_{W_k}(u_k^*)^{\chi_k}$。

证明。将 $\chi_k \circ \pi_k$ 逐系数作用于定理 3 中的等式。 □

如果 $u$在 $\tau$中的次数为 $d$，我们知道 CharPoly($u$) 的所有系数的次数至多为 $d$，因此可以通过它们模 $\mathfrak{p}^k$ 的约化，在 $k = \lceil \frac{d+1}{m} \rceil \in O((d+m)/m)$ 中恢复这些系数。在素域情形下， $m = n$时，以及在特殊情形 $u = \tau^n$下，上述公式给出 $k = 2$，但我们可以改用 $k = 1$； 第6.4节将对此进行讨论。

Note 还要注意，如果我们取 $k = d + 1$，就无需考虑映射 $\chi_k$：在 $W_{d+1}$的表示上 as

$$W_{d+1} = \mathbb{F}_q[x,t,y]/(\mathfrak{p}(x), g(x,t), (y-x)^{d+1}),$$

对于次数至多为 $d$的 $f$， $\iota_k(f)$ 就是多项式 $f(y)$，因此我们可以直接从 $\iota_k(f)$ 中恢复 $f$。不过我们不会这样做，因为这会使 $k$ 增大。

## 6 主要算法

现在，我们将看到如何通过仅用斜多项式来重新表述前面的讨论，使其更加具体。求值映射 $\eta \mapsto \eta_x$给出一个加性双射 $D(\phi,\ \mathbb{L}) \to \mathbb{L}\{\tau\}\tau$。这使我们能够将 $\mathbb{L}[y]$-模结构从 $D(\phi,\ \mathbb{L})$ 转移到 $\mathbb{L}\{\tau\}\tau$：可以验证，它由 $(cy^i * \eta) = c\eta\phi_{x^i}$ 给出，其中 $\eta$属于 $\mathbb{L}\{\tau\}\tau$， $c$属于 $\mathbb{L}$，且 $i \ge 0$，并且 B $=(\tau, \ldots\ldots, \tau^r)$ 是 $\mathbb{L}\{\tau\}\tau$ 上的一个基，其中底环为 $\mathbb{L}[y]$。

此外，现在一个自同态 $u \in \mathrm{End}_{\mathbb{L}}(\phi)$ 会诱导出一个 $\mathbb{L}[y]$-线性自同态 $u\star$： $\mathbb{L}\{\tau\}\tau \to \mathbb{L}\{\tau\}\tau$，其定义很简单： $u\star(v) = vu$，其中 $v$属于 $\mathbb{L}\{\tau\}\tau$。模去理想 $I^k \subset \mathbb{L}[y]$后，我们用 $u\star_k$表示商模 $\mathbb{L}\{\tau\}\tau/I^k_{\mathbb{L}}\mathbb{L}\{\tau\}\tau \simeq H_k^*(\phi,\ \mathbb{L})$ 上相应的 $W_k$- 线性自同态。

接下来，我们可以概述定理 1 和定理 2 中提到的算法；其正确性可直接由推论 4 和此前给出的 $k$ 界推出。

(1) 取 $k = \lceil \frac{d+1}{m} \rceil$，使得 $d = \deg_\tau(u)$，但若 $n = m$ and $u = \tau^n$，则可取 $k = 1$。(2) 在基 B 上，计算 $i = 1, \ldots, r$ 对 $\tau^i u \bmod I^k$ 的作用所对应的系数 $u_{i,}1, \ldots, u_{i,r} \in W_k$。(3) 使用步骤 2 中计算出的系数，构造 $u\star_k$ 在 $\mathbb{L}\{\tau\}\tau/I^k_{\mathbb{L}}\mathbb{L}\{\tau\}\tau$ 上作用的矩阵，并计算其特征多项式 $\mathrm{CharPoly}_{W_k}(u\star_k) \in W_k[Z]$。(4) 将映射 $\chi_k$ 应用于 $\mathrm{CharPoly}_{W_k}(u\star_k)$ 的系数，以求得 CharPoly$(u)^{\theta_k}$，从而得到 CharPoly($u$）。

在小节 6.1 至 6.3 中，我们讨论如何完成步骤 2：针对任意自同态 $u$，我们给出两种解决方案；针对 $u = \tau^n$，则给出一种专门且效率更高的方案。我们将使用以下记号：

- 对于 $\mathbb{L}$ 中的 $c$ 和 $t \in \mathbb{Z}$，令 $c^{[t]}$ 表示将第 $t$ 次幂 Frobenius 作用于 $c$ 所得的值，即 $c^{[t]} = c^{q^t}$
- 对于 $\mathbb{L}[y]$ 中的 $f$，$f^{[t]} \in \mathbb{L}[y]$ 是将前一个算子逐系数作用后得到的，因此 $\deg(f) = \deg(f^{[t]})$
- 对于 $\mathbb{L}[y]^{u\times v}$ 中的 $M = (m_{i,j})_{1\le i\le u,\ 1\le j\le v}$，$M^{[t]}$ 是一个矩阵，其元素为 $(m_i^{[t]},\ j)_{1\le i\le u,\ 1\le j\le v}$。

Fin另外，我们定义 $\mu = (y - \gamma_x)^k \in \mathbb{L}[y]$（其中 $k$ 的值如上所定义）；它生成了 $\mathbb{L}[y$ 中的理想 $I^k$ ].

### 6.1 使用递推关系

以下引理是 Gekeler 在 [19, 第 5] 节为 $r = 2$指出的递推关系的推广。回想一下，我们记作 $\phi_x = \gamma_x + \Delta_1\tau^1 + \ldots + \Delta_r\tau^r$，其中所有 $\Delta_i$ 都属于 $\mathbb{L}$；在下列表达式中，我们记作 $\Delta_0 = \gamma_x$。

引理 1. 对于任意 $t \ge 1$，以下关系在 $\mathbb{L}[y]$-模 $\mathbb{L}\{\tau\}\tau$ 中成立：

$$\sum_{i=0}^{r} \Delta_i^{[t]} \tau^{t+i} = y * \tau^t. \tag{4}$$

证明。由 $\mathbb{L}[y]$ 在 $\mathbb{L}\{\tau\}\tau$ 上的模作用可直接推出，只需将 $\tau^t$ 移过定义系数 $\Delta_i$（属于 $\phi$）：

$$y * \tau^t = \tau^t \phi_x = \tau^t \sum_{i=0}^{r} \Delta_i \tau^i = \sum_{i=0}^{r} \Delta_i^{[t]} \tau^{t+i}. \quad \square$$

对于 $i = 0, \ldots, r-1$，令 $\Lambda_i = -\frac{\Delta_i}{\Delta_r}$，并将递推关系的 $t$ 阶伴随矩阵定义为 $\mathrm{A}_t \in \mathbb{L}[y]^{r\times r}$：

$$\mathcal{A}_t = \begin{bmatrix} \Lambda_{r-1}^{[t]} & \Lambda_{r-2}^{[t]} & \ldots & \Lambda_1^{[t]} & \Lambda_0^{[t]} + \frac{y}{\Delta_r^{[t]}} \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{bmatrix} \tag{5}$$

对于 $t \ge 1$，令 $\kappa_t \in \mathbb{L}[y]^{1\times r}$ 表示 $\tau^t$ 相对于标准基 B 的系数向量。那么，我们有以下关于 $\mathbb{L}[y]$上的 $r \times r$ 矩阵的关系：

$$\begin{bmatrix} \kappa_{t+r} \\ \kappa_{t+r-1} \\ \vdots \\ \kappa_{t+1} \end{bmatrix} = \mathcal{A}_t \begin{bmatrix} \kappa_{t+r-1} \\ \kappa_{t+r-2} \\ \vdots \\ \kappa_t \end{bmatrix} \tag{6}$$

对于 $k \ge 1$，这些关系可以模 $\mu$ 化简，从而得到 $W_k = \mathbb{L}[y]/\mu$上的等式；下文中，我们将记作 $\bar{\kappa}_t = \kappa_t$ 模 $\mu \in W_k^{1\times r}$。

从 $\bar{\kappa}_t$，……，$\bar{\kappa}_{t+r-1}$出发，我们在 $\mathbb{L}$ 中使用 $O(r)$ 次运算（除法、Frobenius）来得到 $\mathrm{A}_t$ 第一行中出现的系数，随后在 $\mathbb{L}$ 中进行 $O(kr)$ 次运算，以推导出 $\bar{\kappa}_{t+r}$的各项。

下面，我们需要 $\bar{\kappa}_1$、……、$\bar{\kappa}_{d+r}$。总的来说，计算它们需要 $((d+r)krn\log q)^{1+o(1)}$位运算；使用我们为 $k$ 选定的值时，这也

$$((d+r)(d+m)rn/m\log q+)^{1+o(1)}.$$

接下来记作 $u = u_0 + \cdots + u_d\tau^d$。对于 $i = 1$、.....、 $r$，我们有

$$\tau^i u = u_0^{[i]}\tau_i + \cdots + u_d^{[i]}\tau^{d+i},$$

因此， $[u_{i,1}\cdots u_{i,\ r}] \in W_k$在基 B 上的 $\tau^i u \bmod I^k$ 的系数向量由以下乘积给出

$$[u_0^{[i]} \ \cdots \ u_d^{[i]}] \begin{bmatrix} \bar{\kappa}_i \\ \bar{\kappa}_{i+1} \\ \vdots \\ \bar{\kappa}_{i+d} \end{bmatrix} \in W_k^{1\times r}.$$

每个此类运算需要在 $\mathbb{L}$ 中进行 $O(dkrn)$ 次运算，因此，如果彼此独立执行，总共需要 $(d(d+m)r^2n/m\log\ q)^{1+o(1)}$ 次位运算（这是算法中的主要开销）。

当 $d$ 相较于 $r$ 不够小时，我们可以利用矩阵运算略微降低开销，因为所需的所有系数向量都可以从一个 $r\times(d+r)\times r$ 矩阵乘积中直接读取，

$$\begin{bmatrix} u_0^{[1]} & \cdots & u_d^{[1]} & 0 & \cdots & \cdots & 0 \\ 0 & u_0^{[2]} & \cdots & u_d^{[1]} & 0 & \cdots & 0 \\ & & \ddots & & \ddots & & \\ 0 & \cdots & \cdots & 0 & u_0^{[r]} & \cdots & u_d^{[r]} \end{bmatrix} \begin{bmatrix} \bar{\kappa}_1 \\ \bar{\kappa}_{i+1} \\ \vdots \\ \bar{\kappa}_{d+r} \end{bmatrix} \in W_k^{r\times r}.$$

这需要 $((d+r)(d+m)r^{\omega-1}n/m\log\ q)^{1+o(1)}$ 次位运算。

### 6.2 使用欧几里得除法

本节介绍一种计算自同态 $u$ 在典范基 B 上的系数的替代方法。计算在 $\mathbb{L}[y]$ 中进行，而非在 $W_k = \mathbb{L}[y]/\mu$ 中进行（在主要递归过程中，我们无法考虑模 $\mu$ 约化）。

该算法受到交换多项式 [14, 第 9 节2]中一个广为人知的类似结果的启发：对于一个次数为 $r$的固定 $a \in \mathbb{L}[y]$，我们可以将 $\mathbb{L}[y]$中的任意 $f$改写为 $f = \acute{\mathrm{I}}_{0\le i<r} f_i(a)y^i$，其中某些系数 $f_0$、.....、 $f_{r-1}$属于 $\mathbb{L}[y]$。这是通过分治方式完成的。

这种方法也适用于非交换情形。我们首先说明，如何将 $\mathbb{L}\{\tau\}$ 中次数为 $d$的 $f$改写为

$$f = \sum_i f_i\phi_x^i,$$

其中某个 $f_i$属于 $\mathbb{L}\{\tau\}$，且次数小于 $r$。若令 $K$满足 $d < Kr \le 2d$，其中 $K$是 2 的幂，则上式求和中的指标 $i$ 从 0 到 $K-1$。

如果 $K = 1$，我们就完成了。否则，令 $K\prime = K/2$，并通过右欧几里得除法计算 $f$ 除以 $\phi_x^{K'}$ 所得的商 $g$和余数 $h$，使得 $f = g\phi_x^{K'} + h$。然后递归计算 $g_0\ldots,\ g_{K'-1}$和 $h_0,\ \ldots,\ h_{K'-1}$，使得

$$g = \sum_{0\le i<K'} g_i\phi_x^i \quad \text{and} \quad h = \sum_{0\le i<K'} h_i\phi_x^i.$$

然后，我们返回 $h_0$、.....、 $h_{K'-1}$、 $g_0$、.....、 $g_{K'-1}$。整个过程的运行时间为 $O^{\sim}(\mathrm{SM}(d,\ n,\ q))$ 次位运算，其中 SM 的定义见第 3 节（分析与交换情形中的分析相同，参见 [14],，并利用了 SM 关于 $d$的超线性性质）。

由此，我们能够计算 $f \in \mathbb{L}\{\tau\}\tau$ 在单项式基 B 上的系数。这实质上归结为使用上述过程，同时注意到 $f$ 是 $\tau$ 的倍数。将 $\tau$ 提到左边，写成 $f=\tau g$：若 $f = F\tau$，则 $g = F^{[-1]}$。应用前述过程，可写出 $g = \acute{\mathrm{I}}_{0\le i\le s} g_i \phi_x^i$，其中所有 $g_i$的次数都小于 $r$，且$s \le d/r$。

这给出 $f = \tau g = \acute{\mathrm{I}}_{0\le i\le s}(g_i^{[1]}\tau)\phi_x^i$，其中所有系数 $g_i^{[1]}\tau$都支撑在 $\tau, \ldots, \tau^r$ 上。提取$\tau, \ldots, \tau^r$的系数，我们得到次数至多为 $s$、关于 $\mathbb{L}[\tau]$ 的多项式 $G_1, \ldots, G_r$，使得 $f = \acute{\mathrm{I}}_{1\le i\le r} G_i * \tau^i$。

对 $\tau$ 在 $f$ 中进行左因子分解，以及将 $g$ 的所有系数乘以 $\tau$ 乘回去，代价为 $(dn\log q)^{1+o(1)}$，因此主要代价来自分治过程所需的 $\breve{O}(\mathrm{SM}(d,n,q))$ 次位运算。要计算次数为 $d$ 的自同态$u$的矩阵，我们对项 $\tau^i u$、 $i = 1, \ldots, r$ 各执行 $r$ 次该操作。因此，运行时间主要由 $\breve{O}(r\mathrm{SM}(d+r,n,q))$ 决定。最后，将矩阵的元素模 $\mu = (y-\gamma_x)^k$约简所需的时间相对于这些元素的大小是软线性的，因此可以忽略。

### 6.3 Frobenius 端同态的特殊情形

在 $u = \tau^n$ 这一特殊情形下，我们可以采用基于 [10] 中所用方法的小步大步法来加快计算。首先请注意，对于 $u = \tau^n$、 $d = n$ 和 $k$，它们属于 $O(n/m)$。

在这种情况下，只需计算向量 $\bar{\kappa}_{n+1}$、……、 $\bar{\kappa}_{n+r}$。它们为

$$\begin{bmatrix} \bar{\kappa}_{n+r} \\ \bar{\kappa}_{n+r-1} \\ \vdots \\ \bar{\kappa}_{n+1} \end{bmatrix} = \bar{\mathcal{A}}_n \ldots \bar{\mathcal{A}}_1, \tag{7}$$

其中 $\bar{\mathrm{A}}_t$ 表示 $\mathrm{A}_t$模 $\mu = (y-\gamma_x)^k$的像，对所有 $t$均如此。为了计算矩阵乘积 $\bar{\mathrm{A}} = \bar{\mathrm{A}}_n \ldots \bar{\mathrm{A}}1$，我们对 [10] 中使用的方法稍作扩展（该方法处理的是 $k = 1$的情形）。考虑以下 $\mathbb{L}[y]^{r\times r}$中的元素：

$$\mathcal{B} = \begin{bmatrix} \Lambda_{r-1} & \Lambda_{r-2} & \ldots & \Lambda_1 & \Lambda_0 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & \ldots & \Delta_r^{-1} \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{bmatrix} y. \tag{8}$$

特别地可得，对于 $t \ge 1$,

$$\mathcal{A}_t = \mathcal{B}^{[t]} \quad \text{and} \quad \bar{\mathcal{A}}_t = \mathcal{B}^{[t]} \bmod \mu,$$

其中按系数逐项进行约化。

设 $n^* = \lceil\sqrt{nk}\rceil \in O(n/\sqrt{m})$，并将 $n$写成 $n = n^* n_1 + n_0$，其中 $0 \le n_0 < n^*$，从而 $n_1 \le \mathrm{p}n/k$。令 $\overline{\phantom{xx}}$

$$C = \mathcal{B}^{[n^*+n_0]} \ldots \mathcal{B}^{[n_0+1]}$$

and

$$C_0 = \mathcal{B}^{[n_0]} \ldots \mathcal{B}^{[1]},$$

矩阵 A 是以下乘积

$$\mathcal{A} = C^{[(n_1-1)n^*]} \ldots C^{[n^*]} C C_0.$$

1：过程 CharPolyFrobenius 2：输入：域扩张 $\mathbb{L}$，次数为 $n$，在 $\mathbb{F}_q$ 上，$(\Delta_1, \ldots, \Delta_r) \in \mathbb{L}^r$表示一个秩为 $r$ 的 Drinfeld 模 $\phi$，定义在 $(\mathbb{L}, \gamma)$ 上。3：输出 $a_i \in A$，使得 Frobenius 的特征多项式为 $X^r + \text{Í}_{i=0}^{r-1} a_i X^i$。4：$n^*, n_1, n_0 \leftarrow \lceil \sqrt{nk} \rceil, \lfloor n/n^* \rfloor, n$ 对 $n^*$ 取模。5：B 如式 (8) 所示 6：C $\leftarrow$B $^{[n^*+n_0]} \ldots$B $^{[n_0+1]}$。7 $_0 \leftarrow$ $\mu$：¯C B $^{[n_0]} \ldots$B $^{[1]}$ 对 : C (C 对 )$^{[in^*]}$ 取模，其中 $0 \leq i < n_1$。9：¯A $\leftarrow \left(\text{Ö}_{i=0}^{n_1-1}\right.$ 8 $_{\bar{}}{}^{[in^*]} \leftarrow$ $\mu^{[-in^*]}$ $\bar{a}_i \leftarrow$ $Z^i$ ：det( ¯A $- ZI$) 中的系数 11：返回 $a_i = \chi_k(\bar{a}_i)$，其中 $0 \leq i < r$

我们的目标是在不计算 A 本身的情况下，计算 ¯A = A 模 $\mu$。

任意一次 Frobenius 映射（指数为正或负）在 $\mathbb{L}$ 中耗费 $(n\log q)^{1+o}(1)$次位运算。特别地，计算 C 和 C0 的定义中出现的所有矩阵 B $^{[i]}$，需要 $(rn^2/\sqrt{m}\log q)^{1+o}(1)$次位运算。

已知这些矩阵后，算法的下一阶段会在 $\mathbb{L}[y]$ 中计算 C 和 C0。此过程使用矩阵子积树算法 [14, 第 10], 章，运算次数在 $\mathbb{L}$ 中关于 $r^\omega n^*$ 为软线性。这需要 $(r^\omega n^2/\sqrt{m}\log q)^{1+o}(1)$次位运算。

为了推导移位后的矩阵

$$C^{[(n_1-1)n^*]} \bmod \mu, \ldots, C^{[n^*]} \bmod \mu,$$

我们使用以下引理。

引理 2. </style}对于 $f$属于 $\mathbb{L}[y]$ 和 $t \geq 0$,

$$f^{[t]} \bmod \mu = (f \bmod \mu^{[-t]})^{[t]}$$

证明。设 $g = f$模 $\mu^{[-t]}$，因此有如下形式的等式： $f = a\mu^{[-t]} + g$属于 $\mathbb{L}[y]$。我们对各个系数取 $q^t$ 次幂，得到 $f^{[t]} = a^{[t]}\mu + g^{[t]}$。由于 $g$和 $g^{[t]}$的次数都小于 $k$，这说明$g^{[t]} = f^{[t]}$模 $\mu$。□

逐项应用这一方法，我们通过先将 C 的所有项模 $\mu^{[-in^*]}$化简，再将结果中的所有系数提升至 $q^{in^*}$ 次幂，计算得到 C$^{[in^*]}$ 模 $\mu$，其中 $i = 1$、……、$(n_1 - 1)$。

矩阵 C 的次数为 $O(n/\sqrt{m})$，模数 $\mu^{[-t]}$的次数之和为 $kn_1$，这也等于 $O(n/\sqrt{m})$。总而言之，在 $\mathbb{L}$中应用 Frobenius $O(r^2 n/\sqrt{m})$ 次，并进行 $O(r^2 n/\sqrt{m})$ 次算术运算，即可完成 [14, 第 10] 章中的所有欧几里得除法。因此，运行时间为 $(r^2 n^2/\sqrt{m}\log q)^{1+o}(1)$ 位运算。

最后，我们将所有矩阵 C$^{[in^*]}$模 $\mu$和 C0 模 $\mu$相乘。这需要 $(r^\omega n^2/\sqrt{m}\log q)^{1+o}(1)$次位运算。

### 6.4 其他运算

已知斜多项式 $\tau^i u$ 在基 B 上的系数模 $\mu$后，我们计算由这些系数组成的矩阵的特征多项式。当矩阵的元素属于 $W_k$时，可以用 $(r^\lambda kn\log q)^{1+o}(1)$次位运算完成，其中 $\lambda$是第 2.3 节中定义的指数。

到目前为止，我们已经得到了 $W_k$ 中 CharPoly$^{W_k}(u\star k)$ 的所有系数。接下来只需对每个系数应用映射 $\chi_k$，即可求得 CharPoly$(u)$。

$W_k = \mathbb{F}_q[t,y]/(\ell(t),\ (y-\gamma_x)^k)$ 中的元素表示为关于 $t$、$y$ 的二元多项式，其关于 $t$ 的次数小于 $n$，关于 $y$ 的次数小于 $k$。为了通过 $\chi_k$ 计算它们的像，我们首先应用同构

$$W_k = \mathbb{F}_q[t,y]/(\ell(t),(y-\gamma_x)^k) \xrightarrow{A_k} \mathbb{F}_q[x,t,y]/(\mathfrak{p}(x),g(x,t),(y-x)^k)$$
$$\xrightarrow{B_k} \mathbb{F}_q[y,t]/(\mathfrak{p}(y)^k, G_k(y,t))$$

由 (3) 可得，$\mathfrak{p}(y)^k$ 的次数为 $km$，而 $G_k$ 在 $t$ 中的次数为 $n/m$。

我们在第 3 节提到，对于 $\mathbb{L} = \mathbb{F}_q[t]/(\ell(t))$ 中的 $c$，可以使用 $(n\log\ q)^{1+o}$（1）位运算，计算其在 $\mathbb{F}_q[x,t]/(\mathfrak{p}(x)\ g(x,\ t)$ 中的像 $\alpha(c)$。关于 $y$ 逐系数进行处理可知，对于 $W_k$ 中的 $C$，可以使用 $(kn\log q)^{1+o}$（1）位运算计算 $A_k(C)$。

[21, §4 的缠结映射提供了一种算法，可以使用 $(km\log\ q)^{1+o}$（1）位运算计算同构 $\mathbb{F}_q[x,y]/(\mathfrak{p}(x),\ (y-x)^k) \to \mathbb{F}_q[y]/(\mathfrak{p}(y)^k)$（也可以通过模复合完成，具有类似的渐近运行时间，但 [21] 中的算法更简单、更快速）。关于 $t$ 逐系数应用该算法后，可以再次使用 $(kn\log q)^{1+o}$（1）位运算计算 $B_k(A_k(C))$。此时，映射 $\chi_k$ 只是提取 $t$ 中次数为 0 的系数。

我们应用此过程 $r$ 次，总成本为 $(rkn\log q)^{1+o}(1)$ 位运算。这在运行时间分析中可以忽略不计。

在素域情形下使用精度 $k=1$，对于 $u=\tau^n$，必须单独计算常数系数$a_0$。这通过公式 $a_0 = (-1)^{n(r+1)^{+r}} N_{\mathbb{L}/\mathbb{F}_q}(\gamma_{\Delta_r})^{-1}\mathfrak{p}$，由 [13] 得出，所需位运算数为 $(n\log q)^{1+o}(1)$。

Sum将算法各步骤迄今所需的成本相加，即完成主定理的证明 s.

### 6.5 例子

令 $\mathbb{F}_q = \mathbb{Z}/2\mathbb{Z}, n=3$，并设 $\ell(t) = t^3+t+1$ 和 $\mathbb{L} = \mathbb{F}_2[t]/(\ell(t))$。令 $\gamma_x = t+1$ 模 $\ell(t)$，于是

$$\mathfrak{p} = x^3+x^2+1 = \ell(x+1),$$

以及 $\mathbb{L} \cong \mathbb{F}_\mathfrak{p} = \mathbb{F}_q[x]/(\mathfrak{p}(x))$，其同构由 $f(t) \mapsto f(x+1)$ 给出。考虑秩为 4 的 Drinfeld 模$\phi_x = t\tau^4 + (t^2+t)\tau^3 + \tau^2 + t^2\tau + t + 1$。我们使用德拉姆上同调计算特征多项式，也就是说，使用截断于次数 $k=1$ 的晶体上同调。换言之，所有计算均在$\mathbb{L}$上进行

方程 (4) 的递推关系变为 $\tau^{k+4} = (t+1)^{2^k}\tau^{(k+3)} + (t^2+1)^{2^k}\tau^{k+2} + t^{2^k}\tau^{k+1} + (1+t^{1-2^k})\tau^k$。将递推关系运行 $n=3$ 次，得到：

- $\tau^5 = (t^2+1)\tau^4 + (t^2+t+1)\tau^3 + t^2\tau^2 + t^2\tau^1$
- $\tau^6 = (t^2+1)\tau^4 + (t^2+1)\tau^3 + (t^2+t)\tau^2 + \tau^1$
- $\tau^7 = \tau^4 + t\tau^3 + (t+1)\tau^2 + \tau^1$

可以推知，Frobenius 端同态的矩阵为

$$\begin{bmatrix} 1 & t & t+1 & 1 \\ t^2+1 & t^2+1 & t^2+t & 1 \\ t^2+1 & t^2+t+1 & t^2 & t^2 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

其特征多项式为 $Z^4 + (t+1)Z^2 + (t+1)Z$。利用在素域情形下成立的 $a_0$ 表达式，可以推知弗罗贝尼乌斯范数为 $a_0 = x^3 + x^2 + 1$。

为了恢复最终系数，注意到 $t \mapsto x + 1$ 给出了所需的映射 $\chi_1 \colon W_1 = \mathbb{L} \to \mathbb{F}_{\mathfrak{p}}$。最后，我们得出 $\tau^n$ 的特征多项式为 $Z^4 + xZ^2 + xZ + x^3 + x^2 + 1$。

## 7 实验结果

我们在 SageMath [37] 中实现了第 (6.3) 节的算法，并已公开发布于 https://github.com/ymusleh/dri MAGMA [3] 中的实现也已公开发布于 https://github.com/ymusleh/drinfeld-magma，并用于生成本文中的实验结果。我们的实现与理论版本在几个方面有所不同。

- MAGMA 很可能不会使用 Kedlaya-Umans 算法来计算 $\mathbb{L}$中元素的弗罗贝尼乌斯映射。
- 为了计算系数在映射 $\chi_k$ 下的像，我们采用一种更简单的过程，即对二元格罗布纳基取模，而不是使用 van der Hoeven 和 Lecerf 的缠绕映射。无论如何，这不会影响所展示的运行时间。

## 致谢

我们感谢 Xav ier Caruso、Antoine Leudière 和 Pierre-Jean Spaenlehauer 的精彩讨论。Schost 得到了 p- 资助，资助方为 N SERC 发现基金。

| 运行时间 $m = 10$ $q = 25$ （秒） | | | | | | | |
|---|---|---|---|---|---|---|---|
| | $n = 100$ | $n = 150$ | $n = 200$ | $n = 300$ | $n = 400$ | $n = 500$ | $n = 600$ |
| $r = 5$ | 0.400 | 2.260 | 42.190 | 86.830 | 269.760 | 635.170 | 1099.110 |
| $r = 9$ | 0.790 | 4.210 | 78.860 | 157.100 | 481.090 | 1129.670 | |
| $r = 12$ | 1.170 | 6.080 | 104.630 | 220.430 | 658.950 | 1531.580 | |
| $r = 18$ | 2.300 | 11.360 | 170.790 | 366.690 | 1074.840 | 2451.530 | |
| $r = 23$ | 3.820 | 17.580 | 240.100 | 525.670 | 1518.370 | | |

## 参考文献

[1] G. W. Anderson. 1986. *t*-动机。《杜克数学杂志》53, 2 (1986), 457 – 502. https://doi.org/10.1215/S0012-7094-86-05328-7[2] B. Anglès. 1997. 关于附属于有限 Drinfeld 模的一些特征多项式。《数学手稿》93, 1 (1997年8月1日), 369–379. https://doi.org/10.1007/BF02677478[3] W. Bosma, J. Cannon, and C. Playoust. 1997. Magma 代数系统：I. 用户语言。《符号计算杂志》24, 3-4 (1997), 235–265. https://doi.org/10.1006/jsco.1996.0125 计算代数与数论（伦敦，1993）。[4] R. P. Brent and H. T. Kung. 1978. 形式幂级数运算的快速算法。《*ACM* 杂志》25, 4 (1978), 581–595.[5] D. G. Cantor and E. Kaltofen. 1991. 任意代数上的快速多项式乘法。《信息学学报》28 (1991), 693–701.[6] P. Caranay, M. Greenberg, and R. Scheidler. 2020. 在有限域上计算秩二 Drinfeld 模的模多项式与同源。《计算数学七十五年》(2020).[7] X. Caruso and J. Le Borgne. 2017. 斜多项式的快速乘法。载于*ISSAC'17*。ACM，77–84.[8] J.-M. Couveignes and R. Lercier. 2009. 有限域上的椭圆周期。《有限域及其应用》15, 1 (2009), 1–22.[9] P. Deligne and D. Husemoller. 1987. Drinfel'd 模综述。载于《算术代数几何当前趋势（阿卡塔，加利福尼亚州，*1985*）》。《当代数学》，第67卷。美国数学会，普罗维登斯，罗得岛州，25–91。https://doi.org/10.1090/conm/067/902591

[10] J. Doliskani, A. K. Narayanan, and É. Schost. 2021. 具有复乘的 Drinfeld 模、Hasse 不变量以及有限域上的多项式因式分解。《符号计算杂志》105 (2021), 199–213. https://doi.org/10.1016/j.jsc.2020.06.007 MICA 2016。[11] V. G. Drinfel'd. 1974. 椭圆模。《数学文集》94, 23 (1974), 561–593。[12] R. Duan, H. Wu, and R. Zhou. 2022. 通过非对称哈希实现更快的矩阵乘法。https://arxiv.org/abs/2210.10173[13] S. Garai and M. Papikian. 2018. Drinfeld 模约化的自同态环。《数论杂志》212 (2018年4月), https://doi.org/10.1016/j.jnt.2019.02.008[14] J. von zur Gathen and J. Gerhard. 2013.《现代计算机代数》（第三版）。剑桥大学出版社, 剑桥。[15] J. von zur Gathen and V. Shoup. 1992. 计算 Frobenius 映射与多项式因式分解。《计算复杂性》2, 3 (1992), 187–224。[16] E.-U. Gekeler. 1988/89. Drinfeld 模的德拉姆上同调。《巴黎数论研讨班》(1988/89), 57–85。[17] E.-U. Gekeler. 1991. 关于有限 Drinfeld 模。《代数杂志》141, 1 (1991), 187–203。[18] E.-U. Gekeler. 2008. 有限域上 Drinfeld 模的 Frobenius 分布。《美国数学会汇刊》360, 4 (2008), 1695–1721. http://www.jstor.org/stable/20161942[19] E.-U. Gekeler. 2011. Frobenius 在 Drinfeld 模德拉姆上同调上的作用。《美国数学会汇刊》363 (2011年6月). https://doi.org/10.1090/S0002-9947-2011-05422-X[20] D. Harvey, J. van der Hoeven, and G. Lecerf. 2017. 有限域上的快速多项式乘法。《ACM 杂志》63, 6, 文章52 (2017). https://doi.org/10.1145/3005344[21] J. van der Hoeven and G. Lecerf. 2017. 模多项式幂的复合。载于 ISSAC'17。ACM, 445–452。[22] J. van der Hoeven and G. Lecerf. 2020. 重新审视快速多元多点求值。《复杂性杂志》56 (2020), 101405. https://doi.org/10.1016/j.jco.2019.04.001[23] A. Joux and A. K. Narayanan. 2019. Drinfeld 模不适用于基于同源的密码学。IACR 密码学电子印本档案 2019 (2019), 1329。[24] E. Kaltofen and G. Villard. 2004. 关于计算行列式的复杂度。《计算复杂性》13, 3-4 (2004), 91–130。[25] K. Kedlaya. 2001. 使用 Monsky-Washnitzer 上同调计算超椭圆曲线上的点。《拉马努金数学学会杂志》16 (2001年6月)。[26]K. Kedlaya and C. Umans. 2008. 快速多项式因式分解与模复合。《SIAM 计算杂志》40 (2008年1月). https://doi.org/10.1137/08073408X[27]N. Kuhn and R. Pink. 2016. 寻找 Drinfeld 模的自同态。《数论杂志》232 (2016年8月). https://doi.org/10.1016/j.jnt.2021.02.013[28] A. Leudière and P.-J. Spaenlehauer. 2022. 从虚超椭圆函数域的类域论计算群作用。https://doi.org/10.48550/ARXIV.2203.06970[29] E. Mehrabi and É. Schost. 2016. 一种用于求解整数上二元多项式系统的近乎最优蒙特卡罗算法。《复杂性杂志》34 (2016), 78–128。[30] Y. Musleh and É. Schost. 2019. 计算有限秩二 Drinfeld 模的特征多项式。载于 ISSAC'19。ACM 出版社。[31] A. K. Narayanan. 2018. 通过计算 Drinfeld 模的 Euler-Poincaré 特征，在有限域上进行多项式因式分解。《有限域及其应用》54 (2018), 335–365。[32]V. Neiger and C. Pernet. 2020. 在矩阵乘法所需时间内确定性计算特征多项式。https://doi.org/10.48550/ARXIV.2010.04662[33] A. Poteaux and É. Schost. 2013. 模三角集的模复合及其应用。《计算复杂性》22, 3 (2013), 463–516。[34] S. Puchinger and A. Wachter-Zeh. 2017. 线性化多项式的快速运算及其在编码理论中的应用。《符号计算杂志》(2017)。[35] I. Reiner. 2003.《极大阶》。克拉伦登出版社。[36] T. Scanlon. 2001. 基于 Drinfeld 模的公钥密码系统并不安全。《密码学杂志》14, 4 (2001), 225–230。[37] Sage 开发团队。2020. SageMath, Sage 数学软件系统（9.2 版）。https://www.sagemath.org。[38]B. Wesolowski. 2022. 计算有限 Drinfeld 模之间的同源。《密码学电子印本档案》, 论文 2022/438。https://eprint.iacr.org/2022/438 https://eprint.iacr.org/2022/438。