Computing endomorphism rings and Frobenius matrices of Drinfeld modules

Mihran Papikian

Pennsylvania State University

Around Frobenius distributions and related topics
June 28–29, 2021

Notation

$A = \mathbb{F}_q[T]$	$\mathbb{Z}$
$F = \mathbb{F}_q(T)$	$\mathbb{Q}$
$F_\infty = \mathbb{F}_q((1/T))$	$\mathbb{R}$
$\mathbb{C}_\infty = \widehat{\overline{F_\infty}}$	$\mathbb{C}$

Drinfeld modules

Let K be a field equipped with a homomorphism $\gamma : A \to K$. Let

$$K\langle x \rangle := \left\{ \sum_{i=0}^{n} c_i x^{q^i} \mid c_i \in K, n \geq 0 \right\}$$

be the set of $\mathbb{F}_q$-linear polynomials. This is a **non-commutative** ring with usual addition but multiplication given by substitution $(f * g)(x) := f(g(x))$. The multiplicative identity is $f(x) = x$.

Definition

A **Drinfeld module of rank** r **over** K is a ring homomorphism

$$\phi : A \longrightarrow K\langle x \rangle, \qquad a \longmapsto \phi_a(x),$$

such that

$$\phi_T(x) = \gamma(T)x + g_1 x^q + \cdots + g_r x^{q^r}$$

for some $g_1, \ldots, g_r \in \mathbb{C}_\infty$, $g_r \neq 0$.

Drinfeld modules and lattices

Let $\Lambda \subset \mathbb{C}_\infty$ be an A-lattice of rank $r \geq 1$, i.e.,
$\Lambda \cong A^r$ and $\Lambda \subset \mathbb{C}_\infty$ is discrete.

The **Carlitz-Drinfeld exponential** of Λ is

$$\exp_\Lambda(x) = x \prod_{0 \neq \lambda \in \Lambda} \left(1 - \frac{x}{\lambda}\right).$$

Then

- $\exp_\Lambda(x + y) = \exp_\Lambda(x) + \exp_\Lambda(y)$.
- $\exp_\Lambda(\beta x) = \beta \exp_\Lambda(x)$ for all $\beta \in \mathbb{F}_q$.
- $\exp_\Lambda(ax) = \phi_a^\Lambda(\exp_\Lambda(x))$ for some Drinfeld module ϕ^Λ of rank r.
- $\Lambda \rightsquigarrow \phi^\Lambda$ gives a *bijection* between the set of lattices of rank r in $\mathbb{C}_\infty$ and the set of Drinfeld modules of rank r over $\mathbb{C}_\infty$.

We get

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \Lambda & \longrightarrow & \mathbb{C}_\infty & \xrightarrow{\exp_\Lambda} & \mathbb{C}_\infty & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \lambda \mapsto a\lambda} & & \downarrow{\scriptstyle z \mapsto az} & & \downarrow{\scriptstyle z \mapsto \phi_a^\Lambda(z)} & & \\
0 & \longrightarrow & \Lambda & \longrightarrow & \mathbb{C}_\infty & \xrightarrow[\exp_\Lambda]{} & \mathbb{C}_\infty & \longrightarrow & 0,
\end{array}
$$

which should be compared with

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & 2\pi i\mathbb{Z} & \longrightarrow & \mathbb{C} & \xrightarrow{e^x} & \mathbb{C}^\times & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \lambda \mapsto n\lambda} & & \downarrow{\scriptstyle z \mapsto nz} & & \downarrow{\scriptstyle z \mapsto z^n} & & \\
0 & \longrightarrow & 2\pi i\mathbb{Z} & \longrightarrow & \mathbb{C} & \xrightarrow[e^x]{} & \mathbb{C}^\times & \longrightarrow & 0.
\end{array}
$$

Note that

- $\phi^\Lambda[a] := \ker(\phi_a^\Lambda) = \{z \in \mathbb{C}_\infty \mid \phi_a^\Lambda(z) = 0\} \cong \Lambda/a\Lambda \cong (A/aA)^r$.

Carlitz cyclotomic extensions

- The **Carlitz module** $\psi_T(x) = Tx + x^q$ has rank 1.
- $$\exp_\psi(x) = x + \sum_{n\geq 1} \frac{x^{q^n}}{(T^{q^n} - T)(T^{q^n} - T^q)\cdots(T^{q^n} - T^{q^{n-1}})}.$$
- $\Lambda_\psi = \pi_C A$; it is known that π_C is transcendental over F.
- $\mathrm{Gal}(F(\psi[a])/F) \cong (A/aA)^\times$.
- Let $\mathfrak{p} \subset A$ be a maximal ideal. Denote the monic generator of $\mathfrak{p}$ by $\mathfrak{p}_+$. Then $\mathfrak{p}$ splits completely in $F(\psi[a])$ if and only if $\mathfrak{p}_+ \equiv 1 \pmod{a}$.

Example

Let $a = T$. Then $F(\psi[T])$ is the splitting field of $xT + x^q = x(T + x^{q-1})$. In this case, the previous theorem says that $x^{q-1} + T$ has $q-1$ distinct roots modulo $\mathfrak{p}$ if and only if the constant term of $\mathfrak{p}_+$ is 1. For example, if $q = 3$ and $\mathfrak{p} = T^2 + 1$, then

$$x^2 + T = (x + (T+1))(x - (T+1)) \bmod \mathfrak{p}.$$

But if $\mathfrak{p} = T^2 + T - 1$, then $x^2 + T$ has no roots modulo $\mathfrak{p}$.

Suppose ϕ is a Drinfeld module over F of rank $r \geq 2$. For $0 \neq \mathfrak{n} \in A$, the splitting field $F(\phi[\mathfrak{n}])$ of $\phi_{\mathfrak{n}}(x)$ is a Galois extension of F, but generally $F(\phi[\mathfrak{n}])/F$ is not abelian. The action of $\mathrm{Gal}(F(\phi[\mathfrak{n}])/F)$ on the roots of $\phi_{\mathfrak{n}}(x)$ commutes with the action of A, so there is a natural injective homomorphism

$$\mathrm{Gal}(F(\phi[\mathfrak{n}])/F) \hookrightarrow \mathrm{Aut}_A((A/\mathfrak{n}A)^r) \cong \mathrm{GL}_r(A/\mathfrak{n}A).$$

This is usually an isomorphism.

Example

Let $q = 5$, $\phi_T(x) = Tx + Tx^q + Tx^{q^2} + x^{q^3}$, and $\mathfrak{n} = T$. In this case,

$$\mathrm{Gal}(F(\phi[\mathfrak{n}])/F) \cong \mathrm{GL}_3(A/TA) \cong \mathrm{GL}_3(\mathbb{F}_5).$$

Non-abelian reciprocity

Theorem (Garai-P.)

Let ϕ be a Drinfeld module over F of rank $r \geq 2$. Assume the characteristic of F does not divide r. For each maximal ideal $\mathfrak{p} \subset A$ where ϕ has good reduction, there are two (effectively computable) elements $a(\mathfrak{p}), b(\mathfrak{p}) \in A$ such that for any $\mathfrak{n} \in A$ not divisible by $\mathfrak{p}$ we have

$$\mathfrak{p} \text{ splits completely in } F(\phi[\mathfrak{n}]) \iff a(\mathfrak{p}) \equiv r \pmod{\mathfrak{n}} \text{ and } b(\mathfrak{p}) \equiv 0 \pmod{\mathfrak{n}}.$$

- $a(\mathfrak{p})$ and $b(\mathfrak{p})$ depend only on ϕ and $\mathfrak{p}$, i.e., they **do not** depend on $\mathfrak{n}$.

Example

Let $q = 5$, $\phi_T(x) = Tx + Tx^q + Tx^{q^2} + x^{q^3}$, and $\mathfrak{p} = T^6 + 3T^5 + T^2 + 3T + 3$. In this case,

$$a(\mathfrak{p}) = 3T^2, \qquad b(\mathfrak{p}) = T - 1.$$

Hence $\mathfrak{p}$ splits completely in $F(\phi[\mathfrak{n}])$ if and only if $\mathfrak{n} = T - 1$.

Endomorphism rings of Drinfeld modules

Definition

The endomorphism ring of a Drinfeld module ϕ over K is

$$\begin{aligned}\mathrm{End}_K(\phi) &:= \{u(x) \in K\langle x\rangle \mid u(\phi_a(x)) = \phi_a(u(x)) \text{ for all } a \in A\} \\ &= \{u(x) \in K\langle x\rangle \mid u(\phi_T(x)) = \phi_T(u(x))\}.\end{aligned}$$

Let $\mathfrak{p} \subset A$ be a maximal ideal and let $\mathbb{F}_{\mathfrak{p}} := A/\mathfrak{p}$. Let $\gamma : A \to \mathbb{F}_{\mathfrak{p}}$ be the natural quotient homomorphism. Let ϕ be a Drinfeld module over $\mathbb{F}_{\mathfrak{p}}$ of rank r. Denote

$$\mathcal{E} = \mathrm{End}_{\mathbb{F}_{\mathfrak{p}}}(\phi).$$

- $\pi := x^{q^{\deg_T(\mathfrak{p}_+)}} \in \mathcal{E}$;
- $A[\pi]$ and $\mathcal{E}$ are A-orders in an "imaginary" extension of F of degree r;
- $$\mathcal{E}/A[\pi] \cong A/b_1A \times A/b_2A \times \cdots \times A/b_{r-1}A$$
  for uniquely determined nonzero monic polynomials $b_1, \ldots, b_{r-1} \in A$ such that
  $$b_1 \mid b_2 \mid \cdots \mid b_{r-1}.$$

Theorem (Garai-P.)

For each $1 \leq i \leq r-1$ *there is a monic polynomial* $f_i(x) \in A[x]$ *of degree* i *such that* $f_i(\pi) \in b_i\mathcal{E}$*. Moreover, if there is a monic polynomial* $g(x) \in A[x]$ *of degree* i *and* $b \in A$ *such that* $g(\pi) \in b\mathcal{E}$ *then* b *divides* b_i*.*

Proof.

The proof is based on the existence of a special basis of $\mathcal{E}$ as a free A-module:

$$\left\{1, \frac{f_1(\pi)}{b_1}, \ldots, \frac{f_{r-1}(\pi)}{b_{r-1}}\right\}$$

where $f_i(x) \in A[x]$ is monic and has degree i. □

Theorem 2 $\implies$ Theorem 1

Suppose ϕ is the reduction at $\mathfrak{p}$ of a Drinfeld module Φ over F. Let $\mathfrak{n} \in A$ be a polynomial not divisible by $\mathfrak{p}$. Then we have an isomorphism $\Phi[\mathfrak{n}] \cong \phi[\mathfrak{n}]$ compatible with the action of the Frobenius at $\mathfrak{p}$ on $\Phi[\mathfrak{n}]$ and the action of π on $\phi[\mathfrak{n}]$. Then it follows from the previous theorem that π acts as a scalar on $\phi[\mathfrak{n}]$ if and only if $\mathfrak{n} \mid b_1$. On the other hand, if π acts as a scalar on $\phi[\mathfrak{n}]$, then π acts as 1 if and only if its trace is congruent to r modulo $\mathfrak{n}$, assuming r is not divisible by the characteristic of F. Thus, the previous theorem is a refinement of the reciprocity theorem since it gives a Galois-theoretic interpretation of all b_i's, not just b_1.

Algorithm for computing $\mathcal{E}$

It is more convenient to work in the twisted polynomial ring $K\{\tau\} \cong K\langle x\rangle$, which is the ring of polynomials $\alpha_0 + \alpha_1\tau + \cdots + \alpha_d\tau^d$, $d \geq 0$, where multiplication satisfies the commutation rule $\tau\alpha = \alpha^q\tau$ for $\alpha \in K$.

Step 1: Let $P(x) = x^r + a_1x^{r-1} + \cdots + a_r \in A[x]$ be the minimal polynomial of π. Let $d := \deg_T(\mathfrak{p})$. It is known that for $1 \leq i \leq r-1$ we have

$$\deg_T(a_i) \leq i\frac{d}{r}.$$

In particular, $a_1, \ldots, a_{r-1}$ are uniquely determined by their residues modulo $\mathfrak{p}$. Moreover, it is known that a_r is a specific $\mathbb{F}_q^\times$-multiple of $\mathfrak{p}_+$. The equation $P(\pi) = 0$ implies that in $\mathbb{F}_\mathfrak{p}\{\tau\}$ we have

$$\gamma(a_{i-1}) = -\text{coefficient of } \tau^{d(r-i+1)} \text{ in } \phi_{a_i}\tau^{d(r-i)} + \phi_{a_{i+1}}\tau^{d(r-i+1)} + \cdots + \phi_{a_r}.$$

Thus, we can compute a_i recursively using $a_r, \ldots, a_{r-1}$.

Step 2: Assume for simplicity that $P(x)$ is separable. Then we can make a finite list of possible $(b_1, \ldots, b_{r-1})$ because $(b_1 \cdots b_{r-1})^2$ divides the discriminant of $A[\pi]$. (There are other restrictions: $b_i \mid b_{i+1}$; if $i + j < r$, then $b_i b_j \mid b_{i+j}$.)

Step 3: For each possible $(b_1, \ldots, b_{r-1})$, check whether this is the actual index of $A[\pi]$ in $\mathcal{E}$, i.e., if for all i we have $f_i(\pi) \in b_i\mathcal{E}$ for some monic $f_i(x) \in A[x]$ of degree i. For this we can assume that the coefficients of $f_i(x) \in A[x]$, as polynomials in T, have degrees $< \deg_T(b_i)$. Thus, for each $(b_1, \ldots, b_{r-1})$ we obtain a finite list of possible $f_1, \ldots, f_{r-1}$.

Step 3.1: Given a polynomial $g(x) = x^s + c_{s-1}x^{s-1} + \cdots + c_0$, checking whether $g(\pi) \in b\mathcal{E}$ can be done as follows. First, compute the residue of

$$\tau^{ds} + \phi_{c_{s-1}}\tau^{d(s-1)} + \cdots + \phi_{c_0}$$

modulo ϕ_b using the right division algorithm in $\mathbb{F}_{\mathfrak{p}}\{\tau\}$. If the residue is nonzero, then $g(\pi) \notin b\mathcal{E}$. If the residue is 0, then $g(\pi) = u\phi_b$ for an explicit $u \in \mathbb{F}_{\mathfrak{p}}\{\tau\}$ produced by the division algorithm. Now check if the commutation relation $u\phi_T = \phi_T u$ holds in $\mathbb{F}_{\mathfrak{p}}\{\tau\}$ (this relation holds if and only if $u \in \mathcal{E}$).

Example

Let $q = 5$, $\mathfrak{p} = T^6 + 3T^5 + T^2 + 3T + 3$, and $\phi : A \to \mathbb{F}_{\mathfrak{p}}\{\tau\}$ be given by

$$\phi_T = t + t\tau + t\tau^2 + \tau^3,$$

where t denotes the image of T under the canonical reduction map $A \to \mathbb{F}_{\mathfrak{p}}$. The minimal polynomial of π is

$$P(x) = x^3 + 2T^2x^2 + (3T^4 + T^2 + 3T + 1)x + 4\mathfrak{p}$$

From this we compute that

$$\mathrm{disc}(A[\pi]) = (T + 4)^6(T^4 + 2T^3 + 4T^2 + 3T + 4).$$

Hence b_1b_2 divides $(T + 4)^3$. We deduce that either $b_1 = T + 4$ and $b_2 = (T + 4)^2$, or $b_1 = 1$ and $b_2 = (T + 4)^n$ for some $0 \leq n \leq 3$. Our algorithm confirms that in fact $b_1 = T + 4$ and $b_2 = (T + 4)^2$. Moreover, the corresponding polynomials are $f_1(x) = x + 4$ and $f_2(x) = (x + 4)^2$. An A-basis of $\mathcal{E}$ is given by

$$e_1 = 1, \quad e_2 = \frac{\pi + 4}{T + 4}, \quad e_3 = e_2^2.$$

Finally, the element in $\mathbb{F}_{\mathfrak{p}}\{\tau\}$ corresponding to e_2 is

$$e_2 = \tau^3 + (2t^5 + 3t^4 + t + 1)\tau^2 + (4t^3 + 2t + 3)\tau + t^5 + 4t^4 + 4t^3 + 4t^2 + 3.$$

Matrix of the Frobenius automorphism

Multiplication by π induces an A-linear transformation of $\mathcal{E}$. The matrix of this transformation with respect to the basis $\left\{1, \frac{f_1(\pi)}{b_1}, \ldots, \frac{f_{r-1}(\pi)}{b_{r-1}}\right\}$ has the form

$$\Pi := \begin{pmatrix} * & * & \cdots & * & * \\ b_1 & * & \cdots & * & * \\ 0 & \frac{b_2}{b_1} & * & * & * \\ \vdots & & \ddots & & \\ 0 & 0 & \cdots & \frac{b_{r-1}}{b_{r-2}} & * \end{pmatrix}. \tag{1}$$

The entries of Π marked by $*$ depend explicitly on the coefficients of $f_i(x)$ and $P(x)$. (If $\mathcal{E} = A[\pi]$, then Π is simply the companion matrix of $P(x)$.)

Example

If $r = 2$ and q is odd, then $\mathit{\Pi} := \begin{pmatrix} -a_1/2 & b_1 \cdot \mathrm{disc}(\mathcal{E}) \\ b_1 & -a_1/2 \end{pmatrix}$.

Example

Let $q = 5$, $\mathfrak{p} = T^6 + 3T^5 + T^2 + 3T + 3$, and $\phi : A \to \mathbb{F}_{\mathfrak{p}}\{\tau\}$ be given by

$$\phi_T = t + t\tau + t\tau^2 + \tau^3,$$

where t denotes the image of T under the canonical reduction map $A \to \mathbb{F}_{\mathfrak{p}}$. Then

$$\mathit{\Pi} = \begin{pmatrix} 1 & 0 & T^4 + T^2 + 2T + 1 \\ T + 4 & 1 & 2T^3 + 2T^2 + 2T + 4 \\ 0 & T + 4 & 3(T^2 + 1) \end{pmatrix},$$

Theorem (Garai-P.)

Let Φ be a Drinfeld module over F of rank $r \geq 2$. Let $\mathfrak{p}$ be a prime of good reduction of ϕ, and let ϕ denote the reduction of Φ at $\mathfrak{p}$. Let $\mathfrak{n} \in A$ be a nonzero element not divisible by $\mathfrak{p}$. Suppose for every maximal ideal $\mathfrak{l} \subset A$ dividing $\mathfrak{n}$ the Tate module $T_{\mathfrak{l}}(\phi)$ is a free $\mathcal{E} \otimes A_{\mathfrak{l}}$-module of rank 1. Then Π, reduced modulo $\mathfrak{n}$, represents the class of the Frobenius at $\mathfrak{p}$ in $\mathrm{Gal}(F(\Phi[\mathfrak{n}])/F) \subseteq \mathrm{GL}_r(A/\mathfrak{n}A)$.

- The assumption of the theorem is satisfied if $\mathcal{E} \otimes A_{\mathfrak{l}}$ is a **Gorenstein ring**.
- $\mathcal{E} \otimes A_{\mathfrak{l}}$ is Gorenstein if one of the following holds:
  - $r = 2$.
  - $\mathcal{E} \otimes A_{\mathfrak{l}} = A_{\mathfrak{l}}[\pi]$.
  - $\mathfrak{l}$ does not divide the conductor of $\mathcal{E}$.

Example

Let $q = 5$, $\mathfrak{p}$ be a maximal ideal, and $\phi : A \to \mathbb{F}_{\mathfrak{p}}\{\tau\}$ be given by

$$\phi_T = t + t\tau + t\tau^2 + \tau^3, \quad t = \gamma(T).$$

If $\mathfrak{p} = T^6 + 3T^5 + T^2 + 3T + 3$, then $\mathcal{E} \otimes A_{\mathfrak{l}}$ is Gorenstein for all $\mathfrak{l}$ (in this case the conductor of $\mathcal{E}$ is 1).

If $\mathfrak{p} = T^6 + 4T^4 + 4T^2 + T + 1$, then $b_1 = 1$, $b_2 = T - 1$, and $\mathcal{E} \otimes A_{\mathfrak{l}}$ is **not** Gorenstein for $\mathfrak{l} = T - 1$.

Asymptotic behavior of Frobenius indices

Let Φ be a Drinfeld module of rank $r \geq 3$ over F. For a maximal ideal $\mathfrak{p} \subset A$ where Φ has good reduction ϕ, let $\mathcal{E}(\mathfrak{p}) = \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\phi)$, and let $b_{1,\mathfrak{p}}, \ldots, b_{r-1,\mathfrak{p}}$ be the invariant factors of $\mathcal{E}(\mathfrak{p})/A[\pi_\mathfrak{p}]$. Let $B(\mathfrak{p})$ be the integral closure of A in $F(\pi_\mathfrak{p})$. Assume $\mathrm{End}_{\overline{F}}(\Phi) = A$.

- (Garai-P.) For any fixed nonzero $\mathfrak{m}, \mathfrak{n} \in A$, the set of maximal ideals $\mathfrak{p}$ such that $\mathfrak{m} \mid \chi(\mathcal{E}(\mathfrak{p})/A[\pi_\mathfrak{p}])$ and $\mathfrak{n} \mid \chi(B(\mathfrak{p})/\mathcal{E}(\mathfrak{p}))$ has positive density, where χ denotes the Fitting ideal.
- (Cojocaru-P.) If $r = 2$, then there is an explicit formula for the density of the set $\{\mathfrak{p} \mid b_{1,\mathfrak{p}} = 1\}$.
  Are there such formulas for $r \geq 3$?
- (Cojocaru-P.) If $r = 2$, then $\deg_T \mathrm{disc}(\mathcal{E}(\mathfrak{p})) \to \infty$ as $\deg_T(\mathfrak{p}) \to \infty$.
  Is the same true when $r \geq 3$?