ARTICLE IN PRESS YJNTH:6455

Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Computing endomorphism rings and Frobenius matrices of Drinfeld modules

Sumita Garai, Mihran Papikian *,[1]

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

ARTICLE INFO

Article history:
Received 23 August 2019
Received in revised form 24 November 2019
Accepted 25 November 2019
Available online xxxx
Communicated by F. Breuer

MSC:
11G09
11R58

Keywords:
Drinfeld modules
Endomorphism rings
Gorenstein rings

ABSTRACT

Let $\mathbb{F}_q[T]$ be the polynomial ring over a finite field $\mathbb{F}_q$. We study the endomorphism rings of Drinfeld $\mathbb{F}_q[T]$-modules of arbitrary rank over finite fields. We compare the endomorphism rings to their subrings generated by the Frobenius endomorphism and deduce from this a refinement of a reciprocity law for division fields of Drinfeld modules proved in our earlier paper. We then use these results to give an efficient algorithm for computing the endomorphism rings and discuss some interesting examples produced by our algorithm.

1. Introduction

1.1. Drinfeld modules

We first recall some basic concepts from the theory of Drinfeld modules.

* Corresponding author.
E-mail addresses: sxg386@psu.edu (S. Garai), papikian@psu.edu (M. Papikian).
[1] The second author was supported by a Collaboration Grant for Mathematicians of the Simons Foundation (# 637364).

https://doi.org/10.1016/j.jnt.2019.11.018

Let $\mathbb{F}_q$ be a finite field with q elements. Let $A = \mathbb{F}_q[T]$ be the ring of polynomials in T with coefficients in $\mathbb{F}_q$. Let $F = \mathbb{F}_q(T)$ be the field of fractions of A. We will call a nonzero prime ideal of A simply a *prime* of A. Given a prime $\mathfrak{p}$ of A, we denote by $A_\mathfrak{p}$ (resp. $F_\mathfrak{p}$) the completion of A at $\mathfrak{p}$ (resp. the field of fractions of $A_\mathfrak{p}$). By abuse of notation we will denote the monic generator of $\mathfrak{p}$ by the same symbol.

Let L be a field equipped with a structure $\gamma : A \to L$ of an A-algebra. Let τ be the Frobenius endomorphism of L relative to $\mathbb{F}_q$, that is, the map $\alpha \mapsto \alpha^q$. Let $L\{\tau\}$ be the noncommutative ring of polynomials in τ with coefficients in L and commutation rule $\tau c = c^q\tau$, $c \in L$. A *Drinfeld module of rank* $r \geq 1$ *defined over* L is a ring homomorphism $\phi : A \to L\{\tau\}$, $a \mapsto \phi_a$, uniquely determined by the image of T

$$\phi_T = \gamma(T) + \sum_{i=1}^{r} g_i(T)\tau^i, \quad g_r(T) \neq 0.$$

The *endomorphism ring* of ϕ is the centralizer of $\phi(A)$ in $L\{\tau\}$:

$$\begin{aligned}\mathrm{End}_L(\phi) &= \{u \in L\{\tau\} \mid u\phi_a = \phi_a u \text{ for all } a \in A\}\\ &= \{u \in L\{\tau\} \mid u\phi_T = \phi_T u\}.\end{aligned}$$

It is clear that $\mathrm{End}_L(\phi)$ contains in its center the subring $\phi(A) \cong A$, hence is an A-algebra. It can be shown that $\mathrm{End}_L(\phi)$ is a free A-module of rank $\leq r^2$; see [6].

The Drinfeld module ϕ endows the algebraic closure $\overline{L}$ of L with an A-module structure, where $a \in A$ acts by ϕ_a. The *a-torsion* $\phi[a] \subset \overline{L}$ of ϕ is the kernel of ϕ_a, that is, the set of zeros of the polynomial

$$\phi_a(x) = \gamma(a)x + \sum_{i=1}^{r\cdot\deg(a)} g_i(a)x^{q^i} \in L[x].$$

It is easy to see that $\phi[a]$ has a natural structure of an A-module, where A acts via ϕ. Moreover, if a is not divisible by $\ker(\gamma)$, then $\phi[a] \cong (A/aA)^{\oplus r}$ and $\phi[a]$ is contained in the separable closure $L^{\mathrm{sep}} \subset \overline{L}$ (since $\phi_a'(x) = \gamma(a) \neq 0$).

For a prime $\mathfrak{l} \lhd A$ different from $\ker(\gamma)$, the *$\mathfrak{l}$-adic Tate module of* ϕ is the inverse limit

$$T_\mathfrak{l}(\phi) = \varprojlim \phi[\mathfrak{l}^n] \cong A_\mathfrak{l}^{\oplus r}.$$

1.2. Main results

Let $\mathfrak{p} \lhd A$ be a prime and k a finite extension of $\mathbb{F}_\mathfrak{p} := A/\mathfrak{p}$. We consider k as an A-algebra via the composition $\gamma : A \to A/\mathfrak{p} \hookrightarrow k$. Let ϕ be a Drinfeld module of rank r defined over k. Denote $\mathcal{E} = \mathrm{End}_k(\phi)$ and $D = \mathcal{E} \otimes_A F$. Let $\pi := \tau^{[k:\mathbb{F}_q]} \in k\{\tau\}$. It is clear that π is in the center of $k\{\tau\}$. In particular, π commutes with $\phi(A)$, so $\pi \in \mathcal{E}$. Let $K = F(\pi)$ be the subfield of D generated by π. The following is well-known (cf. [7], [12]):

- The degree of the field extension K/F divides r.
- D is a central division algebra over K of dimension $(r/[K:F])^2$.
- There is a unique place of K over the place $\infty = 1/T$ of F.

The endomorphism rings (and algebras) of Drinfeld modules over finite fields have been extensively studied; cf. [7], [1], [12], [13], [26]. They play an important role in the theory of Drinfeld modules, as well as their applications to other areas, such as the theory of central simple algebras (cf. [11]), the Langlands conjecture over function fields (cf. [7], [17]), or the study of the splitting behavior of primes in certain non-abelian extensions of F (cf. [4], [10], [5]). In this paper, we are interested in comparing $\mathcal{E}$ to $A[\pi]$. We then deduce from this a method for computing $\mathcal{E}$.

Throughout the paper, we make the following assumption:

$$[K:F] = r. \tag{1.1}$$

This assumption is satisfied if, for example, $k = \mathbb{F}_{\mathfrak{p}}$ (cf. [10, Prop. 2.1]) or $\phi[\mathfrak{p}] \cong (A/\mathfrak{p})^{r-1}$, i.e., ϕ is ordinary (cf. [17, (2.5)]). It is equivalent to the assumption that the endomorphism algebra D is commutative, or more precisely, that $\mathcal{E}$ is an A-order in K. In that case, $A[\pi] \subset \mathcal{E}$ are A-orders in K, so by the theory of finitely generated modules over principal ideal domains we have

$$\mathcal{E}/A[\pi] \cong A/b_1A \times A/b_2A \times \cdots \times A/b_{r-1}A$$

for uniquely determined nonzero monic polynomials $b_1, \dots, b_{r-1} \in A$ such that

$$b_1 \mid b_2 \mid \cdots \mid b_{r-1}.$$

We call the $(r-1)$-tuple $(b_1, \dots, b_{r-1})$ the *Frobenius index* of ϕ. The first main result of this paper is the following:

Theorem 1.1. *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.*

The proof of this theorem is given in Section 3. It is based on the existence of special bases of A-orders; this crucial fact about orders is discussed separately in Section 2. As we explain in Remark 3.2, Theorem 1.1 can be considered as a refinement of the reciprocity law proved in our earlier paper [10, Thm. 1.2] (see also [4, Cor. 2] for the rank-2 case).

The condition $f_i(\pi) \in b_i\mathcal{E}$ means that we have an equality $f_i(\pi) = u\phi_{b_i}$ in $k\{\tau\}$ for some $u \in \mathcal{E}$. For given b_i and f_i, the validity of equality $f_i(\pi) = u\phi_{b_i}$ can be easily checked using the division algorithm in $k\{\tau\}$. On the other hand, a finite list of possible Frobenius indices of ϕ can be deduced either by computing the discriminant of $A[\pi]$, or by computing an A-basis of the integral closure of A in K. Since we can assume that the coefficients of $f_i(x) \in A[x]$ have degrees less than the degree of b_i, the Frobenius index of π can be determined by performing finitely many calculations. This leads to an efficient algorithm for computing the Frobenius index of ϕ and an A-basis of $\mathcal{E}$. The algorithm is described in detail in Section 3. We have implemented this algorithm in the `Magma` software package. In Section 3, the reader will find an explicit example of a calculation of the endomorphism ring of a Drinfeld module of rank 3. In the rank-2 case, we gave another algorithm for computing $\mathcal{E}$ in [10]; the present algorithm is different from the one in [10], even when specialized to $r = 2$.

A completely different algorithm from ours for computing the endomorphism rings of Drinfeld modules was proposed by Kuhn and Pink in [15]. This algorithm works in all cases, without the restriction (1.1), and determines a basis of $\mathcal{E}$ as an $\mathbb{F}_q[\pi]$-module. However, it is not quite clear how easily one can deduce from this the A-module structure of $\mathcal{E}$, e.g., determine the Frobenius index or the discriminant of $\mathcal{E}$ over A. We discuss the algorithm of Kuhn and Pink in more detail in Remark 3.5.

Next, we explain a theoretical application of Theorem 1.1. Let $\Phi : A \to F\{\tau\}$ be a Drinfeld module of rank r over F defined by

$$\Phi_T = T + g_1\tau + \cdots + g_r\tau^r.$$

(We will always implicitly assume that $\gamma : A \to F$ is the canonical embedding of A into its field of fractions.) We say that a prime $\mathfrak{p} \lhd A$ is a *prime of good reduction* for Φ if $\mathrm{ord}_{\mathfrak{p}}(g_i) \geq 0$ for $1 \leq i \leq r-1$, and $\mathrm{ord}_{\mathfrak{p}}(g_r) = 0$. (All but finitely many primes of A are primes of good reduction for a given Drinfeld module Φ.) Let $n \in A$ be a monic polynomial and $F(\Phi[n])$ be the splitting field of the polynomial $\Phi_n(x)$; such fields are called *division fields* (or *torsion fields*) of Φ. If $\mathfrak{p}$ is a prime of good reduction of Φ and $\mathfrak{p} \nmid n$, then $\mathfrak{p}$ does not ramify in $F(\Phi[n])$. One is interested in the splitting behavior of $\mathfrak{p}$ in $F(\Phi[n])$ as n varies, e.g., a "reciprocity law" in the form of congruence conditions modulo n which guarantee that $\mathfrak{p}$ splits completely $F(\Phi[n])$. The primes which split completely in $F(\Phi[n])$ have been studied before, e.g. [5], [10], [16].

We can consider $g_1, \ldots, g_r$ as elements of $A_{\mathfrak{p}}$; denote by $\overline{g}$ the image of $g \in A_{\mathfrak{p}}$ under the canonical homomorphism $A_{\mathfrak{p}} \to A_{\mathfrak{p}}/\mathfrak{p} = \mathbb{F}_{\mathfrak{p}}$. The *reduction of* Φ *at* $\mathfrak{p}$ is the Drinfeld module ϕ over $\mathbb{F}_{\mathfrak{p}}$ given by

$$\phi_T = \overline{T} + \overline{g_1}\tau + \cdots + \overline{g_r}\tau^r.$$

Note that ϕ has rank r since $\overline{g_r} \neq 0$. Let $\mathcal{E} = \mathrm{End}_{\mathbb{F}_{\mathfrak{p}}}(\phi)$ and $\pi = \tau^{\deg(\mathfrak{p})}$. We have the inclusion of orders $A[\pi] \subset \mathcal{E}$. Theorem 1.1, or rather its proof, provides an explicit basis of $\mathcal{E}$ as a free A-module of rank r. With respect to this basis, the action of π on $\mathcal{E}$ by multiplication can be described by an explicit matrix $\mathcal{F}(\mathfrak{p}) \in \mathrm{Mat}_r(A)$ which depends on the Frobenius index of ϕ, the coefficients of the polynomials f_i, and the coefficients of the minimal polynomial of π. We explain in Section 4 that under a mild (but subtle) technical assumption on $\mathcal{E}$, the integral matrix $\mathcal{F}(\mathfrak{p})$, when reduced modulo n, represents the conjugacy class of the Frobenius at $\mathfrak{p}$ in $\mathrm{Gal}(F(\Phi[n])/F) \subset \mathrm{GL}_r(A/nA)$. This result in the rank-2 case was proved in [4, Thm. 1]. The analogue of this result for elliptic curves goes back to Duke and Tóth [8], which was our initial motivation for considering this problem in the setting of Drinfeld modules. (For a refinement of the result of Duke and Tóth for elliptic curves see the paper by Centeleghe [3].)

The technical assumption mentioned in the previous paragraph is the assumption that $\mathcal{E} \otimes_A A_\mathfrak{l}$ is a Gorenstein ring for all primes $\mathfrak{l} \mid n$. It is often satisfied (see Proposition 4.10), but not always when $r \geq 3$. At the end of Section 4 we give an interesting example of $\mathcal{E} \otimes_A A_\mathfrak{l}$ which is not Gorenstein. The study of the Gorenstein property of endomorphism rings of abelian varieties, especially the Jacobian varieties of modular curves, has played an important role in many fundamental developments in arithmetic geometry (cf. [20]), but, as far as we are aware, it has not been studied at all in the context of Drinfeld modules.

2. Some facts about orders

Let A be a principal ideal domain with field of fraction F. Let $f(x) \in A[x]$ be a monic irreducible polynomial of degree r with coefficients in A. Fix a root π of $f(x)$ in $\overline{F}$ and denote $K = F(\pi) \subset \overline{F}$. Let B be the integral closure of A in K.

The field K is an r-dimensional vector space over F. For a given $\alpha \in K$, multiplication by α on K defines an F-linear transformation $M_\alpha : K \to K$. Let $\mathrm{Tr}_{K/F}(\alpha) \in F$ (resp. norm $\mathrm{Nr}_{K/F}(\alpha) \in F$) be the trace (resp. determinant) of M_α. The *discriminant* of an r-tuple $\alpha_1, \dots, \alpha_r \in K$ is

$$\mathrm{disc}(\alpha_1, \dots, \alpha_r) = \det\left(\mathrm{Tr}_{K/F}(\alpha_i\alpha_j)\right).$$

The discriminant does not depend of the ordering of the elements α_j. It is known that $\mathrm{disc}(\alpha_1, \dots, \alpha_r) = 0$ if and only if either K/F is inseparable or $\alpha_1, \dots, \alpha_r$ are linearly dependent over F. Moreover, (cf. [21, Ch. III]):

(i) $\mathrm{disc}(1, \pi, \dots, \pi^{n-1}) = (-1)^{n(n-1)/2}\mathrm{Nr}_{K/F}(f'(\pi))$.

(ii) If $\begin{bmatrix}\beta_1\\ \vdots \\ \beta_r\end{bmatrix} = M \begin{bmatrix}\alpha_1\\ \vdots \\ \alpha_r\end{bmatrix}$ with $M \in \mathrm{Mat}_r(F)$, then

$$\mathrm{disc}(\beta_1, \dots, \beta_r) = \det(M)^2 \cdot \mathrm{disc}(\alpha_1, \dots, \alpha_r).$$

An A-*order* in K is an A-subalgebra $\mathcal{O}$ of B with the same unity element and such that $B/\mathcal{O}$ has finite cardinality. Note that any A-order $\mathcal{O}$ is a free A-modules of rank r. An example of an A-order in K is

$$A[\pi] = A + A\pi + \cdots + A\pi^{r-1}.$$

Let $\mathcal{O} \subset \mathcal{O}'$ be two A-orders in K. Since both modules $\mathcal{O}$ and $\mathcal{O}'$ have the same rank over A, and both contain 1, we have

$$\mathcal{O}'/\mathcal{O} \cong A/b_1A \times A/b_2A \times \cdots \times A/b_{r-1}A,$$

for uniquely determined (up to multiplication by units in A) non-zero elements $b_1, \ldots, b_{r-1} \in A$ such that

$$b_1 \mid b_2 \mid \cdots \mid b_{r-1}.$$

This is an easy consequence of the theory of finitely generated modules over principal ideal domains; cf. [9, Thm. 12.5]. We call the ideal $\chi(\mathcal{O}'/\mathcal{O})$ of A generated by $\prod_{i=1}^{r-1} b_i$ the *index* of $\mathcal{O}$ in $\mathcal{O}'$, and $(b_1, \ldots, b_{r-1})$ the *refined index* of $\mathcal{O}$ in $\mathcal{O}'$ (in a more standard terminology, the elements $b_1, \ldots, b_{r-1} \in A$ are the *invariant factors* of $\mathcal{O}'/\mathcal{O}$).

Let $\mathcal{O}$ be an A-order in K. Let $\alpha_1, \ldots, \alpha_r$ be a basis of $\mathcal{O}$ over A:

$$\mathcal{O} = A\alpha_1 + \cdots + A\alpha_r.$$

Define the discriminant $\mathrm{disc}(\mathcal{O})$ of $\mathcal{O}$ to be the ideal of A generated by $\mathrm{disc}(\alpha_1, \ldots, \alpha_r)$. By (ii) above, $\mathrm{disc}(\mathcal{O})$ does not depend on the choice of a basis $\alpha_1, \ldots, \alpha_r$. Moreover, by the same property (see also [21, Ch. III]), if $\mathcal{O} \subseteq \mathcal{O}'$ is an inclusion of orders, then

$$\mathrm{disc}(\mathcal{O}) = \chi(\mathcal{O}'/\mathcal{O})^2 \cdot \mathrm{disc}(\mathcal{O}'), \tag{2.1}$$

and for an inclusion of orders $\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}''$ we have

$$\chi(\mathcal{O}''/\mathcal{O}) = \chi(\mathcal{O}''/\mathcal{O}') \cdot \chi(\mathcal{O}'/\mathcal{O}). \tag{2.2}$$

The following theorem is essentially Theorem 13 in [18]. Since this fact is crucial for our later purposes and we need the statement in a more general setting than in [18], we give the proof for the sake of completeness.

Theorem 2.1. *Assume $\mathcal{O}$ is an A-order in K such that $A[\pi] \subset \mathcal{O}$. Let $(b_1, \ldots, b_{r-1})$ be the refined index of $A[\pi]$ in $\mathcal{O}$. There are polynomials $f_i(x) \in A[x]$, $1 \le i \le r-1$, such that f_i is monic, $\deg(f_i) = i$, and*

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

is an A-basis of $\mathcal{O}$.

Proof. Fix a generator d of the ideal $\chi(\mathcal{O}/A[\pi])$. For each k, $1 \le k \le r$, let G_k be the free A-submodule of K generated by $1/d, \pi/d, \ldots, \pi^{k-1}/d$. Let $\mathcal{O}_k = \mathcal{O} \cap G_k$. Note that $\mathcal{O}_1 = A$, $\mathrm{rank}_A \mathcal{O}_k = k$ (since $A + A\pi + \cdots + A\pi^k \subset \mathcal{O}_k$) and $\mathcal{O}_r = \mathcal{O}$ (since for any $\alpha \in \mathcal{O}$ we have $d\alpha \in A[\pi]$).

We will define $d_1 \mid d_2 \mid \cdots \mid d_{n-1} \mid d$ and monic polynomials $f_i(x) \in A[x]$ of degree i, $1 \le i \le r-1$, such that for each $1 \le k \le r$

$$1, f_1(\pi)/d_1, \dots, f_{k-1}(\pi)/d_{k-1}$$

is an A-basis of $\mathcal{O}_k$. This is certainly true for $k = 1$. Now fix some $1 \le k < r$ and assume we were able to prove this claim for $\mathcal{O}_k$. Let

$$\eta : G_{k+1} \longrightarrow A, \qquad \sum_{i=0}^{k} a_i \frac{\pi^i}{d} \longmapsto a_k,$$

be the projection onto the last factor. Let $I = \eta(\mathcal{O}_{k+1})$ be the image of $\mathcal{O}_{k+1}$ under this homomorphism. Clearly I is an ideal of A, thus can be generated by a single element. Fix some $\beta \in \mathcal{O}_{k+1}$ such that $\eta(\beta)$ generates I. Note that $I \neq 0$ (since $\pi^k \in \mathcal{O}_{k+1}$ maps to $d \neq 0$), and $\mathcal{O}_k \subseteq \ker(\eta|\mathcal{O}_{k+1})$. Since I is a free A-module of rank 1, comparing the ranks we conclude that $\mathcal{O}_k = \ker(\eta|\mathcal{O}_{k+1})$ and $\mathcal{O}_{k+1} = \mathcal{O}_k \oplus A\beta$. It remains to show that $\beta = f_k(\pi)/d_k$. We have

$$\eta\left(\frac{\pi f_{k-1}(\pi)}{d_{k-1}}\right) = \eta\left(\frac{1}{d_{k-1}}\pi^k + \cdots\right) = \eta\left(\frac{d}{d_{k-1}}\frac{\pi^k}{d} + \cdots\right) = \frac{d}{d_{k-1}} \in I.$$

It follows that $a\eta(\beta) = d/d_{k-1}$ for some $a \in A$. Defining $d_k = ad_{k-1}$, we have $\eta(\beta) = d/d_k$, which implies that $\beta = f_k(\pi)/d_k$ for some $f_k(x) = x^k$+lower degree terms. Note that by construction $d_{k-1} \mid d_k \mid d$, so it remains to show that the coefficients of $f_k(x)$ are in A. However, since $f_k(\pi)/d_{k-1} = a\beta \in \mathcal{O}_{k+1}$, we have

$$\frac{f_k(\pi) - \pi f_{k-1}(\pi)}{d_{k-1}} =: \gamma \in \mathcal{O}_{k+1}.$$

On the other hand, $\eta(\gamma) = a\eta(\beta) - d/d_{k-1} = 0$, so in fact, $\gamma \in \mathcal{O}_k$. Using our basis for $\mathcal{O}_k$ we can write $\gamma = g(\pi)/d_{k-1}$ for some $g(x) \in A[x]$ having degree $< k$. This implies that $f_k(\pi) - \pi f_{k-1}(\pi) = g(\pi)$. Since the degree of the minimal polynomial of π over F is r and the degree of $f_k(x) - \pi f_{k-1}(x) - g(x)$ is strictly less than r, we must have $f_k(x) = xf_{k-1}(x) + g(x) \in A[x]$.

It remains to show that $(d_1, \dots, d_{r-1})$ is the refined index of $A[\pi]$ in $\mathcal{O}$. Since the polynomials $f_i(x)$ are monic, the elements $1, f_1(\pi), \dots, f_{n-1}(\pi)$ form an A-basis of $A[\pi]$ (the transition matrix from $1, \pi, \dots, \pi^{n-1}$ to this basis is upper triangular with 1's on the diagonal, so has determinant 1). But now, using $1, f_1(\pi)/d_1, \dots, f_{n-1}(\pi)/d_{n-1}$ as a basis of $\mathcal{O}$, we obviously have $\mathcal{O}/A[\pi] \cong A/d_1A \times \cdots \times A/d_{r-1}A$ with $d_1 \mid \cdots \mid d_{r-1}$. Since the invariant factors of $\mathcal{O}/A[\pi]$ are unique, up to multiplication by units, $d_1, d_2, \dots, d_{r-1}$ must be the invariant factors. $\square$

Please cite this article in press as: S. Garai, M. Papikian, Computing endomorphism rings and Frobenius matrices of Drinfeld modules, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2019.11.018

Remark 2.2. The polynomials $f_i \in A[x]$, $1 \le i \le r-1$, in Theorem 2.1 are not unique. It is easy to see that they can be replaced by any other monic polynomials $g_i \in A[x]$ such that g_i has degree i and all $g_i(\pi)/b_i$ are in $\mathcal{O}$.

Proposition 2.3. *Let $\mathcal{O}$ be an A-order in K such that $A[\pi] \subset \mathcal{O}$. Let $(b_1, \dots, b_{r-1})$ be the refined index of $A[\pi]$ in $\mathcal{O}$.*

1. *If $i + j < r$, then $b_i b_j \mid b_{i+j}$.*
2. *For any $i < r$, we have $b_1^i \mid b_i$.*
3. *$b_1^{r(r-1)} \mid \mathrm{disc}(A[\pi])$.*
4. *If $b_1 \neq 1$, then the inclusion of ideals $(b_1) \supsetneq (b_2) \supsetneq \cdots \supsetneq (b_{r-1})$ is strict.*

Proof. Let $f_1(\pi)/b_1, \dots, f_{r-1}(\pi)/b_{r-1}$ be the A-basis of $\mathcal{O}$ supplied by Theorem 2.1. Consider $\alpha = f_i(\pi)f_j(\pi)/b_ib_j \in \mathcal{O}$. We can express α as an A-linear combination $\alpha = a_0 + \sum_{k=1}^{i+j} a_k f_k(\pi)/b_k$. (The basis elements $f_k(\pi)/b_k$ for $k > i+j$ do not appear in this linear combination since otherwise π would a root of a non-zero polynomial of degree $< r$.) Comparing the coefficients of π^{i+j} on both sides we get $1/b_ib_j = a_{i+j}/b_{i+j}$ for some nonzero $a_{i+j} \in A$. Thus, b_ib_j divides b_{i+j}. This proves (1).

(2) and (4) immediately follow from (1). Next, by (2.1), $\chi(\mathcal{O}/A[\pi])^2 = (b_1 \cdots b_{r-1})^2$ divides $\mathrm{disc}(A[\pi])$. On the other hand, b_1^i divides b_i, so $b_1^{2(1+2+3+\cdots+(r-1))} = b_1^{r(r-1)}$ divides $\mathrm{disc}(A[\pi])$. This proves (3). □

3. Endomorphism rings of Drinfeld modules

Let the notation and assumptions be as at the beginning of Section 1.2. In particular, ϕ is a Drinfeld module of rank r over a finite extension k of $\mathbb{F}_{\mathfrak{p}}$, $\mathcal{E} = \mathrm{End}_k(\phi)$, and $A[\pi] \subset \mathcal{E}$ is the suborder generated by the Frobenius endomorphism of ϕ. As in Section 1.2, assume (1.1).

Theorem 3.1. *Let $(b_1, \dots, b_{r-1})$ be the Frobenius index of ϕ. For each $1 \le i \le r-1$, 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. Theorem 2.1, applied to $A[\pi] \subset \mathcal{E}$, implies the existence of monic polynomials f_i of degree i, $1 \le i \le r-1$, such that $f_i(\pi) \in b_i\mathcal{E}$.

Now assume there is a monic polynomial $g(x) \in A[x]$ of degree i and $b \in A$ such that $g(\pi) \in b\mathcal{E}$. Suppose there is a prime $\mathfrak{q} \in A$ such that $\mathfrak{q} \mid b$ but $\mathfrak{q} \nmid b_i$. Then we can find $z_1, z_2 \in A$ such that $z_1 b_i + z_2 \mathfrak{q} = 1$. The polynomial $z_1 b_i g(x) + z_2 \mathfrak{q} f_i(x) \in A[x]$ is monic of degree i, and $(z_1 b_i g(\pi) + z_2 \mathfrak{q} f_i(\pi))/\mathfrak{q} b_i \in \mathcal{E}$. Since the largest exponent of π in $z_1 b_i g(\pi) + z_2 \mathfrak{q} f_i(\pi)$ is i, there exist $a_0, \dots, a_i \in A$ such that

$$\frac{z_1 b_i g(\pi) + z_2 \mathfrak{q} f_i(\pi)}{\mathfrak{q} b_i} = a_0 + a_1 \frac{f_1(\pi)}{b_1} + \cdots + a_i \frac{f_i(\pi)}{b_i}.$$

Multiplying both sides by $b_i\mathfrak{q}$, we get an equation in $A[\pi]$ where the left hand side is a monic polynomial in π of degree i, while the right hand side has degree i in π and leading coefficient $a_i\mathfrak{q}$. This implies that π satisfies a polynomial in $A[x]$ of degree less than r, contradicting (1.1). Hence every prime divisor of b is also a divisor of b_i. Write $b = x_1 y_1$ and $b_i = x_2 y_2 z$, where x_1 and x_2 have the same prime divisors, y_1 and y_2 have the same prime divisors, $x_2 \mid x_1$, $y_1 \mid y_2$, and $\gcd(x_1, y_1) = \gcd(x_2, y_2) = \gcd(x_2, z) = \gcd(y_2, z) = 1$. As earlier, since $g(\pi)/b \in \mathcal{E}$, we can write

$$\frac{g(\pi)}{x_1 y_1} = a_0 + a_1 \frac{f_1(\pi)}{b_1} + \cdots + a_i \frac{f_i(\pi)}{x_2 y_2 z}.$$

After multiplying both sides by $x_1 y_2 z$, the coefficient of π^i on the left hand side of the resulting equation is $y_2 z/y_1$, whereas on the right hand side the corresponding coefficient is $a_i x_1/x_2$. Since x_1/x_2 is coprime to $y_2 z/y_1$, x_1 and x_2 must be equal, up to multiplicative units. Since $y_1 \mid y_2$, we see that b divides b_i. $\square$

Remark 3.2. The condition $f_i(\pi) \in b_i\mathcal{E}$ means that we have an equality $f_i(\pi) = u\phi_{b_i}$ in $k\{\tau\}$ for some $u \in \mathcal{E}$. From this it is obvious that $f_i(\pi)$ acts as 0 on $\phi[b_i]$. Conversely, it is not hard to prove that if b is coprime to $\mathfrak{p}$ and $g(\pi)$ acts as 0 on $\phi[b]$, then $g(\pi) \in b\mathcal{E}$; see the proof of Theorem 1.2 in [10]. Hence the previous theorem essentially says that $b_i \in A$ is the element of largest degree such that π acting on $\phi[b_i]$ satisfies a polynomial of degree i, whereas the minimal polynomial of π acting on any Tate module $T_{\mathfrak{l}}(\phi)$ has degree r.

Now suppose ϕ is the reduction at $\mathfrak{p}$ of a Drinfeld module Φ over F. Let $n \in A$ be a polynomial not divisible by $\mathfrak{p}$. Assume r is coprime to the characteristic of F. In [10], we proved a reciprocity law which says that $\mathfrak{p}$ splits completely in the Galois extension $F(\Phi[n])$ of F if and only if n divides both b_1 and $a_{r-1} + r$, where a_{r-1} is the coefficient of x^{r-1} in the minimal polynomial of π. The starting point of the proof of this result is the observation that we have an isomorphism $\Phi[n] \cong \phi[n]$ compatible with the action of the Frobenius at $\mathfrak{p}$ on $\Phi[n]$ and the action of π on $\phi[n]$. Then the proof proceeds by showing that π acts as a scalar on $\phi[n]$ if and only if $n \mid b_1$. As follows from the previous paragraph, this last fact is a special case of Theorem 3.1. Thus, Theorem 3.1 is a refinement of our reciprocity law in the sense that we give a Galois-theoretic interpretation of all b_i's, not just b_1. Moreover, as we will see Section 4, $b_1, \dots, b_{r-1}$ appear in a matrix representing the Frobenius at $\mathfrak{p}$ in $\mathrm{Gal}(F(\Phi[n])/F) \subseteq \mathrm{GL}_r(A/nA)$.

Theorem 3.1 can be used to give an efficient algorithm for computing the Frobenius index of a Drinfeld module and an A-basis of its endomorphism ring. The algorithm has two main steps.

Step 1. Let ϕ be a Drinfeld module of rank r over k given in terms of $\phi_T \in k\{\tau\}$. Let B be the integral closure of A in K.

Start by computing the minimal polynomial $P(x) \in A[x]$ of π over A. (Note that under our assumption (1.1), $P(x)$ is also the characteristic polynomial of the Frobenius automorphism $\alpha \mapsto \alpha^{\#k}$ of $\mathrm{Gal}(\bar{k}/k)$ acting on $T_{\mathfrak{l}}(\phi)$ for any $\mathfrak{l} \neq \mathfrak{p}$.) When $k = \mathbb{F}_{\mathfrak{p}}$, computing $P(x)$ is relatively easy and quick; see [10, §5.1]. When $[k : \mathbb{F}_{\mathfrak{p}}] > 1$, this calculation becomes more involved. An algorithm for computing $P(x)$ for $r = 2$ and arbitrary k is described in [13, §3]. For general k and r, one can compute $P(x)$ using the following effective, but rather inefficient, method. One knows that $P(x) = \sum_{i=0}^{r_1} c_i x^i \in A[x]$ is a monic polynomial of degree $r_1 \mid r$ (our assumption (1.1) is equivalent to $r_1 = r$); moreover, from the analogue of the Riemann hypothesis for Drinfeld modules, one can deduce that $\deg(c_i) \leq [k : \mathbb{F}_q](r_1 - i)/r$ for all $0 \leq i \leq r_1 - 1$. This gives finitely many possibilities for $P(x)$, so, after arranging these polynomials by increasing degrees, one can simply go through this list, and the first polynomial that satisfies $P(\pi) = 0$ will be the minimal polynomial.

Next, compute the index $\chi(B/A[\pi])$. There are known algorithms for computing a basis of the integral closure of A in a field extension of F given by an explicit polynomial (the polynomial in our case is $P(x)$); such an algorithm is implemented in `Magma`. The index $\chi(B/A[\pi])$ can be computed by expressing π in a given A-basis of B. Alternatively, if K/F is separable, then $\chi(B/A[\pi])$ can be computed from $\mathrm{disc}(A[\pi])$ and $\mathrm{disc}(B)$, since by (2.1)

$$\mathrm{disc}(A[\pi]) = \chi(B/A[\pi])^2 \cdot \mathrm{disc}(B).$$

(In fact, for our purposes, it is enough to have an upper bound on $\chi(B/A[\pi])$ which is already provided by $\mathrm{disc}(A[\pi])$.)

Having computed the index $\chi(B/A[\pi])$, one can produce a finite list of possible Frobenius indices $(b_1, \dots, b_{r-1})$. Indeed, by (2.2),

$$\chi(B/A[\pi]) = \chi(B/\mathcal{E}) \cdot \chi(\mathcal{E}/A[\pi]),$$

and $\chi(\mathcal{E}/A[\pi]) = \left(\prod_{i=1}^{r-1} b_i\right)$ divides $\chi(B/A[\pi])$. We get further constrains on possible $(b_1, \dots, b_{r-1})$ from the divisibilities (cf. Proposition 2.3)

$$\begin{aligned}
&b_i \mid b_j, \quad 1 \leq i < j \leq r-1, \\
&b_i b_j \mid b_{i+j}, \quad i + j < r, \\
&\text{if } 0 < \deg(b_1), \text{ then } \deg(b_1) < \deg(b_2) < \cdots < \deg(b_{r-1}), \\
&b_1^{r(r-1)} \mid \mathrm{disc}(A[\pi]).
\end{aligned}$$

We arrange all possible $(b_1, \dots, b_{r-1})$ by the degrees of products $\prod_{i=1}^{r-1} b_i$, from the highest to zero.

Step 2. Starting with the first entry in our list of possible $(b_1, \dots, b_{r-1})$, check if for all $i = 1, \dots, r-1$ there are polynomials $f_i(x) \in A[x]$, $\deg_x(f_i(x)) = i$, such that $f_i(\pi) \in b_i\mathcal{E}$.

Given a polynomial

$$g(x) = x^s + a_{s-1}x^{s-1} + \cdots + a_0,$$

checking whether $g(\pi) \in b\mathcal{E}$ can be done as follows. First, compute the residue of $\pi^s + \phi_{a_{s-1}}\pi^{s-1} + \cdots + \phi_{a_0}$ modulo ϕ_b using the right division algorithm in $k\{\tau\}$. 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 $u \in k\{\tau\}$ produced by the division algorithm. Now check if the commutation relation $u\phi_T = \phi_T u$ holds in $k\{\tau\}$; this relation holds if and only if $u \in \mathcal{E}$.

Since we can assume that the coefficients of $f_i(x) \in A[x]$ have degrees $< \deg(b_i)$ (as polynomials in T), there are only finitely many possibilities for $f_i(x)$. If for some possible choice of $f_1, \dots, f_{r-1}$ we have $f_i(\pi) \in b_i\mathcal{E}$, then $(b_1, \dots, b_{r-1})$ is the Frobenius index of ϕ. If none of the choices of $f_1, \dots, f_{r-1}$ work, then $(b_1, \dots, b_{r-1})$ is not the Frobenius index and we move to the next possible Frobenius index. Since one of $(b_1, \dots, b_{r-1})$'s is the actual Frobenius index, this step will eventually find it. (There can be several "candidate" Frobenius indices satisfying the necessary condition of this step, i.e., the existence of f_i's. One can distinguish the actual Frobenius index among these "candidate" Frobenius indices using the maximality property of Frobenius indices given by Theorem 1.1. Since we have arranged the list of possible Frobenius indices by decreasing degrees of $\prod_{i=1}^{r-1} b_i$, we always find the actual Frobenius index first.)

Finally, having determined the Frobenius index $(b_1, \dots, b_{r-1})$ of ϕ and the polynomials $f_1, \dots, f_{r-1}$ such that $f_i(\pi) \in b_i\mathcal{E}$, we compute an explicit A-basis of $\mathcal{E}$ in $k\{\tau\}$ by dividing $f_i(\pi)$ by ϕ_{b_i} using the division algorithm for $k\{\tau\}$.

We have implemented the above algorithm in `Magma` and computed the Frobenius indices and bases of endomorphism rings for various Drinfeld modules of rank $r = 2$ and 3. For rank 2 this algorithm corroborates the data found by our previous (different) algorithm [10]. For rank 3, we have found many examples where b_1 and b_2 have positive degrees.

Example 3.3. Let $q = 5$, $r = 3$, $\mathfrak{p} = T^6+3T^5+T^2+3T+3$, and $k = \mathbb{F}_\mathfrak{p}$. Let $\phi : A \to \mathbb{F}_\mathfrak{p}\{\tau\}$ 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

$$\begin{aligned} \operatorname{disc}(A[\pi]) &= (T+4)^6(T^4 + 2T^3 + 4T^2 + 3T + 4), \\ \operatorname{disc}(B) &= (T^4 + 2T^3 + 4T^2 + 3T + 4). \end{aligned}$$

Hence $\chi(B/A[\pi]) = (T+4)^3$. 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 $0 \le n \le 3$. The second step of our algorithm confirms that in fact $b_1 = T+4$ and $b_2 = (T+4)^2$. In particular, $\mathcal{E} = B$. 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

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

Example 3.4. Let $q=7$, $r=3$, $\mathfrak{p} = T^5+T^4+4T^3+2T^2+1$, and $k = \mathbb{F}_\mathfrak{p}$. Let $\phi : A \to \mathbb{F}_\mathfrak{p}\{\tau\}$ 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 $A \to \mathbb{F}_\mathfrak{p}$. In this case, $P(x) = x^3 + (3T+3)x^2 + (6T^3+5T^2+3T+6)x + 6\mathfrak{p}$, $b_1 = 1$, $b_2 = T+6$, and $f_1(x) = x$, $f_2(x) = x^2+x+1$.

Remark 3.5. In [15], Kuhn and Pink gave a different algorithm for computing $\mathrm{End}_k(\phi)$. They work in the most general setting where A is a finitely generated normal integral domain of transcendence degree 1 over a finite field $\mathbb{F}_q$, k is an arbitrary finitely generated field, and no restrictions on D are imposed. On the other hand, the emphasis of [15] is on the existence of a deterministic algorithm that computes $\mathrm{End}_k(\phi)$ rather that its practicality, so some of the details of the algorithm are left out.

In the case where $A = \mathbb{F}_q[T]$ and k is finite, the approach of Kuhn and Pink is the following. Consider $k\{\tau\}$ as a free module of finite rank over $R := \mathbb{F}_q[\pi]$. (Note that R is the center of $k\{\tau\}$). Choose an R-basis of $k\{\tau\}$. For example, if $n = [k : \mathbb{F}_q]$ and $\alpha_0, \dots, \alpha_{n-1}$ is an $\mathbb{F}_q$-basis of k, then $\{\beta_{ij} := \alpha_i\tau^j \mid 0 \le i,j \le n-1\}$ is a basis of $k\{\tau\}$ over R. Express $\phi_T \in k\{\tau\}$ in terms of this basis $\phi_T = \sum_{0\le i,j\le r-1} m_{ij}\beta_{ij}$. Let $u = \sum_{0\le i,j\le r-1} x_{ij}\beta_{ij}$, where x_{ij} are indeterminates. Now $u \in \mathrm{End}_k(\phi)$ if and only if $u\phi_T = \phi_T u$. This leads to a system of linear equations in x_{ij}'s (note that β_{ij}'s do not commute with each other, so expanding both sides $u\phi_T = \phi_T u$ in terms of the chosen basis leads to nontrivial linear equations for x_{ij}). Choosing a basis for the space of solutions of the resulting system of linear equations gives a basis $e_1, \dots, e_s \in k\{\tau\}$ of $\mathrm{End}_k(\phi)$ as an R-module. Next, one computes the action of ϕ_T on this basis, which gives an explicit matrix for the action of ϕ_T as an R-linear transformation of $\mathrm{End}_k(\phi)$. It is then claimed in [15] (proof of Proposition 5.14) that this calculation yields a basis of $\mathrm{End}_k(\phi)$ as an A-module, although the details of this deduction are not explained. We have not pursued this line of calculations, so we are unable to say how complicated it is in practice, and whether it suffices for deducing the finer number-theoretic properties of $\mathrm{End}_k(\phi)$, such as its discriminant over A or the Frobenius index.

Please cite this article in press as: S. Garai, M. Papikian, Computing endomorphism rings and Frobenius matrices of Drinfeld modules, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2019.11.018

4. Matrix of the Frobenius automorphism

Let the notation and assumptions be as in Section 3. In particular, ϕ is a Drinfeld module of rank r over a finite extension k of $\mathbb{F}_\mathfrak{p}$, and ϕ satisfies (1.1). Moreover, $\mathcal{E} = \mathrm{End}_k(\phi)$, $A[\pi] \subset \mathcal{E}$ is the suborder generated by the Frobenius endomorphism of ϕ, and B is the integral closure of A in $F(\pi)$.

Let

$$P(x) = x^r + c_{r-1}x^{r-1} + \cdots + c_1 x + c_0$$

be the minimal polynomial of π over A, and

$$f_i(x) = x^i + \sum_{j=0}^{i-1} a_{ij}x^j, \qquad 1 \leq i \leq r-1$$

be the polynomials from Theorem 2.1. Multiplication by π induces an A-linear transformation of $\mathcal{E}$. The matrix of this transformation with respect to the basis in Theorem 2.1 has the form

$$\mathcal{F}_k := \begin{bmatrix} -a_{10} & * & \cdots & * & * \\ b_1 & a_{10}-a_{21} & \cdots & * & * \\ 0 & \frac{b_2}{b_1} & a_{21}-a_{32} & * & * \\ \vdots & & \ddots & & \\ 0 & 0 & \cdots & \frac{b_{r-1}}{b_{r-2}} & a_{r-1,r-2}-c_{r-1} \end{bmatrix}. \tag{4.1}$$

(If $\mathcal{E} = A[\pi]$, then $b_1 = \cdots = b_{r-1} = 1$, all $a_{ij} = 0$, and $\mathcal{F}_k$ is simply the companion matrix of $P(x)$.) The entries of $\mathcal{F}_k$ marked by $*$ are complicated expressions in the coefficients of f_i and P.

Example 4.1. For $r = 2$, the full matrix is $\begin{bmatrix} -a_{10} & \frac{-a_{10}(a_{10}-c_1)-c_0}{b_1} \\ b_1 & a_{10}-c_1 \end{bmatrix}$. Assume now that $r = 2$ and q is odd. Let $\Delta = \mathrm{disc}(\mathcal{E})$, so that $\mathcal{E} = A + \sqrt{\Delta}A$. Then $A[\pi] = A + b_1\sqrt{\Delta}A$. Thus, $\pi = \alpha + b_1\sqrt{\Delta}\beta$ with $\alpha, \beta \in A$. This implies $(\pi - \alpha)/b_1 \in \mathcal{E}$, so $\alpha = -a_{10}$. Now

$$\pi^2 = (\alpha + b_1\sqrt{\Delta}\beta)^2 = (\alpha^2 + b_1^2\Delta\beta^2) + 2\alpha\beta b_1\sqrt{\Delta},$$

and also $\pi^2 + c_1\pi + c_0 = 0$. Therefore,

$$(\alpha^2 + b_1^2\Delta\beta^2) + 2\alpha\beta b_1\sqrt{\Delta} + c_1\alpha + c_1 b_1\sqrt{\Delta}\beta + c_0 = 0,$$

which implies $(2\alpha + c_1)b_1\beta\sqrt{\Delta} = 0$. Thus, $\alpha = -c_1/2$. Combining this with our earlier observation, we obtain $a_{10} = c_1/2$, which, when substituted into the matrix of the

Please cite this article in press as: S. Garai, M. Papikian, Computing endomorphism rings and Frobenius matrices of Drinfeld modules, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2019.11.018

Frobenius, gives $\begin{bmatrix} -\frac{c_1}{2} & (c_1^2/4 - c_0)/b_1 \\ b_1 & -\frac{c_1}{2} \end{bmatrix}$. On the other hand, $c_1^2 - 4c_0 = \mathrm{disc}(A[\pi]) = b_1^2\Delta$. Therefore,

$$\mathcal{F}_k = \begin{bmatrix} -\frac{c_1}{2} & \frac{b_1 \cdot \mathrm{disc}(\mathcal{E})}{4} \\ b_1 & -\frac{c_1}{2} \end{bmatrix}.$$

Example 4.2. For $r = 3$, the full matrix is

$$\begin{bmatrix} -a_{10} & \frac{a_{10}(a_{21}-a_{10})-a_{20}}{b_1} & \frac{a_{10}a_{21}(a_{21}-c_2)-a_{10}(a_{20}-c_1)-a_{20}(a_{21}-c_2)-c_0}{b_2} \\ b_1 & a_{10} - a_{21} & \frac{(a_{20}-c_1)-a_{21}(a_{21}-c_2)}{b_2/b_1} \\ 0 & \frac{b_2}{b_1} & a_{21} - c_2 \end{bmatrix}. \tag{4.2}$$

As an explicit example, the matrix corresponding to Example 3.3 is

$$\begin{bmatrix} 1 & 0 & T^4 + T^2 + 2T + 1 \\ T + 4 & 1 & 2T^3 + 2T^2 + 2T + 4 \\ 0 & T + 4 & 3(T^2 + 1) \end{bmatrix}, \tag{4.3}$$

and the matrix corresponding to Example 3.4 is

$$\begin{bmatrix} 0 & 6 & T^4 + 2T^3 + 6T^2 + T + 4 \\ 1 & 6 & T^2 + 3T + 3 \\ 0 & T + 6 & 4T + 5 \end{bmatrix}.$$

Remark 4.3. Even though fractions appear in $\mathcal{F}_k$, all entries of this matrix are in A. This implies that there are non-obvious congruence relations between the coefficients of f_i, P, and the Frobenius indices b_j. For example, from (4.2) we get $a_{10}(a_{21} - a_{10}) \equiv a_{20} \pmod{b_1}$. Also note that by Proposition 2.3, b_1 divides all b_i/b_{i-1}, $2 \leq i \leq r-1$, appearing below the main diagonal in $\mathcal{F}_k$, so if $n \mid b_1$, then $\mathcal{F}_k$ is upper-triangular modulo n. In fact, it follows from Theorem 3.1 in [10] that if $n \mid b_1$ then $\mathcal{F}_k$ modulo n is a scalar matrix.

Let $\mathfrak{l} \lhd A$ be a prime different from $\mathfrak{p}$. The arithmetic Frobenius automorphism $\mathrm{Frob}_k \in \mathrm{Gal}(\bar{k}/k)$ naturally acts on $T_\mathfrak{l}(\phi)$. Let $\mathrm{ch}_k(x) \in A_\mathfrak{l}[x]$ denote the characteristic polynomial of $\mathrm{Frob}_k \in \mathrm{Aut}_{A_\mathfrak{l}}(T_\mathfrak{l}(\phi)) \cong \mathrm{GL}_r(A_\mathfrak{l})$. The conjugacy class of Frob_k in $\mathrm{Aut}_{F_\mathfrak{l}}(T_\mathfrak{l}(\phi) \otimes F_\mathfrak{l}) \cong \mathrm{GL}_r(F_\mathfrak{l})$ is uniquely determined by $\mathrm{ch}_k(x)$ because $T_\mathfrak{l}(\phi) \otimes F_\mathfrak{l}$ is a semi-simple $F_\mathfrak{l}[\mathrm{Frob}_k]$-module; cf. [23]. On the other hand, $\mathrm{ch}_k(x)$ alone is not sufficient for determining the conjugacy class of Frob_k in $\mathrm{Aut}_{A_\mathfrak{l}}(T_\mathfrak{l}(\phi))$.

Theorem 4.4. *Assume $T_\mathfrak{l}(\phi)$, under the natural action of $\mathcal{E}_\mathfrak{l} := \mathcal{E} \otimes_A A_\mathfrak{l}$, is a free module of rank 1. Then the matrix $\mathcal{F}_k$ describes the action of* Frob_k *on $T_\mathfrak{l}(\phi)$, with respect to a suitable $A_\mathfrak{l}$-basis.*

Please cite this article in press as: S. Garai, M. Papikian, Computing endomorphism rings and Frobenius matrices of Drinfeld modules, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2019.11.018

Proof. The action of Frob_k on $T_\mathfrak{l}(\phi)$ agrees with the action induced by $\pi \in \mathcal{E}$. If the assumption of the theorem holds, then there is an isomorphism $T_\mathfrak{l}(\phi) \cong \mathcal{E}_\mathfrak{l}$ compatible with the actions of π on both sides. For the choice of a basis of $\mathcal{E}$ from Theorem 2.1, π acts on $\mathcal{E}$ by the matrix $\mathcal{F}_k$. $\square$

Remark 4.5. Note that $\mathcal{E}_\mathfrak{l} \otimes F_\mathfrak{l}$ is a semi-simple $F_\mathfrak{l}$-algebra which acts faithfully on $T_\mathfrak{l}(\phi) \otimes F_\mathfrak{l}$, so $T_\mathfrak{l}(\phi) \otimes F_\mathfrak{l}$ is free of rank 1 over $\mathcal{E}_\mathfrak{l} \otimes F_\mathfrak{l}$. On the other hand, as we will see later in this section, $T_\mathfrak{l}(\phi)$ is not always free over $\mathcal{E}_\mathfrak{l}$. Also note that in our case the characteristic polynomial $\mathrm{ch}_k(x)$ is the minimal polynomial $P(x)$ of π over A.

Let $\Phi : A \to F\{\tau\}$ be a Drinfeld module of rank r over F. Let $\mathfrak{p}$ be a prime of good reduction of Φ. Denote by ϕ the reduction of Φ modulo $\mathfrak{p}$. Let $\mathcal{E} = \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\phi)$ and $A[\pi] \subset \mathcal{E}$ be its suborder generated by the Frobenius endomorphism $\pi = \tau^{\deg(\mathfrak{p})}$ of ϕ. Note that since we are working over the field $\mathbb{F}_\mathfrak{p}$, the assumption (1.1) is satisfied for ϕ; cf. [10, Prop. 2.1]. Denote by $\mathcal{F}(\mathfrak{p})$ the matrix (4.1) for ϕ over $\mathbb{F}_\mathfrak{p}$.

Theorem 4.6. *Let $n \in A$ be a nonzero element not divisible by $\mathfrak{p}$. The Galois extension $F(\Phi[n])/F$ is unramified at $\mathfrak{p}$. Suppose for every prime $\mathfrak{l} \lhd A$ dividing n the Tate module $T_\mathfrak{l}(\phi)$ is a free $\mathcal{E}_\mathfrak{l}$-module of rank 1. Then the integral matrix $\mathcal{F}(\mathfrak{p})$, when reduced modulo n, represents the class of the Frobenius at $\mathfrak{p}$ in $\mathrm{Gal}(F(\Phi[n])/F) \subseteq \mathrm{GL}_r(A/nA)$.*

Proof. The fact that $\mathfrak{p}$ is unramified in $F(\Phi[n])/F$ is well-known, since $\mathfrak{p}$ is a prime of good reduction for Φ and does not divide n; cf. [24]. In fact, by [24], the Tate module $T_\mathfrak{l}(\Phi)$ is unramified at $\mathfrak{p}$, i.e., for any place $\bar{\mathfrak{p}}$ in F^{sep} extending $\mathfrak{p}$, the inertia group of $\bar{\mathfrak{p}}$ acts trivially on $T_\mathfrak{l}(\Phi)$. There is a canonical isomorphism $T_\mathfrak{l}(\Phi) \cong T_\mathfrak{l}(\phi)$ which is compatible with the action of a Frobenius element in the decomposition group of $\bar{\mathfrak{p}}$ on $T_\mathfrak{l}(\Phi)$ and the action of the arithmetic Frobenius automorphism $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(\overline{\mathbb{F}}_\mathfrak{p}/\mathbb{F}_\mathfrak{p})$ on $T_\mathfrak{l}(\phi)$; cf. [24, p. 479]. On the other hand, the action of $\mathrm{Frob}_\mathfrak{p}$ on $T_\mathfrak{l}(\phi)$ agrees with the action induced by $\pi \in \mathcal{E}$.

If the assumption of the theorem holds, then there is an isomorphism $\phi[n] \cong \mathcal{E}/n\mathcal{E}$ compatible with the actions of π on both sides. For the choice of a basis of $\mathcal{E}$ from Theorem 2.1, π acts on $\mathcal{E}/n\mathcal{E} \cong (A/nA)^r$ by the matrix $\mathcal{F}(\mathfrak{p})$ reduced modulo n. Combining this with the isomorphism $\Phi[n] \cong \phi[n]$ compatible with the action of the Frobenius automorphism on both sides, we see that $\mathcal{F}(\mathfrak{p}) \pmod n$ indeed represents the class of the Frobenius at $\mathfrak{p}$ in $\mathrm{Gal}(F(\Phi[n])/F) \subseteq \mathrm{GL}_r(A/nA)$. $\square$

Remark 4.7. Theorems 4.4 and 4.6 are analogues of a result of Duke and Tóth [8] for elliptic curves (see also Theorems 2 and 3 in [3]).

Theorem 4.6 essentially says that the matrix $\mathcal{F}(\mathfrak{p}) \in \mathrm{Mat}_r(A)$ is a "universal" matrix of the Frobenius automorphism at $\mathfrak{p}$ in the division fields of Φ, in the sense that to get a matrix in the conjugacy class of the Frobenius in the Galois groups of different division fields $F(\Phi[n])$ we just need to reduce $\mathcal{F}(\mathfrak{p})$ modulo the correspond n. But there

Please cite this article in press as: S. Garai, M. Papikian, Computing endomorphism rings and Frobenius matrices of Drinfeld modules, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2019.11.018

is a technical assumption in the theorem about the freeness of the Tate modules of ϕ as modules over the endomorphism ring of ϕ. For the rest of this section we examine this assumption more carefully and show that it is a mild assumption, although quite subtle. Our considerations are motivated by [22, §4] and [3].

Definition 4.8. Let $\mathfrak{l} \lhd A$ be a prime. Let R be a finite flat local $A_\mathfrak{l}$-algebra with maximal ideal $\mathfrak{M}$. Let $\bar{R} = R/\mathfrak{l}R$, and denote the maximal ideal of $\bar{R}$ by $\overline{\mathfrak{M}}$. The following statements are equivalent (see [25, Prop. 1.4], [2], [19, §18]):

1. $\mathrm{Hom}_{A_\mathfrak{l}}(R, A_\mathfrak{l})$ is free of rank 1 over R.
2. $\mathrm{Hom}_{\mathbb{F}_\mathfrak{l}}(\bar{R}, \mathbb{F}_\mathfrak{l})$ is free of rank 1 over $\bar{R}$.
3. $\bar{R}[\overline{\mathfrak{M}}] = \{a \in \bar{R} \mid ma = 0 \text{ for all } m \in \overline{\mathfrak{M}}\}$ is 1-dimensional over $\overline{R}/\overline{\mathfrak{M}}$.

We say that R is *Gorenstein* if it satisfies these conditions. We say that a finite flat (not necessarily local) $A_\mathfrak{l}$-algebra R is *Gorenstein* if its localization at every maximal ideal is a Gorenstein local ring.

Theorem 4.9. *Let $\mathfrak{l} \lhd A$ be a prime different from $\mathfrak{p}$. If $\mathcal{E}_\mathfrak{l}$ is a Gorenstein ring, then $T_\mathfrak{l}(\phi)$ is a free $\mathcal{E}_\mathfrak{l}$-module of rank 1.*

Proof. The ring $\mathcal{E}_\mathfrak{l}$ is a finite flat $A_\mathfrak{l}$-algebra. The module $T_\mathfrak{l}(\phi)$ is a torsion-free $\mathcal{E}_\mathfrak{l}$-module. Suppose $\mathcal{E}_\mathfrak{l}$ is Gorenstein. Then by Theorem 6.2 and Proposition 7.2 in [2], either $T_\mathfrak{l}(\phi)$ is a projective $\mathcal{E}_\mathfrak{l}$-module or $T_\mathfrak{l}(\phi)$ is an $\mathcal{E}'_\mathfrak{l}$-module for some $\mathcal{E}_\mathfrak{l} \subsetneq \mathcal{E}'_\mathfrak{l} \subset B \otimes_A A_\mathfrak{l}$. Suppose the latter is the case. Let $G := \mathrm{Gal}(\overline{\mathbb{F}}_\mathfrak{p}/\mathbb{F}_\mathfrak{p})$. By [26, Thm. 2], we have an isomorphism

$$\mathcal{E}_\mathfrak{l} \xrightarrow{\sim} \mathrm{End}_{A_\mathfrak{l}[G]}(T_\mathfrak{l}(\phi)). \tag{4.4}$$

Since $\mathcal{E}'_\mathfrak{l} \otimes F_\mathfrak{l} = \mathcal{E}_\mathfrak{l} \otimes F_\mathfrak{l}$ and $\mathcal{E}_\mathfrak{l} \otimes F_\mathfrak{l} \xrightarrow{\sim} \mathrm{End}_{F_\mathfrak{l}[G]}(T_\mathfrak{l}(\phi) \otimes F_\mathfrak{l})$, the action of $\mathcal{E}'_\mathfrak{l}$ on $T_\mathfrak{l}(\phi)$ has to commute with the action of G. Hence $\mathcal{E}'_\mathfrak{l} \subseteq \mathrm{End}_{A_\mathfrak{l}[G]}(T_\mathfrak{l}(\phi)) = \mathcal{E}_\mathfrak{l}$. This contradicts our earlier assumption. We conclude that $T_\mathfrak{l}(\phi)$ is a projective $\mathcal{E}_\mathfrak{l}$-module. Since $\mathcal{E}_\mathfrak{l}$ is a semilocal ring, a projective module over $\mathcal{E}_\mathfrak{l}$ is free by [19, Thm. 2.5]. In particular, $T_\mathfrak{l}(\phi)$ is free. Finally, since the ranks of $T_\mathfrak{l}(\phi)$ and $\mathcal{E}_\mathfrak{l}$ over $A_\mathfrak{l}$ are the same, $T_\mathfrak{l}(\phi)$ is a free $\mathcal{E}_\mathfrak{l}$-module of rank 1. $\square$

Proposition 4.10. *Suppose one of the following conditions holds:*

1. $\mathcal{E}_\mathfrak{l} = A_\mathfrak{l}[\pi]$.
2. $r = 2$.
3. $\mathcal{E}_\mathfrak{l} = B \otimes_A A_\mathfrak{l}$.

Then $\mathcal{E}_\mathfrak{l}$ is Gorenstein. In particular, if $\mathfrak{l}$ does not divide $\chi(\mathcal{E}/A[\pi])$ or $\chi(B/\mathcal{E})$, then $\mathcal{E}_\mathfrak{l}$ is Gorenstein.

Proof. (1) If $\mathcal{E}_\mathfrak{l}$ is generated over $A_\mathfrak{l}$ by one element, then $\mathcal{E}_\mathfrak{l}$ is Gorenstein; cf. [25, p. 329]. (2) If $r = 2$, then $\mathcal{E}_\mathfrak{l}$ is obviously generated by one element (any of the elements which is not in $A_\mathfrak{l} \subset \mathcal{E}_\mathfrak{l}$). (3) $B \otimes_A A_\mathfrak{l}$ is a product of discrete valuation rings, and such rings are Gorenstein (see again [25, p. 329]). □

Example 4.11. Let $q = 5$ and $\Phi : A \to F\{\tau\}$ be given by $\Phi_T = T + T\tau + T\tau^2 + \tau^3$. Every prime of A is a prime of good reduction for Φ. Take $\mathfrak{p} = T^6 + 3T^5 + T^2 + 3T + 3$. Then ϕ, the reduction of Φ modulo $\mathfrak{p}$, is the Drinfeld module from Example 3.3. We showed that in this case $\mathcal{E} = B$, so the assumption of Theorem 4.6 is satisfied for every prime $\mathfrak{l} \neq \mathfrak{p}$. Note that the matrix (4.3), which is $\mathcal{F}(\mathfrak{p})$ associated to ϕ, is congruent to the identity matrix modulo n if and only if $n = T + 4$. This means that $\mathfrak{p}$ splits completely in $F(\Phi[n])$ if and only if $n = T + 4$.

Example 4.12. We give an example where $\mathcal{E}_\mathfrak{l}$ is not Gorenstein by changing $\mathfrak{p}$ in Example 4.11. Let Φ be as in that example, but ϕ be the reduction of Φ modulo

$$\mathfrak{p} = T^6 + 4T^4 + 4T^2 + T + 1.$$

The minimal polynomial of π is

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

and

$$\begin{aligned} \operatorname{disc}(A[\pi]) &= (T+4)^6(T^4 + 3T^3 + T^2 + 2), \\ \operatorname{disc}(B) &= T^4 + 3T^3 + T^2 + 2. \end{aligned}$$

Our algorithm shows that

$$b_1 = 1, \quad b_2 = T + 4, \quad \chi(\mathcal{E}/A[\pi]) = T + 4, \quad \chi(B/\mathcal{E}) = (T+4)^2,$$

and an A-basis of $\mathcal{E}$ is given by

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

(Although we will not need this, an A-basis of B is given by $e_1, e_2/(T+4), e_3/(T+4)$.)

Let $\mathfrak{l} = T + 4$. We claim that $\mathcal{E}_\mathfrak{l}$ is not Gorenstein. By a routine calculation one obtains the relations

$$\begin{aligned} e_2^2 &= (T+4)e_3 \\ e_3^2 &= (T+1)(T+3)(T+4)^2(T^2+2)e_1 + (T+4)(T^3+3T+2)e_2 + (T+4)T^2e_3 \\ e_2e_3 &= (T+3)(T+4)^2(T^2+2)e_1 + 2(T+2)(T+4)^2e_2 + 3(T+1)(T+4)e_3. \end{aligned}$$

From this it is easy to see that $\mathcal{E}_\mathfrak{l}$ is local with maximal ideal $\mathfrak{M} = (\mathfrak{l}, e_2, e_3)$. To prove that $\mathcal{E}_\mathfrak{l}$ is not Gorenstein, we check (3) from Definition 4.8. In our case, $\bar{\mathcal{E}}_\mathfrak{l} = \mathbb{F}_\mathfrak{l} + \mathbb{F}_\mathfrak{l}\bar{e}_2 + \mathbb{F}_\mathfrak{l}\bar{e}_3$, $\overline{\mathfrak{M}} = (\bar{e}_2, \bar{e}_3)$, and

$$\bar{e}_2^2 = \bar{e}_3^2 = \bar{e}_2\bar{e}_3 = 0. \tag{4.5}$$

Hence $\bar{\mathcal{E}}_\mathfrak{l}[\overline{\mathfrak{M}}] = \overline{\mathfrak{M}}$ is two-dimensional over $\mathbb{F}_\mathfrak{l}$, so $\mathcal{E}_\mathfrak{l}$ is not Gorenstein.

Of course, the fact that $R := \mathcal{E}_\mathfrak{l}$ is not Gorenstein does not necessarily imply that $M := T_\mathfrak{l}(\phi)$ is not free over R. For that, one needs an additional calculation. By a standard argument involving Nakayama's lemma one shows that M is a free R-module of rank 1 if and only if $\bar{M} = M/\mathfrak{l}M = \phi[\mathfrak{l}]$ is a free $\bar{R} = R/\mathfrak{l}R$-module of rank 1. We need to compute the action of $\bar{R}$ on $\phi[\mathfrak{l}]$ as a 3-dimensional vector space over $A/\mathfrak{l} \cong \mathbb{F}_5$.

Now $\phi[\mathfrak{l}]$ is the set of roots of the polynomial $\phi_\mathfrak{l}(x) = x^{125} + tx^{25} + tx^5 + (t+4)x \in \mathbb{F}_\mathfrak{p}[x]$, where t is the image of T in $\mathbb{F}_\mathfrak{p}$. This polynomial decomposes over $\mathbb{F}_\mathfrak{p}$ into a product of irreducible polynomials all of which have either degree 1 or degree 5. One of the irreducible factors of $\phi_\mathfrak{l}(x)$ of degree 5 is $g(x) = x^5 + (3t^3 + 2t^2 + 2t)x + t^5 + 3t^4 + 3t^2 + 2t$. Let α be a root of $g(x)$. Then the splitting field of $\phi_\mathfrak{l}(x)$ is $\mathbb{F}_\mathfrak{p}(\alpha)$. The following is an $\mathbb{F}_5$-basis of $\phi[\mathfrak{l}]$ in $\mathbb{F}_\mathfrak{p}(\alpha)$:

$$v_1 = t^5 + 2t^3 + t^2 + 3, \quad v_2 = \alpha, \quad v_3 = \alpha + t^5 + 3t^3 + 4t.$$

(We simply chose three, more-or-less random, roots v_1, v_2, v_3 of $\phi_\mathfrak{l}(x)$ and verified that they are linearly independent over $\mathbb{F}_5$.) To compute the action of e_2 and e_3 on $\phi[\mathfrak{l}]$ we use their explicit expressions in $\mathbb{F}_\mathfrak{p}\{\tau\}$ provided by our algorithm

$$\begin{aligned}
e_2 &= \tau^6 + 4 \\
e_3 &= \tau^9 + (3t^5 + 2t^3 + 2t^2 + 1)\tau^8 + (t^5 + t^4 + 4t^3 + 4t^2 + t + 3)\tau^7 \\
&\quad + (3t^5 + t^4 + 2t^2 + 3t + 1)\tau^6 + (2t^5 + 3t^4 + 3t^3 + t^2 + 3)\tau^5 \\
&\quad + (3t^4 + 2t^3 + 2t + 4)\tau^4 + (4t^5 + t^2 + 3t + 2)\tau^3 + (2t^4 + t^3 + t^2 + 4t + 4)\tau^2 \\
&\quad + (3t^5 + t^4 + 3t^3 + 4t^2 + t + 1)\tau + 4t^5 + 4t^4 + t.
\end{aligned}$$

With respect to the basis $\{v_1, v_2, v_3\}$ (as column vectors), e_2 and e_3 correspond to the following matrices:

$$\bar{e}_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 3 & 3 \\ 0 & 2 & 2 \end{bmatrix}, \qquad \bar{e}_3 = \begin{bmatrix} 0 & 0 & 0 \\ 4 & 3 & 3 \\ 1 & 2 & 2 \end{bmatrix}.$$

$\bar{M}$ is a free $\bar{R}$-module of rank 1 if and only if there is a vector $v \in \mathbb{F}_5^3$ such that $v, \bar{e}_2 v, \bar{e}_3 v$ are linearly independent over $\mathbb{F}_5$. It is easy to check that such a vector does not exist. Thus, in this example we encounter the strange phenomenon where $T_\mathfrak{l}(\phi)$ is not free over $\mathcal{E}_\mathfrak{l}$. Note also that one can consider ϕ as a Drinfeld $\mathcal{E}$-module of rank 1 in

Please cite this article in press as: S. Garai, M. Papikian, Computing endomorphism rings and Frobenius matrices of Drinfeld modules, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2019.11.018

the sense of Hayes [14, p. 180], and our calculation shows that, unlike the usual Drinfeld modules, $\phi[\mathfrak{l}]$ is not isomorphic to $\mathcal{E}/\mathfrak{l}\mathcal{E}$ as an $\mathcal{E}$-module.

Remark 4.13. The matrix $\mathcal{F}(\mathfrak{p})$ for the previous example is

$$\mathcal{F}(\mathfrak{p}) = \begin{bmatrix} 0 & 4 & (T+4)^2(T^3+3T^2+2) \\ 1 & 2 & 2(T+2)(T+4)^2 \\ 0 & T+4 & 3(T+2)(T+3) \end{bmatrix}$$

Hence $\mathcal{F}(\mathfrak{p}) \equiv \begin{bmatrix} 0 & 4 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix} \pmod{\mathfrak{l}}$. With respect to the basis $\{v_1, v_2, v_3\}$ of $\phi[\mathfrak{l}]$, the action of π on $\phi[\mathfrak{l}]$ is given by $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 3 \\ 0 & 2 & 3 \end{bmatrix}$, which is conjugate to $\mathcal{F}(\mathfrak{p}) \bmod \mathfrak{l}$ in $\mathrm{GL}_3(\mathbb{F}_5)$. Thus, the conclusion of Theorem 4.6 is still valid for $n = T+4$, even though its assumption fails.

References

[1] B. Angles, On some subrings of Ore polynomials connected with finite Drinfeld modules, J. Algebra 181 (2) (1996) 507–522.
[2] H. Bass, On the ubiquity of Gorenstein rings, Math. Z. 82 (1963) 8–28.
[3] T.G. Centeleghe, Integral Tate modules and splitting of primes in torsion fields of elliptic curves, Int. J. Number Theory 12 (1) (2016) 237–248.
[4] A.C. Cojocaru, M. Papikian, Drinfeld modules, Frobenius endomorphisms, and CM-liftings, Int. Math. Res. Not. 17 (2015) 7787–7825.
[5] A.C. Cojocaru, A.M. Shulman, The distribution of the first elementary divisor of the reductions of a generic Drinfeld module of arbitrary rank, Can. J. Math. 67 (6) (2015) 1326–1357.
[6] V.G. Drinfeld, Elliptic modules, Mat. Sb. (N. S.) 94 (136) (1974) 594–627, p. 656.
[7] V.G. Drinfeld, Elliptic modules. II, Mat. Sb. (N. S.) 102(144) (2) (1977) 182–194, p. 325.
[8] W. Duke, A. Tóth, The splitting of primes in division fields of elliptic curves, Exp. Math. 11 (4) (2002) 555–565, 2003.
[9] D.S. Dummit, R.M. Foote, Abstract Algebra, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004.
[10] S. Garai, M. Papikian, Endomorphism rings of reductions of Drinfeld modules, J. Number Theory (2020), in press, https://doi.org/10.1016/j.jnt.2019.02.008.
[11] E.-U. Gekeler, Sur les classes d'idéaux des ordres de certains corps gauches, C. R. Acad. Sci. Paris Sér. I Math. 309 (9) (1989) 577–580.
[12] E.-U. Gekeler, On finite Drinfeld modules, J. Algebra 141 (1) (1991) 187–203.
[13] E.-U. Gekeler, Frobenius distributions of Drinfeld modules over finite fields, Trans. Am. Math. Soc. 360 (4) (2008) 1695–1721.
[14] D.R. Hayes, Explicit class field theory in global function fields, in: Studies in Algebra and Number Theory, in: Adv. in Math. Suppl. Stud., vol. 6, Academic Press, New York–London, 1979, pp. 173–217.
[15] N. Kuhn, R. Pink, Finding endomorphisms of Drinfeld modules, arXiv:1608.02788.
[16] W. Kuo, Y.-R. Liu, Cyclicity of finite Drinfeld modules, J. Lond. Math. Soc. (2) 80 (3) (2009) 567–584.
[17] G. Laumon, Cohomology of Drinfeld modular varieties. Part I, in: Geometry, Counting of Points and Local Harmonic Analysis, in: Cambridge Studies in Advanced Mathematics, vol. 41, Cambridge University Press, Cambridge, 1996.
[18] D.A. Marcus, Number Fields, second edition, Universitext, Springer, Cham, 2018, with a foreword by Barry Mazur.

Please cite this article in press as: S. Garai, M. Papikian, Computing endomorphism rings and Frobenius matrices of Drinfeld modules, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2019.11.018

[19] H. Matsumura, Commutative Ring Theory, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989, translated from the Japanese by M. Reid.
[20] B. Mazur, Modular curves and the Eisenstein ideal, Publ. Math. IHÉS 47 (1977) 33–186, 1978, with an appendix by Mazur and M. Rapoport.
[21] J.-P. Serre, Local Fields, Graduate Texts in Mathematics, vol. 67, Springer, New York–Berlin, 1979, translated from the French by Marvin Jay Greenberg.
[22] J.-P. Serre, J. Tate, Good reduction of Abelian varieties, Ann. Math. (2) 88 (1968) 492–517.
[23] Y. Taguchi, Semisimplicity of the Galois representations attached to Drinfeld modules over fields of "finite characteristics", Duke Math. J. 62 (3) (1991) 593–599.
[24] T. Takahashi, Good reduction of elliptic modules, J. Math. Soc. Jpn. 34 (3) (1982) 475–487.
[25] J. Tilouine, Hecke algebras and the Gorenstein property, in: Modular Forms and Fermat's Last Theorem, Boston, MA, 1995, Springer, New York, 1997, pp. 327–342.
[26] J.-K. Yu, Isogenies of Drinfeld modules over finite fields, J. Number Theory 54 (1) (1995) 161–171.

Please cite this article in press as: S. Garai, M. Papikian, Computing endomorphism rings and Frobenius matrices of Drinfeld modules, J. Number Theory (2020), https://doi.org/10.1016/j.jnt.2019.11.018