Algorithms for computing norms and characteristic polynomials on general Drinfeld modules

Xavier Caruso, Antoine Leudière

Algorithms for computing norms and characteristic polynomials on general Drinfeld modules

Xavier Caruso[*], Antoine Leudière[†]

December 11, 2023

Abstract

We provide two families of algorithms to compute characteristic polynomials of endomorphisms and norms of isogenies of Drinfeld modules. Our algorithms work for Drinfeld modules of any rank, defined over any base curve. When the base curve is $\mathbb{P}^1_{\mathbb{F}_q}$, we do a thorough study of the complexity, demonstrating that our algorithms are, in many cases, the most asymptotically performant. The first family of algorithms relies on the correspondence between Drinfeld modules and Anderson motives, reducing the computation to linear algebra over a polynomial ring. The second family, available only for the Frobenius endomorphism, is based on a new formula expressing the characteristic polynomial of the Frobenius as a reduced norm in a central simple algebra.

Contents

[*]Université de Bordeaux, CNRS, INRIA, 351, cours de la Libération, 33405 Talence, France
[†]Université de Lorraine, INRIA, CNRS, 615 rue du Jardin Botanique, 54600 Villers-lès-Nancy, France

Introduction

Drinfeld modules were introduced in 1974 to serve as the fundations of the class field theory of function fields [Dri74]. Although they were initially considered as mathematical abstract objects, recent papers highlighted a growing interest for the computational aspects in these topics: in the recent years, a PhD thesis [Car18] and at least three papers focused on the algorithmics of Drinfeld modules [CGS20, MS19, MS23]. Due to their striking similarities with elliptic curves, Drinfeld modules were considered several times for their applications in cryptography [JN19, Sca01, BCDA22, LS23]. Other applications saw them being used to efficiently factor polynomials in $\mathbb{F}_q[T]$ [DNS21].

The present paper is a contribution to the algorithmic toolbox of Drinfeld modules. More precisely, we focus on the effective and efficient computation of characteristic polynomials of endomorphisms of Drinfeld modules, as well as norms of general isogenies.

Context. Before going deeper into our results, we recall briefly the purpose and the most significant achievements of the theory of Drinfeld modules. Classical class field theory aims at describing abelian extensions of local and global fields, using information available solely at the field's level [Che40, Con09]. Premises of the theory go back to Gauß' *Disquisitiones Arithmeticae*, and in 1853, Kronecker stated the famous Kronecker-Weber theorem: every abelian number field lies within a cyclotomic field [Kro53, Hil32]. Another crucial theorem from class field theory is the Kronecker *Jugendtraum*, relating maximal abelian unramified extensions of quadratic imaginary number fields and the theory of complex multiplication of elliptic curves. More generally, a result conjectured by Hilbert, and proved by Takagi in 1920 [Tak14], asserts that every number field K is contained within a maximal abelian unramified extension H whose class group is isomorphic to $\mathrm{Gal}(H/K)$. The field H is called the *Hilbert class field* of K and, apart from abelian number fields and imaginary quadratic number fields, it is generally hard to describe, yet even to compute.

The goal of Drinfeld modules is to set up an analogue ot these results for function fields. A Drinfeld module is an algebraic object which is defined within the following setting: a base curve C over $\mathbb{F}_q$ which is projective, smooth and geometrically connected (*e.g.* $C = \mathbb{P}^1_{\mathbb{F}_q}$); a fixed point ∞ of C; the ring A of rational functions on C regular outside ∞ (*e.g.* $A = \mathbb{F}_q[T]$); a base field K with a structure of A-algebra. We then talk about Drinfeld A-modules. An important feature of Drinfeld modules is that they endow the algebraic closure $\overline{K}$ of K with a structure of A-module. When $A = \mathbb{F}_q[T]$, this structure surprisingly ressembles to the $\mathbb{Z}$-module structure on the points of an elliptic curve. Important references on Drinfeld modules include [Gek91, Gos98, Ros02, Poo22, VS06, Hay11, Pap23].

The simplest Drinfeld modules are the rank 1 Drinfeld modules over the curve $\mathbb{P}^1_{\mathbb{F}_q}$, where K is the function field $\mathbb{F}_q(T)$, *i.e.* the Drinfeld $\mathbb{F}_q[T]$-modules of rank 1 over $\mathbb{F}_q(T)$. They were studied by Carlitz [Car35], and provide function field analogues of roots of unity, and consequently, of cyclotomic fields; the analogue of the Kronecker-Weber theorem was subsequently proved by Hayes [Hay74]. Coming to the *Jugendtraum*, we need to go to Drinfeld modules of rank 1 over general curves and Drinfeld $\mathbb{F}_q[T]$-modules or rank 2 over finite fields. The latter have a theory of complex multiplication which shares many similarities with that of elliptic curves over finite fields. As an illustration, we mention that the endomorphism ring of such a Drinfeld module is either an order in a quadratic imaginary function field or a maximal order in a quaternion algebra.

Algorithmic results. Like in the classical setting, the theory of complex multiplication of Drinfeld modules depends heavily on the notion of *characteristic polynomial of the Frobenius endomorphism*, which we compute in this paper. This polynomial lies in $A[X]$ and is an invariant of primary importance: it determines the isogeny class of the underlying Drinfeld module, it controls the theory of complex multiplication and it is the main building block in the construction of the attached L-function [Tae09]. Moreover, in the case of rank 2 Drinfeld modules over $\mathbb{F}_q[T]$, being ordinary is equivalent to having a middle term not divisible by the function field characteristic. The characteristic polynomial of the Frobenius also defines curves and extensions that naturally arise in the class field theory of function fields [LS23]. More generally, characteristic polynomials can be defined for any endomorphism in any rank and over any base.

In the present paper, we design algorithms for computing the characteristic polynomial of any endomorphism of a Drinfeld module on the one hand, and for computing the norm of any isogeny between Drinfeld modules on the other hand. When $A = \mathbb{F}_q[T]$, we moreover do a thorough analysis of their complexity. To state our complexity results, it is convenient to use Laudau's O-notation and some of its variants. Precisely, if f and g are two positive quantities depending on parameters, we write

- $g \in O(f)$ if there exists an absolute positive constant C such that $g \leqslant C \cdot f$,
- $g \in O^{\sim}(f)$ if there exist absolute positive constant C and k such that $g \leqslant C \cdot f \log^k f$,
- $g \in O^{\bullet}(f)$ if, for all $\varepsilon > 0$, there exists a positive constant C_ε such that $g \leqslant C_\varepsilon \cdot f^{1+\varepsilon}$,

where all inequalities are required to hold true for *all* choices of parameters.

Let also $\omega \in [2, 3]$ denote a feasible exponent for matrix multiplication; by this, we mean that we are given an algorithm which is able to compute the product of two $n \times n$ matrices over a ring R for a cost of $O(n^\omega)$ operations in R. The naive algorithm leads to $\omega = 3$; however, better algorithms do exist and the best known value for ω, nowadays, is less than 2.37188 [DWZ22]. Similarly, let Ω be a feasible exponent for the computation of the characteristic polynomial of a matrix over polynomials rings over a field. Using Kaltofen and Villard's algorithm, it is known that one can reach $\Omega < 2.69497$ [KV05]. If K is a finite extension of $\mathbb{F}_q$ of degree d, we also denote by $\mathrm{SM}^{\geqslant 1}(n, d)$ a log-concave function with respect to the variable n having the following property: the number of operations in $\mathbb{F}_q$[1] needed for multiplying two Ore polynomials in $K\{\tau\}$ of degree n is in $O^{\sim}(\mathrm{SM}^{\geqslant 1}(n, d))$.

Our first result is about the computation of the characteristic polynomial of an endomor-

[1]Here, we assume that applying the Frobenius of K counts for $O^{\sim}(d)$ operations in $\mathbb{F}_q$, see §1.2.3 for more details.

phism of a Drinfeld module.

Theorem A (see Theorems 2.15 and 2.16)**.** *Let ϕ be a Drinfeld $\mathbb{F}_q[T]$-module of rank r over a field K, and let u be an endomorphism of ϕ of degree n. The characteristic polynomial of u can be computed for a cost of $O^{\sim}(n^2 + (n+r)r^{\Omega-1})$ operations in K and $O(n^2 + r^2)$ applications of the Frobenius.*

Moreover, when K is a finite extension of $\mathbb{F}_q$ of degree d, the characteristic polynomial of u can be computed for a cost of

$$O^{\sim}(d \log^2 q) + O^{\bullet}\left(\left(\mathrm{SM}^{\geqslant 1}(n,d) + ndr + (n+d)r^{\omega}\right) \cdot \log q\right)$$

bit operations.

We then study more particularly the special case of the Frobenius endomorphism (which is only defined when K is a finite field), for which we provide three different algorithms that we call `F-MFF`, `F-MKU` and `F-CSA` respectively.

Theorem B. *Let ϕ be a Drinfeld $\mathbb{F}_q[T]$-module of rank r over a finite extenstion K of $\mathbb{F}_q$ of degree d. The characteristic polynomial of the Frobenius endomorphism of ϕ can be computed for a cost of either*

- [`F-MFF` algorithm, see §2.2.2] $O^{\sim}(d \log^2 q) + O^{\bullet}\left(\left(\mathrm{SM}^{\geqslant 1}(d,d) + d^2 r + dr^{\omega}\right) \cdot \log q\right)$, *or*
- [`F-MKU` algorithm, see §2.2.3] $O^{\sim}(d \log^2 q) + O^{\bullet}\left(\left(d^2 r^{\omega-1} + dr^{\omega}\right) \cdot \log q\right)$, *or*
- [`F-CSA` algorithm, see §4.2] $O^{\sim}(d \log^2 q) + O^{\bullet}(rd^{\omega} \log q)$

bit operations.

We finally come to general isogenies between different Drinfeld modules. In this case, the characteristic polynomial is not well-defined, but the norm is.

Theorem C (see Theorems 3.4 and 3.5)**.** *Let ϕ and ψ be two Drinfeld $\mathbb{F}_q[T]$-modules of rank r over a field K, and let $u : \phi \to \psi$ be an isogeny of degree n. The norm of u can be computed for a cost of $O^{\sim}(n^2 + nr^{\omega-1} + r^{\omega})$ operations in K and $O(n^2 + r^2)$ applications of the Frobenius.*

Moreover, when K is a finite extension of $\mathbb{F}_q$ of degree d, the norm of u can be computed for a cost of

$$O^{\sim}(d \log^2 q) + O^{\bullet}\left(\left(\mathrm{SM}^{\geqslant 1}(n,d) + ndr + n\min(d,r)r^{\omega-1} + dr^{\omega}\right) \cdot \log q\right)$$

bit operations.

Moreover, we propose extensions of all our algorithms to Drinfeld modules defined over a general curve C (and not just $\mathbb{P}^1_{\mathbb{F}_q}$). However, we do not carry out, in the present paper, a thorough study of the complexity in this general setting.

Finally, we mention that, in the case of $\mathbb{P}^1_{\mathbb{F}_q}$, our algorithms have been implemented in SageMath [ACLM23] and will be hopefully publicly available soon in the standard distribution. Meanwhile, the interested user may read tutorials and try out our software package online on the platform plm-binder at:

`https://xavier.caruso.ovh/notebook/drinfeld-modules`

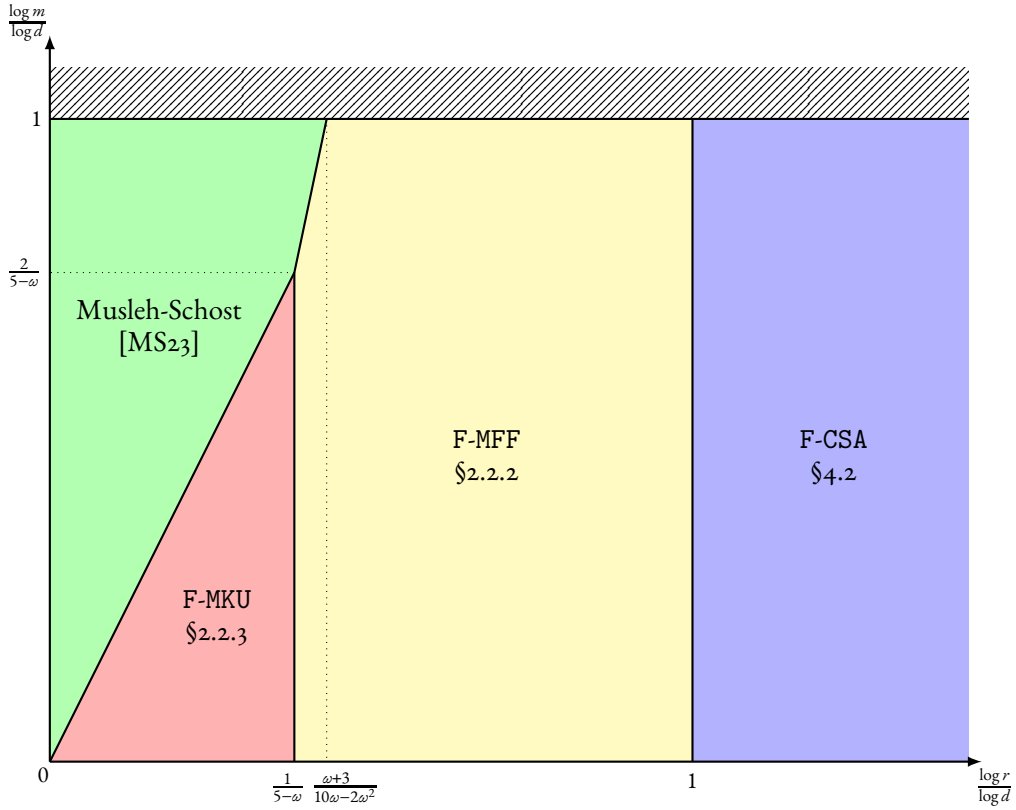

Figure 1: The best algorithm for computing the characteristic polynomial of the Frobenius endomorphism, depending on the size of r, d and m.
Assumptions: $2 \leqslant \omega \leqslant 3$ and $\omega \leqslant \Omega \leqslant \omega + 1$.

Comparison with previous results. To the authors' knowledge, it is the first time that algorithms are presented for Drinfeld modules defined over a general curve; so far, only the case of $\mathbb{P}^1_{\mathbb{F}_q}$ was adressed. Also, we are not aware of previous works on the explicit computations of norms of general isogenies between different Drinfeld modules.

In contrast, the question of the explicit computation of the characteristic polynomial of the Frobenius endomorphism, especially in the case of rank 2, was already considered by many authors [Nar18, DNS21, GP20, MS19, MS23]. Our algorithms for this task are however new and they turn out to be competitive for a large range of parameters. More precisely, prior to our work, the most efficient algorithm was due to Musleh and Schost [MS23]. Depending on the relative values of $r, d = [K : \mathbb{F}_q]$ and $m = \deg(\mathfrak{p})$, all four algorithms (`F-MFF`, `F-MKU`, `F-CSA` and Musleh-Schost's algorithm) achieve the best asymptotic complexity in at least one regime, as shown in Figure 1. As a rule of thumb, the reader can memorize that our algorithms are better when $r \gg \sqrt{d}$ (or even $r \gg d^{0.431}$ if one takes into account fast algorithms for matrix multiplication); on the contrary, when $r \ll \sqrt{d}$, our algorithms may still be competitive, depending on the relative values of $\log(m)/\log(d)$ and $\log(r)/\log(d)$.

For a more complete review on existing algorithms and comparison between complexities, we refer to the tables of Appendix A (page 42).

Anderson motives. The main theoretical input upon which all our algorithms are based is the *motive* attached to a Drinfeld module, introduced by Anderson in 1986 [And86] (see also [Gos98, vdH04, GL20]). In the classical setting of algebraic geometry, Grothendieck describes the motive $\mathbb{M}(X)$ of an algebraic variety X as the ultimate object able to encode all the "linear" properties of X. Since characteristic polynomials and norms are obviously constructions of linear nature, we expect to be able to recover them at the level of motives. However, in the classical setting, motives are usually quite complicated objects, often defined by accumulating subtle categorical constructions. More or less, this totally prevents using them for algorithmic applications.

It is striking that the situation for Drinfeld modules is much more tractable: the Anderson motive $\mathbb{M}(\phi)$ of a Drinfeld module ϕ is a very explicit object—concretely, it is just $K\{\tau\}$ equipped with extra structures—which is very well-adapted to algorithmic manipulations. However, $\mathbb{M}(\phi)$ exhibits all the theoretical features one expects; in particular, it retains all the information we need on characteristic polynomials of endomorphisms and norms of isogenies. In the present paper, we make an intersive use of this yoga. In particular, we highlight that our methods are not an adaptation of existing methods from elliptic curves.

More precisely, an endomorphism u of a Drinfeld module corresponds to a linear endomorphism $\mathbb{M}(u)$ at the level of Anderson motives. It is moreover a well-known fact that the characteristic polynomial of $\mathbb{M}(u)$ agrees with that of u (see [Pap23, Proposition 3.6.7] for the case of $\mathbb{P}^1_{\mathbb{F}_q}$). In the present paper, we give a new proof of this theorem, and extend it to general isogenies, establishing that the norm of an isogeny u is the ideal generated by the determinant of $\mathbb{M}(u)$ (see Theorem 3.2). We then use this result to reduce the computations we are interested in to the computation of the determinant or the characteristic polynomial of an actual matrix. In the case of $\mathbb{P}^1_{\mathbb{F}_q}$, this is immediate since Anderson motives are free over $K[T]$, with an explicit canonical basis. For a general curve, Anderson motives are not always free but only projective, which induces technical difficulties for algorithmics. Although it should be doable to tackle these issues head-on, we choose to work around them by reducing the problem to the case of $\mathbb{P}^1_{\mathbb{F}_q}$ treated previously.

The previous discussion applies to all our algorithms, except the algorithm `F-CSA` which is different in nature: it is based on a new formula interpreting the characteristic polynomial of the Frobenius endomorphism as a reduced norm in some well-suited central simple algebra. For the sake of simplicity, we only state our result for the case of $\mathbb{P}^1_{\mathbb{F}_q}$ in this introduction.

Theorem D (see Theorem 4.5)**.** *Let ϕ be a Drinfeld $\mathbb{F}_q[T]$-module over a finite field K and let $\pi(T, U) \in \mathbb{F}_q[T][U]$ be the characteristic polynomial of the Frobenius endomorphism of ϕ. Let also $\chi(\tau^d, V) \in \mathbb{F}_q[\tau^d][V]$ be the reduced characteristic polynomial of $\phi_T \in K\{\tau\}$. Then*

$$\pi(T, U) = \chi(U, T).$$

The above theorem reduces the computation of the characteristic polynomial of the Frobenius endomorphism to the computation of a reduced characteristic polymonial which, using classical techniques, further reduces to the computation of the characteristic polynomial of an actual matrix over of size $d \times d$ (with $d = [K : \mathbb{F}_q]$ as above) over $\mathbb{F}_q[T]$.

To conclude, we would like to mention that, on the theoretical side, Anderson motives are not only a powerful tool for studying Drinfeld modules; they are nowadays considered as a vast generalization of Drinfeld modules, providing more flexibility in the constructions and having their

own interest. The methods presented in this article strongly suggest that designing algorithms in the framework of general Anderson motives is completely within our reach (and maybe easier!). We then do believe that time is ripe to go beyond Drinfeld modules and start working with Anderson motives at the algorithmic level.

Acknowledgements. We thank Pierre-Jean Spaenlehauer and Emmanuel Thomé for their guidance. We thank Cécile Armana, Alain Couvreur, Quentin Gazda, Federico Pellarin and Floric Tavarès-Ribeiro for helpful discussions. This work benefited from the financial support of the ANR projects CLap-CLap (ANR-18-CE40-0026-01), Barracuda (ANR-21-CE39-0009) and PadLEfAn (ANR-22-CE40-0013).

1 Background

This section serves as a gentle preliminary part in which we introduce the setup of this article. On the theoretical side, we recall basic definitions and constructions on Drinfeld modules while, on the computational side, we specify our complexity model and discuss several algorithmic primitives we shall constantly use throughout this article.

1.1 Drinfeld modules

Throughout this paper, we fix a finite field $\mathbb{F}_q$ of cardinality q. Let C be smooth, projective, geometrically connected curve over $\mathbb{F}_q$. Let ∞ be a distinguished closed point on C and let A denote the ring of rational functions on X that are regular outside ∞. If F is an extension of $\mathbb{F}_q$, we write $A_F = F \otimes_{\mathbb{F}_q} A$. Thanks to our assumptions on C, the ring A_F is a Dedekind domain. We recall that the *degree* of an ideal $\mathfrak{a}$ of A_F, denoted by $\deg(\mathfrak{a})$, is defined as the F-dimension of $A_F/\mathfrak{a}$. For $a \in A_F$, we will often write $\deg(a)$ for $\deg(aA_F)$.

We consider an extension K of $\mathbb{F}_q$ and fix an algebraic closure $\overline{K}$ of K. We fix in addition a homomorphism of $\mathbb{F}_q$-algebras

$$\gamma : A \to K.$$

The kernel of γ, a prime ideal of A, is denoted by $\mathfrak{p}$ and referred to as the *characteristic*. An ideal of A is said *away from the characteristic* if it is coprime to $\mathfrak{p}$. Finally, we let $K\{\tau\}$ be the algebra of *Ore polynomials* over K in τ, in which the multiplication is twisted according to the rule $\tau a = a^q \tau$ for all $a \in K$.

1.1.1 Drinfeld modules and isogenies

We define Drinfeld modules and their morphisms.

Definition 1.1 (Drinfeld modules)**.** A *Drinfeld A-module* (or a *Drinfeld module* for short) over K is a ring homomorphism

$$\phi : A \to K\{\tau\}$$

whose constant coefficient agrees with γ and whose image is not contained in K.

For $a \in A$, we write ϕ_a for $\phi(a)$. By definition, the *rank* of ϕ is the unique positive integer r such that $\deg(\phi_a) = r \deg(a)$ for all $a \in A$ (see [Gek91, Definition 1.1]).

Example 1.2. The simplest Drinfeld modules are those for which $C = \mathbb{P}^1_{\mathbb{F}_q}$ and ∞ is the point at infinity, *i.e.* $A = \mathbb{F}_q[T]$. In this case, a Drinfeld module ϕ of rank r is defined by the datum of an Ore polynomial

$$\phi_T = \gamma(T) + g_1\tau \cdots + g_r\tau^r,$$

with $g_1, \ldots, g_r \in K$ and $g_r \neq 0$. Carlitz modules are those Drinfeld $\mathbb{F}_q[T]$-modules for which $K = \mathbb{F}_q(T)$ and $r = 1$.

Definition 1.3 (Morphisms)**.** Let ϕ, ψ be two Drinfeld modules. A *morphism* $u : \phi \to \psi$ is, by definition, an Ore polynomial u such that $u\phi_a = \psi_a u$ for every $a \in A$. An *isogeny* is a nonzero morphism.

This definition equips the class of Drinfeld modules with a structure of category, in which the composition is given by the product in the ring of Ore polynomials. We say that ϕ and ψ are *isogenous* if there exists an isogeny between ϕ and ψ. One checks that two isogenous Drinfeld modules have the same rank. For any $a \in A$, ϕ_a defines an endomorphism of ϕ. If K is a finite field of degree d over $\mathbb{F}_q$, then τ^d defines an endomorphism called the *Frobenius endomorphism* of ϕ; it is denoted by F_ϕ.

Let $u : \phi \to \psi$ be an isogeny defined by the degree n Ore polynomial

$$u = u_0 + u_1\tau + \cdots + u_n\tau^n.$$

We say that n is the τ-degree of u. By definition, the *height* of u is the smallest integer h for which $u_h \neq 0$. In what follows, we denote it by $h(u)$. When $h(u) = 0$, we say that u is *separable*. When the characteristic $\mathfrak{p}$ is zero, any isogeny is separable. On the contrary, when $\mathfrak{p}$ does not vanish, $h(u)$ is a necessarily multiple of $\deg(\mathfrak{p})$, and u decomposes as $u = u_s \circ \tau^{h(u)}$, where $\tau^{h(u)}$ defines an isogeny from ϕ to a second Drinfeld module ϕ' and $u_s : \phi' \to \psi$ is a *separable* isogeny.

1.1.2 Torsion points, Tate module, and Anderson motives

Let ϕ and ψ be two rank r Drinfeld modules. We define the most important algebraic structures attached to a Drinfeld module.

Definition 1.4 (A-module)**.** (i) The *A-module* of ϕ, denoted $\mathbb{E}(\phi)$, is the A-module $\overline{K}$ equipped with the structure given by

$$a \cdot z = \phi_a(z)$$

for $a \in A$ and $z \in \mathbb{E}(\phi)$.

(ii) Given an additional ideal $\mathfrak{a}$ of A, we define the $\mathfrak{a}$-torsion $\mathbb{E}_\mathfrak{a}(\phi)$ of ϕ as the *$\mathfrak{a}$-torsion* of the module $\mathbb{E}(\phi)$, that is the subset of $\overline{K}$ consisting of elements z for which $\phi_a(z) = 0$ for all $a \in \mathfrak{a}$. For an element $a \in A$, we write $\mathbb{E}_a(\phi)$ for $\mathbb{E}_{aA}(\phi)$.

Any morphism of Drinfeld modules $u : \phi \to \psi$ induces A-linear morphisms

$$\begin{array}{rccc} \mathbb{E}(u): & \mathbb{E}(\phi) & \to & \mathbb{E}(\psi) \\ & z & \mapsto & z(u) \end{array}$$

and $\mathbb{E}_{\mathfrak{a}}(u) : \mathbb{E}_{\mathfrak{a}}(\phi) \to \mathbb{E}_{\mathfrak{a}}(\psi)$. For any nonzero ideal $\mathfrak{a} \subset A$ away from the characteristic, the module $\mathbb{E}_{\mathfrak{a}}(\phi)$ is free of rank r over $A/\mathfrak{a}$, *i.e.* $\mathbb{E}_{\mathfrak{a}}(\phi) \simeq (A/\mathfrak{a})^r$ [Gos98, Remark 4.5.5.1]. This classical fact highlights one of the first similarities with elliptic curves, of which rank two Drinfeld modules are said to be function field analogues.

Definition 1.5 (Tate module)**.** Let $\mathfrak{q}$ be a maximal ideal of A, away from the characteristic. We define the $\mathfrak{q}$-adic *Tate module* of ϕ as the inverse limit

$$\mathbb{T}_{\mathfrak{q}}(\phi) = \varprojlim \mathbb{E}_{\mathfrak{q}^n}(\phi).$$

The Tate module $\mathbb{T}_{\mathfrak{q}}(\phi)$ is a module over the completion $A_{\mathfrak{q}}$ of A with respect to the place $\mathfrak{q}$. It is free of rank r, and morphisms $u : \phi \to \psi$ give rise to $A_{\mathfrak{q}}$-linear maps $\mathbb{T}_{\mathfrak{q}}(u) : \mathbb{T}_{\mathfrak{q}}(\phi) \to \mathbb{T}_{\mathfrak{q}}(\psi)$.

Definition 1.6 (Anderson motive)**.** (i) The *A-motive* of ϕ, denoted by $\mathbb{M}(\phi)$, is the A_K-module $K\{\tau\}$ equipped with the structure given by

$$(\lambda \otimes a) \cdot f = \lambda f \phi_a$$

where $\lambda \in K, a \in A, f \in \mathbb{M}(\phi)$ and the multiplication in the right hand side is computed in $K\{\tau\}$.

(ii) Given in addition an ideal $\mathfrak{a}$ of A, we define

$$\mathbb{M}_{\mathfrak{a}}(\phi) = A/\mathfrak{a} \otimes_A \mathbb{M}(\phi) = \mathbb{M}(\phi)/\mathfrak{a}\mathbb{M}(\phi).$$

For an element $a \in A$, we write $\mathbb{M}_a(\phi)$ for $\mathbb{M}_{aA}(\phi)$.

Remark 1.7. In classical references (*e.g.* [Gos98, Section 5.4]), the A-motive $\mathbb{M}(\phi)$ carries more structure: it is a module over the noncommutative ring $K\{\tau\} \otimes_{\mathbb{F}_q} A = A_K\{\tau\}$. This additional τ-action is important, but never used in this article. Therefore, for simplicity, we only retain the structure of A_K-module.

It is well known that $\mathbb{M}(\phi)$ is projective of rank r over A_K (see [Gos98, Lemma 5.4.1]). When $A = \mathbb{F}_q[T]$, we have $A_K \simeq K[T]$ and $\mathbb{M}(\phi)$ is free with basis $(1, \tau, \dots, \tau^{r-1})$ [Pap23, Lemma 3.4.4]. We stress that this has significant importance for our algorithmic purpose. In general, a morphism of Drinfeld modules $u : \phi \to \psi$ induces a morphisms of A_K-modules

$$\begin{array}{rccc} \mathbb{M}(u): & \mathbb{M}(\psi) & \to & \mathbb{M}(\phi) \\ & f & \mapsto & fu \end{array}$$

and $\mathbb{M}_{\mathfrak{a}}(u) : \mathbb{M}_{\mathfrak{a}}(\psi) \to \mathbb{M}_{\mathfrak{a}}(\phi)$. We refer to [Gos98, Ch. 5] or [vdH04, Section 2] for more details and generalizations. The degree of the Ore polynomial defining an element $f \in \mathbb{M}(\phi)$ (resp. $\mathbb{M}(u)$) is called the τ-degree of f (resp. $\mathbb{M}(u)$).

Remark 1.8. Let $\mathfrak{a}$ and $\mathfrak{q}$ be ideals of A, with $\mathfrak{q}$ maximal. The constructions $\mathbb{E}$, $\mathbb{E}_{\mathfrak{a}}$, $\mathbb{T}_{\mathfrak{q}}$, $\mathbb{M}$ and $\mathbb{M}_{\mathfrak{a}}$ define functors from the category of Drinfeld modules:

- $\mathbb{E}$ (resp. $\mathbb{E}_{\mathfrak{a}}$) is a covariant functor to the category of A-modules (resp. $A/\mathfrak{a}$-modules);
- $\mathbb{T}_{\mathfrak{q}}$ is a covariant functor to the category of $A_{\mathfrak{q}}$-modules;

- $\mathbb{M}$ (resp. $\mathbb{M}_{\mathfrak{a}}$) is a contravariant functor to the category of A_K-modules[2] (resp. $A_K/\mathfrak{a}A_K$-modules).

In standard references, the $\mathfrak{a}$-torsion is denoted by $\phi[\mathfrak{a}]$. In this article, we prefer the notation $\mathbb{E}_{\mathfrak{a}}(\phi)$ because it better underlines the functorial properties of the construction, which will later play a leading role.

1.1.3 Norms and characteristic polynomials

The norm of an isogeny is defined in [Gek91, §3.9], in terms of *Euler-Poincaré characteristic*. Let us take a step back, and fix a Dedekind domain $\mathcal{A}$. The Euler-Poincaré characteristic, denoted by $\chi_{\mathcal{A}}$, is a function defined on the class of finitely generated $\mathcal{A}$-modules and assuming values in the set of ideals of $\mathcal{A}$. It is uniquely determined by the following conditions:

(i) $\chi_{\mathcal{A}}(\mathcal{A}/\mathfrak{a}) = \mathfrak{a}$ for every ideal $\mathfrak{a}$ of $\mathcal{A}$;

(ii) $\chi_{\mathcal{A}}(M_2) = \chi_{\mathcal{A}}(M_1) \cdot \chi_{\mathcal{A}}(M_3)$ for every exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ of finitely generated $\mathcal{A}$-modules.

The formation of Euler-Poincaré characteristic commutes with flat scalar extension. In particular, given a finitely generated $\mathcal{A}$-module M and a maximal ideal $\mathfrak{q} \subset \mathcal{A}$, we have

$$\chi_{\mathcal{A}}(M) \otimes_{\mathcal{A}} \mathcal{A}_{\mathfrak{q}} = \chi_{\mathcal{A}_{\mathfrak{q}}}(M \otimes_{\mathcal{A}} \mathcal{A}_{\mathfrak{q}}).$$

Similarly, if $\mathcal{A}'$ is another Dedekind domain lying above $\mathcal{A}$, we have

$$\chi_{\mathcal{A}}(M) \otimes_{\mathcal{A}} \mathcal{A}' = \chi_{\mathcal{A}'}(M \otimes_{\mathcal{A}} \mathcal{A}').$$

If M is torsion, the Noether's theorem on the structure of finitely generated modules over Dedekind domains [Eis95, Exercise 19.6] implies that M decomposes as $M \simeq \mathcal{A}/\mathfrak{a}_1 \times \cdots \times \mathcal{A}/\mathfrak{a}_\ell$, where $\mathfrak{a}_1, \ldots, \mathfrak{a}_\ell$ are ideals of $\mathcal{A}$. In that case, $\chi_{\mathcal{A}}(M) = \mathfrak{a}_1 \cdots \mathfrak{a}_\ell$.

Definition 1.9 (Norm)**.** Let $u : \phi \to \psi$ be an isogeny. The norm of u, denoted by $\mathfrak{n}(u)$, is defined as

$$\mathfrak{n}(u) = \mathfrak{p}^{\frac{h(u)}{\deg(\mathfrak{p})}} \cdot \chi_A(\ker \mathbb{E}(u)).$$

Remark 1.10. We recall that $h(u)$ denotes the height of u. This definition takes into account that an isogeny and its separable part have the same kernel: the correction by the factor $\mathfrak{p}^{h(u)/\deg(\mathfrak{p})}$ corresponds to the purely inseparable part.

Example 1.11. Let r be the rank of ϕ. For $a \in A$, we have $\mathfrak{n}(\phi_a) = a^r A$. If $\mathfrak{p} \neq 0$ then $\mathfrak{n}(\tau^{\ell \deg(\mathfrak{p})}) = \mathfrak{p}^\ell$ for all $\ell \in \mathbb{Z}_{\geqslant 0}$. In particular, when K is a finite extension of degree d of $\mathbb{F}_q$, the norm of the Frobenius endomorphism F_ϕ is explicitly given by $\mathfrak{n}(F_\phi) = \mathfrak{p}^{d/\deg(\mathfrak{p})}$.

One proves [Gek91, Lemma 3.10] that the norm is multiplicative: if u and v are composable isogenies, we have $\mathfrak{n}(v \circ u) = \mathfrak{n}(v) \cdot \mathfrak{n}(u)$. When u is an endomorphism, its action on the Tate module $\mathbb{T}_{\mathfrak{q}}(u)$ is a linear endomorphism, whose determinant lies in A and generates $\mathfrak{n}(u)$ [Gek91, Lemma 3.10.iii]:

$$\mathfrak{n}(u) = \det(\mathbb{T}_{\mathfrak{q}}(u)) \cdot A.$$

[2] More precisely, $\mathbb{M}$ is a functor to the category of Anderson motives.

Definition 1.12 (Characteristic polynomial)**.** Let $u : \phi \to \phi$ be an endomorphism. We define the *characteristic polynomial* of u as the characteristic polynomial of $\mathbb{T}_q(u)$.

Since $\mathbb{T}_q(\phi)$ has rank r over $A_\mathfrak{q}$, the characteristic polynomial of u has degree r. It is also proven that it has coefficients in A [Gek91, Corollary 3.4].

Example 1.13. In this example, we assume that $A = \mathbb{F}_q[T]$, that K is finite of degree d over $\mathbb{F}_q$, and that ϕ is a rank two Drinfeld module defined by $\phi_T = \gamma(T) + g\tau + \Delta\tau^2$. The characteristic polynomial of the Frobenius endomorphism of ϕ takes the form [Gek08, Theorem 2.11]

$$X^2 - tX + (-1)^n \mathrm{N}_{K/\mathbb{F}_q}(\Delta)^{-1}\mathfrak{p}^{n/\deg(\mathfrak{p})}$$

where $\mathrm{N}_{K/\mathbb{F}_q}$ is the norm from K to $\mathbb{F}_q$ and, in a slight abuse of notation, the notation $\mathfrak{p}$ is used to denote the monic generator of the characteristic. The coefficient $t \in \mathbb{F}_q[T]$ is called the *Frobenius trace* of ϕ and we have $\deg_T(t) \leqslant d/2$. We refer to Remark 3.7 for more information about the *Frobenius norm*. The endeavour of computing this polynomial has been the object of many research articles, leading to a variety of algorithms. We refer to Appendix A for a review of their respective complexities.

1.1.4 Restriction of Drinfeld modules

We consider $\gamma' : A' \to K$, a second base for Drinfeld modules satisfying the assumptions of §1.1, and we assume that we are given in addition an injective homomorphism of rings $f : A' \to A$ such that $\gamma' = \gamma \circ f$. Thanks to our assumptions on A and A', we find that f endows A' with a structure of finite A-algebra. If $\phi : A \to K\{\tau\}$ is a Drinfeld module, the composite

$$\phi \circ f : A' \to A \to K\{\tau\}$$

defines a Drinfeld module over A', denoted by $f^*\phi$ and referred to as the *restriction* of ϕ along f.

Considering two Drinfeld A-modules as well as a morphism $u : \phi \to \psi$, one checks that the Ore polynomial defining u also defines an isogeny $f^*\phi \to f^*\psi$, which we denote by f^*u. The construction f^* defines a functor from the category of Drinfeld modules over A to the category of Drinfeld modules over A'. The action of f^* on the motives is easy to describe: the motive $\mathbb{M}(f^*\phi)$ is simply $\mathbb{M}(\phi)$ with the restricted action of A and, for any morphism $u : \phi \to \psi$, the maps $\mathbb{M}(f^*u)$ and $\mathbb{M}(u)$ are the same (up to the above identification).

1.2 Algorithmics

We now move to algorithmics and discuss the complexity of performing basic operations on matrices on the one hand, and on Ore polynomials on the other hand.

1.2.1 Complexity model

We recall the Landau's notation O, $O^{\tilde{}}$ and $O^\bullet$ from the introduction: if f and g are two positive quantities depending on parameters, we write

- $g \in O(f)$ if there exists an absolute positive constant C such that $g \leqslant C \cdot f$ for all choices of parameters,

- $g \in O^{\sim}(f)$ if there exist absolute positive constants C and k such that $g \leqslant C \cdot f \log^k f$ for all choices of parameters,
- $g \in O^{\bullet}(f)$ if, for all $\varepsilon > 0$, there exists a positive constant C_ε such that $g \leqslant C_\varepsilon \cdot f^{1+\varepsilon}$ for all choices of parameters.

We notice that $O(f) \subset O^{\sim}(f) \subset O^{\bullet}(f)$ for all f as above. Moreover, if f_1 and f_2 are two quantities as above, one checks that $O(f_1) + O(f_2) \subset O(f_1 + f_2)$, $O^{\sim}(f_1) + O^{\sim}(f_2) \subset O^{\sim}(f_1 + f_2)$ and, similarly, $O^{\bullet}(f_1) + O^{\bullet}(f_2) \subset O^{\bullet}(f_1 + f_2)$.

In this article, we measure complexity in two different ways. When K is an arbitrary field, we use *arithmetic complexity*, meaning that we count separately arithmetic operations (addition, subtraction, multiplication and division) in K on the one hand, and applications of Frobenius (that is the computation of x^q for a given $x \in K$) on the other hand.

On the contrary, when K is a finite field, we rather use *bit complexity*, meaning that we count operations on bits. When K is a finite extension of $\mathbb{F}_q$ of degree d presented as a quotient $K = \mathbb{F}_q[X]/Q(X)$ (for some irreducible polynomial $Q(X) \in \mathbb{F}_q[X]$ of degree d) and when $\mathbb{F}_q$ is itself presented as a quotient of $\mathbb{F}_p[X]$, classical algorithms based on Fast Fourier Transform allows for performing all arithmetic operations in K for a cost of $O^{\sim}(d \log q)$ bit operations (see for instance [vzGG13, Chapter II]).

Estimating the cost of applying the Frobenius endomorphism of K is more challenging, even though partial results are available in the literature. First of all, Kedlaya and Umans' algorithm [KU11] for fast modular composition is theoretically capable to compute an image by Frobenius for a cost of $O^{\bullet}(d \log q)$ bit operations. However, if α denotes the image of X in K, one needs nevertheless to precompute α^q, *i.e.* to write α^q on the canonical monomial basis $(1, \alpha, \ldots, \alpha^{d-1})$. Using a fast exponentiation algorithm, this can be done for an initial cost of $O^{\sim}(d \log^2 q)$ bit operations. Another flaw with this approach is that, as far as we know, one still lacks an efficient implementation of Kedlaya and Umans' algorithm.

Another option, which achieves quasi-optimal complexity, is to use the elliptic normal bases of Couveignes and Lercier [CL09] instead of the classical monomial basis. Indeed, in those bases, all arithmetic operations and applications of Frobenius can be computed for a cost of $O^{\sim}(d)$ operations in $\mathbb{F}_q$, corresponding to $O^{\sim}(d \log q)$ bit operations. The drawback of this solution is that constructing an elliptic normal basis can be costly. Nevertheless this needs to be done only once, at the instanciation of K.

Taking all of this into account, we choose to follow the convention of [MS23] and opt for the first option: we make the assumption that all arithmetic operations and applications of Frobenius in K costs $O^{\bullet}(d \log q)$ bit operations, plus a unique initial cost of $O^{\sim}(d \log^2 q)$ operations for the precomputation of α^q.

1.2.2 Polynomial matrices

We give a rough review of the literature on the computation of determinants and characteristic polynomials of polynomial matrices. We recall from the introduction that the notation $\omega \in [2, 3]$ refers to feasible exponent for matrix multiplication. When matrices have coefficients in a field L, both computing determinants and characteristic polynomials reduce to matrix multiplication [NP21, PS07]. Computing the determinant of a polynomial matrix also reduces to matrix

multiplication [GJV03, JV05]. However, the situation of the characteristic polynomial is more delicate. Consider a s-by-s matrix with entries in $L[T]$. Computing its characteristic polynomial can be done for a cost of $O^{\sim}(s^{\Omega}n)$ operations in L with $\Omega < 2.69497$ [Kal92, KV05].

When M is a s-by-s matrix, we use the notation $\pi(M)$ to be to its monic characteristic polynomial, that is $\pi(M) = \det(X \cdot I_s - M)$ where I_s is the identity matrix of size s. In the next two lemmas, we derive two useful algorithms, for two specific situations.

Lemma 1.14. *We assume that L is a finite field of degree d over $\mathbb{F}_q$. Let M be a s-by-s matrix with coefficients in $L[T]$. Let n be a uniform upper bound on the degree of the coefficients of $\pi(M)$. There exists a Las Vegas algorithm that computes the $\pi(M)$ for a cost of $O^{\bullet}(n/d) + O^{\sim}((n+d)s^{\omega})$ operations in $\mathbb{F}_q$.*

Proof. Let L' be an extension of L of degree $\lceil n/d \rceil$; such an extension, altogether with a generator α of L' over $\mathbb{F}_q$, can be found out using Couveignes and Lercier's Las Vegas algorithm, whose complexity is in $O^{\bullet}(\frac{n}{d})$ operations in $\mathbb{F}_q$ [CL13]. The degree of the extension $L'/\mathbb{F}_q$ is then in the range $[n, n+d]$. Let $M(\alpha)$ denote the evaluation of M at $T = \alpha$, and write its characteristic polynomial as follows:

$$\pi(M(\alpha)) = \sum_{i=0}^{s} \sum_{j=0}^{n} a_{i,j} \alpha^i X^i.$$

where the coefficients $a_{i,j}$ are in $\mathbb{F}_q$. Then

$$\pi(M) = \sum_{i=0}^{s} \sum_{j=0}^{n} a_{i,j} T^i X^i.$$

The generator α being known, computing $\pi(M(\alpha))$ costs $O^{\sim}(s^{\omega})$ operations in L', which corresponds to $O^{\sim}((n+d)s^{\omega})$ operations in $\mathbb{F}_q$. □

Lemma 1.15. *Let M be a s-by-s matrix with coefficients in $\mathbb{F}_q[T]$ and let n be a uniform upper bound on the degress of the entries of M. We assume that the coefficients of $\pi(M)$ fall in $\mathbb{F}_q[T^s]$. There exists a Las Vegas algorithm that computes $\pi(M)$ with probability at least $\frac{1}{2}$ for a cost of $O^{\sim}(ns^{\omega})$ operations in $\mathbb{F}_q$.*

Proof. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ be such that $\alpha_i^s \neq \alpha_j^s$ whenever $i \neq j$. We compute the matrices $M(\alpha_1), \ldots, M(\alpha_n)$ and compute their characteristic polynomials $\pi(M(\alpha_1)), \ldots, \pi(M(\alpha_n))$, for a total cost of $O^{\sim}(ns^{\omega})$ operations in $\mathbb{F}_q$. Thanks to our assumption, $\pi(M)$ can be seen as having s polynomial coefficients of degree at most n. Using fast interpolation algorithms [vzGG13, §II.10], $\pi(M)$ can therefore be recovered from the $\pi(M(\alpha_i))$'s for a cost of $O^{\sim}(ns)$ operations in $\mathbb{F}_q$. We end up with a total of $O^{\sim}(ns^{\omega})$ operations in $\mathbb{F}_q$.

This procedure only works if $\mathbb{F}_q$ is large enough to pick a valid set $\{\alpha_1, \ldots, \alpha_n\}$. Let $\rho = \frac{\gcd(q-1,s)}{q-1}$ be the proportion of elements in $\mathbb{F}_q^{\times}$ that are d-th roots of unity. A family $(\alpha_1, \ldots, \alpha_n) \in (\mathbb{F}_q^{\times})^n$ has probability $p_n = (1-\rho)(1-2\rho)\cdots(1-n\rho)$ to form a valid set. As $p_n \geqslant 1 - \frac{n(n+1)}{2}\rho$, the process has a chance of success greater than $\frac{1}{2}$ as soon as $q > 1 + sn(n+1)$. If $\mathbb{F}_q$ is not large enough, we do all computations in a finite extension of $\mathbb{F}_q$. With these estimations, we conclude that it is enough to work in an extension whose degree has order of magnitude $\log_q(sn^2)$. Building this extension, as well as computing in it, does not affect the announced complexity. □

1.2.3 Ore polynomials

In full generality, multiplications and Euclidean divisions of Ore polynomials in $K\{\tau\}$ of degree at most n can be achieved with the naive algorithm for a cost of $O(n^2)$ operations in K and $O(n^2)$ extra applications of the Frobenius endomorphism.

However, when K is a finite field, we can take advantage of fast Ore polynomial multiplication [CLB17b, CLB17a]. As before, we use the letter d to denote the degree of the extension $K/\mathbb{F}_q$. Let $\mathrm{SM}(n, d)$ denote a function having the following property: the number of bit operations needed for multiplying two Ore polynomials in $K\{\tau\}$ of degree less than n is within $O^\bullet(\mathrm{SM}(n, d)\log q)$. At the time of writing this article, the best known value of SM is given in [CLB17a][3,4]:

$$\begin{aligned}\mathrm{SM}(n, d) &= n^{\frac{\omega+1}{2}}d && \text{for } n \leqslant d^{\frac{2}{5-\omega}},\\ &= n^{\omega-2}d^2 && \text{for } d^{\frac{2}{5-\omega}} \leqslant n \leqslant d,\\ &= nd^{\omega-1} && \text{for } d \leqslant n.\end{aligned}$$

Let also $\mathrm{SM}^{\geqslant 1}$ be the function defined by

$$\mathrm{SM}^{\geqslant 1}(n, d) = \sup_{0<m\leqslant n} \mathrm{SM}(m, d)\frac{n}{m}.$$

The function $\mathrm{SM}^{\geqslant 1}$ is the smallest log-concave function above SM. It is proved in [CLB17a] that computing the right-Euclidean division of Ore polynomials in $K\{\tau\}$ of degree less than n requires at most $O^\bullet(\mathrm{SM}^{\geqslant 1}(n, d)\log q)$ bit operations. With the above values for $\mathrm{SM}(n, d)$, we have

$$\begin{aligned}\mathrm{SM}^{\geqslant 1}(n, d) &= n^{\frac{\omega+1}{2}}d && \text{for } n \leqslant d^{\frac{2}{5-\omega}},\\ &= nd^{\frac{4}{5-\omega}} && \text{for } d^{\frac{2}{5-\omega}} \leqslant n.\end{aligned}$$

2 Characteristic polynomials of endomorphisms

In this section, we recall that characteristic polynomials of *endomorphisms* of Drinfeld modules can be read off at the level of Anderson motives. We then take advantage of this motivic interpretation to design fast algorithms (including the algorithms `F-MFF` and `F-MKU` mentioned in the introduction) for computing Drinfeld module endomorphism characteristic polynomials.

2.1 Duality between torsion points and A-motives

It is a standard result in the theory of Drinfeld modules that A-motives are duals to the so-called A-modules which, in some sense, correspond to torsion points (see for instance [Gos98, Sections 5.4, 5.6] or [Pap23, §3.6]). We hereby propose a concrete incarnation of this yoga, establishing a duality

[3] In [CLB17a], the complexity is given in number of operations in the ground field $\mathbb{F}_q$, with the assumption that applying the Frobenius endomorphism of K requires at most $O^\sim(d)$ operations in $\mathbb{F}_q$. Consequently one operation in $\mathbb{F}_q$ in the setting of [CLB17a] corresponds to $O^\bullet(\log q)$ bit operations in the complexity model of this article (see §1.2.1).

[4] Note that there is a typo in [CLB17a]: the critical exponent is not $\frac{5-\omega}{2}$ but $\frac{2}{5-\omega}$.

between the functors $\mathbb{E}_{\mathfrak{a}}$ and $\mathbb{M}_{\mathfrak{a}}$. The material presented in this subsection is somehow classical. However, we believe that our presentation is more elementary than those from aforementioned references: for instance, we do not need the introduction of (abelian) A-modules. As such, we include all proofs, hoping they will be of interest for some readers.

Let $\mathfrak{a}$ be an ideal of A away from the characteristic. We consider the evaluation map

$$\begin{aligned} \mathcal{B}: \quad \mathbb{E}(\phi) \times \mathbb{M}(\phi) &\to \overline{K} \\ (z, f) &\mapsto f(z). \end{aligned}$$

It is easily checked that $\mathcal{B}$ is $\mathbb{F}_q$-linear with respect to the variable z and K-linear with respect to the variable f. Moreover, it follows from the definitions that $\mathcal{B}$ vanishes on the subset $\mathbb{E}_{\mathfrak{a}}(\phi) \times \mathfrak{a}\mathbb{M}(\phi)$ and therefore induces a bilinear mapping

$$\mathcal{B}_{\mathfrak{a}}: \quad \mathbb{E}_{\mathfrak{a}}(\phi) \times \mathbb{M}_{\mathfrak{a}}(\phi) \to \overline{K}.$$

We consider the scalar extensions $\mathbb{E}_{\mathfrak{a}}(\phi)_{\overline{K}} = \overline{K} \otimes_{\mathbb{F}_q} \mathbb{E}_{\mathfrak{a}}(\phi)$ and $\mathbb{M}_{\mathfrak{a}}(\phi)_{\overline{K}} = \overline{K} \otimes_K \mathbb{M}_{\mathfrak{a}}(\phi)$. The map $\mathcal{B}_{\mathfrak{a}}$ induces a $\overline{K}$-bilinear form

$$\mathcal{B}_{\mathfrak{a},\overline{K}}: \quad \mathbb{E}_{\mathfrak{a}}(\phi)_{\overline{K}} \times \mathbb{M}_{\mathfrak{a}}(\phi)_{\overline{K}} \to \overline{K}.$$

Proposition 2.1. *The bilinear form $\mathcal{B}_{\mathfrak{a},\overline{K}}$ is a perfect pairing.*

Proof. Recall that, since $\mathfrak{a}$ is away from the characteristic, $\mathbb{E}_{\mathfrak{a}}(\phi)$ is free with rank r over $A/\mathfrak{a}$. Therefore, $\dim_{\mathbb{F}_q} \mathbb{E}_{\mathfrak{a}}(\phi) = r \cdot \deg(\mathfrak{a}) = \dim_K \mathbb{M}_{\mathfrak{a}}(\phi)$, and $\mathbb{E}_{\mathfrak{a}}(\phi)_{\overline{K}}$ and $\mathbb{M}_{\mathfrak{a}}(\phi)_{\overline{K}}$ have the same dimension over $\overline{K}$.

It is then enough to prove that $\mathcal{B}_{\mathfrak{a},\overline{K}}$ is nondegenerate on the left, meaning that if $x \in \mathbb{E}_{\mathfrak{a}}(\phi)_{\overline{K}}$ satisfies $\mathcal{B}_{\mathfrak{a},\overline{K}}(x, y) = 0$ for all $y \in \mathbb{M}_{\mathfrak{a}}(\phi)_{\overline{K}}$, then x must vanish. More generally, we are going to prove that there is no nonzero $x \in \mathbb{E}_{\mathfrak{a}}(\phi)_{\overline{K}}$ having the following property: $\mathcal{B}_{\mathfrak{a},\overline{K}}(x, 1 \otimes \tau^j) = 0$ for all j large enough. We argue by contradiction and consider an element $x \in \mathbb{E}_{\mathfrak{a}}(\phi)_{\overline{K}}$ satisfying the above property. We write

$$x = \lambda_1 \otimes z_1 + \cdots + \lambda_n \otimes z_n.$$

with $\lambda_i \in \overline{K}$ and $z_i \in \mathbb{E}_{\mathfrak{a}}(\phi)$. Moreover, we assume that x is chosen in such a way that the number of terms n is minimal. This ensures in particular that the z_i's are linearly independent over $\mathbb{F}_q$. Writing that $\mathcal{B}_{\mathfrak{a},\overline{K}}(x, 1 \otimes \tau^j)$ vanishes, we obtain the relation

$$(E_j): \quad \lambda_1 z_1^{q^j} + \cdots + \lambda_n z_n^{q^j} = 0,$$

which, in turn, implies

$$(E'_j): \quad \lambda_1^q z_1^{q^{j+1}} + \cdots + \lambda_n^q z_n^{q^{j+1}} = 0.$$

Combining the relations (E_{j+1}) and (E'_j), we find

$$(\lambda_1^q - \lambda_n^{q-1}\lambda_1) \cdot z_1^{q^{j+1}} + \cdots + (\lambda_{n-1}^q - \lambda_n^{q-1}\lambda_{n-1}) \cdot z_{n-1}^{q^{j+1}} = 0.$$

In other words, the vector

$$y = (\lambda_1^q - \lambda_n^{q-1}\lambda_1) \otimes z_1^{q^{j+1}} + \cdots + (\lambda_{n-1}^q - \lambda_n^{q-1}\lambda_{n-1}) \otimes z_{n-1}^{q^{j+1}} \in \mathbb{E}_{\mathfrak{a}}(\phi)_{\overline{K}}$$

is a new solution to our problem.

This will contradict the minimality condition in the choice of x if we can prove that y does not vanish. To do this, we again argue by contradiction. Given that the z_i's are linearly independent over $\mathbb{F}_q$, the vanishing of y would imply $\lambda_i^q - \lambda_n^{q-1}\lambda_i = 0$ for all i, from which we would deduce that all the quotients $\frac{\lambda_i}{\lambda_n}$ lie in $\mathbb{F}_q$. Thanks to the relations (E_j), this again contradicts the linear independence of the z_i's over $\mathbb{F}_q$. □

Remark 2.2. Proposition 2.1 can be seen as a Drinfeld analogue of the classical pairing between the singular homology and the de Rham cohomology of a complex abelian variety: the space $\mathbb{E}_{\mathfrak{a}}(\phi)$ plays the role of the singular homology (*via* the étale viewpoint), while the space $\mathbb{M}_{\mathfrak{a}}(\phi)$ can be thought of as the incarnation of the de Rham cohomology (see [Ang94]).

Proposition 2.1 gives a natural identification

$$\alpha_\phi : \quad \mathbb{E}_{\mathfrak{a}}(\phi)_{\overline{K}} \simeq \mathrm{Hom}_{\overline{K}}\left(\mathbb{M}_{\mathfrak{a}}(\phi)_{\overline{K}}, \overline{K}\right) \simeq \mathrm{Hom}_K\left(\mathbb{M}_{\mathfrak{a}}(\phi), \overline{K}\right),$$

where $\mathrm{Hom}_{\overline{K}}$ (resp. Hom_K) refers to the space of $\overline{K}$-linear (resp. K-linear) morphisms. *A priori*, the isomorphism α_ϕ is only $\overline{K}$-linear; we upgrade it and make it $A_{\overline{K}}$-linear.

Definition 2.3. Let M be a module over A_K. We set $M^* = \mathrm{Hom}_K(M, K)$ and equip it with the structure of A_K-module given by

$$a \cdot \xi = \big(m \mapsto \xi(am)\big),$$

where $a \in A_K$ and $\xi \in M^*$.

One checks that the construction $M \mapsto M^*$ is functorial, in the sense that if $g : M_1 \to M_2$ is a morphism of A_K-modules, then the dual map $g^* : M_2^* \to M_1^*$ is A_K-linear as well. We define $\mathbb{M}_{\mathfrak{a}}(\phi)^*_{\overline{K}} = \overline{K} \otimes_K \mathbb{M}_{\mathfrak{a}}(\phi)^*$; it is a module over $A_{\overline{K}}$. A direct adaptation of [Pap23, Lemma 3.6.2] using Noether's structure theorem for finitely generated modules over a Dedekind domain [Eis95, Theorem A3.2] gives the following lemma.

Lemma 2.4. *Any torsion finitely generated A_K-module M is (noncanonically) isomorphic to its dual M^*.*

Theorem 2.5. *The perfect pairing $\mathcal{B}_{\mathfrak{a},\overline{K}}$ induces an $A_{\overline{K}}$-linear isomorphism:*

$$\alpha_\phi : \quad \mathbb{E}_{\mathfrak{a}}(\phi)_{\overline{K}} \xrightarrow{\sim} \mathbb{M}_{\mathfrak{a}}(\phi)^*_{\overline{K}},$$

Moreover, given a Drinfeld module morphism $u : \phi \to \psi$, the following diagram is commutative:

$$\begin{array}{ccc} \mathbb{E}_{\mathfrak{a}}(\phi)_{\overline{K}} & \xrightarrow{\mathrm{id}\otimes\mathbb{E}_{\mathfrak{a}}(u)} & \mathbb{E}_{\mathfrak{a}}(\psi)_{\overline{K}} \\ \downarrow{\scriptstyle \alpha_\phi} & & \downarrow{\scriptstyle \alpha_\psi} \\ \mathbb{M}_{\mathfrak{a}}(\phi)^*_{\overline{K}} & \xrightarrow[\mathrm{id}\otimes\mathbb{M}_{\mathfrak{a}}(u)^*]{} & \mathbb{M}_{\mathfrak{a}}(\psi)^*_{\overline{K}} \end{array}$$

Proof. For the first assertion, we already know that α_ϕ is a $\overline{K}$-linear isomorphism. It then only remains to verify that it is A-linear. Let $a \in A$ and $z \in \mathbb{E}_\mathfrak{a}(\phi)$. By definition $a{\cdot}z = \phi_a(z)$ and $a{\cdot}f = f\phi_a$ for $f \in \mathbb{M}(\phi)$. Hence $\alpha_\phi(a{\cdot}z)$ is the function $f \mapsto f\big(\phi_a(z)\big) = (f\phi_a)(z) = (a{\cdot}f)(z)$, which means that $\alpha_\phi(a{\cdot}z) = a{\cdot}\alpha_\phi(z)$ as desired. The second assertion is easily checked. □

Remark 2.6. Theorem 2.5 shows that $\mathbb{E}_\mathfrak{a}(\phi)_{\overline{K}}$ determines $\mathbb{M}_\mathfrak{a}(\phi)_{\overline{K}}$ and *vice versa*. One can actually do much better and obtain a direct correspondence between $\mathbb{E}_\mathfrak{a}(\phi)$ and $\mathbb{M}_\mathfrak{a}(\phi)$ without extending scalars to $\overline{K}$ (see, for instance, [Pap23, Equation (3.6.9)]). For this, we need to add more structures. On the one hand, on $\mathbb{M}_\mathfrak{a}(\phi)$, we retain the τ-action as discussed in Remark 1.7. On the other hand, on $\mathbb{E}_\mathfrak{a}(\phi)$, we have a Galois action. Precisely let K^{sep} denote the separable closure of K inside $\overline{K}$. From the fact that $\mathfrak{a}$ is away from the characteristic, we deduce that $\mathbb{E}_\mathfrak{a}(\phi)$ lies in K^{sep}, and endow with an action of the Galois group $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$. We now have the following identifications refining those of Theorem 2.5:

$$\mathbb{E}_\mathfrak{a}(\phi) \simeq \mathrm{Hom}_{K\{\tau\}}\left(\mathbb{M}_\mathfrak{a}(\phi), K^{\mathrm{sep}}\right)$$
$$\mathbb{M}_\mathfrak{a}(\phi) \simeq \mathrm{Hom}_{\mathbb{F}_q[G_K]}\left(\mathbb{E}_\mathfrak{a}(\phi), K^{\mathrm{sep}}\right)$$

where, in the first (resp. second) line, we consider K-linear morphisms commuting with the τ-action (resp. $\mathbb{F}_q$-linear morphisms commutating with the Galois action). In other words, the Galois representation $\mathbb{E}_\mathfrak{a}(\phi)$ and the τ-module $\mathbb{M}_\mathfrak{a}(\phi)$ correspond one to the other under Katz' anti-equivalence of categories [Kat73, Proposition 4.1.1].

Remark 2.7. In [vdH04], van der Heiden proposes another approach, proving that there is a canonical A-linear isomorphism:

$$\mathbb{E}_\mathfrak{a}(\phi) \simeq \mathrm{Hom}_{A/\mathfrak{a}}\left(\mathbb{M}_\mathfrak{a}(\phi)^\tau, \Omega_A/\mathfrak{a}\Omega_A\right)$$

where $\mathbb{M}_\mathfrak{a}(\phi)^\tau$ denotes the subset of fixed points of $\mathbb{M}_\mathfrak{a}(\phi)$ by the τ-action and Ω_A is the module of Kähler differential forms of A over $\mathbb{F}_q$ (see Proposition 4.3 of *loc. cit.*). However, the formulation of Theorem 2.5 is better suited for the applications we shall develop in this article.

If M is a finitely generated projective A_K-module of rank n, we let

$$\det M = \bigwedge^n M$$

denote the maximal exterior power of M. Any A_K-linear endomorphism $f : M \to M$ induces a linear map $\det f : \det M \to \det M$. The latter is the multiplication by some element of A_K, that we call the *determinant* of f and denote by $\det f$ in a slight abuse of notation. Similarly, we define the characteristic polynomial of f as the determinant of the $A_K[X]$-linear map $X - f$ acting on $A_K[X] \otimes_{A_K} M$.

A classical consequence of Theorem 2.5 is the following.

Theorem 2.8. *Let ϕ be a Drinfeld module and let $u : \phi \to \phi$ be an endomorphism. Let $\mathfrak{q} \subset A$ be a maximal ideal away from the characteristic. Then the characteristic polynomials of $\mathbb{T}_\mathfrak{q}(u)$ and $\mathbb{M}(u)$ are equal.*

In particular, $\mathfrak{n}(u)$ is the principal ideal generated by $\det(\mathbb{M}(u))$.

Proof. Let $n \in \mathbb{Z}_{\geqslant 0}$. Applying Theorem 2.5 with $\mathfrak{a} = \mathfrak{q}^n$, we find

$$\pi\big(\mathbb{E}_{\mathfrak{q}^n}(u)\big) = \pi\big(\mathbb{E}_{\mathfrak{q}^n}(u)_{\overline{K}}\big) = \pi\big(\mathbb{M}_{\mathfrak{q}^n}(u)_{\overline{K}}\big) = \pi\big(\mathbb{M}_{\mathfrak{q}^n}(u)\big),$$

the second equality being a consequence of Theorem 2.5 and the fact that two dual morphisms have the same determinant (in suitable bases, their matrices are transposed one to the other). Thus we obtain $\pi(\mathbb{T}_{\mathfrak{q}}(u)) \equiv \pi(\mathbb{M}(u)) \pmod{\mathfrak{q}^n}$. Since this holds for all positive integer n, we conclude that $\pi(\mathbb{T}_{\mathfrak{q}}(u)) = \pi(\mathbb{M}(u))$.

The last statement now follows from [Gek91, Lemma 3.10]. □

2.2 Algorithms: the case of $\mathbb{P}^1$

In this subsection, we assume that $A = \mathbb{F}_q[T]$, and we let ϕ be a Drinfeld module of rank r. We fix an endomorphism $u : \phi \to \phi$ and aim at designing an algorithm that computes the characteristic polynomial (resp. norm) of u. Under the assumption that $A = \mathbb{F}_q[T]$, the ring $A_K \simeq K[T]$ is a principal ideal domain and $\mathbb{M}(\phi)$ is free of rank r. Moreover, a canonical basis is given by $(1, \tau, \dots, \tau^{r-1})$. Our strategy is then clear: we compute the matrix representing the $K[T]$-linear map $\mathbb{M}(u)$ in the aforementioned canonical basis and then return its characteristic polynomial (resp. determinant); Theorem 2.8 ensures that it is the characteristic polynomial (resp. norm) of u.

2.2.1 Generic algorithm

Our first need is to design an algorithm for computing the coordinates of an element $f \in \mathbb{M}(\phi)$, represented as an Ore polynomial, in the canonical basis of $\mathbb{M}(\phi)$. This is achieved by Algorithm 1, whose correctness is immediately proved by induction on the τ-degree of f.

Algorithm 1: MotiveCoordinates

Input: An element f in the motive $\mathbb{M}(\phi)$
Output: The coordinates $(f_0, \dots, f_{r-1})$ of f in the canonical basis of $\mathbb{M}(\phi)$

```
If deg f < r then
    Return the vector defined by the coefficients of f
Else
    Set m = max(1, ⌊deg(f)/2r⌋)
    Write f = a · φ_X^m + b with deg(b) < rm (right Euclidean division)
    Return X^m · MotiveCoordinates(a) + MotiveCoordinates(b)
Endif
```

Lemma 2.9. *For an input $f \in \mathbb{M}(\phi)$ of τ-degree n. Algorithm 1 requires $O(n^2)$ applications of the Frobenius endomorphism and $O(n^2)$ operations in K.*

Proof. The first step of the algorithm consists in computing ϕ_X^m. Using fast exponentiation, this costs $O(n^2)$ applications of the Frobenius endomorphism and $O(n^2)$ operations in K. The Euclidean division requires $O(n^2)$ applications of the Frobenius endomorphism and $O(n^2)$ operations in K as well.

Let $C(s)$ be the cost of running the algorithm on an entry with degree s. By what precedes, $C(s)$ is less than $C(\lceil \frac{s}{2} \rceil)$, plus $O(s^2)$ operations in K and $O(s^2)$ applications of the Frobenius endomorphism. We conclude using the Master Theorem [CLRS22, Theorem 4.1]. □

From Algorithm 1, we also derive the following bounds on the size of the coefficients.

Lemma 2.10. *Let $f \in \mathbb{M}(\phi)$ and let $f_0, \dots, f_{r-1} \in K[T]$ be the coordinates of f in the canonical basis. Then for $0 \leqslant i < r$ we have*

$$\deg_T(f_i) \leqslant \frac{\deg_\tau(f) - i}{r}.$$

Corollary 2.11. *Let $(P_{i,j})_{0 \leqslant i,j < r}$ be the matrix of $\mathbb{M}(u)$ in the canonical bases. Then for every $0 \leqslant i, j \leqslant r-1$ we have*

$$\deg(P_{i,j}) \leqslant \frac{\deg(u) + j - i}{r}.$$

Proof. By definition, $P_{i,j}$ is the coefficient in front of τ^i in the decomposition of $\tau^j u$ in the canonical basis. The corollary then follows from Lemma 2.10. □

As a consequence of the previous statements, we obtain an alternative proof of the following classical result [Pap23, Theorem 4.2.7].

Proposition 2.12. *Let $\pi = \pi_0(T) + \cdots + \pi_r(T)X^r$ be the characteristic polynomial of the Frobenius endomorphism of ϕ. Then for every $0 \leqslant i \leqslant r$ we have*

$$\deg(\pi_i) \leqslant \frac{r-i}{r} d.$$

Proof. Using Theorem 2.8, we know that π is the characteristic polynomial of the matrix P of $\mathbb{M}(\tau^d)$ in the canonical bases. Therefore, for every $0 \leqslant i \leqslant d$, π is the trace of $\bigwedge^i \mathbb{M}(\tau^d)$, which is an alternated sum on the minors of P with size i. We conclude using Corollary 2.11. □

Instead of independently computing all columns using Algorithm 1, a more intelligent approach can be employed to calculate the matrix of $\mathbb{M}(u)$: in order to speed up the computation of a column, we may reuse those that are already computed. For this, we write

$$\phi_T = g_0 + g_1\tau + \cdots + g_r\tau^r$$

with $g_i \in K, g_r \neq 0$. For a polynomial $h \in K[T]$, we let h^τ denote the polynomial deduced from h by raising all its coefficients to the q-th power. An easy computation then shows that if $(f_0, \dots, f_{r-1})$ are the coordinates of some $f \in \mathbb{M}(\phi)$ in the canonical basis, then the coordinates $(f'_0, \dots, f'_{r-1})$ of τf are defined by the following matrix equality:

$$\begin{pmatrix} f'_0 \\ f'_1 \\ \vdots \\ f'_{r-1} \end{pmatrix} = \begin{pmatrix} 0 & 0 & \dots & 0 & \frac{T-g_0}{g_r} \\ 1 & 0 & \dots & 0 & -\frac{g_1}{g_r} \\ & & \ddots & & \\ 0 & 0 & \dots & 1 & -\frac{g_{r-1}}{g_r} \end{pmatrix} \cdot \begin{pmatrix} f_0^\tau \\ f_1^\tau \\ \vdots \\ f_{r-1}^\tau \end{pmatrix}. \tag{1}$$

This readily yields Algorithm 2.

Algorithm 2: MotiveTauAction

Input: The coordinates $(f_0, \dots, f_{r-1})$ of an element $f \in \mathbb{M}(\rho)$
Output: The coordinates of $\tau f \in \mathbb{M}(\rho)$

1 Compute the polynomials $f_0^\tau, \dots, f_{r-1}^\tau$
2 Compute the polynomial $f_0' = \frac{T - g_0}{g_r} f_{r-1}^\tau$
3 For $1 \leqslant i \leqslant r-1$
4 | Compute the polynomial $f_i' = f_i^\tau - \frac{g_{i+1}}{g_r} f_{r-1}^\tau$
5 Return $(f_0', \dots, f_{r-1}')$

Lemma 2.13. *For an input $f \in \mathbb{M}(\phi)$ of τ-degree n, Algorithm 2 requires at most $O(n)$ applications of the Frobenius endomorphism and $O(n)$ operations in K.*

Proof. By Lemma 2.10, the polynomial $f_i \in K[T]$ has degree at most $\frac{n-i}{r}$. As a consequence, computing f_i^τ requires at most $\left\lfloor \frac{n-i}{r} \right\rfloor + 1$ applications of the Frobenius endomorphism, and the pre-computation on line 1 costs

$$\sum_{i=0}^{r-1} \left(\left\lfloor \frac{n-i}{r} \right\rfloor + 1 \right) = n + 1$$

such applications. The remaining steps can be done in $O(n)$ arithmetic operations in K. □

Computing the matrix of $\mathbb{M}(u)$ is now just a matter of computing the coordinates of u and iteratively applying r times the τ-action. The precise procedure is presented in Algorithm 3.

Algorithm 3: MotiveMatrix

Input: An endomorphism $u : \phi \to \phi$ encoded by its defining Ore polynomial
Output: The matrix of $\mathbb{M}(u)$ in the canonical bases

1 Compute $U_0 = \text{MotiveCoordinates}(u, \phi)$
2 For $1 \leqslant i \leqslant r-1$
3 | Compute $U_i = \text{MotiveTauAction}(U_{i-1})$
4 Return the matrix whose columns are $(U_0, \dots, U_{r-1})$

Lemma 2.14. *For an input u of τ-degree n, Algorithm 3 requires at most $O(n^2 + r^2)$ applications of the Frobenius endomorphism, and $O(n^2 + r^2)$ operations in K.*

Proof. Computing U_0 requires $O(n^2)$ applications of the Frobenius endomorphism and $O(n^2)$ operations in K (Lemma 2.9). Then, knowing U_i for some $1 \leqslant i \leqslant r-1$, the computation of U_{i+1} requires at most $O(n+i)$ applications of the Frobenius and $O(n+i)$ operations in K by Lemma 2.13. Summing all the contributions, we end up with the announced complexity. □

We now have all the ingredients to write down Algorithm 4, which is the main algorithm of this section.

Algorithm 4: EndomorphismCharpoly

Input: An endomorphism $u : \phi \to \phi$ encoded by its defining Ore polynomial
Output: The characteristic polynomial of u

1 Compute $M = \text{MotiveMatrix}(u)$
2 Return the characteristic polynomial of M

Theorem 2.15. *For a morphism of Drinfeld modules $u : \phi \to \phi$ of τ-degree n, Algorithm 4 computes the characteristic polynomial of u for a cost of $O(n^2 + r^2)$ applications of the Frobenius and $O^{\sim}(n^2 + (n+r)r^{\Omega-1})$ operations in K.*

Proof. The cost of computing the matrix of $\mathbb{M}(u)$ is $O(n^2 + r^2)$ applications of the Frobenius endomorphism, and $O(n^2 + r^2)$ operations in K. The matrix has size r and, thanks to Corollary 2.11, we know that all its entries have degree less than $1 + \frac{n}{r}$. Its characteristic polynomial can then be computed within $O^{\sim}((n+r)r^{\Omega-1})$ operations in K (see §1.2.2). The theorem follows. □

2.2.2 The case of finite fields

If K is a finite field, we can speed up the computation by using specific algorithmic primitives to compute characteristic polynomial of polynomial matrices (see §1.2.2) on the one hand, and to compute Ore Euclidean divisions (see §1.2.3) on the other hand.

Theorem 2.16. *If K is a finite extension of $\mathbb{F}_q$ of degree d and u is an endomorphism of τ-degree n of a Drinfeld module ϕ of rank r, then Algorithm 4 computes the characteristic polynomial of u for a cost of*

$$O^{\sim}(d \log^2 q) + O^{\bullet}\left(\left(\mathrm{SM}^{\geqslant 1}(n, d) + ndr + nr^{\omega} + dr^{\omega}\right) \cdot \log q\right)$$

bit operations.

Proof. The complexity analysis is similar to that of Theorem 2.15, except that the Ore Euclidean division of Algorithm 1 now costs $O^{\sim}(d \log^2 q) + O^{\bullet}(\mathrm{SM}^{\geqslant 1}(n, d) \log q)$ bit operations. The computation of the matrix of $\mathbb{M}(u)$ therefore requires

$$O^{\sim}(d \log^2 q) + O^{\bullet}\left(\left(\mathrm{SM}^{\geqslant 1}(n, d) + dr(n + r)\right) \log q\right)$$

bit operations. Finally, it remains to compute the characteristic polynomial of the matrix. For this, we first notice that all its coefficients of have degree at most n (Corollary 2.11). Therefore, using Lemma 1.14, the computation of the characteristic polynomial costs $O^{\bullet}((n+d)r^{\omega})$ operations in $\mathbb{F}_q$. The theorem follows. □

Remark 2.17. Comparing with the algorithms of [MS23], we find that Algorithm 4 exhibits a better theoretical complexity, except when the degree of $\gamma(T)$ is close to d and the rank r is very small compared to d and n; in this case, the algorithm of [MS23, Theorem 2(1)] has quadratic complexity in $\max(n, d)$, beating the term $\mathrm{SM}^{\geqslant 1}(n, d)$.

When u is the Frobenius endomorphism, Algorithm 4 leads to the algorithm `F-MFF` discussed in the introduction, whose complexity is given by Corollary 2.18.

Corollary 2.18 (Variant F-MFF)**.** *If K is a finite field of degree d over $\mathbb{F}_q$, Algorithm 4 computes the characteristic polynomial of the Frobenius endomorphism of ϕ for a cost of*

$$O^{\sim}(d \log^2 q) + O^{\bullet}\left(\left(\mathrm{SM}^{\geqslant 1}(d, d) + d^2 r + d r^{\omega}\right) \cdot \log q\right)$$

bit operations.

Proof. This is a direct application of Theorem 2.16 with $n = d$. □

2.2.3 The case of the Frobenius endomorphism: another approach

Below, we present yet another method to compute the characteristic polynomial of the Frobenius endomorphism F_ϕ. This leads to the algorithm F-MKU, as mentioned in the introduction, which performs better for some ranges of parameters (at least theoretically). It is based on the two following remarks:

- As the Ore polynomial τ^d is central in $K\{\tau\}$, and its action on the motive can unambiguously be defined as a left or right multiplication.
- The left multiplication by τ on $\mathbb{M}(\phi)$ is a semi-linear application, whose matrix is the companion matrix appearing in Equation (1), which is easy to compute.

More precisely, for a nonnegative integer s, let μ_s be the $K[T]$-semi-linear endomorphism of $\mathbb{M}(\phi)$ defined by $f \mapsto \tau^s f$. We denote its matrix by M_s. In other words, M_s is the matrix whose j-th column contains the coefficients of $\tau^{j+s} \in \mathbb{M}(\phi)$ in the canonical basis. The matrix M_1 is the companion matrix of Equation (1) and, by definition, the matrix of $\mathbb{M}(u)$ is M_d.

For a polynomial $P \in \mathbb{F}_q[T]$, we define P^{τ^s} as the polynomial obtained by raising each coefficient of P to power q^s. Similarly, given a matrix M with entries in $\mathbb{F}_q[T]$, we write M^{τ^s} for the matrix obtained from M by applying $P \mapsto P^{\tau^s}$ to each of its entry. A calculation shows that

$$M_s = M_1 \cdot M_1^{\tau} \cdots M_1^{\tau^{s-1}}.$$

This equation leads to the following *square and multiply*-like formulas:

$$M_{2s} = M_s \cdot M_s^{\tau^s}, \tag{2}$$

$$M_{2s+1} = M_1 \cdot M_s^{\tau} \cdot M_s^{\tau^{s+1}}. \tag{3}$$

Let α be a generator of K over $\mathbb{F}_q$. Elements of K are classically represented as polynomials in α with coefficients in $\mathbb{F}_q$ and degree $d - 1$. Applying τ^s to an element $\sum_{i=0}^{r-1} a_i \alpha^i \in K$ amounts to applying the substitution $\alpha \mapsto \tau^s(\alpha)$. Thus, this can be efficiently computed using Kedlaya-Umans' algorithm for modular composition [KU11] for a cost of $O^{\bullet}(d \log q)$ bit operations. As mentioned in §1.2.1, an initial precomputation of α^q must be performed once and for all, for a cost of $O^{\sim}(d \log^2 q)$ bit operations.

Theorem 2.19 (Variant F-MKU)**.** *If K is a finite extension of $\mathbb{F}_q$ of degree d, the characteristic polynomial of the Frobenius endomorphism of a Drinfeld module ϕ of rank r can be computed for a cost of*

$$O^{\sim}(d \log^2 q) + O^{\bullet}\left(\left(d^2 r^{\omega-1} + d r^{\omega}\right) \cdot \log q\right)$$

bit operations.

Proof. Let $\mathrm{C}(s)$ be the cost, counted in bit operations, of computing the pair $\mathcal{P}_s = (M_s, \tau^s(\alpha))$. To compute $\mathcal{P}_{2s}$ and $\mathcal{P}_{2s+1}$, one uses the recurrence relations (2) and (3). As M_s has r^2 polynomial coefficients of degree at most s/r (Lemma 2.10), computing $\tau^s(M)$ requires $O(sr)$ modular compositions of degree d. As previously mentioned, we use Kedlaya-Umans' algorithm [KU11] for this task, leading to a total cost of $O^\bullet(nrd\cdot\log q)$ bit operations. Similarly $\tau^{2s}(\alpha)$ can be computed by composing $\tau^s(\alpha)$ with itself; using again Kedlaya-Umans' algorithm, this can be done within $O^\bullet(d\cdot\log q)$ bit operations. Moreover, the matrix product $M_s\cdot\tau^s(M)$ requires $O^\sim(dsr^{\omega-1})$ extra operations in $\mathbb{F}_q$. Given that one operation in $\mathbb{F}_q$ corresponds to $O^\sim(\log q) \subset O^\bullet(\log q)$ bit operations, we conclude that

$$\mathrm{C}(2s) \leqslant \mathrm{C}(s) + O^\bullet(dsr^{\omega-1}\log q).$$

A similar analysis provides a similar bound for $\mathrm{C}(2s+1)$. Solving the recurrence, we obtain $\mathrm{C}(s) \in O^\bullet(dsr^{\omega-1}\log q)$. Therefore, the computation of $\mathbb{M}(u)$ can be done within $O^\bullet(d^2r^{\omega-1}\log q)$ bit operations.

Finally, the characteristic polynomial of the matrix of $\mathbb{M}(u)$ is computed as previously, using Lemma 1.14, for a cost of $O^\sim(dr^\omega)$ operations in $\mathbb{F}_q$, which is no more than $O^\bullet(dr^\omega\cdot\log q)$ bit operations. Adding both contributions and taking into account the precomputation of α^q, we obtain the corollary. □

2.3 Algorithms: the case of a general curve

We now drop the assumption that $A = \mathbb{F}_q[T]$. In full generality, it is not true that the motive $\mathbb{M}(\phi)$ is free over A_K, and the matrix of $\mathbb{M}(u)$ is not defined. One can nevertheless easily work around this difficulty, by extending scalars to the fraction field of A_K, denoted by $\mathrm{Frac}(A_K)$. Indeed, $\mathrm{Frac}(A_K)\otimes_{A_K}\mathbb{M}(\phi)$ is obviously free over $\mathrm{Frac}(A_K)$ given that the latter is a field. It is also clear that the determinants of $\mathbb{M}(u)$ and $\mathrm{Frac}(A_K)\otimes_{A_K}\mathbb{M}(u)$ are equal.

Our first need is to design an algorithm for computing a basis of $\mathrm{Frac}(A_K)\otimes_{A_K}\mathbb{M}(\phi)$. For this, we will rely on the case of $\mathbb{F}_q[T]$, previously treated. We consider an element $T \in A$, $T \notin \mathbb{F}_q$. Since the underlying curve C is absolutely irreducible, T must be transcendental over $\mathbb{F}_q$. This gives an embedding $\mathbb{F}_q[T] \to A$, which extends to an inclusion of fields $K(T) \to \mathrm{Frac}(A_K)$. The resulting extension is finite of degree $t = \deg(T)$. Let $(b_1, \dots, b_t)$ be a basis of $\mathrm{Frac}(A_K)$ over $K(T)$.

In what follows, T and $(b_1, \dots, b_t)$ are assumed to be known. Finding them depends on the way C is given, but we believe that our hypothesis is reasonable. For instance, if C is presented as a plane smooth curve, *i.e.* if A is given as

$$A = \mathbb{F}_q[X, Y]/P(X, Y) \quad \text{with} \quad P \in \mathbb{F}_q[X, Y]$$

one may choose $T = X$, $t = \deg_Y P$ and $b_i = Y^{i-1}$ for $1 \leqslant j \leqslant t$.

Remark 2.20. Let g be the genus of C. The Riemann-Roch theorem indicates that the Riemann-Roch space $\mathcal{L}\big((g+1)\cdot[\infty]\big)$ has dimension at least 2. Hence it must contain a transcendental function, which shows that there always exists T for which $t \leqslant g+1$. In practice, T can be computed through various different algorithms (see [LGS20, ACL22] and the references therein).

Now given a Drinfeld module $\phi : A \to K\{\tau\}$ over A, we restrict it to $\mathbb{F}_q[T]$ *via* the embedding $\mathbb{F}_q[T] \to A$, obtaining a second Drinfeld module $\phi' : \mathbb{F}_q[T] \to K\{\tau\}$ (see §1.1.4). Then $\mathbb{M}(\phi') = \mathbb{M}(\phi)$, with the same structure of $K[T]$-modules. Moreover, if ϕ has rank r, we have

$$\deg \phi'_T = \deg \phi_T = r \cdot \deg(T) = rt$$

showing that ϕ' has rank rt. The family $(1, \tau, \dots, \tau^{rt-1})$ is a basis of $\mathbb{M}(\phi)$ over $K[T]$, and we can use Algorithm 1 to compute the coordinates of any element of $\mathbb{M}(\phi)$ with respect to this basis. Let $\Gamma : \mathbb{M}(\phi) \to K[T]^{rt}$ be the map taking an element of $\mathbb{M}(\phi)$ to the column vector representing its coordinate in the above basis. Both Γ and Γ^{-1} are efficiently computable.

Let e_1 be an arbitrary nonzero element of $\mathbb{M}(\phi)$, *e.g.* $e_1 = 1$. A $K(T)$-basis of the $\mathrm{Frac}(A_K)$-line generated by e_1 is explicitly given by the family $e_1\phi_{b_1}, \dots, e_1\phi_{b_t}$. For $1 \leqslant j \leqslant t$, we set $C_{1,j} = \Gamma(e_1\phi_{b_j})$ and we form the following matrix, with rt rows and t columns:

$$M_1 = \begin{pmatrix} C_{1,1} & \cdots & C_{1,t} \end{pmatrix}.$$

We now consider a column vector E_2 outside the image of M_1 and define $e_2 = \Gamma^{-1}(E_2)$; e_2 is not $\mathrm{Frac}(A_K)$-collinear to e_1, and we have constructed a free family of cardinality 2. We then continue the same process, by setting $C_{2,j} = \Gamma(e_2\phi_{b,j})$ and considering the $rt \times 2t$ matrix

$$M_2 = \begin{pmatrix} C_{1,1} & \cdots & C_{1,t} & C_{2,1} & \cdots & C_{2,t} \end{pmatrix}.$$

We pick a column vector E_3 outside the image of M_2 and define $e_3 = \Gamma^{-1}(E_3)$, as well as M_3. We repeat this construction until we reach e_r. The vectors $e_1, \dots, e_r$ being linearly independent over $\mathrm{Frac}(A_K)$, they form a $\mathrm{Frac}(A_K)$-basis of $\mathrm{Frac}(A_K) \otimes_{A_K} \mathbb{M}(\phi)$. The matrix M_r is nothing but the change-of-basis matrix from the canonical $K[T]$-basis of $\mathbb{M}(\phi)$ to the newly computed basis $\mathcal{B} = (e_1\phi_{b_1}, \dots, e_1\phi_{b_t}, \dots, e_r\phi_{b_1}, \dots, e_r\phi_{b_t})$. If $f \in \mathbb{M}(\phi)$, the product $M_r^{-1} \cdot \Gamma^{-1}(f)$ gives the coordinates of f in $\mathcal{B}$. From this, we eventually read the coordinates of f in the $\mathrm{Frac}(A_K)$-basis $(e_1, \dots, e_r)$.

To summarize, we have constructed a $\mathrm{Frac}(A_K)$-basis of $\mathrm{Frac}(A_K) \otimes_{A_K} \mathbb{M}(\phi)$ and designed an algorithm to compute coordinates in this basis. Using these inputs as primitives, it is now straightforward to extend the results of §2.2 to the case of a general curve.

3 Norms of isogenies

In Section 2, we have only covered the case of *endomorphisms* between Drinfeld modules. We now consider general morphisms and isogenies. Let ϕ, ψ be two rank r Drinfeld A-modules, and let $u : \phi \to \psi$ be an isogeny. In this setting, the caracteristic polynomial is no longer defined but the norm of u continues to make sense (see §1.1.3); we recall that it is an ideal of A, denoted by $\mathfrak{n}(u)$. The purpose of this section is twofold: first, to establish explicit formulas that recover $\mathfrak{n}(u)$ at the motive level, and secondly, to offer efficient algorithms for the computation of $\mathfrak{n}(u)$ using those formulas.

3.1 Reading norms on the motive

In our general context, the determinant of u can no longer be defined as previously. In §3.1.1, we set up important definitions and statements about determinants in projective modules. Our main results are stated in §3.1.2.

3.1.1 Determinants on projective modules

Let $\mathcal{A}$ be a Dedekind domain. Let M, M' be two finitely generated projective $\mathcal{A}$-modules of rank n. Let $f : M \to M'$ be an $\mathcal{A}$-linear mapping. The morphism f gives rise to the $\mathcal{A}$-linear map $\det f : \det M \to \det M'$. However, when f has different domain and codomain, *i.e.* $M \neq M'$, it no longer makes sense to interpret $\det f$ as the multiplication by some scalar. Instead, we define the "determinant" of f, denoted by $\mathfrak{det} f$, as the ideal quotient $(\det M' : \mathrm{im}(\det f))$, that is

$$\mathfrak{det} f = (\det M' : \mathrm{im}(\det f)) = \left\{a \in \mathcal{A} : a \det M' \subset \mathrm{im}(\det f)\right\}.$$

Equivalently $\mathfrak{det} f$ is the annihilator ideal of the cokernel of $\det f$.

Since $\mathcal{A}$ is a Dedekind domain, $\mathfrak{det} f$ can be decomposed as a product

$$\mathfrak{det} f = \prod_{\mathfrak{q}} \mathfrak{q}^{v_{\mathfrak{q}}(\mathfrak{det} f)},$$

where the product runs over all maximal ideals $\mathfrak{q}$ of $\mathcal{A}$ and the exponent $v_{\mathfrak{q}}(\mathfrak{det} f)$ is a nonnegative integer referred to as the $\mathfrak{q}$-*adic valuation* of $\mathfrak{det} f$.

For the purpose of this article, it is fundamental to notice that $v_{\mathfrak{q}}(\mathfrak{det} f)$ can be found out by computing the classical determinant of an actual matrix. Indeed, letting as before $\mathcal{A}_{\mathfrak{q}}$ denote the completion[5] of $\mathcal{A}$ at $\mathfrak{q}$, we define $M_{\mathfrak{q}} = \mathcal{A}_{\mathfrak{q}} \otimes_{\mathcal{A}} M$ and $M'_{\mathfrak{q}} = \mathcal{A}_{\mathfrak{q}} \otimes_{\mathcal{A}} M'$. The map f induces a $\mathcal{A}_{\mathfrak{q}}$-linear morphism $f_{\mathfrak{q}} : M_{\mathfrak{q}} \to M'_{\mathfrak{q}}$. We deduce from the flatness of $\mathcal{A}_{\mathfrak{q}}$ over $\mathcal{A}$ that

$$\mathfrak{det} f_{\mathfrak{q}} = \mathcal{A}_{\mathfrak{q}} \otimes_{\mathcal{A}} \mathfrak{det} f = (\mathfrak{q}\cdot\mathcal{A}_{\mathfrak{q}})^{v_{\mathfrak{q}}(\mathfrak{det} f)}, \tag{4}$$

where $\mathfrak{det} f_{\mathfrak{q}}$ is defined, similarly to $\mathfrak{det} f$, as the annihilator ideal of the cokernel of $f_{\mathfrak{q}}$.

On the other hand, we know that $\mathcal{A}_{\mathfrak{q}}$ is a principal domain. Hence both $M_{\mathfrak{q}}$ and $M'_{\mathfrak{q}}$ are free of rank n over $\mathcal{A}_{\mathfrak{q}}$. We choose bases $\mathcal{B}_{(\mathfrak{q})}$ and $\mathcal{B}'_{(\mathfrak{q})}$ of $M_{\mathfrak{q}}$ and $M'_{\mathfrak{q}}$ respectively, and let $F_{\mathfrak{q}}$ denote the matrix of $f_{\mathfrak{q}}$ in these bases. It follows from the definition that $\mathfrak{det} f_{\mathfrak{q}} = \det(F_{\mathfrak{q}})\ \mathcal{A}_{\mathfrak{q}}$. Comparing with Equation (4), we finally conclude that

$$v_{\mathfrak{q}}(\mathfrak{det} f) = v_{\mathfrak{q}}(\det F_{\mathfrak{q}}).$$

We notice in particular that, although the determinant itself depends on the choices of $\mathcal{B}_{(\mathfrak{q})}$ and $\mathcal{B}'_{(\mathfrak{q})}$, its $\mathfrak{q}$-adic valuation does not. Indeed, changing $\mathcal{B}_{(\mathfrak{q})}$ (resp. $\mathcal{B}'_{(\mathfrak{q})}$) boils down to multiplying $F_{\mathfrak{q}}$ by an invertible matrix on the left (resp. on the right), which only multiplies the determinant a unit, and as such, does not affect its $\mathfrak{q}$-adic valuation.

In a similar fashion, one can relate $\mathfrak{det} f$ to the Euler-Poincaré characteristic of the cokernel of f, which is essential to establish our main theorem.

[5] When studying projective modules, it is more common to consider the localization $\mathcal{A}_{(\mathfrak{q})}$ instead of the completion $\mathcal{A}_{\mathfrak{q}}$. Although the first setting is simpler, the second better suits our needs.

Proposition 3.1. *We have*

$$\mathfrak{det} f = \chi_{\mathcal{A}}(\operatorname{coker} f).$$

Proof. As we have seen, the Euler-Poincaré characteristic commutes with localization. Therefore, it is enough to prove that $\mathfrak{det} f_{\mathfrak{q}} = \chi_{\mathcal{A}_{\mathfrak{q}}}(\operatorname{coker} f_{\mathfrak{q}})$ for each maximal ideal $\mathfrak{q}$ of $\mathcal{A}$.

Let then $\mathfrak{q}$ be a maximal ideal of $\mathcal{A}$. It follows from the structure theorem of finitely generated modules over principal domains that there exist bases $\mathcal{B}_{\mathfrak{q}}$ and $\mathcal{B}'_{\mathfrak{q}}$ in which the matrix $F_{\mathfrak{q}}$ of $f_{\mathfrak{q}}$ is diagonal. If $\delta_1, \dots, \delta_r$ denote its diagonal coefficients, we have

$$\operatorname{coker} f_{\mathfrak{q}} \simeq \left(\mathcal{A}_{\mathfrak{q}}/\delta_1\mathcal{A}_{\mathfrak{q}}\right) \times \cdots \times \left(\mathcal{A}_{\mathfrak{q}}/\delta_r\mathcal{A}_{\mathfrak{q}}\right).$$

Hence

$$\chi_{\mathcal{A}_{\mathfrak{q}}}(\operatorname{coker} f_{\mathfrak{q}}) = \delta_1 \cdots \delta_r \cdot \mathcal{A}_{\mathfrak{q}} = (\det F_{\mathfrak{q}}) \cdot \mathcal{A}_{\mathfrak{q}} = \mathfrak{det} f_{\mathfrak{q}}$$

which is what we wanted to prove. □

3.1.2 Main results

We may now state and prove the main theoretical results of this subsection.

Theorem 3.2. *Let ϕ and ψ be two Drinfeld modules, and let $u : \phi \to \psi$ be an isogeny. We have*

$$\mathfrak{n}(u) = \mathfrak{det}\, \mathbb{M}(u).$$

Proof. Writing u as the product of a purely inseparable isogeny with a separable isogeny, and noticing that (1) $\mathfrak{det}$ is multiplicative and (2) $\mathbb{M}$ is functorial, we are reduced to prove the theorem when $u = \tau^{\deg(\mathfrak{p})}$ on the one hand and when u is separable on the other hand.

Purely inseparable case. We assume that $u = \tau^{\deg(\mathfrak{p})}$. We follow Gekeler's idea for proving [Gek91, Lemma 3.10]. Let $\mathfrak{q} \subset \mathcal{A}$ be a maximal ideal away from the characteristic. Note that the map $\mathbb{E}_{\mathfrak{q}}(u) : \mathbb{E}_{\mathfrak{q}}(\phi) \to \mathbb{E}_{\mathfrak{q}}(\psi)$ is an isomorphism because τ is coprime with the right gcd of ϕ_q for q varying in $\mathfrak{q}$. By Theorem 2.5, we conclude that $\mathbb{M}_{\mathfrak{q}}(u) : \mathbb{M}_{\mathfrak{q}}(\psi) \to \mathbb{M}_{\mathfrak{q}}(\phi)$ is an isomorphism as well, showing that $\mathfrak{q}$ is coprime with $\chi_{A_K}(\operatorname{coker} \mathbb{M}(u))$. Consequently, $\mathfrak{det}\, \mathbb{M}(u)$ is a power of $\mathfrak{p}$. On the other hand, observe that, by definition,

$$\deg(u) = \dim_K(\operatorname{coker} \mathbb{M}(u)) = \deg(\chi_{A_K}(\mathbb{M}(u))).$$

Proposition 3.1 then implies that $\deg(\mathfrak{det}\, \mathbb{M}(u)) = \deg(u) = \deg(\mathfrak{p})$. Putting all together, we conclude that $\mathfrak{det}\, \mathbb{M}(u) = \mathfrak{p} = \mathfrak{n}(u)$.

Separable case. Given that u is nonzero, the kernel of the A-linear map $\mathbb{E}(u)$ is a torsion A-module. Let $a \in A$ such that $a \cdot \ker \mathbb{E}(u) = 0$. For all elements $z \in \overline{K}$, we then have the following implication: if $u(z) = 0$, then $\phi_a(z) = 0$. Since u is separable, this implies that u right-divides ϕ_a, from which we deduce that a annihilates $\operatorname{coker} \mathbb{M}(u)$ as well. Applying successively the right exact functor $- \otimes_A A/aA$ and the left exact functor $\operatorname{Hom}_K(-, \overline{K})$ to the exact sequence of A_K-modules

$$0 \to \mathbb{M}(\psi) \to \mathbb{M}(\phi) \to \operatorname{coker} \mathbb{M}(u) \to 0,$$

we get the following exact sequence of $A_{\overline{K}}$-modules

$$0 \to \big(\operatorname{coker}\mathbb{M}(u)\big)^* \otimes_K \overline{K} \to \mathbb{M}_a(\phi)^* \otimes_K \overline{K} \to \mathbb{M}_a(\psi)^* \otimes_K \overline{K}.$$

This shows that

$$\big(\operatorname{coker}\mathbb{M}(u)\big)^* \otimes_K \overline{K} \simeq \ker\big(\mathbb{M}_a(u)^*\big) \otimes_K \overline{K} \simeq \ker\big(\mathbb{M}_a(u)^* \otimes_K \overline{K}\big).$$

From Theorem 2.5, we then derive the following isomorphisms of $A_{\overline{K}}$-modules:

$$\begin{aligned}\big(\operatorname{coker}\mathbb{M}(u)\big)^* \otimes_K \overline{K} &\simeq \ker\big(\mathbb{E}_a(u) \otimes_{\mathbb{F}_q} \overline{K}\big)\\ &= \ker\big(\mathbb{E}(u) \otimes_{\mathbb{F}_q} \overline{K}\big)\\ &\simeq \ker\mathbb{E}(u) \otimes_{\mathbb{F}_q} \overline{K}.\end{aligned}$$

Consequently, u being separable, we find that

$$\mathfrak{n}(u) = \chi_A\big(\ker\mathbb{E}(u)\big) = \chi_{A_K}\big((\operatorname{coker}\mathbb{M}(u))^*\big).$$

Using finally Lemma 2.4, we end up with $\mathfrak{n}(u) = \chi_{A_K}(\operatorname{coker}\mathbb{M}(u)) = \mathfrak{det}\,\mathbb{M}(u)$, proving the theorem. □

An interesting consequence of Theorem 3.2 is a compatibility result between norms of isogenies and restrictions of Drinfeld modules (see §1.1.4), which will be particularly useful to us when Drinfeld A-modules are restricted to $A' = \mathbb{F}_q[T]$.

Corollary 3.3. *Let $\gamma' : A' \to K$ be a second base for Drinfeld modules satisfying the assumptions of §1.1, coming together with an injective homomorphism of rings $f : A' \to A$ such that $\gamma = \gamma' \circ f$. Let $\phi, \psi : A \to K\{\tau\}$ be two Drinfeld A-modules and let $u : \phi \to \psi$ be a morphism. Then*

$$\mathfrak{n}\big(f^*u\big) = N_{A/A'}\big(\mathfrak{n}(u)\big)$$

where $N_{A/A'} : A \to A'$ is the norm map from A to A' via *f.*

Proof. Let $\mathfrak{p}$ be a prime ideal of A'_K, and let $A'_{K,\mathfrak{p}}$ be the completion of A'_K at $\mathfrak{p}$. Write $A_{K,\mathfrak{p}} = A'_{K,\mathfrak{p}} \otimes_{A'_K} A_K$, $\mathbb{M}(\phi)_\mathfrak{p} = A'_{K,\mathfrak{p}} \otimes_{A'_K} \mathbb{M}(\phi)$, and $\mathbb{M}(\psi)_\mathfrak{p} = A'_{K,\mathfrak{p}} \otimes_{A'_K} \mathbb{M}(\psi)$. Since $A_{K,\mathfrak{p}}$ is a product of local rings, the module $\mathbb{M}(\phi)_\mathfrak{p}$ is free over $A_{K,\mathfrak{p}}$. We pick a basis $\mathcal{B}_\phi = (e_{\phi,i})_{1\leqslant i\leqslant r}$ of it, together with a basis $\mathcal{B} = (a_m)_{1\leqslant m\leqslant n}$ of $A_{K,\mathfrak{p}}$ over $A'_{K,\mathfrak{p}}$. Note that the family $\mathcal{B}'_\phi = (a_m \cdot e_{\phi,i})_{1\leqslant i\leqslant r, 1\leqslant m\leqslant n}$ is a $A'_{K,\mathfrak{p}}$-basis of $\mathbb{M}(\phi)_\mathfrak{p} = \mathbb{M}(f^*\phi)_\mathfrak{p}$. We define similarly $\mathcal{B}_\psi$ and $\mathcal{B}'_\psi$. Let $C = (c_{ij})_{1\leqslant i,j\leqslant r}$ be the matrix of $\mathbb{M}(u)$ with respect to the bases $\mathcal{B}_\psi$ and $\mathcal{B}_\phi$ and, for $a \in A'_{K,\mathfrak{p}}$, let $M(a) \in (A'_{K,\mathfrak{p}})^{n\times n}$ be the matrix of the multiplication by a over $A_{K,\mathfrak{p}}$. The matrix of f^*u in the bases $\mathcal{B}'_\psi$ and $\mathcal{B}'_\phi$ is the block matrix

$$D = \begin{pmatrix} M(c_{1,1}) & \cdots & M(c_{1,r}) \\ \vdots & & \vdots \\ M(c_{r,1}) & \cdots & M(c_{r,r}) \end{pmatrix}$$

The main result of [Siloo] implies that $\det D = N_{A_{K,\mathfrak{p}}/A'_{K,\mathfrak{p}}}(\det C)$. The proposition then follows from Theorem 3.2. □

Algorithm 5: IsogenyNorm

Input: An isogeny $u : \phi \to \psi$ encoded by its defining Ore polynomial
Output: The norm of u

1 Compute $M = \text{MotiveMatrix}(u)$
2 Return the ideal generated by determinant of M

3.2 Algorithms: the case of $\mathbb{P}^1$

Let $A = \mathbb{F}_q[T]$ as in §2.2. Theorem 3.2 readily translates to an algorithm for computing the norm of an isogeny between Drinfeld modules; this is Algorithm 5.

Theorem 3.4. *Let ϕ and ψ be two Drinfeld $\mathbb{F}_q[T]$-modules of rank r and let $u : \phi \to \psi$ be an isogeny of τ-degree n. Algorithm 5 computes the norm of u for a cost of $O(n^2 + r^2)$ applications of the Frobenius endomorphism of K and $O^{\sim}(n^2 + nr^{\omega-1} + r^{\omega})$ operations in K.*

Proof. Per Lemma 2.14, the cost of computing the matrix of $\mathbb{M}(u)$ is $O(n^2+r^2)$ applications of the Frobenius endomorphism, and $O(n^2+r^2)$ operations in K. Besides, this matrix has size r and its entries have degrees all less than $1 + \frac{n}{r}$ (Lemma 2.10, which is also valid for isogenies). Therefore, using the algorithmic primitives of §1.2.2, computing its determinant requires $O^{\sim}((n+r)r^{\omega-1})$ operations in K. □

When K is a finite field, one can speed up Algorithm 5 using the optimized primitives of §1.2.3 for manipulating Ore polynomials, as for the endomorphism case. Precisely, we have the following.

Theorem 3.5. *If K is a finite field of degree d over $\mathbb{F}_q$, Algorithm 5 computes the norm of the isogeny u for a cost of*

$$O^{\sim}(d \log^2 q) + O^{\bullet}\left(\left(\mathrm{SM}^{\geqslant 1}(n, d) + ndr + n \min(d, r) r^{\omega-1} + dr^{\omega}\right) \cdot \log q\right)$$

bit operations.

Proof. Per the first part of the proof of Theorem 2.16, the computation of $\mathbb{M}(u)$ requires

$$O^{\sim}(d \log^2 q) + O^{\bullet}\left(\left(\mathrm{SM}^{\geqslant 1}(n, d) + dr(n + r)\right) \log q\right)$$

bit operations. Then, for the computation of the determinant, we distinguish between two cases. If $d \leqslant r$, we keep on using the algorithms of [GJV03, JV05], for a cost of $O^{\sim}(nr^{\omega-1}+r^{\omega})$ operations in K, that is $O^{\sim}(ndr^{\omega-1}+dr^{\omega})$ operations in $\mathbb{F}_q$. On the contrary, when $d \geqslant r$, we use Lemma 1.14, performing then $O^{\bullet}(nr^{\omega} + dr^{\omega})$ operations in $\mathbb{F}_q$. Putting all together, and remembering that an operation in $\mathbb{F}_q$ corresponds to $O^{\sim}(\log q)$ bit operations, we get the theorem. □

Remark 3.6. When u is an endomorphism, the norm can be computed as the constant coefficient of the characteristic polynomial of u, up to a sign. We notice that the algorithms of the present subsection in some cases run faster than those of §2.2. This is because we compute the determinant of the matrix of $\mathbb{M}(u)$ instead of its whole characteristic polynomial. However, we stress that the asymptotic costs of computing the characteristic polynomial and the norm of an endomorphism

may be equal. This owes to the fact that in some cases, computing the characteristic polynomial of a matrix, or computing its determinant, both reduces to matrix multiplication.

Remark 3.7. In the special case where $u = F_\phi$ is the Frobenius endomorphism, the norm is given by a simple closed-formula (see [Gek08, Theorem 2.11] and [Pap23, Theorem 2.4.7]), namely

$$\mathfrak{n}(F_\phi) = (-1)^{rd-r-d} N_{K/\mathbb{F}_q}(\Delta)^{-1} \mathfrak{p}^{\frac{d}{\deg(\mathfrak{p})}}, \tag{5}$$

where Δ is the leading coefficient of ϕ_T. Computing the Frobenius norm using Equation (5) costs $O^{\sim}(d \log^2 q) + O^{\bullet}(d \log q)$ bit operations [MS19, Proposition 3]. Noticing that the *Frobenius norm* is a degree d polynomial in $\mathbb{F}_q[T]$, this complexity is essentially optimal with respect to d, and asymptotically better than other algorithms mentioned in this paper (see also Appendix A).

3.3 Algorithms: the case of a general curve

When A is arbitrary, determining the norm of an isogeny $u : \phi \to \psi$ becomes more complex due to the nonfreeness of the motives $\mathbb{M}(\phi)$ and $\mathbb{M}(\psi)$ in general. This necessitates working with arbitrary torsion-free modules over Dedekind rings. While this approach appears viable, we will follow an alternative strategy that simplifies the general scenario by reducing the computation to the previously addressed case of $\mathbb{F}_q[T]$.

From now on, we assume for simplicity that A is presented as

$$A = \mathbb{F}_q[X, Y]/P(X, Y)$$

and that $\deg(x) > \deg(y)$, where x and y denote the images in A of X and Y respectively. Let $\phi, \psi : A \to K\{\tau\}$ be two Drinfeld modules of rank r, and let $u : \phi \to \psi$ be an isogeny between them. We consider a new variable Λ and form the polynomial rings $K[\Lambda]$ and $A_K[\Lambda]$. We set

$$\mathbb{M}(\phi)[\Lambda] = A_K[\Lambda] \otimes_{A_K} \mathbb{M}(\phi)$$

and endow it with the structure of $K[T, \Lambda]$-module inherited from its structure of $A_K[\Lambda]$-module through the ring homomorphism

$$f : K[T, \Lambda] \to A_K[\Lambda], \quad T \mapsto x + \Lambda \cdot y, \ \Lambda \mapsto \Lambda.$$

Similarly, we define $\mathbb{M}(\psi)[\Lambda]$ and endow it with a structure of $K[T, \Lambda]$-module.

The assumption $\deg(x) > \deg(y)$ ensures that $\phi_x + \Lambda \cdot \phi_y$ is an Ore polynomial of degree $r \cdot \deg(x)$ with leading coefficient lying in K. Writing $s = r \cdot \deg(x)$, we deduce that the family $(1, \tau, \dots, \tau^{s-1})$ is a $K[T, \Lambda]$-basis of both $\mathbb{M}(\phi)[\Lambda]$ and $\mathbb{M}(\psi)[\Lambda]$. On the other hand, we observe that, after extending scalars to $A_K[\Lambda]$, the morphism $\mathbb{M}(u) : \mathbb{M}(\psi) \to \mathbb{M}(\phi)$ induces a $K[T, \Lambda]$-linear map $\mathbb{M}(u)[\Lambda] : \mathbb{M}(\psi)[\Lambda] \to \mathbb{M}(\phi)[\Lambda]$. Its determinant in the aforementioned distinguished bases is a bivariate polynomial, that we call $\delta(T, \Lambda)$. Evaluating it at $T = x + \Lambda y$, we obtain a univariate polynomial in Λ with coefficients in A_K.

Theorem 3.8. *With the above notation and hypothesis, the leading coefficient of $\delta(T, \Lambda)$ with respect to T is a nonzero constant $c \in K^\times$. Moreover, if we write*

$$\delta(x + \Lambda y, \Lambda) = \delta_0 + \delta_1 \cdot \Lambda + \cdots + \delta_n \cdot \Lambda^n \qquad (n \in \mathbb{Z}_{\geqslant 0}, \delta_i \in A_K),$$

then $c^{-1}\delta_0, \dots, c^{-1}\delta_n$ all lie in A and generate $\mathfrak{n}(u)$.

Proof. For any fixed element $\lambda \in \overline{K}$, notice that the degree of the univariate polynomial $\delta(T, \lambda)$ is equal to the τ-degree of u. Since the latter remains constant when λ varies in $\overline{K}$, so does the former. The first assertion of the theorem follows.

Set $I = \overline{K} \otimes_{Fq} \mathfrak{n}(u)$, which is an ideal of $A_{\overline{K}}$. Recall that the maximal ideals of $A_{\overline{K}}$ are all of the form

$$\mathfrak{m}_{(x_0,y_0)} = (x - x_0)A_{\overline{K}} + (y - y_0)A_{\overline{K}}$$

with $x_0, y_0 \in \overline{K}$. We write the decomposition of I into a product of prime ideals:

$$I = \mathfrak{m}_{(x_1,y_1)} \cdot \mathfrak{m}_{(x_2,y_2)} \cdots \mathfrak{m}_{(x_\ell,y_\ell)} \tag{6}$$

where ℓ is a nonnegative integer and $x_i, y_i \in \overline{K}$ for all i between 1 and ℓ.

We fix an element $\lambda \in \overline{K}$ and consider the ring homomorphism $f_\lambda : \overline{K}[T] \to A_{\overline{K}}$ defined by $T \mapsto x + \lambda y$. The map f_λ is the specialization of f at λ, and a finite morphism whose degree does not depend on λ. Let $N_\lambda : A_{\overline{K}} \to \overline{K}[T]$ denote the norm map with respect to f_λ. It follows from the decomposition (6) that $N_\lambda(I)$ is the ideal of $\overline{K}[T]$ generated by the polynomial

$$P_\lambda(T) = (T - x_1 - \lambda y_1) \cdots (T - x_\ell - \lambda y_\ell).$$

On the other hand, repeating the proof of Corollary 3.3, we find that $N_\lambda(I)$ is also the ideal generated by $\delta(T, \lambda)$. Therefore $\delta(T, \lambda) = c \cdot P_\lambda(T)$. Since this equality holds for any $\lambda \in \overline{K}$, it is safe to replace λ by the formal variable Λ. Specializing at $T = x + \Lambda y$, we obtain

$$\delta(x + \Lambda y, \Lambda) = c \cdot \prod_{i=1}^{\ell} \big((x - x_i) + \Lambda \cdot (y - y_i)\big)$$

Expanding the latter product and comparing with the definition of I, we find that I is the ideal of $A_{\overline{K}}$ generated by $\delta_0, \ldots, \delta_n$. Finally, the fact that I is defined over A implies that the pairs (x_i, y_i) are conjugated under the Galois action, which eventually shows that the $c^{-1} \cdot \delta_i$'s are in A. The theorem follows. □

Theorem 3.8 readily translates to an algorithm for computing the norm $\mathfrak{n}(u)$, namely:

1. we compute the matrix of $\mathbb{M}(u)[\Lambda]$ using Algorithm 3 (treating Λ as a formal parameter),
2. we compute the determinant $\delta(T, \Lambda)$ of this matrix and let $c \in K^\times$ be its leading coefficient with respect to T,
3. we write
$$c^{-1} \cdot \delta(x + \Lambda y, \Lambda) = \delta'_0 + \delta'_1 \cdot \Lambda + \cdots + \delta'_n \cdot \Lambda^n \qquad (\delta'_i \in A_K).$$
4. we return the ideal of A generated by $\delta'_0, \ldots, \delta'_n$.

It follows from the proof of Theorem 3.8 that the degree n of $\delta(x + \Lambda y, \Lambda)$ is equal to ℓ, on the one hand, and to the τ-degree of the isogeny u, on the other hand. Unfortunately, this quantity may be large, especially when we compare it with the minimal number of generators of $\mathfrak{n}(u)$, which is at most 2 because A is a Dedeking domain.

To overcome this issue, an option could be to compute the δ'_i's one by one by using relaxed arithmetics [vdH97]: each time a new δ'_i is computed, we form the ideal I_i generated by $\delta'_0, \ldots, \delta'_i$

and stop the process when I_i has degree n; we then have the guarantee that $\mathfrak{n}(u) = I_i$ and that we have computed the ideal we were looking for. When $x_1, \dots, x_\ell$ are pairwise disjoint (which is the most favorable case), we already have $\mathfrak{n}(u) = I_1$, so that the above procedure stops very rapidly.

Another option consists in picking random elements $\lambda \in K$ and computing the evaluations $\delta(T, \lambda)$ and $c^{-1} \cdot \delta(x+\lambda y, y)$. Doing so, we obtain elements in $\mathfrak{n}(u)$ and we can hope, as above, that only a few number of them will generate the ideal. Again, this can be checked by looking at the degree of the candidate ideals.

4 The central simple algebra method

Throughout this section, we assume that K is a finite extension of $\mathbb{F}_q$ and we let d denote the degree of $K/\mathbb{F}_q$. Our aim is to design an alternative algorithm (namely the algorithm referred to as `F-CSA` in the introduction) for computing the characteristic polynomial of the Frobenius endomorphism F_ϕ of a rank r Drinfeld A-module ϕ. We recall that, by definition, F_ϕ is the endomorphism corresponding to the Ore polynomial $\tau^d \in K\{\tau\}$.

Our algorithm is based on Theorem 4.5, which provides a new formula for the characteristic polynomial of F_ϕ by means of reduced norms in a certain central simple algebra.

4.1 The characteristic polynomial of the Frobenius as a reduced norm

Theorem 4.5, the main result of this section and stated in §4.1.2, requires a preliminary introduction on general Ore polynomials and reduced norms. This is the goal of §4.1.1.

4.1.1 General Ore polynomials and reduced norms

We first recall some standard facts about Ore polynomials[6]. Given a ring L equipped with a ring endomorphism $\theta : L \to L$, we form the ring $L[t; \theta]$ whose elements are formal expressions of the form

$$a_0 + a_1 t + \cdots + a_n t^n \quad (n \in \mathbb{Z}_{\geqslant 0},\ a_0, \dots, a_n \in L)$$

subject to the usual addition and multiplication driven by the rule $tb = \theta(b)t$ for $b \in L$. The ring $L[t; \theta]$ is the so-called ring of Ore polynomials over L twisted by θ; it is noncommutative unless θ is the identity morphism.

From this point onward, we focus on the case where L is a field, as it holds significant importance for this section. The ring $L[t; \theta]$ then shares many properties with classical polynomial rings over a field. Notably, it is equipped with a notion of degree and with an Euclidean division on the right: given two Ore polynomial $A, B \in L[t; \theta]$ with $B \neq 0$, there exist uniquely determined $Q, R \in L[t; \theta]$ such that $A = QB + R$ and $\deg R < \deg B$. As in the classical commutative case, this implies that $L[t; \theta]$ is left Euclidean, *i.e.* all left ideals of $L[t; \theta]$ are generated by one element. From this property, we derive the existence of right gcd: given $P, Q \in L[t; \theta]$, the right gcd of P and Q, denoted by $\operatorname{rgcd}(P, Q)$, is the unique monic polynomial satisfying the relation

$$L[t; \theta] \cdot P + L[t; \theta] \cdot Q = L[t; \theta] \cdot \operatorname{rgcd}(P, Q).$$

[6] For a more detailed survey on this topic, we refer to [Jac96, §I].

From now on, we assume further that θ has finite order d. This hypothesis ensures in particular that the center of $L[t;\theta]$ is large; precisely, it is the subring $F[t^d]$ where F denotes the subfield of L fixed by θ. By standard Galois theory, the extension L/F has degree d and it is Galois with cyclic Galois group generated by θ. In this situation, the field of fractions of $L[t;\theta]$ can be obtained by inverting the elements in the center, *i.e.* we have

$$\mathrm{Frac}(L[t;\theta]) = F(t^d) \otimes_{F[t^d]} L[t;\theta].$$

Besides, the latter is a central simple algebra over $F(t^d)$ [Jac96, Theorem 1.4.6]. This provides us with a reduced norm map

$$N_{\mathrm{rd}} : \quad \mathrm{Frac}(L[t;\theta]) \ \to \ F(t^d)$$

which is multiplicative and acts as the d-th power on $F(t^d)$. Let $P \in L[t;\theta]$, $P \neq 0$. We form the quotient $D_P = L[t;\theta]/L[t;\theta]P$, which is a L-vector space of dimension $\deg(P)$ with basis $(1, t, \dots, t^{\deg(P)-1})$. Since t^d is a central element in $L[t;\theta]$, the multiplication by t^d defines a L-linear endomorphism of D_P, which we denote by γ_P. Its characteristic polynomial $\pi(\gamma_P)$ is then a monic polynomial of degree $\deg(P)$.

Proposition 4.1. *For all $P \in L[t;\theta]$, $P \neq 0$, we have*

$$N_{\mathrm{rd}}(P) = N_{L/F}\big(\mathrm{lc}(P)\big) \cdot \pi(\gamma_P)(t^d)$$

where $\mathrm{lc}(P)$ *is the leading coefficient of P and $N_{L/F}$ is the norm map from L to F,* i.e. $N_{L/F}(x) = x \cdot \theta(x) \cdots \theta^{r-1}(x)$.

Proof. See [CLB17b, Lemma 2.1.15]. □

Remark 4.2. Proposition 4.1 implies in particular that $N_{\mathrm{rd}}(P)$ is a polynomial whenever $P \in L[t;\theta]$ and that $\pi(\gamma_P)$ has coefficients in F. Both of them are not immediate from the definition.

4.1.2 Main results

We come back to our setting: we assume that K is a finite extension of $\mathbb{F}_q$ of degree d and consider a Drinfeld module $\phi : A \to K\{\tau\}$ of rank r. We notice that $K\{\tau\}$ can be alternatively depicted as the ring of Ore polynomials $K[t;\mathrm{Frob}]$ where $\mathrm{Frob} : K \to K$ is the Frobenius endomorphism taking x to x^q. Recall that we have set $A_K = K \otimes_{\mathbb{F}_q} A$, and define $\theta = \mathrm{Frob} \otimes \mathrm{id}_A$, which is a ring endomorphism of A_K of order d with fixed subring A. We form the Ore algebra $A_K[t;\theta]$; it contains $K[t;\theta] \simeq K\{\tau\}$ as a subring. In particular, the elements ϕ_a ($a \in A$) naturally sit in $A_K[t;\theta]$.

We define the ideal

$$I(\phi) = \sum_{a \in A} A_K[t;\theta] \cdot (\phi_a - a).$$

In other words, $I(\phi)$ is the left ideal of $A_K[t;\theta]$ generated by the elements $(\phi_a - a)$ for a running over A.

Lemma 4.3. *We assume that A is generated as a $\mathbb{F}_q$-algebra by the elements $a_1, \dots, a_n$. Then $I(\phi)$ is generated as a left ideal of $A_K[t;\theta]$ by $\phi_{a_1} - a_1, \dots, \phi_{a_n} - a_n$.*

Proof. Let I' be the left ideal of $A_K[t;\theta]$ generated by $\phi_{a_1}-a_1, \ldots, \phi_{a_n}-a_n$. We need to prove that $I' = I(\phi)$. The inclusion $I' \subset I(\phi)$ is obvious. For the reverse inclusion, consider $\lambda \in \mathbb{F}_q$ and $a, b \in A$ such that $\phi_a - a$, $\phi_b - b \in I'$. The equalities

$$\begin{aligned} \phi_{\lambda a} - \lambda a &= \lambda \cdot (\phi_a - a) \\ \phi_{a+b} - (a+b) &= (\phi_a - a) + (\phi_b - b) \\ \phi_{ab} - ab &= \phi_a \cdot (\phi_b - b) + b \cdot (\phi_a - a) \end{aligned}$$

(recall that b is central, so it commutes with ϕ_a) show that the three elements on the left hand side belong to I' as well. This stability property eventually ensures that I' contains all elements of the form $\phi_a - a$. Hence $I(\phi) \subset I'$ as desired. □

We recall from §1.1.2 that the A-motive of ϕ, denoted by $\mathbb{M}(\phi)$, is isomorphic to $K\{\tau\}$ as a K-vector space. This gives a K-linear inclusion $\mathbb{M}(\phi) \to A_K[t;\theta]$ (mapping τ to t). We consider the composite

$$\alpha_\phi : \quad \mathbb{M}(\phi) \;\to\; A_K[t;\theta] \;\to\; A_K[t;\theta]/I(\phi).$$

Proposition 4.4. *The map α_ϕ is a A_K-linear isomorphism.*

Proof. We first check linearity. Let $\lambda \in K$, $a \in A$ and $f \in \mathbb{M}(\phi)$. By definition, we have $(\lambda \otimes a)\cdot f = \lambda f \phi_a$. Hence

$$\alpha_\phi\big((\lambda \otimes a)\cdot f\big) = \lambda f \phi_a \equiv \lambda f a \pmod{I(\phi)}.$$

Moreover a is a central element in $A_K[t;\theta]$. We conclude that $\alpha_\phi\big((\lambda \otimes a)\cdot f\big) = \lambda a f$ and linearity follows.

In order to prove that α_ϕ is an isomorphism, we observe that $A_K[t;\theta] \simeq K\{\tau\} \otimes_{\mathbb{F}_q} A$ and we define the K-linear map $\beta_\phi : A_K[t;\theta] \to K\{\tau\}$ (as sets, $K\{\tau\} = \mathbb{M}(\phi)$) that takes $f \otimes a$ to $f\phi_a$ (for $f \in K\{\tau\}$ and $a \in A$). We claim that β_ϕ vanishes on $I(\phi)$. Indeed, for $a, b \in A$ and $g \in K\{\tau\}$, we have

$$\begin{aligned} \beta_\phi\big((g \otimes b)\cdot(\phi_a \otimes 1 - 1 \otimes a)\big) &= \beta_\phi(g\phi_a \otimes b - g \otimes ab) \\ &= g\phi_a\phi_b - g\phi_{ab} = 0. \end{aligned}$$

Consequently, β_ϕ induces a mapping $\bar\beta_\phi : A_K[t;\theta]/I(\phi) \to \mathbb{M}(\phi)$. It is now formal to check that $\bar\beta_\phi$ is a left and right inverse of α_ϕ, showing that α_ϕ is an isomorphism. □

We write $\mathrm{Frac}(A_K)$ for the field of fractions of A_K. The morphism θ extends to a ring endomorphism of $\mathrm{Frac}(A_K)$ that, in a slight abuse of notation, we continue to denote by θ. On $\mathrm{Frac}(A_K)$, θ has order d and its fixed subfield is $\mathrm{Frac}(A)$. We consider the Ore polynomial ring $\mathrm{Frac}(A_K)[t;\theta]$. By what we have seen previously, its center is $\mathrm{Frac}(A)[t^d]$ and there is a reduced norm map

$$N_{\mathrm{rd}} : \quad \mathrm{Frac}(A_K)[t;\theta] \;\to\; \mathrm{Frac}(A)[t^d].$$

We define $I_0(\phi) = \mathrm{Frac}(A_K) \otimes_{A_K} I(\phi)$; it is a left ideal of $\mathrm{Frac}(A_K)[t;\theta]$. Since the latter is a principal ideal domain, $I_0(\phi)$ is generated by a unique element $g(\phi)$, which we assume to be monic. Concretely $g(\phi)$ is the right gcd of the elements $(\phi_a - a)$ when a varies in A. After Lemma 4.3, we even have $g(\phi) = \mathrm{rgcd}\big(\phi_{a_1}-a_1, \ldots, \phi_{a_n}-a_n\big)$ as soon as $a_1, \ldots, a_n$ generate A as an $\mathbb{F}_q$-algebra.

Theorem 4.5. *We keep the previous notation and assumptions. Let F_ϕ be the Frobenius endomorphism of ϕ and let $\pi(F_\phi)$ be its monic characteristic polynomial. Then*

$$\pi(F_\phi)(t^d) = N_{\mathrm{rd}}\big(g(\phi)\big).$$

Proof. Write $\mathbb{M}_0(\phi) = \mathrm{Frac}(A_K) \otimes_{A_K} \mathbb{M}(\phi)$. On the one hand, it follows from Proposition 4.4 that α_ϕ induces an isomorphism

$$\mathbb{M}_0(\phi) \simeq \mathrm{Frac}(A_K)[t;\theta] \,/\, \mathrm{Frac}(A_K)[t;\theta]\cdot g(\phi).$$

With Proposition 4.4, we realize that $N_{\mathrm{rd}}(g(\phi))$ is equal to the characteristic polynomial of the right multiplication by t^d on $\mathbb{M}_0(\phi)$, that is

$$N_{\mathrm{rd}}\big(g(\phi)\big) = \pi\big(\,\mathrm{Frac}(A_K) \otimes_{A_K} \mathbb{M}(F_\phi)\big) = \pi\big(\mathbb{M}(F_\phi)\big).$$

We conclude by invoking Theorem 2.8. □

Remark 4.6. When $A = \mathbb{F}_q[T]$, it follows from Lemma 4.3 that $g(\phi)$ is $K(T)$-collinear to $\phi_T - T$. Therefore, its reduced norm is the reduced characteristic polynomial of ϕ_T and we recover Theorem D, stated in the introduction.

4.2 Algorithms: the case of $\mathbb{P}^1$

We move to algorithmical purpose. By Theorem 4.5, the computation of the characteristic polynomial of F_ϕ reduces to the computation of a reduced norm. On the other hand, it is a classical fact that the reduced norm of a polynomial $P \in A_K[t;\theta]$ can be computed as a usual norm. Precisely, we consider the subalgebra $A[t]$ of $A_K[t;\theta]$; it is commutative and étale over the center $A[t^d]$. Moreover $A_K[t;\theta]$ appears as a free left module of rank d over $A[t]$. Thus, there exists a norm map $N_{A_K[t;\theta]/A[t]}$ which takes a polynomial P to the determinant of the $A[t]$-linear endomorphism of

$$\begin{array}{rccc} \mu_P : & A_K[t;\theta] & \to & A_K[t;\theta] \\ & Q & \mapsto & QP. \end{array}$$

With this notation, we have

$$N_{\mathrm{rd}}(P) = N_{A_K[t;\theta]/A[t]}(P) \in A[t].$$

We now assume that $A = \mathbb{F}_q[T]$ and fix a Drinfeld module $\phi : \mathbb{F}_q[T] \to K\{\tau\}$. It follows from Lemma 4.3 that $g(\phi)$ is $K(T)$-collinear to $\phi_T - T$. Fix a basis $\mathcal{B} = (e_1, \dots, e_d)$ of K over $\mathbb{F}_q$ and observe that $\mathcal{B}$ is an $A[t]$-basis of $A_K[t;\theta]$ as well. Let M be the matrix of μ_{ϕ_T} in $\mathcal{B}$. Its entries all lie in $\mathbb{F}_q[t]$ given that ϕ_T has coefficients in K. Observing moreover that $\mu_{g(\phi)} = \mu_{\phi_T} - \mu_T = \mu_{\phi_T} - T$, we conclude that

$$\pi(F_\phi)(t^d) = \pi(M)(T) \tag{7}$$

where $\pi(M)$ is the characteristic polynomial of M. We emphasize that the two variables t and T play different roles in the two sides of the Equality (7): in the left hand side, t appears in the

variable at which the characteristic polynomial is evaluated whereas, in the right hand side, it is an internal variable appearing in the matrix M; and conversely for T.

In order to explicitly compute the matrix of μ_P for a given Ore polynomial $P \in K[t;\theta]$, we can proceed as follows. We write $P = g_0 + g_1 t + \cdots + g_n t^n$ ($g_i \in K$) and notice that

$$\mu_P = \mu_{g_0} + \mu_t \circ \mu_{g_1} + \cdots + \mu_t^n \circ \mu_{g_n}.$$

Moreover the set of equalities $e_i t = t e_i^{1/q}$ for $1 \leqslant i \leqslant d$ shows that the matrix of μ_t is $t \cdot F^{-1}$ where F is the matrix of the Frobenius endomorphism acting on K (which is $\mathbb{F}_q$-linear). These observations readily lead to Algorithm 6.

Algorithm 6: MATRIX-CSA

Input: An Ore polynomial $P = \sum_{j=0}^{n} g_j t^j \in K[t;\theta]$, a basis $\mathcal{B} = (e_1, \ldots, e_d)$ of K over $\mathbb{F}_q$
Output: The matrix of μ_P in the basis $\mathcal{B}$

1 Compute the matrix $F \in \mathbb{F}_q^{d \times d}$ of the Frobenius $K \longrightarrow K, x \mapsto x^q$ in the basis $\mathcal{B}$
2 For $0 \leqslant j \leqslant n$
3 | Compute the matrix $G_j \in \mathbb{F}_q^{d \times d}$ of the map $K \longrightarrow K, x \mapsto g_j x$ in the basis $\mathcal{B}$
4 Return $\sum_{j=0}^{n} F^{-j} \cdot G_j \cdot t^j$

Lemma 4.7. *If $\mathcal{B}$ is the working basis of $K/\mathbb{F}_q$, Algorithm 6 requires d applications of the Frobenius endomorphism and $O^{\sim}(nd^{\omega})$ operations in $\mathbb{F}_q$.*

Proof. Since $\mathcal{B}$ is the working basis, writing the coordinates of an element of K in $\mathcal{B}$ costs nothing. Therefore, computing the matrix F amounts to computing each g_i^q for $1 \leqslant i \leqslant d$. This then requires d applications of the Frobenius endomorphism. Similarly computing each G_j requires d multiplications in K, corresponding to $O^{\sim}(d^2)$ operations in $\mathbb{F}_q$. Finally, the computation on line 4 requires one inversion and $O(n)$ multiplications of $r \times r$ matrices over $\mathbb{F}_q$. The cost of this computation is then $O^{\sim}(nd^{\omega})$ operations in $\mathbb{F}_q$. □

We now have everything we need to compute the characteristic polynomial of the Frobenius endomorphism: see Algorithm 7.

Algorithm 7: FROBENIUSCHARPOLY-CSA

Input: A Drinfeld $\mathbb{F}_q[T]$-module ϕ
Output: The characteristic polynomial of the Frobenius endomorphism of ϕ

1 Compute $M =$ MATRIX-CSA(ϕ_T)
2 Compute the characteristic polynomial of M and write it $\sum_{i=0}^{d} (\sum_{j=0}^{r} \lambda_{i,j} t^{jd}) X^i$
3 Return $\sum_{j=0}^{r} (\sum_{i=0}^{d} \lambda_{i,j} T^j) X^i$

Theorem 4.8 (Variant `F-CSA`). *Algorithm 7 computes the characteristic polynomial of the Frobenius endomorphism of ϕ for a cost of $O^{\sim}(d \log^2 q) + O^{\bullet}(rd^{\omega} \log q)$ bit operations.*

Proof. Per Lemma 4.7, computing the matrix of μ_{ϕ_T} requires $O(d)$ applications of the Frobenius and $O^{\sim}(rd^\omega)$ operations in $\mathbb{F}_q$. Using Lemma 1.15, computing its characteristic polynomial can be achieved for an extra cost of $O^{\sim}(rd^\omega)$ operations in $\mathbb{F}_q$. All of this correspond to $O^{\sim}(d\log^2 q) + O^{\bullet}(rd^\omega \log q)$ bit operations in our complexity model (see §1.2.1). □

4.3 Algorithms: the case of a general curve

When A is a general curve, it is possible to follow the same strategy as before. However several simplifications that were previously applicable cannot be implemented in this case. First of all, finding $g(\phi)$ requires some computation. By Lemma 4.3, however, $g(\phi)$ can be obtained as the right gcd of a finite number of Ore polynomials, as soon as we have a finite presentation of the ring A. Fortunately, such a right gcd can be computed using a noncommutative variant of the Euclidean algorithm. Once $g(\phi)$ is known, one can compute its reduced norm using the method of §4.2: we form the matrix of the $\mathrm{Frac}(A)[t]$-linear map $\mu_{g(\phi)} : \mathrm{Frac}(A_K)[t;\theta] \to \mathrm{Frac}(A_K)[t;\theta]$, defined by $Q \mapsto Q{\cdot}g(\phi)$, and view $N_{\mathrm{rd}}(g(\phi))$ as the determinant of $\mu_{g(\phi)}$.

This approach yields a working algorithm for computing $\pi(F_\phi)$. It has nevertheless two drawbacks. First, the computation of the right gcd may be costly and have an impact on the size of the coefficients in the base ring $\mathrm{Frac}(A_K)$, which is not finite. One may gain a certain level of control by using the theory of noncommutative subresultants introduced by Li in [Li98], but this requires additional caution. The second disadvantage is that the Ore polynomial $g(\phi)$ is in general not of the form $\phi_a - a$, implying that the computation of its reduced norm no longer boils down to finding the characteristic polynomial of a matrix with entries in $\mathbb{F}_q$. Instead, we need to compute the determinant of a general matrix over $\mathrm{Frac}(A)[t]$, which can be a more costly operation.

It turns out that we can overcome these two issues by following the same strategy as in §3.3 and reducing the problem to the case of $\mathbb{F}_q[T]$. For simplicity, we assume again that A is presented as

$$A = \mathbb{F}_q[X, Y]/P(X, Y) \quad \text{with} \quad P \in \mathbb{F}_q[X, Y]$$

and that $\deg(x) > \deg(y)$ where x and y denote the images in A of the variables X and Y. We introduce a new variable Λ and the Ore polynomial ring $K[T, \Lambda][t;\theta]$ where θ acts on K *via* the Frobenius map $x \mapsto x^q$ and acts trivially on T and Λ. In this setting, we have a reduced norm map

$$N_{\mathrm{rd}} : K[T, \Lambda][t;\theta] \to \mathbb{F}_q[T, \Lambda][t^d].$$

We consider the trivariate polynomial $\varpi(T, \Lambda, t^d) = N_{\mathrm{rd}}\big(\phi_x + \Lambda{\cdot}\phi_y - T\big)$ and write

$$\varpi(x + \Lambda y, \Lambda, t^d) = \varpi_0(t^d) + \varpi_1(t^d){\cdot}\Lambda + \cdots + \varpi_n(t^d){\cdot}\Lambda^n$$

where the ϖ_i's are univariate polynomials over $\mathrm{Frac}(A)$. This gives the following theorem, which is an analogue of Theorem 3.8 and whose proof is similar.

Theorem 4.9. *We keep the previous notation and assumptions. Let F_ϕ be the Frobenius endomorphism of ϕ and let $\pi(F_\phi)$ be its monic characteristic polynomial. Then*

$$\pi(F_\phi) = \gcd(\varpi_0, \varpi_1, \ldots, \varpi_n).$$

The formula of Theorem 4.9 readily provides an algorithm for computing $\pi(F_\phi)$. This strategy is not hindered by the two aforementioned disadvantages. Moreover, as mentioned in §3.3, it may occur that $\pi(F_\phi)$ is already the gcd of the first polynomials $\varpi_0, \dots, \varpi_i$, for some $i < n$. Therefore, it can be beneficial to compute the ϖ_i's one by one (using relaxed arithmetics), determining the corresponding gcd at each step, and stopping the computation as soon as the resulting polynomial reaches degree d. As also discussed in §3.3, another option is to work with evaluations at random values $\lambda \in \overline{K}$ instead of working with the formal variable Λ.

References

[ACL22] Simon Abelard, Alain Couvreur, and Grégoire Lecerf. Efficient computation of riemann–roch spaces for plane curves with ordinary singularities. *AAECC*, 2022.

[ACLM23] David Ayotte, Xavier Caruso, Antoine Leudière, and Joseph Musleh. Drinfeld modules in SageMath. *ACM Communications in Computer Algebra*, to appear, 2023.

[And86] Greg W. Anderson. t-Motives. *Duke Mathematical Journal*, 53(2):457–502, June 1986. Publisher: Duke University Press.

[Ang94] Bruno Anglès. *Modules de Drinfeld sur les corps finis*. PhD thesis, 1994.

[BCDA22] Maxime Bombar, Alain Couvreur, and Thomas Debris-Alazard. On Codes and Learning with Errors over Function Fields. In *Advances in Cryptology – CRYPTO 2022*, Lecture Notes in Computer Science, pages 513–540. Springer Nature Switzerland, 2022.

[Car35] Leonard Carlitz. On certain functions connected with polynomials in a Galois field. *Duke Mathematical Journal*, 1(2), June 1935.

[Car18] Perlas Caranay. *Computing isogeny volcanoes of rank two Drinfeld Modules*. PhD thesis, University of Calgary, 2018.

[CGS20] Perlas Caranay, Matthew Greenberg, and Renate Scheidler. Computing modular polynomials and isogenies of rank two Drinfeld modules over finite fields. *Contemporary mathematics*, 754:283–313, 2020.

[Che40] Claude Chevalley. La Théorie du Corps de Classes. *Annals of Mathematics*, 41(2):394–418, 1940.

[CL09] Jean-Marc Couveignes and Reynald Lercier. Elliptic periods for finite fields. *Finite Fields Appl.*, 15(1):1–22, 2009.

[CL13] Jean-Marc Couveignes and Reynald Lercier. Fast construction of irreducible polynomials over finite fields. *Israel J. Math.*, 194(1):77–105, 2013.

[CLB17a] Xavier Caruso and Jérémy Le Borgne. Fast multiplication for skew polynomials. *Proceedings of the 2017 International Symposium on Symbolic and Algebraic Computation*, 2017.

[CLB17b] Xavier Caruso and Jérémy Le Borgne. A new faster algorithm for factoring skew polynomials over finite fields. *Journal of Symbolic Computation*, 79:411–443, 2017.

[CLRS22] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms, fourth edition*. MIT Press, 2022.

[Con09] Keith Conrad. History of Class Field Theory. 2009.

[DNS21] Javad Doliskani, Anand Kumar Narayana, and Éric Schost. Drinfeld modules with complex multiplication, hasse invariants and factoring polynomials over finite fields. *Journal of Symbolic Computation*, 105:199–213, 2021.

[Dri74] Vladimir G. Drinfeld. Elliptic modules. *Mathematics of the Ussr-Sbornik*, 23(4):561–592, 1974.

[DWZ22] Ran Duan, Hongxun Wu, and Renfei Zhou. Faster matrix multiplication via asymmetric hashing, 2022. Technical Report 2210.10173, arXiv.

[Eis95] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer, 1995.

[Gek91] Ernst-Ulrich Gekeler. On finite Drinfeld modules. *Journal of algebra*, 1(141):187–203, 1991.

[Gek08] Ernst-Ulrich Gekeler. Frobenius distributions of drinfeld modules over finite fields. *Transactions of the American Mathematical Society*, 4(360):1695–1721, 2008.

[GJV03] Pascal Giorgi, Claude-Pierre Jeannerod, and Gilles Villard. On the complexity of polynomial matrix computations. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, ISSAC '03, pages 135–142. Association for Computing Machinery, 2003.

[GL20] Alexandre Grishkov and Dmitry Logachev. Introduction to Anderson t-motives: a survey, August 2020. arXiv:2008.10657v3.

[Gos98] David Goss. *Basic Structures of Function Field Arithmetic*. Springer, 1998.

[GP20] Sumita Garai and Mihran Papikian. Endomorphism rings of reductions of Drinfeld modules. *Journal of Number Theory*, 212:18–39, 2020.

[Hay74] David R. Hayes. Explicit class field theory for rational function fields. *Transactions of the American Mathematical Society*, 189(0):77–91, 1974.

[Hay11] David R. Hayes. A Brief Introduction to Drinfeld Modules. In *A Brief Introduction to Drinfeld Modules*, pages 1–32. De Gruyter, June 2011.

[Hil32] David Hilbert. Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper. In David Hilbert, editor, *Gesammelte Abhandlungen: Erster Band Zahlentheorie*, pages 53–62. Springer, 1932.

[Jac96] Nathan Jacobson. *Finite-dimensional division algebras over fields*. Springer-Verlag, Berlin, 1996.

[JN19] Antoine Joux and Anand Kumar Narayanan. Drinfeld modules may not be for isogeny based cryptography, 2019. Report Number: 1329.

[JV05] Claude-Pierre Jeannerod and Gilles Villard. Asymptotically fast polynomial matrix algorithms for multivariable systems. *International Journal of Control*, 79:1359–1367, 2005.

[Kal92] Erich Kaltofen. On computing determinants of matrices without divisions. In *Proceedings of the 1992 International Symposium on Symbolic and Algebraic Computation*, ISSAC '92. Association for Computing Machinery, 1992.

[Kat73] Nicholas M. Katz. p-adic properties of modular schemes and modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 69–190. Lecture Notes in Mathematics, Vol. 350. Springer, 1973.

[Kro53] Leopold Kronecker. Über die algebraisch auflösbaren gleichungen. In K. Hensel, editor, *Leopold Kronecker's Werke, Part 4*, pages 4–11. American Mathematical Society, 1853.

[KU11] Kiran S. Kedlaya and Christopher Umans. Fast Polynomial Factorization and Modular Composition. *SIAM Journal on Computing*, 40(6):1767–1802, January 2011. Publisher: Society for Industrial and Applied Mathematics.

[KV05] Erich Kaltofen and Gilles Villard. On the complexity of computing determinants. 13(3–4):91–130, feb 2005.

[LGS20] Aude Le Gluher and Pierre-Jean Spaenlehauer. A fast randomized geometric algorithm for computing Riemann-Roch spaces. *Math. Comp.*, 89(325):2399–2433, 2020.

[Li98] Ziming Li. A subresultant theory for Ore polynomials with applications. In *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation*, pages 132–139. ACM, New York, 1998.

[LS23] Antoine Leudière and Pierre-Jean Spaenlehauer. Computing a Group Action from the Class Field Theory of Imaginary Hyperelliptic Function Fields, May 2023. arXiv:2203.06970.

[MS19] Yossef Musleh and Éric Schost. Computing the characteristic polynomial of a finite rank two Drinfeld module. In *Proceedings of the 2019 International Symposium on Symbolic and Algebraic Computation*, ISSAC '19, pages 307–314. Association for Computing Machinery, 2019.

[MS23] Yossef Musleh and Éric Schost. Computing the characteristic polynomial of endomorphisms of a finite Drinfeld module using crystalline cohomology. 2023. arXiv:2302.08611.

[Nar18] Anand Kumar Narayanan. Polynomial factorization over finite fields by computing Euler–Poincaré characteristics of Drinfeld modules. *Finite Fields and Their Applications*, 54:335–365, 2018.

[NP21] Vincent Neiger and Clément Pernet. Deterministic computation of the characteristic polynomial in the time of matrix multiplication. *Journal of Complexity*, 67:101572, 2021.

[Pap23] Mihran Papikian. *Drinfeld Modules*, volume 296 of *Graduate Texts in Mathematics*. Springer International Publishing, 2023.

[Poo22] Bjorn Poonen. Introduction to Drinfeld modules. *Arithmetic, Geometry, Cryptography, and Coding Theory*, 779, January 2022.

[PS07] Clément. Pernet and Arne Storjohann. Faster algorithms for the characteristic polynomial. In *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation*, ISSAC '07, pages 307–314. Association for Computing Machinery, 2007.

[Ros02] Michael Rosen. *Number Theory in Function Fields*, volume 210 of *Graduate Texts in Mathematics*. Springer, 2002.

[Sca01] Thomas Scanlon. Public Key Cryptosystems Based on Drinfeld Modules Are Insecure. *Journal of Cryptology*, 14(4):225–230, September 2001.

[Sil00] John R. Silvester. Determinants of block matrices. *The Mathematical Gazette*, 84(501):460–467, 2000.

[Tae09] Lenny Taelman. Special L-values of t-motives: a conjecture. (16):2957–2977, 2009.

[Tak14] Teiji Takagi. *Collected Papers*. Springer Collected Works in Mathematics. Springer Tokyo, 2 edition, November 2014.

[vdH97] Joris van der Hoeven. Lazy multiplication of formal power series. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, ISSAC '97, pages 17–20. Association for Computing Machinery, 1997.

[vdH04] Gert Jan van der Heiden. Weil pairing for Drinfeld modules. *Monatshefte für Mathematik*, 143:115–143, 2004.

[VS06] Gabriel Daniel Villa Salvador. *Topics in the Theory of Algebraic Function Fields*. Mathematics: Theory & Applications. Birkhäuser, 2006.

[vzGG13] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, third edition, 2013.

A Review of existing algorithms

In all this Section, ϕ is a rank r Drinfeld $\mathbb{F}_q[T]$-module over a field K. The field K may not be finite, but when it is, its degree over $\mathbb{F}_q$ is denoted by d. The function field characteristic of K is an ideal $\mathfrak{p}$ of $\mathbb{F}_q[T]$ whose degree is denoted by m. We consider an endomorphism or an isogeny u whose degree as an Ore polynomial is n. We let ω be a feasible exponent for matrix multiplication and Ω be a feasible exponent for matrix characteristic polynomial computation.

We underline that any algorithm the computes the characteristic polynomial of an endomorphism computes its norm as a byproduct. Furthermore, the Frobenius norm can be computed in $O^{\sim}(d\log^2 q) + O^{\bullet}(d\log q)$ bit operations (see Remark 3.7), which is strictly better than any other algorithm mentioned in this paper.

In all the tables below, the term $O^{\sim}(d\log^2 q)$ which appears in blue on many lines always correspond to the precompution of the image of a generator of $K/\mathbb{F}_q$ by the Frobenius endomorphism (see §1.2.1).

Table 1: Algorithms for the characteristic polynomial of the Frobenius endomorphism in rank two

Algorithm	*Bit complexity*	*Constraints*
[Gek08] [1]	$O^{\bullet}(d^3\log q) + O^{\sim}(d\log^2 q)$	
[MS19, § 5] [2]	$O^{\bullet}(d^{1.885}\log q) + O^{\sim}(d\log^2 q)$	$m = d$
[MS19, § 7] [3]	$O^{\bullet}(d^2\log^2 q)$	
[MS19, § 6] [4]	$O^{\bullet}(d^2\log q) + O^{\sim}(d\log^2 q)$	
[GP20, § 5.1] ♯	$O^{\sim}(d^3\log q)$	$m = d$
[DNS21, Th 1] [5]	$O^{\bullet}(d^{1.5}\log q) + O^{\sim}(d\log^2 q)$	$m = d$
[MS23, Th. 1(1)] ♯	$O^{\bullet}(d^{1.5}\log q) + O^{\sim}(d\log^2 q)$	$m = d$
[MS23, Th. 1(2)] ♯	$O^{\bullet}\left(\frac{d^2}{\sqrt{m}}\log q\right) + O^{\sim}(d\log^2 q)$	$m < d$
[MS23, Th. 2(1)] ♭	$O^{\bullet}(d^2\frac{d+m}{m}\log q) + O^{\sim}(d\log^2 q)$	
[MS23, Th. 2(2)] ♭	$O^{\bullet}(\mathrm{SM}^{\geqslant 1}(d,d)\log q) + O^{\sim}(d\log^2 q)$	
Cor. 2.18, `F-MFF` ♯	$O^{\bullet}(\mathrm{SM}^{\geqslant 1}(d,d)\log q) + O^{\sim}(d\log^2 q)$	
Th. 2.19, `F-MKU` ♯	$O^{\bullet}(d^2\log q) + O^{\sim}(d\log^2 q)$	
Th. 4.8, `F-CSA` ♯	$O^{\bullet}(d^{\omega}\log q) + O^{\sim}(d\log^2 q)$	

[1] Deterministic algorithm by Gekeler. The Frobenius norm is directly computed, and the Frobenius trace is computed as the solution of a linear system. See also [MS19, § 4.1].

[2] Monte-Carlo algorithm by Musleh and Schost. The algorithm is inspired by ideas from ideas of Narayanan in [Nar18, § 3.1], as well as Copersmith's block Wiedemann algorithm.

[3] Monte-Carlo algorithm by Musleh and Schost. The algorithm computes the Frobenius norm, and the minimal polynomial of ϕ_T using a Monte-Carlo algorithm. After, it recovers F_ϕ by solving a Hankel system.

[4] Deterministic algorithm by Musleh and Schost. Drinfeld analogue of Schoof's algorithm for elliptic curves.

[5] Deterministic Algorithm by Doliskani, Narayanan and Schost, introduced to factorize polynomials in $\mathbb{F}_q[T]$. The algorithm actually computes the *Hasse invariant* of the Drinfeld module, from which the Frobenius trace is recovered thanks to the assumption that $m = d$. The algorithm gets inspiration from elliptic curve algorithms and computes the Hasse invariant as an element in a recursive sequence discovered by Gekeler. See [DNS21, § 2.1].

♯ Algorithm described in Table 2.

♭ Algorithm described in Table 3.

Table 2: Algorithms for the characteristic polynomial of the Frobenius endomorphism in any rank r

Algorithm	*Bit complexity*	*Constraints*
[GP20, § 5.1] [1]	$O^{\sim}(r^2d^3\log q)$	$m = d$
[MS23, Th. 1(1)] [2]	$O^{\bullet}(r^{\omega}d^{\frac{3}{2}}\log q) + O^{\sim}(d\log^2 q)$	$m = d$
[MS23, Th. 1(2)] [2]	$O^{\bullet}\left(\left(\frac{r^{\Omega}}{m} + \frac{r^{\omega}}{\sqrt{m}}\right)d^2\log q\right) + O^{\sim}(d\log^2 q)$	$m < d$
[MS23, Th. 2(1)] [♭]	$O^{\bullet}\left(\left(r^{\Omega} + \min(dr^2, (d+r)r^{\omega-1})\right)\frac{d(d+m)}{m}\log q\right) + O^{\sim}(d\log^2 q)$	
[MS23, Th. 2(2)] [♭]	$O^{\bullet}\left(\left(r^{\Omega}\frac{d(d+m)}{m} + r\cdot\mathrm{SM}^{\geqslant 1}(d+r,d)\right)\log q\right) + O^{\sim}(d\log^2 q)$	
Cor. 2.18, `F-MFF` [3]	$O^{\bullet}((\mathrm{SM}^{\geqslant 1}(d,d) + rd^2 + dr^{\omega})\log q) + O^{\sim}(d\log^2 q)$	
Th. 2.19, `F-MKU` [4]	$O^{\bullet}((d^2r^{\omega-1} + dr^{\omega})\log q) + O^{\sim}(d\log^2 q)$	
Th. 4.8, `F-CSA` [5]	$O^{\bullet}(rd^{\omega}\log q) + O^{\sim}(d\log^2 q)$	

[1] Deterministic algorithm by Garai and Papikian. With Proposition 2.12 and the hypothesis $m = d$, the coefficients of F_{ϕ} are uniquely determined by their images under $\gamma : \mathbb{F}_q[T] \to K$. The Frobenius norm is computed using Equation (5) and the other coefficients are recursively computed.

[2] Two deterministic algorithms by Musleh and Schost. The characteristic polynomial of any endomorphism is the characteristic polynomial of its action on the crystaline cohomology. In the case of the Frobenius endomorphism, algorithmic speed-ups are possible using a *baby step-giant step* method.

[3] Probabilistic algorithm. The characteristic polynomial of the Frobenius endomorphism is the characteristic polynomial of its action on the motive.

[4] Probabilistic algorithm. The characteristic polynomial of the Frobenius endomorphism is the characteristic polynomial of its action on the motive. The corresponding matrix is recursively computed using a *square and multiply*-like procedure.

[5] Probabilistic algorithm. The characteristic polynomial of the Frobenius endomorphism is interpreted as the reduced characteristic polynomial of ϕ_T in the central simple $\mathbb{F}_q[\tau^d]$-algebra $K\{\tau\}$.

[♭] Algorithm described in Table 3.

Table 3: Algorithms for characteristic polynomials of degree n endomorphisms, in any rank r, over a finite field of degree d over $\mathbb{F}_q$

Algorithm	*Bit complexity*	*Constraints*
[MS23, Th. 2(1)] [1]	$O^{\bullet}\left(\left(r^{\Omega} + \min(nr^2, (n+r)r^{\omega-1})\right)\frac{d(n+m)}{m}\log q\right) + O^{\sim}(d\log^2 q)$	
[MS23, Th. 2(2)] [1]	$O^{\bullet}\left(\left(r^{\Omega}\frac{d(n+m)}{m} + r\mathrm{SM}^{\geqslant 1}(n+r,d)\right)\log q\right) + O^{\sim}(d\log^2 q)$	
Th. 2.16, `F-MFF` [2]	$O^{\bullet}((\mathrm{SM}^{\geqslant 1}(n,d) + ndr + nr^{\omega} + dr^{\omega})\log q) + O^{\sim}(d\log^2 q)$	

[1] Two deterministic algorithms by Musleh and Schost. The characteristic polynomial of any endomorphism is the characteristic polynomial of its action on the crystalline cohomology of the Drinfeld module.

[2] Probabilistic algorithm. The characteristic polynomial of any endomorphism is the characteristic polynomial of its action on the motive of the Drinfeld module.

Table 4: Algorithms for characteristic polynomials of degree n endomorphisms, in any rank r, over a generic field

Algorithm	*Operations in the base field & Frobenius applications*	*Constraints*
Th. 2.15 [1]	$O^{\sim}(n^2 + (n+r)r^{\Omega-1})$ & $O(n^2 + r^2)$	

[1] Probabilistic algorithm. The characteristic polynomial of any endomorphism is the characteristic polynomial of its action on the motive of the Drinfeld module.

Table 5: Algorithms for computing norms of degree n isogenies, in any rank r, over a finite field of degree d over $\mathbb{F}_q$

Algorithm	*Bit complexity*	*Constraints*
Th. 3.5 [1]	$O^\bullet\big(\big(\mathrm{SM}^{\geqslant 1}(n,d)+ndr+n\min(d,r)r^{\omega-1}+dr^{\omega}\big)\log q\big)$ + $O^{\sim}(d\log^2 q)$	
See also Table 3.		

[1] Probabilistic algorithm. The norm of any isogeny is the determinant of the motivic application associated to the isogeny.

Table 6: Algorithms for computing norms of degree n isogenies, in any rank r over a finite field of degree d over $\mathbb{F}_q$

Algorithm	*Operations in the base field & Frobenius applications*	*Constraints*
Th. 3.4 [1]	$O^{\sim}(n^2+(n+r)r^{\omega-1})$ & $O(n^2+r^2)$	

[1] Probabilistic algorithm. The norm of any isogeny is the determinant of the motivic application associated to the isogeny.