Computing submodules of points of general Drinfeld modules over finite fields

Antoine Leudière, Renate Scheidler

University of Calgary

 2026

Today

Drinfeld modules

"Function field analogues of elliptic curves."

Fast algorithm

Computing kernels of morphisms of Drinfeld modules. This includes:

- Isogeny kernels (*invariant factors* and a *Frobenius decomposition*).
- Module of rational points (*invariant factors* and a *Frobenius decomposition*).
- Torsion spaces (bases).

Why Drinfeld modules?

What is the role of Drinfeld modules?

Arithmetics of function fields, geometric Langlands program, etc.

Practical applications

- ~~Isogeny-based cryptography.~~
- Computer algebra (Doliskani, Narayanan, Schost).
- Coding theory (Bastioni, Darwish, Micheli, Papikian...).
- Cryptanalysis of code-based PQC (Bombar, Couvreur, Debris-Alazard).

Important analogies

Characteristic zero	**Positive characteristic**
$\mathbb{Z}$	$\mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
Number fields	Function fields
$\mathbb{R}$	$\mathbb{R}_\infty = \mathbb{F}_q((1/T))$
$\mathbb{C}$	$\mathbb{C}_\infty =$ completion of $\overline{\mathbb{R}_\infty}$
Elliptic curves	**Drinfeld modules**
$\mathbb{Z}$-module of points	$\mathbb{F}_q[T]$-module of points
Isogenies, endomorphisms	Isogenies, endomorphisms

But...

- Research on computational aspects of Drinfeld modules is far behind its counterpart for elliptic curves!
- We must go beyond these analogies to find fast algorithms.

Important analogies

Characteristic zero	**Positive characteristic**
$\mathbb{Z}$	$\mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
Number fields	Function fields
$\mathbb{R}$	$\mathbb{R}_\infty = \mathbb{F}_q((1/T))$
$\mathbb{C}$	$\mathbb{C}_\infty$ = completion of $\overline{\mathbb{R}_\infty}$
Elliptic curves	**Drinfeld modules**
$\mathbb{Z}$-module of points	$\mathbb{F}_q[T]$-module of points
Isogenies, endomorphisms	Isogenies, endomorphisms

But...

- Research on computational aspects of Drinfeld modules is far behind its counterpart for elliptic curves!
- We must go beyond these analogies to find fast algorithms.

Main result

Let $u : \phi \to \psi$ be a morphism of Drinfeld modules over a finite field K.

Invariant factors

There exist polynomials $d_1, \dots, d_\ell \in \mathbb{F}_q[T]$ such that

$$\begin{cases} \ker(\phi(u)) \simeq \mathbb{F}_q[T]/(d_1) \times \cdots \times \mathbb{F}_q[T]/(d_\ell), \\ d_1 | \cdots | d_\ell. \end{cases}$$

Frobenius decomposition

There exist (not necessarily unique) K-rational points $x_1, \dots, x_\ell \in \phi(K)$ such that

$$\begin{cases} \ker(\phi(u)) = (\mathbb{F}_q[T] \cdot x_1) \oplus \cdots \oplus (\mathbb{F}_q[T] \cdot x_\ell), \\ \mathbb{F}_q[T] \cdot x_i \simeq \mathbb{F}_q[T]/(d_i), \quad \forall 1 \leqslant i \leqslant \ell. \end{cases}$$

Main result

Fast algorithm to compute $(d_1, \dots, d_\ell)$ and $(x_1, \dots, x_\ell)$.

Previous state of the art

The **product** of the invariant factors is analogue to the *number of points*.

For an isogeny φ of elliptic curves, there exist $d_1, \dots, d_\ell \in \mathbb{Z}$ such that

$$\ker(\varphi) = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_\ell\mathbb{Z}.$$

Then:

$$\#\ker(\varphi) = |d_1 \cdots d_\ell|.$$

For Drinfeld modules, efficient algorithms for:

- *Characteristic polynomials of endomorphisms.*
- *Norms of isogenies.*

[Musleh, Schost, 2023] [Caruso, L. 2024].
Techniques based on *crystalline cohomology* or *Anderson motives*.

Introduction

Background

Our algorithm

Ore polynomials

Fix fields $K/\mathbb{F}_q$ and for all $n \in \mathbb{Z}_{\geqslant 0}$:

$$\begin{array}{rccc} \tau^n : & \overline{K} & \to & \overline{K} \\ & x & \mapsto & x^{q^n}. \end{array}$$

Definition (Ore polynomials)

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

Properties of $K\{\tau\}$

- Ring for addition and composition of endomorphisms.
- Noncommutative: for $\lambda \in K$, $\tau^n \lambda = \lambda^{q^n} \tau^n$.
- Notion of τ-degree.
- Left-euclidean: for any $A, B \in K\{\tau\}$, there exist $Q, R \in K\{\tau\}$ such that $A = QB + R$ and $\deg_\tau(R) < \deg_\tau(B)$.

Drinfeld modules and their points

Definition (almost): Drinfeld module

A *Drinfeld $\mathbb{F}_q[T]$-module over K* is a homomorphism of $\mathbb{F}_q$-algebras

$$\begin{array}{rccc} \phi: & \mathbb{F}_q[T] & \to & K\{\tau\} \\ & a & \mapsto & \phi_a. \end{array}$$

Important details

- A Drinfeld module is **not** a module!
- ϕ is uniquely determined by ϕ_T.

Definition: module of points

The $\mathbb{F}_q[T]$-*module of K-points*, denoted by $\phi(K)$, is given by:

$$\begin{array}{ccc} \mathbb{F}_q[T] \times K & \to & K \\ (a, z) & \mapsto & \phi_a(z). \end{array}$$

Morphisms of Drinfeld modules and their kernels

Morphisms, isogenies

A *morphism* $u : \phi \to \psi$ is an Ore polynomial $u \in K\{\tau\}$ such that

$$\forall a \in \mathbb{F}_q[T], \qquad u\phi_a = \psi_a u.$$

An *isogeny* is a nonzero morphism.

The action of morphisms on points

For a morphism

$$u : \phi \to \psi$$

we get a morphism

$$\begin{array}{rccc} \phi(u): & \phi(K) & \to & \psi(K) \\ & x & \mapsto & u(x). \end{array}$$

$\ker(\phi(u))$ is a submodule of $\phi(K)$!

Main result

Let $u : \phi \to \psi$ be a morphism of Drinfeld modules over a finite field K.

Invariant factors

There exist polynomials $d_1, \dots, d_\ell \in \mathbb{F}_q[T]$ such that

$$\begin{cases} \ker(\phi(u)) \simeq \mathbb{F}_q[T]/(d_1) \times \cdots \times \mathbb{F}_q[T]/(d_\ell), \\ d_1 | \cdots | d_\ell. \end{cases}$$

Frobenius decomposition

There exist (not necessarily unique) K-rational points $x_1, \dots, x_\ell \in \phi(K)$ such that

$$\begin{cases} \ker(\phi(u)) = (\mathbb{F}_q[T] \cdot x_1) \oplus \cdots \oplus (\mathbb{F}_q[T] \cdot x_\ell), \\ \mathbb{F}_q[T] \cdot x_i \simeq \mathbb{F}_q[T]/(d_i), \quad \forall 1 \leqslant i \leqslant \ell. \end{cases}$$

Main result

Fast algorithm to compute $(d_1, \dots, d_\ell)$ and $(x_1, \dots, x_\ell)$.

Introduction

Background

Our algorithm

Preamble

Assumption for simplicity

We only present the computation of the invariant factors and of a Frobenius decomposition of $\phi(K)$.

- This corresponds to taking $u = 0$.
- The general case is a straightforward adaptation of the case $u = 0$.

Presentations of modules

How to extract information from ϕ_T to recover the decompositions of $\phi(K)$?

Definition: presentations of modules

A *presentation* of the $\mathbb{F}_q[T]$-module $\phi(K)$ is an exact sequence of $\mathbb{F}_q[T]$-modules

$$M_1 \xrightarrow{\alpha} M_2 \longrightarrow \phi(K) \longrightarrow 0.$$

Why?

1. First, $\phi(K) \simeq M_2/\operatorname{im}(\alpha) \coloneqq \operatorname{coker}(\alpha)$.
2. Second, if α is given as a diagonal matrix (relative to some given bases) with nonzero diagonal elements $d_1, \ldots, d_\ell$, then,

$$\phi(K) \simeq \mathbb{F}_q[T]/(d_1) \times \cdots \times \mathbb{F}_q[T]/(d_\ell).$$

A presentation of $\phi(K)$

Fix an $\mathbb{F}_q$-basis of K and the matrix M of $x \mapsto \phi_T(x)$ relative to this basis.

What is a matrix that contains the information of ϕ_T using polynomials?

The characteristic matrix $T\,\mathrm{Id} - M$ of M!

$$\mathbb{F}_q[T] \otimes_{\mathbb{F}_q} K \xrightarrow{\mathrm{Char}} \mathbb{F}_q[T] \otimes_{\mathbb{F}_q} K \xrightarrow{\phi^{\otimes}} \phi(K) \longrightarrow 0,$$

$$\begin{aligned} \mathrm{Char}(a \otimes x) &\coloneqq aT \otimes x - a \otimes \phi_T(x), \\ \phi^{\otimes}(a \otimes x) &\coloneqq \phi_a(x). \end{aligned}$$

Then the matrix of Char is the $T\,\mathrm{Id} - M$, *i.e.*

$$\phi(K) \simeq \mathrm{coker}(T\,\mathrm{Id} - M).$$

Normal forms of matrices

Smith form of $T\,\mathrm{Id} - M$

$T\,\mathrm{Id} - M$ is equivalent to its *Smith normal form*:

$$\mathrm{SNF}(T\,\mathrm{Id} - M) \coloneqq \mathrm{diag}(d_1, \ldots, d_\ell, 0, \ldots) \text{ is equivalent to } M.$$

Computational efficiency: Frobenius form of M

M is similar to its *Frobenius normal form*:

$$\mathrm{FNF}(M) \coloneqq \mathrm{diag}\left(\boxed{C_{d_1}}, \ldots, \boxed{C_{d_\ell}}\right) = SMS^{-1},$$

where each block C_{d_i} is the companion matrix of d_i and some $S \in \mathrm{GL}(\mathbb{F}_q)$.

Conclusion

- Retrieve the invariant factors $d_1, \ldots, d_\ell$ of $\phi(K)$ from $\mathrm{FNF}(M)$;
- Retrieve a Frobenius decomposition of $\phi(K)$ from S^{-1}.

Algorithms and costs

Write $d \coloneqq \dim_{\mathbb{F}_q}(K)$, $r \coloneqq \deg_\tau(\phi_T)$.

Main algorithm

Compute the invariant factors and a Frobenius decomposition of $\ker(\phi(u))$ for a cost of $\widetilde{O}(dr + d\deg_\tau(u) + d^\omega)$ operations in $\mathbb{F}_q$.
Special cases:

- Set $u = 0$ to get the invariant factors and a Frobenius decomposition of $\phi(K)$.
- Set $u = \phi_a$ to get an $\mathbb{F}_q[T]/(a)$-basis of the a-torsion.

Algorithmic primitives

- Fast computation of Frobenius normal forms: [Storjohann, 1999].
- Fast arithmetic of Ore polynomials: [Caruso, Le Borgne, 2017], [Puchinger, Wachter-Zeh, 2018], [L., Scheidler, 🐜].
- Evaluating polynomials on matrices: [Storjohann, 1999].
- Manipulation of divisibility chains: [L., Scheidler, 🐜].

SageMath implementation

Drinfeld $\mathbb{F}_q[T]$-modules are in SageMath:

`https://doc.sagemath.org/html/en/reference/drinfeld_modules/index.html`

Implementation of our algorithm

- Code: `https://github.com/kryzar/research-drinfeld-submodules`
- Notebook: `https://mybinder.org/v2/gh/kryzar/research-drinfeld-submodules/HEAD`

Soon

Pull request upstream.

General Drinfeld modules

In this presentation, we have only defined Drinfeld $\mathbb{F}_q[T]$-modules!

General Drinfeld modules

One can define Drinfeld A-modules, where A is a ring of functions on a smooth plane projective curve (and some assumptions).

Problem

- A may have multiple generators (not only T), and so would ϕ!
- A is Dedekind but not necessarily a PID!

Our contribution

Compute the invariant factors of $\ker(\phi(u))$, where u is a morphism by:

- Stacking multiple characteristic matrices (presentation of $\ker(\phi(u))$).
- Computing Fitting ideals.
- Using Gröbner bases to recover the invariant factors.

Bonus result

How to find rational torsion?

Given ϕ, we can quickly compute $g_\phi \in \mathbb{F}_q[T]$ such that:

$$\text{The } a\text{-torsion is rational} \iff a \mid g_\phi.$$

(Technical assumption: ϕ_a has to be separable.)

Uses *Anderson motives*.

Reflecting on our method

Simple method with two main ingredients:

1. Computing matrices of Ore polynomials.
2. Computing Frobenius normal forms of those matrices.

Why this method works

Because we have finite $\mathbb{F}_q$-linear structures!

What about elliptic curves?

A priori, not possible for elliptic curves! ...until we get a field with one element. Instead, see generic algorithms for abelian groups (*e.g.* Sutherland, 2011).

Thank you!