Elliptic curves, Drinfeld modules, and computations

Antoine Leudière

Algebra and Number Theory seminar

March 13th, 2025

Take-home message

Drinfeld modules are to function fields what elliptic curves are to number fields

Zero characteristic	*Positive characteristic*
$\mathbb{Z}$	$\mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
$\mathbb{R}$	$\mathbb{R}_\infty = \mathbb{F}_q((\frac{1}{T}))$
$\mathbb{C}$	$\mathbb{C}_\infty =$ completion of $\overline{\mathbb{R}_\infty}$
Elliptic curves	Drinfeld modules

Elliptic curves

Why Drinfeld modules?

State of the art

Drinfeld modules basics

Computing characteristic polynomials and norms

Computing of a group action from class field theory

Elliptic curves

Why Drinfeld modules?

State of the art

Drinfeld modules basics

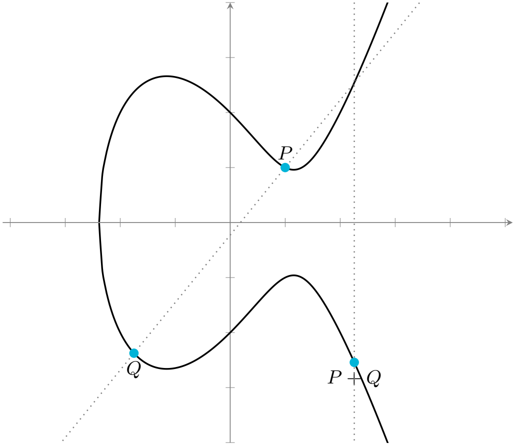
Computing characteristic polynomials and norms

Computing of a group action from class field theory

Why are elliptic curves useful?

Double nature:

- arithmetic
- geometric



Applications to cryptography

Classical cryptography

ECDH:

- Used all the time

Post-quantum cryptograph

SQIsign:

- Still in the NIST competition
- *Very* active research (e.g. IACR ePrint: 2025/271 and 2025/379)
- Short signature sizes

Applications to computer algebra

Primality testing

ECPP method:

- By Goldwasser-Killian, refined by Altkin and Morain
- Las-Vegas algorithm
- Output includes a primality certificate

Integer factorization

ECM method:

- By Hendrik Lenstra
- Las-Vegas algorithm
- Before Number Field Sieve methods, used to be the best
- Still fastest for 64 bits integers; used in CADO-NFS implementation

Theoretical applications

Class field theory

Aims at describing abelian extensions of a given field. The *Hilbert class field* (maximal abelian unramified extension) of a number field is K is the extension generated by j-invariants of elliptic curves that have complex multiplication in K.

Fermat's last theorem

Proved using a subcase of the *modularity theorem*, which states that all elliptic curves over $\mathbb{Q}$ come from a modular form.

Conjectures on elliptic curves

- BSD conjecture
- ABC conjecture

From number fields to function fields

Use geometrical tools for analogous problems.

Proved theorems in function fields

- GRH
- Langlands program for $\mathrm{GL}_n(K)$, K a function field

Algorithmic blocks

- Polynomial derivation
- Polynomial factorization
- Ore polynomials & Anderson motives (see thereafter)
- More unconditional algorithms

Broader questions

Elliptic curves	*vs*	Drinfeld modules
Integers	*vs*	Polynomials
Number fields	*vs*	Function fields
Zero characteristic	*vs*	Positive characteristic

Elliptic curves

Why Drinfeld modules?

State of the art

Drinfeld modules basics

Computing characteristic polynomials and norms

Computing of a group action from class field theory

- First examples of Drinfeld modules: Carlitz, 1935
- Formalization of Drinfeld modules: Drinfeld, 1974
- Roots in the *Kronecker Jugendtraum*, and class field theory

Cryptography:

- *2001* Scanlon (construction, cryptanalysis)
- *2003* Gillard, Leprévost, Panchishkin, Roblot (construction)
- *2006* Blackburn, Cid, Galbraith (cryptanalysis)
- *2019* Joux, Narayanan (construction, cryptanalysis)
- *2022* L., Spaenlehauer (construction)
- *2022* Wesolowski (cryptanalysis)

Reduction of problems:

- *2022* Bombar, Couvreur, Debris-Alazard

Coding theory:

- *2024* Bastioni, Darwish, Micheli

Algorithms:

- *2016* Kuhn, Pink
- *2019* Musleh, Schost
- *2020* Caranay, Greenberg, Scheidler
- *2020* Garai, Papikian
- *2023* Musleh, Schost
- *2025* Caruso, Gazda

Implementations:

- *2023* Ayotte, Caruso, L., Musleh

Computer algebra:

- *2021* Doliskani, Narayanan, Schost

PhD theses:

- *2018* Caranay
- *2023* Ayotte
- *2023* Musleh
- *2024* L.

Elliptic curves

Why Drinfeld modules?

State of the art

Drinfeld modules basics

Computing characteristic polynomials and norms

Computing of a group action from class field theory

Ingredients

- Extensions of finite fields
- Polynomials in $\mathbb{F}_q[T]$
- Ore polynomials

Ore polynomials

Fix fields

$$\mathbb{F}_q \hookrightarrow K \hookrightarrow \overline{K}$$

Fix the Frobenius

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

Let

$$K\{\tau\} = \left\{ \sum_{i=0}^{n} a_i \tau^i, \quad n \in \mathbb{Z}_{\geqslant 0}, \quad a_0, \ldots, a_n \in K \right\}.$$

Definition

$K\{\tau\}$ is the ring (for addition and composition) of *Ore polynomials* with coefficients in K.

Drinfeld modules

An $\mathbb{F}_q[T]$-*Drinfeld module* over K with rank r is (almost!) an $\mathbb{F}_q$-algebra morphism:

$$\begin{array}{rccc} \phi: & \mathbb{F}_q[T] & \to & K\{\tau\} \\ & a & \mapsto & \phi_a := a(\phi_T), \end{array}$$

where

$$\phi_T = \sum_{i=0}^{r} g_i \tau^i, \quad g_0, \ldots, g_r \in K,$$

and $r > 0$.

The action of a Drinfeld module

$\mathbb{F}_q[T]$ acts on $\overline{K}$ via ϕ:

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

Drinfeld module version of the $\mathbb{Z}$-module of points of an elliptic curve

Morphisms of Drinfeld modules

A *morphism* of Drinfeld modules $u : \phi \to \psi$ is an Ore polynomial

$$u = \sum_{i=0}^{n} u_i \tau^i \in K\{\tau\}$$

such that

$$u\phi_T = \psi_T u.$$

Two important facts:

1. Drinfeld modules are not sets
2. $K\{\tau\}$ is noncommutative, but right-euclidean for the τ-degree

Two invariants

Consider the rank 2 Drinfeld module ϕ given by $\phi_T = g_0 + g_1\tau + g_2\tau^2$. Its *j-invariant* is:

$$\mathrm{j}(\phi) = \frac{g_1^{q+1}}{g_2}.$$

Two Drinfeld modules are $\overline{K}$-isomorphic iff they have the same j-invariant.

An *isogeny* is a nonzero morphism.

If K is finite, two Drinfeld modules are K-isogenous iff they have the same *characteristic polynomial of the Frobenius endomorphism.*

Co-author

Joint-work with Xavier Caruso. To appear in *Mathematics of Computation*.

Frobenius endomorphism

Assume K is finite, fix $d = [K : \mathbb{F}_q]$.

The *Frobenius endomorphism* of ϕ is $\tau^d \in K\{\tau\}$.

The *characteristic polynomial* of ϕ is a polynomial $\chi \in \mathbb{F}_q[T][X]$, monic with degree r, such that:

$$\chi\left(\phi_T, \tau^d\right) = 0.$$

Theoretical definition of χ

1. Make $\mathbb{F}_q[T]$ act on $\overline{K}$ via ϕ.
2. Consider the action of τ^d on (almost all) the ℓ-torsion submodules, $\ell \in \mathbb{F}_q[T]$.
3. Show that these are free with rank r on $\mathbb{F}_q[T]/(\ell)$.
4. Show that the characteristic polynomial of the action of τ^d on these modules lifts to a single polynomial $\chi \in \mathbb{F}_q[T][X]$.

State of the art

2008	Gekeler	Frobenius, $r = 2$ generalized to r by Musleh
2019	Musleh, Schost	Frobenius, $r = 2$
2020	Garai, Papikian	Frobenius, $r = 2$
2023	Musleh, Schost	Any endomorphism, any r
2024	Musleh	Any endomorphism, any r

Caruso, L., 2023

- any endomorphism
- any r
- any K
- any function ring
- extends to isogeny norms

Anderson motives

$K[T]$ acts on $K\{\tau\}$ via ϕ:

$$\begin{array}{rcl} K[T] \times K\{\tau\} & \to & K\{\tau\} \\ \left(\sum_i \lambda_i T^i, f(\tau)\right) & \mapsto & \sum_i \lambda_i f(\tau) \phi_T^i \end{array}$$

Definition

This is the *Anderson motive* of ϕ, denoted by $\mathbb{M}(\phi)$

$\mathbb{M}(\phi)$ is free with rank r, and canonical basis $(1, \tau, \dots, \tau^{r-1})$.

Recursive process, using Ore Euclidean division:

$$f(\tau) = Q(\tau)\phi_T + R(\tau), \quad \deg_\tau(R) < r.$$

$$\begin{cases} \mathbb{F}_q = \mathbb{F}_2 \\ K = \mathbb{F}_4 = \{0, 1, i, i+1\} \\ \phi_T = i + \tau + \tau^2 \\ \tau^d = \tau^2 \end{cases}$$

The action of τ^2 on $\mathbb{M}(\phi)$ is given by:

$$\begin{pmatrix} T+i & i \\ T+i & T+i \end{pmatrix}.$$

The characteristic polynomial is:

$$X^2 + T^2 + T + 1,$$

hence

$$(\tau^2)^2 + \phi_T^2 + \phi_T + 1 = 0.$$

```
sage: Fq = GF(2)
sage: A.<T> = Fq[]
sage: K.<i> = Fq.extension(2)
sage: phi = DrinfeldModule(A, [i, 1, 1])
```

```
sage: matrix = phi.frobenius_endomorphism()._motive_matrix()
sage: matrix
[-T - i     -1]
[-T - i -T - i]
```

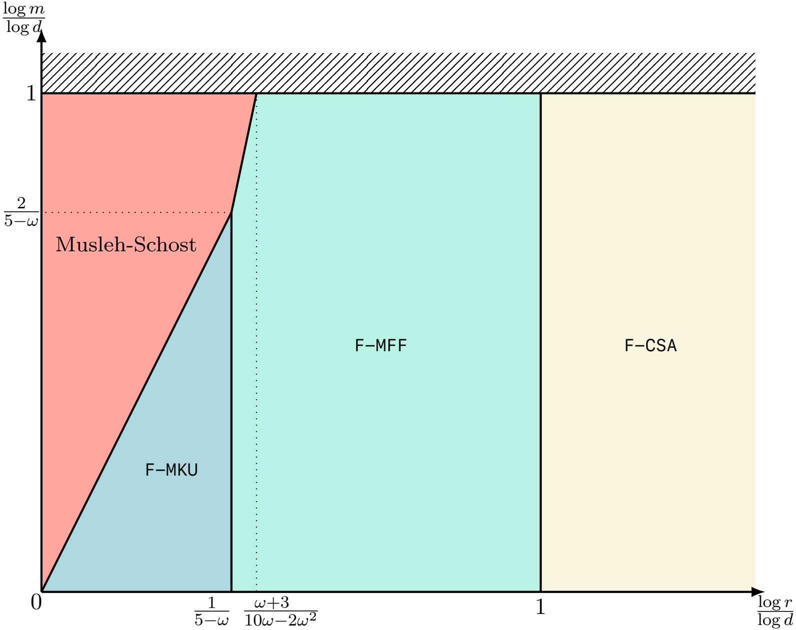
```
sage: matrix.charpoly()
-x^2 - T^2 - T - 1
sage: t = phi.ore_variable()
sage: - (t^2)^2 - phi(T)^2 - phi(T) - 1
0
```

Cost of computing χ

Las Vegas algorithm, cost in bit operations:

- [F−MFF] $O\tilde{}(d \log^2 q) + (\mathrm{SM}^{\geqslant 1}(d, d) + d^2 r + d r^\omega) \log q)^{1+o(1)}$,
- [F−MKU] $O\tilde{}(d \log^2 q) + ((d^2 r^{\omega-1} + d r^\omega) \log q)^{1+o(1)}$,
- [F−CSA] $O\tilde{}(d \log^2 q) + (r d^\omega \log q)^{1+o(1)}$.

d	$=$	$[K : \mathbb{F}_q]$
r	$=$	rank of ϕ
ω	$=$	feasible exponent for matrix multiplication in a field
$\mathrm{SM}^{\geqslant 1}$	$=$	related to fast multiplication of Ore polynomials [Caruso, Le Borgne, 2017]


$\frac{\log m}{\log d}$
1
$\frac{2}{5-\omega}$
Musleh-Schost
F−MKU
F−MFF
F−CSA
0
$\frac{1}{5-\omega}$
$\frac{\omega+3}{10\omega-2\omega^2}$
1
$\frac{\log r}{\log d}$

For general endomorphisms

Deterministic algorithm:

-
  - $O\tilde{}(n^2 + (n+r)r^{\Omega-1})$ operations in K
  - $O(n^2 + r^2)$ q-exponentiations in K

If K is finite, Las Vegas algorithm (cost in binary operations):

- $O\tilde{}(d \log^2 q) + ((\mathrm{SM}^{\geqslant 1}(n,d) + ndr + (n+d)r^{\omega}) \log q)^{1+o(1)}$.

n	=	τ-degree of the endomorphism
d	=	$[K : \mathbb{F}_q]$
r	=	rank of ϕ
ω	=	feasible exponent for matrix multiplication in a field
Ω	=	feasible exponent for characteristic polynomial computation in a field
$\mathrm{SM}^{\geqslant 1}$	=	related to fast multiplication of Ore polynomials [Caruso, Le Borgne, 2017]

For isogeny norms

Deterministic algorithm:

-
  - $\tilde{O}(n^2 + nr^{\omega-1} + r^{\omega})$ operations in K
  - $O(n^2 + r^2)$ q-exponentiations in K

If K is finite, Las Vegas algorithm (cost in bit operations):

- $\tilde{O}(d \log^2 q) + ((\mathrm{SM}^{\geqslant 1}(n, d) + ndr + n \min(d, r) r^{\omega-1} + dr^{\omega}) \log q)^{1+o(1)}$.

n	$=$	τ-degree of the isogeny
d	$=$	$[K : \mathbb{F}_q]$
r	$=$	rank of ϕ
ω	$=$	feasible exponent for matrix multiplication in a field
Ω	$=$	feasible exponent for characteristic polynomial computation in a field
$\mathrm{SM}^{\geqslant 1}$	$=$	related to fast multiplication of Ore polynomials [Caruso, Le Borgne, 2017]

What these computations highlight

- New and better state of the art in many parameters.
- High level of generality thanks to Anderson motives.

Co-author

Joint-work with Pierre-Jean Spaenlehauer. *Journal of Symbolic Computation* 125 (2024).

Building up on χ

χ determines many properties of ϕ:

1. Its isogeny class
2. Its endomorphism ring (to some extent)
3. Whether it is ordinary, supersingular, or in between

Assumptions:

- K is finite
- ϕ has rank 2
- $\chi \in \mathbb{F}_q[T][X]$ defines an imaginary hyperelliptic curve $\mathcal{H}$

Description of $\mathrm{End}(\phi)$

Consider the *coordinates ring of* $\mathcal{H}$:

$$\mathbb{F}_q[\mathcal{H}] = \mathbb{F}_q[T][X]/\langle \chi \rangle.$$

$\mathbb{F}_q[\mathcal{H}]$ embeds in $\mathrm{End}(\phi)$ via

$$\begin{array}{rcl} \mathbb{F}_q[\mathcal{H}] & \to & \mathrm{End}(\phi) \\ P(T, X) & \mapsto & P(\phi_T, \tau^d). \end{array}$$

Under the right assumptions:

- $\mathrm{End}(\phi) \simeq \mathbb{F}_q[\mathcal{H}]$
- $\mathbb{F}_q[\mathcal{H}]$ is a Dedekind ring

A group action

If I is an ideal of $\mathrm{End}(\phi)$, then

$$\iota = \mathrm{rgcd}(\{f : f \in I\}) \in K\{\tau\}$$

is an isogeny to some Drinfeld module ψ:

$$\iota : \phi \to \psi.$$

Fixing

$$I * \phi = \psi,$$

one defines a group action of $\mathrm{Cl}(\mathrm{End}(\phi))$ on the set of j-invariants.

Efficient representation

$\mathcal{H}$ being an imaginary hyperelliptic curve, one has an isomorphism

$$\mathrm{Pic}^0(\mathcal{H}) \simeq \mathrm{Cl}(\mathrm{End}(\phi)).$$

Elements of $\mathrm{Cl}(\mathrm{End}(\phi))$ are represented by *Mumford coordinates* $(u, v) \in \mathbb{F}_q[T]^2$:

$$\begin{array}{rcl} \mathrm{Pic}^0(\mathcal{H}) & \to & \mathrm{Cl}(\mathrm{End}(\phi)) \\ (u, v) & \mapsto & \overline{(\phi_u, \tau^d - \phi_v)}. \end{array}$$

Computing the group action comes down to computing

$$\iota = \mathrm{rgcd}(\phi_u, \tau^d - \phi_v).$$

Comparison with elliptic curves

For ellliptic curves, the action is described in terms of kernels.
It is very important in *post-quantum isogeny-based cryptography*: CRS protocol [Couveignes, 1999; Rostovtsev, Stolbunov, 2006].

Its computation is slow (involves torsion points in large extensions) [de Feo, Kieffer, Smith, 2018].

For cryptography

Our algorithms gives a candidate for a key-exchange protocol.

$$\begin{aligned} \textsc{crs}\text{ Classical} &\quad\longrightarrow\quad \sim 10\text{ min} \\ \textsc{crs}\text{ Drinfeld} &\quad\longrightarrow\quad \sim 400\text{ ms} \end{aligned}$$

The security would be based on the hardness of computing isogenies ...which is easy for Drinfeld modules [Wesolowski, 2022].

What these computations highlight

- We made explicit some very theoretical results.
- One can manipulate kernels by manipulating Ore polynomials directly.
- We directly used function field tools and the geometrical object defined by χ.