Algorithms for Drinfeld Modules and their Isogenies

Antoine Leudière

INRIA

August 8th, 2024

Contents

Outline

Drinfeld Modules in One Frame

Core Philosophy

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

$\mathbb{Z}$	$\mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
Number fields	Function fields
$\mathbb{R}$	$\mathbb{R}_\infty$
$\mathbb{C}$	$\mathbb{C}_\infty$
Characteristic p	$\mathbb{F}_q[T]$-characteristic $\mathfrak{p}$
Elliptic curves	Drinfeld modules
Abelian groups	$\mathbb{F}_q[T]$-modules
Isogenies of elliptic curves	Isogenies of Drinfeld modules
$\mathrm{End}(E)$	$\mathrm{End}(\phi)$

Why Algorithms for Drinfeld Modules?

Algorithmic problems tend to be easier for function fields than for number fields (e.g. factorization).

End Goal

Adapt methods from Drinfeld modules to elliptic curves.
Build a bridge from characteristic p to characteristic 0.

Targeted applications:

1. Computer algebra
2. Cryptography ⚠️

Why Algorithms for Drinfeld Modules?

Algorithmic problems tend to be easier for function fields than for number fields (e.g. factorization).

End Goal

Adapt methods from Drinfeld modules to elliptic curves.
Build a bridge from characteristic p to characteristic 0.

Targeted applications:

1. Computer algebra
2. Cryptography ⚠️

State of the Art

Algorithmics of Drinfeld modules:

- Kuhn-Pink, 2016
- Musleh-Schost, 2019
- Caranay-Greenberg-Scheidler, 2020
- Garai-Papikian, 2020
- Musleh-Schost, 2023
- Caruso-L., 2023

Applications to computer algebra:

- Doliskani-Narayanan-Schost, 2021

Implementation:

- Ayotte-Caruso-L.-Musleh, 2023

Drinfeld modules for cryptography:

- Scanlon, 2001,
- Gillard-Leprévost-Panchishkin-Roblot, 2003
- Joux-Narayanan, 2019.
- L.-Spaenlehauer, 2022.

PhD theses:

- Caranay, 2018
- Musleh, 2023
- Ayotte, 2023
- L., 2024 (in preparation)

Outline

Ore Polynomials

Let $K/\mathbb{F}_q$ be a field, fix

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

and

$$K\{\tau\} = \left\{ \sum_{i=0}^{n} f_i \tau^i : \quad n \in \mathbb{Z}_{\geqslant 0}, \quad f_i \in K \right\}.$$

Proposition

$K\{\tau\}$ is

1. a ring (addition and composition of endomorphisms),
2. noncommutative (if $K \neq \mathbb{F}_q$): for all $x \in K$, $\tau x = x^q \tau$.

Definition

$K\{\tau\}$ is the ring of *Ore polynomials*.

Ore Polynomials

Let $K/\mathbb{F}_q$ be a field, fix

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

and

$$K\{\tau\} = \left\{ \sum_{i=0}^{n} f_i \tau^i : \quad n \in \mathbb{Z}_{\geqslant 0}, \quad f_i \in K \right\}.$$

Proposition

$K\{\tau\}$ is

1. a ring (addition and composition of endomorphisms),
2. noncommutative (if $K \neq \mathbb{F}_q$): for all $x \in K$, $\tau x = x^q \tau$.

Definition

$K\{\tau\}$ is the ring of *Ore polynomials*.

Ore Polynomials

Let $K/\mathbb{F}_q$ be a field, fix

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

and

$$K\{\tau\} = \left\{ \sum_{i=0}^{n} f_i \tau^i : \quad n \in \mathbb{Z}_{\geqslant 0}, \quad f_i \in K \right\}.$$

Proposition

$K\{\tau\}$ is

1. a ring (addition and composition of endomorphisms),
2. noncommutative (if $K \neq \mathbb{F}_q$): for all $x \in K$, $\tau x = x^q \tau$.

Definition

$K\{\tau\}$ is the ring of *Ore polynomials*.

Ore Polynomials are almost Polynomials

Let

$$f = \sum_{i=0}^{n} f_i \tau^i \in K\{\tau\}, \quad f_n \neq 0.$$

Definition

We call n the *τ-degree* of f, and write $n = \deg_\tau(f)$.

Proposition

The ring $K\{\tau\}$ is:

1. left-euclidean for the τ-degree,
2. left-principal.

Consequence: one can compute right-gcd's.

Ore Polynomials are almost Polynomials

Let
$$f = \sum_{i=0}^{n} f_i \tau^i \in K\{\tau\}, \quad f_n \neq 0.$$

Definition

We call n the τ-*degree* of f, and write $n = \deg_\tau(f)$.

Proposition

The ring $K\{\tau\}$ is:

1. left-euclidean for the τ-degree,
2. left-principal.

Consequence: one can compute right-gcd's.

Defining Drinfeld Modules

Definition

A *Drinfeld module* over K is a morphism of $\mathbb{F}_q$-algebras

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

such that $\deg_\tau(\phi_T) > 0$.

A Drinfeld module is **not** a module!

Defining Drinfeld Modules

Definition

A *Drinfeld module* over K is a morphism of $\mathbb{F}_q$-algebras

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

such that $\deg_\tau(\phi_T) > 0$.

A Drinfeld module is **not** a module!

Rank of a Drinfeld Module

Important invariant that does not exist for elliptic curves: the *rank*.
Let

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

be a Drinfeld module.

Definition

The *rank* of ϕ is $\deg_\tau(\phi_T)$.

From now on, all Drinfeld modules have rank 2.

Then, a Drinfeld module is given by $\phi_T \in K\{\tau\}$ given by

$$\phi_T = \omega + g\tau + \Delta\tau^2, \quad \omega, g, \Delta \in K, \quad \Delta \neq 0.$$

Rank of a Drinfeld Module

Important invariant that does not exist for elliptic curves: the *rank*.
Let

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

be a Drinfeld module.

Definition

The *rank* of ϕ is $\deg_\tau(\phi_T)$.

From now on, all Drinfeld modules have rank 2.

Then, a Drinfeld module is given by $\phi_T \in K\{\tau\}$ given by

$$\phi_T = \omega + g\tau + \Delta\tau^2, \quad \omega, g, \Delta \in K, \quad \Delta \neq 0.$$

Morphisms and Isogenies of Drinfeld Modules

Definition

A morphism of Drinfeld modules $\phi \to \psi$ is an $u \in K\{\tau\}$ s.t.

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

Definition

An isogeny is a nonzero morphism.

Morphisms and Isogenies of Drinfeld Modules

Definition

A morphism of Drinfeld modules $\phi \to \psi$ is an $u \in K\{\tau\}$ s.t.

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

Definition

An isogeny is a nonzero morphism.

An Example

Example

Pick $\mathbb{F}_q = \mathbb{F}_2$ and $K = \mathbb{F}_4 = \{0, 1, i, i+1\}$.
Pick

$$\begin{cases} \phi_T = i + i\tau + \tau^2, \\ \psi_T = i + (i+1)\tau + \tau^2. \end{cases}$$

Then $u = (i+1)\tau^2$ is an isogeny $\phi \to \psi$:

$$\begin{cases} u\phi_T = ((i+1)\tau^2) \cdot (i + i\tau + \tau^2) = \cdots = \tau^2 + \tau^3 + (i+1)\tau^4, \\ \psi_T u = (i + (i+1)\tau + \tau^2) \cdot ((i+1)\tau^2) = \cdots = \tau^2 + \tau^3 + (i+1)\tau^4. \end{cases}$$

An Example

Example

Pick $\mathbb{F}_q = \mathbb{F}_2$ and $K = \mathbb{F}_4 = \{0, 1, i, i+1\}$.
Pick
$$\begin{cases} \phi_T = i + i\tau + \tau^2, \\ \psi_T = i + (i+1)\tau + \tau^2. \end{cases}$$
Then $u = (i+1)\tau^2$ is an isogeny $\phi \to \psi$:
$$\begin{cases} u\phi_T = ((i+1)\tau^2) \cdot (i + i\tau + \tau^2) = \cdots = \tau^2 + \tau^3 + (i+1)\tau^4, \\ \psi_T u = (i + (i+1)\tau + \tau^2) \cdot ((i+1)\tau^2) = \cdots = \tau^2 + \tau^3 + (i+1)\tau^4. \end{cases}$$

Outline

$\mathbb{F}_q[T]$-*Module*

An elliptic curve is an abelian group, *i.e.* a $\mathbb{Z}$-module.
For Drinfeld modules, we replace $\mathbb{Z}$ by $\mathbb{F}_q[T]$.

Definition

The $\mathbb{F}_q[T]$-module associated to ϕ, denoted by $\overline{K}_\phi$, is

$$\begin{array}{rcl} \mathbb{F}_q[T] \times \overline{K} & \longrightarrow & \overline{K} \\ (a, x) & \longmapsto & \phi_a(x). \end{array}$$

The notion of point is ambiguous.

$\mathbb{F}_q[T]$-Module

An elliptic curve is an abelian group, *i.e.* a $\mathbb{Z}$-module.
For Drinfeld modules, we replace $\mathbb{Z}$ by $\mathbb{F}_q[T]$.

Definition

The $\mathbb{F}_q[T]$-module associated to ϕ, denoted by $\overline{K}_\phi$, is

$$\begin{array}{rcl} \mathbb{F}_q[T] \times \overline{K} & \longrightarrow & \overline{K} \\ (a, x) & \longmapsto & \phi_a(x). \end{array}$$

The notion of point is ambiguous.

$\mathbb{F}_q[T]$-Module

An elliptic curve is an abelian group, *i.e.* a $\mathbb{Z}$-module.
For Drinfeld modules, we replace $\mathbb{Z}$ by $\mathbb{F}_q[T]$.

Definition

The $\mathbb{F}_q[T]$-module associated to ϕ, denoted by $\overline{K}_\phi$, is

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

The notion of point is ambiguous.

$\mathbb{F}_q[T]$-*Characteristic*

Define the morphism of $\mathbb{F}_q$-algebras

$$\begin{array}{rccl} \gamma : & \mathbb{F}_q[T] & \longrightarrow & K \\ & a & \longmapsto & \text{constant coefficient of } \phi_a. \end{array}$$

Definition

The $\mathbb{F}_q[T]$-*characteristic* is monic generator of the kernel of γ.

Two situations:

1. γ is injective (analogous to elliptic curves over fields of characteristic 0),
2. γ has nonzero kernel $\mathfrak{p}$ (analogous to elliptic curves over fields of characteristic p).

$\mathbb{F}_q[T]$-*Characteristic*

Define the morphism of $\mathbb{F}_q$-algebras

$$\begin{array}{rrcl} \gamma: & \mathbb{F}_q[T] & \longrightarrow & K \\ & a & \longmapsto & \text{constant coefficient of } \phi_a. \end{array}$$

Definition

The $\mathbb{F}_q[T]$-*characteristic* is monic generator of the kernel of γ.

Two situations:

1. γ is injective (analogous to elliptic curves over fields of characteristic 0),
2. γ has nonzero kernel $\mathfrak{p}$ (analogous to elliptic curves over fields of characteristic p).

$\mathbb{F}_q[T]$-*Characteristic*

Define the morphism of $\mathbb{F}_q$-algebras

$$\begin{array}{rrcl} \gamma : & \mathbb{F}_q[T] & \longrightarrow & K \\ & a & \longmapsto & \text{constant coefficient of } \phi_a. \end{array}$$

Definition

The $\mathbb{F}_q[T]$-*characteristic* is monic generator of the kernel of γ.

Two situations:

1. γ is injective (analogous to elliptic curves over fields of characteristic 0),
2. γ has nonzero kernel $\mathfrak{p}$ (analogous to elliptic curves over fields of characteristic p).

Torsion

Definition

Let $a \in \mathbb{F}_q[T]$. The a-*torsion* of ϕ, denoted by $\phi[a]$, is

$$\phi[a] = a\text{-torsion of the module } \overline{\mathrm{K}}_\phi = \mathrm{Ker}(\phi_a).$$

Proposition

There exists $h \in \{1, 2\}$ such that, for all $a, b \in \mathbb{F}_q[T]$:

$$\begin{array}{ll} \text{if } a \text{ is coprime to } \mathfrak{p}, & \text{then } \phi[a] \simeq (\mathbb{F}_q[T]/(a))^2, \\ \text{if } a \text{ is a power of } \mathfrak{p}, & \text{then } \phi[a] \simeq (\mathbb{F}_q[T]/(a))^{2-h}, \\ \text{if } a \text{ and } b \text{ are coprime,} & \text{then } \phi[ab] \simeq \phi[a] \times \phi[b]. \end{array}$$

Torsion

Definition

Let $a \in \mathbb{F}_q[T]$. The *a-torsion* of ϕ, denoted by $\phi[a]$, is

$$\phi[a] = a\text{-torsion of the module } \overline{K}_\phi = \mathrm{Ker}(\phi_a).$$

Proposition

There exists $h \in \{1, 2\}$ such that, for all $a, b \in \mathbb{F}_q[T]$:

$$\begin{array}{ll} \text{if } a \text{ is coprime to } \mathfrak{p}, & \text{then } \phi[a] \simeq (\mathbb{F}_q[T]/(a))^2, \\ \text{if } a \text{ is a power of } \mathfrak{p}, & \text{then } \phi[a] \simeq (\mathbb{F}_q[T]/(a))^{2-h}, \\ \text{if } a \text{ and } b \text{ are coprime,} & \text{then } \phi[ab] \simeq \phi[a] \times \phi[b]. \end{array}$$

Ring of Endomorphisms

Endomorphisms of ϕ form a ring denoted $\mathrm{End}(\phi)$.

There are special endomorphisms:

- For any $a \in \mathbb{F}_q[T]$, ϕ_a is an endomorphism.
- If K is finite, then $\tau^{[K:\mathbb{F}_q]}$ is central in $K\{\tau\}$, and defines the *Frobenius endomorphism* of ϕ.

Remark

ϕ_a is the analogue of the multiplication by an integer.

Ring of Endomorphisms

Endomorphisms of ϕ form a ring denoted $\mathrm{End}(\phi)$.

There are special endomorphisms:

- For any $a \in \mathbb{F}_q[T]$, ϕ_a is an endomorphism.
- If K is finite, then $\tau^{[K:\mathbb{F}_q]}$ is central in $K\{\tau\}$, and defines the *Frobenius endomorphism* of ϕ.

Remark

ϕ_a is the analogue of the multiplication by an integer.

Implementation

Most objects in this talk can be explicitly computed.
SageMath implementation of Drinfeld modules.
(ISSAC software presentation: Ayotte-Caruso-L.-Musleh, 2023.)

```
sage: Fq = GF(2)
sage: K.<i> = Fq.extension(2)
sage: A.<T> = Fq[]
sage: phi = DrinfeldModule(A, [i, i, 1])
sage: psi = DrinfeldModule(A, [i, i + 1, 1])
sage: t = phi.ore_variable()
sage: (i + 1) * t^2 in Hom(phi, psi)
True
```

Outline

Algebra of Endomorphisms

Consider

$$\mathrm{End}^\circ(\phi) = \mathrm{End}(\phi) \otimes_{\mathbb{F}_q[T]} \mathbb{F}_q(T).$$

Theorem

- $\mathrm{End}^\circ(\phi)$ *is a division algebra;*
- $\mathrm{End}(\phi)$ *is free over* $\mathbb{F}_q[T]$ *with rank* 1, 2 *or* 4;
- $\mathrm{End}(\phi)$ *is an order in* $\mathrm{End}^\circ(\phi)$.

Algebra of Endomorphisms

Consider

$$\mathrm{End}^\circ(\phi) = \mathrm{End}(\phi) \otimes_{\mathbb{F}_q[T]} \mathbb{F}_q(T).$$

Theorem

- $\mathrm{End}^\circ(\phi)$ *is a division algebra;*
- $\mathrm{End}(\phi)$ *is free over* $\mathbb{F}_q[T]$ *with rank* 1, 2 *or* 4;
- $\mathrm{End}(\phi)$ *is an order in* $\mathrm{End}^\circ(\phi)$.

Ordinarity and Supersingularity

Assume K is a finite field. Recall we have defined:

- the *function field characteristic* $\mathfrak{p}$,
- the $\mathfrak{p}$-torsion $\phi_{\mathfrak{p}}$.

Definition

ϕ is:

- *supersingular* if the $\mathfrak{p}$-torsion is trivial;
- *ordinary* if ϕ is not supersingular;

Ordinarity and Supersingularity

Assume K is a finite field. Recall we have defined:

- the *function field characteristic* $\mathfrak{p}$,
- the $\mathfrak{p}$-torsion $\phi_{\mathfrak{p}}$.

Definition

ϕ is:

- *supersingular* if the $\mathfrak{p}$-torsion is trivial;
- *ordinary* if ϕ is not supersingular;

Ordinary Drinfeld Modules

Assume ϕ is ordinary.

Theorem

$\mathrm{End}(\phi)$ *is an order in an imaginary quadratic function field.*

(Meaning $\mathrm{End}^\circ(\phi) = \mathrm{End}(\phi) \otimes_{\mathbb{F}_q[T]} \mathbb{F}_q(T)$ is a quadratic extension of $\mathbb{F}_q(T)$ in which the place at infinity of $\mathbb{F}_q(T)$ has two extensions.)

Ordinary Drinfeld Modules

Assume ϕ is ordinary.

Theorem

$\mathrm{End}(\phi)$ *is an order in an imaginary quadratic function field.*

(Meaning $\mathrm{End}^\circ(\phi) = \mathrm{End}(\phi) \otimes_{\mathbb{F}_q[T]} \mathbb{F}_q(T)$ is a quadratic extension of $\mathbb{F}_q(T)$ in which the place at infinity of $\mathbb{F}_q(T)$ has two extensions.)

The CRS Group Action

There is a CRS (Couveignes, 1997; Rostovtsev-Stolbunov, 2006) group action:

Theorem

$\mathrm{Cl}(\mathrm{End}(\phi))$ *acts freely and transitively on the set* S_ϕ *of isomorphism classes of Drinfeld modules isogenous to* ϕ.

The action is described as for elliptic curves: if $\mathfrak{a} \subset \mathrm{End}(\phi)$ is an ideal, then

$$V_{\mathfrak{a}} = \bigcap_{u \in \mathfrak{a}} \mathrm{Ker}(u)$$

is the kernel of an isogeny $u_{\mathfrak{a}}$ from ϕ to some other Drinfeld module ψ. We define

$$\mathfrak{a} * \phi = \psi,$$

and extend to $\mathrm{Cl}(\mathrm{End}(\phi))$ and S_ϕ.

The CRS Group Action

There is a CRS (Couveignes, 1997; Rostovtsev-Stolbunov, 2006) group action:

Theorem

$\mathrm{Cl}(\mathrm{End}(\phi))$ *acts freely and transitively on the set* S_ϕ *of isomorphism classes of Drinfeld modules isogenous to* ϕ.

The action is described as for elliptic curves: if $\mathfrak{a} \subset \mathrm{End}(\phi)$ is an ideal, then

$$V_{\mathfrak{a}} = \bigcap_{u \in \mathfrak{a}} \mathrm{Ker}(u)$$

is the kernel of an isogeny $u_{\mathfrak{a}}$ from ϕ to some other Drinfeld module ψ. We define

$$\mathfrak{a} * \phi = \psi,$$

and extend to $\mathrm{Cl}(\mathrm{End}(\phi))$ and S_ϕ.

Supersingular Drinfeld Modules

Assume ϕ is supersingular.

Theorem

$\mathrm{End}(\phi)$ *is either:*

- *a maximal order in the quaternion algebra ramified at $\mathfrak{p}$ and the ∞ place,*
- *an order in a quadratic imaginary function field.*

Different than for elliptic curves! Classification related to *Weil polynomials* and *Weil numbers* (Caranay, 2018).

Theorem (Deuring correspondence)

Correspondence between:

- *left-ideal classes of $\mathrm{End}(\phi)$,*
- *isomorphism classes of supersingular rank two Drinfeld modules over $\overline{\mathbb{F}_q}$.*

Supersingular Drinfeld Modules

Assume ϕ is supersingular.

Theorem

$\mathrm{End}(\phi)$ *is either:*

- *a maximal order in the quaternion algebra ramified at* $\mathfrak{p}$ *and the* ∞ *place,*
- *an order in a quadratic imaginary function field.*

Different than for elliptic curves! Classification related to *Weil polynomials* and *Weil numbers* (Caranay, 2018).

Theorem (Deuring correspondence)

Correspondence between:

- *left-ideal classes of* $\mathrm{End}(\phi)$*,*
- *isomorphism classes of supersingular rank two Drinfeld modules over* $\overline{\mathbb{F}_q}$*.*

Supersingular Drinfeld Modules

Assume ϕ is supersingular.

Theorem

$\mathrm{End}(\phi)$ *is either:*

- *a maximal order in the quaternion algebra ramified at* $\mathfrak{p}$ *and the* ∞ *place,*
- *an order in a quadratic imaginary function field.*

Different than for elliptic curves! Classification related to *Weil polynomials* and *Weil numbers* (Caranay, 2018).

Theorem (Deuring correspondence)

Correspondence between:

- *left-ideal classes of* $\mathrm{End}(\phi)$*,*
- *isomorphism classes of supersingular rank two Drinfeld modules over* $\overline{\mathbb{F}_q}$*.*

Outline

Computing Isogenies (1/2)

Let ϕ, ψ be two Drinfeld modules.

As $\mathrm{Hom}(\phi, \psi)$ is an $\mathbb{F}_q[T]$-module, it is a $\mathbb{F}_q$-vector space.

Contrast with elliptic curves!

Let $n \in \mathbb{Z}_{\geqslant 0}$. Fix the sub-$\mathbb{F}_q$-vector space

$$\mathrm{Hom}_n(\phi, \psi) = \{u \in \mathrm{Hom}(\phi, \psi) : \deg_\tau(u) \leqslant n\}.$$

Theorem (Wesolowski, 2022)

We can compute an $\mathbb{F}_q$-basis of $\mathrm{Hom}_n(\phi, \psi)$ in polynomial time.

Computing Isogenies (1/2)

Let ϕ, ψ be two Drinfeld modules.

As $\mathrm{Hom}(\phi, \psi)$ is an $\mathbb{F}_q[T]$-module, it is a $\mathbb{F}_q$-vector space.

Contrast with elliptic curves!

Let $n \in \mathbb{Z}_{\geqslant 0}$. Fix the sub-$\mathbb{F}_q$-vector space

$$\mathrm{Hom}_n(\phi, \psi) = \{u \in \mathrm{Hom}(\phi, \psi) : \deg_\tau(u) \leqslant n\}.$$

Theorem (Wesolowski, 2022)

We can compute an $\mathbb{F}_q$-basis of $\mathrm{Hom}_n(\phi, \psi)$ in polynomial time.

Computing Isogenies (1/2)

Let ϕ, ψ be two Drinfeld modules.

As $\mathrm{Hom}(\phi, \psi)$ is an $\mathbb{F}_q[T]$-module, it is a $\mathbb{F}_q$-vector space.

Contrast with elliptic curves!

Let $n \in \mathbb{Z}_{\geqslant 0}$. Fix the sub-$\mathbb{F}_q$-vector space

$$\mathrm{Hom}_n(\phi, \psi) = \{u \in \mathrm{Hom}(\phi, \psi) : \deg_\tau(u) \leqslant n\}.$$

Theorem (Wesolowski, 2022)

We can compute an $\mathbb{F}_q$-basis of $\mathrm{Hom}_n(\phi, \psi)$ in polynomial time.

Computing isogenies (2/2)

Fix

$$\begin{cases} \phi_{\mathrm{T}} = \sum_{i=0}^{2} g_i \tau^i, \\ \psi_{\mathrm{T}} = \sum_{i=0}^{2} g'_i \tau^i, \\ u = \sum_{i=0}^{n} u_i \tau^i. \end{cases}$$

Then u is an isogeny iff

$$u\phi_{\mathrm{T}} = \psi_{\mathrm{T}} u$$

iff

$$\sum_{i=0}^{\min(k,n)} u_i g_{k-i}^{q^i} - g'_{k-i} u_i^{q^{k-i}} = 0, \quad \forall 0 \leqslant k \leqslant n+2.$$

We have obtained a finite system of $\mathbb{F}_q$-linear equations.

Computing isogenies (2/2)

Fix

$$\begin{cases} \phi_{\mathrm{T}} = \sum_{i=0}^{2} g_i \tau^i, \\ \psi_{\mathrm{T}} = \sum_{i=0}^{2} g_i' \tau^i, \\ u = \sum_{i=0}^{n} u_i \tau^i. \end{cases}$$

Then u is an isogeny iff

$$u\phi_{\mathrm{T}} = \psi_{\mathrm{T}} u$$

iff

$$\sum_{i=0}^{\min(k,n)} u_i g_{k-i}^{q^i} - g_{k-i}' u_i^{q^{k-i}} = 0, \quad \forall 0 \leqslant k \leqslant n+2.$$

We have obtained a finite system of $\mathbb{F}_q$-linear equations.

Computing endomorphisms

Variations:

Theorem (Wesolowski, 2022; Musleh, 2023)

Let π be the Frobenius endomorphism of ϕ. One computes:

- *an* $\mathbb{F}_q$*-basis of* $\mathrm{Hom}_n(\phi, \psi)$ *with* $(n^\omega d^\omega \log q + nd^2 \log q + d \log^2 q)^{1+o(1)}$,
- *an* $\mathbb{F}_q[\pi]$*-basis of* $\mathrm{Hom}(\phi, \psi)$ *using* $(d^{2\omega} \log q + d \log^2 q)^{1+o(1)}$,
- *an* $\mathbb{F}_q[T]$*-basis of* $\mathrm{Hom}(\phi, \psi)$ *using* $(d^3 f^2 \log q + d \log^2 q)^{1+o(1)}$,

bit operations.

The previous applies to $\mathrm{End}(\phi) = \mathrm{Hom}(\phi, \phi)$.

Computing endomorphisms

Variations:

Theorem (Wesolowski, 2022; Musleh, 2023)

Let π be the Frobenius endomorphism of ϕ. One computes:

- *an $\mathbb{F}_q$-basis of $\mathrm{Hom}_n(\phi, \psi)$ with $(n^\omega d^\omega \log q + nd^2 \log q + d \log^2 q)^{1+o(1)}$,*
- *an $\mathbb{F}_q[\pi]$-basis of $\mathrm{Hom}(\phi, \psi)$ using $(d^{2\omega} \log q + d \log^2 q)^{1+o(1)}$,*
- *an $\mathbb{F}_q[T]$-basis of $\mathrm{Hom}(\phi, \psi)$ using $(d^3 f^2 \log q + d \log^2 q)^{1+o(1)}$,*

bit operations.

The previous applies to $\mathrm{End}(\phi) = \mathrm{Hom}(\phi, \phi)$.

Computing the CRS Group Action: Definition from Elliptic Curves

Let ϕ be an ordinary Drinfeld module. Let

$$S_\phi = \{\text{isomorphism classes of Drinfeld modules isogenous to } \phi\}.$$

Recall we have a free and transitive group action

$$* : \mathrm{Cl}(\mathrm{End}(\phi)) \times S_\phi \to S_\phi.$$

We have defined $*$ with kernels.

`Jump to the definition.`

Computing the CRS Group Action: Definition from Elliptic Curves

Let ϕ be an ordinary Drinfeld module. Let

$$S_\phi = \{\text{isomorphism classes of Drinfeld modules isogenous to } \phi\}.$$

Recall we have a free and transitive group action

$$* : \mathrm{Cl}(\mathrm{End}(\phi)) \times S_\phi \to S_\phi.$$

We have defined $*$ with kernels.

Jump to the definition.

Computing the CRS Group Action: Definition from Elliptic Curves

Let ϕ be an ordinary Drinfeld module. Let

$$S_\phi = \{\text{isomorphism classes of Drinfeld modules isogenous to } \phi\}.$$

Recall we have a free and transitive group action

$$* : \mathrm{Cl}(\mathrm{End}(\phi)) \times S_\phi \to S_\phi.$$

We have defined $*$ with kernels.

`Jump to the definition.`

Computing the CRS Group Action: Alternative Definition

Two things:

1. $V_{\mathfrak{a}}$ is the kernel of the Ore polynomial $u_{\mathfrak{a}} = \mathrm{rgcd}(\{a : a \in \mathfrak{a}\})$.
2. In some instances, we can describe $\mathrm{Cl}(\mathrm{End}(\phi))$ as the Picard group of an imaginary hyperelliptic curve.

Assume the Frobenius characteristic polynomial

$$\chi_\pi = X^2 + t(T)X + n(T) \in \mathbb{F}_q[T][X]$$

defines an imaginary hyperelliptic curve $\mathcal{H}$.
Then:

- $\mathrm{End}(\phi)$ is the coordinate ring $\mathbb{F}_q[\mathcal{H}]$ of $\mathcal{H}$.
- $\mathrm{Cl}(\mathrm{End}(\phi))$ is the Picard group $\mathrm{Pic}^0(\mathcal{H})$ of $\mathcal{H}$.

Computing the CRS Group Action: Alternative Definition

Two things:

1. $V_{\mathfrak{a}}$ is the kernel of the Ore polynomial $u_{\mathfrak{a}} = \mathrm{rgcd}(\{a : a \in \mathfrak{a}\})$.
2. In some instances, we can describe $\mathrm{Cl}(\mathrm{End}(\phi))$ as the Picard group of an imaginary hyperelliptic curve.

Assume the Frobenius characteristic polynomial

$$\chi_\pi = X^2 + t(T)X + n(T) \in \mathbb{F}_q[T][X]$$

defines an imaginary hyperelliptic curve $\mathcal{H}$.

Then:

- $\mathrm{End}(\phi)$ is the coordinate ring $\mathbb{F}_q[\mathcal{H}]$ of $\mathcal{H}$.
- $\mathrm{Cl}(\mathrm{End}(\phi))$ is the Picard group $\mathrm{Pic}^0(\mathcal{H})$ of $\mathcal{H}$.

Computing the CRS Group Action: Alternative Definition

Two things:

1. $V_{\mathfrak{a}}$ is the kernel of the Ore polynomial $u_{\mathfrak{a}} = \mathrm{rgcd}(\{a : a \in \mathfrak{a}\})$.
2. In some instances, we can describe $\mathrm{Cl}(\mathrm{End}(\phi))$ as the Picard group of an imaginary hyperelliptic curve.

Assume the Frobenius characteristic polynomial

$$\chi_\pi = X^2 + t(T)X + n(T) \in \mathbb{F}_q[T][X]$$

defines an imaginary hyperelliptic curve $\mathcal{H}$.
Then:

- $\mathrm{End}(\phi)$ is the coordinate ring $\mathbb{F}_q[\mathcal{H}]$ of $\mathcal{H}$.
- $\mathrm{Cl}(\mathrm{End}(\phi))$ is the Picard group $\mathrm{Pic}^0(\mathcal{H})$ of $\mathcal{H}$.

Computing the CRS Group Action: Mumford Coordinates

Elements of $\mathrm{Pic}^0(\mathcal{H})$ can be represented by *Mumford coordinates*: pairs $(u, v) \in \mathbb{F}_q[T]^2$ such that:

$$\begin{cases} \deg(u) < \deg(v) \leqslant d \\ (u, v) \text{ represents the ideal class of } \langle \phi_u, \pi - \phi_v \rangle. \end{cases}$$

Then

$$u_{\mathfrak{a}} = \mathrm{rgcd}(\phi_u, \pi - \phi_v).$$

Theorem (L.-Spaenlehauer, 2023)

The group action can be computed with $O(d^2)$ operations in $\mathbb{F}_q$ and $O(d^2)$ applications of the Frobenius endomorphism $x \mapsto x^q$ of K.

Computing the CRS Group Action: Mumford Coordinates

Elements of $\mathrm{Pic}^0(\mathcal{H})$ can be represented by *Mumford coordinates*: pairs $(u, v) \in \mathbb{F}_q[T]^2$ such that:

$$\begin{cases} \deg(u) < \deg(v) \leqslant d \\ (u, v) \text{ represents the ideal class of } \langle \phi_u, \pi - \phi_v \rangle. \end{cases}$$

Then

$$u_{\mathfrak{a}} = \mathrm{rgcd}(\phi_u, \pi - \phi_v).$$

Theorem (L.-Spaenlehauer, 2023)

The group action can be computed with $O(d^2)$ operations in $\mathbb{F}_q$ and $O(d^2)$ applications of the Frobenius endomorphism $x \mapsto x^q$ of K.

Computing the CRS Group Action: For Crypto?

We implemented the action (C++/NTL).

Following the *Hard Homogeneous Space* philosophy of Couveignes (1997), Rostovtsev-Stolbunov (2006), we tried to derive a Key Exchange Protocol with this group action.

Pros

It's faster ($\sim$ 24 ms) than traditional CRS 👍

Cons

It's insecure ☠️

Computing the CRS Group Action: For Crypto?

We implemented the action (C++/NTL).
Following the *Hard Homogeneous Space* philosophy of Couveignes (1997), Rostovtsev-Stolbunov (2006), we tried to derive a Key Exchange Protocol with this group action.

Pros

It's faster ($\sim$ 24 ms) than traditional CRS 👍

Cons

It's insecure ☠️

Computing the CRS Group Action: For Crypto?

We implemented the action (C++/NTL).
Following the *Hard Homogeneous Space* philosophy of Couveignes (1997), Rostovtsev-Stolbunov (2006), we tried to derive a Key Exchange Protocol with this group action.

Pros

It's faster ($\sim$ 24 ms) than traditional CRS 👍

Cons

It's insecure ☠️

Computing the CRS Group Action: For Crypto?

We implemented the action (C++/NTL).
Following the *Hard Homogeneous Space* philosophy of Couveignes (1997), Rostovtsev-Stolbunov (2006), we tried to derive a Key Exchange Protocol with this group action.

Pros

It's faster ($\sim$ 24 ms) than traditional CRS 👍

Cons

It's insecure ☠️

Outline

Lessons

Most famous problems that are difficult for elliptic curves are easy for Drinfeld modules. Because:

1. $\mathbb{F}_q$ acts on most objects,
2. we benefit from the tools of algebraic geometry,
3. (barely mentioned before) we can use *Anderson motives* to represent isogenies as polynomial matrices.

Algorithmically, supersingularity does not seem as crucial for Drinfeld modules as it is for elliptic curves.

Lessons

Most famous problems that are difficult for elliptic curves are easy for Drinfeld modules. Because:

1. $\mathbb{F}_q$ acts on most objects,
2. we benefit from the tools of algebraic geometry,
3. (barely mentioned before) we can use *Anderson motives* to represent isogenies as polynomial matrices.

Algorithmically, supersingularity does not seem as crucial for Drinfeld modules as it is for elliptic curves.

For the Future

Drinfeld Modules are very general objects, and can be computed in a general context (Musleh-Schost, 2023; Caruso-L., 2023).
Let C be a smooth geometrically connected curve over $\mathbb{F}_q$.

$\mathbb{Z}$	$\mathbb{F}_q[T]$	A
$\mathbb{Q}$	$\mathbb{F}_q(T)$	$\mathbb{F}_q(C)$
Number fields	Function fields	Finite extensions of $\mathbb{F}_q(C)$
$\mathbb{R}$	$\mathbb{R}_\infty$	$\mathbb{R}_x$, $x \in C$
$\mathbb{C}$	$\mathbb{C}_\infty$	$\mathbb{C}_x$, $x \in C$
Characteristic p	$\mathbb{F}_q[T]$-characteristic $\mathfrak{p}$	A-characteristic $\mathfrak{p}$
Elliptic curves	Drinfeld $\mathbb{F}_q[T]$-modules	Drinfeld A-modules
Abelian groups	$\mathbb{F}_q[T]$-modules	A-modules
Isogenies of elliptic curves	Isogenies of Dr. $\mathbb{F}_q[T]$-modules	Isogenies of Dr. A-modules
$\mathrm{End}(E)$	$\mathrm{End}(\phi)$	$\mathrm{End}(\phi)$

Relying less on elliptic curves and find original problems for Drinfeld modules.

For the Future

Drinfeld Modules are very general objects, and can be computed in a general context (Musleh-Schost, 2023; Caruso-L., 2023).
Let C be a smooth geometrically connected curve over $\mathbb{F}_q$.

$\mathbb{Z}$	$\mathbb{F}_q[T]$	A
$\mathbb{Q}$	$\mathbb{F}_q(T)$	$\mathbb{F}_q(C)$
Number fields	Function fields	Finite extensions of $\mathbb{F}_q(C)$
$\mathbb{R}$	$\mathbb{R}_\infty$	$\mathbb{R}_x$, $x \in C$
$\mathbb{C}$	$\mathbb{C}_\infty$	$\mathbb{C}_x$, $x \in C$
Characteristic p	$\mathbb{F}_q[T]$-characteristic $\mathfrak{p}$	A-characteristic $\mathfrak{p}$
Elliptic curves	Drinfeld $\mathbb{F}_q[T]$-modules	Drinfeld A-modules
Abelian groups	$\mathbb{F}_q[T]$-modules	A-modules
Isogenies of elliptic curves	Isogenies of Dr. $\mathbb{F}_q[T]$-modules	Isogenies of Dr. A-modules
$\mathrm{End}(E)$	$\mathrm{End}(\phi)$	$\mathrm{End}(\phi)$

Relying less on elliptic curves and find original problems for Drinfeld modules.