Drinfeld modules

Effective class group action and implementation

Antoine Leudière

Institut de recherche mathématique de Rennes, *Géométrie et algèbre effectives* seminar

2022 september 23rd

Post quantum key-exchange and signature (1/2)

The late queen and duke choose an abelian simply transitive group action $G \times X \to X$.

$\longleftarrow$ public agreement on random $x \in X$ $\longrightarrow$

$\longrightarrow$ $a \cdot x$ $\longrightarrow$

$\longleftarrow$ $b \cdot x$ $\longleftarrow$

$\dashleftarrow$ Both calculate $ab \cdot x$ (secret key) $\dashrightarrow$

Definition (Couveignes, 1996)

If computing $ab \cdot x$ knowing x, $a \cdot x$, $b \cdot x$ is hard, this is a hard homogeneous space.

Beullens-Kleinjung-Vercauteren in CSI-FiSh

Knowing the group order, we can build efficient signature schemes.

Post quantum key-exchange and signature (2/2)

Diffie-Hellman ('76)	$G = \mathbb{Z}/n\mathbb{Z}$ X = cyclic group with order n and generator g Quantum-broken
CRS ('96, '04)	$G = \mathrm{Cl}(\mathbb{Q}(\sqrt{-D}))$ X = subset of isomorphism classes of ordinary elliptic curves. Slow to run & hard to know group order
CSIDH ('18)	$G = \mathrm{Cl}(\mathbb{Q}(\sqrt{-D}))$ X = subset of isomorphism classes of supersingular elliptic curves. Hard to know group order

Our hope

- Build a fast "Drinfeld analogue" of the CRS group action.
- Practical computation of the group order using Kedlaya's algorithm.

Why Drinfeld modules?

Drinfeld modules make explicit the class field theory of function fields.
They play the role of elliptic curves for building the Hilbert class field of a function field.

Rule of thumb

$$\text{Elliptic curves} \xleftrightarrow{\text{behave like}} \text{Drinfeld modules with rank two.}$$

Algorithms

- Ore polynomials: Caruso-Leborgne.
- Characteristic polynomial of the Frobenius endomorphism: Schost-Musleh, 2019.
- Modular polynomials of rank 2 Drinfeld modules: Caranay-Greenberg-Scheidler, 2019.
- Tools for isogenies and endomorphisms: Caranay's thesis, 2018; Caranay-Greenberg-Scheidler, 2019; Wesolowski, 2022.
- Factorization over $\mathbb{F}_q[X]$ with Drinfeld modules: Doliskani-Narayanan-Schost, 2019.

Drinfeld modules and elliptic curves

Number fields	**Function fields**
Base ring: $\mathbb{Z}$	Base ring: $\mathbb{F}_q[X]$
Fraction field: $\mathbb{Q}$	Fraction field: $\mathbb{F}_q(X)$
Finite extensions: number fields	Finite extensions: function fields

Elliptic curves	**Drinfeld $\mathbb{F}_q[X]$-modules, rank 2**
$\mathbb{Z}$-module law on $E(K)$	$\mathbb{F}_q[X]$-module law on K
Vélu formulae	
j-invariant encoding $\overline{\mathbb{F}_q}$-isomorphism classes	
Theory of complex multiplication	
...	

Main results [arXiv:2203.06970]

Computer algebra

- Definition & proof of a simply transitive CRS-like group action for Drinfeld modules.
- Efficient algorithm to compute the action.
- Efficient C++/NTL implementation.

Cryptography

- Reduction of the inverse problem to the isogeny-finding problem.
- Conjecture that the best (at the time) algorithm ran in exponential time.
- Wesolowski since found a polynomial algorithm (`ia.cr/2022/438`).

Software

- SageMath implementation from scratch of Drinfeld modules.
- To be integrated in SageMath.

Let's find the definition

Let $K/\mathbb{F}_q$ be a field extension with a ring morphism

$$\gamma : \mathbb{F}_q[X] \to K.$$

Fact: a Drinfeld modules ϕ induces an $\mathbb{F}_q[X]$-module structure on K.
Let's find the definition from there!

Let $a, b \in \mathbb{F}_q[X]$, $x, y \in K$, $\lambda \in \mathbb{F}_q$.

$$\begin{aligned}
(1) &\quad a \cdot (x + y) = a \cdot x + a \cdot y; \\
(2) &\quad \lambda \cdot x = \lambda x; \\
(1) + (2) \Rightarrow &\quad \text{the map } \phi_a : x \mapsto a \cdot x \text{ is in } \mathrm{End}_{\mathbb{F}_q}(K). \\
(3) &\quad a \cdot (b \cdot x) = (ab) \cdot x; \\
(1) + (2) + (3) \Rightarrow &\quad \text{the map } a \mapsto \phi_a \text{ is a ring morphism } \mathbb{F}_q[X] \to \mathrm{End}_{\mathbb{F}_q}(K).
\end{aligned}$$

We *will* define a Drinfeld module as a morphism $\mathbb{F}_q[X] \to \mathrm{End}_{\mathbb{F}_q}(K)$ with extra properties.

Endomorphisms are Ore polynomials

$$\mathrm{End}_{\mathbb{F}_q}(K) = K\{\tau\} = \left\{ \sum_{i=1}^{n} x_i \tau^n : n \geqslant 0, x_i \in K, \tau : x \mapsto x^q \right\}.$$

This is the ring of Ore polynomials; multiplication is endomorphism composition.

- Non-commutative polynomials: $\forall a \in K, \tau a = a^q \tau$.
- Left-Euclidean domain for the τ-degree.
- SageMath implementation by Caruso.

Definition

Definition

A Drinfeld module over γ is an $\mathbb{F}_q$-algebra morphism

$$\begin{aligned}\phi : \mathbb{F}_q[X] &\to K\{\tau\} \\ P &\mapsto \phi_P\end{aligned}$$

such that

$$\phi_X = a_0 + \cdots + a_r\tau^r$$

and $r > 0$, $a_0 = \gamma(X)$.

Module law

We define an $\mathbb{F}_q[X]$-module on K:

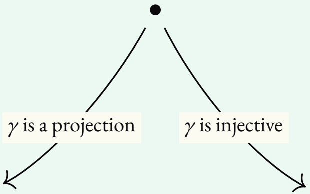
$$\begin{aligned}\mathbb{F}_q[X] \times K &\to K \\ (P, z) &\mapsto \phi_P(z).\end{aligned}$$

Example

In our case, a Drinfeld module is uniquely defined by ϕ_X.

Example

Two main situations for the base morphism $\gamma : \mathbb{F}_q[X] \to K$:



ex. $\phi_X = \overline{X} + \tau + \tau^2$

ex. $\phi_X = X + X^2\tau$

Morphisms, isogenies

Definition

A morphism of Drinfeld modules $\phi \longrightarrow \psi$ is an Ore polynomial $u \in K\{\tau\}$ such that

$$u\phi_P = \psi_P u, \quad \forall P \in \mathbb{F}_q[X],$$

i.e.

$$u\phi_X = \psi_X u.$$

An isogeny is a non-zero morphism.

Example

- $\phi_P \in \mathrm{End}(\phi)$ for all $P \in \mathbb{F}_q[X]$, i.e. $\mathbb{F}_q[X] \subset \mathrm{End}(\phi)$.
- $\mathbb{F}_q = \mathbb{F}_2$, $K = \mathbb{F}_2(i)$, $\phi_X = i + i\tau + \tau^2$, $\psi_X = i + (i+1)\tau + \tau^2$ and $u = i + t$. Then $(i+t)(i + i\tau + \tau^2) = (i+t)(i + (i+1)\tau + \tau^2)$ and u is an isogeny $\phi \longrightarrow \psi$.

Complex multiplication 1/2

Further hypotheses

- γ is surjective (ergo K is finite).
- $\mathrm{rank}(\phi) := \deg_\tau(\phi_X) = 2$.

Definition

Define the Frobenius endomorphism τ_K of ϕ as

$$\tau_K : x \mapsto x^{\#K}.$$

Theorem (Schost-Musleh)

There exists $\chi \in \mathbb{F}_q[X][T]$, *called the polynomial characteristic of the Frobenius endomorphism, such that*

$$\chi(\phi_X)(\tau_K) = 0$$

and $\chi(X)(T) = T^2 - A(X)T + B(X)$ *and* $\deg(A) \leqslant [K : \mathbb{F}_q]$, $\deg(B) \leqslant \deg(A)/2$.

Complex multiplication 2/2

Definition

ϕ is ordinary if the Frobenius trace (middle coefficient of χ) is not in $\mathrm{Ker}(\gamma)$.

The characteristic polynomial χ can be efficiently computed: Schost-Musleh, 2019.

Further hypotheses

- The curve $\mathcal{H}$ defined by χ is hyperelliptic imaginary.
- ϕ is ordinary.

Action definition

Theorem (L.-Spaenlehauer, 2022)

The class group of $\mathrm{End}(\phi)$ *acts freely and transitively on the set* S *of isomorphism classes of rank two Drinfeld module that are isogeneous to* ϕ.

Let $I \subset \mathrm{End}(\phi)$ be an ideal and ψ be a rank two Drinfeld module.
There exists (Vélu formulae) an isogeny with domain ψ whose kernel is

$$\bigcap_{f \in I} \mathrm{Ker}(f).$$

We map (I, ψ) to its codomain.

Action definition

The action is defined as the extension to class group and isomorphism classes of this map.

Representation of the class group (1/2)

$$\mathbb{F}_q[X][T]/(\chi) \simeq \mathrm{End}(\phi) \simeq \{f \in \mathbb{F}_q(\mathcal{H}) : f \text{ regular everywhere outside } \infty\}.$$

Elements of $\mathrm{Pic}^0(\mathcal{H})$ are represented by Mumford coordinates: couples $(u, v) \in \mathbb{F}_q[X]^2$ verifying:

- u is monic;
- $\deg(v) < \deg(u) \leqslant ([K : \mathbb{F}_q] - 1)/2$;
- $u \mid \chi(X, v(X))$.

$$\begin{aligned} \mathrm{Pic}^0(\mathcal{H}) &\xrightarrow{\simeq} \mathrm{Cl}\left(\mathbb{F}_q[X][T]/(\chi)\right) \\ (u, v) &\mapsto \text{class of } \langle u(X), T - v(X)\rangle, \end{aligned}$$

Representation of the class group (2/2)

$$\bigcap_{f \in I} \mathrm{Ker}(f) = \bigcap_{\bar{f} \in \text{ideal of } \mathbb{F}_q[X][T]/(\chi)} \mathrm{Ker}(f(\phi_X, \tau_K))$$
$$= \bigcap_{f \in \langle u(X), T - v(X) \rangle} \mathrm{Ker}(f(\phi_X, \tau_K))$$
$$= \mathrm{Ker}(\phi_u) \cap \mathrm{Ker}(\tau_K - \phi_v)$$

The isogeny corresponding to this kernel (Vélu formula) is

$$\mathrm{rgcd}(\phi_u, \tau_K - \phi_v).$$

Algorithm and benchmark

Input: — Mumford coordinates $(u, v) \in \mathbb{F}_q[X]^2$.
— A j-invariant $j \in K$.

Output: A j-invariant.

$\widetilde{u} \leftarrow u(j^{-1}\tau^2 + \tau + \gamma(X)) \in K\{\tau\}$;

$\widetilde{v} \leftarrow v(j^{-1}\tau^2 + \tau + \gamma(X)) \in K\{\tau\}$;

$\iota \leftarrow \mathrm{rgcd}(\widetilde{u}, \tau^{[K:\mathbb{F}_q]} - \widetilde{v})$;

$\widehat{g} \leftarrow \iota_0^{-q}(\iota_0 + \iota_1(\gamma(X)^q - \gamma(X)))$;

$\widehat{\Delta} \leftarrow j^{-q^{\deg_\tau(\iota)}}$;

Return $\widehat{g}^{q+1}/\widehat{\Delta}$.

C++ / NTL implementation with crypto parameters: ~200 ms computation for $\mathbb{F}_q = \mathbb{F}_2$, $K = \mathbb{F}_{2^{521}}$, genus$(\mathcal{H}) = 260$ and a Jacobian with order

$$2 \times 3154131824675456726041163164150477433504949628897448652594429436560240732956 89.$$

Back to crypto

It's fast. But is it safe?

No.

Security relies on the hardness of finding a fixed-degree isogeny between two Drinfeld modules.
Write $\phi_X = \Delta\tau^2 + g\tau + \omega$, $\psi_X = \Delta'\tau^2 + g'\tau + \omega$, $\iota = \iota_a\tau^a + \cdots + \iota_0 \in L\{\tau\}$.
Then ι is an isogeny $\phi \to \psi$ *iif*

$$\begin{aligned}
\Delta' \iota_a^{q^2} - \Delta^{q^a}\iota_a &= 0, \\
\Delta' \iota_{a-1}^{q^2} - \Delta^{q^{a-1}}\iota_{a-1} &= \iota_a g^{q^a} - g' \iota_a^q, \\
\forall k \in [\![2, a]\!], \quad \Delta' \iota_{a-k}^{q^2} - \Delta^{q^{a-k}}\iota_{a-k} &= \iota_{a-k+1} g^{q^{a-k+1}} - g' \iota_{a-k+1}^q + \iota_{a-k+2}(\omega^{q^{a-k+2}} - \omega), \\
\iota_0 g + \iota_1 \omega^q &= \omega \iota_1 + g' \iota_0^q.
\end{aligned}$$

Wesolowski, 2022: this is a linear system! In our case, it is solvable in time linear of $[K : \mathbb{F}_q]$.

Demo!