Drinfeld modules
Effective class group action and implementation

Antoine Leudière

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

2022 september 23rd
The late queen and duke choose an abelian simply transitive group action \( G \times X \to X \).

- Public agreement on random \( x \in X \)
- \( a \cdot x \)
- \( b \cdot x \)
- Both calculate \( ab \cdot x \) (secret key)

**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)

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Diffie-Hellman</strong> ('76)</td>
<td>( G = \mathbb{Z}/n\mathbb{Z} )&lt;br&gt;( X = \text{cyclic group with order } n \text{ and generator } g )</td>
</tr>
<tr>
<td><strong>CRS</strong> ('96, ’04)</td>
<td>( G = \text{Cl}(\mathbb{Q}(\sqrt{-D})) )&lt;br&gt;( X = \text{subset of isomorphism classes of ordinary elliptic curves} )&lt;br&gt;Slow to run &amp; hard to know group order</td>
</tr>
<tr>
<td><strong>CSIDH</strong> ('18)</td>
<td>( G = \text{Cl}(\mathbb{Q}(\sqrt{-D})) )&lt;br&gt;( X = \text{subset of isomorphism classes of supersingular elliptic curves} )&lt;br&gt;Hard to know group order</td>
</tr>
</tbody>
</table>

**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

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

Algorithms

- Ore polynomials: Caruso-Leborgne.
- Factorization over $\mathbb{F}_q[X]$ with Drinfeld modules: Doliskani-Narayanan-Schost, 2019.
## Drinfeld modules and elliptic curves

<table>
<thead>
<tr>
<th><strong>Number fields</strong></th>
<th><strong>Function fields</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Base ring: $\mathbb{Z}$</td>
<td>Base ring: $\mathbb{F}_q[X]$</td>
</tr>
<tr>
<td>Fraction field: $\mathbb{Q}$</td>
<td>Fraction field: $\mathbb{F}_q(X)$</td>
</tr>
<tr>
<td>Finite extensions: number fields</td>
<td>Finite extensions: function fields</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Elliptic curves</strong></th>
<th><strong>Drinfeld $\mathbb{F}_q[X]$-modules, rank 2</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}$-module law on $E(K)$</td>
<td>$\mathbb{F}_q[X]$-module law on $K$</td>
</tr>
<tr>
<td>Vélu formulae</td>
<td></td>
</tr>
<tr>
<td>j-invariant encoding $\mathbb{F}_q$-isomorphism classes</td>
<td></td>
</tr>
<tr>
<td>Theory of complex multiplication</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>
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 $K/F_q$ be a field extension with a ring morphism

$$\gamma : F_q[X] \to K.$$ 

Fact: a Drinfeld module $\phi$ induces an $F_q[X]$-module structure on $K$. Let’s find the definition from there!

Let $a, b \in F_q[X], x, y \in K, \lambda \in F_q$.

(1) $a \cdot (x + y) = a \cdot x + a \cdot y$;
(2) $\lambda \cdot x = \lambda x$;
(3) $a \cdot (b \cdot x) = (ab) \cdot x$;

(1) + (2) $\Rightarrow$ the map $\phi_a : x \mapsto a \cdot x$ is in $\text{End}_{F_q}(K)$.
(3) $a \cdot (b \cdot x) = (ab) \cdot x$;

(1) + (2) + (3) $\Rightarrow$ the map $a \mapsto \phi_a$ is a ring morphism $F_q[X] \to \text{End}_{F_q}(K)$.

We will define a Drinfeld module as a morphism $F_q[X] \to \text{End}_{F_q}(K)$ with extra properties.
Endomorphisms are Ore polynomials

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

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 \( \tau \)-degree.
- SageMath implementation by Caruso.
A Drinfeld module over $\gamma$ is an $\mathbb{F}_q$-algebra morphism

$$\phi : \mathbb{F}_q[X] \to K\{\tau\}$$

$$P \mapsto \phi_P$$

such that

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

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

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

$$\mathbb{F}_q[X] \times K \to K$$

$$(P, z) \mapsto \phi_P(z).$$
In our case, a Drinfeld module is uniquely defined by $\phi_X$.

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

- $\gamma$ is injective
- $\gamma$ is a projection

Example:

- $\phi_X = \overline{X} + \tau + \tau^2$
- $\phi_X = X + X^2\tau$
Morphisms, isogenies

Definition
A morphism of Drinfeld modules $\phi \rightarrow \psi$ 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
- $\phi_P \in \text{End}(\phi)$ for all $P \in \mathbb{F}_q[X]$, i.e. $\mathbb{F}_q[X] \subset \text{End}(\phi)$.
- $\mathbb{F}_q = \mathbb{F}_2, K = \mathbb{F}_2(i), \phi_X = i + i\tau + \tau^2, \psi_X = i + (i + 1)\tau + \tau^2$ 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 $\phi \rightarrow \psi$. 
Complex multiplication 1/2

Further hypotheses

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

Definition

Define the Frobenius endomorphism $\tau_K$ of $\phi$ 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 $\deg(A) \leq [K : \mathbb{F}_q]$, $\deg(B) \leq \deg(A)/2$. 

Antoine Leudière
**Definition**

\( \phi \) is **ordinary** if the Frobenius trace (middle coefficient of \( \chi \)) is not in \( \text{Ker}(\gamma) \).

The characteristic polynomial \( \chi \) can be efficiently computed: Schost-Musleh, 2019.

**Further hypotheses**

- The curve \( \mathcal{H} \) defined by \( \chi \) is hyperelliptic imaginary.
- \( \phi \) is ordinary.
Theorem (L.-Spaenlehauer, 2022)

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

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

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

We map $(I, \psi)$ 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)

\[ \mathbb{F}_q[X][T]/(\chi) \cong \text{End}(\phi) \cong \{ f \in \mathbb{F}_q(H_f) : f \text{ regular everywhere outside } \infty \} . \]

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

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

\[ \text{Pic}^0(\mathcal{H}) \overset{\sim}{\rightarrow} \text{Cl} \left( \mathbb{F}_q[X][T]/(\chi) \right) \]

\((u, v) \mapsto \text{class of } \langle u(X), T - v(X) \rangle\),
Representation of the class group (2/2)

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

The isogeny corresponding to this kernel (Vélu formula) is

\[ \text{rgcd}(\phi_u, \tau_K - \phi_v). \]
Algorithm and benchmark

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

Output: A \(j\)-invariant.

1 \(\tilde{u} \leftarrow u(j^{-1}\tau^2 + \tau + \gamma(X)) \in K\{\tau}\);
2 \(\tilde{v} \leftarrow v(j^{-1}\tau^2 + \tau + \gamma(X)) \in K\{\tau}\);
3 \(\iota \leftarrow \text{rgcd}(\tilde{u}, \tau[K:\mathbb{F}_q] - \tilde{v});\)
4 \(\hat{g} \leftarrow \iota_0^{-q}(\iota_0 + \iota_1(\gamma(X)^q - \gamma(X)));\)
5 \(\hat{\Delta} \leftarrow j^{-q\deg(\iota)};\)
6 Return \(\hat{g}^{q+1}/\hat{\Delta}\).

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

\[2 \times 315413182467545672604116316415047743350494962889744865259442943656024073295689.\]
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 \( \iota \) is an isogeny \( \phi \rightarrow \psi \) iff

\[
\Delta' \iota^q_a - \Delta^a \iota_a = 0, \\
\Delta' \iota^q_{a-1} - \Delta^{a-1} \iota_{a-1} = \iota_a g^q - g' \iota^q_a, \\
\forall k \in [2, a], \quad \Delta' \iota^q_{a-k} - \Delta^a \iota_{a-k} = \iota_{a-k+1} g^q_{a-k+1} - g' \iota^q_{a-k+1} + \iota_{a-k+2} (\omega g^{a-k+2} - \omega), \\
\iota_0 g + \iota_1 \omega^q = \omega \iota_1 + g' \iota^q_0.
\]

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