Isomorphism classes of polarised abelian varieties and Drinfeld modules over finite fields

Valentijn Karemaker (Utrecht University)

Joint work with Bergström – Marseglia (IMRN, 2023) and Katen – Papikian (arXiv 2209.15033)

NCTS Number Theory Seminar

11 January 2024

Abelian varieties over finite fields: set-up

Definitions

An **abelian variety** is a connected projective group variety.
The **dual variety** $A^\vee$ of an abelian variety A over a field K is such that $A^\vee(\overline{K}) = \mathrm{Pic}^0(A_{\overline{K}})$.
A **polarisation** of an abelian variety A is an isogeny $\mu : A \to A^\vee$ such that there exists an ample line bundle $\mathcal{L}$ on $A_{\overline{K}}$ such that $\mu_{\overline{K}}$ equals $\varphi_{\mathcal{L}} : A \to A^\vee, x \mapsto [t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}]$.

Abelian varieties over finite fields: set-up

Definitions

An **abelian variety** is a connected projective group variety.
The **dual variety** $A^\vee$ of an abelian variety A over a field K is such that $A^\vee(\overline{K}) = \mathrm{Pic}^0(A_{\overline{K}})$.
A **polarisation** of an abelian variety A is an isogeny $\mu : A \to A^\vee$ such that there exists an ample line bundle $\mathcal{L}$ on $A_{\overline{K}}$ such that $\mu_{\overline{K}}$ equals $\varphi_{\mathcal{L}} : A \to A^\vee, x \mapsto [t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}]$.

When $K = \mathbb{F}_q$ is a finite field, abelian varieties over K are partitioned into **isogeny classes**.

Important open problem

Describe and compute (polarised!) isomorphism classes within a fixed polarised isogeny class.

Preliminaries: Complex multiplication

Definitions

A **CM-field** $L/\mathbb{Q}$ is a totally imaginary quadratic extension L/L' of a totally real extension $L'/\mathbb{Q}$. It has a canonical involution $x \mapsto \overline{x}$.
A **CM-algebra** is a finite product of CM-fields.
A **CM-type** for a CM-algebra L is a subset $\Phi \subseteq \mathrm{Hom}(L, \overline{\mathbb{Q}})$ so that

$$\mathrm{Hom}(L, \overline{\mathbb{Q}}) = \Phi \coprod \overline{\Phi}.$$

Preliminaries: Complex multiplication

Definitions

A **CM-field** $L/\mathbb{Q}$ is a totally imaginary quadratic extension L/L' of a totally real extension $L'/\mathbb{Q}$. It has a canonical involution $x \mapsto \overline{x}$.

A **CM-algebra** is a finite product of CM-fields.

A **CM-type** for a CM-algebra L is a subset $\Phi \subseteq \mathrm{Hom}(L, \overline{\mathbb{Q}})$ so that

$$\mathrm{Hom}(L, \overline{\mathbb{Q}}) = \Phi \coprod \overline{\Phi}.$$

An abelian variety A over K of dimension g **has CM (by** (L, Φ)**)** if

$$L \subseteq \mathrm{End}^0(A) := \mathrm{End}(A) \otimes \mathbb{Q}.$$

Preliminaries: Complex multiplication

Definitions

A **CM-field** $L/\mathbb{Q}$ is a totally imaginary quadratic extension L/L' of a totally real extension $L'/\mathbb{Q}$. It has a canonical involution $x \mapsto \overline{x}$.

A **CM-algebra** is a finite product of CM-fields.

A **CM-type** for a CM-algebra L is a subset $\Phi \subseteq \mathrm{Hom}(L, \overline{\mathbb{Q}})$ so that

$$\mathrm{Hom}(L, \overline{\mathbb{Q}}) = \Phi \coprod \overline{\Phi}.$$

An abelian variety A over K of dimension g **has CM (by** (L, Φ)**)** if

$$L \subseteq \mathrm{End}^0(A) := \mathrm{End}(A) \otimes \mathbb{Q}.$$

Fact

Every abelian variety over a finite field has CM.

Complex uniformisation

Consider an abelian variety A over $\mathbb{C}$ of dimension g.
By **complex uniformisation**, we have

$$A(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda, \qquad \Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}.$$

Complex uniformisation

Consider an abelian variety A over $\mathbb{C}$ of dimension g.
By **complex uniformisation**, we have

$$A(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda, \qquad \Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}.$$

When A has CM by (L, Φ), we can say more:
There exists a fractional ideal I in L such that $A(\mathbb{C}) \simeq \mathbb{C}^g/\Phi(I)$.
Then also $A^\vee(\mathbb{C}) \simeq \mathbb{C}^g/\Phi(\bar{I}^t)$, where t is the trace dual. Hence,

$$\mathrm{Hom}_L(A, A^\vee) \leftrightarrow (\bar{I}^t : I) := \{x \in L : xI \subseteq \bar{I}^t\}.$$

Complex uniformisation

Consider an abelian variety A over $\mathbb{C}$ of dimension g.
By **complex uniformisation**, we have

$$A(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda, \qquad \Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}.$$

When A has CM by (L, Φ), we can say more:
There exists a fractional ideal I in L such that $A(\mathbb{C}) \simeq \mathbb{C}^g/\Phi(I)$.
Then also $A^\vee(\mathbb{C}) \simeq \mathbb{C}^g/\Phi(\bar{I}^t)$, where t is the trace dual. Hence,

$$\mathrm{Hom}_L(A, A^\vee) \leftrightarrow (\bar{I}^t : I) := \{x \in L : xI \subseteq \bar{I}^t\}.$$

Definition/construction

Let A be a g-dimensional abelian variety over a p-adic field K and with CM by (L, Φ). Form $A_{\mathbb{C}} = A \otimes \mathbb{C}$; then $A_{\mathbb{C}}(\mathbb{C}) \simeq \mathbb{C}^g/\Phi(I)$.
Write $\mathcal{H}(A) := I$. Then $\mathcal{H}(A^\vee) = \bar{I}^t$ and

$$\mathcal{H}(\mathrm{Hom}_L(A, A^\vee)) := \mathrm{Hom}_L(\mathcal{H}(A), \mathcal{H}(A^\vee)) = (\bar{I}^t : I).$$

Polarisations in characteristic zero

Let $\mathcal{H}(A) = I$, so $\mathcal{H}(A^\vee) = \bar{I}^t$ and $\mathcal{H}(\mathrm{Hom}_L(A, A^\vee)) = (\bar{I}^t : I)$.

By definition, $\{$ polarisations of A $\} \subseteq \mathrm{Hom}(A, A^\vee)$.

Polarisations in characteristic zero

Let $\mathcal{H}(A) = I$, so $\mathcal{H}(A^\vee) = \bar{I}^t$ and $\mathcal{H}(\mathrm{Hom}_L(A, A^\vee)) = (\bar{I}^t : I)$.

By definition, $\{$ polarisations of A $\} \subseteq \mathrm{Hom}(A, A^\vee)$.

Proposition

Let A be a g-dimensional abelian variety over a p-adic field K and with CM by (L, Φ). An L-linear isogeny $\mu : A \to A^\vee \in \mathrm{Hom}(A, A^\vee)$ is a polarisation if and only if:

- $\mathcal{H}(\mu) = \lambda \in L$ is **totally imaginary** (i.e. $\bar{\lambda} = -\lambda$);
- λ is **Φ-positive** (i.e. $\mathrm{Im}(\varphi(\lambda)) > 0$ for all $\varphi \in \Phi$).

(towards) Polarisations in characteristic p

Goal

Describe and compute polarisations of abelian varieties over finite fields $K = \mathbb{F}_q$.

Every $A/\mathbb{F}_q$ has a Frobenius endomorphism π_A with characteristic polynomial $h_A(x) \in \mathbb{Z}[x]$, which is an isogeny invariant:
By Honda-Tate theory, $\{$ isogeny classes $\} \leftrightarrow \{$ char. poly's h_A $\}$.

(towards) Polarisations in characteristic p

Goal

Describe and compute polarisations of abelian varieties over finite fields $K = \mathbb{F}_q$.

Every $A/\mathbb{F}_q$ has a Frobenius endomorphism π_A with characteristic polynomial $h_A(x) \in \mathbb{Z}[x]$, which is an isogeny invariant:
By Honda-Tate theory, $\{$ isogeny classes $\} \leftrightarrow \{$ char. poly's h_A $\}$.

Idea

Give analogous construction to $\mathcal{H}$ for abelian varieties in characteristic p, to describe $\mathrm{Hom}(A, A^\vee) \supseteq \{$ polarisations of A $\}$.

We will use the Centeleghe-Stix equivalence.

Categorical equivalence of Centeleghe-Stix

For this, we need to restrict to abelian varieties A_0 over $\mathbb{F}_p$ such that h_{A_0} is squarefree ($\Leftrightarrow \mathrm{End}(A_0)$ is commutative).

Categorical equivalence of Centeleghe-Stix

For this, we need to restrict to abelian varieties A_0 over $\mathbb{F}_p$ such that h_{A_0} is squarefree ($\Leftrightarrow \mathrm{End}(A_0)$ is commutative).

C-S equivalence

Fix an h as above, or equivalently an isogeny class AV_h.
Let $L := \mathbb{Q}[x]/(h) = \mathbb{Q}[F]$ and $V := p/F$.
Any $A_0 \in \mathrm{AV}_h$ has $\mathrm{End}(A_0) \supseteq \mathbb{Z}[F, V]$.
Choose $A_h \in \mathrm{AV}_h$ with $\mathrm{End}(A_h) = \mathbb{Z}[F, V]$.
Then the functor

$$\begin{aligned} \mathcal{G} : \mathrm{AV}_h &\to \{ \text{ fractional } \mathbb{Z}[F, V]\text{-ideals } \} \\ A_0 &\mapsto \mathrm{Hom}(A_0, A_h), \text{ embedded into } L \end{aligned}$$

is an equivalence of categories.

Properties of the equivalence

We have the equivalence

$$\begin{aligned} \mathcal{G} : \mathrm{AV}_h &\to \{ \text{ fractional } \mathbb{Z}[F, V]\text{-ideals } \} \\ A_0 &\mapsto \mathrm{Hom}(A_0, A_h), \text{ embedded into } L \end{aligned}$$

There are some choices involved here:

- Choosing A_h: these form a $\mathrm{Pic}(\mathbb{Z}[F, V])$-orbit;
- Choosing an embedding into L.

Properties of the equivalence

We have the equivalence

$$\begin{aligned}\mathcal{G} : \mathrm{AV}_h &\to \{ \text{ fractional } \mathbb{Z}[F, V]\text{-ideals } \} \\ A_0 &\mapsto \mathrm{Hom}(A_0, A_h), \text{ embedded into } L\end{aligned}$$

There are some choices involved here:

- Choosing A_h: these form a $\mathrm{Pic}(\mathbb{Z}[F, V])$-orbit;
- Choosing an embedding into L.

Choosing well, we can ensure that $\mathcal{G}(A_0^\vee) = \overline{\mathcal{G}(A_0)}^t$ and hence

$$\mathcal{G}(\mathrm{Hom}_L(A_0, A_0^\vee)) := (\mathcal{G}(A_0) : \mathcal{G}(A_0^\vee)) = (\mathcal{G}(A_0) : \overline{\mathcal{G}(A_0)}^t).$$

Compare: $\mathcal{H}(\mathrm{Hom}(A, A^\vee)) = (\bar{I}^t : I)$.

Properties of the equivalence

We have the equivalence

$$\begin{aligned} \mathcal{G} : \mathrm{AV}_h &\to \{ \text{ fractional } \mathbb{Z}[F, V]\text{-ideals } \} \\ A_0 &\mapsto \mathrm{Hom}(A_0, A_h), \text{ embedded into } L. \end{aligned}$$

Assume that $\mathcal{G}(A_0^\vee) = \overline{\mathcal{G}(A_0)}^t$.

Properties of the equivalence

We have the equivalence

$$\begin{aligned}\mathcal{G} : \mathrm{AV}_h &\to \{ \text{ fractional } \mathbb{Z}[F,V]\text{-ideals } \} \\ A_0 &\mapsto \mathrm{Hom}(A_0, A_h), \text{ embedded into } L.\end{aligned}$$

Assume that $\mathcal{G}(A_0^\vee) = \overline{\mathcal{G}(A_0)}^t$.

For $f : A_0 \to B_0$ and $f^\vee : B_0^\vee \to A_0^\vee$, we have $\mathcal{G}(f^\vee) = \overline{\mathcal{G}(f)}$. Also:

$$\begin{array}{ccc} \mathrm{Hom}(B_0, B_0^\vee) & \xrightarrow{f^*} & \mathrm{Hom}(A_0, A_0^\vee) \\ \downarrow \mathcal{G} & & \downarrow \mathcal{G} \\ (\mathcal{G}(B_0) : \overline{\mathcal{G}(B_0)}^t) & \xrightarrow{\mathcal{G}(f^*)} & (\mathcal{G}(A_0) : \overline{\mathcal{G}(A_0)}^t) \end{array}$$

where $f^* : \varphi \mapsto f^\vee \varphi f$, so $\mathcal{G}(f^*)$ is multiplication by $\mathcal{G}(f)\overline{\mathcal{G}(f)} \in L$.

Canonical liftings

Now $(\mathcal{G}(A_0) : \overline{\mathcal{G}(A_0)}^t) = \mathcal{G}(\mathrm{Hom}(A_0, A_0^\vee)) \supseteq \mathcal{G}(\text{polarisations})$.

Idea

Lift to characteristic zero to access the description of polarisations.
N.B.: $\mathrm{Hom}(A_0, A_0^\vee)$ should be preserved by the lifting process.

Canonical liftings

Now $(\mathcal{G}(A_0) : \overline{\mathcal{G}(A_0)}^t) = \mathcal{G}(\mathrm{Hom}(A_0, A_0^\vee)) \supseteq \mathcal{G}(\text{polarisations})$.

Idea

Lift to characteristic zero to access the description of polarisations. N.B.: $\mathrm{Hom}(A_0, A_0^\vee)$ should be preserved by the lifting process.

Definition

A **canonical lifting** of $A_0/\mathbb{F}_q$ to a local domain $\mathcal{R}$ of characteristic zero with residue field $\mathbb{F}_q$ and fraction field K is an abelian scheme $\mathcal{A}/\mathcal{R}$ such that $\mathrm{End}(A_0) = \mathrm{End}(\mathcal{A})$ and $\mathcal{A} \otimes \mathbb{F}_q \simeq A_0$, $\mathcal{A} \otimes K \simeq A$.

N.B. : We may view $\mathrm{End}(A_0)$ as an order in $L \simeq \mathrm{End}^0(A_0)$; these identifications can be made compatibly with $\mathcal{G}$ and $\mathcal{H}$.

Characteristic p versus characteristic zero

Proposition

If $A_0/\mathbb{F}_q$ has a canonical lifting to A/K, or equivalently if A/K with CM by L has good reduction to $A_0/\mathbb{F}_q$, and if

$$\mathrm{End}(A^\vee) \simeq \mathrm{End}(A) \simeq \mathrm{End}(A_0) \simeq \mathrm{End}(A_0^\vee)$$

and it's Gorenstein, then reduction $\mathrm{Hom}_L(A, A^\vee) \to \mathrm{Hom}_L(A_0, A_0^\vee)$ is multiplication by some $\alpha \in \mathrm{End}(A_0)^*$.

Characteristic p versus characteristic zero

Proposition

If $A_0/\mathbb{F}_q$ has a canonical lifting to A/K, or equivalently if A/K with CM by L has good reduction to $A_0/\mathbb{F}_q$, and if

$$\mathrm{End}(A^\vee) \simeq \mathrm{End}(A) \simeq \mathrm{End}(A_0) \simeq \mathrm{End}(A_0^\vee)$$

and it's Gorenstein, then reduction $\mathrm{Hom}_L(A, A^\vee) \to \mathrm{Hom}_L(A_0, A_0^\vee)$ is multiplication by some $\alpha \in \mathrm{End}(A_0)^*$.

$$\begin{tikzcd}
 & \mathrm{Hom}(A_K, A_K^\vee) \arrow[d, "\mathrm{red}"'] \arrow[dr, "\mathscr{H}"] & \\
\mathrm{Hom}(B_0, B_0^\vee) \arrow[r, "f^*"] \arrow[d, "\mathscr{G}"] & \mathrm{Hom}(A_0, A_0^\vee) \arrow[d, "\mathscr{G}"] & (\bar{I}^t : I) \arrow[d, "\alpha"'] \\
(\mathscr{G}(B_0) : \mathscr{G}(B_0^\vee)) \arrow[r, "\mathscr{G}(f)^*"] & (\mathscr{G}(A_0) : \mathscr{G}(A_0^\vee)) \arrow[r, equal] & (\bar{I}^t : I)
\end{tikzcd}$$

Main result: describing polarisations

Lemmas

1. Let $f : A_0 \to B_0$ and $\mu_0 : B_0 \to B_0^\vee$ be isogenies. Then μ_0 is a polarisation $\Leftrightarrow f^*\mu_0 = f^\vee \mu_0 f$ is a polarisation.
2. Let $\mu : A \to A^\vee$ be an isogeny and $\mu_0 : A_0 \to A_0^\vee$ its reduction. Then μ is a polarisation $\Leftrightarrow \mu_0$ is a polarisation.
3. The element $\alpha \in \mathrm{End}(A) = \mathrm{End}(A_0)$ is totally real: $\overline{\alpha} = \alpha$.

Main result: describing polarisations

Lemmas

1. Let $f : A_0 \to B_0$ and $\mu_0 : B_0 \to B_0^\vee$ be isogenies. Then μ_0 is a polarisation $\Leftrightarrow f^*\mu_0 = f^\vee \mu_0 f$ is a polarisation.
2. Let $\mu : A \to A^\vee$ be an isogeny and $\mu_0 : A_0 \to A_0^\vee$ its reduction. Then μ is a polarisation $\Leftrightarrow \mu_0$ is a polarisation.
3. The element $\alpha \in \mathrm{End}(A) = \mathrm{End}(A_0)$ is totally real: $\overline{\alpha} = \alpha$.

Theorem

Let h be a squarefree characteristic polynomial corresponding to the isogeny class AV_h over $\mathbb{F}_p$. Let $L \simeq \mathbb{Q}[x]/(h)$ and choose a CM-type Φ for L. Let $S = \overline{S}$ be a Gorenstein order in L such that there is an $A_0 \in \mathrm{AV}_h$ with $\mathrm{End}(A_0) = S$ which admits a canonical lifting to a p-adic field K.

Main result: describing polarisations

Lemmas

1. Let $f : A_0 \to B_0$ and $\mu_0 : B_0 \to B_0^\vee$ be isogenies. Then μ_0 is a polarisation $\Leftrightarrow f^*\mu_0 = f^\vee \mu_0 f$ is a polarisation.
2. Let $\mu : A \to A^\vee$ be an isogeny and $\mu_0 : A_0 \to A_0^\vee$ its reduction. Then μ is a polarisation $\Leftrightarrow \mu_0$ is a polarisation.
3. The element $\alpha \in \mathrm{End}(A) = \mathrm{End}(A_0)$ is totally real: $\overline{\alpha} = \alpha$.

Theorem

Let h be a squarefree characteristic polynomial corresponding to the isogeny class AV_h over $\mathbb{F}_p$. Let $L \simeq \mathbb{Q}[x]/(h)$ and choose a CM-type Φ for L. Let $S = \overline{S}$ be a Gorenstein order in L such that there is an $A_0 \in \mathrm{AV}_h$ with $\mathrm{End}(A_0) = S$ which admits a canonical lifting to a p-adic field K. Then there exists a totally real $\alpha \in S^*$ such that for **any** $B_0 \in \mathrm{AV}_h$ and any isogeny $\mu_0 : B_0 \to B_0^\vee$, μ_0 is a polarisation $\Leftrightarrow \alpha^{-1}\mathcal{G}(\mu) \in L$ is totally imaginary and Φ-positive.

When do canonical liftings exist?

Known results

1. (Serre-Tate) Every **ordinary** AV has a canonical lifting.
2. (Oswal-Shankar and BKM) Every **almost-ordinary** AV with commutative endomorphism ring has a canonical lifting.
3. (Bhatnagar-Fu) Certain abelian varieties with **real multiplication** have a canonical lifting.
4. (Chai-Conrad-Oort) Let h be irreducible, $L = \mathbb{Q}[x]/(h) = \mathbb{Q}[\pi]$ and Φ a CM-type such that (L, Φ) satisfies the **residual reflex condition (RRC)**.
   Then the isogeny class corresponding to h contains an $A_0/\mathbb{F}_q$ such that $\mathrm{End}(A_0) = \mathcal{O}_L$ which has a canonical lifting.

When do canonical liftings exist?

Known results

1. (Serre-Tate) Every **ordinary** AV has a canonical lifting.
2. (Oswal-Shankar and BKM) Every **almost-ordinary** AV with commutative endomorphism ring has a canonical lifting.
3. (Bhatnagar-Fu) Certain abelian varieties with **real multiplication** have a canonical lifting.
4. (Chai-Conrad-Oort) Let h be irreducible, $L = \mathbb{Q}[x]/(h) = \mathbb{Q}[\pi]$ and Φ a CM-type such that (L, Φ) satisfies the **residual reflex condition (RRC)**.
   Then the isogeny class corresponding to h contains an $A_0/\mathbb{F}_q$ such that $\mathrm{End}(A_0) = \mathcal{O}_L$ which has a canonical lifting.

- We generalised the RRC to squarefree h.
- Any AV separably isogenous to A_0 then also has a lifting.
- We implemented the (generalised) RRC in Magma.

Computation of polarisations

Under the assumptions of our theorem, there exists totally real $\alpha \in S^*$ such that $\mu_0 : B_0 \to B_0^\vee$ is a polarisation if and only if $\alpha^{-1}\mathcal{G}(\mu_0) \in L$ is totally imaginary and Φ-positive.

Computation of polarisations

Under the assumptions of our theorem, there exists totally real $\alpha \in S^*$ such that $\mu_0 : B_0 \to B_0^\vee$ is a polarisation if and only if $\alpha^{-1}\mathcal{G}(\mu_0) \in L$ is totally imaginary and Φ-positive.

To find all (principal) polarisations of B_0 starting with a given $\mathcal{G}(\mu_0) = i_0 \in L^*$, we need to compute

$\{ i_0 u : u \in \mathrm{End}(B_0)^*/\langle \nu\overline{\nu}\rangle$ s.t. $\alpha^{-1} i_0 u$ totally imaginary and Φ-positive $\}$.

- $(B_0, \mu_0) \simeq (B_0, \mu_0') \Leftrightarrow \exists \nu \in \mathrm{End}(B_0)^*$ s.t. $\mathcal{G}(\mu_0) = \nu\overline{\nu}\mathcal{G}(\mu_0')$.
- Can often ignore α! E.g. if an AV with $\mathrm{End} = \mathbb{Z}[F, V]$ lifts.

Aggregate examples

squarefree dimension 3			$p=2$	$p=3$	$p=5$	$p=7$
total			185	621	2863	7847
ordinary			82	390	2280	6700
almost ordinary			58	170	474	996
p-rank 1	no RRC		0	0	0	0
	yes RRC	5.5.2(R_w) yes	20	26	76	118
		5.5.2(R_w) no	4	16	12	8
p-rank 0	no RRC		0	3	2	1
	yes RRC	5.5.2(R_w) yes	20	15	17	23
		5.5.2(R_w) no	1	1	2	1

Aggregate examples

squarefree dimension 3			$p=2$	$p=3$	$p=5$	$p=7$
total			185	621	2863	7847
ordinary			82	390	2280	6700
almost ordinary			58	170	474	996
p-rank 1	no RRC		0	0	0	0
	yes RRC	5.5.2(R_w) yes	20	26	76	118
		5.5.2(R_w) no	4	16	12	8
p-rank 0	no RRC		0	3	2	1
	yes RRC	5.5.2(R_w) yes	20	15	17	23
		5.5.2(R_w) no	1	1	2	1

squarefree dimension 4			$p=2$	$p=3$
total			1431	10453
ordinary			656	6742
almost ordinary			392	2506
p-rank 2	no RRC		0	0
	yes RRC	5.5.2(R_w) yes	149	500
		5.5.2(R_w) no	49	312
p-rank 1	no RRC		6	36
	yes RRC	5.5.2(R_w) yes	80	184
		5.5.2(R_w) no	14	40
p-rank 0	no RRC		3	6
	yes RRC	5.5.2(R_w) yes	73	88
		5.5.2(R_w) no	9	39

Drinfeld modules over finite fields: set-up

We fix some notation:

- $A = \mathbb{F}_q[T]$, $F = \mathbb{F}_q(T)$.
- $\mathfrak{p} \trianglelefteq A$ is a prime of degree d, monic generator denoted by $\mathfrak{p}$.
- $k \cong \mathbb{F}_{q^n}$ is a finite extension of $A/\mathfrak{p} = \mathbb{F}_\mathfrak{p} \cong \mathbb{F}_{q^d}$.
- $\gamma\colon A \to A/\mathfrak{p} \hookrightarrow k$ is the A-field structure on k.

Drinfeld modules over finite fields: set-up

We fix some notation:

- $A = \mathbb{F}_q[T]$, $F = \mathbb{F}_q(T)$.
- $\mathfrak{p} \trianglelefteq A$ is a prime of degree d, monic generator denoted by $\mathfrak{p}$.
- $k \cong \mathbb{F}_{q^n}$ is a finite extension of $A/\mathfrak{p} = \mathbb{F}_{\mathfrak{p}} \cong \mathbb{F}_{q^d}$.
- $\gamma\colon A \to A/\mathfrak{p} \hookrightarrow k$ is the A-field structure on k.

Let $\phi : A \to k\{\tau\}$ be a Drinfeld module over k of rank r,
with $\mathcal{E} := \mathrm{End}_k(\phi)$ and $D := \mathcal{E} \otimes_A F = \mathrm{End}_k^0(\phi)$.
Let $\pi = \tau^n$ be the Frobenius endomorphism of k.

$$\begin{tikzcd}
 & D \arrow[d, dash] & \\
 & \tilde{F} = F(\pi) \arrow[dl, dash] \arrow[dr, dash] & \\
F & & K = \mathbb{F}_q(\pi)
\end{tikzcd}$$

We will consider the case where $D = \tilde{F}$ is commutative.

Guiding questions

The minimal polynomial of π over F determines an **isogeny class** of Drinfeld modules over k.

Important open problem

Describe, determine, and count the isomorphism classes within a fixed isogeny class.

Guiding questions

The minimal polynomial of π over F determines an **isogeny class** of Drinfeld modules over k.

Important open problem

Describe, determine, and count the isomorphism classes within a fixed isogeny class.

- Brute force results for $r = 2, 3$. [Assong].
- Description of endomorphism rings due to Anglès, Garai-Papikian, Kuhn-Pink, and others.
- Related to calculating zeta functions of Drinfeld modular varieties.

Isogenies, subgroups, lattices, ideals [Laumon]

Let $u : \phi \to \psi$ be an isogeny of Drinfeld modules of rank r over k. The kernel of $u \in k\{\tau\}$ is a finite group scheme G_u in A-modules.

Isogenies, subgroups, lattices, ideals [Laumon]

Let $u : \phi \to \psi$ be an isogeny of Drinfeld modules of rank r over k. The kernel of $u \in k\{\tau\}$ is a finite group scheme G_u in A-modules.

Let $H_\mathfrak{p}$ denote the Dieudonné module and $T_\mathfrak{l}$ the Tate module. Via injective maps $u_\mathfrak{p} : H_\mathfrak{p}(\psi) \hookrightarrow H_\mathfrak{p}(\phi)$ and $u_\mathfrak{l} : T_\mathfrak{l}(\phi) \hookrightarrow T_\mathfrak{l}(\psi)$ for $\mathfrak{l} \neq \mathfrak{p}$, we find sublattices $M_\mathfrak{p} := u_\mathfrak{p}(H_\mathfrak{p}(\psi)) \subseteq H_\mathfrak{p}(\phi)$ and $M_\mathfrak{l} := \mathrm{Hom}(u_\mathfrak{l}^{-1} T_\mathfrak{l}(\psi), A_\mathfrak{l}) \subseteq \mathrm{Hom}(T_\mathfrak{l}(\phi), A_\mathfrak{l}) =: H_\mathfrak{l}(\phi)$ for $\mathfrak{l} \neq \mathfrak{p}$, and hence a sublattice $M := \prod_\mathfrak{l} M_\mathfrak{l} \subseteq \prod_\mathfrak{l} H_\mathfrak{l}(\phi) =: \mathbb{H}(\phi)$.
By construction, $G_u \simeq \prod_{\mathfrak{l} \neq \mathfrak{p}} H_\mathfrak{l}(\phi)/M_\mathfrak{l} \times H_\mathfrak{p}(\phi)/M_\mathfrak{p} = \mathbb{H}(\phi)/M$.

Isogenies, subgroups, lattices, ideals [Laumon]

Let $u : \phi \to \psi$ be an isogeny of Drinfeld modules of rank r over k. The kernel of $u \in k\{\tau\}$ is a finite group scheme G_u in A-modules.

Let $H_{\mathfrak{p}}$ denote the Dieudonné module and $T_{\mathfrak{l}}$ the Tate module. Via injective maps $u_{\mathfrak{p}} : H_{\mathfrak{p}}(\psi) \hookrightarrow H_{\mathfrak{p}}(\phi)$ and $u_{\mathfrak{l}} : T_{\mathfrak{l}}(\phi) \hookrightarrow T_{\mathfrak{l}}(\psi)$ for $\mathfrak{l} \neq \mathfrak{p}$, we find sublattices $M_{\mathfrak{p}} := u_{\mathfrak{p}}(H_{\mathfrak{p}}(\psi)) \subseteq H_{\mathfrak{p}}(\phi)$ and $M_{\mathfrak{l}} := \mathrm{Hom}(u_{\mathfrak{l}}^{-1} T_{\mathfrak{l}}(\psi), A_{\mathfrak{l}}) \subseteq \mathrm{Hom}(T_{\mathfrak{l}}(\phi), A_{\mathfrak{l}}) =: H_{\mathfrak{l}}(\phi)$ for $\mathfrak{l} \neq \mathfrak{p}$, and hence a sublattice $M := \prod_{\mathfrak{l}} M_{\mathfrak{l}} \subseteq \prod_{\mathfrak{l}} H_{\mathfrak{l}}(\phi) =: \mathbb{H}(\phi)$. By construction, $G_u \simeq \prod_{\mathfrak{l} \neq \mathfrak{p}} H_{\mathfrak{l}}(\phi)/M_{\mathfrak{l}} \times H_{\mathfrak{p}}(\phi)/M_{\mathfrak{p}} = \mathbb{H}(\phi)/M$.

For an ideal $I \trianglelefteq \mathcal{E}$, we have $k\{\tau\}I = k\{\tau\}u_I$ for some $u_I \in k\{\tau\}$. The sublattice corresponding to u_I is $I\mathbb{H}(\phi) = \prod_{\mathfrak{l}} IH_{\mathfrak{l}}(\phi)$, since $\ker(u_I) = \phi[I] = \cap_{\alpha \in I} \ker(\alpha)$.

Ideal action on isomorphism classes [Hayes]

Recall $\phi : A \to k\{\tau\}$ is a Drinfeld module with $\mathcal{E} := \mathrm{End}_k(\phi)$.
For an ideal $I \trianglelefteq \mathcal{E}$, again write $k\{\tau\}I = k\{\tau\}u_I$ with $u_I \in k\{\tau\}$.

A Drinfeld module over k is determined by its value at T.
Setting $\psi_T = u_I \phi_T u_I^{-1}$ determines a Drinfeld module ψ over k, isogenous to ϕ via $u_I : \phi \to \psi$. We write $\psi = I * \phi$.

Ideal action on isomorphism classes [Hayes]

Recall $\phi : A \to k\{\tau\}$ is a Drinfeld module with $\mathcal{E} := \mathrm{End}_k(\phi)$.
For an ideal $I \trianglelefteq \mathcal{E}$, again write $k\{\tau\}I = k\{\tau\}u_I$ with $u_I \in k\{\tau\}$.

A Drinfeld module over k is determined by its value at T.
Setting $\psi_T = u_I \phi_T u_I^{-1}$ determines a Drinfeld module ψ over k, isogenous to ϕ via $u_I : \phi \to \psi$. We write $\psi = I * \phi$.

Lemma

The map $I \mapsto I * \phi$ determines an action of the monoid of fractional ideals of $\mathcal{E}$ up to linear equivalence on the set of isomorphism classes in the isogeny class of ϕ whose endomorphism ring is the order of an $\mathcal{E}$-ideal (hence an overorder of $\mathcal{E}$).

When is this action free? When is it transitive?

Kernel ideals

Let $I \trianglelefteq \mathcal{E} := \mathrm{End}_k(\phi) = D \cap k\{\tau\}$ be an ideal.

Definition

The ideal I is a **kernel ideal** if any of the following equivalent properties holds:

1. $I = (k\{\tau\}I) \cap D$. (Generally $\subseteq$.) [Yu]
2. $I = \mathrm{Ann}_{\mathcal{E}}(\phi[I])$. (Generally $\subseteq$.)
3. For any $J \trianglelefteq \mathcal{E}$, we have $J\mathbb{H}(\phi) \subseteq I\mathbb{H}(\phi) \Rightarrow J \subseteq I$. ($\Leftarrow$ holds.)

Kernel ideals

Let $I \trianglelefteq \mathcal{E} := \mathrm{End}_k(\phi) = D \cap k\{\tau\}$ be an ideal.

Definition

The ideal I is a **kernel ideal** if any of the following equivalent properties holds:

1. $I = (k\{\tau\}I) \cap D$. (Generally $\subseteq$.) [Yu]
2. $I = \mathrm{Ann}_{\mathcal{E}}(\phi[I])$. (Generally $\subseteq$.)
3. For any $J \trianglelefteq \mathcal{E}$, we have $J\mathbb{H}(\phi) \subseteq I\mathbb{H}(\phi) \Rightarrow J \subseteq I$. ($\Leftarrow$ holds.)

Lemma

Upon restricting to kernel ideals, the ideal action $I \mapsto I * \phi$ is free.

Kernel ideals

Let $I \trianglelefteq \mathcal{E} := \mathrm{End}_k(\phi) = D \cap k\{\tau\}$ be an ideal.

Definition

The ideal I is a **kernel ideal** if any of the following equivalent properties holds:

1. $I = (k\{\tau\}I) \cap D$. (Generally $\subseteq$.) [Yu]
2. $I = \mathrm{Ann}_{\mathcal{E}}(\phi[I])$. (Generally $\subseteq$.)
3. For any $J \trianglelefteq \mathcal{E}$, we have $J\mathbb{H}(\phi) \subseteq I\mathbb{H}(\phi) \Rightarrow J \subseteq I$. ($\Leftarrow$ holds.)

Lemma

Upon restricting to kernel ideals, the ideal action $I \mapsto I * \phi$ is free.

Lemma

Every ideal is a kernel ideal when $\mathcal{E}$ is maximal, or when $\mathcal{E}$ is Gorenstein, e.g., when $\mathcal{E} = A[\pi]$.

Endomorphism rings (under the ideal action)

Fix an isogeny class with commutative endomorphism algebra D.
The endomorphism ring $\mathcal{E}$ of a Drinfeld module ϕ in the isogeny class is an order in D containing the minimal order $A[\pi]$.
For $I \trianglelefteq \mathcal{E}$, let $(I : I) = \{g \in D : Ig \subseteq I\}$ be its order.
Write $k\{\tau\}I = k\{\tau\}u_I$ as before.

Endomorphism rings (under the ideal action)

Fix an isogeny class with commutative endomorphism algebra D.
The endomorphism ring $\mathcal{E}$ of a Drinfeld module ϕ in the isogeny class is an order in D containing the minimal order $A[\pi]$.
For $I \trianglelefteq \mathcal{E}$, let $(I : I) = \{g \in D : Ig \subseteq I\}$ be its order.
Write $k\{\tau\}I = k\{\tau\}u_I$ as before.

Lemma, cf. [Yu] and [Waterhouse]

For any $I \trianglelefteq \mathcal{E}$, we have $\mathrm{End}_k(I * \phi) \supseteq u_I(I : I)u_I^{-1} \simeq (I : I)$.
Equality holds when I is a kernel ideal.

Endomorphism rings (under the ideal action)

Fix an isogeny class with commutative endomorphism algebra D.
The endomorphism ring $\mathcal{E}$ of a Drinfeld module ϕ in the isogeny class is an order in D containing the minimal order $A[\pi]$.
For $I \trianglelefteq \mathcal{E}$, let $(I : I) = \{g \in D : Ig \subseteq I\}$ be its order.
Write $k\{\tau\}I = k\{\tau\}u_I$ as before.

Lemma, cf. [Yu] and [Waterhouse]

For any $I \trianglelefteq \mathcal{E}$, we have $\mathrm{End}_k(I * \phi) \supseteq u_I(I : I)u_I^{-1} \simeq (I : I)$.
Equality holds when I is a kernel ideal.

Since $\mathcal{E} \subseteq (I : I)$, "endomorphism rings grow under ideal action".
For transitivity of $I \mapsto I * \phi$, every occurring endomorphism ring in the isogeny class should be an overorder of $\mathcal{E}$.
When does the minimal order $A[\pi]$ occur as endomorphism ring?

Local maximality of $A[\pi]$

$$\begin{array}{ccccc} & & D = \tilde{F} = F(\pi) & & \\ & \diagup & & \diagdown & \\ F & & & & K = \mathbb{F}_q(\pi) \end{array} \qquad \begin{array}{ccc} & \tilde{\mathfrak{p}} & \\ \diagup & & \diagdown \\ \mathfrak{p} & & (\pi) \end{array}$$

Definition, cf. [Anglès]

Let $B_{\tilde{\mathfrak{p}}}$ be the ring of integers of $\tilde{F}_{\tilde{\mathfrak{p}}} := \tilde{F} \otimes_K \mathbb{F}_q((\pi))$ and write $A[\pi]_{\tilde{\mathfrak{p}}} := A[\pi] \otimes_{\mathbb{F}_q[\pi]} \mathbb{F}_q[[\pi]]$. Then $A[\pi]$ is **locally maximal** at π if $A[\pi]_{\tilde{\mathfrak{p}}} = B_{\tilde{\mathfrak{p}}}$.

Local maximality of $A[\pi]$

$$
\begin{tikzcd}[column sep=small]
 & D = \tilde{F} = F(\pi) \arrow[dl, dash] \arrow[dr, dash] & \\
F & & K = \mathbb{F}_q(\pi)
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \tilde{\mathfrak{p}} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathfrak{p} & & (\pi)
\end{tikzcd}
$$

Definition, cf. [Anglès]

Let $B_{\tilde{\mathfrak{p}}}$ be the ring of integers of $\tilde{F}_{\tilde{\mathfrak{p}}} := \tilde{F} \otimes_K \mathbb{F}_q((\pi))$ and write $A[\pi]_{\tilde{\mathfrak{p}}} := A[\pi] \otimes_{\mathbb{F}_q[\pi]} \mathbb{F}_q[[\pi]]$. Then $A[\pi]$ is **locally maximal** at π if $A[\pi]_{\tilde{\mathfrak{p}}} = B_{\tilde{\mathfrak{p}}}$.

Theorem

Recall $\deg(\mathfrak{p}) = d$ and $k \simeq \mathbb{F}_{q^n}$. Let H be the height of ϕ.

Then $\left\lceil \frac{n}{H \cdot d} \right\rceil \leq \frac{[\tilde{F}:K]}{d}$, with equality $\Leftrightarrow$ $A[\pi]$ is locally maximal at π. Hence, $A[\pi]$ is locally maximal at $\pi \Leftrightarrow \phi$ is ordinary or $k = \mathbb{F}_{\mathfrak{p}}$.

$A[\pi]$ as an endomorphism ring

Fix an isogeny class with commutative endomorphism algebra D.

Lemma

Let R be any A-order in D containing π. There exists a Drinfeld module ϕ in the isogeny class such that $\mathrm{End}_k(\phi) = R$ if and only if R is locally maximal at π.

$A[\pi]$ as an endomorphism ring

Fix an isogeny class with commutative endomorphism algebra D.

Lemma

Let R be any A-order in D containing π. There exists a Drinfeld module ϕ in the isogeny class such that $\mathrm{End}_k(\phi) = R$ if and only if R is locally maximal at π.

At $\mathfrak{p}$, i.e. at π, any endomorphism ring is locally maximal. [Yu]
At all $\mathfrak{l} \neq \mathfrak{p}$, the order is almost always maximal and can be adjusted at the remaining places ($\leftrightarrow$ isogeny).
Theorem: $A[\pi]$ is locally maximal at $\pi \Leftrightarrow \phi$ is ordinary or $k = \mathbb{F}_{\mathfrak{p}}$.

$A[\pi]$ as an endomorphism ring

Fix an isogeny class with commutative endomorphism algebra D.

Lemma

Let R be any A-order in D containing π. There exists a Drinfeld module ϕ in the isogeny class such that $\mathrm{End}_k(\phi) = R$ if and only if R is locally maximal at π.

At $\mathfrak{p}$, i.e. at π, any endomorphism ring is locally maximal. [Yu]
At all $\mathfrak{l} \neq \mathfrak{p}$, the order is almost always maximal and can be adjusted at the remaining places ($\leftrightarrow$ isogeny).
Theorem: $A[\pi]$ is locally maximal at $\pi \Leftrightarrow \phi$ is ordinary or $k = \mathbb{F}_{\mathfrak{p}}$.

Corollary

$A[\pi]$ occurs as an endomorphism ring if and only if it is locally maximal at π, if and only if the isogeny class is ordinary or $k = \mathbb{F}_{\mathfrak{p}}$. So does any overorder of $A[\pi]$.

Main result

Theorem

Suppose that $\mathcal{E} := \mathrm{End}_k(\phi) = A[\pi]$. Then the action $I \mapsto I * \phi$ of the monoid of fractional ideals of $A[\pi]$ is free and transitive on the isomorphism classes in the isogeny class of ϕ.
In other words, all isomorphism classes in the isogeny class of ϕ are of the form $I * \phi$ for some $A[\pi]$-ideal I.

Main result

Theorem

Suppose that $\mathcal{E} := \mathrm{End}_k(\phi) = A[\pi]$. Then the action $I \mapsto I * \phi$ of the monoid of fractional ideals of $A[\pi]$ is free and transitive on the isomorphism classes in the isogeny class of ϕ.
In other words, all isomorphism classes in the isogeny class of ϕ are of the form $I * \phi$ for some $A[\pi]$-ideal I.

- If $\mathcal{E} = A[\pi]$ then ϕ is ordinary or $k = \mathbb{F}_{\mathfrak{p}}$.
- For the Gorenstein order $A[\pi]$, every ideal is a kernel ideal.
- Kernel ideals act freely.
- Kernel ideals of $A[\pi]$ act transitively on isomorphism classes whose endomorphism ring is an overorder of $A[\pi]$, i.e. on all isomorphism classes.

Example

Let $q = 2$, $k = \mathbb{F}_4$, $\mathfrak{p} = T$. Fix $\alpha \in k \setminus \mathbb{F}_q$.
Let $\phi_1 : A \to k\{\tau\}$ be the (rank 7, height 1) Drinfeld module given by $(\phi_1)_T = \alpha\tau + \tau^2 + \tau^7$. Then $\mathrm{End}_k(\phi_1) = A[\pi]$, $\pi = \tau^2$.
There are 15 isomorphism classes in the isogeny class of ϕ_1:

I	u_I	$I * \phi_1$
(1)	1	ϕ_1
(T, π)	τ	ϕ_2
$(T^2 + T, \pi^3 + 1)$	$\alpha + \tau^3$	ϕ_3
$(T^2, \pi^2 + T + 1)$	$(\alpha + 1) + (\alpha + 1)\tau + \tau^3$	ϕ_4
$(T, \pi^4 + \pi^2 + \pi + 1)$	$1 + \alpha\tau^2 + \tau^3 + \tau^4$	ϕ_5
$(T + 1, \pi^3 + \pi + 1)$	$1 + (\alpha + 1)\tau + \tau^2 + \tau^3$	ϕ_6
$(T, \pi^2 + 1)$	$(\alpha + 1) + \tau + \tau^2$	ϕ_7
$(T^2 + T, \pi^3 + \pi^2 + \pi)$	$\tau + \alpha\tau^2 + \tau^3$	ϕ_8
$(T^2, \pi^2 + \pi + T)$	$(\alpha + 1)\tau + (\alpha + 1)\tau^2 + \tau^3$	ϕ_9
$(T, \pi^6 + \pi^5 + \pi^4 + \pi)$	$(\alpha + 1)\tau + \tau^2 + \alpha\tau^3 + \tau^4 + \alpha\tau^5 + \tau^6$	ϕ_{10}
$(T, \pi^3 + \pi^2 + 1)$	$(\alpha + 1) + \tau + \alpha\tau^2 + \tau^3$	ϕ_{11}
$(T^2, \pi + T + 1)$	$\alpha + \alpha\tau + \tau^2$	ϕ_{12}
$(T + 1, \pi^5 + \pi^4 + 1)$	$1 + \tau + (\alpha + 1)\tau^2 + (\alpha + 1)\tau^4 + \tau^5$	ϕ_{13}
$(T, \pi^4 + \pi^3 + \pi)$	$\alpha\tau + \tau^2 + (\alpha + 1)\tau^3 + \tau^4$	ϕ_{14}
$(T, \pi^2 + \pi)$	$(\alpha + 1)\tau + \tau^2$	ϕ_{15}

Comparing (polarised) abelian varieties and Drinfeld modules over finite fields k

In both cases we want to describe the isomorphism classes within a fixed isogeny class, determined by π.
We get the best results when the varieties/modules are **ordinary** or when k is the **prime field**.

Comparing (polarised) abelian varieties and Drinfeld modules over finite fields k

In both cases we want to describe the isomorphism classes within a fixed isogeny class, determined by π.
We get the best results when the varieties/modules are **ordinary** or when k is the **prime field**.

Ordinary: canonical liftings exist; fractional End-ideals act on isomorphism classes – via ideal action (DM) or via complex uniformisation/Deligne's equivalence (AV).

Comparing (polarised) abelian varieties and Drinfeld modules over finite fields k

In both cases we want to describe the isomorphism classes within a fixed isogeny class, determined by π.
We get the best results when the varieties/modules are **ordinary** or when k is the **prime field**.

Ordinary: canonical liftings exist; fractional End-ideals act on isomorphism classes – via ideal action (DM) or via complex uniformisation/Deligne's equivalence (AV).

Prime fields: elements with minimal endomorphism ring are key.
Centeleghe-Stix map $A_0 \mapsto \mathrm{Hom}(A_0, A_h)$ with $\mathrm{End}(A_h) = \mathbb{Z}[F, V]$.
Cf.: If $\phi = I * \phi_w$ with $\mathrm{End}_k(\phi_w) = A[\pi]$ and I a kernel $A[\pi]$-ideal, then $\mathrm{Hom}_k(\phi, \phi_w) = I$.