Abelian varieties over finite fields isogenous to a power

Marseglia Stefano

MPI/Stockholms University

16 October 2018 - IRMAR

Introduction

Today's plan:

- Brief review of the material.
- AV A isogenous to B^r, for B ordinary square-free defined over $\mathbb{F}_q$.
- Isomorphism classes.
- Polarizations.
- Computations of polarizations and period matrices ($r = 1$).

Abelian varieties ($\mathbb{C}$ vs $\mathbb{F}_q$)

- Goal: compute **isomorphism classes** of abelian varieties over a **finite field** $\mathbb{F}_q$.
- in dimension $g > 1$ it is not easy to produce equations.
- for $g > 3$ it is not enough to consider Jacobians.
- over $\mathbb{C}$:

$$\{\text{abelian varieties } /\mathbb{C}\} \longleftrightarrow \left\{ \begin{matrix} \mathbb{C}^g/L \text{ with } L \simeq \mathbb{Z}^{2g} \\ + \text{ Riemann form} \end{matrix} \right\}.$$

- in positive characteristic we don't have such equivalence (on the whole category).

Isogeny classes

Recall

- for an abelian variety $A/\mathbb{F}_q$ there are simple B_i and positive integers e_i s.t.

$$A \sim_{\mathbb{F}_q} B_1^{e_1} \times \ldots \times B_s^{e_s} \qquad \text{Poincaré decomposition}$$

- If h_A is the characteristic polynomial of Frobenius π_A (acting on $T_l A$, for some $l \neq p$) then
  - $h_A \in \mathbb{Z}[x]$ and roots of size $\sqrt{q}$ $\qquad$ q-Weil polynomial
  - $h_A = h_{B_1}^{e_1} \cdots h_{B_s}^{e_s}$
  - $\deg h_A = 2 \dim A$.

Theorem (Honda-Tate)

There is a bijection betweeen the set of simple abelian varieties over $\mathbb{F}_q$ up to isogeny and the set of q-Weil numbers up to conjugacy.

Ordinary AV

An abelian variety $A/\mathbb{F}_q$ of dimension g is called ordinary if one of the following equivalent conditions holds:

(a) $A[p](\overline{\mathbb{F}}_p) \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^g$ (i.e. the max possible)

(b) exactly half of the roots of h_A over $\overline{\mathbb{Q}}_p$ are p-adic units

(c) the mid-coefficient of h_A is coprime with p

Proposition

For B ordinary over $\mathbb{F}_q$:

$$h_B \text{ is irreducible} \iff B \text{ is simple}$$

Deligne's equivalence

Theorem (Deligne '69)

Let $q = p^d$, with p a prime. There is an equivalence of categories:

$$\mathrm{AV}^{ord}(q) := \{\textbf{\textit{Ordinary}} \textit{ abelian varieties over } \mathbb{F}_q\}$$

$$\updownarrow$$

$$\mathscr{M}^{ord}(q) := \left\{ \begin{array}{l} \textit{pairs } (T,F)\textit{, where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \textit{ and } T \xrightarrow{F} T \textit{ s.t.} \\ \textit{- } F \otimes \mathbb{Q} \textit{ is semisimple} \\ \textit{- the roots of } \mathrm{char}_{F\otimes\mathbb{Q}}(x) \textit{ have abs. value } \sqrt{q} \\ \textbf{\textit{- half of them are p-adic units}} \\ \textit{- } \exists V : T \to T \textit{ such that } FV = VF = q \end{array} \right\}$$

Deligne's equivalence - the functor

- fix an embedding of $\varepsilon : W = W(\overline{\mathbb{F}}_p) \hookrightarrow \mathbb{C}$
- take $A \in \mathrm{AV}^{\mathrm{ord}}(q)$
- let A' be the canonical lift of A to W
- put $A_{\mathbb{C}} := A' \otimes_{\varepsilon} \mathbb{C}$
- finally, let $T(A) := H_1(A_{\mathbb{C}}, \mathbb{Z})$
- the construction is functorial: Frobenius $\pi(A) \rightsquigarrow F(A)$.

Observe if $\dim(A) = g$ then $\mathrm{Rank}(T(A)) = 2g$;

AV isogenous to a power

Today's setup:

let g be a q-Weil polynomial which is ordinary and square-free

Put

$$\mathrm{AV}(g^r) := \left\{ A \in \mathrm{AV}^{\mathrm{ord}}(q) : h_A = g^r \right\}$$

and

$$\mathscr{M}(g^r) := \left\{ (T,F) \in \mathscr{M}^{\mathrm{ord}}(q) : char_F = g^r \right\}.$$

Observe: if $A \in \mathrm{AV}(g^r)$ then

$$A \sim (B_1 \times \ldots \times B_s)^r$$

with

$$g = h_{B_1 \times \ldots \times B_s}$$

Main theorem

Consider the CM étale $\mathbb{Q}$-algebra

$$K = \mathbb{Q}[F] = {}^{\mathbb{Q}[x]}\!/_{g} \qquad \text{where } F = x \bmod g$$

and the order in K given by

$$R = \mathbb{Z}[F, V], \qquad \text{where } V = q/F = \overline{F}$$

Define

$$\mathscr{B}(g^r) := \{\text{fin. gen. torsion-free } R\text{-modules } M \text{ s.t. } M \otimes_R K \simeq K^r\}$$

Theorem (M.)

There are equivalences of categories

$$\mathrm{AV}(g^r) \overset{Deligne}{\longleftrightarrow} \mathscr{M}(g^r) \longleftrightarrow \mathscr{B}(g^r)$$

The category $\mathscr{B}(g^r)$

Recall that an R-module M is **torsion-free** if the canonical morphism

$$M \to M \otimes_R K$$

is injective.
We can think of modules $M \in \mathscr{B}(g^r)$ as **embedded** in K^r.
The category $\mathscr{B}(g^r)$ becomes more explicit and computable under certain assumption on the order R.

Bass orders

Recall

- a fractional R-ideal I is a sub-R-module of K which is also a lattice
- a fractional R-ideal is invertible in R if $I(R:I) = R$.

Define

$$\mathrm{ICM}(R) = {}^{\{\text{fractional } R\text{-ideals}\}}\big/_{\simeq_R} \qquad \text{ideal class monoid}$$

and

$$\mathrm{Pic}(R) = {}^{\{\text{fractional } R\text{-ideals invertible in } R\}}\big/_{\simeq_R} \qquad \text{Picard group}$$

An order R is called Bass if one of the following equivalent conditions holds:

- every over-order $R \subseteq S \subseteq \mathcal{O}_K$ is Gorenstein.
- every fractional R-ideal I is invertible in $(I:I)$.
- $\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathcal{O}_K} \mathrm{Pic}(S)$.

$\mathscr{B}(g^r)$ in the Bass case

Theorem (Bass)

Assume that R is a Bass order. Then for every $M \in \mathscr{B}(g^r)$ there are fractional R-ideals $I_1, \ldots, I_r$ such that

$$M \simeq_R I_1 \oplus \ldots \oplus I_r.$$

everything is a direct sum of fractional ideals

Moreover, given $M = \bigoplus_{k=1}^r I_k$ and $M' = \bigoplus_{k=1}^r J_k$ we have that

$$M \simeq_R M' \iff \begin{cases} (I_k : I_k) = (J_k : J_k) \text{ for every } k, \text{ and} \\ \prod_{k=1}^r I_k \simeq_R \prod_{k=1}^r J_k \end{cases}$$

generalization of Steinitz theory

$\mathscr{B}(g^r)$ in the Bass case

Corollary

Assume that R is Bass. Then for every $M \in \mathscr{B}(g^r)$ there are over orders $S_1 \subseteq \ldots \subseteq S_r$ of R and a fractional ideal I invertible in S_r such that

$$M \simeq S_1 \oplus \ldots \oplus S_{r-1} \oplus I$$

Simple description of morphisms in $\mathscr{B}(g^r)$.
For example, for M as above:

$$\mathrm{End}_R(M) = \begin{pmatrix} S_1 & S_2 & \ldots & S_{r-1} & I \\ (S_1 : S_2) & S_2 & \ldots & S_{r-1} & I \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ (S_1 : S_{r-1}) & (S_2 : S_{r-1}) & \ldots & S_{r-1} & I \\ (S_1 : I) & (S_2 : I) & \ldots & (S_{r-1} : I) & (I : I) \end{pmatrix}$$

and

$$\mathrm{Aut}_R(M) = \{A \in \mathrm{End}_R(M) \cap \mathrm{GL}_r(K) : A^{-1} \in \mathrm{End}_R(M)\}.$$

Consequences for $\mathrm{AV}(g^r)$

Corollary

Assume $R = \mathbb{Z}[F,V]$ is Bass. Then

- $$\mathrm{AV}(g^r)_{/\simeq} \longleftrightarrow \left\{ (S_1 \subseteq S_2 \subseteq \ldots \subseteq S_r, [I]_{\simeq}) : \begin{array}{l} R \subseteq S_1, \\ I \text{ a frac. } R\text{-ideal} \\ \text{with } (I:I) = S_r \end{array} \right\}$$

- *for every* $A \in \mathrm{AV}(g^r)$, *say* $A \sim B^r$ *with* $h_B = g$, *there are*

  $$C_1, \ldots, C_r \sim B \text{ such that } A \simeq C_1 \times \ldots \times C_r$$

  everything is a product

- *if*

  $$A \longleftrightarrow \bigoplus_k I_k \text{ and } B \longleftrightarrow \bigoplus_k J_k$$

  then $$\mu \in \mathrm{Hom}(A,B) \longleftrightarrow \Lambda \in \mathrm{Mat}_{r\times r}(K) \text{ s.t. } \Lambda_{h,k} \in (J_h : I_k)$$

  Moreover, μ *is an isogeny if and only if* $\det(\Lambda) \in K^\times$

Example

Let $g = x^6 - 3x^5 + 6x^4 - 10x^3 + 18x^2 - 27x + 27$.
Note $\mathrm{AV}(g)$ is an isogeny class of simple ordinary abelian varieties over $\mathbb{F}_3$.
Define $K = \mathbb{Q}[x]/(g) = \mathbb{Q}(F)$ and $R = \mathbb{Z}[F, V]$.
The only over-order of R is the maximal order $\mathcal{O}_K$ of K and, since R is Gorenstein R is Bass.
Observe

$$\mathrm{Pic}(R) \simeq {}^{\mathbb{Z}}\!/\!_{3\mathbb{Z}} \text{ and } \mathrm{Pic}(\mathcal{O}_K) = \{1\}.$$

Let I be a representatives of a generator of $\mathrm{Pic}(R)$.
We now list the representatives of the isomorphism classes in $\mathrm{AV}(g^3)$:

$$M_1 = R \oplus R \oplus R \qquad M_2 = R \oplus R \oplus I \qquad M_3 = R \oplus R \oplus I^2$$
$$M_4 = R \oplus R \oplus \mathcal{O}_K \qquad M_5 = R \oplus \mathcal{O}_K \oplus \mathcal{O}_K \qquad M_6 = \mathcal{O}_K \oplus \mathcal{O}_K \oplus \mathcal{O}_K$$

$$\mathrm{End}(M_1) = \mathrm{Mat}_3(R) \text{ and } \mathrm{End}(M_2) = \begin{pmatrix} R & R & I \\ R & R & I \\ (R:I) & (R:I) & R \end{pmatrix}$$

Dual modules

Let $M \in \mathscr{B}(g^r)$ and let $\mathrm{Tr} : K^r \to \mathbb{Q}$ be the map induced by $\mathrm{Tr}_{K/\mathbb{Q}}$
Put

$$M^\vee := \overline{M^t} = \{\overline{x} \in K^r : \mathrm{Tr}(xM) \subseteq \mathbb{Z}\}.$$

In particular if $M = \bigoplus_k I_k$ then $M^\vee = \bigoplus_k \overline{I_k}^t$.

Proposition

If $\mu : A \to B$ in $\mathrm{AV}(g^r)$ corresponds to $\Lambda : M \to N$ in $\mathscr{B}(g^r)$, then $\mu^\vee : B^\vee \to A^\vee$ in $\mathrm{AV}(g^r)$ corresponds to $\Lambda^\vee : N^\vee \to M^\vee$ in $\mathscr{B}(g^r)$, where

$$\Lambda^\vee := \overline{\Lambda}^T$$

"Proof": Howe (1995) described dual modules in $\mathscr{M}^{\mathrm{ord}}(q)$.

Polarizations

Fix

$$\Phi := \{\varphi : K \to \mathbb{C} : v_p(\varphi(F)) > 0\},$$ tricky to compute!

where v_p is the p-adic valuation induced by $\varepsilon : W(\overline{\mathbb{F}}_p) \hookrightarrow \mathbb{C}$.
Observe that Φ is a **CM-type** of K since the isogeny class is ordinary.

Theorem

Let $\mu : A \to A^\vee$ in $\mathrm{AV}(g^r)$ be an isogeny, corresponding to $\Lambda : M \to M^\vee$. Then μ is a polarization if and only if

- $\Lambda = -\overline{\Lambda}^T$, *and*
- *for every a in K^r, the element $c = a^T \overline{\Lambda} \overline{a}$ is Φ-non-positive, that is $\mathrm{Im}(\varphi(c)) \leq 0$ for every φ in Φ.*

We have $\deg \mu = [M^\vee : \Lambda M]$.

"Proof": Howe (1995) put polarizations in Deligne's category $\mathscr{M}^{\mathrm{ord}}(q)$.
We translated this notion to $\mathscr{B}(g^r)$.

Automorphisms

Let (M, Λ) and (M', Λ') correspond to polarized variety in $\mathrm{AV}(g^r)$.
A morphism of polarized abelian varieties is a map $\Psi : M \to M'$ such that

$$\Psi^\vee \Lambda' \Psi = \Lambda.$$

Let $\mathrm{Pol}(M)$ be the set of polarizations of M.

Theorem

There is a degree-preserving action of $\mathrm{Aut}(M)$ *on* $\mathrm{Pol}(M)$ *given by*

$$\mathrm{Aut}(M) \times \mathrm{Pol}(M) \longmapsto \mathrm{Pol}(M)$$
$$(U, \Lambda) \longmapsto U^\vee \Lambda U$$

Unfortunately

$$\mathrm{Pol}(M) \big/ \mathrm{Aut}(M) \text{ is hard to understand if } r \geq 2$$

The case $r = 1$

We don't need R Bass now!

- $$\mathrm{AV}(g)_{/\simeq} \longleftrightarrow \mathrm{ICM}(R)$$
- Concretely, if $A \leftrightarrow I$, then $A^\vee \leftrightarrow \bar{I}^t$, and
- a polarization μ of A corresponds to a $\lambda \in K^\times$ such that
  - $\lambda I \subseteq \bar{I}^t$ (isogeny);
  - λ is totally imaginary ($\bar{\lambda} = -\lambda$);
  - λ is Φ-positive, where Φ is the CM-type of K. "coming from char p"

  Also: $\deg \mu = [\bar{I}^t : \lambda I]$.
- if $(A, \mu) \leftrightarrow (I, \lambda)$ and $S = (I : I)$ then

$$\begin{Bmatrix} \text{non-isomorphic} \\ \text{polarizations of } A \end{Bmatrix} \longleftrightarrow \frac{\{\text{totally positive } u \in S^\times\}}{\{v\bar{v} : v \in S^\times\}}$$

and $\mathrm{Aut}(A, \mu) = \{\text{torsion units of } S\}$

Example

- Let $h(x) = x^8 - 5x^7 + 13x^6 - 25x^5 + 44x^4 - 75x^3 + 117x^2 - 135x + 81$;
- $\rightsquigarrow$ isogeny class of an simple ordinary abelian varieties over $\mathbb{F}_3$ of dimension 4;
- Let F be a root of $h(x)$ and put $R := \mathbb{Z}[F, 3/F] \subset \mathbb{Q}(F)$;
- 8 over-orders of R: two of them are not Gorenstein;
- $\#\mathrm{ICM}(R) = 18 \rightsquigarrow 18$ isom. classes of AV in the isogeny class;
- 5 are not invertible in their multiplicator ring;
- 8 classes admit principal polarizations;
- 10 isomorphism classes of princ. polarized AV.

Example

Concretely:

$$
\begin{aligned}
I_1 =& 2645633792595191\mathbb{Z} \oplus (F + 836920075614551)\mathbb{Z} \oplus (F^2 + 1474295643839839)\mathbb{Z} \oplus \\
&\oplus (F^3 + 1372829830503387)\mathbb{Z} \oplus (F^4 + 1072904687510)\mathbb{Z} \oplus \\
&\oplus \frac{1}{3}(F^5 + F^4 + F^3 + 2F^2 + 2F + 6704806986143610)\mathbb{Z} \oplus \\
&\oplus \frac{1}{9}(F^6 + F^5 + F^4 + 8F^3 + 2F^2 + 2991665243621169)\mathbb{Z} \oplus \\
&\oplus \frac{1}{27}(F^7 + F^6 + F^5 + 17F^4 + 20F^3 + 9F^2 + 68015312518722201)\mathbb{Z}
\end{aligned}
$$

principal polarizations:

$$
\begin{aligned}
x_{1,1} = & \frac{1}{27}(-121922F^7 + 588604F^6 - 1422437F^5 + \\
& + 1464239F^4 + 1196576F^3 - 7570722F^2 + 15316479F - 12821193) \\
x_{1,2} = & \frac{1}{27}(3015467F^7 - 17689816F^6 + 35965592F^5 - \\
& - 64660346F^4 + 121230619F^3 - 191117052F^2 + 315021546F - 300025458) \\
& \mathrm{End}(I_1) = R \\
& \#\mathrm{Aut}(I_1, x_{1,1}) = \#\mathrm{Aut}(I_1, x_{1,2}) = 2
\end{aligned}
$$

Example

$$
\begin{aligned}
I_7 = & 2\mathbb{Z} \oplus (F+1)\mathbb{Z} \oplus (F^2+1)\mathbb{Z} \oplus (F^3+1)\mathbb{Z} \oplus (F^4+1)\mathbb{Z} \oplus \frac{1}{3}(F^5+F^4+F^3+2F^2+2F+3)\mathbb{Z} \oplus \\
& \oplus \frac{1}{36}(F^6+F^5+10F^4+26F^3+2F^2+27F+45)\mathbb{Z} \oplus \\
& \oplus \frac{1}{216}(F^7+4F^6+49F^5+200F^4+116F^3+105F^2+198F+351)\mathbb{Z}
\end{aligned}
$$

principal polarization:

$$x_{7,1} = \frac{1}{54}(20F^7 - 43F^6 + 155F^5 - 308F^4 + 580F^3 - 1116F^2 + 2205F - 1809)$$

$$
\begin{aligned}
\mathrm{End}(I_7) = & \mathbb{Z} \oplus F\mathbb{Z} \oplus F^2\mathbb{Z} \oplus F^3\mathbb{Z} \oplus F^4\mathbb{Z} \oplus \frac{1}{3}(F^5+F^4+F^3+2F^2+2F)\mathbb{Z} \oplus \\
& \oplus \frac{1}{18}(F^6+F^5+10F^4+8F^3+2F^2+9F+9)\mathbb{Z} \oplus \\
& \oplus \frac{1}{108}(F^7+4F^6+13F^5+56F^4+80F^3+33F^2+18F+27)\mathbb{Z}
\end{aligned}
$$

$$\#\mathrm{Aut}(I_7, x_{7,1}) = 2$$

I_1 is invertible in R, but I_7 is not invertible in $\mathrm{End}(I_7)$.

Period matrices

We can also compute the period matrix of the canonical lifts of a principally polarized square-free ordinary abelian variety:
Assume

$$(A,\mu) \longleftrightarrow (I,\lambda)$$

Write

$$I = \alpha_1\mathbb{Z} \oplus \ldots \alpha_{2g}\mathbb{Z}$$

Let $\Phi = \{\varphi_1, \ldots, \varphi_g\}$ be the CM-type.
Let (A', μ') be the (complex) canonical lift of (A,μ).
We have an isomorphism of complex tori

$$A'(\mathbb{C}) \simeq {}^{\mathbb{C}^g}\!\big/_{\Phi(I)}, \qquad \Phi(I) = \langle(\varphi_1(\alpha_i), \ldots, \varphi_g(\alpha_i)) \qquad i = 1, \ldots, 2g\rangle\,.$$

Period matrices

The Riemann form associated to λ is given by

$$b : I \times I \to \mathbb{Z} \quad (s,t) \mapsto \mathrm{Tr}(\overline{t\lambda} s).$$

Pick a symplectic $\mathbb{Z}$-basis of I with respect to the form b, that is,

$$I = \gamma_1\mathbb{Z} \oplus \ldots \oplus \gamma_g\mathbb{Z} \oplus \beta_1\mathbb{Z} \oplus \ldots \oplus \beta_g\mathbb{Z},$$

with

$$b(\gamma_i, \beta_i) = 1 \text{ for all } i, \text{ and}$$

$$b(\gamma_h, \gamma_k) = b(\beta_h, \beta_k) = b(\gamma_h, \beta_k) = 0 \text{ for all } h \neq k.$$

Consider the $g \times 2g$ matrix Ω whose i-th row is

$$(\varphi_i(\gamma_1), \ldots, \varphi_i(\gamma_g), \varphi_i(\beta_1), \ldots, \varphi_i(\beta_g)).$$

This is big period matrix of (A', λ').

Period matrices - Example

Let $g = (x^4 - 4x^3 + 8x^2 - 12x + 9)(x^4 - 2x^3 + 2x^2 - 6x + 9)$. We compute the principally polarized abelian varieties and we find that 4 isomorphism classes admit a unique principal polarization. Here is one of them with the period matrix of the canonical lift.

$$\begin{aligned}
I = {} & \frac{1}{54}\left(432 - 549\alpha + 441\alpha^2 - 331\alpha^3 + 186\alpha^4 - 81\alpha^5 + 33\alpha^6 - 7\alpha^7\right)\mathbb{Z}\oplus \\
& \oplus \frac{1}{6}\left(63 - 78\alpha + 65\alpha^2 - 49\alpha^3 + 27\alpha^4 - 12\alpha^5 + 5\alpha^6 - 1\alpha^7\right)\mathbb{Z}\oplus \\
& \oplus \frac{1}{6}\left(81 - 99\alpha + 84\alpha^2 - 61\alpha^3 + 33\alpha^4 - 15\alpha^5 + 6\alpha^6 - 1\alpha^7\right)\mathbb{Z}\oplus \\
& \oplus \frac{1}{18}\left(-63 + 96\alpha - 86\alpha^2 + 68\alpha^3 - 39\alpha^4 + 18\alpha^5 - 8\alpha^6 + 2\alpha^7\right)\mathbb{Z}\oplus(-1)\mathbb{Z}\oplus \\
& \oplus(-\alpha)\mathbb{Z}\oplus(-\alpha^2)\mathbb{Z}\oplus\frac{1}{9}\left(81 - 96\alpha + 81\alpha^2 - 64\alpha^3 + 33\alpha^4 - 15\alpha^5 + 6\alpha^6 - \alpha^7\right)\mathbb{Z}
\end{aligned}$$

$$\lambda = \frac{537}{80} - \frac{1343}{120}\alpha + \frac{1343}{144}\alpha^2 - \frac{419}{60}\alpha^3 + \frac{337}{80}\alpha^4 - \frac{15}{8}\alpha^5 + \frac{559}{720}\alpha^6 - \frac{1}{5}\alpha^7$$

$$\Omega = \begin{pmatrix}
2.8 - i & -2.8 + 0.59i & 0 & 0 & 1 & 1.7 - 0.29i & 0 & 0 \\
-2.8 + i & 2.8 - 3.4i & 0 & 0 & 1 & 0.29 + 1.7i & 0 & 0 \\
0 & 0 & -1 & -0.38 - 0.15i & 0 & 0 & -1.6 - 0.62i & -0.15 - 0.15i \\
0 & 0 & -1 & -2.6 + 6.9i & 0 & 0 & 0.62 - 1.6i & -6.9 + 6.9i
\end{pmatrix}$$

Thank you!