Abelian varieties without algebraic geometry (revised slides)

Everett W. Howe

Center for Communications Research, La Jolla

Geometric Cryptography
Guadeloupe, 27 April – 1 May 2009

The goal of this talk

Forty years ago:	Deligne gave a nice description of the category of ordinary abelian varieties.
Fifteen years ago:	I added dual varieties and polarizations.
Today:	I'll explain all this, and give applications.

Philosophy

Understand ordinary abelian varieties in terms of lattices over number rings.

Motivation (for me, not Deligne)

Objects with two or more dimensions are hard to understand.

Ordinary abelian varieties

Definition

Suppose

- k is a finite field of characteristic p,
- A is a g-dimensional abelian variety over k,
- f is the characteristic polynomial of Frobenius for A (the *Weil polynomial* for A).

We say that A is ordinary if one of the following equivalent conditions holds:

- $\#A(\overline{k})[p] = p^g$;
- The local-local group scheme α_p can't be embedded in A;
- Exactly half of the roots of f in $\overline{\mathbb{Q}}_p$ are p-adic units;
- The middle coefficient of f is coprime to p.

The category of Deligne modules

Definition

Let $\mathcal{L}_q$ be the category whose objects are pairs (T, F), where

- T is a finitely-generated free $\mathbb{Z}$-module of even rank,
- F is an endomorphism of T such that
  - The endomorphism $F \otimes \mathbb{Q}$ of $T \otimes \mathbb{Q}$ is a semi-simple, and its complex eigenvalues have magnitude $\sqrt{q}$;
  - Exactly half of the roots of the characteristic polynomial of F in $\overline{\mathbb{Q}}_p$ are p-adic units;
  - There is an endomorphism V of T with $FV = q$.

and whose morphisms are $\mathbb{Z}$-module morphisms that respect F.

We call $\mathcal{L}_q$ the category of Deligne modules over $\mathbb{F}_q$.

Deligne's equivalence of categories

Theorem

There is an equivalence between the category of ordinary abelian varieties over $\mathbb{F}_q$ and the category $\mathcal{L}_q$ that takes g-dimensional varieties to pairs (T, F) with $\operatorname{rank}_{\mathbb{Z}} T = 2g$.

The equivalence requires a nasty choice

Let W be the ring of Witt vectors over $\overline{\mathbb{F}}_q$.
Let ε be an embedding of W into $\mathbb{C}$.
Let v be the corresponding p-adic valuation on $\overline{\mathbb{Q}}$.

Given $A/\mathbb{F}_q$, let $\widetilde{A}$ be the complex abelian variety obtained from the canonical lift of A over W by base extension to $\mathbb{C}$ via ε.

Let $T = H_1(\widetilde{A})$, and let F be the lift of Frobenius.

Extending the equivalence: Dual varieties

Definition

Given (T, F) in $\mathcal{L}_q$, let $\widehat{T} = \mathrm{Hom}(T, \mathbb{Z})$.
Let $\widehat{F}$ be the endomorphism of $\widehat{T}$ such that for $\psi \in \widehat{T}$

$$\widehat{F}\psi(x) = \psi(Vx) \qquad \text{for all } x \in T.$$

The dual of (T, F) is $(\widehat{T}, \widehat{F})$.

Theorem

Deligne's equivalence respects duality.

Extending the equivalence: Polarizations

Given $(T, F) \in \mathcal{L}_q$, let

$$R = \mathbb{Z}[F, V] \subseteq \operatorname{End}(T, F)$$
$$K = R \otimes \mathbb{Q} = \prod K_i$$

The p-adic valuation v on $\mathbb{C}$ obtained from $\varepsilon : W \hookrightarrow \mathbb{C}$ gives us a CM-type on K:

$$\Phi := \{\varphi : K \to \mathbb{C} \mid v(\varphi(F)) > 0\}.$$

Let ι be any element of K such that

$$\forall \varphi \in \Phi : \varphi(\iota) \text{ is positive imaginary.}$$

Polarizations, continued

Suppose λ is an isogeny from (T, F) to its dual $(\widehat{T}, \widehat{F})$.
This gives us a pairing $b : T \times T \to \mathbb{Z}$.

Definition

The isogeny λ is a polarization if

- The pairing b is alternating, and
- The pairing $(x, y) \mapsto b(\iota x, y)$ on $T \times T$ is symmetric and positive definite.

Theorem

Deligne's equivalence takes polarizations to polarizations.

Extending the equivalence: Kernels of isogenies

Let $\lambda : (T_1, F_1) \to (T_2, F_2)$ be an isogeny of Deligne modules.
Let $\lambda_{\mathbb{Q}}$ be the induced isomorphism $T_1 \otimes \mathbb{Q} \to T_2 \otimes \mathbb{Q}$.
The kernel of λ is the $\mathbb{Z}[F_1, V_1]$-module $\lambda_{\mathbb{Q}}^{-1}(T_2)/T_1$.

Theorem

Suppose $\mu : A_1 \to A_2$ is the isogeny of abelian varieties corresponding to λ. Then

$$\#\ker\mu = \#\ker\lambda$$

and the action of Frobenius on the étale quotient of $\ker\mu$ is isomorphic to the action of F_1 on the quotient of $\ker\lambda$ by the submodule where F_1 acts as 0.

Application 1: Galois descent (w/Lauter)

Suppose $\mathcal{I}$ is an ordinary isogeny class over $\mathbb{F}_q$. Let h be the *minimal* polynomial of $F + V$.

The action of $\mathbb{Z}[F, V]$ on a Deligne module T factors through

$$\mathbb{Z}[X, Y]/(h(X + Y), XY - q) =: \mathbb{Z}[\pi, \overline{\pi}].$$

Let $\mathcal{I}_n$ be the base extension of $\mathcal{I}$ to $\mathbb{F}_{q^n}$.

Theorem

If $\mathbb{Z}[\pi^n, \overline{\pi}^n] = \mathbb{Z}[\pi, \overline{\pi}]$ then every variety in $\mathcal{I}_n$ comes from a variety in $\mathcal{I}$.

Note: Ordinariness is quite important here.

Restricting to a simple isogeny class

Notation

$$\begin{aligned} \mathcal{I} &= \text{a simple ordinary isogeny class in } \mathcal{L}_q \\ R &= \mathbb{Z}[\pi, \overline{\pi}] \\ K &= R \otimes \mathbb{Q} \\ K^+ &= \text{maximal real subfield of } K \\ \Phi &= \text{CM-type on } K \text{ as above.} \end{aligned}$$

If (T, F) is a Deligne module in $\mathcal{I}$, then $T \otimes \mathbb{Q}$ is a 1-dimensional K-vector space. So

$$\Big\{\text{Deligne modules in } \mathcal{I}\Big\} \longleftrightarrow \left\{\begin{matrix}\text{isomorphism classes of} \\ \text{fractional } R\text{-ideals in } K\end{matrix}\right\}$$

Polarizations in a simple isogeny class

Let $\mathfrak{A}$ be a fractional R-ideal.
Identify $\mathrm{Hom}(\mathfrak{A}, \mathbb{Z})$ with the dual $\mathfrak{A}^\dagger$ of $\mathfrak{A}$ under the trace pairing

$$\begin{aligned} K \times K &\to \mathbb{Q} \\ (x, y) &\mapsto \mathrm{Trace}_{K/\mathbb{Q}}(xy) \end{aligned}$$

Then $\widehat{\mathfrak{A}} = \overline{\mathfrak{A}^\dagger}$, where the overline means complex conjugation.

Theorem

A polarization of $\mathfrak{A}$ is a $\lambda \in K^*$ such that

- $\lambda\mathfrak{A} \subseteq \widehat{\mathfrak{A}}$,
- λ *is totally imaginary,*
- $\varphi(\lambda)$ *is positive imaginary for all* $\varphi \in \Phi$.

Deligne modules with maximal endomorphism rings

If $\mathfrak{A}$ is actually an $\mathcal{O}_K$-ideal, then

$$\widehat{\mathfrak{A}} = \overline{\mathfrak{d}^{-1}\mathfrak{A}^{-1}} = \mathfrak{d}^{-1}\overline{\mathfrak{A}^{-1}}$$

where $\mathfrak{d}$ is the different of $K/\mathbb{Q}$.

Theorem

Let N be the norm from $\operatorname{Cl} K$ to $\operatorname{Cl}^+ K^+$. There is an ideal class $[\mathfrak{B}] \in \operatorname{Cl}^+ K^+$ such that a Deligne module $\mathfrak{A}$ with $\operatorname{End}\mathfrak{A} = \mathcal{O}_K$ has a principal polarization if and only if $N([\mathfrak{A}]) = [\mathfrak{B}]$.

Proof: Note that $\lambda\mathfrak{A} = \mathfrak{d}^{-1}\overline{\mathfrak{A}^{-1}} \iff \mathfrak{A}\overline{\mathfrak{A}} = 1/(\lambda\mathfrak{d})$.
Then prove that $\lambda\mathfrak{d}$ is an ideal of K^+ whose strict class doesn't depend on the choice of positive imaginary λ.

Application 2: Near-ubiquity of principal polarizations

Class field theory

The norm map $\operatorname{Cl} K \to \operatorname{Cl}^+ K^+$ is surjective if K/K^+ is ramified at a finite prime.

Theorem

A simple ordinary isogeny class contains a principally polarized variety if K/K^+ is ramified at a finite prime.

In particular, a simple ordinary odd-dimensional isogeny class contains a principally polarized variety.

Application 3: Non-existence of principal polarizations

Theorem

A 2-dimensional isogeny class of abelian varieties over $\mathbb{F}_q$ contains no principally-polarized varieties if and only if its real Weil polynomial is $x^2 + ax + (a^2 + q)$, where

- $a^2 < q$,
- $\gcd(a, q) = 1$, *and*
- $a^2 \equiv q \bmod p \Longrightarrow p \equiv 1 \bmod 3$.

From simple to non-simple isogeny classes

We can piece together information about simple classes to learn about non-simple classes.

Example: Principal polarizations

Suppose $\mathcal{I}_1$ and $\mathcal{I}_2$ are isogeny classes with $\mathrm{Hom}(\mathcal{I}_1, \mathcal{I}_2) = 0$.
Goal: Study principally polarized varieties in the isogeny class

$$\begin{aligned}\mathcal{J} &= \mathcal{I}_1 \times \mathcal{I}_2 \\ &= \{\text{abelian varieties isogenous to } A_1 \times A_2\text{: } A_1 \in \mathcal{I}_1, A_2 \in \mathcal{I}_2\}\end{aligned}$$

Suppose P in $\mathcal{J}$ has a principal polarization μ.
P is isogenous to $A_1 \times A_2$, so. . .

Reducing the size of the kernel

$$0 \longrightarrow \Delta' \longrightarrow A_1 \times A_2 \longrightarrow P \longrightarrow 0$$

Reducing the size of the kernel

$$\begin{array}{ccccccccc} & & \Delta_1 \times \Delta_2 & = & \Delta_1 \times \Delta_2 & & & & \\ & & \downarrow & & \downarrow & & & & \\ 0 & \longrightarrow & \Delta' & \longrightarrow & A_1 \times A_2 & \longrightarrow & P & \longrightarrow & 0 \end{array}$$

Reducing the size of the kernel

$$
\begin{array}{ccccccccc}
 & & \Delta_1 \times \Delta_2 & = & \Delta_1 \times \Delta_2 & & & & \\
 & & \big\downarrow & & \big\downarrow & & & & \\
0 & \longrightarrow & \Delta' & \longrightarrow & A_1 \times A_2 & \longrightarrow & P & \longrightarrow & 0 \\
 & & \big\downarrow & & \big\downarrow & & \big\downarrow & & \\
0 & \longrightarrow & \Delta & \longrightarrow & B_1 \times B_2 & \longrightarrow & P & \longrightarrow & 0
\end{array}
$$

Reducing the size of the kernel

$$
\begin{array}{ccccccccc}
 & & \Delta_1 \times \Delta_2 & = & \Delta_1 \times \Delta_2 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \Delta' & \longrightarrow & A_1 \times A_2 & \longrightarrow & P & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \Delta & \longrightarrow & B_1 \times B_2 & \longrightarrow & P & \longrightarrow & 0
\end{array}
$$

Projections $B_1 \times B_2 \rightarrow B_i$ give *injections* $\Delta \hookrightarrow B_1$ and $\Delta \hookrightarrow B_2$.

Pullback of μ to $B_1 \times B_2$ is $\lambda_1 \times \lambda_2$, and $\ker \lambda_1 \cong \Delta \cong \ker \lambda_2$.

As per Kristin: Can bound size of Δ.

Application 4: Ordinary times supersingular (w/Lauter)

Suppose $q = s^2$ and h is an ordinary real Weil polynomial.

Theorem

Suppose

- $n := h(2s)$ *is squarefree and coprime to* q*,*
- P *is an abelian variety over* $\mathbb{F}_q$ *with real Weil polynomial* $h(x) \cdot (x - 2s)^n$*,*
- μ *is a principal polarization on* P*.*

Then there is an isomorphism $P \cong B_1 \times B_2$ *that takes* μ *to a product polarization* $\lambda_1 \times \lambda_2$*, where* B_1 *is ordinary and* B_2 *is isogenous to a power of a supersingular elliptic curve.*

Ordinary times supersingular: Sketch of proof

We already know that we can write

$$0 \longrightarrow \Delta \longrightarrow B_1 \times B_2 \longrightarrow P \longrightarrow 0$$

and pull back μ to $\lambda_1 \times \lambda_2$, where $\ker \lambda_1 \cong \Delta \cong \ker \lambda_2$.

Note:

- $F + V$ acts as $2s$ on $\ker \lambda_2$.
- $F + V$ satisfies h on $\ker \lambda_1$.
- So $0 = h(F + V) = h(2s) = n$ on Δ.

Question: Can we fit an n-torsion Δ with a non-degenerate pairing into B_1 and B_2?
Suffices to consider case where n is prime.

Sketch of proof: Further restrictions on Δ

On the supersingular variety B_2 we know that F and V act as s.

So the image of Δ in B_1 lies in the portion of B_1 where

$$n = 0 \text{ and } F = s \text{ and } V = s.$$

Let $\mathfrak{p}$ be the ideal $(n, \pi_1 - s, \overline{\pi}_1 - s)$ of $R = \mathbb{Z}[\pi_1, \overline{\pi}_1]$.

Check:

- $\mathfrak{p}$ is a non-singular prime of R with residue field $\mathbb{F}_n$.
- If $\mathfrak{A}$ is a Deligne module with real Weil polynomial h, then the kernel of $\mathfrak{p}$ acting on $\mathfrak{A}$ has order n.
- There are no étale group schemes of prime order with non-degenerate pairings.

Sketch of proof: The end

So in our exact sequence

$$0 \longrightarrow \Delta \longrightarrow B_1 \times B_2 \longrightarrow P \longrightarrow 0$$

we have $\Delta = 0$.

Corollary

If $q = s^2$ and h is an ordinary real Weil polynomial with $h(2s)$ squarefree and coprime to q, then there is no Jacobian with real Weil polynomial

$$h(x) \cdot (x - 2s)^n \quad \text{for } n > 0.$$