Pairing-based algorithms for jacobians of hyperelliptic curves

Sorina Ionica

Projet Caramel, LORIA

December 6, 2011

What is an isogeny?

- a morphism of algebraic curves $\phi : E_1 \rightarrow E_2$
- a group morphism?
- Take $\phi(O_{E_1}) = O_{E_2}$ and get all at once!
- Take $\phi : E \rightarrow E$ and get endomorphisms $\mathrm{End}(E)$
- In this talk, only curves defined over a finite field $\mathbb{F}_q$.

Crypto Isogeny Party

- multiscalar multiplication in many protocols: given P, compute λP
- pairing based crypto
  - "good isogenies" may give self pairings $e(P, \phi(P))$
- counting the number of points on an elliptic curve (SEA)
- hash functions (Charles-Goren-Lauter)
- transfer the discrete logarithm problem from one curve to another

Motivation

Distinguished isogenies:

- endomorphisms $I : E \to E$.
- An ℓ-isogeny $I : E_1 \to E_2$ is horizontal iff $\mathrm{End}(E_1) \simeq \mathrm{End}(E_2)$.

An endomorphism is a composition of isogenies of prime degree:

$$E_1 \to E_2 \to E_3 \ldots \to E_1$$

How do we compute horizontal isogenies?

Some examples of endomorphisms

- multiplication by $\ell \in \mathbb{Z}$:$P \rightarrow \ell P$
  - $\mathrm{End}(E)$ is a ring containing a subring isomorphic to $\mathbb{Z}$
- the Frobenius for $E/\mathbb{F}_q$

$$\begin{array}{rcl} \pi : E & \rightarrow & E \\ (x, y) & \rightarrow & (x^q, y^q) \end{array}$$

- π is not a multiplication by ℓ map $\Rightarrow \mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$

The endomorphism ring of an ordinary elliptic curve

- Let $K = \mathbb{Q}(\sqrt{N})$, $N < 0$ and $\mathcal{O}_K$ is the ring of integers.
- As a $\mathbb{Z}$-module, $\mathcal{O}_K = [1, \omega_K]$, with $\omega_K = \frac{d_K + \sqrt{d_K}}{2}$.
- An order $\mathcal{O}$ is a subring of K and a $\mathbb{Z}$-module of rank 2.
- Actually we can think of it as $\mathcal{O} = [1, f\omega_K]$.
- f is called the conductor of the order and $D = f^2 d_K$ the discriminant.

The endomorphism ring of an ordinary elliptic curve

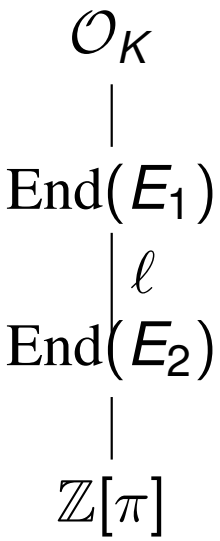
- $\mathrm{End}(E)$ is an order in a quadratic imaginary field K
- Denote by $f = [\mathcal{O}_K : \mathrm{End}(E)]$ the conductor and by $d_E = f^2 d_K$ the discriminant

$$\begin{array}{ll} \mathcal{O}_K & \leftarrow [1, \omega_K] \\ | \ f & \\ \mathrm{End}(E) & \leftarrow [1, f\omega_K] \\ |\frac{g}{f} & \\ \mathbb{Z}[\pi] & \leftarrow [1, g\omega_K] \end{array}$$

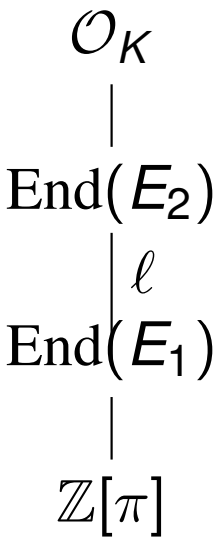
$$d_\pi = g^2 d_K = t^2 - 4q$$

Isogenies and endomorphism rings

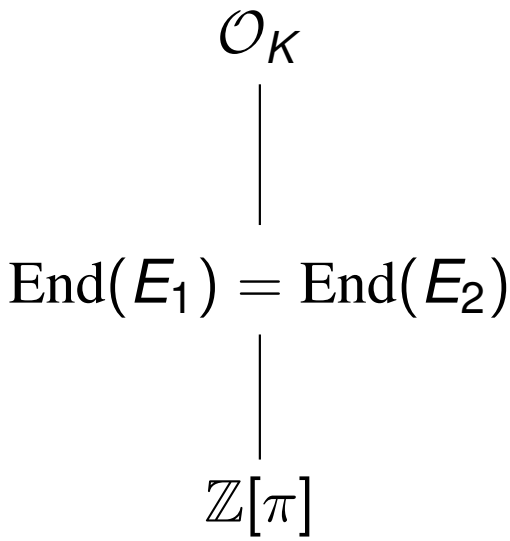
Let $\phi : E_1 \to E_2$ be an isogeny of degree ℓ (i.e. $\#\mathrm{Ker}\ I = \ell$).



descending



ascending



horizontal

The ℓ-isogeny graph has vertices $Ell_t(\mathbb{F}_q)$ and edges ℓ-isogenies defined over $\mathbb{F}_q$.

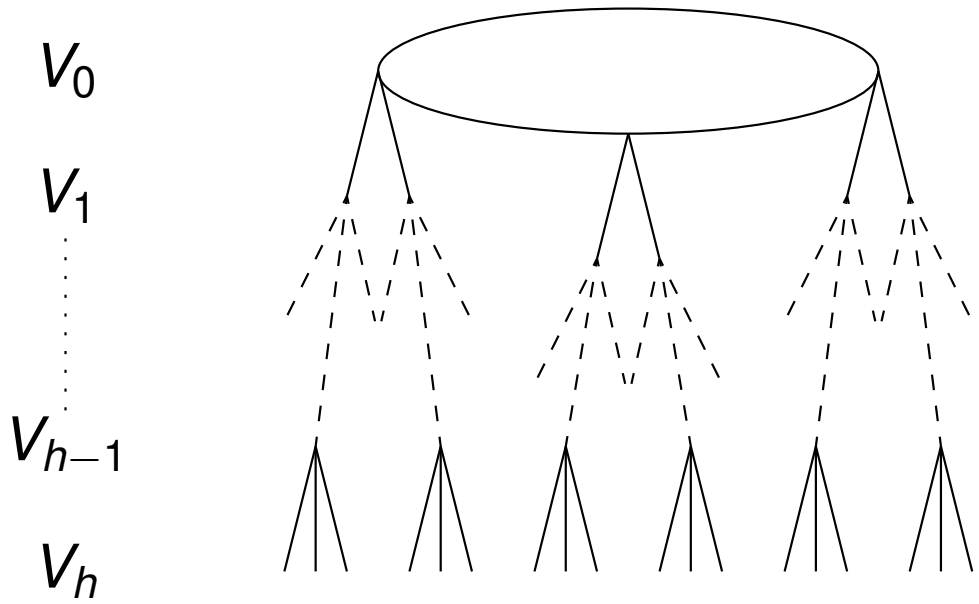
Isogenies and ℓ-volcanoes

Let h be the ℓ-adic valuation of the conductor g of $\mathbb{Z}[\pi]$.

Kohel's theorem

Connected components of $Ell_t(\mathbb{F}_q)$ are ℓ-volcanoes of height h (assuming $j \neq 0, 1728$).

What is a ℓ-volcano?



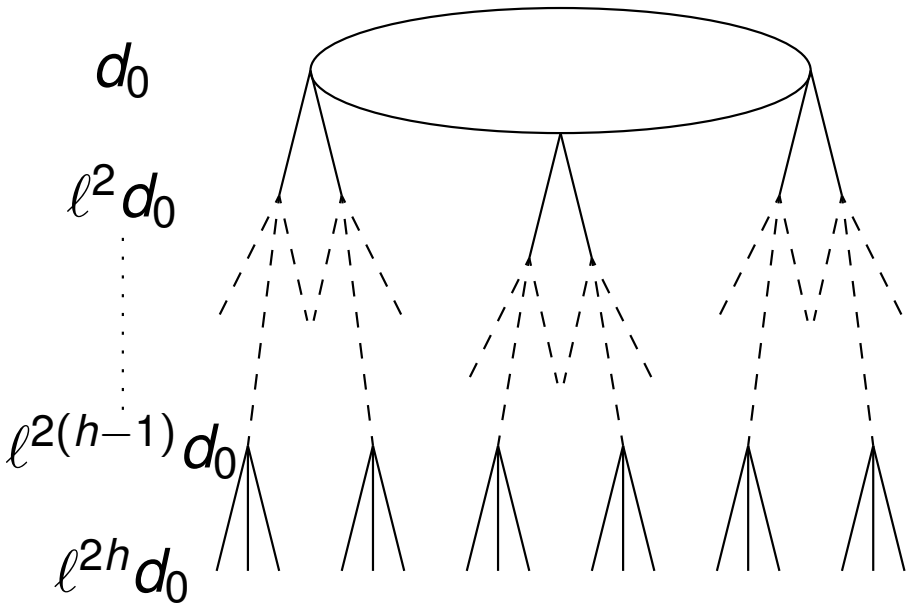
- V_0 (the *crater*) is regular connected of degree at most 2
- For $i > 0$, each vertex in V_i has one edge leading to a vertex in V_{i-1}
- For $i < h$, each vertex in V_i has degree $\ell + 1$.

Isogenies and ℓ-volcanoes

Let h be the ℓ-adic valuation of the conductor g of $\mathbb{Z}[\pi]$.

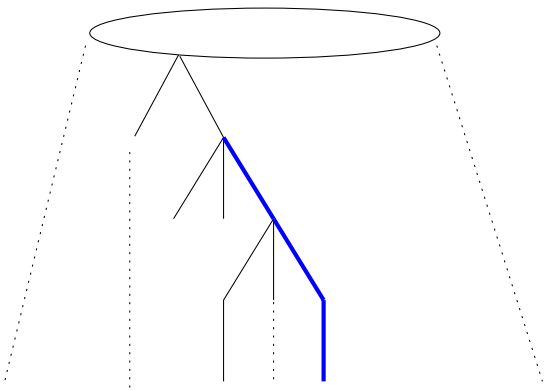
Kohel's theorem

Connected components of $Ell_t(\mathbb{F}_q)$ are ℓ-volcanoes of height h (assuming $j \neq 0, 1728$).



Curves on a fixed level have the same endomorphism ring.

Computing the ℓ-adic valuation of the conductor (Kohel 1996)



- Find shortest path to the floor.
- Cost of one step: an isogeny computation
- Modular polynomial factorization $O(\ell^2 + M(\ell)\log q)$ with $M(\ell) = \ell \log \ell \log\log \ell$

Total cost $O(h(\ell^2 + M(\ell)\log q))$

- Bottleneck: isogeny computation $\Rightarrow \ell$ is small
- If ℓ is large, we compute
  - *smooth* relations in the class group
  - corresponding *smooth* isogenies
- Kohel 1996, Bisson-Sutherland 2010, Bisson 2011

$$O(L[1/2, 1/\sqrt{2}](q)) \text{ (under GRH)}$$

Computing the ℓ-adic valuation of the conductor

Let $\theta \in \mathcal{O}$. We define

$$v_{\ell,\mathcal{O}}(\theta) := max\{m | \theta \in \mathbb{Z} + \ell^m \mathcal{O}\}$$

How do we compute this?

Consider a $\mathbb{Z}$-basis $1, \omega$ for $\mathcal{O}$:

Write $\theta = a_1 + a_2\omega$. Then

$$v_{\ell,\mathcal{O}}(\theta) := v_\ell(a_2).$$

Computing the ℓ-adic valuation of the conductor

We consider $v_\ell(\pi) := v_{\ell,\mathrm{End(J)}}(\pi)$.

Remember $\pi = a_1 + a_2(f\omega_K)$ and $a_2 * f = g$.

How do we compute $v_\ell(\pi)$?

That's where pairings come into play.

The Weil pairing

Let A be an abelian variety defined over a field K.
$A[m]$ is the m-torsion and $\hat{A}[m] \simeq \mathrm{Hom}(A[m], \mu_m)$.

Weil pairing

$$e_m : A[m] \times \hat{A}[m] \to \mu_m$$
is a bilinear, non-degenerate map.

If A is a principally polarized variety

$$\begin{aligned} e_m : A[m] \times A[m] &\to \mu_m \\ (P, Q) &\to e_m(P, Q). \end{aligned}$$

The Tate pairing

We denote by $G_K = \mathrm{Gal}(\bar{K}/K)$ the Galois group.

Consider $0 \to A[m] \to A(\bar{K}) \to A(\bar{K}) \to 0$.

Take Galois cohomology and get connecting morphism

$$\begin{aligned} \delta : A(K)/mA(K) = H^0(G_K, A)/mH^0(G_K, A) &\to H^1(G_K, A[m]) \\ P &\to F_P, \end{aligned}$$

where we take $\bar{P}$ such that $m\bar{P} = P$ and define

$$\begin{aligned} F_P(\sigma) : G_K &\to A(\bar{K})[m] \\ \sigma &\to \sigma \cdot \bar{P} - \bar{P}. \end{aligned}$$

The Tate pairing

We get the map

$$\begin{aligned} A(K)/mA(K) \times \hat{A}[m](K) &\rightarrow H^1(G_K, \mu_m) \\ (P, Q) &\rightarrow [\sigma \rightarrow e_m(F_P(\sigma), Q)] \end{aligned}$$

For a principally polarized abelian variety over a finite field $\mathbb{F}_q$

The Tate pairing

$$\begin{aligned} A(\mathbb{F}_q)/mA(\mathbb{F}_q) \times A[m](\mathbb{F}_q) &\rightarrow \mu_m \\ (P, Q) &\rightarrow e_m(\pi(\bar{P}) - \bar{P}, Q) \end{aligned}$$

bilinear, non-degenerate, efficiently computable $O(\log m)$

Pairings on kernels

Assume $E[\ell^n] \subseteq E(\mathbb{F}_q)$ and $E[\ell^{n+1}] \not\subseteq E(\mathbb{F}_q)$.

We denote by $\mathcal{W}$ the set of subgroups G of order ℓ in $E[\ell^n]$.

$$k_E := \max_{G \in \mathcal{W}} \{k | \exists P \in G \text{ s.t. } T_{\ell^n}(P, P) \in \mu_{\ell^k} \setminus \mu_{\ell^{k-1}}\}$$

Non-degeneracy on subgroups

Let $G \in \mathcal{W}$. The Tate pairing is k_E-non-degenerate on $G \times G$ if

$$T_{\ell^n} : G \times G \longrightarrow \mu_{\ell^{k_E}}$$

is surjective.

Computing $v_\ell(\pi)$

Theorem

Suppose $\pi - 1$ is exactly divisible by ℓ^n. If $v_\ell(\pi) < 2n$, then $k_E = 2n - v_\ell(\pi)$.

Proof:

$v_\ell(\pi)$ is the largest integer such that the Frobenius matrix is of the form

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \bmod \ell^m$$

Galois cohomology+linear algebra (Schmoyer)

Corollary

If E has locally maximal endomorphism ring at ℓ, points in $E[\ell^n]$ with degenerate self-pairing generate kernels of horizontal ℓ-isogenies.

Algorithm (I.-Joux, 2011)

- Compute $E(\ell^n)(\mathbb{F}_{q^r}) =< P, Q >$
- Note $T_{\ell^n}(aP + bQ, aP + bQ) = T_{\ell^n}(P, P)^{a^2}(T_{\ell^n}(P, Q)T_{\ell^n}(Q, P))^{ab}T_{\ell^n}(Q, Q)^{b^2}$
- Compute $S(P, P)$, $S(P, Q)$ and $S(Q, Q)$ and get k_E.
- Compute $v_\ell(\pi) = 2n - k_E$

$$P(k_E = 0) \approx \frac{1}{\ell^4}$$

Complexity

Kohel 1996	Isogeny walk $h(\ell^2 + M(\ell)\log q)$
This work best case worst case $r \approx \ell/2$	Group structure and pairings $\log q + n\log \ell$ $rM(r)(\log q + n\log \ell)$

Table: Endomorphism ring computation: Benchmarks

Parameters	Kohel	This work
$D = 1009$, $\ell = 31$, $h = 10$, $r = 1$	1.80 s	0.01 s
$D = 1009$, $\ell = 101$, $h = 3$, $r = 10$	1.18 s	0.75 s
$D = 1009$, $\ell = 31$, $h = 6$, $r = 5$	1.15 s	0.33 s
$D = 4 * 919$, $h = 2$, $\ell = 1009$, $r = 84$	-	43 s

The endomorphism ring of an ordinary jacobian

- Let K be a quartic CM field, i.e. a purely imaginary degree 2 extension of a totally real quadratic field.
- We assume $K_0 = \mathbb{Q}(\sqrt{d})$ has class number one and that $K = \mathbb{Q}(i\sqrt{a + b\sqrt{d}})$, $a, b \in \mathbb{Z}/2$
- Let J be a jacobian of a genus 2 curve defined over $\mathbb{F}_q$.
- J is ordinary, i.e. $\mathrm{End}(J)$ is an order of K

$$\mathbb{Z}[\pi, \bar{\pi}] \subset \mathrm{End}(J) \subset \mathcal{O}_K$$

The Frobenius action

Let $\theta \in \mathcal{O}$. We define

$$v_{\ell,\mathcal{O}}(\theta) := max\{m | \theta \in \mathbb{Z} + \ell^m \mathcal{O}\}$$

How do we compute this?

Consider a $\mathbb{Z}$-basis $1, \delta, \gamma, \eta$ for $\mathcal{O}$:

Write $\theta = a_1 + a_2\delta + a_3\gamma + a_4\eta$. Then

$$v_{\ell,\mathcal{O}}(\theta) := v_\ell(\gcd(a_2, a_3, a_4)).$$

Work in progress (with B. Smith)

We assume that $n > 0$ is maximal such that $J[\ell^n] \subset J(\mathbb{F}_q)$.
We denote by $\mathcal{W}$ the set of subgroups G of rank 2 in $J[\ell^n]$ such that $\ell^{n-1} G$ is maximal isotropic with respect to the Weil pairing.

$$k_J := \max_{G \in \mathcal{W}} \{k | \exists P, Q \in G \text{ s.t. } T_{\ell^n}(P, Q) \in \mu_{\ell^k} \setminus \mu_{\ell^{k-1}}\}$$

Non-degeneracy on subgroups

Let G be a rank 2 subgroup of $J[\ell^n]$ in $\mathcal{W}$. The Tate pairing is k_J-non-degenerate on $G \times G$ if

$$T_{\ell^n} : G \times G \longrightarrow \mu_{\ell^{k_J}}$$

is surjective.

Checking locally maximal orders

Assume that $\pi = a_1 + a_2\omega_{K_0} + (a_3 + a_4\omega_{K_0})i\sqrt{a + b\sqrt{d}}$, $a_i \in \mathbb{Z}$.

A simple criterion

Assuming $v_\ell(a_3 - a_4) = \min(v_\ell(a_3), v_\ell(a_4))$ then $v_{\ell,\mathcal{O}}(\pi) < v_{\ell,\mathcal{O}_K}(\pi)$ for any order $\mathcal{O}$ such that $\mathbb{Z}[\pi] \in \mathcal{O}$ and $[\mathcal{O}_K : \mathcal{O}]$ is divisible by a power of ℓ.

Check that $\mathrm{End}(J)$ is locally maximal at ℓ: $v_\ell(\pi) = v_{\ell,\mathcal{O}_K}(\pi)$

Same formula as in the genus 1 case: $k_J = 2n - v_\ell(\pi)$.

Computing horizontal isogenies

Theorem

Let J be a jacobian whose endomorphism ring is locally maximal at ℓ. Let G be a maximal isotropic subgroup of $J[\ell]$ and assume $\pi - 1$ is exactly divisible by ℓ^n. Consider $\bar{G} \leq J[\ell^n]$ such that $\ell^{n-1}\bar{G} = G$. Then the isogeny of kernel G is horizontal if the Tate pairing is degenerate on $\bar{G} \times \bar{G}$ and is descending otherwise.