Pairing the volcano

Sorina Ionica and Antoine Joux

Université de Versailles Saint-Quentin-en-Yvelines
PR*i*SM, 45 avenue des États-Unis, F-78035, Versailles CEDEX, France

DGA

ANTS, Nancy, June 19th, 2010

UNIVERSITÉ DE VERSAILLES
SAINT-QUENTIN-EN-YVELINES

Laboratoire PRiSM

Motivation

An isogeny cycle is a sequence of isogenies

$$E_1 \longrightarrow E_2 \longrightarrow E_3 \longrightarrow \ldots \longrightarrow E_{n-1} \longrightarrow E_1$$

- SEA algorithm (Couveignes and Morain)
- Hilbert polynomial computation (Couveignes and Henocq, Broker, Charles and Lauter, Belding et al., Sutherland)

Question: How can we build isogeny cycles?

Answer: Kohel's work on the computation of the endomorphism ring (isogeny volcanoes) and pairings.

The endomorphism ring of an ordinary elliptic curve

Let E be an ordinary elliptic curve defined over $\mathbb{F}_q$.

Examples: multiplication by $\ell \in \mathbb{Z}$

$$P \to \ell P$$

$$\pi : (x, y) \to (x^q, y^q).$$

$$\boxed{\mathbb{Z}[\pi] \subseteq End(E)}$$

- $\mathrm{End}(E)$ is an order in a quadratic imaginary field K, i.e. a subring and $\mathbb{Z}$-submodule of the ring of integers $\mathcal{O}_K$
- Denote by $f = [\mathcal{O}_K : \mathrm{End}(E)]$ the conductor and by $d_E = f^2 d_K$ the discriminant

$$\begin{array}{ll} \mathcal{O}_K & \leftarrow d_K \\ \mid f & \\ \mathrm{End}(E) & \leftarrow f^2 d_K \\ \mid \frac{g}{f} & \\ \mathbb{Z}[\pi] & \leftarrow g^2 d_K \end{array}$$

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

Isogenies and endomorphism rings

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

Let $\phi : E_1 \to E_2$ be an isogeny of degree ℓ.

$$\begin{tikzcd} \mathcal{O}_K \arrow[d, dash] \\ \mathrm{End}(E_1) \arrow[d, dash, "\ell"] \\ \mathrm{End}(E_2) \arrow[d, dash] \\ \mathbb{Z}[\pi] \end{tikzcd} \qquad \begin{tikzcd} \mathcal{O}_K \arrow[d, dash] \\ \mathrm{End}(E_2) \arrow[d, dash, "\ell"] \\ \mathrm{End}(E_1) \arrow[d, dash] \\ \mathbb{Z}[\pi] \end{tikzcd} \qquad \begin{tikzcd} \mathcal{O}_K \arrow[d, dash] \\ \mathrm{End}(E_1) = \mathrm{End}(E_2) \arrow[d, dash] \\ \mathbb{Z}[\pi] \end{tikzcd}$$

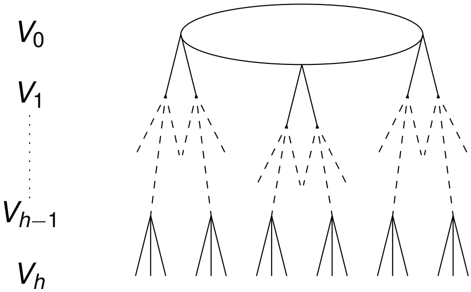
descending ascending horizontal

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?

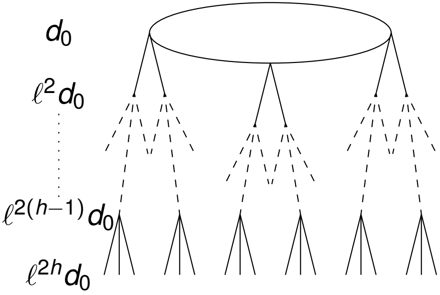


- V_0 (the *crater*) is regular connected of degree at most 2
- For $i > 0$, each vertex in V_i has one edge leading to a vertex in V_{i-1}
- For $i < h$, each vertex in V_i has degree $\ell + 1$.

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.

Exploring the volcano (First method)

- Assume E has $\ell + 1$ neighbours. Then $E[\ell](\mathbb{F}_{q^r}) =< P, Q >$ with $r < \ell$.
- Subgroups of order ℓ are: $< P >, < Q >, < P + Q >, \ldots, < P + (\ell - 1)Q >$
- Use classical Vélu's formulae

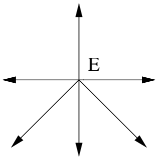
$$O(M(r)(\ell + \log q)) \text{ with } M(r) = r \log r \log\log r$$

Exploring the volcano (Second method)

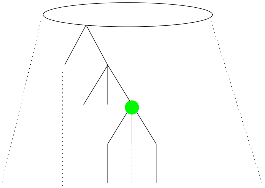
- The modular polynomial $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$ is a symmetric polynomial of degree $\ell + 1$ in each variable
- E and E' are ℓ-isogenous over $\mathbb{F}_q \Leftrightarrow \#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$ and $\Phi_\ell(j(E), j(E')) = 0$.
- Roots of $\Phi_\ell(X, j(E))$ in $\mathbb{F}_q$ give curves ℓ-isogenous to E.

$$O(\ell^2 + M(\ell)\log q) \text{ with } M(\ell) = \ell \log \ell \log\log \ell$$

- Use modular polynomials
- Blind walking



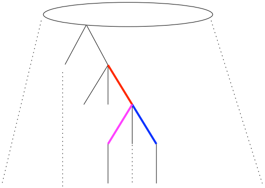
Descending (Kohel 1996, Fouquet-Morain 2001)



- It is easy to detect the floor.
- From a given curve one $\uparrow$ or at most two $\rightarrow$ isogenies.
- No backtracking $\Rightarrow$ gravity is our friend!

Descent: Construct three paths in parallel.
The first that reaches the floor is descending.

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

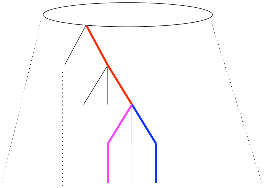


- It is easy to detect the floor.
- From a given curve one $\uparrow$ or at most two $\rightarrow$ isogenies.
- No backtracking $\Rightarrow$ gravity is our friend!

Descent: Construct three paths in parallel.
The first that reaches the floor is descending.

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

Descending (Kohel 1996, Fouquet-Morain 2001)

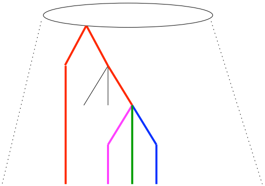


- It is easy to detect the floor.
- From a given curve one $\uparrow$ or at most two $\rightarrow$ isogenies.
- No backtracking $\Rightarrow$ gravity is our friend!

Descent: Construct three paths in parallel.
The first that reaches the floor is descending.

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

Ascending or walking on the crater (Fouquet-Morain, 2001)

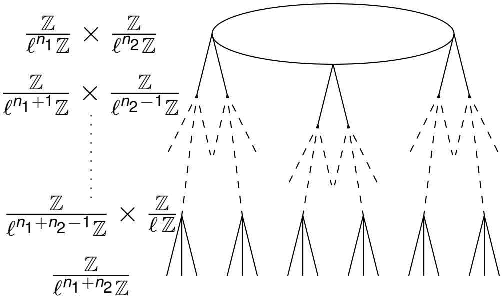


- Construct descending paths for the $\ell + 1$ neighbours
- The curve with the longest path is either above or at the same level $\mathcal{O}(h(\ell^3 + \ell M(\ell) \log q)$

Parallel walk: Construct $\ell + 1$ paths in parallel and use multipoint evaluation to compute $\Phi_\ell(X, j(E))$

$$\mathcal{O}(h\ell M(\ell)(\log \ell + \log q))$$

Determining directions on a regular volcano



Miret et al. 2006

Determine direction thanks to the ℓ-Sylow group structure

Our approach

Construct a compass using self-pairings.

Self-pairings

$E[\ell^\infty](\mathbb{F}_{q^r}) \simeq \mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$
with $n_1 \geq n_2$
$E[\ell^{n_2}](\mathbb{F}_{q^r}) \simeq \mathbb{Z}/\ell^{n_2}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$ $\Rightarrow$ $\ell^{n_2} | q^r - 1$

The reduced Tate pairing is a bilinear, non-degenerate map

$$
\begin{array}{rcl}
T_{\ell^{n_2}} : E[\ell^{n_2}] \times E(\mathbb{F}_{q^r})/\ell^{n_2}E(\mathbb{F}_{q^r}) & \rightarrow & \mu_{\ell^{n_2}} \\
(P, Q) & \rightarrow & \left(\dfrac{f_{\ell^{n_2},P}(Q+R)}{f_{\ell^{n_2},P}(R)} \right)^{\frac{q-1}{\ell^{n_2}}}
\end{array}
$$

efficiently computable with Miller's algorithm
$O(n_2 \log \ell)$

Self-pairings

- For $P, Q \in E[\ell^{n_2}]$ define

$$S(P,Q) = (T_{\ell^{n_2}}(P,Q)\,T_{\ell^{n_2}}(Q,P))^{\frac{1}{2}} \text{ (Joux, Nguyen 2003)}$$

- S symmetric $\Rightarrow S(P,P) = T_{\ell^{n_2}}(P,P)$
- If $S \neq 1$ there is $k > 0$ such that

$$S(\cdot,\cdot) : E[\ell^{n_2}] \times E[\ell^{n_2}] \to \mu_{\ell^k} \subseteq \mu_{\ell^{n_2}} \text{ surjective}$$

We say P has non-degenerate self-pairing iff $T_{\ell^{n_2}}(P,P)$ is a primitive ℓ^k-th root of unity and degenerate otherwise.

How many degenerate self-pairings? (Joux-Nguyen/I.-Joux)

- Take P and Q generating $E[\ell^{n_2}]$

$$S(aP+bQ, aP+bQ) = S(P,P)^{a^2} S(P,Q)^{2ab} S(Q,Q)^{b^2}$$

- Consider the polynomial

$$\begin{aligned}\mathcal{P}_{E,\ell^{n_2}}(a,b) &= \log(S(P,P))a^2 + \log(S(Q,Q))b^2 \\ &\quad + 2\log(S(P,Q))ab \mod \ell^{k-1}\end{aligned}$$

homogenous roots of $\mathcal{P}_{E,\ell^{n_2}}$ $\Longleftrightarrow$ subgroups of order ℓ in $E[\ell^{n_2}]/E[\ell^{n_2-1}]$ with degenerate pairing

at most two subgroups with degenerate self-pairing (modulo $E[\ell^{n_2-1}]$)

Our pairing compass

Let P be a point of order ℓ^{n_2} on E and ϕ the isogeny of kernel $< \ell^{n_2-1}P >$.

Theorem

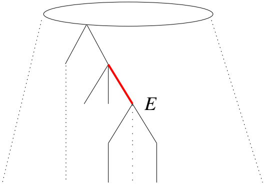
- If P has non-degenerate self-pairing then the isogeny is descending.
- If P has degenerate self-pairing, then the isogeny is ascending or horizontal.

Corollary

If $\mathcal{P}_{\ell^{n_2},E}$ has two distinct roots, then E is on the crater of its ℓ-volcano.

Regular volcanoes
$\ell \geq 3$

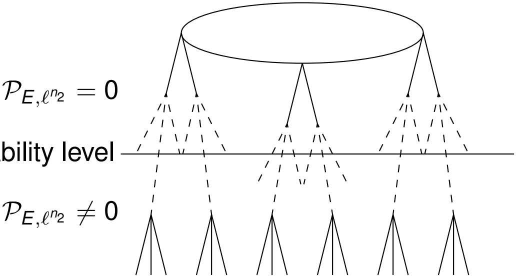
$\mathcal{P}_{E,\ell^{n_2}} \neq 0$



- Compute P and Q two generators of $E[\ell^{n_2}](\mathbb{F}_{q^r})$.
- Compute $\mathcal{P}_{E,l^{n_2}}$, compute its roots and find a point $aP + bQ$ with degenerate pairing.
- Compute vertical/horizontal isogenies via Vélu's formulae

$$O(rM(r)(1 + \log q))$$

Walking on irregular volcanoes



In theory: Move to some finite extension $\mathbb{F}_{q^{\ell^s}}$ such that the polynomial $\mathcal{P}_{E,\ell^{n_2}}$ corresponding to $E/\mathbb{F}_{q^{\ell^s}}$ is not zero.
In practice: Use Kohel/Fouquet-Morain algorithms until the stability level is reached and our algorithms in the regular part of the volcano.

Luckily, most volcanoes are regular!

Walking on the volcano: Cost per step

	Descending path	Ascending/Horizontal
Kohel, Fouquet-Morain	$h(\ell^2 + M(\ell)\log q)$	$h(\ell^3 + \ell\, M(\ell)\log q)$
Parallel evaluation	-	$h\ell\, M(\ell)(\log \ell + \log q)$
Regular volcanoes	Regular volcanoes	
Best case	$\ell + \log q$	$\ell + \log q$
Worst case $r \approx \ell/2$	$rM(r)(1 + \log q)$	$r\, M(r)(1 + \log q)$
Irregular volcanoes (worst case)	No improvement	

implementation under MAGMA 2.15-15 on an Intel Core 2 Duo 2.66 GHz

ℓ	q	ℓ-torsion	length of crater	time
100003	61900742833426666852501391	over $\mathbb{F}_q$	22 curves	154 sec.
1009	953202937996763	over $\mathbb{F}_{q^r}$ with $r = 84$	19 curves	20 min.

If you plan to go hiking this summer, you'd better get a compass!

Questions?