Vers un nouvel algorithme pour le calcul de l'anneau d'endomorphismes d'une courbe elliptique

Sorina Ionica

LIX, Ecole Polytechnique and Inria Saclay, projet TANC

travail commun avec Antoine Joux

Motivation

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

- The GLV method uses endomorphisms to speed up scalar multiplication.
- The CRT method for class polynomial computation

Motivation

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

- The GLV method uses endomorphisms to speed up scalar multiplication.
- The CRT method for class polynomial computation

WANTED

$$\mathrm{End}(E)$$

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

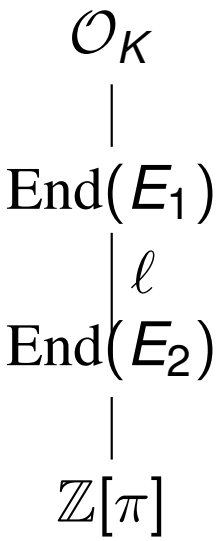
- $\mathrm{End}(E)$ is an order in a quadratic imaginary field K, i.e. a subring and $\mathbb{Z}$-submodule of the ring of integers $\mathcal{O}_K$
- Denote by $f = [\mathcal{O}_K : \mathrm{End}(E)]$ the conductor and by $d_E = f^2 d_K$ the discriminant

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

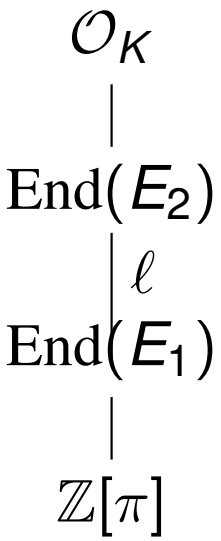
$$d_\pi = g^2 d_K = t^2 - 4q$$

Isogenies and endomorphism rings

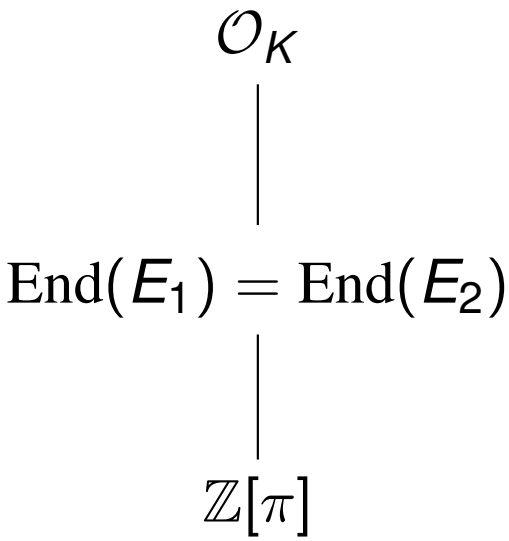
Let $\phi : E_1 \to E_2$ be an isogeny of degree ℓ.



descending



ascending



horizontal

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

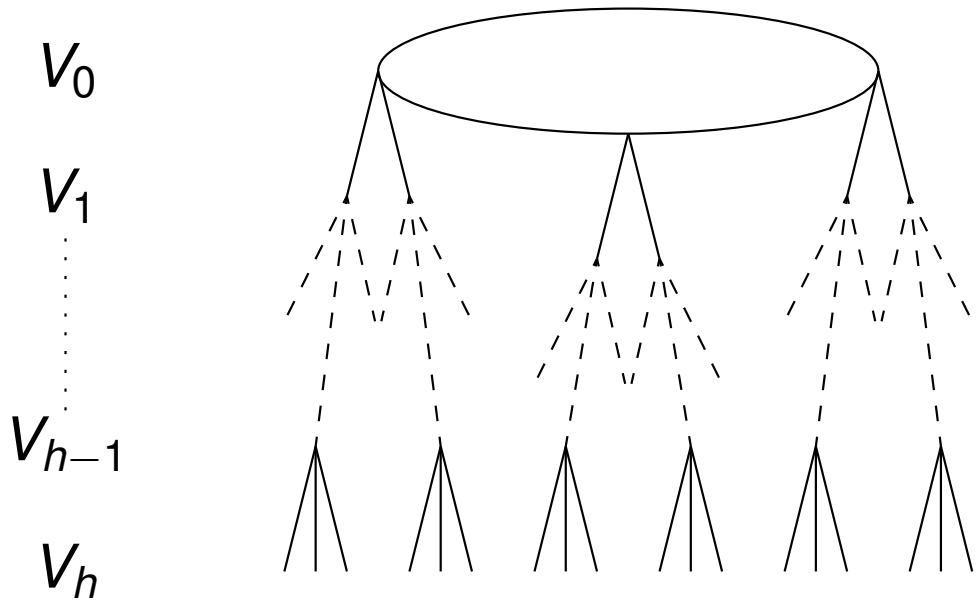
Isogenies and ℓ-volcanoes

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?



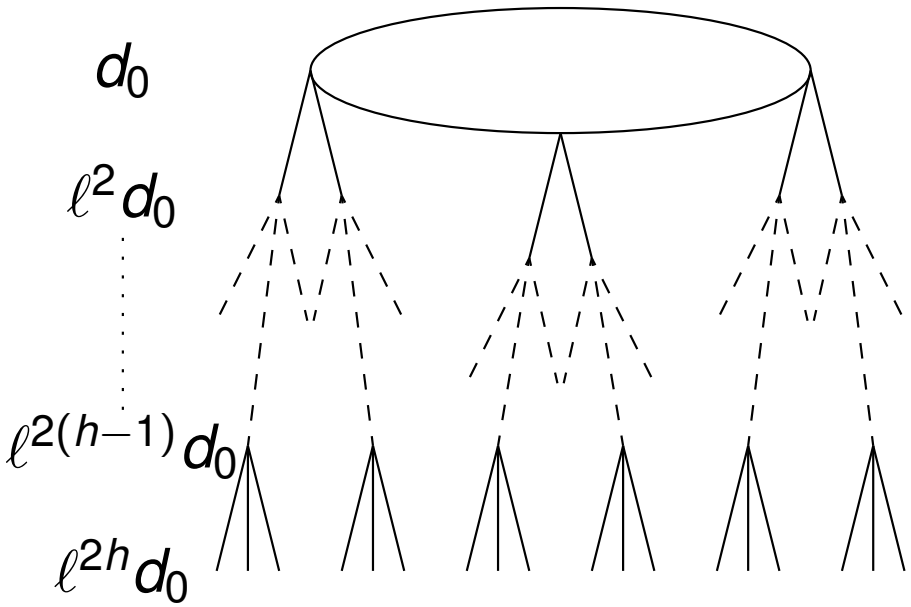
- V_0 (the *crater*) is regular connected of degree at most 2
- For $i > 0$, each vertex in V_i has one edge leading to a vertex in V_{i-1}
- For $i < h$, each vertex in V_i has degree $\ell + 1$.

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 $j \neq 0, 1728$).



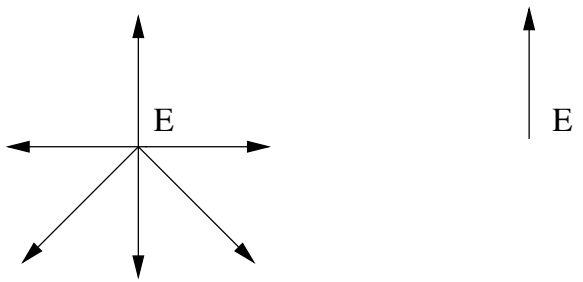
Curves on a fixed level have the same endomorphism ring.

Exploring the volcano

For a given curve E we want to find its neighbours

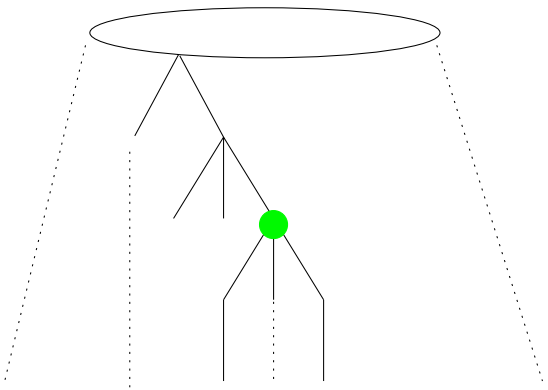
- Compute $E[\ell] \subset E(\mathbb{F}_{q^r})$ with $r < \ell$ and use Vélu's formulae $O(M(r)(\ell + \log q))$ with $M(r) = r \log r \log\log r$
- Use pairings to distinguish the ascending isogeny from the others (I.-Joux 2010)

or,



- Compute the modular polynomial $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$.
- Roots of $\Phi_\ell(X, j(E))$ in $\mathbb{F}_q$ give curves ℓ-isogenous to E. $O(\ell^2 + M(\ell) \log q)$ with $M(\ell) = \ell \log \ell \log\log \ell$

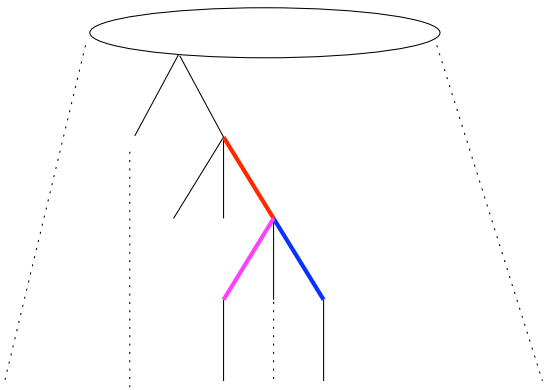
Descending (Kohel 1996, Fouquet-Morain 2002)



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

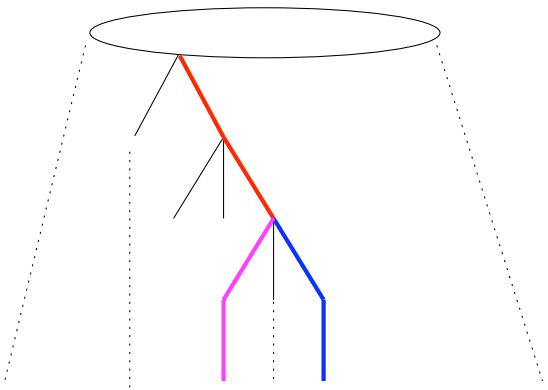
Descending (Kohel 1996, Fouquet-Morain 2002)



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

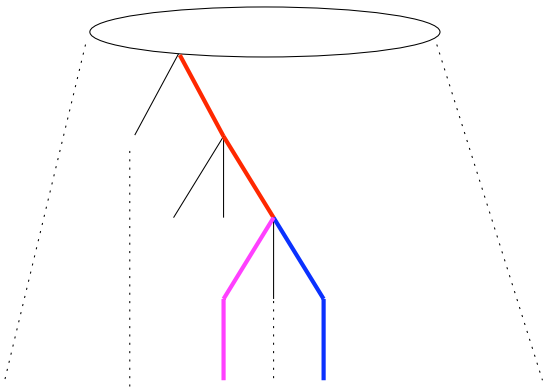
Descending (Kohel 1996, Fouquet-Morain 2002)



- 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 2002)



- 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
$O(h(\ell^2 + M(\ell)\log q))$
Use pairings as a compass. Construct one path
$O(h(rM(r)\log q + n_2 \log \ell))$

- Bottlenecks: isogeny computation, group structure 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

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

Isogeny walk is expensive...

and dangerous!

The Tate pairing

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

$$\Rightarrow \quad \ell^{n_2} | q^r - 1$$

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

$$T_{\ell^{n_2}} : E[\ell^{n_2}] \times E(\mathbb{F}_{q^r})/\ell^{n_2}E(\mathbb{F}_{q^r}) \longrightarrow \mu_{\ell^{n_2}}$$

$$(P, Q) \longrightarrow \left(\frac{f_{\ell^{n_2},P}(Q+R)}{f_{\ell^{n_2},P}(R)}\right)^{\frac{q-1}{\ell^{n_2}}}$$

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

A symmetric pairing

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

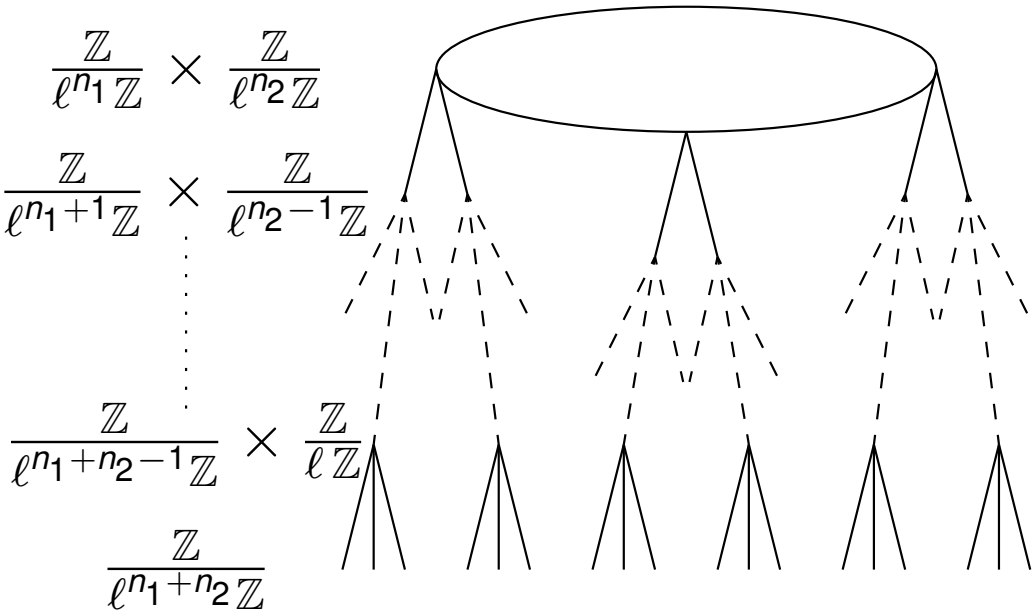
$$S(P,Q) = T_{\ell^{n_2}}(P,Q)\,T_{\ell^{n_2}}(Q,P)$$

- S symmetric
- If $S \neq 1$ there is $k > 0$ such that

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

When is S non-degenerate? What is k?

Regular volcanoes



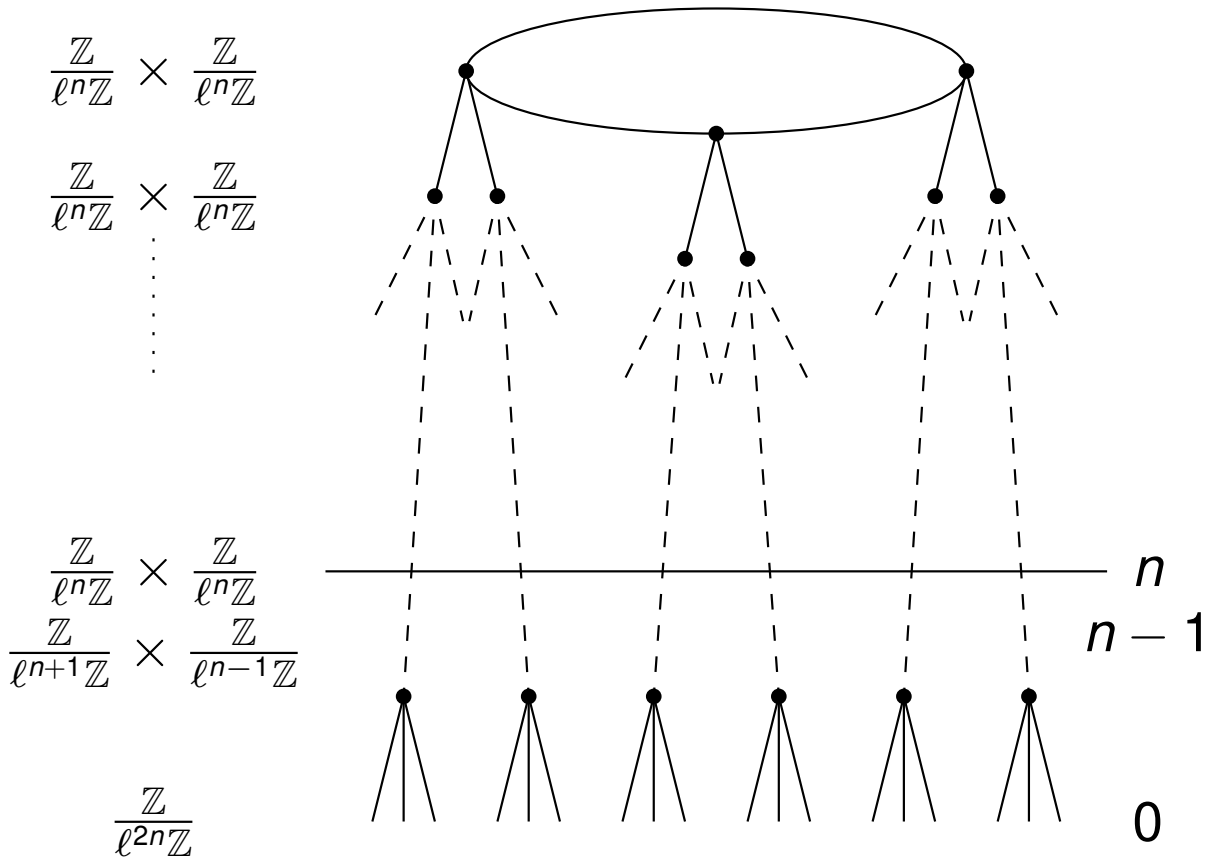
Miret et al. 2006

ℓ-Sylow group structure is different at every level.

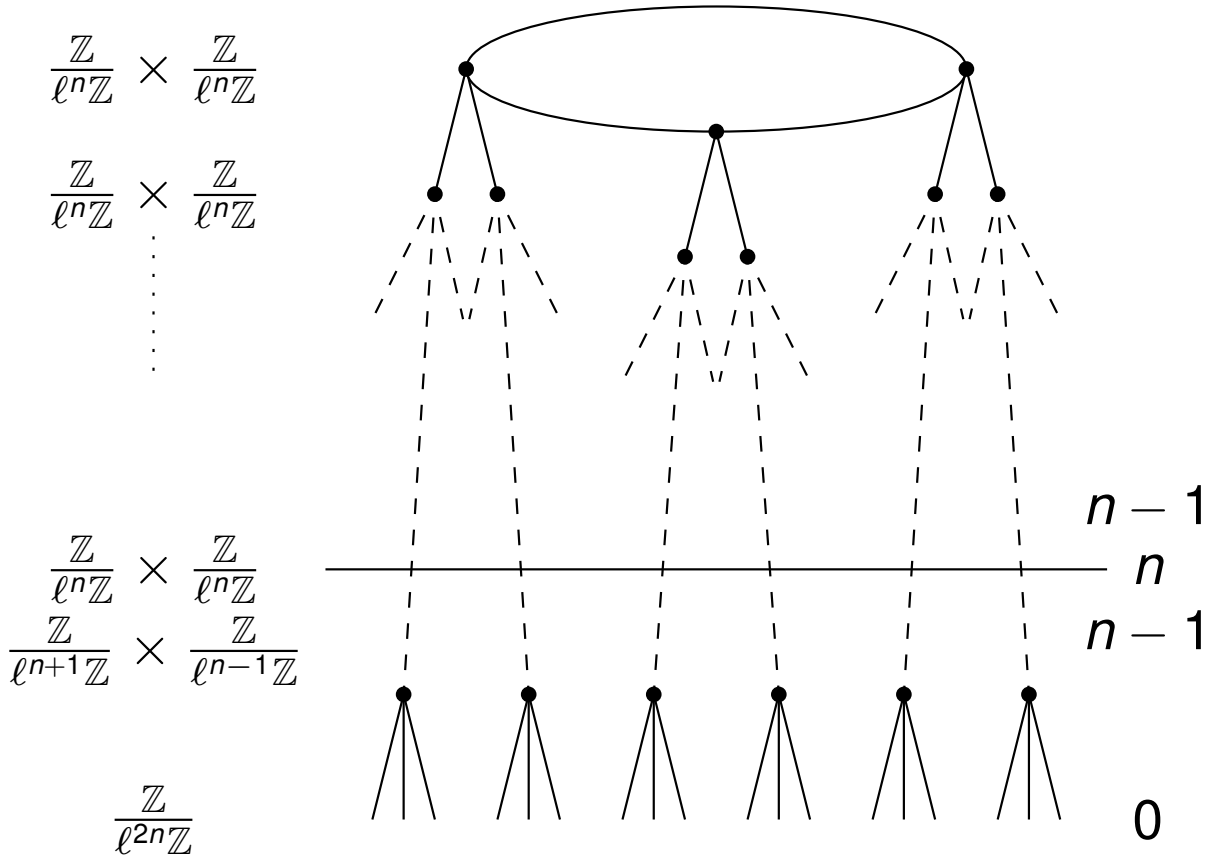
Regular volcanoes

On regular volcanoes S is a non-degenerate pairing ($k = n_2$).

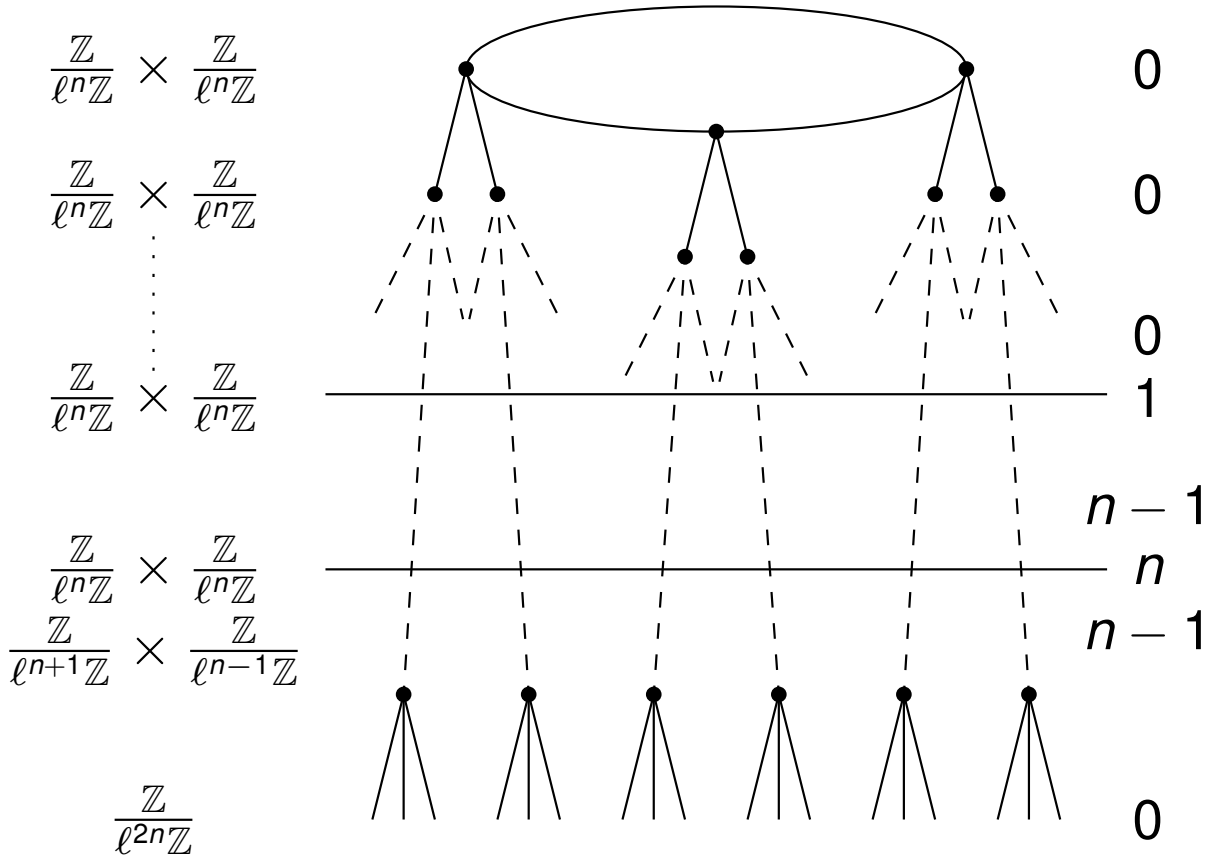
Towards endomorphism ring computation via pairings



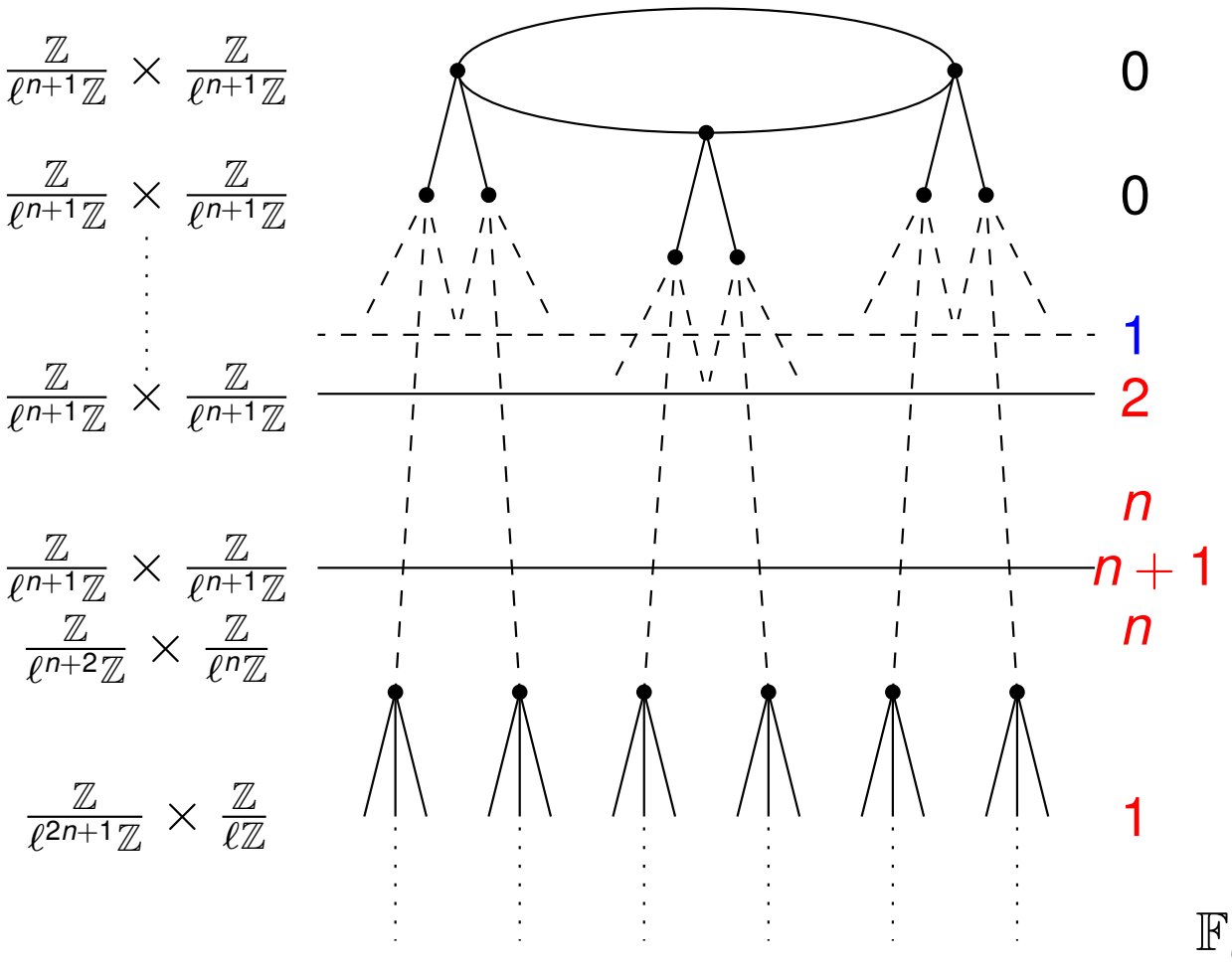
Towards endomorphism ring computation via pairings



Towards endomorphism ring computation via pairings



Towards endomorphism ring computation via pairings



Algorithm

- Compute $E(\ell^{n_2})(F_{q^r}) =< P, Q >$
- Note
  $S(aP + bQ, cP + dQ) = S(P, P)^{ac} S(P, Q)^{ad+bc} S(Q, Q)^{bd}$
- Compute $S(P, P)$, $S(P, Q)$ and $S(Q, Q)$ and get k.
- If $k = n_2$ then $v_\ell(f) = h - n_2$
- If $k < n_2$ then $v_\ell(f) = h - (2n_2 - k)$
- If $k = 0$ might need to roll down a little.

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

Computing the distance to the floor

<table>
<tr><td>Kohel (1996)
Fouquet-Morain (2002)</td><td colspan="2">Isogeny walk
$h(\ell^2 + M(\ell)\log q)$</td></tr>
<tr><td>I.-Joux (2010)
$r \approx \ell/2$</td><td>Group structure and pairings
$h(rM(r)(\log q + n_2 \log \ell))$</td><td>Isogeny walk
$h(r\,M(r)(1 + \log q))$</td></tr>
<tr><td>This work
$r \approx \ell/2$</td><td colspan="2">Group structure and pairings
$rM(r)\log q + n_2 \log \ell$</td></tr>
</table>

QUESTIONS?