MATHEMATICS OF COMPUTATION
Volume 82, Number 281, January 2013, Pages 581–603
S 0025-5718(2012)02622-6
Article electronically published on July 24, 2012

PAIRING THE VOLCANO

SORINA IONICA AND ANTOINE JOUX

Abstract. Isogeny volcanoes are graphs whose vertices are elliptic curves and whose edges are ℓ-isogenies. Algorithms allowing to travel on these graphs were developed by Kohel in his thesis (1996) and later on, by Fouquet and Morain (2001). However, up to now, no method was known, to predict, before taking a step on the volcano, the direction of this step. Hence, in Kohel's and Fouquet-Morain's algorithms, many steps are taken before choosing the right direction. In particular, ascending or horizontal isogenies are usually found using a trial-and-error approach. In this paper, we propose an alternative method that efficiently finds all points P of order ℓ such that the subgroup generated by P is the kernel of a horizontal or an ascending isogeny. In many cases, our method is faster than previous methods. This is an extended version of a paper published in the proceedings of ANTS 2010. In addition, we treat the case of 2-isogeny volcanoes and we derive from the group structure of the curve and the pairing a new invariant of the endomorphism class of an elliptic curve. Our benchmarks show that the resulting algorithm for endomorphism ring computation is faster than Kohel's method for computing the ℓ-adic valuation of the conductor of the endomorphism ring for small ℓ.

1. Introduction

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, where $q = p^r$ is a prime power. Let π be the Frobenius endomorphism, i.e., $\pi(x, y) \mapsto (x^q, y^q)$ and denote by t its trace. Assume that E is an ordinary curve and let $\mathcal{O}_E$ denotes its ring of endomorphisms. We know [22, Th. V.3.1] that $\mathcal{O}_E$ is an order in an imaginary quadratic field K. Let $d_\pi = t^2 - 4q$ be the discriminant of π. We can write $d_\pi = g^2 d_K$, where d_K is the discriminant of the quadratic field K. There are only a finite number of possibilities for $\mathcal{O}_E$, since $\mathbb{Z}[\pi] \subset \mathcal{O}_E \subset \mathcal{O}_{d_K}$. Indeed, this requires that f, the conductor of $\mathcal{O}_E$, divides g, the conductor of $\mathbb{Z}[\pi]$. The cardinality of E over $\mathbb{F}_q$ is $\#E(\mathbb{F}_q) = q + 1 - t$. Two isogenous elliptic curves over $\mathbb{F}_q$ have the same cardinality, and thus the same trace t. In his thesis [14], Kohel studies how curves in $\mathrm{Ell}_t(\mathbb{F}_q)$, the set of curves defined over $\mathbb{F}_q$ with trace t, are related via isogenies of degree ℓ. More precisely, he describes the structure of the graph of ℓ-isogenies defined on $\mathrm{Ell}_t(\mathbb{F}_q)$. He relates this graph to orders in $\mathcal{O}_K$ and uses modular polynomials to find the conductor of $\mathrm{End}(E)$.

Fouquet and Morain [8] call the connected components of this graph *isogeny volcanoes* and show that it is possible to travel through these structures using modular polynomials, even without knowing the cardinality of the curve. Moreover, they compute the ℓ-adic valuation of the trace t, for $\ell | g$ and hence obtain some

Received by the editor November 16, 2010 and, in revised form, August 30, 2011.
2010 *Mathematics Subject Classification.* Primary 14H52; Secondary 14K02.
This work has been carried out at Prism Laboratory, University of Versailles and is part of the author's PhD thesis.

information on the cardinality of the curve. Recently, more applications of isogeny volcanoes were found: the computation of Hilbert class polynomials [1, 24], of modular polynomials [3] and of endomorphism rings of elliptic curves [2].

All the above methods make use of algorithms for traveling efficiently on volcanoes. These algorithms need to walk on the crater, to descend from the crater to the floor or to ascend from the floor to the crater. In many cases, the structure of the ℓ-Sylow subgroup of the elliptic curve, allows one, after taking a step on the volcano, to decide whether this step is ascending, descending or horizontal (see [17, 18]). Note that, since a large fraction of isogenies are descending, finding one of them is quite easy. However, no known method can find horizontal or ascending isogenies without using a trial-and-error approach. In this paper, we describe a first solution to this open problem, which applies when the cardinality of the curve is known, and propose a method that efficiently finds a point P of order ℓ that spans the kernel of an ascending (or horizontal isogeny). Our approach relies on the computation of a small number of pairings. We then show that our algorithms for traveling on the volcano are, in many cases, faster than the ones from [14] and [8]. In addition, we obtain a simple method that detects most curves on the crater of their volcano. Until now, the only curves that were easily identified were those on the floor of volcanoes. Finally, we introduce an invariant for curves lying at the same level in the ℓ-volcano. In order to compute this invariant, we need to compute the group structure and a few pairings. This paper is organized as follows: Sections 2 and 3 present definitions and properties of isogeny volcanoes and pairings. Section 4 explains our method to find ascending or horizontal isogenies using pairing computations. Finally, in Section 5, we use this method to improve the algorithms for ascending a volcano, for walking on its crater and for computing the ℓ-adic valuation of the conductor of the endomorphism ring.

2. Background on isogeny volcanoes

In this paper, we rely on some results from complex multiplication theory and on Deuring's lifting theorems. We denote by $\mathcal{Ell}_d(\mathbb{C})$ the set of $\mathbb{C}$-isomorphism classes of elliptic curves whose endomorphism ring is the order $\mathcal{O}_d$, with discriminant $d < 0$. In this setting, there is an action of the class group of $\mathcal{O}_d$ on $\mathcal{Ell}_d(\mathbb{C})$. Let $E \in \mathcal{Ell}_d(\mathbb{C})$, Λ its corresponding lattice and $\mathfrak{a}$ an $\mathcal{O}_d$-ideal. We have a canonical homomorphism from $\mathbb{C}/\Lambda$ to $\mathbb{C}/\mathfrak{a}^{-1}\Lambda$ which induces an isogeny usually denoted by $E \to \hat{\mathfrak{a}} * E$. This action on $\mathcal{Ell}_d(\mathbb{C})$ is transitive and free [23, Prop. II.1.2]. Moreover [23, Cor. II.1.5], the degree of the application $E \to \hat{\mathfrak{a}} * E$ is $N(\mathfrak{a})$, the norm of the ideal $\mathfrak{a}$.

Let $\mathbb{F}_q$ be a finite field, with $q = p^r$ and p a prime number. We denote by $\mathcal{Ell}_d(\mathbb{F}_q)$ the set of isomorphism classes of elliptic curves defined over $\mathbb{F}_q$, having endomorphism ring $\mathcal{O}_d$. From Deuring's theorems [6], if p is a prime number that splits completely in the ring class field of $\mathcal{O}_d$, we get a bijection $\mathcal{Ell}_d(\mathbb{C}) \to \mathcal{Ell}_d(\mathbb{F}_q)$. Furthermore, the class group action in characteristic zero respects this bijection, and we get an action of the class group also on $\mathcal{Ell}_d(\mathbb{F}_q)$.

2.1. **Isogeny volcanoes.** Consider an elliptic curve E defined over a finite field $\mathbb{F}_q$. Let ℓ be a prime different from $\mathrm{char}(\mathbb{F}_q)$ and $I : E \to E'$ be an ℓ-isogeny, i.e., an isogeny of degree ℓ. We denote by $\mathcal{O}_d$ and $\mathcal{O}_{d'}$ the endomorphism rings of E and E', respectively. As shown in [14], this means that $\mathcal{O}_d$ contains $\mathcal{O}_{d'}$ or $\mathcal{O}_{d'}$ contains $\mathcal{O}_d$ or the two endomorphism rings coincide. If $\mathcal{O}_d$ contains $\mathcal{O}_{d'}$, we say that I is

a *descending* isogeny. Otherwise, if $\mathcal{O}_d$ is contained in $\mathcal{O}_{d'}$, we say that I is an *ascending* isogeny. If $\mathcal{O}_d$ and $\mathcal{O}_{d'}$ are equal, then we call the isogeny *horizontal*. In his thesis, Kohel shows that horizontal isogenies exist only if the conductor of $\mathcal{O}_d$ is not divisible by ℓ. Moreover, in this case there are exactly $\left(\frac{d}{\ell}\right)+1$ horizontal ℓ-isogenies, where d is the discriminant of $\mathcal{O}_d$. If $\left(\frac{d}{\ell}\right)=1$, then ℓ is split in $\mathcal{O}_d$ and the two horizontal isogenies correspond to the two actions $E \to \hat{\mathfrak{l}} * E$ and $E \to \hat{\bar{\mathfrak{l}}} * E$, where the two ideals $\mathfrak{l}$ and $\bar{\mathfrak{l}}$ satisfy $(\ell) = \mathfrak{l}\bar{\mathfrak{l}}$. In a similar way, if $\left(\frac{d}{\ell}\right)=0$, then ℓ is ramified, i.e., $(\ell) = \mathfrak{l}^2$ and there is exactly one horizontal isogeny starting from E. In order to describe the structure of the graph whose vertices are (isomorphism classes of) elliptic curves with a fixed number of points and whose edges are ℓ-isogenies, we recall the following definition [24].

Definition 2.1. An ℓ-volcano is a connected undirected graph with vertices partitioned into levels $V_0, \ldots, V_h$, in which the subgraph on V_0 (the *crater*) is a regular connected graph of degree at most 2 and

(a) for $i > 0$, each vertex in V_i has exactly one edge leading to a vertex in V_{i-1}, and every edge not on the crater is of this form;
(b) for $i < h$, each vertex in V_i has degree $\ell + 1$.

We call the level V_h *the floor* of the volcano. Vertices lying on the floor have degree 1. The following proposition [24] follows essentially from [14, Prop. 23].

Proposition 2.2. *Let p be a prime number, $q = p^r$, and $d_\pi = t^2 - 4q$. Take $\ell \neq p$ another prime number. Let G be the undirected graph with vertex set* $\mathrm{Ell}_t(\mathbb{F}_q)$ and edges ℓ-isogenies defined over $\mathbb{F}_q$. We denote by ℓ^h the largest power of ℓ dividing the conductor of d_π. Then the connected components of G that do not contain curves with j-invariant 0 or 1728 are ℓ-volcanoes of height h and for each component V, we have:

(a) The elliptic curves whose j-invariants lie in V_0 have endomorphism rings isomorphic to some $\mathcal{O}_{d_0} \supseteq \mathcal{O}_{d_\pi}$ whose conductor is not divisible by ℓ.
(b) The elliptic curves whose j-invariants lie in V_i have endomorphism rings isomorphic to $\mathcal{O}_{d_i}$, where $d_i = \ell^{2i} d_0$.

Elliptic curves are determined by their j-invariant, up to a twist[1]. Throughout the paper, we refer to a vertex in a volcano by giving the curve or its j-invariant.

2.2. **Exploring the volcano.** Given a curve E on an ℓ-volcano, two methods are known to find its neighbours. The first method relies on the use of modular polynomials. The ℓ-th *modular polynomial*, denoted by $\Phi_\ell(X, Y)$ is a polynomial with integer coefficients. It satisfies the following property: given two elliptic curves E and E' with j-invariants $j(E)$ and $j(E')$ in $\mathbb{F}_q$, there is an ℓ-isogeny from E to E' defined over $\mathbb{F}_q$, if and only if, $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$ and $\Phi_\ell(j(E), j(E')) = 0$. As a consequence, the curves related to E via an ℓ-isogeny can be found by solving $\Phi_\ell(X, j(E)) = 0$. As stated in [21], this polynomial[2] may have 0, 1, 2 or $\ell+1$ roots in $\mathbb{F}_q$. In order to find an edge on the volcano, it suffices to find a root j' of this polynomial. Finally, if we need the equation of the curve E' with j-invariant j', we may use the formula in [21].

[1] For a definition of twists of elliptic curves, refer to [22].

[2] The case where the modular polynomial does not have any root corresponds to a degenerate case of isogeny volcanoes containing a single curve and no ℓ-isogenies.

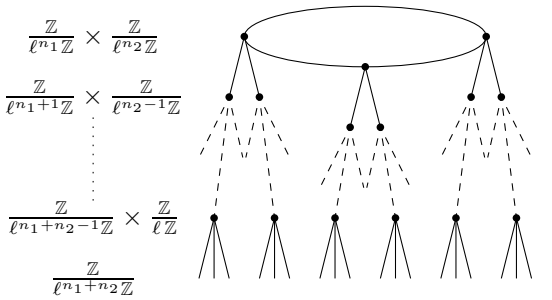

FIGURE 1. A regular volcano

The second method to build ℓ-isogenous curves constructs, given a point P of order ℓ on E, the ℓ-isogeny $I : E \to E'$ whose kernel G is generated by P using Vélu's classical formulae [25] in an extension field $\mathbb{F}_{q^r}$. To use this approach, we need the explicit coordinates of points of order ℓ on E. We denote by G_i, $1 \leq i \leq \ell+1$, the $\ell+1$ subgroups of order ℓ of E. Miret et al. [18] give the degree r_i of the smallest extension field of $\mathbb{F}_q$ such that $G_i \subset \mathbb{F}_{q^{r_i}}$, $1 \leq i \leq \ell+1$. This degree is related to the order of q in the group $\mathbb{F}_\ell^*$, that we denote by $\mathrm{ord}_\ell(q)$.

Proposition 2.3. *Let E defined over $\mathbb{F}_q$ be an elliptic curve with κ rational ℓ-isogenies, with $\ell > 2$. Let G_i, $1 \leq i \leq \kappa$, be the kernels of these isogenies, and let r_i be the minimum value for which $G_i \subset E(\mathbb{F}_{q^{r_i}})$.*

(a) *If $\kappa = 1$, then $r_1 = ord_\ell(q)$ or $r_1 = 2ord_\ell(q)$.*
(b) *If $\kappa = \ell+1$, then either $r_i = ord_\ell(q)$ for all i, or $r_i = 2ord_\ell(q)$ for all i.*
(c) *If $\kappa = 2$, then $r_i | \ell - 1$ for $i = 1, 2$.*

In some cases, if the ℓ-torsion is not defined over $\mathbb{F}_q$, it may be preferable to replace the curve by its twist, if the ℓ-torsion of the twist is defined over an extension field of smaller degree. We also need the following corollary [18].

Corollary 2.4. *Let $E/\mathbb{F}_q$ be an elliptic curve over $\mathbb{F}_q$ and $\tilde{E}$ its quadratic twist. If $E/\mathbb{F}_q$ has 1 or $\ell+1$ rational ℓ-isogenies, then $\#E(\mathbb{F}_{q^{ord_\ell q}})$ or $\#\tilde{E}(\mathbb{F}_{q^{ord_\ell q}})$ is a multiple of ℓ. Moreover, if there are $\ell+1$ rational isogenies, then it is a multiple of ℓ^2.*

2.3. **The group structure of the elliptic curve on the volcano.** Lenstra [13] relates the group structure of an elliptic curve to its endomorphism ring by proving that $E(\mathbb{F}_q) \simeq \mathcal{O}_E/(\pi - 1)$ as $\mathcal{O}_E$-modules. It is thus natural to see how this structure relates to the isogeny volcano. From Lenstra's equation, we can deduce that $E(\mathbb{F}_q) \simeq \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, for some positive integers N and M with $N|M$. We denote by g the conductor of $\mathbb{Z}[\pi]$ and we write $\pi = a + g\omega$, with:

$$a = \begin{cases} (t-g)/2 \\ t/2 \end{cases} \quad \text{and } \omega = \begin{cases} \frac{1+\sqrt{d_K}}{2} & \text{if } d_K \equiv 1 \pmod 4, \\ \sqrt{\frac{d_K}{4}} & \text{if } d_K \equiv 0 \pmod 4. \end{cases}$$

where d_K is the discriminant of the quadratic imaginary field containing $\mathcal{O}_E$. Note that N is maximal such that $E[N] \subset E(\mathbb{F}_q)$ and by [20, Lemma 1] we get that $N = \gcd(a-1, g/f)$, with f the conductor of $\mathrm{End}(E)$. Note, moreover, that $N|M$, $N|(q-1)$ and $MN = \#E(\mathbb{F}_q)$. This implies that on an ℓ-volcano the group structure of all the curves in a given level is the same.

Let E be a curve on the isogeny volcano such that $v_\ell(N) < v_\ell(M)$. As explained in [17] (in the case $\ell = 2$, but the result is general), a is such that $v_\ell(a-1) \geq \min\{v_\ell(g), v_\ell(\#E(\mathbb{F}_q))/2\}$.

Since $N = \gcd(a-1, g/f)$ and $v_\ell(N) \leq v_\ell(\#E(\mathbb{F}_q))/2$, it follows that $v_\ell(N) = v_\ell(g/f)$. As we descend, the valuation at ℓ of the conductor f increases by 1 at each level (by Proposition 2.2b). This implies that the ℓ-valuation of N for curves at each level decreases by 1 and is equal to 0 for curves lying on the floor. Note that if $v_\ell(\#E(\mathbb{F}_q))$ is even and the height h of the volcano is greater than $v_\ell(\#E(\mathbb{F}_q))$, the structure of the ℓ-torsion group is unaltered from the crater down to the level $h - v_\ell(\#E(\mathbb{F}_q))/2$. From this level down, the structure of the ℓ-torsion groups starts changing as explained above. In the sequel, we call this level the *first stability level*.[3] A volcano with first stability level equal to 0, i.e., on the crater, is called *regular* (see Figure 1).

Notations. Let $n \geq 0$. We denote by $E[\ell^n]$ the ℓ^n-torsion subgroup, i.e., the subgroup of points of order dividing ℓ^n on the curve E, by $E[\ell^n](\mathbb{F}_{q^k})$ the subgroup of points of order dividing ℓ^n defined over an extension field of $\mathbb{F}_q$ and by $E[\ell^\infty](\mathbb{F}_q)$ the ℓ-Sylow subgroup of $E(\mathbb{F}_q)$.

3. Background on pairings

Let E be an elliptic curve defined over some finite field $\mathbb{F}_q$, m an integer such that $m|\#E(\mathbb{F}_q)$. Let k be the embedding degree, i.e., the smallest integer such that $m|q^k - 1$. Let $P \in E[m](\mathbb{F}_{q^k})$ and $Q \in E(\mathbb{F}_{q^k})/mE(\mathbb{F}_{q^k})$. Let $f_{m,P}$ be the function whose divisor[4] is $m(P) - m(O)$, where O is the point at infinity of the curve E. Take R a random point in $E(\mathbb{F}_{q^k})$ such that the support of the divisor $D = (Q+R) - (R)$ is disjoint from the support of $f_{m,P}$. Then we can define the Tate pairing as follows:

$$\begin{aligned} t_m : E[m](\mathbb{F}_{q^k}) \times E(\mathbb{F}_{q^k})/mE(\mathbb{F}_{q^k}) &\to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^m \\ (P, Q) &\to f_{m,P}(Q+R)/f_{m,P}(R). \end{aligned}$$

The Tate pairing is a bilinear non-degenerate map, i.e., for all $P \in E[m](\mathbb{F}_{q^k})$ different from O there is a $Q \in E(\mathbb{F}_{q^k})/mE(\mathbb{F}_{q^k})$ such that $T_m(P,Q) \neq 1$. The output of the pairing is only defined up to a coset of $(\mathbb{F}_{q^k}^*)^m$. However, for implementation purposes, it is useful to have a uniquely defined value and to use the *reduced* Tate pairing, i.e., $T_m(P,Q) = t_m(P,Q)^{(q-1)/m} \in \mu_m$, where μ_m denotes the group of m-th roots of unity. Pairing computation can be done in $O(\log m)$ operations in $\mathbb{F}_q$ using Miller's algorithm [16]. For more details and properties of pairings, the reader can refer to [9]. Note that in recent years, in view of cryptographic applications, many implementation techniques have been developed and pairings on elliptic curves can be computed very efficiently[5].

In the remainder of this paper we assume that the embedding degree is always 1, i.e., $m|q-1$. We will denote by k a different integer. Suppose now that $m = \ell^n$, with $n \geq 1$ and ℓ prime. Now let P and Q be two ℓ^n-torsion points on E. We define the following symmetric pairing [12]:

$$S(P,Q) = (T_{\ell^n}(P,Q)\, T_{\ell^n}(Q,P))^{\frac{1}{2}}. \tag{3.1}$$

[3] Miret et al. call it simply *the stability level*.

[4] For background on divisors, see [22].

[5] See [10] for a fast recent implementation.

Note that for any point P, $T_{\ell^n}(P,P) = S(P,P)$. In the remainder of this paper, we call $S(P,P)$ *the self-pairing* of P. We focus on the case where the pairing S is non-constant. Suppose now that P and Q are two linearly independent ℓ^n-torsion points. Then all ℓ^n-torsion points R can be expressed as $R = aP + bQ$. Using bilinearity and symmetry of the S-pairing, we get

$$\log(S(R,R)) = a^2 \log(S(P,P)) + 2ab \log(S(P,Q)) + b^2 \log(S(Q,Q)) \pmod{\ell^n},$$

where log is a discrete logarithm function in μ_{ℓ^n}. We denote by $k(E)$ the largest integer such that the polynomial

$$\mathcal{P}(a,b) = a^2 \log(S(P,P)) + 2ab \log(S(P,Q)) + b^2 \log(S(Q,Q)) \tag{3.2}$$

is identically zero modulo $\ell^{n-k(E)-1}$ and non-zero modulo $\ell^{n-k(E)}$. Obviously, since S is non-constant we have $0 \leq k(E) < n$. Dividing by $\ell^{n-k(E)-1}$, we may thus view $\mathcal{P}$ as a polynomial in $\mathbb{F}_\ell[a,b]$. When we want to emphasize the choice of E and ℓ^n, we write $\mathcal{P}_{E,\ell^n}$ instead of $\mathcal{P}$.

Since $\mathcal{P}$ is a non-zero quadratic polynomial, it has at most two homogeneous roots, which means that from all the $\ell+1$ subgroups of $E[\ell^n]/E[\ell^{n-1}] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$, at most 2 have self-pairings in $\mu_{\ell^{k(E)}}$ (see also [12]). In the remainder of this paper, we denote by N_{E,ℓ^n} the number of zeros of $\mathcal{P}_{E,\ell^n}$. Note that this number does not depend on the choice of the two generators P and Q of the ℓ^n-torsion subgroup $E[\ell^n]$. Moreover, we say that a ℓ^n-torsion point R has *degenerate self-pairing* if $T_{\ell^n}(R,R)$ is a $\ell^{k(E)}$-th root of unity and that R has *non-degenerate self-pairing* if $T_{\ell^n}(R,R)$ is a primitive $\ell^{k(E)+1}$-th root of unity. Also, if $T_{\ell^n}(R,R)$ is a primitive ℓ^n-th root of unity, we say that R has *primitive self-pairing*.

4. Determining directions on the volcano

In this section, we explain how we can distinguish between different directions on the volcano by making use of pairings. Given a point $P \in E[\ell^n](\mathbb{F}_q)$, we also need to know the degree of the smallest extension field containing an ℓ^{n+1}-torsion point such that $\ell\tilde{P} = P$. The following result is taken from [7].

Proposition 4.1. *Let $\ell > 2$ and $E/\mathbb{F}_q$ be an elliptic curve which lies on an ℓ-volcano whose height $h(V)$ is different from 0. Then the height of V', the ℓ-volcano of the curve $E/\mathbb{F}_{q^s}$ is $h(V') = h(V) + v_\ell(s)$.*

From this proposition, it follows easily that if the structure of the subgroup $E[\ell^\infty](\mathbb{F}_q)$ on the curve E is $\mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$, then the smallest extension K of $\mathbb{F}_q$ such that $E[\ell^\infty](K)$ is not isomorphic to $E[\ell^\infty](\mathbb{F}_q)$ is $\mathbb{F}_{q^\ell}$.

Proposition 4.2. *Let $\ell > 2$ and $E/\mathbb{F}_q$ be an elliptic curve with $E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$, with $n_2 \geq 1$. Then*

$$E[\ell^\infty](\mathbb{F}_{q^\ell}) \simeq \mathbb{Z}/\ell^{n_1+1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2+1}\mathbb{Z}.$$

Proof. Note that E lies on an ℓ-volcano $V/\mathbb{F}_q$ of height at least n_2. We consider a curve E' lying on the floor of $V/\mathbb{F}_q$ such that there is a descending path of isogenies between E and E'. Obviously, we have $E'[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^{n_1+n_2}\mathbb{Z}$. By Proposition 4.1, $V/\mathbb{F}_{q^\ell}$ has one extra down level, which means that the curve E' is no longer on the floor, but on the level just above the floor. Consequently, we have that $E'[\ell] \subset E'(\mathbb{F}_{q^\ell})$ and, moreover, $E'[\ell^\infty](\mathbb{F}_{q^\ell}) \simeq \mathbb{Z}/\ell^{n_1+n_2+\Delta}\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.

We now show that $\Delta = 1$. Note first that $\ell^{n_2} | q-1$ and that $v_\ell(q^\ell - 1) = v_\ell(q-1) + 1$. We denote by P a point of order $\ell^{n_1+n_2+\Delta}$ on the curve $E'/\mathbb{F}_{q^\ell}$. Then, without restraining the generality, we may assume that

$$T_{\ell^{n_2}}^{(\mathbb{F}_q)}(\ell^{n_1+\Delta}P, \ell^\Delta P) = f_{\ell^{n_2}, \ell^{n_1+\Delta}P}(\ell^\Delta P)^{\frac{q-1}{\ell^{n_2}}} \in \mu_{\ell^{n_2}} \backslash \mu_{\ell^{n_2-1}} \tag{4.1}$$

and

$$T_{\ell^{n_2+1}}^{(\mathbb{F}_{q^\ell})}(\ell^{n_1+\Delta-1}P, P) = f_{\ell^{n_2+1}, \ell^{n_1+\Delta-1}P}(P)^{\frac{q^\ell-1}{\ell^{n_2+1}}} \in \mu_{\ell^{n_2+1}} \backslash \mu_{\ell^{n_2}}. \tag{4.2}$$

By using the bilinearity of the pairing and the fact that $f_{\ell^{n_2+1},R} = f_{\ell^{n_2},R}^\ell$ for a point of order ℓ^{n_2} (up to a constant), we get from equation (4.1)

$$f_{\ell^{n_2}, \ell^{n_1+\Delta}P}(P)^{\ell \frac{q^\ell-1}{\ell^{n_2+1}}} \in \mu_{\ell^{n_2}} \backslash \mu_{\ell^{n_2-1}}.$$

By using equality (4.1), this is true if and only if $\Delta = 1$. By ascending on the volcano from E' to E, we deduce that the structure of the ℓ-torsion of E over $\mathbb{F}_{q^\ell}$ is necessarily

$$E[\ell^\infty](\mathbb{F}_{q^\ell}) \simeq \mathbb{Z}/\ell^{n_1+1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2+1}\mathbb{Z}. \qquad \square$$

Remark 4.3. If $\ell = 2$, the only problematic case is when the ℓ-adic valuation of the conductor of $\mathbb{Z}[\pi]$ is 1. In all the other cases, the volcano gets exactly one extra level over $\mathbb{F}_{q^2}$ (see [7]). Reasoning as in the proof of Proposition 4.2, we get that for a curve E on a 2-volcano of height at least 2 such that $E[2^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/2^{n_1}\mathbb{Z} \times \mathbb{Z}/2^{n_2}\mathbb{Z}$, the 2-Sylow group structure over $\mathbb{F}_{q^2}$ is

$$E[2^\infty](\mathbb{F}_{q^2}) \simeq \mathbb{Z}/2^{n_1+\Delta}\mathbb{Z} \times \mathbb{Z}/2^{n_2+1}\mathbb{Z}.$$

However, the following example shows that when $\ell = 2$, Δ is not always 1.

Example 4.4. Let E be an an elliptic curve defined over $\mathbb{F}_q$ with $q = 257$ given by the equation

$$y^2 = x^3 + 206x^2 + 221x + 33.$$

Then $E[2^\infty][\mathbb{F}_q] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $E[2^\infty][\mathbb{F}_{q^2}] \simeq \mathbb{Z}/2^4\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z}$.

Remark 4.5. We note that in the general context of ordinary abelian varieties, Freeman and Lauter [15] proved that if the ℓ^n-torsion is defined over a finite field $\mathbb{F}_q$, then the ℓ^{n+1}-torsion is defined over $\mathbb{F}_{q^\ell}$.

We give some lemmas explaining the relations between pairings on two isogenous curves.

Lemma 4.6. *Suppose $E/\mathbb{F}_q$ is an elliptic curve and P, Q are points in $E(\mathbb{F}_q)$ of order ℓ^n, $n \geq 1$. Denote by $\tilde{P}, \tilde{Q} \in E[\bar{\mathbb{F}}_q]$ two points such that $\ell\tilde{P} = P$ and $\ell\tilde{Q} = Q$. Suppose that $\ell^n | q-1$. Then we have the following relations for the Tate pairing:*

(a) *If $\tilde{P}, \tilde{Q} \in E[\mathbb{F}_q]$, then $T_{\ell^{n+1}}(\tilde{P}, \tilde{Q})^{\ell^2} = T_{\ell^n}(P, Q)$.*

(b) *Suppose $\ell \geq 3$. If $\tilde{Q} \in E[\mathbb{F}_{q^\ell}] \backslash E[\mathbb{F}_q]$, then $T_{\ell^{n+1}}(\tilde{P}, \tilde{Q})^\ell = T_{\ell^n}(P, Q)$.*

(c) *Let $\ell = 2$ and $\tilde{Q} \in E[\mathbb{F}_{q^2}] \backslash E[\mathbb{F}_q]$. Then $T_{2^{n+1}}(\tilde{P}, \tilde{Q})^\ell = T_{2^n}(P, Q) T_{2^n}(P, T)$, where T is a point of order 2.*

Proof. (a) By writing down the divisors of the functions $f_{\ell^{n+1},\tilde{P}}$, $f_{\ell^n,\tilde{P}}$, $f_{\ell^n,P}$, one can easily check that

$$f_{\ell^{n+1},\tilde{P}} = (f_{\ell,\tilde{P}})^{\ell^n} \cdot f_{\ell^n,P}.$$

We evaluate these functions at some points $Q+R$ and R (where R is carefully chosen) and raise the equality to the power $(q-1)/\ell^n$.

(b) Due to the equality on divisors $\mathrm{div}(f_{\ell^{n+1},P}) = \mathrm{div}(f^{\ell}_{\ell^n,P})$, we have

$$T_{\ell^{n+1}}(\tilde{P},\tilde{Q})^{\ell} = T_{\ell^n}^{(\mathbb{F}_{q^\ell})}(P,\tilde{Q}),$$

where $T_{\ell^n}^{(\mathbb{F}_{q^\ell})}$ is the ℓ^n-Tate pairing for E defined over $\mathbb{F}_{q^\ell}$. It suffices then to show that $T_{\ell^n}^{(\mathbb{F}_{q^\ell})}(P,\tilde{Q}) = T_{\ell^n}(P,Q)$. We have

$$\begin{aligned} T_{\ell^n}^{(\mathbb{F}_{q^\ell})}(P,\tilde{Q}) &= f_{\ell^n,P}([\tilde{Q}+R]-[R])^{\frac{(1+q+\cdots+q^{\ell-1})(q-1)}{\ell^n}} \\ &= f_{\ell^n,P}((\tilde{Q}+R)+(\pi(\tilde{Q})+R)+(\pi^2(\tilde{Q})+R)+\dots \\ &+ (\pi^{\ell-1}(\tilde{Q})+R)-\ell(R))^{\frac{(q-1)}{\ell^n}} \end{aligned} \tag{4.3}$$

where R is a random point defined over $\mathbb{F}_q$. It is now easy to see that for $\ell \geq 3$,

$$\tilde{Q}+\pi(\tilde{Q})+\pi^2(\tilde{Q})+\cdots+\pi^{\ell-1}(\tilde{Q}) = \ell\tilde{Q} = Q, \tag{4.4}$$

because $\pi(\tilde{Q}) = \tilde{Q}+T$, where T is a point of order ℓ. By applying Weil's reciprocity law [22, Ex. II.2.11], it follows that the equation (4.3) becomes

$$T_{\ell^n}^{(\mathbb{F}_{q^\ell})}(P,\tilde{Q}) = \left(\frac{f_{\ell^n,P}(Q+R)}{f_{\ell^n,P}(R)}\right)^{\frac{q-1}{\ell^n}} f((P)-(O))^{q-1}, \tag{4.5}$$

where f is such that $\mathrm{div}(f) = (\tilde{Q}+R)+(\pi(\tilde{Q})+R)+(\pi^2(\tilde{Q})+R)+\cdots+(\pi^{\ell-1}(\tilde{Q})+R)-(Q+T+R)-(\ell-1)(R)$. Note that this divisor is $\mathbb{F}_q$-rational, so $f((P)-(O))^{q-1}=1$. This concludes the proof.

(c) The sum at (4.4) becomes

$$\tilde{Q}+\pi(\tilde{Q}) = Q+T, \tag{4.6}$$

where T is a point of order 2. Consequently, we have an equation similar to equation (4.5)

$$T_{2^n}^{(\mathbb{F}_{q^2})}(P,\tilde{Q}) = \left(\frac{f_{2^n,P}(Q+T+R)}{f_{2^n,P}(R)}\right)^{\frac{q-1}{2^n}} f((P)-(O))^{q-1},$$

where f is such that $\mathrm{div}(f) = (\tilde{Q}+R)+(\pi(\tilde{Q})+R)-(Q+T+R)-(R)$. We know that f is rational, hence $f((P)-(O))^{q-1}=1$. We conclude that

$$T_{2^{n+1}}(\tilde{P},\tilde{Q})^2 = T_{2^n}(P,Q)T_{2^n}(P,T). \qquad \square$$

Lemma 4.7. *Let $\phi : E \to E'$ be a separable isogeny defined over a finite field $\mathbb{F}_q$, $\ell \in \mathbb{Z}$ such that $\ell | q-1$.*

(a) *Denote by d the degree of the isogeny and by P an ℓ-torsion on the curve E such that $\phi(P)$ is an ℓ-torsion point on E', and Q a point on E. Then we have*

$$T_\ell(\phi(P),\phi(Q)) = T_\ell(P,Q)^d.$$

(b) *Let $\phi : E \to E'$ be a separable isogeny of degree ℓ defined over $\mathbb{F}_q$, P a $\ell\ell'$-torsion point such that $Ker\ \phi = \langle \ell' P \rangle$ and Q a point on the curve E. Then we have*

$$T_\ell(\phi(P),\phi(Q)) = T_{\ell\ell'}(P,Q)^{\ell}.$$

Proof. (a) We have

$$\begin{aligned}(\phi)^*(f_{\ell,\phi(P)}) &= \ell \sum_{K\in\mathrm{Ker}\phi}((P+K)-(K)) = \ell \sum_{K\in\mathrm{Ker}\phi}((P)-(O)) \\ &+ \mathrm{div}\left(\left(\prod_{K\in\mathrm{Ker}\phi}\frac{l_{K,P}}{v_{K+P}}\right)^{\ell}\right),\end{aligned}$$

where $l_{K,P}$ is the straight line passing through K and P and v_{K+P} is the vertical line passing through $K+P$. It follows that for some point S on E

$$f_{\ell,\phi(P)}\circ\phi(S) = f_{\ell,P}^{d}(S)\left(\prod_{K\in\mathrm{Ker}\phi}\frac{l_{K,P}(S)}{v_{K+P}(S)}\right)^{\ell}.$$

We obtain the desired formula by evaluating the equality above at two points carefully chosen $Q+R$ and R, and then by raising to the power $\frac{q-1}{\ell}$.

(b) This time we have

$$\begin{aligned}(\phi)^*(f_{\ell',\phi(P)}) &= \ell' \sum_{K\in\mathrm{Ker}\phi}((P+K)-(K)) = \ell' \sum_{K\in\mathrm{Ker}\phi}((P)-(O)) \\ &+\mathrm{div}\left(\left(\prod_{K\in\mathrm{Ker}\phi}\frac{l_{K,P}}{v_{K+P}}\right)^{\ell'}\right).\end{aligned}$$

Since $\#\mathrm{Ker}\phi = \ell$, we get

$$f_{\ell',\phi(P)}\circ\phi(Q) = f_{\ell\ell',P}(Q)\left(\prod_{K\in\mathrm{Ker}\phi}\frac{l_{K,P}(Q)}{v_{K+P}(Q)}\right)^{\ell'}.$$

We raise this equality to the power $\frac{q-1}{\ell'}$ and get the announced result. □

Proposition 4.8. *Let E be an elliptic curve defined as a finite field $\mathbb{F}_q$ and assume that $E[\ell^\infty](\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/\ell^{n_1}\mathbb{Z}\times\mathbb{Z}/\ell^{n_2}\mathbb{Z}$ (with $n_1\geq n_2\geq 1$). Suppose that there is an ℓ^{n_2}-torsion point P such that $T_{\ell^{n_2}}(P,P)$ is a primitive ℓ^{n_2}-th root of unity. Then the ℓ-isogeny whose kernel is generated by $\ell^{n_2-1}P$ is descending. Moreover, the curve E does not lie above the first stability level of the corresponding ℓ-volcano.*

Proof. Let $I_1 : E\to E_1$ be the isogeny whose kernel is generated by $\ell^{n_2-1}P$ and suppose this isogeny is ascending or horizontal. This means that $E_1[\ell^{n_2}]$ is defined over $\mathbb{F}_q$. Take Q another ℓ^{n_2}-torsion point on E, such that $E[\ell^{n_2}] = \langle P,Q\rangle$ and denote by $Q_1 = I_1(Q)$. One can easily check that the dual of I_1 has kernel generated by $\ell^{n_2-1}Q_1$. It follows that there is a point $P_1\in E_1[\ell^{n_2}]$ such that $P = \hat{I_1}(P_1)$. By Lemma 4.7 this means that $T_\ell(P,P)\in\mu_{\ell^{n_2-1}}$, which is false. This proves not only that the isogeny is descending, but also that the structure of the ℓ-torsion is different at the level of E_1. Hence E cannot be above the stability level. □

Proposition 4.9. *Let $E/\mathbb{F}_q$ be a curve which lies in an ℓ-volcano and on the first stability level. Suppose $E[\ell^\infty](\mathbb{F}_q)\simeq\mathbb{Z}/\ell^{n_1}\mathbb{Z}\times\mathbb{Z}/\ell^{n_2}\mathbb{Z}$, $n_1\geq n_2\geq 1$.*

(a) *Suppose $\ell\geq 3$. Then there is at least one ℓ^{n_2}-torsion point $E(\mathbb{F}_q)$ with primitive self-pairing.*

(b) *If $\ell = 2$ and the height of the volcano is greater than 1, then there is at least one ℓ^{n_2}-torsion point $E(\mathbb{F}_q)$ with primitive self-pairing.*

Proof. (a) Let P be a ℓ^{n_1}-torsion point and Q be a ℓ^{n_2}-torsion point such that $\{P, Q\}$ generates $E[\ell^\infty](\mathbb{F}_q)$.

Case 1. Suppose $n_1 \geq n_2 \geq 2$. Let $E \xrightarrow{I_1} E_1$ be a descending ℓ-isogeny and denote by P_1 and Q_1 the ℓ^{n_1+1} and ℓ^{n_2-1}-torsion points generating $E_1[\ell^\infty](\mathbb{F}_p)$. Moreover, without loss of generality, we may assume that $I_1(P) = \ell P_1$ and $I_1(Q) = Q_1$. If $T_{\ell^{n_2-1}}(Q_1, Q_1)$ is a primitive ℓ^{n_2-1}-th root of unity, $T_{\ell^{n_2}}(Q, Q)$ is a primitive ℓ^{n_2}-th root of unity by Lemma 4.7. If not, from the non-degeneration of the pairing, we deduce that $T_{\ell^{n_2-1}}(Q_1, P_1)$ is a primitive ℓ^{n_2-1}-th root of unity, which means that $T_{\ell^{n_2-1}}(Q_1, \ell P_1)$ is a ℓ^{n_2-2}-th primitive root of unity. By applying Lemma 4.7, we get $T_{\ell^{n_2}}(Q, P) \in \mu_{\ell^{n_2-1}}$ at best. It follows that $T_{\ell^{n_2}}(Q, Q) \in \mu_{\ell^{n_2}}$ by the non-degeneracy of the pairing.

Case 2. If $n_2 = 1$, then consider the volcano defined over the extension field $\mathbb{F}_{q^\ell}$. There is an ℓ^2-torsion point $\tilde{Q} \in E(\mathbb{F}_{q^\ell})$ with $Q = \ell\tilde{Q}$. We obviously have $\ell^2 | q^\ell - 1$ and from Lemma 4.6, we get $T_{\ell^2}(\tilde{P}, \tilde{P})^\ell = T_\ell(P, P)$. By applying Case 1, we get that $T_{\ell^2}(\tilde{P}, \tilde{P})$ is a primitive ℓ^2-th root of unity, so $T_\ell(P, P)$ is a primitive ℓ-th root of unity.

(b) If $n_2 > 1$, the proof is similar to that of (a) Case 1. Suppose now that $n_2 = 1$. Since $4 | \#E(\mathbb{F}_q)$, we have $q + 1 - t \equiv 0 \bmod 4$. Then $t^2 - 4q \equiv (q-1)^2 \bmod 4$. We deduce that E lies on a 2-volcano with height greater than 1 if and only if $q \equiv 1 \bmod 4$. Let E' be a curve on the floor of the ℓ-volcano such that there is a 2-ascending isogeny $I : E' \to E$. The fact that $4 | q - 1$ implies that the 4-th Tate pairing is well-defined over $\mathbb{F}_q$ and non-degenerate. We have $E'[2^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/4\mathbb{Z}$ and thus there is a point $P \in E'[4](\mathbb{F}_q)$ such that $T_4(P, P) \in \mu_4^*$ and that $I(2P) = 0$. By applying Lemma 4.7, we get that

$$T_2(I(P), I(P)) \in \mu_2^*. \qquad \square$$

We now make use of a result on the representation of ideal classes of orders in imaginary quadratic fields. This is Corollary 7.17 from [5].

Lemma 4.10. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. Given a nonzero integer M, then every ideal class in $Cl(\mathcal{O})$ contains a proper $\mathcal{O}$-ideal whose norm is relatively prime to M.*

Proposition 4.11. *We use the notations and assumptions from Proposition* 2.2. *Furthermore, we assume that for all curves E_i lying at a fixed level i in V the curve structure is $\mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$, with $n_1 \geq n_2 \geq 1$. The value of $N_{E_i, \ell^{n_2}}$, the number of zeros of the polynomial defined at* (3.2)*, is constant for all curves lying at level i in the volcano.*

Proof. Let E_1 and E_2 be two curves lying at level i in the volcano V. Then by Proposition 2.2 they both have endomorphism ring isomorphic to some order $\mathcal{O}_{d_i}$. Now by taking into account the fact that the action of $\mathrm{Cl}(\mathcal{O}_{d_i})$ on $\mathcal{E}\ell\ell_{d_i}(\mathbb{F}_q)$ is transitive, we consider an isogeny $\phi : E_1 \to E_2$ of degree ℓ_1. By applying Lemma 4.10, we may assume that $(\ell_1, \ell) = 1$. Now take, P and Q two independent ℓ^{n_2}-torsion points on E_1 and denote by $\mathcal{P}_{E_1, \ell^{n_2}}$ the quadratic polynomial corresponding to the ℓ^{n_2}-torsion on E_1 as in (3.2). We use Lemma 4.7 to compute $S(\phi(P), \phi(P))$,

$S(\phi(P),\phi(Q))$ and $S(\phi(Q),\phi(Q))$ and deduce that a polynomial $\mathcal{P}_{E_2,\ell^{n_2}}(a,b)$ on the curve E_2 computed from $\phi(P)$ and $\phi(Q)$ is such that

$$\mathcal{P}_{E_1,\ell^{n_2}}(a,b) = \mathcal{P}_{E_2,\ell^{n_2}}(a,b).$$

This means that $N_{E_1,\ell^{n_2}}$ and $N_{E_2,\ell^{n_2}}$ coincide, which concludes the proof. Moreover, we have showed that the value of $k(E_1) = k(E_2)$. □

Proposition 4.12. *Let E be an elliptic curve defined as a finite field $\mathbb{F}_q$ and let $E[\ell^\infty](\mathbb{F}_q)$ be isomorphic to $\mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$ with $n_1 \geq n_2 \geq 1$. Suppose $N_{E,\ell^{n_2}} \in \{1,2\}$ and let P be an ℓ^{n_2}-torsion point with degenerate self-pairing. Then the ℓ-isogeny whose kernel is generated by $\ell^{n_2-1}P$ is either ascending or horizontal. Moreover, for any ℓ^{n_2}-torsion point Q whose self-pairing is non-degenerate, the isogeny with kernel spanned by $\ell^{n_2-1}Q$ is descending.*

Proof.

Case 1. Suppose $T_{\ell^{n_2}}(P,P) \in \mu_{\ell^{k(E)}}$, $k(E) \geq 1$ and that $T_{\ell^{n_2}}(Q,Q) \in \mu_{\ell^{k(E)+1}} \setminus \mu_{\ell^{k(E)}}$. Denote by $I_1 : E \to E_1$ the isogeny whose kernel is generated by $\ell^{n_2-1}P$ and $I_2 : E \to E_2$ the isogeny whose kernel is generated by $\ell^{n_2-1}Q$. By repeatedly applying Lemmas 4.6 and 4.7, we get the following relations for points generating the ℓ^{n_2-1}-torsion on E_1 and E_2:

$$\begin{aligned} T_{\ell^{n_2-1}}(I_1(P), I_1(P)) &\in \mu_{\ell^{k(E)-1}},\ T_{\ell^{n_2-1}}(\ell I_1(Q), \ell I_1(Q)) \in \mu_{\ell^{k(E)-2}} \setminus \mu_{\ell^{k(E)-3}}, \\ T_{\ell^{n_2-1}}(\ell I_2(P), \ell I_2(P)) &\in \mu_{\ell^{k(E)-3}},\ T_{\ell^{n_2-1}}(I_2(Q), I_2(Q)) \in \mu_{\ell^{k(E)}} \setminus \mu_{\ell^{k(E)-1}} \end{aligned}$$

with the convention that $\mu_{\ell^h} = \emptyset$ whenever $h \leq 0$. From the relations above, we deduce that on the ℓ-volcano having E, E_1 and E_2 as vertices, E_1 and E_2 do not lie at the same level. Given the fact that there are at least $\ell - 1$ descending rational ℓ-isogenies parting from E and that Q is any of the $\ell - 1$ (or more) ℓ^{n_2}-torsion points with non-degenerate self-pairing, we conclude that I_1 is horizontal or ascending and that I_2 is descending.

Case 2. Suppose now that $k(E) = 0$. Note that the case $n_2 = 1$ was already treated in Proposition 4.8. If $n_2 > 1$, we consider the curve E defined over $\mathbb{F}_{q^\ell}$. For $\ell > 3$, by Lemma 4.6b we have $k(E) = 1$ for points on $E/\mathbb{F}_{q^\ell}$, and we may apply *Case* 1. The case $\ell = 2$ is treated inside the proof of Theorem 4.15. □

Remark 4.13. If E is a curve lying under the first stability level and that $E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$, with $n_1 > n_2$, then it suffices to find a point P_1 of order ℓ^{n_1} and the point $\ell^{n_1-1}P_1$ generates the kernel of a horizontal or ascending isogeny (P_1 has degenerate self-pairing).

Corollary 4.14. *Let E be a curve on an ℓ-volcano such that the polynomial $\mathcal{P}_{E,\ell^{n_2}}$ is non-zero over $\mathbb{F}_q$. If ℓ is split in the maximal order $\mathcal{O}_{d_K}$, then E is on the crater if and only if $N_{E,\ell^{n_2}}$ is 2. Otherwise, ℓ is inert in $\mathcal{O}_{d_K}$ if and only if $N_{E,\ell^{n_2}} = 0$.*

Two stability levels. Remember that in any irregular volcano, $v_\ell(\#E(\mathbb{F}_q))$ is even and the height h of the volcano is greater than $v_\ell(\#E(\mathbb{F}_q))$. Moreover, all curves at the top of the volcano have $E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^{n_2}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$ with $n_2 = \frac{v_\ell(\#E(\mathbb{F}_q))}{2}$. The existence of a primitive self-pairing of an ℓ^{n_2}-torsion point on any curve lying on the first stability level implies that the polynomial $\mathcal{P}$ is non-zero at every level from the first stability level up to the level $\max(h + 1 - 2n_2, 0)$ (by Lemma 4.7). We call this level *the second level of stability*. This is illustrated in

Figure 2. When the second stability level of a volcano is 0, we say that the volcano is *almost regular*.

Consider now E a curve on the second stability level and $I : E \to E_1$ an ascending isogeny. Let P be an ℓ^{n_2}-torsion point on E and assume that $T_{\ell^{n_2}}(P, P) \in \mu_\ell^*$. We denote by $\bar{P} \in E(\mathbb{F}_{q^\ell})\backslash E(\mathbb{F}_q)$ a point such that $\ell\bar{P} = P$. By Lemma 4.6, $T_{\ell^{n_2+1}}(\bar{P}, \bar{P})$ is a primitive ℓ^2-th root of unity. It follows by Lemma 4.7 that $T_{\ell^{n_2}}(I(P), I(P))$ is a primitive ℓ-th root of unity. We deduce that $\mathcal{P}_{E_1,\ell^{n_2+1}}$ corresponding to $E_1/\mathbb{F}_{q^\ell}$ is non-zero. Applying this reasoning repeatedly, we conclude that for every curve E above the second stability level there is an extension field $\mathbb{F}_{q^{\ell^s}}$ such that the polynomial $\mathcal{P}_{E,\ell^{n_2+s}}$ associated to the curve defined over $\mathbb{F}_{q^{\ell^s}}$ is non-zero. We will show that the degree of this extension field characterizes uniquely curves lying on a fixed level of the volcano, above the second stability level.

Let E be an elliptic curve. We suppose that

$$E(\mathbb{F}_q)[\ell^\infty] \simeq \mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}.$$

We define $\mathcal{L}_{\ell,E}$ as follows

$$\mathcal{L}_{\ell,E} = \begin{cases} n_1, \text{ if } E \text{ is under/on the first stability level} \\ \\ k(E)+1, \text{ if } E \text{ is above the first stability level and} \\ \text{ below the second stability level,} \\ \\ -s+1, \text{ if } E \text{ is above the second stability level,} \end{cases}$$

where s is the smallest integer such that the polynomial $\mathcal{P}$ of the curve E defined over $\mathbb{F}_{q^{\ell^s}}$ is non-zero.

Theorem 4.15. *Let E be an elliptic curve in* $\mathrm{Ell}_t(\mathbb{F}_q)$. Then $\mathcal{L}_{\ell,E}$ is an invariant of the level of the curve in its ℓ-volcano.

Proof.

Case 1. Suppose $\ell \geq 3$. If E lies below the first stability level, then the structure of the ℓ-Sylow group of the curve changes from one level to another and n_1 characterizes the level of the curve in its ℓ-volcano.

Suppose now that E lies below the crater, on the first stability level or above it. Take P and Q to be two points such that $E[\ell^{n_2}] = \langle P, Q\rangle$ and we may assume that P has non-degenerate self-pairing, i.e., $T_{\ell^{n_2}}(P, P) \in \mu_{\ell^{k(E)+1}}\backslash\mu_{\ell^{k(E)}}$, and that Q has degenerate self-pairing, i.e., $T_{\ell^{n_2}}(Q, Q) \in \mu_{\ell^{k(E)}}$. The point $\ell^{n_2-1}Q$ generates the kernel of an ascending isogeny $I : E \to E'$. We denote by $P' = I(P)$ and, by using Lemma 4.7, we get

$$T_{\ell^{n_2}}(P', P') \in \mu_{\ell^{k(E)}}\backslash\mu_{\ell^{k(E)-1}}.$$

Note that P' is such that $\ell^{n_2-1}P'$ generates the kernel of $\hat{I}$, which is a descending isogeny. Consequently, the self-pairing of P' is non-degenerate, which means that $k(E') = k(E) - 1$. By Proposition 4.9, we have that $k(E) = n_2 - 1$ if the curve E lies on the first stability level. The reasoning above implies that $k(E) = n_2 - 2$ for all curves lying one level above the first stability level. Iterating this procedure, it also follows that as we ascend from the first stability level to the second one, the value of $k(E)$ decreases by 1 at each level. In particular, it equals 0 at the second stability level and -1 at all levels above the second stability level (all self-pairings of curves on these levels are degenerate).

Suppose now that E is a curve below the crater, on the second stability level or above it. We show by induction that if the value of $k(E)$ corresponding to E defined over $\mathbb{F}_{q^{\ell^s}}$ is 0, then for a curve E' lying one level above the value $k(E')$ is 0 over $\mathbb{F}_{q^{\ell^{s+1}}}$ and $\mathbb{F}_{q^{\ell^{s+1}}}$ is the smallest extension field with this property. We suppose that

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

with $n_1 \geq n_2$. We consider P and Q two ℓ^{n_2}-torsion points such that $\langle P, Q\rangle = E[\ell^{n_2}]$ and that P has primitive self-pairing, while Q has degenerate self-pairing. We denote by $I : E \to E'$ the ascending isogeny whose kernel is generated by $\langle \ell^{n_2-1}Q\rangle$ and by $P' = I(P)$. By Lemma 4.7 we have

$$T_{\ell^{n_2}}(P', P') = 1.$$

Since $\ell^{n_2-1}P'$ generates the kernel of the dual $\hat{I}$, it follows that $k(E') = -1$ over $\mathbb{F}_{q^{\ell^s}}$. We denote by $\bar{P} \in E(\mathbb{F}_{q^{\ell^{s+1}}})$ a point such that $\ell\bar{P} = P$. By Lemma 4.6 we have that

$$T_{\ell^{n_2+1}}^{(\mathbb{F}_{q^{\ell^{s+1}}})}(\bar{P}, \bar{P}) \in \mu_{\ell^2} \backslash \mu_\ell.$$

By denoting $P'' = I(\bar{P})$, we get that

$$T_{\ell^{n_2+1}}(P'', P'') \in \mu_\ell^*.$$

It follows that $k(E') = 0$ over $\mathbb{F}_{q^{\ell^{s+1}}}$ and this is the smallest extension field with this property.

Case 2. We treat the case $\ell = 2$. Suppose that

$$E[2^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/2^{n_1}\mathbb{Z} \times \mathbb{Z}/2^{n_2}\mathbb{Z}.$$

If $n_2 > 1$, then

$$E[2^\infty](\mathbb{F}_{q^2}) \simeq \mathbb{Z}/2^{n_1+\Delta}\mathbb{Z} \times \mathbb{Z}/2^{n_2+1}\mathbb{Z}.$$

We consider points $\bar{P}, \bar{Q} \in E[2^{n_2+1}]$ and $P, Q \in E[2^{n_2}]$ such that $P = 2\bar{P}$ and $Q = 2\bar{Q}$. Then, by Lemma 4.6, we have

$$T_{2^{n_2+1}}(\tilde{P}, \tilde{Q})^2 = \pm T_{2^{n_2}}(P, Q).$$

Hence, if $k(E) \geq 2$, the proof is similar to the one of *Case 1*. We consider the curve E such that $k(E) = 1$ and we take a curve E' lying one level above such that there is an ascending isogeny $I : E \to E'$. Since $k(E) = 1$ and the kernel of I is degenerate, then there is a point $P \in E[\ell^{n_2}]$ such that $P' = I(P)$ generates the kernel of $\hat{I}$. By Lemma 4.7 we get that

$$T_{\ell^{n_2}}(P', P') \in \mu_\ell^*.$$

Hence the points of the kernel of any descending isogeny starting at E' have self-pairings primitive ℓ-th roots of unity. Reasoning as in the case $k(E) \geq 2$ over $\mathbb{F}_{q^2}$, we get that $k(E') = 1$ over $\mathbb{F}_{q^2}$. A point generating the kernel of an ascending or horizontal isogeny does not have distortion maps (see [4, Thm. 2.1]). Hence we have

$$T_{2^{n_2+1}}^2(\tilde{Q}, \tilde{Q}) = T_{2^{n_2}}(Q, Q), \tag{4.7}$$

for $Q \in E[\ell^{n_2}](\mathbb{F}_q), \tilde{Q} \in E[\mathbb{F}_{q^2}]$ such that $\ell\tilde{Q} = Q$ and that $\ell^{n_2-1}Q$ generates the kernel of an ascending isogeny. Since $k(E') = 1$ for E' defined over $\mathbb{F}_{q^2}$, we get that $T_{\ell^{n_2}}(Q, Q) = 1$. We conclude that $k(E') = 0$ over $\mathbb{F}_q$. By induction, we may show in a similar manner that there is an extension field over which all curves lying

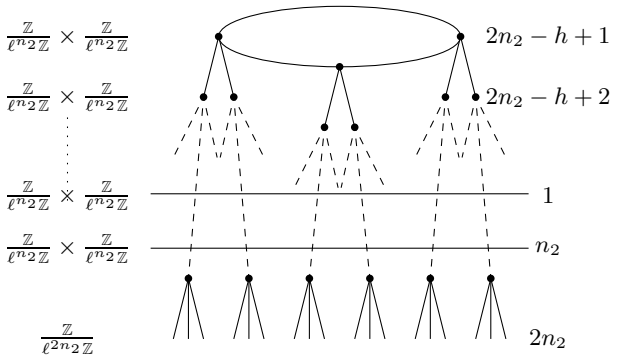

FIGURE 2. A level invariant in an ℓ-volcano

above the second stability level have polynomials $\mathcal{P}$ different from zero. If $n_2 = 1$, the first stability level and the second one coincide. If E is a curve on the first stability level of an irregular 2-volcano (i.e., $q \equiv 1 \bmod 4$), we consider the volcano defined over $\mathbb{F}_{q^2}$. As explained in Remark 4.3,

$$E[2^\infty](\mathbb{F}_{q^2}) \simeq \mathbb{Z}/2^{n_1+\Delta}\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z}$$

and since the curve lies on the first stability level, there are points of order 4 with primitive self-pairing, which implies that for any curve lying one level above, the polynomial $\mathcal{P}$ is different from zero. Over $\mathbb{F}_{q^2}$, we may reason as in the case $n_2 > 1$ and show that there is an extension field over which all curves lying above the first stability level have polynomials $\mathcal{P}$ different from zero.

Finally, if $n_2 = 1$ and the volcano is regular of height 1 (i.e., $q \equiv 3 \bmod p$), it is obvious that $\mathcal{L}_{\ell,E}$ is an invariant at every level of the volcano. □

We conclude this section by presenting an algorithm which determines the group structure of the ℓ^∞-torsion group of a curve E (Algorithm 1) and also an algorithm which outputs the kernel of a horizontal (ascending) isogeny from E, when $E[\ell^\infty](\mathbb{F}_q)$ is given (Algorithm 2).

We assume that the height of the volcano is $h \leq 2n_2 + 1$, or, equivalently, that the curve E lies on or below the second stability level, which implies that the polynomial $\mathcal{P}$ is non-zero at every level in the volcano. This allows us to distinguish between different directions of ℓ-isogenies departing from E. Algorithm 2 computes the level in the volcano of the curve E, which is equivalent to computing the level invariant $\mathcal{L}_{\ell,E}$.

Of course, similar algorithms can be given for curves lying above the second stability level, but in this case we need to consider the volcano over an extension field $\mathbb{F}_{q^{\ell^s}}$. Since computing points defined over extension fields of degree greater than ℓ is expensive, our complexity analysis in Section 5 will show that it is more efficient to use Kohel's and Fouquet-Morain algorithms to explore the volcano until the second level of stability is reached and to use Algorithms 1 and 2 afterwards.

Algorithm 1. Computing the structure of the ℓ^∞-torsion of E over $\mathbb{F}_q$ (assuming volcano height ≥ 1)

Require: A curve E defined over $\mathbb{F}_q$, a prime ℓ
Compute: Structure $\mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$, generators P_1 and P_2
Check that $q \equiv 1 \pmod{\ell}$ (if not, need to move to extension field: **abort**)
Let t be the trace of $E(\mathbb{F}_q)$
Check $q + 1 - t \equiv 0 \pmod{\ell}$ (if not, consider twist or **abort**)
Let $d_\pi = t^2 - 4q$, let z be the largest integer such that $\ell^z | d_\pi$ and $h = \lfloor \frac{z}{2} \rfloor$
Let n be the largest integer such that $\ell^n | q + 1 - t$ and $N = \frac{q+1-t}{\ell^n}$
Take a random point R_1 on $E(\mathbb{F}_q)$, let $P_1 = N \cdot R_1$
Let n_1 be the smallest integer such that $\ell^{n_1} P_1 = 0$
if $n_1 = n$ **then**
    Output: Structure is $\frac{\mathbb{Z}}{\ell^n\mathbb{Z}}$, generator P_1. **Exit**
    (E is on the floor, ascending isogeny with kernel $\langle \ell^{n-1} P_1 \rangle$)
end if
Take a random point R_2 on $E(\mathbb{F}_q)$, let $P_2 = N \cdot R_2$ and $n_2 = n - n_1$
Let $\alpha = \log_{\ell^{n_2} P_1}(\ell^{n_2} P_2) \pmod{\ell^{n_1 - n_2}}$
if α is undefined **then**
    Goto 6 ($\ell^{n_2} P_2$ does not belong to $\langle \ell^{n_2} P_1 \rangle$)
end if
Let $P_2 = P_2 - \alpha P_1$
If $\text{WeilPairing}_\ell(\ell^{n_1 - 1} P_1, \ell^{n_2 - 1} P_2) = 1$ **goto** 6 (This checks linear independence)
Output: Structure is $\frac{\mathbb{Z}}{\ell^{n_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^{n_2}\mathbb{Z}}$, generators (P_1, P_2)

Algorithm 2. Finding the level in the volcano and the kernel of ascending or horizontal isogenies
(Assuming curve not on floor and below the second stability level)

Require: A curve E, its structure $\frac{\mathbb{Z}}{\ell^{n_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^{n_2}\mathbb{Z}}$ and generators (P_1, P_2)
if $n_1 > n_2$ **then**
    The isogeny with kernel $\langle \ell^{n_1 - 1} P_1 \rangle$ is ascending or horizontal
    To check whether there is another, continue the algorithm
end if
Let g be a primitive ℓ-th root of unity in $\mathbb{F}_q$
Let $Q_1 = \ell^{n_1 - n_2} P_1$
Let $a = T_{\ell^{n_2}}(Q_1, Q_1)$, $b = T_{\ell^{n_2}}(Q_1, P_2) \cdot T_{\ell^{n_2}}(P_2, Q_1)$ and $c = T_{\ell^{n_2}}(P_2, P_2)$
If $(a, b, c) = (1, 1, 1)$ **abort** (Above the second stability level)
Let Count = 0.
repeat
    Let $a' = a$, $b' = b$ and $c' = c$
    Let $a = a^\ell$, $b = b^\ell$ and $c = c^\ell$
    Let Count = Count + 1
until $a = 1$ and $b = 1$ and $c = 1$
Let $L_a = \log_g(a')$, $L_b = \log_g(b')$ and $L_c = \log_g(c') \pmod{\ell}$
Let $\mathcal{P}(x, y) = L_a x^2 + L_b xy + L_c y^2 \pmod{\ell}$
If $n_1 = n_2$, let *LevelInvariant* = Count − 1 **else** *LevelInvariant* = n_1
Output: Level Invariant ($\mathcal{L}_{\ell,E}$) is *LevelInvariant*
If $\mathcal{P}$ has no homogenous roots modulo ℓ, **Output:** No isogeny (a single point on the crater)
If single root (x_1, x_2) **Output:** One isogeny with kernel $\langle \ell^{n_2 - 1}(x_1 Q_1 + x_2 P_2) \rangle$
if $\mathcal{P}$ has two roots (x_1, x_2) and (y_1, y_2) **then**
    Two isogenies with kernel $\langle \ell^{n_2 - 1}(x_1 Q_1 + x_2 P_2) \rangle$ and $\langle \ell^{n_2 - 1}(y_1 Q_1 + y_2 P_2) \rangle$
end if

5. Walking the volcano: modified algorithms

As mentioned in the introduction, several applications of isogeny volcanoes have recently been proposed. These applications require the ability to walk descending and ascending paths on the volcano and also to walk on the crater of the volcano. We recall that a *path* is a sequence of isogenies that never backtracks. We start this section with a brief description of existing algorithms for these tasks, based on methods given by Kohel [14] and by Fouquet and Morain in [8]. We present modified algorithms, which rely on the method presented in Algorithm 2 to find ascending or horizontal isogenies and to compute the level invariant $\mathcal{L}_{\ell,E}$. Then, we give complexity analysis for these algorithms and show that in many cases our method is competitive. Finally, we give two concrete examples in which the new algorithms can walk the crater of an isogeny volcano very efficiently compared to existing algorithms.

A brief description of existing algorithms. Existing algorithms rely on three essential properties in isogeny volcanoes. First, it is easy to detect that a curve lies on the floor of a volcano, since in that case, there is a single isogeny from this curve. Moreover, this isogeny can only be ascending (or horizontal if the height is 0). Second, if in an arbitrary path in a volcano there is a descending isogeny, then all the subsequent isogenies in the path are also descending. Third, from a given curve, there is either exactly one ascending isogeny or at most two horizontal ones. As a consequence, finding a descending isogeny from any curve is easy: it suffices to walk three paths in parallel until one path reaches the floor. This shortest path is necessarily descending and its length gives the level of the starting curve in the volcano. To find an ascending or horizontal isogeny, the classical algorithms try all possible isogenies until they find one which leads to a curve either at the same level or above the starting curve. This property is tested by constructing descending paths from all the neighbours of the initial curve and picking the curve which gave the longest path.

Note that alternatively, one could walk in parallel all of the $\ell + 1$ paths starting from the initial curve and keep the (two) longest as horizontal or ascending. As far as we know, this has not been proposed in the literature, but this variant of existing algorithms offers a slightly better asymptotic time complexity. For completeness, we give a pseudo-code description of this parallel variant of Kohel and Fouquet-Morain algorithms as Algorithm 3.

Basic idea of the modified algorithms. In our algorithms, we first need to choose a large enough extension field to guarantee that the kernels of all required isogenies are spanned by ℓ-torsion points defined on this extension field. As explained in Corollary 2.4, the degree r of this extension field is the order of q modulo ℓ and it can be computed very quickly after factoring $\ell - 1$. As usual, we choose an arbitrary irreducible polynomial of degree r to represent $\mathbb{F}_{q^r}$. Points of order ℓ are computed by running Algorithm 1, this time over $\mathbb{F}_{q^r}$. Once this is done, assuming that we are starting from a curve below the second level of stability, we use Algorithm 2 to find all ascending or horizontal isogenies from the initial curve. In order to walk a descending path, it suffices to choose any other isogeny. Note that, in the subsequent steps of a descending path, in the cases where the group structure satisfies $n_1 > n_2$, it is not necessary to run Algorithm 2 as a whole. Indeed, since we know that we are not on the crater, there is a single ascending isogeny and it is

Algorithm 3. Parallel variant of ascending/horizontal step (using modular polynomials)

Require: A j-invariant j_0 in $\mathbb{F}_q$, a prime ℓ, the modular polynomial $\Phi_\ell(X, Y)$.
Let $f(x) = \Phi_\ell(X, j_0)$
Compute J_0 the list of roots of $f(x)$ in $\mathbb{F}_q$
If $\#J_0 = 0$ **Output:** "Trivial volcano" **Exit**
If $\#J_0 = 1$ **Output:** "On the floor, step leads to:", $J_0[1]$ **Exit**
If $\#J_0 = 2$ **Output:** "On the floor, two horizontal steps to:", $J_0[1]$ and $J_0[2]$ **Exit**
Let $J = J_0$. Let J' and K be empty lists. Let Done = **false**.
repeat
  Perform multipoint evaluation of $\Phi_\ell(X, j)$, for each $j \in J$. Store in list F
  for i from 1 to $\ell + 1$ **do**
    Perform partial factorization of $F[i]$, computing at most two roots r_1 and r_2
    if $F[i]$ has less than two roots **then**
      Let Done = **true**. Append $\perp$ to K (Reaching floor)
    else
      If $r_1 \in J'$ **then** append r_1 to K **else** append r_2 to K. (Don't backtrack)
    end if
  end for
  Let $J' = J$, $J = K$ and K be the empty list
until Done
for each i from 1 to $\ell + 1$ such that $J[i] \neq \perp$ append $J_0[i]$ to K
Output: "Possible step(s) lead to:" K (One or two outputs)

spanned by $\ell^{n_1-1}P_1$. Note that in order to determine the level of the curve in the volcano and hence the ℓ-adic valuation of the endomorphism ring we do not need to take any steps on the volcano. Indeed, Algorithm 2 computes the level invariant $\mathcal{L}_{\ell,E}$ with three pairing computations and several exponentiations to the power ℓ. Finally, above the second stability level, we have two options. In theory, we can consider curves over larger extension fields (in order to get polynomials $\mathcal{P} \neq 0$). Note that this is too costly in practice. Therefore, we use pre-existing algorithms, but it is not necessary to follow descending paths all the way to the floor. Instead, we can stop these paths at the second stability level, where our methods can be used.

Computing endomorphism rings. Kohel [14] describes a deterministic algorithm to compute the endomorphism ring of an elliptic curve. For small values of ℓ and when a large power of ℓ divides the conductor of the endomorphism ring, he uses algorithms traveling on isogeny volcanoes to find the shortest path from the curve to the floor and thus determine the level of the curve in the volcano. We propose replacing the descent to the floor by a computation of the level invariant $\mathcal{L}_{\ell,E}$. On an almost regular volcano this is done by computing the structure of the ℓ-Sylow group and then by computing the value of $k(E)$.

5.1. **Complexity analysis.**

Computing a single isogeny. Before analyzing the complete algorithms, we first compare the costs of taking a single step on a volcano by using the two methods existing in the literature: modular polynomials and classical Vélu's formulae. Suppose that we wish to take a step from a curve E. With the modular polynomial approach, we have to evaluate the polynomial $f(X) = \Phi_\ell(X, j(E))$ and find its roots in $\mathbb{F}_q$. Assuming that the modular polynomial (modulo the characteristic of

$\mathbb{F}_q$) is given as input and using asymptotically fast probabilistic algorithms to factor $f(X)$, the cost of a step in terms of arithmetic operations in $\mathbb{F}_q$ is $O(\ell^2 + M(\ell)\log q)$, where $M(\ell)$ denotes the operation count of multiplying polynomials of degree ℓ. In this formula, the first term corresponds to evaluation of $\Phi_\ell(X, j(E_{i-1}))$ and the second term to root finding[6].

With Vélu's formulae, we need to take into account the fact that the required ℓ-torsion points are not necessarily defined over $\mathbb{F}_q$. Let r denote the smallest integer such that the required points are all defined over $\mathbb{F}_{q^r}$. We know that $1 \leq r \leq \ell - 1$. Using asymptotically efficient algorithms to perform arithmetic operations in $\mathbb{F}_{q^r}$, multiplications in $\mathbb{F}_{q^r}$ cost $M(r)$ $\mathbb{F}_q$-operations. Given an ℓ-torsion point P in $E(\mathbb{F}_{q^r})$, the cost of using Vélu's formulae is $O(\ell)$ operations in $\mathbb{F}_{q^r}$. As a consequence, in terms of $\mathbb{F}_q$ operations, each isogeny costs $O(\ell M(r))$ operations. As a consequence, when q is not too large and r is close to ℓ, using Vélu formulae is more expensive by a logarithmic factor.

Computing an ascending or horizontal path. With the classical algorithms, each step in an ascending or horizontal path requires considering all the $O(\ell)$ neighbours of the curve and testing each of them by walking descending paths of height bounded by h. The expected cost of each descending path is $O(h(\ell^2 + M(\ell)\log q))$ and the total cost is $O(h(\ell^3 + \ell M(\ell)\log q))$ (see [14, 24]). When $\ell >> \log q$, this cost is dominated by the evaluations of the polynomial Φ_ℓ at each j-invariant. Thus, by walking in parallel $\ell+1$ paths from the original curve, we can amortize the evaluation of $\Phi_\ell(X, j)$ over many j-invariants using fast multipoint evaluation (see [19, Section 3.7] or [26]), thus replacing ℓ^3 by $\ell\, M(\ell)\log\ell$ and reducing the complexity of a step to $O(h\ell\, M(\ell)(\log\ell + \log q))$. However, this increases the memory requirements.

With our modified algorithms, we need to find the ℓ^∞-structure of each curve, compute some discrete logarithms in ℓ-groups, perform a small number of pairing computations and compute the roots of $\mathcal{P}_{E,\ell^{n_2}}$. Except for the computation of discrete logarithms, it is clear that all these additional operations are polynomial in n_2 and $\log\ell$ and they take negligible time in practice (see Section 5.2). Using generic algorithms, the discrete logarithms cost $O(\sqrt{\ell})$ operations, and this can be reduced to $\log\ell$ by storing a sorted table of precomputed logarithms. After this is done, we have to compute at most two isogenies, ignoring the one that backtracks. Thus, the computation of one ascending or horizontal step is dominated by the computation of isogenies and costs $O(\ell M(r))$.

For completeness, we also mention the complexity analysis of Algorithm 1. The dominating step here is the multiplication by N of randomly chosen points. When we consider the curve over an extension field $\mathbb{F}_{q^r}$, the expected cost is $O(r\log q)$ operations in $\mathbb{F}_{q^r}$, i.e., $O(rM(r)\log q)$ operations in $\mathbb{F}_q$.

Finally, comparing the two approaches on a regular volcano, we see that even in the less favorable case, we gain a factor h compared to the classical algorithms. More precisely, the two are comparable, when the height h is small and r is close to ℓ. In all the other cases, our modified algorithms are more efficient. This analysis is summarized in Table 1. For compactness $O(\cdot)$s are omitted from the table.

[6]Completely splitting $f(X)$ to find all its roots would cost $O(M(\ell)\log\ell\log q)$, but this is reduced to $O(M(\ell)\log q)$ because we only need a constant number of roots for each polynomial $f(X)$.

TABLE 1. Walking the volcano: Order of the expected cost per step

	Descending path		Ascending/Horizontal
	One step	Many steps	
[14, 8]	$h(\ell^2 + M(\ell)\log q)$	$(\ell^2 + M(\ell)\log q)$	$h(\ell^3 + \ell\, M(\ell)\log q)$
Parallel evaluation	–	–	$h\ell\, M(\ell)(\log \ell + \log q)$
Regular volcanoes	Structure determination		
Best case	$\log q$		$\log q$
Worst case $r \approx \ell/2$	$r\, M(r)\log q$		$r\, M(r)\log q$
Regular volcanoes	Isogeny construction		
Best case	ℓ		ℓ
Worst case $r \approx \ell/2$	$r\, M(r)$		$r\, M(r)$
Irregular volcanoes (worst case)	No improvement		

Computing endomorphism rings. On a regular volcano, computing the invariant $\mathcal{L}_{\ell,E}$ involves computing the group structure and some pairings. Hence, the expected running time of the computation is $O(rM(r)\log q + n_2 \log \ell)$, while the complexity of Kohel's algorithm is $O(h(\ell^2 + M(\ell)\log q))$.

Irregular volcanoes. Consider a fixed value of q and let $s = v_\ell(q-1)$. First of all, note that all curves lying on irregular volcanoes satisfy $\ell^{2s} | q+1-t$ and $\ell^{2s+2} | t^2 - 4q$. For traces that satisfy only the first condition, we obtain a regular volcano. We estimate the total number of different traces of elliptic curves lying on ℓ-volcanoes by $\#\{t \text{ s.t. } \ell^{2s} | q+1-t \text{ and } t \in [-2\sqrt{q}, 2\sqrt{q}]\} \sim \frac{4\sqrt{q}}{\ell^{2s}}$.

Next, we estimate traces of curves lying on irregular volcanoes by

$$\#\{t \text{ s.t. } \ell^{2s} | q+1-t \ , \ell^{2s+2} | t^2 - 4q \text{ and } t \in [-2\sqrt{q}, 2\sqrt{q}]\} \sim \frac{4\sqrt{q}}{\ell^{2s+2}}.$$

Indeed, by writing $q = 1 + \gamma\ell^s$ and $t = 2 + \gamma\ell^s + \mu\ell^{2s}$, and imposing the condition $\ell^{2s+2} | t^2 - 4q$, we find that $t \cong t_0(\gamma, \mu) (\mathrm{mod}\ \ell^{2s+2})$.

Thus, we estimate the probability of picking a curve whose volcano is not regular, among curves lying on volcanoes of height greater than 0, by $\frac{1}{\ell^2}$. (This is a crude estimate because the number of curves for each trace is proportional to the Hurwitz class number[7] $H(t^2 - 4q)$.) This probability is not negligible for small values of ℓ. However, since our method also works everywhere on almost regular volcano, the probability of finding a volcano where we need to combine our modified algorithm with the classical algorithms is even lower. Furthermore, in some applications, it is possible to restrict ourselves to regular volcanoes.

5.2. **Some practical examples.**

A favorable case. In order to demonstrate the potential of the modified algorithm, we consider the favorable case of a volcano of height 2, where all the necessary ℓ-torsion points are defined over the base field $\mathbb{F}_p$, where

$$p = 619074283342666852501391$$

is prime. We choose $\ell = 100003$.

[7] See [5, Th. 14.18] for q prime.

Let E be the elliptic curve whose Weierstrass equation is

$$y^2 = x^3 + 198950713578094615678321\,x + 32044133215969807107747.$$

The group $E[\ell^\infty]$ over $\mathbb{F}_p$ has structure $\frac{\mathbb{Z}}{\ell^4\mathbb{Z}}$. It is spanned by the point

$$P = (1106467197343152147985 87, 5215053399922246279321 73).$$

Taking the ℓ-isogeny I_1 with kernel $\langle \ell^3 P\rangle$, we obtain the curve

$$E_1 : y^2 = x^3 + 476298723694969288644436\,x + 260540808216901292162091,$$

with structure of the ℓ^∞-torsion $\frac{\mathbb{Z}}{\ell^3\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell\mathbb{Z}}$ and generators

$$P_1 = (22630045752997075604069, 20769418778970580093 0332) \text{ and}$$
$$Q_1 = (30478274535808072705812 9, 19390482983716803279 1973).$$

The ℓ-isogeny I_2 with kernel $\langle \ell^2 P_1\rangle$ leads to the curve

$$E_2 : y^2 = x^3 + 212075995763000386527 90\,x + 471086215466928725193841,$$

on the volcano's crater and with structure $\frac{\mathbb{Z}}{\ell^2\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^2\mathbb{Z}}$ and generators

$$P_2 = (54533300276080306757675 5, 36754828044827678313 3614) \text{ and}$$
$$Q_2 = (40151536837100485640095 1, 22542004406628002549 5795).$$

Using pairings on these points, we construct the polynomial,

$$\mathcal{P}(x, y) = 97540\,x^2 + 68114\,x\,y + 38120\,y^2,$$

having homogeneous roots $(x, y) = (26568, 1)$ and $(72407, 1)$. As a consequence, we have two horizontal isogenies with kernels $\langle \ell(26568\,P_2+Q_2)\rangle$ and $\langle \ell(72407\,P_2+Q_2)\rangle$. We can continue and make a complete walk around the crater which contains 22 different curves. Using a simple implementation under Magma 2.15-15, a typical execution takes about 134 seconds[8] on a single core of an Intel Core 2 Duo at 2.66 GHz. Most of the time is taken by the computation of Vélu's formulas (132 seconds) and the computation of discrete logarithms (1.5 seconds) which are not tabulated in the implementation. The computation of pairings only takes 20 milliseconds.

A larger example. We have also implemented the computation for $\ell = 1009$ using an elliptic curve with j-invariant $j = 34098711889917$ in the prime field defined by $p = 953202937996763$. The ℓ-torsion appears in a extension field of degree 84. The ℓ-volcano has height two and the crater contains 19 curves. Our implementation walks the crater in 20 minutes. More precisely, 750 seconds are needed to generate the curves' structures, 450 to compute Vélu's formulas, 28 seconds for the pairings and 2 seconds for the discrete logarithms.

Computing the endomorphism ring. Our benchmarks show that our method is very efficient in the favorable case, i.e., when the ℓ-torsion points are defined over the base field. Otherwise, if ℓ is small, the efficiency of our method depends asymptotically on the ratio h/r. We have implemented our algorithm and Kohel's method with MAGMA and ran experiments for various values of h, r and ℓ. Results are given in Table 2. For large ℓ ($\ell \geq 2^{10}$), we could not test Kohel's method since modular polynomials may not be precomputed with MAGMA.

[8]This timing varies between executions. The reason that we first try one root of $\mathcal{P}$, if it backtracks on the crater, we need to try the other one. On average, 1.5 root is tried for each step, but this varies depending on the random choices.

TABLE 2. 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
$D = 4 * 919$, $\ell = 1009$, $h = 2$, $r = 84$	-	43 s

An example. For curves such that the index of $\mathbb{Z}[\pi]$ is divisible by a large power of a small prime ℓ, we use Kohel's algorithm combined with our method to compute the largest power of ℓ dividing the conductor of the endomorphism ring. Suppose we are given the curve with j-invariant

$$j_0 = 718924956294504807965250555741205779292913599 32$$

over the prime field defined by

$$p = 555574087029024034910907703752286309950415657009.$$

The discriminant of $\mathbb{Z}[\pi]$ is

$$d_\pi = 2^2 \cdot 31^{30} \cdot 1009,$$

hence the height of the 31-volcano is 15. The 31-Sylow group structure is $\frac{\mathbb{Z}}{31^3\mathbb{Z}} \times \frac{\mathbb{Z}}{31^3\mathbb{Z}}$ and the corresponding $k(E) = -1$, hence we may not determine the level of the curve in the 31-volcano by using pairings over $\mathbb{F}_p$. We could move to $\mathbb{F}_{p^\ell}$ and compute pairings over this field, but it is rather expensive. Instead, we use Kohel's algorithm to find the shortest path to the second stability level. For each curve we consider, we compute the corresponding pairings over $\mathbb{F}_p$ to see whether we get a polynomial $\mathcal{P}$ different from zero. When we get such a polynomial, we stop because we have reached the second stability level. For example, a random walk in the volcano produces a shortest path to the second stability level given by the curves with j-invariants

$$j_1 = 304777814376748778212312171834280090074154445427 \text{ and } k(E_1) = -1,$$
$$j_2 = 191449283692968031770360270038328919070842850348 \text{ and } k(E_2) = -1,$$
$$j_3 = 500824144736236330809586376475032618300606767898 \text{ and } k(E_3) = -1,$$
$$j_4 = 439660047668527271074847223836176503148636315832 \text{ and } k(E_4) = 0.$$

The curve E_4 lies on the second stability level, hence we deduce that the 31-valuation of the index of $\mathbb{Z}[\pi]$ in $\mathrm{End}(E)$ is 9.

6. Conclusion and perspectives

In this paper, we have proposed a method which allows one to determine, given a curve E in the regular part of an isogeny volcano and an ℓ-torsion point P on the curve, the type of the ℓ-isogeny whose kernel is spanned by P. In addition, this method permits one to find the ascending isogeny (or horizontal isogenies) from E, if a basis for the ℓ-torsion is given. We expect that this method can be used to improve the performance of several volcano-based algorithms, such as the computation of the Hilbert class polynomial [24] or of modular polynomials [3].

Finally, on an ℓ-volcano, we have given a level invariant which can be determined by computing the structure of the ℓ-Sylow group and a small number of pairings.

This gives a new method to compute the ℓ-adic valuation of the conductor of the endomorphism ring of an elliptic curve, for small values of ℓ, and may thus be used in algorithms computing the endomorphism ring of an elliptic curve.

Acknowledgments

The authors thank Jean-Marc Couveignes for the idea in the proof of Lemma 1 and anonymous reviewers of the conference version [11] for helpful comments. The first author is grateful to Ariane Mézard for many discussions on number theory and isogeny volcanoes, prior to this work. This work was partially supported by the French Agence Nationale de la Recherche through the ECLIPSES project under Contract ANR-09-VERS-018 and by the Direction Générale de l'Armement through the AMIGA project under Contract 2010.60.055.

References

[1] J. Belding, R. Broker, A. Enge, and K. Lauter. Computing Hilbert Class Polynomials. In A.J. van der Poorten and A. Stein, editors, *Algorithmic Number Theory Symposium-ANTS VIII*, volume 5011 of *Lecture Notes in Computer Science*, pages 282–295. Springer-Verlag, 2008. MR2467854 (2009j:11200)

[2] G. Bisson and A. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *Journal of Number Theory*, 213(5):815–831. MR2772473

[3] R. Broker, K. Lauter, and A. Sutherland. Computing modular polynomials with the chinese remainder theorem. http://arxiv.org/abs/1001.0402, 2009.

[4] D. Charles. On the existence of distortion maps on ordinary curves. `http://eprint.iacr.org/2006/128`.

[5] D. A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. John Wiley & Sons, Inc, 1989. MR1028322 (90m:11016)

[6] M. Deuring. *Die Typen der Multiplikatorenringe elliptischer Funktionenkorper*. Abh. Math. Sem. Hansischen Univ. 14, 1941. MR0005125 (3:104f)

[7] M. Fouquet. *Anneau d'endomorphismes et cardinalité des courbes elliptiques: aspects algorithmiques*. PhD thesis, Ecole Polytechnique, 2001.

[8] M. Fouquet and F. Morain. Isogeny Volcanoes and the SEA Algorithm. In *ANTS-V*, volume 2369 of *Lecture Notes in Computer Science*, pages 276–291. Springer, 2002. MR2041091 (2005c:11077)

[9] G. Frey. Applications of arithmetical geometry to cryptographic constructions. In *Proceedings of the Fifth International Conference on Finite Fields and Applications*, pages 128–161. Springer, 2001. MR1849086 (2002h:11136)

[10] P. Grabher, J. Großschädl, and D. Page. On software parallel implementation of cryptographic pairings. In *Selected Areas in Cryptography 2008*, volume 5381 of *Lecture Notes in Computer Science*, pages 35–50. Springer, 2009.

[11] S. Ionica and A. Joux. Pairing the volcano. In *Algorithmic Number Theory Symposium*, volume 6197 of *Lecture Notes in Computer Science*, pages 201–218. Springer, 2010. MR2721422

[12] A. Joux and K. Nguyen. Separating decision Diffie–Hellman from computational Diffie–Hellman in cryptographic groups. *Journal of Cryptology*, 16(4):239–247, 2003. MR2002044 (2004h:94045)

[13] H.W. Lenstra Jr. Complex multiplication structure of elliptic curves. *Journal of Number Theory*, 56(2):227–241, 1996. MR1373549 (97a:11096)

[14] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California, Berkeley, 1996. MR2695524

[15] K. Lauter and D. Freeman. Computing endomorphism rings of jacobians of genus 2 curves over finite fields. *Symposium on Algebraic Geometry and its Applications*, pages 29–66, 2008. MR2484047 (2010a:14042)

[16] V. S. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, 17(4):235–261, September 2004. MR2090556 (2005g:11112)

[17] J. Miret, R. Moreno, D. Sadornil, J. Tena, and M. Valls. An algorithm to compute volcanoes of 2-isogenies of elliptic curves over finite fields. *Applied Mathematics and Computation*, 176(2):739–750, 2006. MR2232066

[18] J. Miret, R. Moreno, D. Sadornil, J. Tena, and M. Valls. Computing the height of volcanoes of l-isogenies of elliptic curves over finite fields. *Applied Mathematics and Computation*, 196(1):67–76, 2008. MR2382590 (2008m:11122)

[19] P.L. Montgomery. *A FFT extension of the elliptic curve method of factorization*. PhD thesis, University of California, 1992. MR2688742

[20] H.-G. Ruck. A note on elliptic curves over finite fields. *Mathematics of Computation*, 179:301–304, 1987. MR890272 (88d:11058)

[21] R. Schoof. Counting points on elliptic curves over finite fields. *Journal de Theorie des Nombres de Bordeaux*, 7:219–254, 1995. MR1413578 (97i:11070)

[22] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 1986. MR817210 (87g:11070)

[23] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, 1994. MR1312368 (96b:11074)

[24] A. Sutherland. Computing Hilbert Class Polynomials with the Chinese Remainder Theorem. *Mathematics of Computation*, 2010. MR2728992 (2011k:11177)

[25] J. Vélu. Isogenies entre courbes elliptiques. *Comptes Rendus De L'Academie Des Sciences Paris, Serie I-Mathematique, Serie A.*, 273:238–241, 1971. MR0294345 (45:3414)

[26] J. von zur Gathen and V. Shoup. Computing Frobenius maps and factoring polynomials. *Computational Complexity*, 2:187–224, 1992. MR1220071 (94d:12011)

Laboratoire d'Informatique de l'Ecole Polytechnique (LIX) 91128 Palaiseau CEDEX, France

Current address: LORIA (UMR 7503), Equipe-projet CARAMEL, Bâtiment A, Campus Scientifique – BP 239, 54506 Vandœuvre-lès-Nancy Cedex, France

E-mail address: sorina.ionica@gmail.com

DGA and Université de Versailles Saint-Quentin-en-Yvelines, 45 avenue des États-Unis, 78035 Versailles CEDEX, France

E-mail address: antoine.joux@m4x.org