Isogenies between ordinary elliptic curves with large conductor gap

Parsa Tasbihgou

Abstract. Robert showed that the endomorphism ring of an ordinary elliptic curve can be computed in polynomial time when the factorization of its conductor is known. Despite that, finding isogenies between ordinary curves remains hard, as not all isogenies correspond to invertible ideals of the endomorphism ring (in contrast to the supersingular case).
When two ordinary curves have smooth conductor gap it is easy[1] to find isogenies between them but when the conductor gap has large prime factors the problem is more involved. Galbreith [**?**] studied this problem (and a couple of related problems) and he gave algorithms that in the worst case find an isogeny in $O(q^{2/5})$ where q is the field size.
In this note we give a brief overview of the algorithms proposed by Galbreith, talk about some failed attempts to find better algorithms and apply quantum algorithms to Galbreith's ideas to get an algorithm that in worst case runs in $O(q^{2/9})$.

1 Ordinary elliptic curves

An abelian variety $A/\mathbb{F}_q$ where $q = p^r$ is supersingular if it is isogenous to a product of supersingular elliptic curves, it is superspecial if it is isomorphic to a product of elliptic curves. In dimension g it is called ordinary if $A[n] \simeq (\mathbb{Z}/n\mathbb{Z})^g$.
For elliptic curves (dimension 1 A.V.) there is equivalent condition for being ordinary: $E/\mathbb{F}_q$ is ordinary when $|E(\mathbb{F}_q)| \not\equiv 1 \mod p$ equiv. $t \not\equiv 0 \mod p$.

The endomorphism ring of ordinary curve E is isomorphic to an order $\mathcal{O}$ in $K = Q(\sqrt{t^2 - 4q})$. $\pi : E \to E; (x, y) \to (x^q, y^q)$ is an endomorphism of all elliptic curves therefore $\mathbb{Z}[\pi] \subseteq \mathcal{O}$. So we have $\mathbb{Z}[\sqrt{t^2 - 4q}] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$.
Robert gave a poly-time algorithm to compute $\mathrm{End}(E)$ when the factorization of its conductor is given, so in general we have a subexponential algorithm. This is in contrast to the supersingular case where the endomorphism ring problem is assumed to have exponential complexity for both classical and quantum computers.
Even though the endomorphism ring problem is relatively easier for ordinary curves, the isogeny problem is still difficult. In the supersingular case these two problems are more or less equivalent: If the endomorphism ring is known we can find outgoing isogenies of arbitrary degree and if the endomorphism ring of two curves are known we can find isogenies between them. This is because all supersingular isogenies correspond to ideals classes of quaternion orders and each ideal class has representatives of smooth norm. Once the endomorphism rings are known we can find connecting ideals and then find representatives of the connecting ideal of smooth norm.
On the other hand, if we can find isogenies between curves then we can find non-scalar endomorphisms and we know from [**?**] that finding one endomorphism (for any given curve) is enough to find the full endomorphism ring.

E-mail: parsa.tasbihgou@epfl.ch (Parsa Tasbihgou)
[1]The problem reduces to the class group action inversion problem in the fundamental class group

Not all isogenies between ordinary curves correspond to ideals, in particular horizontal isogenies correspond to invertible isogenies (eqv. the class group of the endomorphism ring) ascending isogenies correspond to non-invertible ideals and descending isogenies don't correspond to any ideals. We can hope to find horizontal isogenies when the class group of the endomorphism ring is known (similar to SCI-FiSh) and Clapotis [**?**] evaluates invertible ideal isogenies in poly-time.
The non-invertible ideal that generates the ascending isogeny is unique and known however we don't know any efficient method to compute its isogeny, the best method we know at the moment is to explicitly compute its kernel and apply Velu formulae.
The descending isogenies are more challenging since they don't correspond to any ideals. However, for any $\ell | \frac{t^2-4q}{f_E}$ there are approximately ℓ descending isogenies from E.

2 Computing isogenies between ordinary elliptic curves

Galbraith [**?**] studied the problem of finding isogenies between ordinary elliptic curves. When isogenies of smooth degree are considered, we know poly-time algorithms. However, when isogenies of large prime degree are considered we generally don't know poly-time algorithms. The following four problems are discussed by Galbraith and problem (5) is also separately discussed by Galbraith and Stolbunov [**?**] [2]:
E_0, E_1 are ordinary elliptic curves defined over $\mathbb{F}_q$ of characteristic $p > 0$. t is their trace of Frobenius, f is the conductor of $\mathbb{Z}[\sqrt{t^2-4q}]$ so $t^2 - 4q = f^2 D_K$, $N|f$ is a large prime, $\mathbb{Z}[\sqrt{t^2-4q}] \subseteq \mathcal{O}_1 = \mathrm{End}(E_1) \subseteq \mathcal{O}_0 \simeq \mathrm{End}(E_0) \subseteq \mathcal{O}_K$, $K = \mathbb{Q}(\sqrt{t^2-4q})$ is isomorphic to their endomorphism algebra, $\mathcal{O}_K$ is the maximal order in K (the integer ring), $f_0 = [\mathcal{O}_K : \mathcal{O}_0], f_1 = [\mathcal{O}_K : \mathcal{O}_1]$ are the conductors of E_0 and E_1 respectively.
D_K is the discriminant of the maximal order and h_K is the class number of K (eqv. $h(\mathcal{O}_K)$).

1. E_0 is on the crater. Find any descending N-isogeny $\phi : E_0 \to E_1$. Notice that E_1 is not known.

2. E_0 and E_1 are connected by a descending N-isogeny $\phi : E_0 \to E_1$ and E_0 is directly above E_1. In this situation the conductor gap $[\mathcal{O}_0 : \mathcal{O}_1] = N$.

3. E_0 is two levels above E_1, meaning that there is a descending N^2-isogeny $\phi : E_0 \to E_1$. In this situation the conductor gap $[\mathcal{O}_0 : \mathcal{O}_1] = N^2$.

4. E_0 is a curve on the crater ($\mathcal{O}_0 = \mathcal{O}_K$) and E_1 is one level down, find an isogeny $\phi : E_0 \to E_1$. In this case $[\mathcal{O}_0 : \mathcal{O}_1] = N$ so $N|\deg(\phi)$ but if E_0 isn't directly above E_1 then $N \neq \deg(\phi)$.
   Notice that this case is different from (1) since E_0 isn't necessarily directly above E_1.

5. E_0 and E_1 are in the same level ($\mathcal{O}_0 = \mathcal{O}_1$). Find a horizontal isogeny $\phi : E_0 \to E_1$.

Since we are working with isogenies of large prime degree, we don't now a "standard" efficient representation for them, so we implicitly assume all such isogenies are in their high-dimensional representation.

2.1 Problem 5

A meet-in-the-middle algorithm by Galbraith solves problem (5) in $O(q^{1/4})$. Furthermore a quantum computer can solve this problem in subexponential time using Kuperburg's algorithm [**?**, JaoSukharevChilds]

[2] We have slightly changed the problem descriptions to reflect the main case of interest in each one

2.2 Problems 2 and 3

Descending isogenies don't correspond to any ideals so to compute $\phi : E_0 \to E_1$ directly, the only known method is to try random isogenies until we find ϕ. There are approximately N such isogenies and computing an isogeny from its kernel generator using Velu formulae takes time $O(N^{1/2})$ field operations and the generator of the kernel of ϕ might be defined over an extension of size $O(N)$. So this method is not efficient.
When $N|f_1$ there is unique ascending N-isogeny from E_1 which is the dual of $\phi : E_0 \to E_1$, generated by the non-invertible ideal $\mathfrak{a} = (\mathcal{F}_1, N)$, where $\mathcal{F}_1 = \mathbb{Z} + f_1\mathcal{O}_K$ is the conductor ideal.
Since $\mathfrak{a}$ is non-invertible it doesn't have a representative in the class group $\mathrm{cl}(\mathcal{O}_1)$ and efficient ideal-to-isogeny algorithms [**?**] don't apply to it. The best known algorithm to find the ascending isogeny is to compute the kernel of $\mathfrak{a}$ and apply Velu formulae. It takes time $O(N^2 \log(q))$.
Galbraith gave an algorithm to solve problem (2) and (3) in time $O(N^{1/2}) = O(q^{1/4})$.
We start from a simpler algorithm that runs in $O(N)$ and then see how it can be improved.
Let $\phi : E_0 \to E_1$ be the descending N-isogeny is question. Let $M = N + m$ be smooth and $m = m_1^2 + m_2^2$ [3]. Using Kani's reduction lemma we can embed ϕ in a dimension 4 isogeny of abelian varieties $\mathcal{F} : E_0^2 \times E_1^2 \to E_1^2 \times E_0^2$ of degree M.
Let $\gamma = \begin{pmatrix} m_1 & -m_2 \\ m_2 & m_1 \end{pmatrix}$ be an isogeny $E_0^2 \to E_0^2$ and $\overline{\gamma} = \begin{pmatrix} m_1 & m_2 \\ -m_2 & m_1 \end{pmatrix}$ and let γ' be the isogeny acting on E_1^2 by the same matrix. Then $\mathcal{F}$ acts on $E_0^2 \times E_1^2$ by the matrix $\begin{pmatrix} \phi & -\hat{\gamma'} \\ \gamma & \hat{\phi'} \end{pmatrix}$. To compute the kernel of $\mathcal{F}$ it is enough to to know $\phi(P), \phi(Q)$ such that $E_0[M] = \langle P, Q \rangle$. The main challenge is finding this information.
Let P and Q be an eigenbasis of the q-Frobenius. Since ϕ is defined over $\mathbb{F}_q$, $\phi(P)$ and $\phi(Q)$ are also eigenvectors. Let P' and Q' be eigenbasis of $E_1[M]$ such that $\phi(P) \in \langle P \rangle$ and $\phi(Q) \in \langle Q \rangle$, then there is $a, b \in \mathbb{Z}/M\mathbb{Z}$ such that $\phi(P) = aP', \phi(Q) = bQ'$.
Weil pairing is isogeny-compatible therefore $e_M(P,Q)^N = e_M(\phi(P), \phi(q)) = e_M(aP', bQ') = e_M(P', Q')^{ab}$. Let $\alpha = e_M(P,Q)^N, \beta = e_M(P', Q') \in \mu_M$ and $x = \log_\beta^\alpha$ then $ab = x$ therefore $a = b^{-1}x$, so we only need to guess a single value in $\mathbb{Z}/M\mathbb{Z}$. We recall that $M \simeq N$. We use a meet-in-the-middle trick to reduce the domain of the unknown parameter to $O(N^{1/2})$.
An Elkies prime ℓ is a prime integer that splits in $\mathbb{Q}(\sqrt{t^2 - 4q})$ (eqv. $\left(\frac{D_K}{\ell}\right) = 1$). The characteristic polynomial of Frobenius $\pi^2 - t\pi + q$ factors into linear terms $(\pi - \lambda)(\pi - \lambda')$ mod ℓ. So λ and λ' are eigenvalues of π on $E_[\ell]$ with eigenbasis $(P_{0,\ell}, Q_{0,\ell})$.
Let $A = \prod \ell_i$ be a product of small Elkies primes so that $A^2 \leq N/2$ and n the smallest integer that $M = 3^n A^2 > N$. We let $m = M - N$. $M < 3N$ therefore $m < 2N$. As before for simplicity we assume m is the sum of two squares. We can build the 4-dimensional M-isogeny $\mathcal{F} : E_0^2 \times E_1^2 \to E_1^2 \to E_0^2$ as before.
Let's write $M = 3^n A^2 = (3^{\lceil n/2 \rceil} A)(3^{\lfloor n/2 \rfloor} A) = M_1 M_2$. Notice that $M_1 \leq 3\sqrt{N}$. We can decompose $\mathcal{F} = \mathcal{F}_2 \circ \mathcal{F}_1$ where $\mathcal{F}_i$ has degree M_i. Then $\mathcal{F}_1$ and $\overline{\mathcal{F}_2}$ have the same abelian variety V as their codomain.

$$E_0^2 \times E_1^2 \xrightarrow{\mathcal{F}_1} V \xleftarrow{\overline{\mathcal{F}_2}} E_1^2 \times E_0^2$$

To compute $\ker(\mathcal{F}_1)$ and $\ker(\overline{\mathcal{F}_2})$ it suffices to know $\hat{\phi}(P_1)$ and $\hat{\phi}(Q_1)$ for some basis of $E_1[M_1]$. For each prime $\ell|A$ let $(P_{1,\ell}, Q_{1,\ell})$ be an eigenbasis of $E_1[\ell]$ and $(P_{0,\ell}, Q_{0,\ell})$ be an eigenbasis of $E_0[\ell]$ then for some $a, b \in \mathbb{Z}/\ell\mathbb{Z}$ we have $e_\ell(P_{1,\ell}, Q_{1,\ell})^N = e_\ell(P_{0,\ell}, Q_{0,\ell})^{ab}$. Now same as before we can find $\hat{\phi}(P_{1,\ell})$ and $\hat{\phi}(Q_{0,\ell})$ by guessing a single unknown value in

[3] In general probability of m being the sum of two squares is $\frac{1}{\sqrt{\log(N)}}$, and it is always the sum of four squares.

$\mathbb{Z}/\ell\mathbb{Z}$. If the correct value is chosen for each prime the codomain of $\mathcal{F}_1$ and $\overline{\mathcal{F}_2}$ will agree. Then $\mathcal{F} = \mathcal{F}_2 \circ \mathcal{F}_1$.

2.3 Problem 4

To solve (4) there are two approaches:

1. Going up; Compute the ascending isogeny $\phi_{\mathfrak{a}} : E_1 \to E_0'$ such that $\mathrm{End}(E_0') = \mathcal{O}_0$, then find a horizontal isogeny $\phi_h : E_0' \to E_0$ using the algorithm from (5). Then $\phi = \hat{\phi_a} \circ \hat{\phi_h} : E_0 \to E_1$ is the required descending isogeny.
   Finding $\phi_{\mathfrak{a}}$ has complexity $O(N^2 \log(q))$ and ϕ_h complexity, $O(h_K^{1/2})$, together $\tilde{O}(h_K^{1/2} + N^2)$.

2. Going down; Let E_0' be the curve on the crater directly above E_1. If $\phi_h : E_0 \to E_0'$ is known, $\phi_d : E_0' \to E_1$ can be computed in $O(N^{1/2})$. Unfortunately we don't know any method to find E_0' other than the naive method: Start from E_0 and walk on the crater (class group). At each curve, run the algorithm for (2) if an isogeny is found stop, else continue.
   This search can go through the whole class group before finding E_0' so its complexity is $O(h_K N^{1/2})$.

Depending on the parameters going up/down is the most efficient approach. When $N < q^{1/5}$ we go up and when $q^{1/5} < N < q^{1/2}$ go down. Overall this gives complexity $O(q^{2/5})$ in the worst case.

2.4 New approaches

Together with Fre and Wouter we discussed some other approaches to solve problem 4, some of which might be also useful for problem 1.

1. **Isogenies from sum of the x-coordinated**
   In [**?**, Book, Blake-Seroussi-Smart]here is an algorithm that computes an isogeny when the sum of the x-coordinates of the kernel is given. While the kernel points of an N-isogeny might all live in an extension of degree $N-1$ since the isogeny is defined over $\mathbb{F}_q$, the sum of the x-coordinates is in $\mathbb{F}_q$.
   Said algorithm computed the kernel polynomial iteratively in n

2. **Computing $\phi : E_1 \to E_0$ directly**
   One can try to directly compute the isogeny $\phi : E_1 \to E_0$ by applying Galbraith's meet-in-the-middle algorithm (problem 2). ϕ is the composition of two isogenies: 1) $\phi_h : E_0' \to E_0$, a horizontal isogeny on the crater with unknown degree. 2) $\phi_v : E_1 \to E_0'$, a vertical isogeny of degree N. The problem here is that Galbraith's algorithm requires the degree of ϕ be known [4], we know the degree of ϕ_v but degree of ϕ_h is unknown. We can resolve this issue by selecting some integer D such that we know there is an isogeny $E_0' \to E_0$ of degree D. Now we know the degree of ϕ is ND and we can apply Galbraith's algorithm to find ϕ in $O(\sqrt{ND})$.
   Wouter came up with this idea: E_0 and E_0' are on the crater and their isogenies correspond to an ideal class in $\mathrm{cl}(\mathcal{O})$. The ideal class is generated by a basis of $m = \log_2(h)$ prime ideals of norm ℓ_i with exponents in $\{-1, +1\}$. Notice that in this representation each ideal class has norm $D = \prod_{i \le m} \ell_i$. So for any E_0' there is a horizontal D-isogeny $E_0' \to E_0$. The problem with this idea is that D is too large therefore $O(\sqrt{ND})$ is too large.

[4] also it shouldn't have small prime factors, but this requirement can be dealt with

Primorial of m denoted $p_m\#$ is the the product of the first m primes (similar to factorial) and $p_m\# = e^{(1+o(1))m\log(m)}$. Obviously for any choice of basis for the class group, $D = \prod \ell_i \geq p_m\# \simeq e^{m\log(m)}$, replacing $m = \log_2(h)$ we have $D \simeq h^{\log\log(h)}$ which is too large. For this approach to be better than the current method we must have $D \leq o(h^2)$.

3. **Two-way random sampling**
The main challenge in problem 4 is to find E_0'. In the the going up method we pay the $O(N^2)$ price to exactly compute E_0'. In the going down method we sample random curves until we pick E_0'.
Looking at the previous approach (direct computation) we observe that picking degree of the horizontal isogeny gives a method to pick random curves on the crater. Notice that picking a degree d doesn't specify a single curve but a subset of curves that have a d-isogeny to E_0'. On the other hand, ideal classes also specify random curves on the crater. When we pick a class $[a]$ it uniquely specifies E/a. Contrary to the degree method, we can compute E/a in poly-time.
Even though we can't explicitly compute the curves that are specified by the degree method, if ideal class a and degree d point to the same curve we can detect this collision in $O(\sqrt{Nd}) + poly$ by computing E/a and applying the MiM algorithm.
We were hoping that by random sampling something similar to the birthday paradox can help us find a collision by taking less that h samples. Let's say we sample m random ideal classes and n random degrees and we want the probability of collision be at least $1-\epsilon$ then we must have $nm = \frac{\ln\epsilon}{\ln(1-1/h)} \simeq h$. This means if we take $n \simeq m$ then we only need to take $O(\sqrt{h})$ random ideal classes and about the same number of random degrees. The issue is that checking for a collision takes $O(mn) = O(h)$. Can we check for collisions more efficiently?

4. **Ordinary non-simple abelian surfaces**
Another interesting approach is looking for ascending isogenies in higher dimension. This approach is motivated by the structure of the isogeny graph of ordinary simple abelian surfaces [**?**, jetchev]
Assume E_0 is on the crater and E_1 one level down and not directly under E_0 with conductor gap N a large prime. The barrier for finding an isogeny $\phi : E_0 \to E_1$ is that the lattice of orders in an imaginary quadratic field is linear, meaning that the degree of any isogeny between two curves with endomorphism rings $\mathcal{O}_1 \subset \mathcal{O}_0$ has to divide $[\mathcal{O}_0 : \mathcal{O}_1]$ in particular any isogeny connecting E_1 and E_0 factors through some isogeny of degree N.
On the other hand, the lattice of orders in CM fields is not linear and the same rule about inclusion and divisibility doesn't apply. (However when restricted to orders with maximal real suborder (eqv. curves with maximal real-multiplication) the lattice is again linear).
The idea of using abelian surfaces is that instead of finding isogenies between E_0 and E_1 we can try to find isogenies from $E_0 \times E_0 \to E_1 \times E_1$ or endomorphisms of $E_0 \times E_1$
We couldn't find information regarding the isogeny graph or the endomorphism algebra of the ordinary non-simple abelian varieties, so unfortunately we couldn't follow this idea further.
Another flaw in this idea is as ponted out by Wouter is that endomorphism of $E_0 \times E_1$ are of the form $\begin{pmatrix} \alpha & \phi \\ \psi & \beta \end{pmatrix}$ where α and β are endomorphisms of E_0 and E_1 resp. and ϕ and ψ are isogenies between them. So understanding the endomorphsims ring must somehow require understanding the isogenies between E_0 and E_1. So it is unlikely that a non-trivial endomorphism can be found without knowing isogenies.

2.5 Problem 1

Prior to Galbraith, best known algorithms either used modular polynomials to find the kernel of such isogeny or class polynomials to compute E_1, resulting in $O(q)$ at best.
Galbraith suggests guessing E_1 to obtain an algorithm with complexity $O(q^{1/2})$. When $N < 2q^{1/4}$ the previous algorithms satisfy the bound, so we assume $N > 2q^{1/4}$.
The width of the Hasse bound is $4\sqrt{q}$ so a random curve is isogenous to E_0 with probability $\Omega(\frac{1}{\sqrt{q}})$. So in $O(\sqrt{q})$ we can find a curve E_1' in the same component as E_0. With high probability E_1' is on (or close to) the floor eqv. $f_{E_1'} = f$, what we care about is that $N|f_{E_1'}$.
If E_0 happens to be above E_1' and $f_{E_1'} = N$ we can find the N-isogeny $\phi : E_0 \to E_1'$ using the algorithm from (2). This conditions are automatically satisfied when $f = N$ and $h_K = 1$. When $h_K > 1$ similar to (4) we have to search the crater for the curve that is above E_1' so the complexity is multiplied by h_K.
Let $f = NN'$, we know $f < q^{1/2}, N|f$ and $N > 2q^{1/4}$ therefore $N' < \frac{f}{N} < q^{1/4} < N$. We can compute the ascending N'-isogeny $\phi_a' : E_1' \to E_1''$ in $O(N'^2 \log(q) = \tilde{O}(N^2) = \tilde{O}(q^{1/2})$. Notice that $f_{E_1''} = N$, using the going down approach we compute an N-isogeny $\phi' : E_0' \to E_1''$, where E_0' is the curve on the crater directly above E_1". This computation takes $O(h_K N^{1/2})$.
Then compute a horizontal isogeny $\psi : E_0' \to E_0$ of degree co-prime to N. We can use the meet-in-the-middle algorithm with ideals of norm co-prime to N. This computation takes $O(h_0^{1/2})$. Now we can push ϕ' through ψ by computing $\psi(\mathrm{Ker}(\phi'))$ to get the N-isogeny $\phi : E_0 \to E_1$.
Complexity of this algorithm is $\tilde{O}(q^{1/2})$.

3 Random ordinary elliptic curves

Sampling a random ordinary elliptic curve over $\mathbb{F}_q$ where $q = p^r$ is easy: sample $a, b \in \mathbb{F}_q$ and check that $y^2 = x^3 + ax + b$ is non-singular and ordinary. With high probability it is non-singular and with probability $\frac{p-1}{p}$ it is ordinary. Supersingularity can be checked in poly-time using Schoof's point counting algorithm and more efficient methods exist [**?**, **?**].
The sampled curve E has random trace in $[-2\sqrt{q}, +2\sqrt{q}]$. We want to sample curves with prescribed order (eqv. prescribed trace). Currently we have two methods to do this: 1) Keep sampling curves until we find one with correct trace which is expected to require $O(\sqrt{q})$ guesses or use the CM-method that computes a root of the Hilbert class polynomial which takes $O(D_{\mathcal{O}})$ field operations. Both of these methods are exponential in q.
There are algortihms [**?**] that given N find p and $E/\mathbb{F}_p$ such that $|E(\mathbb{F}_p)| = N$. For some purposes this is sufficient as we only care about the order of the curve and not the field of definition. But for the purpose of problem (1) the field of definition is fixed so these algorithms don't help.

4 Quantum complexity of isogeny finding

In this section we look the quantum complexity of finding isogenies between two ordinary elliptic curves.
Let E_0 and E_1 be ordinary elliptic curves defined over $\mathbb{F}_q$ with trace t. We want to find an isogeny $\phi : E_0 \to E_1$. We will show that there is a quantum algorithm that solves this problem in $\tilde{O}(q^{2/9})$. The subalgorithms we use are the same as Steven's but we get better running time by applying quantum speedups.
First case is when E_0 is directly above E_1. The MiM algorithm proposed by Steven guesses a vector of integers in a space of $\sqrt{N}$ possible vectors. Using Grover's search algorithm this vector can be found with $N^{1/4}$ queries. Now assume E_0 is not known to be directly

above E_1. Recall that to find an isogeny we have two approaches: Walking up from E_1 or Walking down from E_0.
We can walk up from both E_0 and E_1 to the crater in time $O(N^2)$ and find a horizontal isogeny on the crater in subexponential (in the class number) time. So there is an algorithm that always solves this problem in $O(N^2)$. This implies that we can restrict to the case where there are at most four levels of descending N-isogenies. Assume there are five levels of descending N-isogenies, this means that $N^{10}D_K \leq f^2 D_K \simeq q$, this in turn means that $N = O(q^{1/10})$.
The walking down algorithm consists of searching for the curve on the same level as E_0 that is directly above E_1. Lets say E_0 is on level i and E_1 on level $i+j$. Level i has as many curves as the class number of $End(E_0)$ which is $N^i h_K$ so by using Grover's search algorithm we have to make $N^{i/2}\sqrt{h_K}$ many queries and testing whether a curve is directly above E_1 costs $O(N^{j/4})$ so overall it costs $O(\sqrt{h_K}N^{i/2+j/4})$.
Recall that $i+j$ is bounded by the number of descending N-isogeny levels so the worst case is when i is as large as possible but $j > 0$ other wise the isogeny is horizontal and can be computed using Kuperberg's algorithm, therefore the worst case is when i is as large as possible and $j = 1$.
There are at most 4 levels of descending N-isogenies, we treat each case individually:

1. 1 level.
   $Nh_K \leq f\sqrt{D_K} \simeq \sqrt{q} \to \sqrt{h_K} \leq \frac{q^{1/4}}{N^{1/2}} \to O(\sqrt{h_K}N^{1/4}) = O(\frac{q^{1/4}}{N^{1/4}})$. Now we find the tip over point between using the walking up and down algorithms.
   $\frac{q^{1/4}}{N^{1/4}} = N^2 \to q^{1/4} = N^{9/4} \to N = q^{1/9}$ therefore the worst case complexity of the algorithm is $O(q^{2/9})$.

2. 2 levels.
   $N^2h_K \leq f\sqrt{D_K} \simeq \sqrt{q} \to \sqrt{h_K} \leq \frac{q^{1/4}}{N} \to O(\sqrt{h_K}N^{1/2+1/4}) = O(\frac{q^{1/4}}{N^{1/4}})$. Now we find the tip over point between using the walking up and down algorithms.
   $\frac{q^{1/4}}{N^{1/4}} = N^2 \to q^{1/4} = N^{9/4} \to N = q^{1/9}$ therefore the worst case complexity of the algorithm is $O(q^{2/9})$.

3. 3 levels.
   $N^3h_K \leq f\sqrt{D_K} \simeq \sqrt{q} \to \sqrt{h_K} \leq \frac{q^{1/4}}{N^3/2} \to O(\sqrt{h_K}N^{2/2+1/4}) = O(\frac{q^{1/4}}{N^{1/4}})$. Now we find the tip over point between using the walking up and down algorithms.
   $\frac{q^{1/4}}{N^{1/4}} = N^2 \to q^{1/4} = N^{9/4} \to N = q^{1/9}$ therefore the worst case complexity of the algorithm is $O(q^{2/9})$.

4. 4 levels.
   $N^4h_K \leq f\sqrt{D_K} \simeq \sqrt{q} \to \sqrt{h_K} \leq \frac{q^{1/4}}{N^2} \to O(\sqrt{h_K}N^{3/2+1/4}) = O(\frac{q^{1/4}}{N^{1/8}})$. Now we find the tip over point between using the walking up and down algorithms.
   $\frac{q^{1/4}}{N^{1/8}} = N^2 \to q^{1/4} = N^{17/8} \to N = q^{2/17}$ therefore the worst case complexity of the algorithm is $O(q^{4/17})$ which is less that $q^{2/9}$.