Some applications of higher dimensional isogenies to elliptic curves
Preliminary version

DAMIEN ROBERT

Abstract. We give two applications of the "embedding Lemma". The first one is a deterministic polynomial time (in \(\log q\)) algorithm to compute the endomorphism ring \(\text{End}(E)\) of an ordinary elliptic curve \(E/\mathbb{F}_q\), provided we are given the factorisation of \(\Delta_x\).

The second application is an algorithm to compute the canonical lift of \(E/\mathbb{F}_q\), \(q = p^n\), (still assuming that \(E\) is ordinary) to precision \(m\) in time \(\tilde{O}(nm \log \tilde{O}(1) p)\). We deduce a point counting algorithm of complexity \(\tilde{O}(n^2 \log \tilde{O}(1) p)\). In particular the complexity is polynomial in \(\log p\), by contrast of what is usually expected of a \(p\)-adic cohomology computation. This algorithm generalizes to ordinary abelian varieties.

1. Introduction

By combining Kani’s lemma [Kan97, § 2] (extended to higher dimension) with Zarhin’s trick, we obtained in [Rob22a] the following embedding lemma: for any \(m > 0\), an \(N\)-isogeny \(f : A \to B\) in dimension \(g\) of principally polarised abelian varieties can always be efficiently embedded into an \(N + m\)-isogeny \(F\) in dimension \(8g\) (and sometimes \(4g\) or \(2g\)). \(F\) will actually be an endomorphism of \(A^u \times B^u\) where \(u = 1, 2\) or \(4\) depending on whether \(m\) is a sum of \(1, 2\) or \(4\) squares. Indeed, if \(u\) is as above we can build \(m\)-isogenies \(\alpha_A, \alpha_B\) on \(A^u, B^u\) such that \(\alpha_B f = f \alpha_A\), and take \(F = \left(\frac{\alpha_A}{\alpha_B}, -f\right)\). We remark that \(F\) embeds both \(f\) and its dual \(\tilde{f}\).

This has been applied to break SIDH in [CD22; MM22; Rob22a]. More generally, let us define the \(N\)-evaluation problem as follow: given an \(N\)-isogeny \(f : A \to B\) in dimension \(g\) of principally polarised abelian varieties can always be efficiently embedded into an \(N + m\)-isogeny \(F\) in dimension \(8g\) (and sometimes \(4g\) or \(2g\)). \(F\) will actually be an endomorphism of \(A^u \times B^u\) where \(u = 1, 2\) or \(4\) depending on whether \(m\) is a sum of \(1, 2\) or \(4\) squares. Indeed, if \(u\) is as above we can build \(m\)-isogenies \(\alpha_A, \alpha_B\) on \(A^u, B^u\) such that \(\alpha_B f = f \alpha_A\), and take \(F = \left(\frac{\alpha_A}{\alpha_B}, -f\right)\). We remark that \(F\) embeds both \(f\) and its dual \(f\).

This has been applied to break SIDH in [CD22; MM22; Rob22a]. More generally, let us define the \(N\)-evaluation problem as follow: given an \(N\)-isogeny \(f : A \to B/k\) and a point \(Q \in A(k)\), evaluate \(f(Q)\). Here we remain deliberately vague about how \(f\) is specified, usually it will be by its kernel \(K\), which is a maximal isotropic subgroup in \(A[N]\). The converse problem may be defined as follow: given an \(N\)-isogeny \(f\) as above, \(P \in A[N']\) and the tuple \((P, f(P))\) along with a point \(Q \in A(k)\), the \((N, N')\)-interpolation problem ask to evaluate \(f(Q)\). Of course, \(N'\) needs to be large enough compared to \(N\) so that \(f\) is uniquely determined by the data \(P, f(P)\). We will be interested in the following weaker variant: the \((N, N')\)-weak interpolation problem ask to evaluate \(f(Q)\) provided we are given the value of \(f\) on a basis of \(A[N]\).

Note that if \(N = N'\), given the value of \(f\) on a basis of \(A[N]\) we can (up to DLP computations) recover the kernel of \(f\), hence the weak evaluation problem reduces to the evaluation problem in this case.

We may apply the embedding lemma to solve the weak interpolation problem in the general case. Namely the embedding lemma gives us an \(N'\)-isogeny \(F\) that embeds \(f\), so evaluating \(f(Q)\) can be done by evaluating \(F(Q)\). Furthermore, if \(N'\) is prime to \(N\), \(\text{Ker} F\) can be completely determined by the value of \(f(A[N])\): \(\text{Ker} F = \{(\alpha_A x, -f x) : x \in A[N]\}\). A fun fact is that in this case we do not even need to compute DLPs to recover \(\text{Ker} F\). So the
weak \((N,N')\)-interpolation problem can always be reduced to an \(N'\)-evaluation problem in higher dimension, provided that \(N' > N\) is prime to \(N\). In fact, by considering the contragredient isogeny of \(F\), we only need \(N'^2 > N\), see [Rob22a, § 6.4].

This is interesting because if \(k = F_q\) is a finite field and \(N'\) is powersmooth (or if \(N'\) is smooth and \(A[N']\) lives in a small extension), the \(N'\)-evaluation problem can be done in polynomial time in \(\log q\) and the smoothness bound \(B\) of \(N'\) (here we assume the dimension \(g\) fixed). This has the following application to the \(N\)-evaluation problem: if we can evaluate \(f\) on the \(N'\)-torsion, it reduces trivially to the \((N,N')\)-weak interpolation problem, and we have just seen that this reduces to the \(N'\)-evaluation problem in higher dimension. So assuming that we have an oracle giving us this evaluation of \(f\) on \(A[N']\), we can reduce the \(N\)-evaluation problem into the \(N'\)-evaluation problem (in higher dimension), which we have seen can be computed in polynomial time if \(N'\) is powersmooth. In other words, we embed the \(N\)-isogeny \(f\) into a powersmooth \(N'\)-isogeny \(F\). This application is described in more details in [Rob22b].

Now the main obstacle of this idea is the need to evaluate \(f\) on the \(N'\)-torsion first. The main idea of this paper is that if \(\alpha\) is an \(N\)-isogeny, taking \(N' > N\) powersmooth and prime to \(N\) and the index \(f_{\alpha}\), we can evaluate the endomorphism \(\alpha\) represented abstractly as above on any point \(Q \in A(F_q)\) in time polynomial in \(\log q\) and the height of the coefficients of \(P_{\alpha}/D\). This allow us to embed \(\alpha\) into a higher dimensional endomorphism \(F_{\alpha}\).

Thus, if \(\alpha\) is an \(N\)-isogeny, taking \(N' > N\) powersmooth and prime to \(N\) and the index \(f_{\alpha}\), we can evaluate the endomorphism \(\alpha\) represented abstractly as above on any point \(Q \in A(F_q)\) in time polynomial in \(\log q\) and the height of the coefficients of \(P_{\alpha}/D\). Indeed, we can use Mahler’s bound to bound linearly the height of \(P_{\alpha}\) from the height of \(\alpha\) and of the characteristic polynomial \(\chi_{\alpha}\) of \(\alpha\) (we assume the dimension \(g\) fixed here). And by Weil’s theorem, the height of \(\chi_{\alpha}\) is linear in \(\log q\).

We will see how to apply these techniques to the computation of endomorphism rings and canonical lifts. This paper is just a preliminary version to give a brief leisurely description of the main algorithms, it will be followed by two technical papers giving more details and a finer complexity analysis.

1.1. Thanks. I thank Andrew Sutherland who asked me if higher dimensional isogenies could help computing the endomorphism ring of an elliptic curve. This led to Section 3. I thank Jean-Marc Couveignes and Pierrick Gaudry for various discussion about other applications of canonical lifts than point counting, and Aurel Page for brainstorming sessions.
about trying to apply the same techniques as Section 4 to compute the crystalline cohomology of a general ordinary scheme.

2. Embedding an isogeny

For our complexity analysis, we need to briefly review the results of [Rob22b].

Given an $N$-isogeny: $f : E \to E'$ over $\mathbb{F}_q$, we try to find $N'$ powersmooth (with powersmoothness bound $B$), such that $m = N' - N$ is a sum of $1, 2$ or $4$ squares. This allows to embed $f$ into a $N'$-isogeny in dimension $2u$.

To recover the kernel of $F$ and decompose it as a product of $(\leq B)$-isogenies, we need to work with algebras of degree up to $O(B^4)$. We need to push up to $\log N'$ points at each step, and each $(\leq B)$-isogeny evaluation cost $O(B^{2u})$. Since there are up to $\log N'$ steps, the complexity of decomposing $F$ is $O(B^4B^{2u}\log^2N')$ arithmetic operations. For subsequent isogeny evaluations, to evaluate $f(Q)$ if $Q \in E(\mathbb{F}_q)$, we work with algebra of degree up to $O(B^2)$, and follow $\log N'$ $(\leq B)$-isogenies, for a total cost of $O(B^2B^{2u}\log N')$ arithmetic operations. In practice, we will take a bound $B = O(\log N)$ and try to find $N'$ such that $\log N' = O(\log N)$, so the decomposition cost is $O(\log^{6+2u}B)$ arithmetic operations and further evaluations are in $O(\log^{3+2u}B)$ arithmetic operations.

So the smaller $u$, the better complexity, but the harder to find a suitable $N'$. The easiest case is $u = 4$, we just need to find a powersmooth $N' > N$ and prime to $N$. We simply take the product of the first $O(\log N)$ primes to $N$, and then decompose $N' - N$ as a sum of squares. This cost $O(\log^2 N)$. The hardest case is $u = 1$, we need to find $N'$ such that $N' - N$ is a square. In general this will not be possible. This could still have some applications, e.g. as in Section 4 where $N = p$, if we take the base field to be of a special form. The middle case is $u = 2$. It is difficult to test if an integer $N' - N$ is a sum of two squares (this requires factorizing it), so a solution is to test if $N' - N$ is prime and a sum of squares. A probabilistic algorithm (missing a few primes) cost $O(\log^2(N' - N))$. There is a heuristically a probability of $\Omega(1/\log N)$ that $N' - N$ is both a square and a sum of two primes, so we need to test $O(\log N)N'$. So we can find a suitable $N'$ in heuristic time $O(\log^3N)$. Of course once $N'$ and the decomposition of $N' - N$ as a sum of two squares is found, it is easy to check that $N'$ work.

3. Computing the endomorphism ring of an ordinary elliptic curve

If $E/\mathbb{F}_q$ is an ordinary elliptic curve, we can recover the characteristic polynomial $\chi_\pi = X^2 - tX + q$ of $\pi$ in polynomial time in $\log q$ by a point counting algorithm. We can thus recover $\Delta_\pi = t^2 - 4q$. If we know the factorisation of this discriminant, we can compute its associated fundamental discriminant, hence the maximal order $O_K = \mathbb{Z}[\omega]$ of $K = \mathbb{Q}(\sqrt{\Delta_\pi}) = \text{End}^0(E)$, and the factorisation of the conductor $f_\pi = [O_K : \mathbb{Z}[\pi]]$. We can write $\pi = a + f_\pi \omega$ (where $a$ will depends on the trace of $\pi$, so has height $O(\log q)$). We know that $\pi - a \in \text{End}(E)$. To determine $\text{End}(E)$ is equivalent to determining the index of $\text{End}(E)$ in $O_K$ or the index of $\mathbb{Z}[\pi]$ in $\text{End}(E)$, and so is equivalent to determining the largest divisor $f_E$ of $f_\pi$ such that $\frac{\pi - a}{f_E} \in \text{End}(E)$.

Since we know the factorisation of $f_\pi$, we are reduced to the following problem: let $g$ be a factor of $f_\pi$. Is $\frac{\pi - a}{g}$ in $\text{End}(E)$? This can be done by checking that $\pi - a$ is trivial on $E[g]$, but computing the $g$ torsion will be expensive if $g$ has a large prime power as a factor.

Remark 3.1. This approach to endomorphism ring computations is used in [EL07; FLO8] in dimension 2. The standard approach to compute the endomorphism ring of an ordinary
elliptic curve is to follow paths in the isogeny volcano and is due to Kohel [Koh06] (see also [FM02]). These algorithms are exponential in the worst case. An heuristic subexponential algorithm is presented in [BS09], and further improved in [Bis11] to only rely on the GRH.

Instead we use the embedding lemma. We know how \( \alpha = \frac{\pi - a}{8} \) is supposed to act on \( E[N'] \) (taking \( N' > N(\alpha) \) prime to \( g \) and \( N(\alpha) \)), if it exists as an endomorphism. If \( \alpha \) exists, we get an endomorphism \( F \) of \( E^{2u} \) (where \( u = 1, 2, 4 \)) that embeds \( \alpha \) as one of its matrix coefficient. So we first compute \( E^{2u}/\text{Ker} F \) to check that \( F \) is indeed an endomorphism. This can be done in polynomial time if \( N' \) is powersmooth. If not, we know that \( \alpha \) is not an endomorphism. If it is, since we can evaluate \( F \) efficiently, we can check if one of the matrix coefficient \( \beta \) of \( F \) acts like \( \alpha \) on \( E[N'' \) ], where \( N'' \) is powersmooth (we just need to check it on a basis of the \( N'' \)-torsion).\(^3\) Since \( F \) is an \( N'' \)-isogeny (because we have specified its kernel to be maximal isotropic in the \( N'' \)-torsion), the individual components are \((\leq N'')\)-isogenies.

Now by Cauchy-Schwarz, if \( \alpha \) and \( \beta \) are two endomorphisms of degree \( \leq M \), then \( \alpha + \beta \) is of degree \( \leq 4M \). So if the endomorphisms \( \alpha, \beta \) agree on \( E[N'' \) ], they are equal as long as \( N''^2 > 4M \).

So we check if we can find a matrix coefficient \( \beta \) that acts like \( \alpha \) on \( E[N'' \) ]. Then \( g\beta \) acts like \( \pi - a \) on \( E[N'' \) ], so by the above result we have that \( g\beta = \pi - a \) as long as \( N''^2 > 4 \max(g^2N', \deg (\pi - a)) = 4g^2N' \) (since we take \( N' > \deg((\pi - a)/g) \)). In this case, \( (\pi - a)/g \) is indeed an endomorphism, and the converse is immediate. Of course we will do that step by step, so we already know that say \( (\pi - a)\ell/g \) (with \( \ell \mid g \)) is an endomorphism and we just need to check that \( \ell\beta \) acts like \( (\pi - a)\ell/g \), which allows to take a smaller \( N'' \).

We do at most \( \log|\Delta_{\pi}\) steps, and the index \( f_{\pi} \), hence its divisors, is at most \( |\Delta_{\pi}| \). The full computation is thus polynomial in \( \log q \) and \( \log|\Delta_{\pi}| \). Since \( \log|\Delta_{\pi}| = \log(q^2 - 4t) = O(\log q) \), we get using Section 2:

**Theorem 3.2.** Given an ordinary elliptic curve \( E/\mathbb{F}_q \) and the factorisation of the discriminant of the Frobenius \( \pi \), \( \text{End}(E) \) can be determined in polynomial time \( O(\log^7 2^{2u} q) \) arithmetic operations.

Here we can take \( u = 4 \) to get a proven complexity, or \( u = 2 \) to get an heuristic one.

**Remark 3.3.** The same framework should allow to compute the endomorphism ring of an ordinary abelian variety, provided that we can work with real multiplication isogenies (and embed powersmoothly). We leave that for future work. It would also be very interesting to be able to move in the \( \ell \)-isogeny volcano in time polynomial in \( \log \ell \).

4. **Point counting and canonical lifts**

Let \( E/\mathbb{F}_q, q = p^n \) be an ordinary elliptic curve. The Frobenius \( \pi_q \) has two eigenvalues, one \( \lambda \) which is invertible modulo \( p \), and the other is \( q/\lambda \). Since \( \pi_q \) is easy to evaluate, we can evaluate its action on the tangent space \( T_0 E \), but this gives us \( 0 \) since it is inseparable. The action of the Verschiebung \( \pi_q \) on \( T_0 E \) allows us to recover \( \lambda \mod p \), hence the trace of \( \pi \) modulo \( p \). Since \( [q] = \pi_q \circ \pi_q^{-1} \), it is easy to evaluate the Verschiebung on a point \( P \) which is in the image of \( \pi_q \). Unfortunately this does not help us to evaluate it on the tangent space, since the image of the Frobenius there is trivial. An alternative is to compute the kernel of

---

\(^3\)To be more precise, we need to test \( \gamma\beta \) for all automorphisms \( \gamma \) of \( E \). But \( E \) has no automorphisms apart from \( (-1) \), unless \( j(E) = 0 \) or 1728. And we know the endomorphism ring of these curves.

\(^4\)We can also write \( \pi_q = t - \pi_q \), this is closer in spirit to the description of Section 1, but of course at this point we do not know the trace \( t \) yet.
the Verschiebung and apply Vélu’s formula, but since the degree of the Verschiebung is $q$, this is too expensive. (At this point we would actually compute the small Verschiebung instead which is of degree $p$).

Instead, since the Verschiebung is easy to compute on the $N'$-torsion ($N' > q$ powersmooth), we can embed it into a higher dimensional endomorphism $F$ of $E^{2u}$, this also embeds its dual $\pi_q$. We can then evaluate $F$ on the tangent space at $0$, this recover the action of $\pi_q$ and $\pi_q$ on $T_0E$. We thus get a polynomial time algorithm to recover $\lambda \mod p$. Like above, it is more efficient to only embed $\pi_q$ and $\pi_p$ and recover $\lambda$ via a norm, see [Rob21, § 6].

Using Section 2, this algorithm to recover $\lambda \mod p$ costs $O((\log p)^{6+2u})$ arithmetic operations.

Notice the similarity with Schoof algorithm: in Schoof we compute the action of $\pi_q$ on small $\ell'$-torsions groups $E[\ell']$, recover $\chi_{\pi}$ mod $\ell'$ via some DLP computations in $E[\ell']$, then reconstruct $\chi_{\pi}$ mod $\prod \ell'$ by the CRT. In our approach, we also compute $\pi_q$ (or $\pi_p$) on these $E[\ell']$, but we instead use the action to reconstruct $F$ a $\prod \ell'$ isogeny embedding $\pi_q$ and $\pi_p$ (or $\pi_p$ and $\pi_p$).

The nice thing about having the isogeny $F$ is that lifting $F$ gives a lift of the Frobenius. We can thus use $F$ to see how $\pi_p$ acts on the deformation space of $E$, and recover the canonical lift to precision $m$ as in [MR22].

Usually, the action of $\pi_p$ on the deformation space was computed using the modular polynomial $\phi_p$. The modular polynomial $\phi_p$ is of size $O(p^3)$, and then evaluating to $p$-adic precision $m$ cost $O((\log p)^2)$. In [MR22], we explained how to compute the action via lifting the kernel of the Verschiebung $\pi_p$ instead; since it is of degree $p$ this allows co compute canonical lift in time $O(p\log p)$. (A slight annoyance is that by using the Verschiebung rather than the Frobenius, we lose one bit in the $p$-adic precision at each step. In particular we need another method to boostrap to precision $m = 2$: we use the fact that the étale $p$-torsion only lifts to $\hat{E}$ if $\hat{E} = \hat{E}$ modulo $p^2$). Here we are going to use $F$ instead, this way we can recover the action of $\pi_p$ rather than $\pi_p$ so there is no loss of precision, but more importantly $F$ (and its lift) can be evaluated in time polynomial in $\log p$.

Let us describe this in more details. Assume for now for simplicity that our $F$ is in dimension 2. Let $\sigma$ be the lift of the Frobenius to $\mathbb{Q}_d$, and $\hat{E}$ denote the canonical lift of $E$. $\sigma'(E)$ is then the canonical lift of $\sigma'(E)$. $F$ is an endomorphism of $E \times \sigma'(E)$. The canonical lift $\hat{E}$ is the unique lift $\hat{E}$ of $E$ such that $\pi_p$ lifts to $\pi_p : \hat{E} \to \sigma'(\hat{E})$. We thus look for $\hat{E}$ such that the unique lift of $F$ (as an isogeny) to $\hat{E} \times \sigma'(\hat{E})$ is still an endomorphism (the lift is unique since $F$ is étale). We remark that lifting $F$ amount to lifting its kernel, which can be done by lifting generators of this kernel to points of $N'$ torsion in $\hat{E}$ via a Newton iteration.

Let us look at how to lift from precision $m = 1$ to precision $m = 2$, then $m = 4$, and so on. We fix an arbitrary lift $E_1$ of $E$ and another $E_2$ of $\sigma(E)$. We lift $F$ to compute its action on $E_1 \times E_2$. We can then deform $E_1$ to another lift $E_1'$, compute the action of $F$ again, and then deform $E_2'$ to $E_2$ and compute the action of $F$. This is enough, via linear algebra, to be able to compute the action of $F$ on arbitrary lifts of $E_1$ and $E_2$, namely if $j(\bar{E}_1) = j(\bar{E}_1') + \varepsilon_1p$, $j(\bar{E}_2) = j(\bar{E}_2') + \varepsilon_2p$, we can compute $J(\bar{E}_1 \times \bar{E}_2/\text{Ker} F) = J(\bar{E}_1' \times \bar{E}_2'/\text{Ker} F) + \varepsilon_1q + \varepsilon_2q$, where $J$ is a set of modular invariants in dimension 2. Note that we only care about the deformation of $E_1 \times E_2$ to a product abelian surface, that is why we only have two parameters $\varepsilon_1, \varepsilon_2$ rather than three.
If $\bar{E}$ is a lift of $E$, the Frobenius $\pi_p : E \to \sigma(E)$ lifts uniquely to $\bar{E} \to \bar{E}_2$. However in general the Verschiebung $\sigma(E) \to E$ does not lift to an arbitrary lift $\bar{E}_2$, and if it does the lift is not unique. In other words, the stack of elliptic curves with a degree $p$ isogeny is étale at $(E, \pi_p)$ when $E$ is ordinary, but not at $(E, \pi_p)$. In fact, by looking at the Serre-Tate formal moduli, it is classical that if $\bar{E} = \hat{E}$ to precision $m$, and $\hat{\pi}_p : \hat{E} \to \hat{E}_2$ is a lift of $\pi_p$, then $\bar{E}_2 = \sigma(\hat{E})$ to precision $m + 1$. Hence the Verschiebung $\bar{\pi}_p$ can be lifted to $\bar{E}_2$ if $\bar{E}_2 = \hat{E}$ to precision at least 2, and in this case, among the multiple possible lifts, there is a canonical one which is the dual of the lift of the Frobenius $\bar{E}_1 \to \bar{E}_2$. It is characterised by being the unique lift whose kernel lies in the maximal unramified extension of $\mathbb{Q}_p$.

Anyway going back to our situation, when taking an arbitrary lift $\bar{E}_1$ and $\bar{E}_2$ of $E$ and $\sigma(E)$, the lift of $\pi_p$ to $\bar{E}_1$ has codomain another elliptic curve $\bar{E}_{2,can}$, and so the codomain of the lift $\bar{F}$ of $F$ will not be a product abelian surface unless $\bar{E}_2 = \bar{E}_{2,can}$. On the moduli of abelian surfaces, the modular form $\chi_{10}$ has for locus the split surfaces, so plugging up $\chi_{10}$ in the expression of $J(\bar{E}_1 \times \bar{E}_2 / \text{Ker} \bar{F})$ above we get a linear equation between $\varepsilon_1$ and $\varepsilon_2$ giving the locus where $\bar{E}_2 = \bar{E}_{2,can}$. On this locus, the Verschiebung lifts from $\bar{E}_2$ to $\bar{E}_1$ by the above discussion, hence $F$ lifts as a matrix. Alternatively, we could plug the equation $J(\bar{E}_1 \times \bar{E}_2 / \text{Ker} \bar{F}) = J(\bar{E}_1 \times \bar{E}_2)$.

The canonical lift $\hat{E}$ at precision 2 can then be recovered by plugging the further equation $j(\hat{E}_{2,can}) = \sigma(j(\hat{E}_1))$. This way we obtain an Artin-Schreier equation $A\sigma(\varepsilon_1) + B\varepsilon_1 + C = 0$. Since the solution is unique, $A$ and $B$ are not both 0, so they are uniquely determined (up to normalising $C$) from $j(\hat{E})$ and $\sigma(j(\hat{E}))$. In the general case where we are in dimension $2u$, we also use the equations $j(\hat{E}_{2,can}) = \sigma(j(\hat{E}_1))$ and $J(\hat{E}_1 \times \hat{E}_2 / \text{Ker} \bar{F}) = J(\hat{E}_1 \times \hat{E}_2)$ where $J$ is a set of modular equations to recover this Artin-Schreier equation.

From the Serre-Tate formal moduli, we then know that $A$ is of valuation 0 and $B$ of valuation 1. We can thus solve the equation to precision $m' = 1$ and then lift it via Newton iterations to the precision we need. This allows us to compute our canonical lift from precision 1 to 2, and we iterate.

Of course, we can also use the lift $\hat{F}$ to compute the action of $\hat{\pi}_p$ on $T_0\sigma\hat{E}$ to precision $m$. By Section 2, the dominating cost is the initial decomposition of $\hat{F}$ as a product of small isogenies which cost $O(\log^{6+2u} p)$ arithmetic operations, then the evaluations of $\hat{F}$ at precision $m$ which cost $O(nm \log^{3+2u} p)$ arithmetic operations. In summary:

**Theorem 4.1.** Given $E / \mathbb{F}_q$ an ordinary elliptic curve, $q = p^u$, the canonical lift $\hat{E}$ of $E$ can be computed to precision $m$ in time $\tilde{O}(nm \log^{4+2u} p + n \log^{7+2u} p)$, and the cardinal of $E$ in time $\tilde{O}(n^2 \log^{4+2u} p + n \log^{7+2u} p)$.

Here $u = 1, 2$ or 4. We can only take $u = 1$ when $p$ is a special form. We can always take $u = 4$. We can also take $u = 2$, the cost of finding $N'$ described in Section 2 is heuristic, but once it is found it is easy to check that $N'$ works. Furthermore this can be seen as a precomputation depending only on $p$.

**Remark 4.2.** Over an ordinary abelian variety, the same method allows to recover the tangent matrix of $\hat{\pi}_p$ and $\hat{\pi}_p$ to precision $m$ in time $O(nm \log^{O(1)} p)$ (where the $O(1)$ hides a dependency at least linear in $g$).

**Remark 4.3.** Another way to compute a canonical lift with a complexity sublinear in $p$ is to compute the endomorphism ring and its class group, and then find a decomposition of the Frobenius as a product of small ideals. In other word, to find a cycle of small isogenies
from $E$ to $E$. (To forgo having to compute $\text{End}(E)$, one can also work with the class group of $\mathbb{Z}[\pi_E]$.) This gives an algorithm which is subexponential (under GRH) in $p$, see [CH02, Theorem 2]. (A similar approach is also implicit in [Koh08, § 4.2], where Kohel tries to find a path of small isogenies from $E$ to $\sigma(E)$.) Since small ideal decomposition can be found in quantum polynomial time, the approach of [CH02] also leads to a quantum polynomial time in $\log q$ algorithm. The main feature of Theorem 4.1 is of course that it works classically.

References


