Computing separable isogenies in quasi-optimal time

David Lubicz, Damien Robert

LMS J. Comput. Math. 18 (1) (2015) 198–216
doi:10.1112/S146115701400045X

Computing separable isogenies in quasi-optimal time

David Lubicz and Damien Robert

Abstract

Let A be an abelian variety of dimension g together with a principal polarization $\varphi : A \to \hat{A}$ defined over a field k. Let ℓ be an odd integer prime to the characteristic of k and let K be a subgroup of $A[\ell]$ which is maximal isotropic for the Riemann form associated to φ. We suppose that K is defined over k and let $B = A/K$ be the quotient abelian variety together with a polarization compatible with φ. Then B, as a polarized abelian variety, and the isogeny $f : A \to B$ are also defined over k. In this paper, we describe an algorithm that takes as input a theta null point of A and a polynomial system defining K and outputs a theta null point of B as well as formulas for the isogeny f. We obtain a complexity of $\widetilde{O}(\ell^{(rg)/2})$ operations in k where $r = 2$ (respectively, $r = 4$) if ℓ is a sum of two (respectively, four) squares which constitutes an improvement over the algorithm described in Cosset and Robert (*Math. Comput.* (2013) accepted for publication). We note that the algorithm is quasi-optimal if ℓ is a sum of two squares since its complexity is quasi-linear in the degree of f.

1. *Introduction*

Let k be a field and let A be a principally polarized abelian variety of dimension g defined over k. Let ℓ be an odd integer prime to the characteristic of k and let K be a subgroup of exponent ℓ of A. Let $B = A/K$ be the quotient abelian variety. In this paper, we are interested in computing the isogeny $f : A \to B = A/K$. Being able to compute isogenies between abelian varieties has many applications in algebraic number theory [**1**, **7**, **9**, **12**, **15**, **18**, **28**, **29**, **31**].

In order to have a concrete description of A, we consider a projective embedding of A provided by the global sections $H^0(A, \mathscr{L})$ of a symmetric ample line bundle $\mathscr{L}$. In the following, if $\mathscr{X}$ is an ample line bundle on A, we denote by $\varphi_{\mathscr{X}} : A \to \hat{A}$ the polarization corresponding to $\mathscr{X}$ and by $e_{\mathscr{X}} : A \times A \to \mathbb{G}_m$, the associated Riemann form. We suppose that $\mathscr{L} = \mathscr{L}_0^n$ with $\mathscr{L}_0$ a principal line bundle of A and $n \in \mathbb{N}$ which we call the level of $\mathscr{L}$. If $4|n$, we have a very convenient description of A as the intersection of a set of quadrics, given by the Riemann equations, in $\mathbb{P}^{H^0(A,\mathscr{L})}$, the projective space over the k-vector space $H^0(A, \mathscr{L})$ of dimension n^g. A choice of a basis of $H^0(A, \mathscr{L})$ and as a consequence of a choice of an embedding of A into the projective space $\mathbb{P}^{n^g-1}$ is fixed by a choice of a *theta structure* for $(A, \mathscr{L})$ (see [**26**, Definition p. 297]).

We suppose that this embedding is defined over k, which implies that k contains the field of definition of $\varphi_{\mathscr{L}}$. In order to avoid field extensions and have a more compact representation of A, we want to take n as small as possible. Most of the time, in applications, $n = 2$ or $n = 4$. In the following, we assume that $2|n$ and that ℓ is prime to n.

Now let K be a subgroup of $A[\ell]$ maximal isotropic for the Riemann form $e_{\mathscr{L}^\ell}$, that is given as input by a set of homogeneous equations in $\mathbb{P}^{H^0(A,\mathscr{L})}$, and let $f : A \to B = A/K$ be the

Received 14 May 2014; revised 2 August 2014.

2010 Mathematics Subject Classification 14K02, 14K25, 11G10.

The first and second authors were supported by the ANR Peace (reference ANR-12-BS01-0010-01), and the second author was also supported by the ERC Starting Grant ANTICS 278537 and the Lirima Laboratory through the Macisa project team.

corresponding isogeny. Then $\mathscr{L}$ descends by f to a line bundle $\mathscr{M}$ on B which is a n-power of a principal polarization $\mathscr{M}_0$. If K is k-rational, then both B and the polarization $\mathscr{M}$ are also rational. Our goal is to compute an embedding of B in $\mathbb{P}^{H^0(B,\mathscr{M})}$ as well as formulas for the isogeny $f : A \to B$. We can prove the following theorem.

THEOREM 1.1. *Let $(A, \mathscr{L}, \Theta_n)$ be a polarized abelian variety of dimension g with a symmetric theta structure of level n even, defined over a field k. Let ℓ be an integer prime to n and assume that ℓn is prime to the characteristic of k. Let K be a subgroup of $A[\ell]$ maximal isotropic for $e_{\mathscr{L}^\ell}$. Then one can compute the isogeny $A \to A/K$ in theta coordinates of level n by using $\widetilde{O}(\ell^{(rg)/2})$ operations in k where $r = 2$ (respectively, $r = 4$) if ℓ is a sum of two (respectively, four) squares.*

This is the same result as [**11**, Theorem 1.1] except that in [**11**] the input kernel K is given by generators of the group $K(\overline{k})$, and the resulting theorem is that the isogeny can be computed in $\widetilde{O}(\ell^{(rg)/2})$ operations in k', where k' is the compositum of the fields of definition of the geometric points of K. When k is a finite field, this yields a complexity of $\widetilde{O}(\ell^{(rg^2)/2})$ operations in k for the algorithm of [**11**], complexity that can be much worse when k is a number field. In the case $r = 2$, we remark that the complexity of the algorithm presented in this paper is quasi-linear in the degree of the kernel of the isogeny which is quasi-optimal for a very natural setting of the isogeny computation problem.

Our algorithm is very similar to that of [**11**, Theorem 1.1] which is based, on the one hand, on the algorithm described in [**24**] to compute an isogeny $f : A \to B$ between A together with a line bundle of level n and B with a line bundle of level $n\ell$, and, on the other hand, on the Koizumi general addition formula [**19**] from which a change of level formula is deduced (see [**11**, Proposition 4.1]). Our main improvement consists in working with 'formal points' rather than with geometric points of the kernel K.

One may ask how to find a description as an algebraic variety for a subgroup K of $A[\ell]$, i.e. obtain polynomial equations for it, which is one of the inputs of the algorithm presented in this paper. In the case where A is a Jacobian of a curve over a finite field the zeta function of which is known, it is possible to work with the geometric points of ℓ-torsion by taking random points in an appropriate extension (for more details, see [**5**]). One can then try to find directly a basis of a rational kernel K. Generating the equations of K from such a basis takes $\widetilde{O}(\ell^g)$ operations in the field k' (where k' is defined above as the compositum of the fields of definitions of the geometric points of K). As we already have the geometric points of the kernel, it might seem easier to directly use the algorithm from [**11**], but actually when ℓ is a sum of four squares this algorithm takes $\widetilde{O}(\ell^{2g})$ operations in k', so it is slower than the algorithm presented in this paper ($\widetilde{O}(\ell^g)$ operations in k' to find the equation of the kernel and $\widetilde{O}(\ell^{2g})$ operations in k to compute the isogeny). In particular, in the worst case where the points of K are in an extension of k of degree $O(\ell^g)$, we find that Theorem 1.1 gives a complexity of $\widetilde{O}(\ell^{2g})$ operations in k for all odd prime ℓ, whereas the algorithm from [**11**] gives a complexity of $\widetilde{O}(\ell^{2g})$ for primes congruent to 1 mod 4 and $\widetilde{O}(\ell^{4g})$ for primes congruent to 3 mod 4.

Another method would be to use modular polynomials as in the elliptic case to construct rational kernels. Unfortunately, there is a lack of a database of modular polynomials for higher-dimension abelian varieties, and there is as yet no known method to recover a kernel associated to a root of these modular polynomials. What can still be done though is to work with ℓ-division polynomials directly. An ℓ-division polynomial is a univariate polynomial of degree ℓ^{2g} parametrizing the variety $A[\ell]$, and by looking at rational factors of degree ℓ^g of this polynomial we can find rational kernels. This approach is mostly useful in the case where the base field k is a number field, because it yields an algorithm polynomial (but not quasi-linear) in ℓ to construct equations for a rational kernel K.

In particular, we explain in § 8 that if $(A, \mathscr{L}, \Theta_n)$ is a polarized abelian variety of dimension g with a symmetric theta structure of even level n defined over a number field k and ℓ is an integer prime to n then one can compute all rational isogenies $A \to A/K$ where K is a maximal isotropic subgroup of the ℓ-torsion $A[\ell]$ in time polynomial in ℓ. More generally we have a similar result over over any field k where we have an algorithm to construct rational subvarieties of a given zero-dimensional projective variety $\mathcal{V}$ that is polynomial in the degree of $\mathcal{V}$. For an application of isogenies over a number field, see [**6**], for instance.

Remark 1.2. Let $\mathscr{M}$ be an ample line bundle on B defining an embedding of B into $\mathbb{P}^{H^0(B,\mathscr{M})}$. If we want to express the isogeny $f : A \to B$ in term of this embedding, it is natural to take $\mathscr{M}$ such that $f^*(\mathscr{M})$ is a power $\mathscr{L}^m$ of $\mathscr{L}$. Indeed in that case f comes from a morphism of the projective spaces $\mathbb{P}^{H^0(A,\mathscr{L}^m)} \to \mathbb{P}^{H^0(B,\mathscr{M})}$ which can be computed without using the equations defining the embedding of A inside $\mathbb{P}^{H^0(A,\mathscr{L})}$. Descent theory tells us (see [**26**, Proposition 2]) that, for $m \in \mathbb{N}^*$, there exists such a line bundle $\mathscr{M}$ on B if and only if K is a subgroup of $\ker \varphi_{\mathscr{L}^m}$ and is isotropic for $e_{\mathscr{L}^m}$. As by [**26**, Proposition 4], $\ker \varphi_{\mathscr{L}^m} = \{x \in A(\bar{k}) \mid m \cdot x \in \ker \varphi_{\mathscr{L}}\}$, we have that K is a subgroup of $\ker \varphi_{\mathscr{L}^m}$ if and only if $\ell | m$. For efficiency reasons, it is better to take $m = \ell$. It is also more convenient to work with power of principal polarizations. When ℓ is prime to n, by [**26**, Proposition 2], $\mathscr{M}$ is a principal polarization if and only if K is maximal isotropic in the ℓ-torsion. This discussion motivates the hypothesis made in Theorem 1.1.

This paper relies heavily on the theory of theta functions which provides a convenient framework to represent and manipulate global sections of ample line bundles of abelian varieties. In order to avoid technical details, we have chosen to present our results using the classical theory of theta functions. For this, we assume that k is a number field and we suppose we are given a fixed embedding of k into $\mathbb{C}$. Nonetheless, it should be understood that, by using Mumford's theory of algebraic theta functions, all our algorithms apply without modification to the case of abelian varieties defined over any field of characteristic not equal to 2. The notations used have been chosen to make the translation into Mumford's formalism straightforward.

Our paper is organized as follows. In § 2 we gather some basic definitions about theta functions. In § 3 we recall the principle of the algorithm of [**11**]. Then, in § 5, we explain how to compute with formal points in K. Section 6 is devoted to the proof of the main results of this paper (in particular, Theorem 1.1), and in § 7 we give some examples. Finally, in § 8 we explain how to compute kernels over a number field.

2. *Notation and basic facts*

In this section, in order to fix the notation, we recall some well-known facts on analytic theta functions (see, for instance, [**4**, **27**]). Let $\mathbb{H}_g$ be the g-dimensional Siegel upper-half space which is the set of $g \times g$ symmetric matrices Ω with coefficients in $\mathbb{C}$ whose imaginary part is positive definite. For $\Omega \in \mathbb{H}_g$, we denote by $\Lambda_\Omega = \mathbb{Z}^g + \Omega\mathbb{Z}^g$ the lattice of $\mathbb{C}^g$. If A is a complex abelian variety of dimension g with a principal polarization then A is analytically isomorphic to $\mathbb{C}^g/\Lambda_\Omega$ for a certain $\Omega \in \mathbb{H}_g$. For $a, b \in \mathbb{Q}^g$, the theta function with rational characteristics (a, b) is the analytic function on $\mathbb{C}^g \times \mathbb{H}_g$:

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega) = \sum_{\nu \in \mathbb{Z}^g} \exp[\pi i^t (\nu + a)\Omega(\nu + a) + 2\pi i^t (\nu + a)(z + b)]. \tag{2.1}$$

We say that a function f on $\mathbb{C}^g$ is Λ_Ω-quasi-periodic of level $n \in \mathbb{N}$ if, for all $z \in \mathbb{C}^g$ and $m \in \mathbb{Z}^g$, we have $f(z + m) = f(z)$, $f(z + \Omega m) = \exp(-\pi i n^t m \Omega m - 2\pi i n^t z m) f(z)$ (where ${}^t v$ is the transpose of the vector v). For any $n \in \mathbb{N}^*$, the set $H_{\Omega,n}$ of Λ_Ω-quasi-periodic functions of

level n is a $\mathbb{C}$-vector space of dimension n^g a basis of which can be given by the theta functions with characteristics $(\theta \left[\begin{smallmatrix} 0 \\ b/n \end{smallmatrix}\right](z, n^{-1}\Omega))_{b\in[0,\dots,n-1]^g}$. There is a well-known correspondence (see [4, Appendix B]) between the vector space $H_{\Omega,n}$ and $H^0(A, \mathscr{L}_0^n)$ where $\mathscr{L}_0$ is the principal line bundle on A canonically defined by a choice of Ω.

Once we have chosen a level $n \in \mathbb{N}^*$ and $\Omega \in \mathbb{H}_g$ such that the abelian variety A is analytically isomorphic to $\mathbb{C}^g/\Lambda_\Omega$, for the rest of this paper, we adopt the following conventions. We let $Z(n) = (\mathbb{Z}/n\mathbb{Z})^g$ and, for a point $z \in \mathbb{C}^g$ and $\nu \in Z(n)$, we put $\theta_\nu^A(z) = \theta \left[\begin{smallmatrix} 0 \\ \nu/n \end{smallmatrix}\right](z, \Omega/n)$. If no confusion is possible, we will write $\theta_\nu(z)$ in place of $\theta_\nu^A(z)$.

A theorem of Lefschetz tells us that if $n \geqslant 3$, the functions in $H_{\Omega,n}$ give a projective embedding of A:

$$\begin{array}{rccc} \rho_n : & \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g) & \to & \mathbb{P}_{\mathbb{C}}^{Z(n)} \\ & z & \mapsto & (\theta_\nu(z))_{\nu\in Z(n)}. \end{array} \tag{2.2}$$

For $n = 2$, the functions in $H_{\Omega,2}$ do not give a projective embedding of A. Actually, it is easy to check that, for all $f \in H_{\Omega,2}$, we have $f(-z) = f(z)$. Under some well-known general conditions [19, Corollary 4.5.2], the image of the morphism defined by $H_{\Omega,2}$ in $\mathbb{P}^{Z(2)}$ is the Kummer variety associated to A, which is the quotient of A by the automorphism -1.

It is natural to look for algebraic relations between theta functions to obtain a description of the abelian variety as a closed subvariety of a projective space. A lot of them are given by a result of Riemann (see [23, Theorem 1]).

THEOREM 2.1. *Let $i, j, k, l \in Z(2n)$. We suppose that $i+j$, $i+k$ and $i+l \in Z(n)$. Let $\hat{Z}(2)$ be the dual group of $Z(2)$. For all $\chi \in \hat{Z}(2)$ and $z_1, z_2 \in \mathbb{C}^g$, we have*

$$\begin{aligned} &\Big(\sum_{\eta\in Z(2)} \chi(\eta)\theta_{i+j+\eta}(z_1+z_2)\theta_{i-j+\eta}(z_1-z_2)\Big)\Big(\sum_{\eta\in Z(2)} \chi(\eta)\theta_{k+l+\eta}(0)\theta_{k-l+\eta}(0)\Big) \\ &\quad = \Big(\sum_{\eta\in Z(2)} \chi(\eta)\theta_{i+k+\eta}(z_1)\theta_{i-k+\eta}(z_1)\Big)\Big(\sum_{\eta\in Z(2)} \chi(\eta)\theta_{j+l+\eta}(z_2)\theta_{j-l+\eta}(z_2)\Big), \end{aligned}$$

where $Z(n)$ (respectively, $Z(2)$) are considered as subgroups of $Z(2n)$ via the map $x \mapsto 2x$ (respectively, $x \mapsto nx$).

For $n \in \mathbb{N}^*$, we can associate to $\Omega \in \mathbb{H}_g$ its level n theta null point $(\theta_\nu(0))_{\nu\in Z(n)}$. By taking $z_2 = 0$ in Theorem 2.1, we obtain a set of quadratic equations which are parametrized by the theta null points of level n. A result of Mumford [26, Theorem 2] tells us that if $4|n$ this system of equations is complete in the sense that it gives the embedding of A into $\mathbb{P}^{Z(n)}$ defined by n and Ω following (2.2).

In the context of Mumford's theory of algebraic theta functions, the data of n and Ω which determine the theta null point is replaced by a level n *theta structure* Θ_n [26, Definition p. 297].

Let $\kappa : \mathbb{A}^{Z(n)} - \{0\} \to \mathbb{P}^{Z(n)}$ be the canonical projection. We denote by $\widetilde{A}$ the affine cone of A that is the closed subvariety defined as the Zariski closure of $\kappa^{-1}(A)$ in $\mathbb{A}^{Z(n)}$. We adopt the following convention. If $P \in \mathbb{P}^{Z(n)}(\mathbb{C})$, we will denote by $\widetilde{P}$ an *affine lift* of P that is an element of $\mathbb{A}^{Z(n)}(\mathbb{C}) - \{0\}$ such that $\kappa(\widetilde{P}) = P$. We denote by $\widetilde{P}_\nu \in \mathbb{C}$ for $\nu \in Z(n)$ the νth coordinate of the point $\widetilde{P}$ and, for $\lambda \in \mathbb{C}$, we let $\lambda \star \widetilde{P} \in \mathbb{A}^{Z(n)}(\mathbb{C})$ be the point such that $(\lambda \star \widetilde{P})_\nu = \lambda\widetilde{P}_\nu$. In the same way, if $P \in A(\mathbb{C})$, we denote by $z_P \in \mathbb{C}^g$ a point such that $\rho_n(z_P) = P$. We remark that z_P actually defines the affine lift $(\theta_\nu(z_P))_{\nu\in Z(n)} \in \widetilde{A}(\mathbb{C})$ of P which we call a *good lift* (note that such a good lift is not unique since z_P is defined by P up to an element of Λ_Ω). We denote by $\widetilde{\rho}_n : \mathbb{C}^g \to \widetilde{A}$, the map given by $z \mapsto (\theta_\nu(z))_{\nu\in Z(n)}$. In the following, we choose $\widetilde{0}_A \in \widetilde{A}(k)$ an affine lift of $\kappa((\theta_\nu(0))_{\nu\in Z(n)})$.

As the canonical line bundle defined by Ω is not defined over k (not even over an algebraic extension of k), we have, in general, $\widetilde{0}_A = \lambda(\theta_\nu(0))_{\nu\in Z(n)}$ for $\lambda \in \mathbb{C}$ not in $\overline{k}$. This subtlety does not change the projective embedding given by Riemann's equations, nor the computations presented in this paper for homogeneity reasons (see Proposition 3.3 and [**23**, Remark 3]), so that we can safely suppose in the following that $\lambda = 1$.

Using Riemann equations, from the data of $\widetilde{0}_A$, $(\theta_\nu(z_1))_{\nu\in Z(n)}$, $(\theta_\nu(z_2))_{\nu\in Z(n)}$, $(\theta_\nu(z_1 - z_2))_{\nu\in Z(n)} \in \widetilde{A}(\mathbb{C})$, one can recover $(\theta_\nu(z_1 + z_2))_{\nu\in Z(n)} \in \widetilde{A}(\mathbb{C})$ provided that, for sufficiently many $\chi \in \hat{Z}(2)$, $k, l \in Z(n)$, we have $\sum_{\eta\in Z(2)} \chi(\eta)\theta_{k+l+\eta}(0)\theta_{k-l+\eta}(0) \neq 0$. This is always the case if the level n is divisible by 4; and if $n = 2$, it is true if the projective embedding of the Kummer variety of A given by level 2 theta functions is projectively normal (see [**23**, § 4]). We will always suppose that these conditions are fulfilled in the following. The operation on affine points that we obtain is called a *differential addition* (see [**23**] for more details). Chaining differential additions in a classical Montgomery ladder [**10**, Algorithm 9.5 p. 148] yields an algorithm that takes as inputs $\widetilde{Q} = (\widetilde{Q}_\nu)_{\nu\in Z(n)}$, $\widetilde{P+Q} = (\widetilde{(P+Q)}_\nu)_{\nu\in Z(n)}$, $\widetilde{P} = (\widetilde{P}_\nu)_{\nu\in Z(n)}$, $\widetilde{0}_A = (\widetilde{0}_\nu)_{\nu\in Z(n)}$ and an integer ℓ and outputs $\widetilde{Q+\ell P}$. We write $\widetilde{Q+\ell P} = \mathrm{ScalarMult}(\ell, \widetilde{P+Q}, \widetilde{P}, \widetilde{Q}, \widetilde{0}_A)$.

If $4|n$, we can compute the 'normal' addition law on the abelian variety: actually, by computing sums of the form $\sum_{\eta\in Z(2)} \chi(\eta)\theta_i(z_1 + z_2)\theta_{j_0}(z_1 + z_2)$ with Riemann relations for a fixed $j_0 \in Z(n)$, from the knowledge of $\widetilde{0}_A$ and the projective points $(\theta_\nu(z_j))_{\nu\in Z(n)}$ for $j = 1, 2$, we can recover the projective point $(\theta_\nu(z_1 + z_2))_{\nu\in Z(n)}$. We call this operation NormalAdd.

3. *Koizumi formula and isogeny computation*

In this section, we briefly recall the principle of the isogeny computation algorithm presented in [**11**]. Let $(A, \mathscr{L}_0)$ be a principally polarized abelian variety given by $\Omega \in \mathbb{H}_g$ such that A is analytically isomorphic to $\mathbb{C}^g/\Lambda_\Omega$. Let ℓ be an odd integer prime to n and let K be a subgroup of $A[\ell]$ maximal isotropic for the Riemann form $e_{\mathscr{L}_0}$. As K is isotropic for $e_{\mathscr{L}_0}$, up to an action of an element of the symplectic group $\mathrm{Sp}_{2g}(\mathbb{Z})$ on Λ_Ω, we can always suppose that $K = (1/\ell)\mathbb{Z}^g/\Lambda_\Omega$ so that our problem comes down to the computation of the isogeny:

$$\begin{array}{ccc} f : A \simeq \mathbb{C}^g/\Lambda_\Omega & \to & B \simeq \mathbb{C}^g/\Lambda_{\ell\Omega} \\ z & \mapsto & \ell z. \end{array}$$

An important ingredient of the isogeny computation algorithm is the following formula derived from the general Koizumi formula (see [**11**, Proposition 4.1]).

PROPOSITION 3.1. *Let M be a matrix of* rank r *with coefficients in $\mathbb{Z}$ such that ${}^tMM = \ell Id$. Let $X \in (\mathbb{C}^g)^r$ and $X = YM^{-1} \in (\mathbb{C}^g)^r$. Let $i \in (Z(n))^r$ and $j = iM^{-1}$. Then we have*

$$\theta^B_{i_1}(Y_1)\dots\theta^B_{i_r}(Y_r) = \sum_{\substack{t_1,\dots,t_r\in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ (t_1,\dots,t_r)M=(0,\dots,0)}} \theta^A_{j_1}(X_1 + t_1)\dots\theta^A_{j_r}(X_r + t_r). \tag{3.1}$$

In particular, the projective coordinates of the theta null point of B are given by the equations

$$\theta^B_k(0)\dots\theta^B_0(0) = \sum_{\substack{t_1,\dots,t_r\in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ (t_1,\dots,t_r)M=(0,\dots,0)}} \theta^A_{j_1}(t_1)\dots\theta^A_{j_r}(t_r), \tag{3.2}$$

where $j = (k, 0, \dots, 0)M^{-1} \in Z(n)^r$.

Likewise, if $P \in A(k)$ we can recover the projective coordinates of $f(P)$ via the equations

$$\theta_k^B(\ell z_P)\dots\theta_0^B(0) = \sum_{\substack{t_1,\dots,t_r\in\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ (t_1,\dots,t_r)M=(0,\dots,0)}} \theta_{j_1}^A(X_1+t_1)\dots\theta_{j_r}^A(X_r+t_r), \tag{3.3}$$

where $z_P \in \mathbb{C}^g$ is such that $\rho_n(z_P) = P$, $X = YM^{-1}$ with $Y = (\ell z_P, 0, 0, 0)$ and $j = (k, 0, \dots, 0)M^{-1}$ for $k \in Z(n)$. We remark that the X_i are integral multiples $\alpha_i z_P$ of z_P, where $(\alpha_1, \dots, \alpha_r) = (1, \dots, 0)^t M$ and $\alpha_i \in \{1, \dots, \ell-1\}$.

The algorithm takes as input the projective theta null point of A, 0_A, as well as a basis $(e_1, \dots, e_g)$ of $K(\overline{k})$. We can suppose that $(e_1, \dots, e_g)$ is the image by ρ_n of the canonical basis of $(1/\ell)\mathbb{Z}^g/\mathbb{Z}^g$ if necessary by acting on Λ_Ω by an element of $\mathrm{Sp}_{2g}(\mathbb{Z})$. In order to compute the isogeny, we need to evaluate expressions of the form of the right-hand side of (3.1) which depends on the knowledge of the good lifts of the form $(\theta_\nu(X_i + t_i))_{\nu\in Z(n)}$ where $X_i = \alpha_i z_P$ is an integral multiple of z_P. Moreover, we note that these good lifts have to be coherent, meaning that they are all derived from the same z_P such that $\rho_n(z_P) = P$ (we cannot change z_P from one term of the sum to another). Of course since everything is homogeneous, we only need to work up to a common projective factor λ and take coherent lifts over any affine lift $\widetilde{P}$ of P. This motivates the following definition:

Definition 3.2. We assume that we have fixed once and for all an affine lift $\widetilde{0}_A$ of 0_A. Suppose that we have fixed affine lifts $\widetilde{Q}$ of every geometric point $Q \in K(\overline{k})$ (we require that the lift of 0_A is $\widetilde{0}_A$). We say that these lifts are *compatible* (with respect to $\widetilde{0}_A$) if they differ from the good lifts $(\theta_\nu(z_Q))_{\nu\in Z(n)}$ for $z_Q \in (1/\ell)\mathbb{Z}^g/\mathbb{Z}^g$ by the same projective factor λ (independently of Q).

Let $P \in A(\overline{k})$ and fix an affine lift $\widetilde{P}$ above it. Suppose that, together with the compatible lifts $\widetilde{Q}$ from above, we have chosen affine lifts of every geometric point $\alpha P+Q$ where $Q \in K(\overline{k})$ and $\alpha \in \{0, \dots, \ell-1\}$ (we require that the lift of P is $\widetilde{P}$). We say that these lifts are *compatible with respect to* $\widetilde{0}_A$ if there exists $z_P \in \mathbb{C}^g$ with $\rho_n(z_P) = P$ such that they differ from the good lifts $(\theta_\nu(\alpha z_P + z_Q))_{\nu\in Z(n)}$ for $z_Q \in (1/\ell)\mathbb{Z}^g/\mathbb{Z}^g$ by the same projective factor λ.

We extend the definition of compatible lifts by saying that a set of points $\{\widetilde{Q}\}$ or $\{\widetilde{P+Q}\}$ (where the points Q are in $K(\overline{k})$ and P is a fixed point in $A(\overline{k})$) are compatible (with $\widetilde{0}_A$ or $\widetilde{P}$) when they are part of a family of compatible points.

We would like to have an algebraic way to identify compatible lifts.

Proposition 3.3. *Let $Q \in K(\overline{k})$ and write $\ell = 2\ell'+1$. Let $\widetilde{Q}$ be an affine lift of Q compatible with $\widetilde{0}_A$. Then*

$$\mathrm{ScalarMult}(\ell'+1, \widetilde{Q}, \widetilde{Q}, \widetilde{0}_A, \widetilde{0}_A) = -\mathrm{ScalarMult}(\ell', \widetilde{Q}, \widetilde{Q}, \widetilde{0}_A, \widetilde{0}_A). \tag{3.4}$$

If $\widetilde{Q}$ satisfies equation (3.4), we say that it is a potential compatible lift of Q (with respect to $\widetilde{0}_A$).

Likewise, let $P \in A(\overline{k})$, $\widetilde{P}$ be any affine lift of P, and let $\widetilde{P+Q}$ be an affine lift of $P+Q$ compatible with $\widetilde{P}$. Then

$$\mathrm{ScalarMult}(\ell, \widetilde{P+Q}, \widetilde{Q}, \widetilde{P}, \widetilde{0}_A) = \widetilde{P}. \tag{3.5}$$

If $\widetilde{P+Q}$ satisfies equation (3.5), we say that it is a potential compatible lift of $P+Q$ (with respect to $\widetilde{P}$).

Proof. We begin with the first claim. By [24, Lemma 3.10], if we let $\chi(\alpha,\beta,m) = \mathrm{ScalarMult}(m,\alpha\star\widetilde{Q},\alpha\star\widetilde{Q},\beta\star\widetilde{0}_A,\beta\star\widetilde{0}_A)$ for $\alpha,\beta\in\mathbb{C}$ and $m\in\mathbb{N}$, we have $\chi(\alpha,\beta,\ell'+1)/\chi(\alpha,\beta,\ell') = (\alpha^\ell/\beta^\ell)(\chi(1,1,\ell'+1)/\chi(1,1,\ell'))$. Thus, by virtue of homogeneity, we can suppose that $\widetilde{0}_A = (\theta_\nu(0))_{\nu\in Z(n)}$. Let $z_Q\in(1/\ell)\mathbb{Z}^g$ be such that $\widetilde{\rho}_n(z_Q)=\widetilde{Q}$; we have $\ell' z_Q = -(\ell'+1)z_Q \mod \mathbb{Z}^g$. As $\mathrm{ScalarMult}(\ell'+1,\widetilde{Q},\widetilde{Q},\widetilde{0}_A,\widetilde{0}_A) = (\theta_\nu((\ell'+1)z_Q))_{\nu\in Z(n)}$ and $\mathrm{ScalarMult}(\ell',\widetilde{Q},\widetilde{Q},\widetilde{0}_A,\widetilde{0}_A) = (\theta_\nu(\ell' z_Q))_{\nu\in Z(n)}$, we obtain (3.4) because of the periodicity of θ_ν with respect to $\mathbb{Z}^g$.

Still using [24, Lemma 3.10], we have $\mathrm{ScalarMult}(\ell,\alpha\star\widetilde{(P+Q)},\beta\star\widetilde{Q},\alpha\star\widetilde{P},\beta\star\widetilde{0}_A) = \alpha\star\mathrm{ScalarMult}(\ell,\widetilde{P+Q},\widetilde{Q},\widetilde{P},\widetilde{0}_A)$ for $\alpha,\beta\in\mathbb{C}$. Thus we can assume that $\widetilde{0}_A=(\theta_\nu(0))_{\nu\in Z(n)}$ and $\widetilde{P}=\widetilde{\rho}_n(z_P)$ for $z_P\in\mathbb{C}^g$. It is then easy to check, using the Λ_Ω-quasi-periodicity property of θ_ν for $\nu\in Z(n)$, that $\theta_\nu(z_P+\ell z_Q)=\theta_\nu(z_P)$. □

If $Q\in K(\overline{k})$, let $\widetilde{Q}$ be any lift, and let $\lambda\in\mathbb{C}$ be such that $\lambda\star\widetilde{Q}$ is a compatible lift $\widetilde{\rho}_n(z_Q)$ for $z_Q\in\mathbb{C}^g$. We remark that because of the symmetry relations [27, Proposition 3.14], for all $\nu\in Z(n)$, we have $\theta_\nu((\ell'+1)z_Q) = \theta_{-\nu}((\ell' z_Q))$. Thus, if $\delta = \widetilde{(\ell' Q)}_\nu/\widetilde{((\ell'+1)Q)}_{-\nu}$ for any $\nu\in Z(n)$, by [23, Remark 3], we have $\lambda^\ell=\delta$. Thus we can obtain λ up to an ℓth root of unity. In the same way, let $\widetilde{P+Q}$ be any affine lift of $P+Q$ and $\mu\in\mathbb{C}$ be such that $\mu\star\widetilde{(P+Q)}$ is a compatible lift. Then from equation (3.5) and [24, Lemma 3.10], if we set $\widetilde{P+\ell Q} = \mathrm{ScalarMult}(\ell,\widetilde{P+Q},\widetilde{Q},\widetilde{P},\widetilde{0}_A)$, we obtain a relation of the form $\mu^\ell\lambda^{\ell(\ell-1)}=\beta$ where $\beta = \widetilde{P}_\nu/\widetilde{(P+\ell Q)}_\nu$, $\nu\in Z(n)$. As we know λ^ℓ from above, we can recover μ^ℓ.

We can summarize [14, Proposition 18] and [24, § 3] in the following theorem.

THEOREM 3.4. *Let $(e_1,\dots,e_g)$ be a basis of a maximal isotropic subgroup K of $A[\ell]$. Assume that we have chosen potential compatible lifts $\widetilde{e}_i$, $\widetilde{e_i+e_j}$ with respect to $\widetilde{0}_A$. Then:*

- *we can use the* ScalarMult *algorithm to compute potential compatible lifts $\widetilde{Q}$ for every point of $K(\overline{k})$ from the data of $\widetilde{e}_i,\widetilde{e_i+e_j}$;*
- *up to an action of $\mathrm{Sp}_{2g}(\mathbb{Z})$ on Λ_Ω which leaves $\mathbb{Z}^g\subset\mathbb{C}^g$ invariant (and also $(\theta_\nu(0))_{\nu\in Z(n)}$), these lifts $\widetilde{Q}$ are compatible with $\widetilde{0}_A$;*
- *if $\widetilde{P}$ is an affine lift of a point $P\in A(\overline{k})$ and we are given potential compatible lifts $\widetilde{P+e_i}$ with respect to $\widetilde{P}$, then they are actually compatible with $\widetilde{P}$ and we can use the* ScalarMult *algorithm to obtain compatible lifts (with respect to $\widetilde{P}$) of all points of the form $\alpha P+Q$ for $\alpha\in\{0,\dots,\ell-1\}$.*

Sketch of proof. We prove the first two claims. Let $\lambda_i,\lambda_{ij}\in\mathbb{C}$ be such that $\lambda_i\star\widetilde{e}_i$, $\lambda_{ij}\star\widetilde{(e_i+e_j)}$ are compatible lifts. We know by the discussion following Proposition 3.3 that the λ_i,λ_{ij} are ℓth roots of unity. Using the transformation formula for theta functions [27, p. 189], we can find a symplectic matrix M in $\mathrm{Sp}_{2g}(\mathbb{Z})$ that leaves K (globally) invariant and acts by $\star$ on the compatible lifts of e_i and e_i+e_j exactly by λ_i^{-1} and λ_{ij}^{-1}. Since ℓ is prime to $2n$ we can even ask for M to be congruent to the identity modulo $2n$ so that it leaves the theta null point $\widetilde{0}_A$ invariant [17]. By definition of differential addition and Riemann equations (see Theorem 2.1), starting from compatible points $\widetilde{e}_i$ and $\widetilde{e_i+e_j}$, we can generate compatible lifts of all geometric points in the kernel with the ScalarMult algorithm.

As for the third claim, by homogeneity, we can assume that $\widetilde{P}$ is a good lift coming from a point $z_P\in\mathbb{C}^g$. Let $\mu_j\in\mathbb{C}$ be such that $\mu_j\star\widetilde{(P+e_j)}$ is a compatible lift with respect to $\widetilde{P}$. Then, Proposition 3.3 shows that the μ_j are ℓth roots of unity. For $j=1,\dots,g$, let $\varepsilon_j\in(1/\ell)\mathbb{Z}^g/\mathbb{Z}^g$ be such that $\rho_n(\varepsilon_j)=e_j$. The functional equation for theta functions [27, p. 123] gives that for $a,b\in\mathbb{Z}^g$ and $j=1,\dots,g$, we have $\theta_\nu(z_P+\varepsilon_j+\Omega a+b) = e^{-\pi i(n^{2t}a\Omega a+2n^t a(z_P+\varepsilon_j))}\theta_\nu(z_P)$.

So up to the common constant $e^{-\pi i(n^t a\Omega a+2n^t a z_P)}$, if necessary by changing z_P to $z_P+\Omega a$ for a well-chosen $a\in\mathbb{Z}^g$, we can suppose that the $\widetilde{P+e_i}$ are compatible lifts with respect to $\widetilde{P}$. By using differential additions one can then generate any compatible lift of the form αz_P+z_Q, $z_Q\in(1/\ell)\mathbb{Z}^g/\mathbb{Z}^g$. □

For $i=1,\dots,g$, we choose any affine lifts $\widetilde{e_i}$ of e_i. By using normal additions, we can compute e_i+e_j and choose affine lifts $\widetilde{e_i+e_j}$. Let $\lambda_i,\lambda_{ij}\in\mathbb{C}$ be such that $\lambda_i\star\widetilde{e_i}$, $\lambda_{ij}\star(\widetilde{e_i+e_j})$ are potential compatible lifts. Note that, by the discussion after Proposition 3.3, we know λ_i^ℓ and λ_{ij}^ℓ. Then Theorem 3.4 tells us that by choosing any root for the λ_i and λ_{ij} we can generate compatible lifts and evaluate equation (3.2) to get the theta null point $(\theta^B_\nu(0))_{\nu\in Z(n)}$ of $B=A/K$. Actually, if we work formally with the λ_i, λ_{ij}, then the right-hand side of (3.2) is a rational function of λ_i, λ_{ij}. But by [**11**, Lemma 4.2], this rational function actually lies in $\mathbb{C}(\lambda_i^\ell,\lambda_{ij}^\ell)$ so that we can evaluate it directly.

In the same way, we can compute the image $f(P)$ of $P\in A(\overline{k})$ given by its projective theta coordinates. Indeed, from the knowledge of P and e_i, we can compute the projective points $P+e_i$ with normal additions. We choose affine lifts $\widetilde{P+e_i}$ of $P+e_i$, and let $\mu_i\in\mathbb{C}$ be such that $\mu_i\star(\widetilde{P+e_i})$ are potential compatible lifts. By Proposition 3.3 we know the value of μ_i^ℓ, and Theorem 3.4 tells us that by choosing any set of roots we get compatible lifts for the points appearing in the right-hand side of (3.3). We can as such find the projective coordinates of $f(P)$. Actually, if we work formally with the $\mu_i,\lambda_{ij},\lambda_i$ we can evaluate the right-hand side of (3.3) as a rational function in $\mathbb{C}(\mu_i,\lambda_i,\lambda_{ij})$. But by [**11**, Lemma 4.4] this rational function is an element of $\mathbb{C}(\mu_i^\ell,\lambda_i^\ell,\lambda_{ij}^\ell)$ so that we can evaluate that directly too.

4. *Equations for the kernel*

We retain the notation of the preceding section. Recall that A together with a projective embedding inside $\mathbb{P}^{Z(n)}$ is given by the data of its theta null point $\widetilde{0}_A$. As K is defined over k, we can suppose that K is represented, as a zero-dimensional subvariety of $\mathbb{P}^{Z(n)}$, by a triangular system of homogeneous polynomial equations with coefficients in k:

$$\begin{aligned} Q_{i_1}(U_{i_0},U_{i_1})&=0\\ Q_{i_2}(U_{i_0},U_{i_1},U_{i_2})&=0\\ &\vdots\\ Q_{i_{n^g-1}}(U_{i_0},U_{i_1},\dots,U_{i_{n^g-1}})&=0, \end{aligned} \tag{4.1}$$

for $i_j\in Z(n)$. Indeed, from the knowledge of a set of generators of a homogeneous ideal defining K as a closed subvariety of $\mathbb{P}^{Z(n)}$, such a triangular system may be obtained by computing the reduced Groebner basis for the lexicographic order on the variables $U_{i_0},\dots,U_{i_{n^g-1}}$.

If necessary, by carrying out a linear change of variables, we can always suppose that $i_0=0\in Z(n)$ and $\mathrm{V}(U_0)(\overline{k})\cap K(\overline{k})=\varnothing$ (where $\mathrm{V}(U_0)$ is the closed subvariety of $\mathbb{P}^{Z(n)}$ defined as the zeros of U_0) and we contend that this linear change of variables is defined over a small extension of k. Indeed, we just have to find a hyperplane of $\mathbb{P}^{Z(n)}$ passing through the origin and avoiding all the points of K. We remark that the set of hyperplanes passing through the origin and a point $x\in K(\overline{k})$ is represented by an hyperplane through the origin in the Grassmannian $\mathrm{Gr}(n-1,Z(n))$. As a consequence, the set of hyperplanes passing through the origin and a point of K is a hypersurface H of degree bounded by $\ell^g=\#K(\overline{k})$ in $\mathrm{Gr}(n-1,Z(n))$. If the field k is infinite there exists a point of $\mathrm{Gr}(n-1,Z(n))(k)$ which is not in $H(k)$ and we are done. If $k=\mathbb{F}_q$ is finite, by a result of Serre [**30**], an upper bound for $\#H(k)$ is $\ell^g q^{n^g-2}+\Pi_{n^g-3}$ where $\Pi_m=(q^{m+1}-1)/(q-1)$ is the cardinality of $\mathbb{P}^m(\mathbb{F}_q)$. Thus, a random

point in $\mathrm{Gr}(n-1, Z(n))(k)$ will not be in $H(k)$ with high probability as soon as q is sufficiently large compared to ℓ^g. We deduce that we can find (probabilistically) a hyperplane in $\mathbb{P}^{Z(n)}$ that avoids K by working over an extension of k of degree $O(\ln(\ell^g))$. Let k' be such an extension, as the arithmetic in k' has the same complexity as the arithmetic in k up to a factor in $O(\ln(\ell^g))$ which we have chosen to neglect in the statement of Theorem 1.1, we can safely suppose in the following that $k = k'$.

From our hypothesis, the variable U_0 plays the role of the normalizing factor of a projective point. We consider the algebra

$$\mathscr{K}_0 = k[U_i \mid i \in Z(n)]/(Q_{i_1}(1, U_{i_1}), \ldots, Q_{i_{n^g-1}}(1, U_{i_1}, \ldots, U_{i_{n^g-1}})).$$

We note that the system (4.1) is generically such that $\deg_{U_{i_1}}(Q_{i_1}) = \ell^g$ and $\deg_{U_i} Q_i = 1$ for $i \in Z(n) - \{0, i_1\}$. Actually, it can be seen exactly as before, by considering the set of hyperplanes in the $\mathrm{Gr}(n-1, Z(n))$ that intersect the vector defined by a pair of elements of $K(\overline{k})$, that this property is always true if we carry out a linear change of coordinates. This is known as the 'shape lemma', which holds in our situation because the kernel is reduced; we refer to [**3**] for more details. This linear change of coordinates may involve an extension of k of degree $O(\ln(\ell^g))$ when k is finite with negligible consequences for the asymptotic complexity of the arithmetic of the base field. From now on, we suppose that $\deg_{U_i} Q_i = 1$ for $i \in Z(n) - \{0, i_1\}$ and we let $Q(U) = Q_{i_1}(1, U) \in k[U]$. The algebra $\mathscr{K}_0$ is then isomorphic to the algebra $\mathscr{K} = k[U]/(Q)$.

The transformation from equation (4.1) to a polynomial system defined by one polynomial Q will not be necessary for the algorithms presented in the next section, but it helps for computations in the algebra associated to $\mathscr{K}$.

5. *Computation with formal points*

We retain the notation of the previous section. We thus have an isomorphism $K \xrightarrow{\sim} \mathrm{Spec}\,\mathscr{K}$ associated to the isomorphism $\mathscr{K} \xrightarrow{\sim} \mathscr{K}_0$ on coordinate functions. We recall that a point $\eta \in A(\mathscr{K})$ is by definition a morphism $\eta : \mathrm{Spec}\,\mathscr{K} \to A$. We call such a point a *formal point*, in opposition to the geometric points in $A(\overline{k})$. Since $\mathscr{K}$ is étale, a formal point $\eta \in A(\mathscr{K})$ is given by the data of a $\mathrm{Gal}(\overline{k}/k)$-equivariant morphism (of sets) $K(\overline{k}) \to A(\overline{k})$. We denote by $I_{\mathscr{K}} \in A(\mathscr{K})$ the point coming from the closed immersion $K \to A$ defined by (4.1) which can be seen as a point in $K(\mathscr{K})$. For instance, if $K \setminus \{0_A\}$ is irreducible then $I_{\mathscr{K}}$ restricts to its generic point. Since A is an abelian variety, $A(\mathscr{K})$ is an abelian group. Let $P \in K(\overline{k})$ be a geometric point $P : \mathrm{Spec}(\overline{k}) \to \mathrm{Spec}(\mathscr{K})$. For a formal point $\eta \in A(\mathscr{K})$, we denote by $\eta(P) \in A(\overline{k})$ the geometric point $\eta \circ P : \mathrm{Spec}(\overline{k}) \to \mathrm{Spec}(A)$ obtained by 'specialization'. In the same way, if $x \in \mathscr{K}$ and $P \in K(\overline{k})$, we denote by $x(P)$ the value of x in P.

Let $Q = \prod_{i \in I} R_i$, for $R_i \in k[U]$, be a decomposition of Q in irreducible elements. Via the projective embedding $A \to \mathbb{P}^{Z(n)}$ a formal point $\eta \in A(\mathscr{K})$ can be seen as a projective point $\eta \in \mathbb{P}^{Z(n)}(\mathscr{K})$. Since $\mathscr{K}$ is an étale algebra such a projective point is given by the data of a $(\eta_\nu)_{\nu \in Z(n)} \in \mathscr{K}^{Z(n)}$ such that, for all $i \in I$, at least one of the η_ν is invertible modulo R_i, modulo the action of invertible elements of $\mathscr{K}$ on $\mathscr{K}^{Z(n)}$. The isomorphism $K \xrightarrow{\sim} \mathrm{Spec}\,\mathscr{K}$ shows that the projective coordinates of $\eta \in A(\mathscr{K})$ are given by $(1, \eta_{i_1}, Q_{i_2}(\eta_{i_1}), \ldots, Q_{i_{n^g-1}}(\eta_{i_1}))$ where the $Q_{i_j} \in k[U]$ are defined in § 4. The formal point $I_{\mathscr{K}} \in A(\mathscr{K})$ is such that $(I_{\mathscr{K}})_{i_1} = U$. As for geometric points, we denote by $\widetilde{\eta} \in \widetilde{A}(\mathscr{K})$ an affine lift of $\eta \in A(\mathscr{K})$ and let $(\widetilde{\eta})_i \in \mathscr{K}$ for $i \in Z(n)$ be its corresponding affine coordinates. A point $P \in A(k)$ corresponds to a formal point $\eta_P \in A(\mathscr{K})$ via the constant morphism $Q \in \mathscr{K}(\overline{k}) \mapsto P$. We will often make this identification in the following.

The arithmetic of geometric points recalled in § 2 translates *mutatis mutandis* into arithmetic with formal points. For instance, from the knowledge of $\widetilde{\eta}_1, \widetilde{\eta}_2 \in \widetilde{A}(\mathscr{K})$, and $\widetilde{\eta_1 - \eta_2} \in \widetilde{A}(\mathscr{K})$,

one can compute the differential addition $\widetilde{\eta_1 + \eta_2} \in \widetilde{A}(\mathscr{K})$. This can be proved exactly in the same way as with geometric points using Riemann's equations and we obtain the same formulas. The case $g = 1$ is given, for instance, in [**23**]. We remark that in order to be able to compute the differential addition, we have to find an invertible coordinate $(\widetilde{\eta_1 - \eta_2})_{\nu_0} \in \mathscr{K}$ for $\nu_0 \in Z(n)$. But in fact, there is always at least one such coordinate modulo R_i for every $i \in I$. So we can always compute the differential addition, provided that we work modulo R_i, which is the case if we know the factorization of Q, the polynomial defining $\mathscr{K}$. Actually we do not even need to compute the factorization beforehand because when we try to invert a non-zero element, if it is non-invertible the Euclidean algorithm will give a factor of Q. We remark that when the difference is a formal point with value in K, then, by the hypothesis made in § 4 on the equations, the coordinate $i = 0$ is always invertible, which helps in the computations. In the same way, if $4|n$, one can compute normal addition of generic points. Addition and multiplication operations in $\mathscr{K}$ take $\widetilde{O}(\ell^g)$ operations in k. Computing the inverse of an element of $\mathscr{K}$ can be done in $\widetilde{O}(\ell^g)$ operations in k via the extended Euclidean algorithm. Thus, differential and normal additions of elements of $\widetilde{A}(\mathscr{K})$ take $\widetilde{O}(\ell^g)$ operations in k.

For $P \in K(\overline{k})$, $\eta \in A(\mathscr{K})$ and $\widetilde{\eta} \in \widetilde{A}(\mathscr{K})$ any affine lift of η, we denote by $\widetilde{\eta}(P) \in \widetilde{A}(\overline{k})$ the point with affine coordinates $(\widetilde{\eta})_i(P)$. As two formal points $\widetilde{\eta}, \widetilde{\eta}' \in \widetilde{A}(\mathscr{K})$ are equal if and only if, for all $P \in K(\overline{k})$, $\widetilde{\eta}(P) = \widetilde{\eta}(P)$, this allows us to verify certain properties by specializing a formal point to geometric points. For instance, the result of a chain of differential addition that one can compute from a set $\widetilde{\eta}_1, \ldots, \widetilde{\eta}_m \in \widetilde{A}(\mathscr{K})$ of affine lifts of $\eta_1, \ldots, \eta_m \in A(\mathscr{K})$ does not depend on the order of the operations because, as proved in [**24**, Corollary 3.13], it is true for geometric points. Also if $\eta \in K(\mathscr{K})$ then $\ell\eta = 0_A$.

Let $\eta = P + \eta_K \in A(\mathscr{K})$ with $\eta_K \in K(\mathscr{K})$ and let $\widetilde{\eta} \in \widetilde{A}(\mathscr{K})$ be an affine lift. We say that $\widetilde{\eta}$ is a compatible lift of η (relative to $\widetilde{P}$) if, for all $Q \in K(\overline{k})$, $\widetilde{\eta}(Q) \in \widetilde{A}(\overline{k})$ is a compatible lift of $P + \eta_K(Q)$ relative to $\widetilde{P}$. It is easy to extend Proposition 3.3 to compute compatible lifts of formal points.

PROPOSITION 5.1. *Let $\eta_K \in K(\mathscr{K})$, and let $\widetilde{\eta}_K \in \widetilde{A}(\mathscr{K})$ be any affine lift. Write $\ell = 2\ell' + 1$, and compute $\ell'\widetilde{\eta}_K = \mathrm{ScalarMult}(\ell', \widetilde{\eta}_K, \widetilde{\eta}_K, \widetilde{0}_A, \widetilde{0}_A)$, $(\ell'+1)\widetilde{\eta}_K = \mathrm{ScalarMult}(\ell'+1, \widetilde{\eta}_K, \widetilde{\eta}_K, \widetilde{0}_A, \widetilde{0}_A)$. Let $\lambda \in \mathscr{K}_{\mathbb{C}}$ (where $\mathscr{K}_{\mathbb{C}} = \mathscr{K} \otimes_k \mathbb{C}$) be an invertible element. Then $\lambda \star \widetilde{\eta}_K$ is a potential compatible lift if and only if*

$$((\ell'+1)\widetilde{\eta}_K)_\nu \lambda^\ell - (\ell'\widetilde{\eta}_K)_{-\nu} = 0, \tag{5.1}$$

for $\nu \in Z(n)$.

Likewise, let $\eta = \eta_K + P \in A(\mathscr{K})$ where $\eta_K \in K(\mathscr{K})$ and $P \in A(k)$. Fix affine lifts $\widetilde{P} \in \widetilde{A}(k)$ of P and $\widetilde{\eta}_K \in \widetilde{A}(\mathscr{K})$ of η_K and denote by $\widetilde{\eta} \in \widetilde{A}(\mathscr{K})$ a compatible lift of η. Let $\widetilde{\eta}^0 = \mathrm{ScalarMult}(\ell, \widetilde{\eta}, \lambda \star \widetilde{\eta}_K, \widetilde{P}, \widetilde{0}_A) \in \widetilde{A}(\mathscr{K}(\lambda))$. Then modulo the equations from (5.1), $\widetilde{\eta}^0$ is in $\widetilde{A}(\mathscr{K})$ and $\mu \in \mathscr{K}_{\mathbb{C}}$ is such that $\mu \star \widetilde{\eta}$ is a potential compatible lift (relative to $\widetilde{P}$) if and only if

$$\mu^\ell \widetilde{\eta}^0_\nu - \widetilde{P}_\nu = 0 \tag{5.2}$$

for $\nu \in Z(n)$.

Proof. By equation (3.4) and [**23**, Remark 3], we have that $\lambda \star \widetilde{\eta}$ is a potential compatible lift if and only if $\lambda^{(\ell'+1)^2} \star ((\ell'+1)\widetilde{\eta}) = -\lambda^{\ell'^2} \star (\ell'\widetilde{\eta})$. We thus obtain that if λ is an element of an étale extension of $\mathscr{K}$ which satisfies equation (5.1) then $\lambda \star \widetilde{\eta}$ is a potential compatible lift.

By [**23**, Remark 3], the coordinates of $\widetilde{\eta}^0$ only have factors of the form $c\lambda^{\ell(\ell-1)}$ where $c \in \mathscr{K}$. By looking at equation (5.1), it is thus clear that $\widetilde{\eta}^0$ does not depend on the choice of a compatible lift for η_K. By equation (3.5) and [**23**, Remark 3] again, we have that $\mu \star \widetilde{\eta}$ is

a potential compatible lift if and only if $\mu^\ell \star \widetilde{\eta}^0 = \widetilde{P}$. Thus, if μ is a root of the polynomials from equation (5.2) in an étale extension of $\mathscr{K}$ then $\mu \star \widetilde{\eta}$ is a potential compatible lift. □

We denote by Normalize$(\widetilde{\eta}, \widetilde{P})$ the algorithm which outputs equation (5.2) defining μ such that $\mu \star \widetilde{\eta}$ is a compatible lift (relative to $\widetilde{P}$). It is clear from its description that Normalize applied to a formal point takes $\widetilde{O}(\ell^g)$ operations in k. In practice, given the hypothesis about the kernel made in § 4, it suffices to use equation (5.1) with coordinate $\nu = 0$ to determine λ^ℓ, and it suffices to use equation (5.2) with a coordinate ν such that $P_\nu \neq 0$ to determine μ^ℓ. The corresponding algorithm (with $\nu = 0$) for Normalize is given in Algorithm 1.

Algorithm 1: Algorithm Normalize

input:
- $\eta = \eta_K + P$ where $\eta_K \in K(\mathscr{K})$ and $P \in A(\overline{k})$;
- $\widetilde{P}$ an affine lift of P and $\widetilde{\eta}$ an affine lift of η.

output: An equation $\mu^\ell = c$ for $c \in \mathscr{K}$ so that $\mu \star \widetilde{\eta}$ is a compatible lift with $\widetilde{P}$ when μ satisfy this equation.

1 $\mu_K^{[1]} \leftarrow \text{ScalarMult}(\ell' + 1, \lambda \star \widetilde{\eta}_K, \lambda \star \widetilde{\eta}_K, \widetilde{0}_A, \widetilde{0}_A)$ and
$\mu_K^{[0]} \leftarrow \text{ScalarMult}(\ell', \lambda \star \widetilde{\eta}_K, \lambda \star \widetilde{\eta}_K, \widetilde{0}_A, \widetilde{0}_A)$ where $\ell = 2\ell' + 1$;

2 $\mu^{[0]} \leftarrow \text{ScalarMult}(\ell, \mu \star \widetilde{\eta}, \lambda \star \widetilde{\eta}_K, \widetilde{P}, \widetilde{0}_A)$;

3 **return** $\mu^\ell = \frac{\widetilde{P}_0}{\mu_0^{[0]}} \left(\frac{\mu_{K,0}^{[0]}}{\mu_{K,0}^{[1]}} \right)^{\ell-1}$;

Remark 5.2. Compared to Proposition 5.1, Theorem 3.4 starts with a basis of potential compatible lifts $\widetilde{e}_i$ and derives compatible lifts for the set of all geometric points of the kernel. By contrast, if $\widetilde{\eta}$ is a compatible lift of a formal point $\eta \in A(\mathscr{K})$ and $\widetilde{P}$ an affine lift of $P = \eta(0) \in A(\overline{k})$, then by definition all the $\widetilde{\eta}(Q), Q \in K(\overline{k})$ are compatible with $\widetilde{P}$, but, in general, they will not be globally compatible with each other.

One can think of the formal point approach that we have presented as doing formal computations with geometric points. We conclude this section by explaining that it is actually possible to follow exactly the same procedure as that of the algorithm of [**11**] to compute isogenies with formal points. Let k' be the compositum of the fields of definition of elements of $K(\overline{k})$. The Galois group $\text{Gal}(k'/k)$ acts on $K(\overline{k})$. As the group law of A is defined over k, this action is linear and $\text{Gal}(k'/k)$ acts on the elements of $A(\mathscr{K})$. Suppose that $K \setminus \{0_A\}$ is irreducible and that $\text{Gal}(k'/k)$ is cyclic generated by g. Let $\eta_1 = \text{Id}_{\mathscr{K}} \in A(\mathscr{K})$ and let $\eta_i = g^i \eta_1$ for $i = 2, \ldots, g$. Then, as by hypothesis g generates $\text{Gal}(k'/k)$, $\eta_1, \ldots, \eta_g$ are linearly independent formal points of K. One can compute $\eta_i + \eta_j$ with normal additions, then compute potential compatible lifts of all the η_i and $\eta_i + \eta_j$ and use chains of differential additions to obtain potential compatible lifts of all the points of the kernel. Thus, it is possible to evaluate the right-hand side of (3.2) with formal points: the result of the computations in $\mathscr{K}$ will actually lie in k. We remark that the algorithm that we have just sketched is just a fancy way to compute with the splitting field defined by Q. This naive approach does not improve the complexity of the algorithm of [**11**] even in the favorable case that we have considered in this paragraph.

6. *An algorithmic improvement*

Returning to the context of § 3, let $(A, \mathscr{L}_0)$ be a principally polarized abelian variety given by $\Omega \in \mathbb{H}_g$. We have seen that the general isogeny computation problem boils down to the case

where $K = (1/\ell)\mathbb{Z}^g/\Lambda_\Omega$ and

$$\begin{array}{ccccc} f : A \simeq \mathbb{C}^g/\Lambda_\Omega & \to & B \simeq \mathbb{C}^g/\Lambda_{\ell\Omega} \\ z & \mapsto & \ell z. \end{array} \tag{6.1}$$

We explain how to evaluate the expression of Proposition 3.1 with formal points and derive an efficient algorithm. Actually, by looking at the right-hand side term of equation (3.2), we need to deal in a 'formal' way with r-tuples of the form $X_i + t_i$. This motivates the following definition.

DEFINITION 6.1. For t a positive integer, let $\mathscr{B} = \mathscr{K}^{\otimes t}$ so that $K^t \xrightarrow{\sim} \operatorname{Spec} \mathscr{B}$. We define a *formal tuple* as a point $\eta \in A(\mathscr{B})$.

For $i = 1, \ldots, t$, let $\mu_i : K^t \to K$ be the ith projection. Note that μ_i induces the natural injection of coordinate algebras given by $x \mapsto 1 \otimes \ldots \otimes x \otimes \ldots \otimes 1$ where x is in the ith position.

For $i = 1, \ldots, t$, we denote $I^{(i)}_{\mathscr{K}} = I_{\mathscr{K}} \circ \mu_i \in A(\mathscr{B})$ so that $\sum_{i=1}^t I^{(i)}_{\mathscr{K}}$ (the sum is the group law of $A(\mathscr{B})$) is the point coming from the canonical morphism associated to the addition: $A^t \to A$.

Since $\mathscr{B}$ is also an étale algebra, everything said in § 5 about the arithmetic of formal points (differential additions, Normalize, ...) also applies to formal tuples. In particular, $\eta \in A(\mathscr{B})$ is represented by its coordinates $\eta_\nu \in \mathscr{B}$ for $\nu \in Z(n)$, addition and multiplication operations in the algebra $\mathscr{B}$ take $\widetilde{O}(\ell^{tg})$ operations in k and computing the inverse of an element of $\mathscr{B}$ can be done in $\widetilde{O}(\ell^{tg})$ operations in k via a recursive use of the extended Euclidean algorithm.

REMARK 6.2. A point $\eta \in A(\mathscr{B})$ that is also an algebraic group morphism is necessarily of the form $\eta^{(1)} \circ \mu_1 + \ldots + \eta^{(t)} \circ \mu_t$ for a tuple $(\eta^{(1)}, \ldots, \eta^{(t)})$ of points in $A(\mathscr{K})$. The formal point $\eta^{(i)}$ can be recovered from the formal tuple η via $\eta^{(i)} = \mu'_i \circ \eta$ where the μ'_i correspond to the canonical inclusions of K into K^t. In practice we will be working with formal tuples coming from linear combinations $P + \sum \lambda_i I^{(i)}_{\mathscr{K}}$ where $P \in A(k)$.

Let M be an $r \times r$ matrix with integer coefficients such that ${}^tMM = \ell Id$. Write $\ell = \ell_1\ell_2$ where ℓ_1 is the biggest square factor of ℓ. If $\ell = \ell_1$, we can take $M = (\sqrt{\ell_1})$ and fix $r = 1$. If $\ell_2 \neq 1$ and all prime factors of ℓ_2 are congruent to 1 mod 4, then there exists $a, b \in \mathbb{N}^*$ such that $\ell_2 = a^2 + b^2$. thus we can take $M = \sqrt{\ell_1} M_0$, with $M_0 = \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ and fix $r = 2$. Finally, if there is a prime factor of ℓ_2 congruent to 3 mod 4, we can write $\ell_2 = a^2 + b^2 + c^2 + d^2$ for $a, b, c, d \in \mathbb{N}$ such that $a^2 + b^2 \not\equiv 0 \mod \ell_2$, take for M_0 the matrix of multiplication by $a + ib + cj + dk$ in the quaternion algebra over $\mathbb{R}$, $M = \sqrt{\ell_1} M_0$, and fix $r = 4$. We consider the isogeny of algebraic groups $F : K^r \to K^r$ acting componentwise by the matrix M. Denote by $\ker F$ the kernel subvariety of F. If $\ell = \ell_1$, $\ker F$ is isomorphic to $\sqrt{\ell_1} K$, an isomorphism being given on geometric points by the identity. If $\ell_2 \neq 1$ is a sum of two (respectively, four) squares, $\ker F$ is isomorphic to $L = \sqrt{\ell_1} K$ (respectively, $L = \sqrt{\ell_1} K^2$), an isomorphism $L \to \ker F$ being given on geometric points by $x \mapsto (x, \beta_0 x)$ with $\beta_0 = -b/a \mod \ell$ (respectively, $(x_1, x_2) \mapsto (x_1, x_2, \alpha x_1 + \beta x_2, \gamma x_1 + \delta x_2)$ with $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)^{-1} \left(\begin{smallmatrix} c & d \\ d & -c \end{smallmatrix}\right) = (1/(a^2 + b^2)) \left(\begin{smallmatrix} ac - db & ad + bc \\ ad + bc & bd - ac \end{smallmatrix}\right)$; note that $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ is invertible modulo ℓ since $a^2 + b^2 \not\equiv 0 \mod \ell$). With this notation, we have the following proposition.

PROPOSITION 6.3. *Let $P \in A(k)$ and let $z_P \in \mathbb{C}^g$ be such that $\rho_n(z_P) = P$. Fix $k \in Z(n)$ and let $j = (k, \ldots, 0)M^{-1} \in Z(n)^r$. Let N be the cardinality of the kernel of the group morphism $K^t(\overline{k}) \to \sqrt{\ell_1} K^t(\overline{k}), x \mapsto \sqrt{\ell_1} x$. If $\ell_2 = 1$ then set $t = 1$; otherwise, set $t = r/2$ and*

let $\mathscr{B} = \mathscr{K}^{\otimes t}$. *Moreover:*

- *If* $\ell_2 = 1$, *let* $\eta^{(1)} = \sqrt{\ell_1} I_{\mathscr{K}} + \zeta P$ *for* $\zeta \in \mathbb{Z}$. *Let* $\widetilde{\eta}^{(1)}$ *be any affine lift of* $\eta^{(1)}$. *Let* $\widetilde{\eta}^{(\mu)} = \mu \star \widetilde{\eta}^{(1)}$ *where* μ *is a formal parameter. Let* $X = \zeta z_P \in \mathbb{C}^g$ *and* $Y = XM$. *Set* $R_\star = \widetilde{\eta}^{(\mu)}_{j_1} \in \mathscr{K}(\mu)$, *and let* R *be the reduction of* $R_\star$ *modulo the equations in* $\mathscr{K}$ *coming from* Normalize$(\widetilde{\eta}^{(1)}, \zeta\widetilde{P})$.
- *If* $\ell_2 \neq 1$ *is a sum of two squares, let* $\eta^{(1)} = \sqrt{\ell_1} I_{\mathscr{K}} + \zeta P$ *for* $\zeta \in \mathbb{Z}$. *Let* $\widetilde{\eta}^{(1)}$ *be any affine lift of* $\eta^{(1)}$. *Let* $\widetilde{\eta}^{(\mu)} = \mu \star \widetilde{\eta}^{(1)}$ *where* μ *is a formal parameter,* $\widetilde{\eta}^{[1]} = \beta_0 \widetilde{\eta}^{(\mu)}$. *Let* $X = (\zeta z_P, \beta_0 \zeta z_P) \in (\mathbb{C}^g)^2$ *and* $Y = XM$. *Set* $R_\star = \widetilde{\eta}^{(\mu)}_{j_1} \widetilde{\eta}^{[1]}_{j_2} \in \mathscr{K}(\mu)$, *and let* R *be the reduction of* $R_\star$ *modulo the equations in* $\mathscr{K}$ *coming from* Normalize$(\widetilde{\eta}^{(1)}, \zeta\widetilde{P})$.
- *If* ℓ_2 *is a sum of four squares, let* $\eta^{(i)} = \sqrt{\ell_1} I^{(i)}_{\mathscr{K}} + \zeta_i P$ *with* $\zeta_i \in \mathbb{Z}$ *for* $i = 1, 2$ *and fix corresponding affine lifts* $\widetilde{\eta}^{(i)}$. *Fix also an affine lift* $\widetilde{\eta}^{(12)}$ *of* $\eta^{(1)} + \eta^{(2)}$. *Let* $\widetilde{\eta}^{(\mu_1)} = \mu_1 \star \widetilde{\eta}^{(1)}$, $\widetilde{\eta}^{(\mu_2)} = \mu_2 \star \widetilde{\eta}^{(2)}$ *and* $\widetilde{\eta}^{(\mu_{12})} = \mu_{12} \star \widetilde{\eta}^{(12)}$ *where* μ_1, μ_2, μ_{12} *are formal parameters. Let* $\widetilde{\eta}^{[1]} = \alpha\widetilde{\eta}^{(\mu_1)} + \beta\widetilde{\eta}^{(\mu_2)}$ *and* $\widetilde{\eta}^{[2]} = \gamma\widetilde{\eta}^{(\mu_1)} + \delta\widetilde{\eta}^{(\mu_2)}$ *in* $\widetilde{A}(\mathscr{B}(\mu_1, \mu_2, \mu_{12}))$ *(bootstrapping from* $\widetilde{\eta}^{(12)}$ *using differential additions). Let* $X = (\zeta_1 z_P, \zeta_2 z_P, (\alpha\zeta_1 + \beta\zeta_2) z_P, (\gamma\zeta_1 + \delta\zeta_2) z_P) \in (\mathbb{C}^g)^4$ *and* $Y = XM$. *Set*

$$R_\star = \widetilde{\eta}^{(\mu_1)}_{j_1} \widetilde{\eta}^{(\mu_2)}_{j_2} \widetilde{\eta}^{[1]}_{j_3} \widetilde{\eta}^{[2]}_{j_4} \in \mathscr{B}(\mu_1, \mu_2, \mu_{12}).$$

  Let R *be the reduction of* $R_\star$ *modulo the equations in* $\mathscr{B}$ *coming from* Normalize$(\widetilde{\eta}^{(1)}, \zeta_1\widetilde{P})$, Normalize$(\widetilde{\eta}^{(2)}, \zeta_2\widetilde{P})$ *and* Normalize$(\widetilde{\eta}^{(12)}, (\zeta_1 + \zeta_2)\widetilde{P})$.

We have that $R \in \mathscr{B}$ *and*

$$\theta^B_k(Y_1) \dots \theta^B_0(Y_r) = \frac{1}{N} \sum_{T \in K^t(\overline{k})} R(T). \tag{6.2}$$

Proof. First, we prove the case where $\ell_2 \neq 1$ is a sum of two squares. In order to prove that R is indeed in $\mathscr{K}$, because of Proposition 5.1, it suffices to show that the rational function $R_\star$ does not change when we act on $\widetilde{\eta}^{(1)}$ by μ in an étale extension of $\mathscr{K}$ that satisfies the equations coming from Normalize$(\widetilde{\eta}^{(1)}, \widetilde{P})$.

For this let $\widetilde{\eta}_\theta$ in $\widetilde{A}(\mathscr{K}_{\mathbb{C}}(\mu))$ be such that $\widetilde{\eta}^{(\mu)} = \mu' \star \widetilde{\eta}_\theta$ where $\mu' \in \mathscr{K}_{\mathbb{C}}$ is a ℓth root of unity because of equation (5.2). Let $\widetilde{\eta}^{[1]}_\theta = \text{ScalarMult}(\beta_0, \widetilde{\eta}_\theta, \widetilde{\eta}_\theta, \widetilde{0}_A, \widetilde{0}_A)$. By [**23**, Remark 3], we have $\widetilde{\eta}^{[1]} = {\mu'}^{\beta_0^2} \star \widetilde{\eta}^{[1]}_\theta$. Thus, we have $R_* = \widetilde{\eta}^{(\mu)}_{j_1} \widetilde{\eta}^{[1]}_{j_2} = \mu' \widetilde{\eta}_\theta(T) {\mu'}^{\beta_0^2} \widetilde{\eta}^{[1]}_\theta$ with $\beta_0^2 \equiv -1 \mod \ell$. We deduce that $R \in \mathscr{K}$ since it is left invariant by the action of μ'.

Now let $\widetilde{\eta}_\theta$ in $\widetilde{A}(\mathscr{K}_{\mathbb{C}})$ be such that $\{\widetilde{\eta}_\theta(Q) \mid Q \in K(\overline{k})\}$ is a system of compatible lifts relative to $\widetilde{P}$. Using Theorem 3.4, we can suppose that $\widetilde{\eta}^{(\mu)} = \widetilde{\eta}_\theta$ modulo the equations coming from Normalize$(\widetilde{\eta}^{(1)}, \zeta\widetilde{P})$. Then we have $R(T) = \widetilde{\eta}_\theta(T)\widetilde{\eta}_\theta(\beta_0 T) = \theta^A_{j_1}(X_1 + z_T)\theta^A_{j_2}(X_2 + \beta_0 z_T)$ for $z_T \in \mathbb{C}^g$ such that $\rho_n(z_T) = T$. Thus the relation (6.2) is just a consequence of Proposition 3.1. The $1/N$ in front of the right-hand side of (6.2) comes from the fact that the parametrization of $(\ker F)(\overline{k})$ by $K(\overline{k})$ we have used is an epimorphism the kernel of which has cardinality N.

Now suppose that ℓ_2 is a sum of four squares. Fix a system of global compatible lifts $\{\alpha P + Q | \alpha \in \{0, \dots, \ell - 1\}, Q \in K(\overline{k})\}$ relative to $\widetilde{P}$. For $i = 1, 2$, let $\widetilde{\eta}^{(i)}_\theta$ be the formal point such that $\widetilde{\eta}^{(i)}_\theta(Q_1, Q_2)$ is the corresponding compatible lift above $\zeta_i P + Q_i$, and define $\theta^{(12)}_\theta$ so that $\widetilde{\eta}^{(12)}_\theta(Q_1, Q_2)$ is the corresponding compatible lift above $(\zeta_1 + \zeta_2)P + Q_1 + Q_2$.

We proceed along the same lines as for the case above. Let μ'_1, μ'_2 and μ'_{12} be roots in $\mathscr{K}_{\mathbb{C}}$ of the equations (E) given by Normalize$(\widetilde{\eta}^{(1)}, \zeta_1\widetilde{P})$, Normalize$(\widetilde{\eta}^{(2)}, \zeta_2\widetilde{P})$ and Normalize$(\widetilde{\eta}^{(12)}, (\zeta_1 + \zeta_2)\widetilde{P})$. By Proposition 5.1, $\mu'_1 \star \widetilde{\eta}^{(1)}, \mu'_2 \star \widetilde{\eta}^{(2)}$ and $\mu'_{12} \star \widetilde{\eta}^{(12)}$ differ from $\widetilde{\eta}^{(1)}_\theta, \widetilde{\eta}^{(2)}_\theta$ and $\widetilde{\eta}^{(12)}_\theta$ by ℓth roots of unity μ_1, μ_2 and μ_{12} respectively.

Let $\widetilde{\eta}^{[1]}_\theta = \alpha\widetilde{\eta}^{(1)}_\theta + \beta\widetilde{\eta}^{(2)}_\theta$ and $\widetilde{\eta}^{[2]}_\theta = \gamma\widetilde{\eta}^{(1)}_\theta + \delta\widetilde{\eta}^{(2)}_\theta$. We can use [**23**, Remark 3] repeatedly to obtain that $\alpha\widetilde{\eta}^{(\mu_1)} + \widetilde{\eta}^{(\mu_2)} = ((\mu_{12}^\alpha \mu_1^{\alpha(\alpha-1)})/(\mu_2^{\alpha-1}))(\alpha\widetilde{\eta}^{(1)}_\theta + \widetilde{\eta}^{(2)}_\theta)$, $\alpha\widetilde{\eta}^{(\mu_1)} = \mu_1^{\alpha^2}(\alpha\widetilde{\eta}^{(1)}_\theta)$ and,

finally, $\widetilde{\eta}^{[1]} = \mu_{12}^{\alpha\beta}\mu_1^{\alpha^2-\alpha\beta}\mu_2^{\beta^2-\alpha\beta}\widetilde{\eta}_\theta^{[1]}$. We have in the same way $\widetilde{\eta}^{[2]} = \mu_{12}^{\gamma\delta}\mu_1^{\gamma^2-\gamma\delta}\mu_2^{\delta^2-\gamma\delta}\widetilde{\eta}_\theta^{[2]}$. Thus, for $T = (T_1, T_1) \in K^2(\overline{k})$, we have $R(T) = \widetilde{\eta}_{j_1}^{(1)}(T)\widetilde{\eta}_{j_2}^{(2)}(T)\widetilde{\eta}_{j_3}^{0}(T)\widetilde{\eta}_{j_4}^{1}(T) = \Delta\widetilde{\eta}_{\theta,j_1}^{(1)}(T)$ $\widetilde{\eta}_{\theta,j_2}^{(2)}(T)\widetilde{\eta}_{\theta,j_3}^{0}(T)\widetilde{\eta}_{\theta,j_4}^{1}(T)$ where

$$\Delta = \mu_{12}^{\alpha\beta+\gamma\delta}\mu_1^{1+\alpha^2+\gamma^2-\alpha\beta-\gamma\delta}\mu_2^{1+\beta^2+\delta^2-\alpha\beta-\gamma\delta}.$$

But an easy computation shows that $\alpha\beta+\gamma\delta = 0$ and $\alpha^2+\gamma^2 = \beta^2+\delta^2 = (b^2+c^2)/(a^2+b^2)$ so that $\Delta = 1$. Finally, we obtain that $R(T) = \theta_{j_1}(X_1 + z_{T_1})\theta_{j_2}(X_2 + z_{T_2})\theta_{j_3}(X_3 + \alpha z_{T_1} + \beta z_{T_1})\theta_{j_4}(X_4 + \gamma z_{T_1} + \delta z_{T_2})$ for $z_{T_i} \in \mathbb{C}^g$ such that $\rho_n(z_{T_i}) = T_i$ for $i = 1, 2$ and relation (6.2) is again a consequence of Proposition 3.1.

The simpler case $\ell_2 = 1$ can be treated in a similar manner as the other cases. We leave it as an exercise for the reader. □

Remark 6.4. The fact that the ℓth roots of unity appearing in the evaluation of the right-hand side of formula (3.1) of Proposition 3.1 cancel out is no miracle. It can be explained with a more conceptual point of view: these ℓth roots of unity correspond to choices of a level ℓn-theta structure for B compatible with the level n-theta structure of A via the contragredient isogeny of $f : A \to B$ and we can interpret the change of level formula (3.2) as 'forgetting' the ℓ-torsion part of these theta structures to recover a level n theta structure for B (see, for instance, [**24**]).

The stronger fact that they also cancel out when only considering the terms in the sum comes from the fact that these terms already forget the part of the ℓ-structure whose automorphisms act by the $\star$ operator [**14**, Proposition 18].

In order to turn Proposition 6.3 into an algorithm, it remains to explain how to compute efficiently the right-hand side of (6.2). This is done by the following lemma.

Lemma 6.5. *Let $W \in \mathscr{K} = k[U]/(Q)$, let $(T, S) \in k[U]$ be respectively the quotient and remainder of the Euclidean division of UWQ' by Q (where Q' is the first derivative of Q). We have*

$$\sum_{P \in K(\overline{k})} W(P) = T(0). \tag{6.3}$$

Proof. Let $\mathscr{R}$ be the set of roots of Q in $\overline{k}$. We want to prove that $\sum_{a\in\mathscr{R}} W(a) = T(0)$. We have

$$\frac{UWQ'}{Q} = \sum_{a\in\mathscr{R}} \frac{UW}{U-a}. \tag{6.4}$$

For $a \in \mathscr{R}$ let T_a be the quotient of the Euclidean division of UW by $(U-a)$ so that we have $UW = T_a(U-a) + aW(a)$. Putting this in (6.4), we obtain that $UWQ'/Q = \sum_{a\in\mathscr{R}}(T_a + aW(a)/(U-a))$. As $Q\sum_{a\in\mathscr{R}} aW(a)/(U-a)$ is an element of $k[U]$ of degree less than $\deg(Q)$, we deduce that $S = Q\sum_{a\in\mathscr{R}} aW(a)/(U-a)$ and $T = \sum_{a\in\mathscr{R}} T_a$. Moreover, $T(0) = \sum_{a\in\mathscr{R}} T_a(0)$ but $-aT_a(0) + aW(a) = 0$ so that $T_a(0) = W(a)$ (it is easy to check that this also holds if $a = 0$) and we are done. (Over $\mathbb{C}$, this lemma is just an easy application of the residue theorem.) □

As R defined in Proposition 6.3 is an element of $\mathscr{K}^{\otimes r/2}$ if $\ell_2 \neq 1$ and an element of $\mathscr{K}$ otherwise, Lemma 6.5 shows that, in the case where ℓ is a sum of two squares, the evaluation of the right-hand side of (6.2) can be done with an Euclidean division of an element of $k[U]$ of degree bounded by ℓ^g at the expense of $\widetilde{O}(\ell^g)$ operations in k. If ℓ is a sum of four squares, R is an element of $\mathscr{K}^{\otimes 2}$ and we can resort twice to Lemma 6.5, to carry out the evaluation

of (6.2). The dominant step is an Euclidean division of an element of $\mathscr{K}[U]$ of degree bounded by ℓ^g which can be done in $\widetilde{O}(\ell^{2g})$ operations in k. We call Evaluate an algorithm which takes as input $R \in \mathscr{K}^{\otimes r/2}$ and returns $\sum_{T \in K^{r/2}(\overline{k})} R(T)$.

If we apply Proposition 6.3, with $P = 0$, we obtain an algorithm to compute $\theta^B_k(0)\dots\theta^B_0(0)$ for any $k \in Z(n)$ that gives the projective theta null point of B associated to $\ell\Omega$. Let $P \in A(k)$ and let $z_P \in \mathbb{C}^g$ be such that $\rho_n(z_P) = P$:

- if ℓ is a square, Proposition 6.3 with $\zeta = \sqrt{\ell}$ gives an expression for $\theta^B_k(\ell z_P)\theta^B_0(0)$ for $k \in Z(n)$;
- if $\ell_2 = a^2 + b^2$, Proposition 6.3 with $\zeta = \sqrt{\ell_1}a$ gives an expression for $\theta^B_k(\ell z_P)\theta^B_0(0)$ for $k \in Z(n)$;
- if $\ell_2 = a^2+b^2+c^2+d^2$, Proposition 6.3 with $\zeta_1 = \sqrt{\ell_1}a$ and $\zeta_2 = \sqrt{\ell_1}b$ gives an expression for $\theta^B_k(\ell z_P)\theta^B_0(0)^3$ for $k \in Z(n)$.

In all cases, we obtain the projective coordinates for $f(P)$ and we have proved Theorem 1.1. Algorithms 2 and 3 recapitulate the isogeny computation algorithms we have described (we leave to the reader the easy adaption in the case where ℓ is a square). To give more details, in Algorithm 2 the line $\widetilde{\eta}^{[1]} \leftarrow \beta_0\widetilde{\eta}^{(\mu)}$ is simply computed as ScalarMult$(\beta_0, \widetilde{\eta}^{(\mu)}, \widetilde{\eta}^{(\mu)}, \widetilde{0}_A, \widetilde{0}_A)$. Likewise, in Algorithm 3, the line $\widetilde{\eta}^{[1]} \leftarrow \alpha\widetilde{\eta}^{(\mu_1)} + \beta\widetilde{\eta}^{(\mu_2)}$ is computed as $\alpha\widetilde{\eta}^{(\mu_1)} + \widetilde{\eta}^{(\mu_2)} \leftarrow$ ScalarMult$(\alpha, \widetilde{\eta}^{(12)}, \widetilde{\eta}^{(\mu_1)}, \widetilde{\eta}^{(\mu_2)}, \widetilde{0}_A)$, $\widetilde{\eta}^{[1]} \leftarrow$ ScalarMult$(\beta, \alpha\widetilde{\eta}^{(\mu_1)} + \widetilde{\eta}^{(\mu_2)}, \widetilde{\eta}^{(\mu_2)}, \alpha\widetilde{\eta}^{(\mu_1)}, \widetilde{0}_A)$ and similarly for $\widetilde{\eta}^{[2]}$.

Algorithm 2: Algorithm GenericIsogeny for ℓ a sum of two squares

input:
- $\widetilde{0}_A$ the level n theta null point of $(A, \mathscr{L}_0)$ associated to $\Omega \in \mathbb{H}$;
- $\ell \in \mathbb{N}$ such that $\ell = \ell_1\ell_2$ where ℓ_1 is the biggest square factor of ℓ and a decomposition $\ell_2 = a^2 + b^2 \neq 1$;
- $Q \in k[U]$ such that $\deg(Q) = \ell^g$ describing K (see § 5);
- $P \in A(\overline{k})$ given its projective coordinates;
- $k \in Z(n)$.

output: $(f(P))_k$ the kth projective coordinates associated to the level n projective embedding of B provided by $\ell\Omega$.

1 $\eta \leftarrow$ NormalAdd$(\sqrt{\ell_1}I_{\mathscr{K}}, \sqrt{\ell_1}aP)$ where $\sqrt{\ell_1}I_{\mathscr{K}}$ and $\sqrt{\ell_1}aP$ are computed with ScalarMult;

2 $\widetilde{\eta}^{(\mu)} \leftarrow \mu \star \widetilde{\eta}$ where μ is a formal parameter;

3 $\widetilde{\eta}^{[1]} \leftarrow \beta_0\widetilde{\eta}^{(\mu)}$ where $\beta_0 = -b/a \mod \ell$;

4 $R \leftarrow \widetilde{\eta}^{(\mu)}_{j_1}\widetilde{\eta}^{[1]}_{j_2} \mod$ Normalize$(\widetilde{\eta}, \sqrt{\ell_1}a\widetilde{P})$ where $j = (k, \dots, 0)M^{-1} \in Z(n)^r$;

5 **return** Evaluate(R);

We note that in Algorithm 3 we need three calls to Normalize, each costing two scalar multiplications by ℓ. We can improve this as follows. First, compute $\eta^{(1)}_0 = I^{(1)}_{\mathscr{K}} + P$ and use Normalize to normalize an affine lift $\widetilde{\eta}^{(1)}_0$ up to a factor μ_1. From this data it is easy to recover a compatible affine lift $\widetilde{\eta}^{(2)}_0$ of $I^{(2)}_{\mathscr{K}} + P$ up to a factor μ_2. Using differential additions, one can then recover the compatible lifts $\widetilde{\eta}^{(1)}$, $\widetilde{\eta}^{(2)}$ of Proposition 6.3. Likewise, one can normalize $I^{(1)}_{\mathscr{K}} + I^{(2)}_{\mathscr{K}}$ up to a factor λ_{12} by using only equation (5.1). One can compute $\widetilde{\eta}^{(12)}$ using differential additions from a compatible affine lift of $P + I^{(1)}_{\mathscr{K}} + I^{(2)}_{\mathscr{K}}$. But the latter point can be computed as a three-way addition [**25**, § 3.6] between the corresponding lifts above of $P + I^{(1)}_{\mathscr{K}}, P + I^{(2)}_{\mathscr{K}}, I^{(1)}_{\mathscr{K}} + I^{(2)}_{\mathscr{K}}$. This method requires only three scalar multiplications by ℓ rather than six to normalize the points.

Algorithm 3: Algorithm GenericIsogeny for ℓ a sum of four squares

input:
- Same as in Algorithm 3 except that we have a decomposition $\ell_2 = a^2 + b^2 + c^2 + d^2$;

output: $(f(P))_k$ the kth projective coordinates associated to the level n projective embedding of B provided by $\ell\Omega$.

1 $\eta^{(i)} \leftarrow \text{NormalAdd}(\sqrt{\ell_1} I_{\mathscr{K}}^{(i)}, \zeta_i P))$ where $\zeta_1 = \sqrt{\ell_1}a$, $\zeta_2 = \sqrt{\ell_1}b$ for $i = 1, 2$ and $\sqrt{\ell_1} I_{\mathscr{K}}^{(i)}$ and $\zeta_i P$ are computed with ScalarMult;

2 $\eta^{(12)} \leftarrow \text{NormalAdd}(\eta^{(1)} + \eta^{(2)})$;

3 $\widetilde{\eta}^{(\mu_1)} \leftarrow \mu_1 \star \widetilde{\eta}^{(1)}$, $\widetilde{\eta}^{(\mu_2)} \leftarrow \mu_2 \star \widetilde{\eta}^{(2)}$, $\widetilde{\eta}^{(\mu_{12})} \leftarrow \mu_{12} \star \widetilde{\eta}^{(12)}$ where μ_1, μ_2, μ_{12} are formal parameters;

4 $(E) \leftarrow \text{Normalize}(\widetilde{\eta}_1, \zeta_1 \widetilde{P}) \cup \text{Normalize}(\widetilde{\eta}_2, \zeta_2 \widetilde{P}) \cup \text{Normalize}(\widetilde{\eta}_{12}, (\zeta_1 + \zeta_2)\widetilde{P})$;

5 $\widetilde{\eta}^{[1]} \leftarrow \alpha \widetilde{\eta}^{(\mu_1)} + \beta \widetilde{\eta}^{(\mu_2)}$, $\widetilde{\eta}^{[2]} \leftarrow \gamma \widetilde{\eta}^{(\mu_1)} + \delta \widetilde{\eta}^{(\mu_2)}$ where $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)^{-1} \left(\begin{smallmatrix} c & d \\ d & -c \end{smallmatrix}\right)$;

6 $R \leftarrow \widetilde{\eta}_{j_1}^{(\mu_1)} \widetilde{\eta}_{j_2}^{(\mu_2)} \widetilde{\eta}_{j_3}^{[1]} \widetilde{\eta}_{j_4}^{[2]}$ modulo (E) where $j = (k, \ldots, 0) M^{-1} \in Z(n)^r$;

7 **return** Evaluate(R);

Throughout this paper we have supposed that $4|n$ so that we can compute normal additions. But actually one can work with level $n = 2$ exactly as in [**11**, § 4.4]. The only difficulty is the case where ℓ is a sum of four squares where we need to compute a point of the form $\eta^{(1)} + \eta^{(2)}$ in Proposition 6.3. Here, we replace the normal addition of the two formal points $\eta^{(1)}$ and $\eta^{(2)}$ by any formal point η such that $\eta(Q) \in \{\eta^{(1)}(Q) + \eta^{(2)}(Q), \eta^{(1)}(Q) - \eta^{(2)}(Q)\}$. Computing such an η requires taking a certain square root in $\mathscr{K}$ as in [**25**, § 3.3] (this square root may have more than two solutions since $\mathscr{K}$ may not be a field). Also $\mathscr{K}$ is no longer an étale algebra because we identify P with $-P$ so the points in $K \setminus \{0_A\}$ have multiplicity 2, but we can instead work directly on $(K \setminus \{0_A\})/\pm 1)$ and gain a factor of 2 in time complexity. See § 7 for an example.

We conclude this section by comparing the algorithm presented in this paper, with the algorithm of [**11**]. In the latter algorithm, all the affine lifts of points of $K(\overline{k})$ are globally compatible in the sense that they are deduced by the way of differential additions from the knowledge of a minimal set of compatible good lifts as in Theorem 3.4. This property is not true if we specialize the lifts of the formal points of Proposition 6.3 to geometric points of K. For instance, in the case $\ell \equiv 1 \mod 4$, ℓ prime, for a fixed $Q \in K(\overline{k})$ the lifts $\widetilde{\eta}^{(\mu)}(Q), \widetilde{\eta}^{[1]}(Q) \in \widetilde{K}(\overline{k})$ (modulo the equations coming from Normalize) of $\zeta P + Q$ and $\beta_0(\zeta P + Q)$ are locally compatible with $\widetilde{P}$, but they may not be globally compatible over all $Q \in K(\overline{k})$. But as seen in the proof of Proposition 6.3, in the evaluation of the right-hand side of (3.2) this local compatibility between the elements appearing in the sum is enough. The authors of [**11**] did not use the local compatibility, because it is actually faster to compute potential compatible lifts for a basis of $K(\overline{k})$ and use differential addition to get the other compatible points than it is to normalize locally for each term in the sum. This shows the usefulness of working with formal points since we can normalize everything once and for all.

7. *Example*

We give a simple example to illustrate the algorithm in the case where the dimension $g = 1$, the base field $k = \mathbb{F}_{1009}$ and the level $n = 2$. Let $\widetilde{0}_A \in \mathbb{A}^{\mathbb{Z}(2)}$ be the level 2 (affine) theta null point with coordinates $(971, 94)$. This theta null point corresponds to the elliptic curve A with Weierstrass equation $y^2 = x^3 + 762x^2 + 246x$. This elliptic curve has a unique subgroup K defined over k in its 5-torsion. If (U_0, U_1) are the theta coordinates of level 2, a system of

equations for this kernel is given by $U_0 = 1$ and $R(U_1) = 0$ where $R(U_1) = U_1^5 + 751U_1^4 + 546U_1^3 + 447U_1^2 + 660U_1 + 339$. We explain how to compute the level 2 theta null point of $B = A/K$.

The polynomial R factorizes as $R(U_1) = (U_1+268)Q(U_1)^2$ where $Q(U_1) = U_1^2+746U_1+353$. The linear term corresponds to the U_1 coordinate of the theta null point of A, while the fact that Q has multiplicity 2 comes from the fact that we are working on the Kummer variety here associated to A (see § 2).

We consider the algebra $\mathscr{K} = k[U]/(Q)$, and we look at the formal point $\eta = (1 : U)$. Let $\widetilde{\eta} = (\lambda, \lambda U)$ be a potential compatible lift. An easy computation shows that $2\widetilde{\eta} = \lambda^4(980U + 906, 103U + 7)$ and $3\widetilde{\eta} = \lambda^9(861U + 437, 572U + 129)$. We thus find that $\lambda^5 = 126U + 129 = (980U + 906)/(861U + 437) = (103U + 7)/(572U + 129)$.

Now from equation (3.2), we have (up to a common factor) that

$$\begin{aligned}\theta_{i_1}^B(0)\theta_{i_2}^B(0) &= \sum_{\substack{t_1,t_2\in K\\ t_1+2t_2=0\\ -2t_1+t_2=0}} \theta_{i_1}^A(t_1)\theta_{i_2}^A(t_2) = \sum_{t\in K} \theta_{i_1}^A(t)\theta_{i_2}^A(2t)\\ &= \theta_{i_1}^A(0)\theta_{i_2}^A(0) + \sum_{t\in K\setminus\{0\}} \theta_{i_1}^A(t)\theta_{i_2}^A(2t).\end{aligned}$$

If we let $W = \theta_{i_1}(\widetilde{\eta})\theta_{i_2}(2\widetilde{\eta})$, we have that $\theta_{i_1}^B(0)\theta_{i_2}^B(0) = \theta_{i_1}^A(0)\theta_{i_2}^A(0) + 2T(0)$ where T is the polynomial defined in Lemma 6.5.

If $i_1 = i_2 = 0$ then $W = \lambda^5(980u + 906)$, $T = 380$ and $\theta_{i_1}^B(0)\theta_{i_2}^B(0) = 186$. If $i_1 = 0, i_2 = 1$ then $W = \lambda^5(103u + 7)$, $T = 629U + 529$ and $\theta_{i_1}^B(0)\theta_{i_2}^B(0) = 513$.

The level 2 theta null point $(186 : 513)$ corresponds to the elliptic B given by the Weierstrass equation $y^2 = x^3 + 133x^2 + 875x$. In this case we could have computed the isogeny by an application of Vélu's formulas, yielding a curve isomorphic to B. (The conversion between theta and Weierstrass coordinates was done using [**5**].)

8. *Constructing kernels over a number field*

In this section we show how higher-dimensional analogs of the ℓ-division polynomials can be used to find equations of rational isotropic kernels over a number field. Let $(A, \mathscr{L}, \Theta_n)$ be a polarized abelian variety of dimension g with a symmetric theta structure of level n even, defined over a number field k. For simplicity we assume that $n \geqslant 4$ so the theta structure yields an embedding of A into the projective space $\mathbb{P}^{Z(n)}$. Let ℓ be an integer prime to n. Let η be the generic point of A in theta coordinates.

By using the same method as in § 5 we can formally compute $\ell\eta$ (in time polynomial in $\log(\ell)$) and deduce equations for $A[\ell]$ in the projective space $\mathbb{P}^{Z(n)}$. As in § 4 we can compute a Groebner basis for a lexicographic order; up to a random change of basis the 'shape lemma' [**3**] says that this Groebner basis contains a univariate polynomial Φ_ℓ of degree ℓ^{2g} the zeros of which parametrize the points of $A[\ell]$.

The Groebner basis step is polynomial in the degree ℓ^{2g} of the variety and the size of the generators of the ideal describing it (in our setting we have $O(n^g)$ equations of degree $O(\ell^2)$), so this step is also polynomial in ℓ (for more details see, for instance, [**2**, **20**–**22**]). One way to compute the Groebner basis for the GrevLex order is to compute the Macaulay matrix up to the degree of regularity of the ideal and put it in row echelon form. Then one can use the change of order algorithm from [**13**] to obtain the lexicographical Groebner basis. Over a number field, the system describing the ℓ-torsion will have coefficients of height $O(\log \ell)$, and during the Groebner basis computation the size of the coefficients will go up to a height polynomial in ℓ.

For practical computations, it is better to use the involution $[-1]$ and work over the Kummer variety, and to construct equations for $A[\ell]$ by writing them as $(\ell'+1)\eta = -\ell'\eta$ for the generic point η. Also, rather than constructing the Groebner basis directly over the number field, it is more convenient to compute the reduced Groebner basis for the lexicographic ordering over small primes p of good reduction and lift them through a CRT algorithm. As noted, over each small field $\mathbb{F}_p$, computing a Groebner basis for the lexicographic ordering will take a time polynomial in ℓ, and since the points of ℓ-torsion have small heights (because their canonical heights is zero), the coefficients of the ℓ-division polynomial have a height polynomial in ℓ, so we only need to work over a polynomial number of finite fields.

We note, however, that computing a Groebner basis can be exponential in the number of variables (for a dimension-zero homogeneous system). Since we have a number of variables that are already exponential in the dimension, we see that we can only hope to carry out such a computation for low-dimensional abelian varieties as in [**14**]. For an example of the computation of a ℓ-division polynomial in dimension 2, see also [**16**].

Now we can factorize the polynomial Φ_ℓ (over a number field this is polynomial in its degree) and look at rational factors of degree ℓ^g. These factors correspond to a rational subvariety $K \subset A[\ell]$ of degree ℓ^g. Now we need to check that K is a subgroup and is isotropic.

For this we will work with the formal couple (μ_1, μ_2) from Definition 6.1. We can compute $\mu_1 + \mu_2$ and $-\mu_1$ as in § 5 and check that they satisfy the equations of K. To check that K is isotropic, we need to formally compute the pairing between μ_1 and μ_2. For this we use the results of [**23**]: the Weil pairing can be computed by taking affine lifts of μ_1, μ_2 and $\mu_1+\mu_2$ and using ScalarMult to compute the points $\ell\widetilde{\mu_1}$, $\widetilde{\mu_2}+\ell\widetilde{\mu_1}$, $\ell\widetilde{\mu_2}$ and $\widetilde{\mu_1}+\ell\widetilde{\mu_2}$. We get an element of $\mathscr{K}^{\otimes 2}$ which is equal to 1 when K is isotropic. This computation requires $O(\log \ell)$ operations in $\mathscr{K}^{\otimes 2}$ so it is polynomial in ℓ, which concludes the proof.

9. *Conclusion*

In this paper we have presented an algorithm to compute isogenies between abelian varieties in the arguably most general setting which takes advantage of the field of definition of the kernel in order to improve the complexity. We note that the quasi-optimality announced in the title is only for the case where ℓ is a sum of two squares. It would be very interesting to extend it to encompass all cases. Another question is to handle the case where ℓ is not prime to $2n$. The problem here is that there may be several ways to descend a symmetric theta structure of $\mathscr{L}^\ell$ along the isogeny defined by K, and it is not clear how to specify the choice of a symmetric theta structure of level n on $B = A/K$ via a set of equations.

A related question is how to improve the method of § 8 to generate a rational maximal isotropic kernel. An obvious way would be to use modular polynomials instead of the ℓ-division polynomials. Even given a modular polynomial, and a root of it giving an abelian variety B that is ℓ-isogenous to A, it is not clear how to recover equations for the kernel K of the isogeny $A \to B$. In the case of elliptic curves, one way is to look at the equation of the isogeny provided by Vélu's formula and to solve a differential additions [**8**]. We hope that Theorem 1.1 will help to generalize this method to abelian varieties.

References

1. A. Atkin, 'The number of points on an elliptic curve modulo a prime', manuscript, Chicago, IL, 1988.

2. M. Bardet, 'Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie', PhD Thesis, Université Paris 6, 2004.

3. E. Becker, T. Mora, M. G. Marinari and C. Traverso, 'The shape of the shape lemma', *Proceedings of the International Symposium on Symbolic and Algebraic Computation* (ACM Press, 1994) 129–133.

4. C. Birkenhake and H. Lange, *Complex abelian varieties*, 2nd edn, Grundlehren der Mathematischen Wissenschaften, Fundamental Principles of Mathematical Sciences 302 (Springer, Berlin, 2004).

5. G. Bisson, R. Cosset and D. Robert, 'AVIsogenies (Abelian Varieties and Isogenies). Magma package for explicit isogeny computation between abelian varieties', 2010, http://avisogenies.gforge.inria.fr/.
6. G. Bisson and M. Streng, 'On polarised class groups of orders in quartic cm-fields', Preprint, 2013, arXiv:1302.3756.
7. G. Bisson and A. V. Sutherland, 'Computing the endomorphism ring of an ordinary elliptic curve over a finite field', *J. Number Theory* 131 (2011) no. 5, 815–831.
8. A. Bostan, F. Morain, B. Salvy and E. Schost, 'Fast algorithms for computing isogenies between elliptic curves', *Math. Comput.* 77 (2008) no. 263, 1755–1778.
9. R. Bröker, K. Lauter and A. V. Sutherland, 'Modular polynomials via isogeny volcanoes', *Math. Comp.* 81 (2012) 1201–1231, doi:10.1090/S0025-5718-2011-02508-1.
10. H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen and F. Vercauteren (eds), *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications (Chapman and Hall/CRC, Boca Raton, FL, 2006).
11. R. Cosset and D. Robert, 'An algorithm for computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of hyperelliptic curves of genus 2', *Math. Comput.* (2013) accepted for publication.
12. N. Elkies, 'Explicit isogenies', manuscript, Boston, 1992.
13. J. C. Faugère, P. Gianni, D. Lazard and T. Mora, 'Efficient computation of zero-dimensional Gröbner bases by change of ordering', *J. Symbolic Comput.* 16 (1993) no. 4, 329–344.
14. J.-C. Faugère, D. Lubicz and D. Robert, 'Computing modular correspondences for abelian varieties', *J. Algebra.* 343 (2011) 248–277.
15. M. Fouquet and F. Morain, 'Isogeny volcanoes and the SEA algorithm', *Algorithmic number theory (Sydney, 2002)*, Lecture Notes in Computer Science 2369 (Springer, Berlin, 2002) 276–291.
16. P. Gaudry and É. Schost, 'Construction of secure random curves of genus 2 over prime fields', *Advances in Cryptology – EUROCRYPT 2004*, Lecture Notes in Computer Science 3027 (eds C. Cachin and J. Camenisch; Springer, 2004) 239–256.
17. J.-I. Igusa, *Theta functions*, Die Grundlehren der mathematischen Wissenschaften, Band 194 (Springer, New York, 1972).
18. D. Kohel, 'Endomorphism rings of elliptic curves over finite fields', PhD Thesis, University of California, 1996.
19. S. Koizumi, 'Theta relations and projective normality of Abelian varieties', *Amer. J. Math.* 98 (1976) no. 4, 865–889.
20. D. Lazard, 'Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations', *Computer algebra (London, 1983)*, Lecture Notes in Computer Science 162 (Springer, Berlin, 1983) 146–156.
21. D. Lazard, 'Ideal bases and primary primary decomposition: case of two variables', *J. Sci. Comput.* 1 (1985) no. 3, 261–270.
22. D. Lazard, 'Solving zero-dimensional algebraic systems', *J. Sci. Comput.* 13 (1992) no. 2, 117–132.
23. D. Lubicz and D. Robert, 'Efficient pairing computation with theta functions', *Algorithmic number theory*, Lecture Notes in Computer Science 6197 (Springer, Berlin, 2010) 251–269, doi:10.1007/978-3-642-14518-6_21.
24. D. Lubicz and D. Robert, 'Computing isogenies between abelian varieties', *Compos. Math.* 148 (2012) no. 5, 1483–1515.
25. D. Lubicz and D. Robert, 'A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties', *J. Symbolic Comput.* 67 (2015) 68–92, doi:10.1016/j.jsc.2014.08.001.
26. D. Mumford, 'On the equations defining abelian varieties, I', *Invent. Math.* 1 (1966) 287–354.
27. D. Mumford, *Tata lectures on theta I*, Progress in Mathematics 28 (Birkhäuser, Boston, 1983), with the assistance of C. Musili, M. Nori, E. Previato and M. Stillman.
28. R. Schoof, 'Elliptic curves over finite fields and the computation of square roots mod p', *Math. Comput.* 44 (1985) no. 170, 483–494.
29. R. Schoof, 'Counting points on elliptic curves over finite fields', *J. Théor. Nombres Bordeaux* 7 (1995) no. 1, 219–254.
30. J.-P. Serre, 'Lettre à M. Tsfasman', *Astérisque* 11 (1991) no. 198–200, 351–353.
31. A. V. Sutherland, 'Computing Hilbert class polynomials with the Chinese remainder theorem', *Math. Comput.* 80 (2011) no. 273, 501–538.

David Lubicz
Université de Rennes 1
Campus de Beaulier
35042 Rennes
France
david.lubicz@univ-rennes1.fr

Damien Robert
INRIA Bordeaux Sud-Ouest
200 avenue de la Vieille Tour
33405 Talence
France
damien.robert@inria.fr