Computing (l,l)-isogenies in polynomial time on Jacobians of genus 2 curves

Romain Cosset, Damien Robert

MATHEMATICS OF COMPUTATION
Volume 00, Number 0, Pages 000–000
S 0025-5718(XX)0000-0

COMPUTING (ℓ,ℓ)-ISOGENIES IN POLYNOMIAL TIME ON JACOBIANS OF GENUS 2 CURVES

ROMAIN COSSET, DAMIEN ROBERT

Abstract. In this paper, we compute ℓ-isogenies between abelian varieties over a field of characteristic different from 2 in polynomial time in ℓ, when ℓ is an odd prime which is coprime to the characteristic. We use level n symmetric theta structure where $n = 2$ or $n = 4$. In a second part of this paper we explain how to convert between Mumford coordinates of Jacobians of genus 2 hyperelliptic curves to theta coordinates of level 2 or 4. Combined with the preceding algorithm, this gives a method to compute (ℓ,ℓ)-isogenies in polynomial time on Jacobians of genus 2 curves.

1. Introduction

The discrete logarithm problem on the group of rational points of an elliptic curve $E/\mathbb{F}_q$ is believed to be hard (except for some special families of elliptic curves [23, 14]...). In fact, if $\#E(\mathbb{F}_q)$ is a prime p, then the best known algorithm to solve the DLP in $E(\mathbb{F}_q)$ is the generic Pollard-rho algorithm in $\widetilde{O}(\sqrt{p})$. Thus in recent years [18], elliptic curves have been used in public key cryptography. Moreover, there exist natural pairings on elliptic curves, which allow for the construction of many new and interesting protocols [16, 5, 4, 39, 33, 15].

Another solution is to work over the group of rational points of the Jacobian of a curve C defined over $\mathbb{F}_q$ (or even any abelian variety). If the genus g of C is strictly greater than 2, we have better algorithms than Pollard-ρ to solve the DLP on the Jacobian of C [10] (these algorithms are still exponential in the largest prime dividing the group when the genus is not too large). Jacobians of genus 2 curves are particularly interesting since they allow the same security as with elliptic curves, while working with fields of half the size.

In the genus 2 case, we still lack some of the efficient algorithms that we have for elliptic curves. One of them is the efficient computation of isogenies. They are used in the elliptic curves case for the construction of Hilbert class polynomials [37], for endomorphism ring computations [19, 12, 3], for modular polynomials [7], and they form a basic ingredient of the amelioration by Atkin and Elkies of the Schoof point counting algorithm [34, 35, 1, 9]. For elliptic curves, one can compute isogenies using Vélu's formulae and modular polynomials (the latter are more suited for the computation of isogeny graphs). For higher dimensional abelian varieties, Richelot formulae [30, 31] allow to compute $(2,2)$-isogenies between Jacobians of genus 2 curves, and [36] give an algorithm to compute $(2,2,2)$-isogenies between Jacobians of genus 3 curves. In [6], the authors explain how to compute $(3,3)$-isogeny graphs of abelian varieties of dimension 2 (but not the explicit form of the isogenies) using theta constants of level 4. A generalisation of Vélu's formulae is given in

[21], which describes algorithm which takes for input a basis of a maximal isotropic subgroup K of an abelian variety A and outputs the isogeny $A \to A/K$ is described. One drawback of this algorithm is that it needs to work with theta functions of different levels on A and on A/K. The authors also describe an algorithm to compute isogenies while working on theta functions of a fixed level n, but it only allows to compute ℓ^2-isogenies. In this paper, we show how one can use the addition formulae from Koizumi [20] to obtain an explicit algorithm for the conversion of theta coordinates of different level. Combined with the algorithm of [21], this yields an algorithm to compute ℓ-isogenies between abelian varieties described by theta coordinates of the same level n:

Theorem 1.1. *Let $(A_k, \mathcal{L}, \Theta_n)$ be a polarised abelian variety of dimension g with a symmetric theta structure of level n (since $\mathcal{L}$ is totally symmetric, n is even). Let ℓ be prime to n and assume that the characteristic of k is prime to ℓn. Let K be a maximal isotropic subgroup of $A[\ell]$ (for the pairing induced by the polarisation $\mathcal{L}$). Then we can compute the isogeny $A \to A/K$ in theta coordinates of level n by using $O(\ell^{\frac{rg}{2}})$ arithmetic operations in k', where k' is the field extension where the theta coordinates of the geometric points of K are defined, and $r = 2$ if $\ell \equiv 1 \mod 4$, $r = 4$ otherwise.*

One drawback of using theta functions of level n is that they are not rational. If $\mathcal{C}$ is an hyperelliptic curve of genus g, Mumford coordinates give rational coordinates on the Jacobian of $\mathcal{C}$. In the second part of this paper, we focus on the genus 2 case. Thomae's formulae only give the fourth power of the coordinates of the theta null point of level 4. When $g = 2$, we show how to take canonical roots up to the action of $\mathrm{PSp}(4, \mathbb{Z})$ in Section 5.1. We describe formulae to convert between Mumford coordinates on the Jacobian of an hyperelliptic curve of genus 2 and theta coordinates of level 2 and 4. Combined with Theorem 1.1 we obtain:

Theorem 1.2. *Let J be the Jacobian of an hyperelliptic curve of genus 2 over a field k of characteristic different form 2. Let K be a maximal isotropic subgroup of $J[\ell]$ for the Weil pairing. Then we can compute the isogeny $J \to J/K$ in Mumfod coordinates by using $O(\ell^r)$ arithmetic operations in k', where k' is the field extension where the Mumford coordinates of the geometric points of K are defined, and $r = 2$ if $\ell \equiv 1 \mod 4$, $r = 4$ otherwise.*

In particular, if k is a finite field, and K is rational, then we can compute the isogeny using $O(\ell^{2+r})$ arithmetic operations in k.

Theorem 1.1 is proved in Section 4 and Theorem 1.2 is proved in Section 5. For simplicity, we assume that we work over a subfield k of $\mathbb{C}$. However our formulae and algorithms apply to any field (of characteristic different from 2). To prove the formulae over a finite field (the cryptographically relevant case), if the abelian variety is ordinary we can consider its canonical lift and invoke Lefschetz's principle. To prove them over any field (and relax the ordinary condition), we can use Mumford theory of algebraic theta functions [25, 26, 27]. We then need an algebraic version of Koizumi's addition formulae [20] given by Kempf [17]. The reader interested to an algebraic proof is referred to [32, Section 7.8].

For the convenience of the reader, we try to be as self contained as possible, so rather than just explaining how to use Koizumi's addition formulae to change the level of theta coordinates and refer to [21], we describe the full isogeny algorithm. In Section 2 we recall some well known facts about analytic theta functions, and

describe the basis of theta functions we are going to use through the paper. Section 3 gives Koizumi's addition formulae, and as a first application how one can use them to obtain an algorithm for differential additions. The isogeny computation is described in Section 4, and the special case of Jacobians of genus 2 hyperelliptic curves where we have complete formulae for the conversion between Mumford and theta coordinates is treated in Section 5. Some of these formulae are quite lengthy, and given in the Appendix.

2. Theta coordinates on abelian varieties

Over $\mathbb{C}$, an abelian variety A of dimension g is analytically isomorphic to a torus $\mathbb{C}^g/(\Omega\mathbb{Z}^g+\mathbb{Z}^g)$ where Ω is an element of the Siegel half-space $\mathcal{H}_g$:

$$\mathcal{H}_g = \{\Omega \in \mathrm{M}_{g\times g}(\mathbb{C}),\ {}^t\Omega = \Omega \text{ and } \Im(\Omega) > 0\}.$$

There is a canonical principal polarisation $\mathcal{L}$ associated to the choice of Ω and given by the Riemann form $E(\Omega x_1 + x_2, \Omega y_1 + y_2) = {}^t x_1 y_2 - {}^t y_1 x_2$ on $\Omega\mathbb{Z}^g + \mathbb{Z}^g$ [2]. We will call a section of $\mathcal{L}^n$ a theta function of level n.

We recall that the classical Riemann theta function associated to Ω is an analytic function from $\mathbb{C}^g$ to $\mathbb{C}$. It is defined by [28]

$$\Theta(z,\Omega) = \sum_{n\in\mathbb{Z}^g} \exp\left(\pi i^t n\Omega n + 2\pi i^t n z\right).$$

For $a, b \in \mathbb{Q}^g$, the theta function of characteristics a, b is a translation of the classical theta up to an exponential factor:

$$\Theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega) = \Theta(z+\Omega a + b, \Omega)\exp\left(\pi i^t a\Omega a + 2\pi i^t a(z+b)\right). \tag{1}$$

These characteristics can be considered modulo $\mathbb{Z}^{2g}$ since for α, β in $\mathbb{Z}^g$ we have

$$\Theta\left[\begin{smallmatrix} a+\alpha \\ b+\beta \end{smallmatrix}\right](z,\Omega) = \Theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega)\exp(2\pi i^t a\beta).$$

A basis of the theta functions of level n is given by [28]

$$\left(\Theta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right](z, \frac{\Omega}{n})\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}.$$

To ease the notations, we note $Z(n) = \mathbb{Z}^g/n\mathbb{Z}^g$, and we fix once and for all a section $Z(n) \to \mathbb{Z}^g$. We then define for $b \in Z(n)$: $\theta_b \coloneqq \Theta\left[\begin{smallmatrix} 0 \\ \frac{b}{n} \end{smallmatrix}\right](\cdot, \frac{\Omega}{n})$.

When $n = k^2$, another choice for the basis of level n theta functions is given by

$$\left(\Theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](kz,\Omega)\right)_{a,b\in(\frac{1}{k}\mathbb{Z}^g)/\mathbb{Z}^g}.$$

We will call this the basis of level (k,k). The linear transformations between the basis of level $n = k^2$ and the basis of level (k,k) are given by [28]:

$$\Theta\left[\begin{smallmatrix} a/k \\ b/k \end{smallmatrix}\right](kz,\Omega) = \frac{1}{k^g}\sum_{\beta\in\mathbb{Z}^g/k\mathbb{Z}^g} \exp\left(-2\pi i\frac{{}^t ab}{k}\right)\Theta\left[\begin{smallmatrix} 0 \\ b/n+\beta/k \end{smallmatrix}\right]\left(z, \frac{\Omega}{n}\right),$$

$$\Theta\left[\begin{smallmatrix} 0 \\ b/n \end{smallmatrix}\right]\left(z, \frac{\Omega}{n}\right) = \sum_{\alpha\in\mathbb{Z}^g/k\mathbb{Z}^g}\Theta\left[\begin{smallmatrix} \alpha/k \\ b/k \end{smallmatrix}\right](kz,\Omega).$$

The advantage of the latter choice is that it comes more naturally as analytic functions over the abelian variety. On the other hand, the formers are more general and "symmetric": $\theta_i(-z) = \theta_{-i}(z)$.

A well known result of Lefschetz states that when $n \geq 3$, the theta functions of level n give a projective embedding:

$$\begin{array}{rccc} \varphi_{\mathcal{L}}\colon & \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g) & \longrightarrow & \mathbb{P}^{n^g-1}(\mathbb{C}) \\ & z & \longmapsto & (\theta_i(z))_{i\in Z(n)} \end{array} .$$

When $n = 2$, and the abelian variety is simple, then the theta functions of level 2 give a projective embedding of the Kummer variety $K_A = A/\pm 1$.

The point $(\theta_i(0))_{i\in Z(n)} = \varphi_{\mathcal{L}}(0_A) \in \mathbb{P}^{n^g-1}(\mathbb{C})$ is called the theta null point (of level n) of A. This point determines $(\varphi_{\mathcal{L}}(A), \varphi_{\mathcal{L}}(A[n]))$ [25].

For arithmetic reasons we want to deal with theta functions of level as small as possible. The reason is that if A is defined over a subfield $K_0 \subset \mathbb{C}$, a necessary condition for the theta functions of level n to be generated by a basis defined over K_0 is that there exists a K_0-rational symplectic isomorphism between $A[n]$ (with the induced Riemann form) and $Z(n) \oplus \hat{Z}(n)$, where $\hat{Z}(n)$ is the Cartier dual of $Z(n)$. Here, if μ_n is the group of n-roots of unity in $\mathbb{C}^*$, then $\hat{Z}(n) = \oplus_{i=1}^g \mu_n$. Since we will heavily use the duplication formulae (and the Riemann relations), we need $2 \mid n$. For these reasons, in this article, we only work with $n = 2$ or $n = 4$. The case $n = 2$ is a bit more tricky since we work over the Kummer variety, but it is worthwhile in practice.

3. The addition formulae

An extension of the usual Riemann relations between theta functions is given in a general form by [20, Theorem 1.3]:

Theorem 3.1 (Koizumi)**.** *Let $(\gamma_1, \ldots, \gamma_r) \in \mathbb{Q}^r$, $(\delta_1, \ldots, \delta_r) \in \mathbb{Q}^r$ and $F \in \mathrm{Gl}_r(\mathbb{Q})$ be such that*

$${}^tF \begin{pmatrix} \gamma_1 & & 0 \\ & \ddots & \\ 0 & & \gamma_r \end{pmatrix} F = \begin{pmatrix} \delta_1 & & 0 \\ & \ddots & \\ 0 & & \delta_r \end{pmatrix}.$$

Let $(x_1, \ldots, x_r) \in (\mathbb{C}^g)^r$, and $(y_1, \ldots, y_r) = (x_1, \ldots, x_r)F$. Let $(a_1, \ldots, a_r)$ and $(b_1, \ldots, b_r)$ be elements of $(\mathbb{C}^g)^r$, and note

$$(a'_1, \ldots, a'_r) = (a_1, \ldots, a_r)\,{}^tF^{-1},$$
$$(b'_1, \ldots, b'_r) = (b_1, \ldots, b_r)F.$$

Let d be the index $[\mathrm{M}_{g\times r}(\mathbb{Z}) + \mathrm{M}_{g\times r}(\mathbb{Z})\,{}^tF : \mathrm{M}_{g\times r}(\mathbb{Z})]$ We have:

$$\begin{aligned} (2)\quad & d\,\Theta\left[\begin{smallmatrix} a_1 \\ b_1 \end{smallmatrix}\right](x_1, \gamma_1\Omega) \times \cdots \times \Theta\left[\begin{smallmatrix} a_r \\ b_r \end{smallmatrix}\right](x_r, \gamma_r\Omega) \\ & \qquad = \sum \Theta\left[\begin{smallmatrix} a'_1+\alpha_1 \\ b'_1+\beta_1 \end{smallmatrix}\right](y_1, \delta_1\Omega) \times \cdots \times \Theta\left[\begin{smallmatrix} a'_r+\alpha_r \\ b'_r+\beta_r \end{smallmatrix}\right](y_r, \delta_r\Omega) \end{aligned}$$

where the sum is over the elements α and β such that

$$\begin{aligned} \alpha &\in \mathrm{M}_{g\times r}(\mathbb{Z})\,{}^tF^{-1}/\left(\mathrm{M}_{g\times r}(\mathbb{Z}) \bigcap \mathrm{M}_{g\times r}(\mathbb{Z})\,{}^tF^{-1}\right), \\ \beta &\in \mathrm{M}_{g\times r}(\mathbb{Z})F/\left(\mathrm{M}_{g\times r}(\mathbb{Z}) \bigcap \mathrm{M}_{g\times r}(\mathbb{Z})F\right). \end{aligned}$$

Corollary 3.2 (Riemann relations)**.** *Recall that for $b \in Z(n)$, we have defined $\theta_b := \Theta \left[\begin{smallmatrix} 0 \\ \frac{b}{n} \end{smallmatrix} \right] (\cdot, \frac{\Omega}{n})$. Let x_1, y_1, u_1 and v_1 in $\mathbb{C}^g$ such that $x_1+y_1+u_1+v_1 = 2z$. We define $x_2 = z-x_1$, $y_2 = z-y_1$, $u_2 = z-u_1$ and $v_2 = z-v_1$. For all $i,j,k,l,m \in Z(n)$ with $i+j+k+l = 2m$, if we let $i' = m-i$, $j' = m-j$, $k' = m-k$ and $l' = m-l$ then for all characters $\chi \in \hat{Z}(\overline{2})$ we have:*

$$(3)\quad \Big(\sum_{t\in Z(2)} \chi(t)\theta_{i+t}(x_1)\theta_{j+t}(y_1)\Big).\Big(\sum_{t\in Z(2)} \chi(t)\theta_{k+t}(u_1)\theta_{l+t}(v_1)\Big) = \Big(\sum_{t\in Z(2)} \chi(t)\theta_{i'+t}(x_2)\theta_{j'+t}(y_2)\Big).\Big(\sum_{t\in Z(2)} \chi(t)\theta_{k'+t}(u_2)\theta_{l'+t}(v_2)\Big).$$

As a particular case, if $x, y \in \mathbb{C}^g$, we have the following differential addition formulae:

$$(4)\quad \Big(\sum_{t\in Z(2)} \chi(t)\theta_{i+t}(x+y)\theta_{j+t}(x-y)\Big).\Big(\sum_{t\in Z(2)} \chi(t)\theta_{k+t}(0)\theta_{l+t}(0)\Big) = \Big(\sum_{t\in Z(2)} \chi(t)\theta_{-i'+t}(y)\theta_{j'+t}(y)\Big).\Big(\sum_{t\in Z(2)} \chi(t)\theta_{k'+t}(x)\theta_{l'+t}(x)\Big).$$

Proof. Equation (3) is a modified form of the usual Riemann relations obtained from Theorem 3.1 with the matrix

$$F = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

The usual Riemann relations can be found in [28, p. 212], and the transformation that gives (3) in [25, p. 334–335]. □

Assume we are in level 4. As was shown in [21], one can use the differential addition formulae (4) to compute $(\theta_i(x+y))_{i\in Z(n)}$ when $x, y \in \mathbb{C}^g$, provided one knows $(\theta_i(x))_{i\in Z(n)}$, $(\theta_i(y))_{i\in Z(n)}$, $(\theta_i(x-y))_{i\in Z(n)}$. Indeed, for sufficiently many $\chi \in \hat{Z}(\overline{2})$, $k, l \in Z(n)$, we have $\big(\sum_{t\in Z(2)} \chi(t)\theta_{k+t}(0)\theta_{l+t}(0)\big) \neq 0$. It is also possible to compute "normal" additions, that is the addition law on the abelian variety. Suppose that we know the theta coordinates $x, y \in A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$. Here we are working modulo the lattice and we see the theta coordinates as *projective* coordinates. But the addition formulae allows to recover $(\theta_i(x+y))_{i\in Z(n)}$ up to a projective factor, so we can indeed compute normal additions.

When the level n is 2, then the embedding of the Kummer variety K_A given by the theta functions of level 2 is projectively normal if and only if the even theta constants

$$\left\{\Theta \left[\begin{smallmatrix} a/2 \\ b/2 \end{smallmatrix} \right] \left(0, 2\frac{\Omega}{n}\right) \mid a, b \in Z(2), (-1)^{{}^t a\cdot b} = 1\right\}$$

are not zero. In this case, we can also always compute differential additions in level 2 [22]. Moreover, when we know $\pm P \in K_A$, $\pm Q \in K_A$ and the even theta constants are not zero, we can use formulae (4) to recover $\{\pm(P+Q), \pm(P-Q)\} \subset K_A$ with a square root. We note that this condition excludes Jacobians of hyperelliptic curves of genus $g \geq 3$, we thus have to work with $n = 4$ to treat them.

A small technical detail is that in the algebraic setting, an abelian variety will be represented by its theta null point given in projective coordinates. Thus in practice

we will work on it with theta coordinates of the form $\theta_b = \lambda\Theta\left[\begin{smallmatrix}0\\ \frac{b}{n}\end{smallmatrix}\right](\cdot, \frac{\Omega}{n})$ where λ is a projective factor. But since Theorem 3.1 is homogeneous, all our algorithms remain valid in this case.

4. Computing ℓ-isogenies between abelian varieties

In this section, we show how we can improve the results of [21] by using Theorem 3.1. We will give an algorithm to compute the isogeny

$$\begin{array}{rccc} f\colon & A = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g) & \longrightarrow & B = \mathbb{C}^g/(\ell\Omega\mathbb{Z}^g + \mathbb{Z}^g) \\ & z & \longmapsto & \ell.z \end{array},$$

provided that we know its kernel $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$.

A maximal isotropic subgroup K of the ℓ-torsion is isomorphic to $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$. We want to compute the isogeny associated to K. Let $\Lambda = \Omega\mathbb{Z}^g + \mathbb{Z}^g$ be the lattice associated to A. The choice of $\Omega \in \mathcal{H}_g$ is equivalent to the choice of a symplectic basis of Λ for the Riemann form (see also Section 5.1). If K is any maximal isotropic subgroup of $A[\ell]$ (for the induced Riemann form), then we can always choose a symplectic basis of Λ such that if $\Lambda = \Omega_0\mathbb{Z}^g + \mathbb{Z}^g$ is the corresponding decomposition, we have $K = \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ [2, 11]. Thus we can apply the preceding algorithm to compute the isogeny associated to any maximal isotropic subgroup.

We proceed in two steps: we first explain how to compute the theta null point of level n of B, and then how to compute $f(x)$ where x is a geometric point in A. For simplicity, we assume here that $n = 4$, we will then discuss how to make the necessary adjustments when $n = 2$. To simplify the notations, we let as in Section 2 for $b \in Z(n)$:

$$\theta_b^A \coloneqq \Theta\left[\begin{smallmatrix}0\\ \frac{b}{n}\end{smallmatrix}\right]\left(\cdot, \frac{\Omega}{n}\right), \quad \theta_b^B \coloneqq \Theta\left[\begin{smallmatrix}0\\ \frac{b}{n}\end{smallmatrix}\right]\left(\cdot, \frac{\ell\Omega}{n}\right).$$

Let F be a matrix of rank r such that ${}^tFF = \ell\,\mathrm{Id}_r$. If $\ell = a^2 + b^2$, we can take $F = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ and $r = 2$. In general, we can always write $\ell = a^2 + b^2 + c^2 + d^2$ and take the matrix of multiplication by $a + bi + cj + dk$ in the quaternions algebra over $\mathbb{R}$, so $r = 4$. With these notations, we get as a particular case of Theorem 3.1:

Proposition 4.1. *Let F be a matrix of rank r such that ${}^tFF = \ell\,\mathrm{Id}_r$. Let X in $(\mathbb{C}^g)^r$ and $Y = XF^{-1} \in (\mathbb{C}^g)^r$. Let $i \in (Z(n))^r$ and $j = iF^{-1}$. Then we have*

$$\theta_{i_1}^B(Y_1)\dots\theta_{i_r}^B(Y_r) = \sum_{\substack{t_1,\dots,t_r \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ (t_1,\dots,t_r)F = (0,\dots,0)}} \theta_{j_1}^A(X_1 + t_1)\dots\theta_{j_r}^A(X_r + t_r), \tag{5}$$

Proof. This is a special case of Theorem 3.1 applied to $\frac{1}{\ell}\,{}^tF$, and with $(a_1,\dots,a_r) = (0,\dots,0)$, remembering that $\Theta\left[\begin{smallmatrix}0\\ b+\beta\end{smallmatrix}\right](x, \frac{\Omega}{n}) = \Theta\left[\begin{smallmatrix}0\\ b\end{smallmatrix}\right](x + \beta, \frac{\Omega}{n})$ by (1). □

We explain how to use these formulae to compute explicitly the isogeny.

4.1. Computing the theta null point of B.

Now we assume that we know the coordinates of a basis $(e_1,\dots,e_g)$ of K in A. Up to a symplectic change of basis, we can assume that this basis is the reduction of the canonical basis $(\tilde{e}_1,\dots,\tilde{e}_g)$ of $\frac{1}{\ell}\mathbb{Z}^g$ to A. This mean that we know the coordinates $(\theta_k^A(\tilde{e}_i))_{k\in Z(n)}$ up to an unknown projective factor λ_i for $i = 1,\dots,g$.

Since we are assuming $n = 4$, we can compute $e_i + e_j \in A$ for $i \neq j \in [1, g]$, so that we know $\left(\theta^A_k(\tilde{e}_i + \tilde{e}_j)\right)$ up to an unknown projective factor λ_{ij}. Now by using the Riemann relations, we can compute all the points $\left(\theta^A_k(n_1\tilde{e}_1 + \dots n_g\tilde{e}_g)\right)$ exactly in terms of the λ_i and λ_{ij}.

We detail this step. First, it is important to note that the result does not depend on the order of the Riemann relations used to compute a point of the form $\left(\theta^A_k(n_1\tilde{e}_1 + \dots n_g\tilde{e}_g)\right)$. Indeed, the same proof as in [22, Lemma 2] applies here. Now, if we had all the coordinates $\left(\theta^A_k(n_1\tilde{e}_1 + \dots n_g\tilde{e}_g)\right)$ with $n_k \in \{0, 1\}$ for $k = 1, \dots, g$, we could use differential additions to compute the rest. To get these coordinates we can proceed as follow: assume for example that $g = 3$. Then by using differential additions, we can compute $\tilde{e}_1 - \tilde{e}_3$. We can then use a differential addition on $\tilde{e}_1 + \tilde{e}_2$ and $\tilde{e}_2 + \tilde{e}_3$ to compute $\tilde{e}_1 + 2\tilde{e}_2 + \tilde{e}_3$. Since ℓ is odd, we can use differential additions to compute $\tilde{e}_1 + (\ell + 1)\tilde{e}_2 + \tilde{e}_3$. Using this method, we can compute an affine lift of any element in the kernel. We need some care with this method, because the polynomial given by $\tilde{e}_1 + (\ell + 1)\tilde{e}_2 + \tilde{e}_3$ differs from the one given by $\tilde{e}_1 + \tilde{e}_2 + \tilde{e}_3$ by a factor in $\mathbb{C}[\lambda^\ell_i, \lambda^\ell_{ij}]$. This is not a problem for the rest of the algorithm, as we can keep track of this factor, and as we will see the ℓ-th power of the λ_i are known.

Perhaps an easier way is to use more general Riemann relations than the ones coming from the differential additions. For instance by setting $x_1 = \tilde{e}_1 + \tilde{e}_2 + \tilde{e}_3$, $y_1 = \tilde{e}_1$, $u_1 = \tilde{e}_2$, $v_1 = \tilde{e}_3$, in equation (3), we can compute directly the (affine) theta coordinates of $\tilde{e}_1 + \tilde{e}_2 + \tilde{e}_3$ in terms of the theta null point and the theta coordinates of $\tilde{e}_1$, $\tilde{e}_2$, $\tilde{e}_3$, $\tilde{e}_2 + \tilde{e}_3$, $\tilde{e}_1 + \tilde{e}_3$, $\tilde{e}_1 + \tilde{e}_2$. We will call this an extended differential addition. With this method, we need to be sure that sufficiently many elements of the form $\left(\sum_{t\in Z(2)} \chi(t)\theta_{k+t}(\tilde{e}_2)\theta_{l+t}(\tilde{e}_3)\right)$ are not zero, so that we can indeed compute the extended differential addition. This follows from the fact that since we are working with an isotropic kernel, we can interpret the theta coordinates of level n of points of this kernel as the theta coordinates of level ℓn of the theta null point of an ℓ-isogenous abelian variety (for the proof, see [21, Section 3.3]).

We can also recover some informations on the λ_i, λ_{ij}. Indeed, write $\ell = 2\ell' + 1$. Then we have $\theta^A_k\left((\ell' + 1)\tilde{e}_i\right) = \theta^A_{-k}(\ell'\tilde{e}_i)$ since $(\ell' + 1)\tilde{e}_i = -(\ell')\tilde{e}_i$ modulo $\mathbb{Z}^g$ and the θ^A_k are invariants by translation by an element in $\mathbb{Z}^g$. In terms of the λ_i, we get an equation of the form $\lambda_i^{(\ell'+1)^2} = \alpha_i\lambda_i^{(\ell')^2}$. We thus know explicitly λ^ℓ_i since it is equal to $\alpha_i \in \mathbb{C}$. Likewise, by considering $e_i + e_j$, we recover λ^ℓ_{ij} explicitly.

We want to compute $\left(\theta^B_k(0)\right)_{k\in Z(n)}$ projectively. From equation (5) with $i_1 = k$, $i_2 = \dots = i_r = 0$ and $X = 0$ we get:

$$\theta^B_k(0)\theta^B_0(0)\dots\theta^B_0(0) = \sum_{\substack{t_1,\dots,t_r\in K\\ (t_1,\dots,t_r)F=(0,\dots,0)}} \theta^A_{j_1}(t_1)\dots\theta^A_{j_r}(t_r), \tag{6}$$

where $j = (k, 0, \dots, 0)F^{-1} \in Z(n)$ (since ℓ is prime to n, F is bijective on $Z(n)$).

For the rest of the discussion, we will suppose that $\theta^B_0(0) \neq 0$, so if we know how to compute the right hand term, we can recover the theta null point of B up to a non zero projective factor. Of course if this is not the case, we just need to apply Equation (5) with $i_2 = \dots = i_r$ equal to a non zero coordinate. As we have seen, we can compute exactly the monomials in the sum of the right hand term up to the

unknown factors λ_i and λ_{ij}. But the following lemma shows that the monomials appearing only depend on these factors to the power of ℓ, which we know.

Lemma 4.2. *Let $(t_1,\dots,t_r) \in K^r$ such that $(t_1,\dots,t_r)F = (0,0,\dots,0)$ and let $(j_1,\dots,j_r) \in Z(n)^r$ such that $(j_1,\dots,j_r)F = (k,0,\dots,0)$. Then when we write the product $\theta^A_{j_1}(t_1)\dots\theta^A_{j_r}(t_r)$ in terms of the λ_i, λ_{ij} seen as indeterminates, it lies in $\mathbb{C}[\lambda_i^\ell, \lambda_{ij}^\ell]$.*

Proof. We want to show that a monomial $\theta^A_{j_1}(t_1)\dots\theta^A_{j_r}(t_r)$ is invariant under any transformation T of $\mathbb{C}[\lambda_i,\lambda_{ij}]$ that acts on the generators by a ℓth-root of unity.

Fix $i_0 \in Z(n)$. We first show that the expression is invariant under the transformation T of $\mathbb{C}[\lambda_i,\lambda_{ij}]$ such that

$$T(\lambda_{i_0}) = \zeta\lambda_{i_0}, \quad T(\lambda_{i_0 j}) = \zeta\lambda_{i_0 j}$$

where ζ is a ℓth-root of unity, $j \neq i_0$, and T leaves invariant the other generators. We let

$$u = [\ell]\left((t_1)_{i_0}, (t_2)_{i_0}, \dots, (t_r)_{i_0}\right).$$

Here, we see $t_i \in K$ as an element of $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ that we identify to $\mathbb{Z}^g/\ell\mathbb{Z}^g$ via the map $[\ell] : x \mapsto \ell.x$. We then have

$$T(\theta^A_{j_1}(t_1)\dots\theta^A_{j_r}(t_r)) = \zeta^{(u_1^2+\dots+u_r^2)}\theta^A_{j_1}(t_1)\dots\theta^A_{j_r}(t_r).$$

But we have $(t_1,\dots,t_r)F = 0 \in K$ so we are reduced to the following problem: show that for an element u in $(\mathbb{Z}/\ell\mathbb{Z})^r$ such that $uF = 0$, we have $u \cdot {}^t u = 0$. But since $uF = 0$, u is of the form $u'\,{}^t F$, so

$$u \cdot {}^t u = u' \cdot {}^t F \cdot F \cdot {}^t u' = \ell u' \cdot {}^t u' = 0.$$

Now we fix $i_0, j_0 \in Z(n)$ and we consider the transformation T such that $T(\lambda_{i_0,j_0}) = \zeta\lambda_{i_0,j_0}$ and T leaves invariant the other generators. Let

$$u = [\ell]\left((t_1)_{i_0}, (t_2)_{i_0}, \dots, (t_r)_{i_0}\right), \quad v = [\ell]\left((t_1)_{j_0}, (t_2)_{j_0}, \dots, (t_r)_{j_0}\right).$$

We then compute:

$$T(\theta^A_{j_1}(t_1)\dots\theta^A_{j_r}(t_r)) = \zeta^{{}^t u\cdot v}\theta^A_{j_1}(t_1)\dots\theta^A_{j_r}(t_r).$$

But since $(t_1,\dots,t_r)F = 0$, we have $uF = vF = 0$, and so ${}^t uv = {}^t u'\,{}^t F F v' = 0$ (where u' and v' are some elements of $(\mathbb{Z}/\ell\mathbb{Z})^r$).

The transformations T we have considered generate all the transformations we are looking at, this concludes the proof. □

Now this gives us an algorithm to compute $\left(\theta^B_k(0)\right)_{k\in Z(n)}$ (projectively), since we may take any ℓth-root of the λ_i^ℓ, λ_{ij}^ℓ, and apply Equation (6). In fact, Lemma 4.2 states that we get the correct result even if we make the wrong choice. Actually, we do not need to take any ℓth-root, we just need to work symbolically over the ring $\mathbb{C}[\lambda_i,\lambda_{ij}]/\{\lambda_i^\ell = \alpha_i, \lambda_{ij}^\ell = \alpha_{ij}\}$.

For the convenience of the reader we give a complete algorithm for $g = 2$, the advantage of this case being that we need only differential additions, not extended differentials. We leave to the reader the complete algorithm for $g > 2$ using extended differential additions.

Algorithm 4.3. ***Input:*** *The basis e_1, e_2 given in theta coordinates of a maximal isotropic subgroup $K \subset A[\ell]$, a complex abelian variety of dimension 2.*
Output: *The theta null point of $B = A/K$.*

- *Fix an integer matrix F of rank r such that ${}^tFF = \ell\,\mathrm{Id}$.*
- *Compute $e_1 + e_2$ in A.*
- *Write the affine theta coordinates of $\tilde{e_1}$, $\tilde{e_2}$ and $\tilde{e_1} + \tilde{e_2}$ up to the unknown projective factors λ_1, λ_2 and $\lambda_{1,2}$ that we see as indeterminates.*
- *Use differential additions to compute the affine theta coordinates of all points of $K = \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ in $\mathbb{C}[\lambda_1, \lambda_2, \lambda_{1,2}]$.*
- *From the affine coordinates of $\ell'\tilde{e}_1$ and $(\ell'+1)\tilde{e}_1$ (where $\ell = 2\ell'+1$), recover a relation $\lambda_1^\ell = \alpha_1$. Likewise, recover relations $\lambda_2^\ell = \alpha_2$ and $\lambda_{1,2}^\ell = \alpha_{1,2}$.*
- *For all $k \in Z(n)$, let $j = (k, 0, \dots, 0)\, F^{-1}$ and compute*

$$\theta_k^B(0)\theta_0^B(0)\dots\theta_0^B(0) = \sum_{\substack{t_1,\dots,t_r \in K \\ (t_1,\dots,t_r)F = (0,\dots,0)}} \theta_{j_1}^A(t_1)\dots\theta_{j_r}^A(t_r),$$

in the ring $\mathbb{C}[\lambda_1, \lambda_2, \lambda_{1,2}]/\{\lambda_1^\ell = \alpha_1, \lambda_2^\ell = \alpha_2, \lambda_{1,2}^\ell = \alpha_{1,2}\}$. By Lemma 4.2 this is actually an element of $\mathbb{C}$.

4.2. **Computing the image of a point.** Now we explain how to compute $f(x)$ from a point $x \in A$. Actually, we fix once and for all $z \in \mathbb{C}^g$ an affine lift of x and explain how to compute $(\theta_i^B(\ell z))_{i\in Z(n)}$ (projectively). Let $Y = (\ell z, 0, \dots, 0)$ and $X = YF^{-1}$ (so that $X_1, \dots, X_r$ are integral multiples of z), let $k \in Z(n)$ and $j = (k, 0, \dots, 0)F^{-1}$. Proposition 4.1 gives

$$\theta_k^B(\ell z)\theta_0^B(0)\dots\theta_0^B(0) = \sum_{\substack{t_1,\dots,t_r \in K \\ (t_1,\dots,t_r)F = (0,\dots,0)}} \theta_{j_1}^A(X_1 + t_1)\dots\theta_{j_r}^A(X_r + t_r). \tag{7}$$

It remains to explain how to compute the $\theta_{j_\alpha}^A(X_\alpha + t_\alpha)$. As with the preceding case, we will only compute them up to unknown projective factors, and then find enough relations on these factors to be able to compute the product

$$\theta_{j_1}^A(X_1 + t_1)\dots\theta_{j_r}^A(X_r + t_r).$$

As before, we let $(\tilde{e}_i)_{i\in[1,g]}$ be the canonical basis of $\frac{1}{\ell}\mathbb{Z}^g$, and $(e_1, \dots, e_g)$ the reduced basis on K.

First, we compute $x + e_i$ using normal additions. This means that we recover the affine theta coordinates of $z + \tilde{e}_i$ up to an unknown projective factor μ_i. Then we can use differential additions (or extended differential additions) to recover the theta coordinates of $z + n_1\tilde{e_1} + \dots + n_g\tilde{e_g}$ in terms of the μ_i for any $n_1, \dots, n_g \in \mathbb{Z}$. Moreover we know that

$$\left(\theta_k^A(z + \ell\tilde{e}_i)\right)_{k\in Z(n)} = \left(\theta_k^A(z)\right)_{k\in Z(n)},$$

so we can recover from it a relation of the form $\mu_i^\ell \lambda_i^{\ell(\ell-1)} = \beta_i'$ for $i \in [1, g]$. (Remember that we know $\tilde{e}_i$ only up to the projective factor λ_i.) But since we know the value $\lambda_i^\ell = \alpha_i$, we thus recover an equation of the form $\mu_i^\ell = \beta_i$ where β_i is in $\mathbb{C}$. Now X is of the form $(a_{11}z, a_{12}z, \dots, a_{1r}z)$ if $(a_{ij})_{i,j\in[1,r]}$ are the coefficients of the matrix F^{-1}. By using differential additions we can then recover the theta coordinates of the point $X_i + n_1\tilde{e}_1 + \dots + n_g\tilde{e}_g$ for $i \in [1, g]$ up to the unknown $\{\mu_i, \lambda_i, \lambda_{ij}\ i, j \in [1, g], i \neq j\}$. But as in the preceding case, the relations we know on the μ_i, λ_i and λ_{ij} are sufficient for our purpose:

Lemma 4.4. *Let $(t_1, \dots, t_r) \in K^r$ such that $(t_1, \dots, t_r)F = (0, 0, \dots, 0)$ and let $(j_1, \dots, j_r) \in Z(n)^r$ such that $(j_1, \dots, j_r)F = (k, 0, \dots, 0)$. Note $X = (\ell z, 0, \dots, 0)F^{-1}$.*

Then, when we write the product $\theta^A_{j_1}(X_1+t_1)\dots\theta^A_{j_r}(X_r+t_r)$ in terms of the μ_i, λ_i and λ_{ij} seen as indeterminates, it lies in $\mathbb{C}[\mu_i^\ell, \lambda_i^\ell, \lambda_{ij}^\ell]$.

Proof. Let $i_0 \in Z(n)$ and T be the transformation of $\mathbb{C}[\mu_i, \lambda_i, \lambda_{ij}]$ such that $T(\mu_{i_0}) = \zeta\mu_{i_0}$ (where ζ is a ℓth-root of unity) and T leaves invariant the other generators. We let

$$u = [\ell]\left((t_1)_{i_0}, (t_2)_{i_0}, \dots, (t_r)_{i_0}\right), \quad (m_1, \dots, m_r) = (\ell, 0, \dots, 0)F^{-1}.$$

We then have

$$T(\theta^A_{j_1}(X_1+t_1)\dots\theta^A_{j_r}(X_r+t_r)) = \zeta^{(m_1u_1+\dots+m_ru_r)}\theta^A_{j_1}(X_1+t_1)\dots\theta^A_{j_r}(X_r+t_r).$$

Since we have $mF = uF = 0$ in $(\mathbb{Z}/\ell\mathbb{Z})^r$, we know (see the proof of Lemma 4.2) that $m \cdot {}^t t = 0$.

Now we let T be the transformation of $\mathbb{C}[\mu_i, \lambda_i, \lambda_{ij}]$ such that $T(\lambda_{i_0}) = \zeta\lambda_{i_0}$ and T leaves invariant the other generators. With the notations from the last paragraph, we then have

$$T(\theta^A_{j_1}(X_1+t_1)\dots\theta^A_{j_r}(X_r+t_r)) = \frac{\zeta^{u_1^2+\dots+u_r^2}}{\zeta^{m_1u_1+\dots+m_ru_r}}\theta^A_{j_1}(X_1+t_1)\dots\theta^A_{j_r}(X_r+t_r).$$

We have already seen that the numerator $\zeta^{u_1^2+\dots+u_r^2}$ and the denominator $\zeta^{m_1u_1+\dots+m_ru_r}$ are equals to one.

Finally, we fix i_0 and $j_0 \neq i_0$ in $Z(n)$ and let T be the transformation thus that $T(\lambda_{i_0,j_0}) = \zeta\lambda_{i_0,j_0}$ and T leaves invariant the other generators. Let

$$u = [\ell]\left((t_1)_{i_0}, (t_2)_{i_0}, \dots, (t_r)_{i_0}\right), \quad v = [\ell]\left((t_1)_{j_0}, (t_2)_{j_0}, \dots, (t_r)_{j_0}\right).$$

We compute:

$$T(\theta^A_{j_1}(X_1+t_1)\dots\theta^A_{j_r}(X_r+t_r)) = \zeta^{{}^t u\cdot v}\theta^A_{j_1}(X_1+t_1)\dots\theta^A_{j_r}(X_r+t_r);$$

and we have already treated this case in the proof of Lemma 4.2. □

Another small technical detail is that in the algebraic setting, we can't fix a lift $z \in \mathbb{C}^g$. The best we can do is choose an affine point $\tilde{x}$ such that $\theta_i(\tilde{x}) = \mu_0\theta_i(z)$. But we have just seen that for an affine lift z, we get a correct result. Since there are infinitely many such affine lift, corresponding to infinitely many μ_0, and the corrective factors are polynomials in μ_0, the result is correct for any affine lift.

Once again, we give the full algorithm for $g = 2$.

Algorithm 4.5. ***Input:*** *The basis e_1, e_2 given in theta coordinates of a maximal isotropic subgroup $K \subset A[\ell]$, a complex abelian variety of dimension 2, and a geometric point x of A.*
Output: *The point $f(x)$ where f is the isogeny $A \mapsto A/K$.*

- *Fix an integer matrix F of rank r such that ${}^tFF = \ell\,\mathrm{Id}$.*
- *Compute $x + e_1$ and $x + e_2$ in A.*
- *Write the affine theta coordinates of $z + \tilde{e_1}$, $z + \tilde{e_2}$ up to the unknown projective factors μ_1, μ_2 that we see as indeterminates (here z is any affine lift of x).*
- *Use (extended) differential additions to compute the affine theta coordinates of the points $z + t$ for $t \in K = \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ in $\mathbb{C}[\mu_1, \mu_2, \lambda_1, \lambda_2, \lambda_{1,2}]$. Use differential additions again to compute the points $m_iz + t$ for $i = 1, \dots, r$ where $(m_1, \dots, m_r)$ are equal to $(\ell, 0, \dots, 0)F^{-1}$.*

- *From the affine coordinates of $z+\ell\tilde{e_1}$ and z recover a relation $\mu_1^\ell=\beta_1$. Likewise, recover a relation $\mu_2^\ell=\beta_2$.*
- *For all $k\in Z(n)$, let $j=(k,0,\dots,0)\,F^{-1}$ and compute*

$$\theta_k^B(\ell\tilde{x})\theta_0^B(0)\dots\theta_0^B(0)=\sum_{\substack{t_1,\dots,t_r\in K\\(t_1,\dots,t_r)F=(0,\dots,0)}}\theta_{j_1}^A(\widetilde{m_1z+t_1})\dots\theta_{j_r}^A(m_rz+t_r),$$

in the ring $\mathbb{C}[\mu_1,\mu_2,\lambda_1,\lambda_2,\lambda_{1,2}]/\{\mu_1^\ell=\beta_1,\mu_2^\ell=\beta_2,\lambda_1^\ell=\alpha_1,\lambda_2^\ell=\alpha_2,\lambda_{1,2}^\ell=\alpha_{1,2}\}$. By Lemma 4.4 this is actually an element of $\mathbb{C}$.

4.3. **Complexity.** Our algorithms depends on many parameters:

- the dimension g of the abelian variety,
- the field k where it is defined,
- the degree ℓ of the isogeny,
- the level n of the theta structure.

The dimension g will be fixed and we assume that n is fixed (remember that in practice we use $n=2$ or $n=4$). We thus look at the complexity in ℓ (and k).

For Algorithms 4.3 and 4.5, the first important step is the computation of $O(\ell^g)$ points using differential additions (or extended differential additions). For computing the theta null point we need all the points in the kernel, so ℓ^g points, and for computing the image of a point we need $r\ell^g$ points. Let k' be the field where the geometric points of the kernel (and also the point we want to send) are defined. Then the scalars α_i and β_i from above live in k'. Since the number of coordinates, n^g, is fixed we need $O(\ell^g)$ operations in k'. (Actually we work over the algebra $k'[\lambda_i,\lambda_{ij},\mu_i]$, but by homogeneity of the addition law we only deal with monomials, so we just need to update the powers in the λ_i).

Next for changing level using Proposition 4.1, the cost is $O(\ell^{rg/2})$ operations in k'. Indeed the space of points $(t_1,\dots,t_r)\in K^r$ such that $(t_1,\dots,t_r)F=0$ is an $\mathbb{Z}/l\mathbb{Z}$-vector space of dimension $rg/2$, so we sum over $O(\ell^{rg/2})$ terms. For each such tuple, we have to reduce the corresponding monomial in the λ_i and μ_i modulo the relations $\lambda_i^\ell=\alpha_i$, $\mu_i^\ell=\beta_i$. But the highest power appearing in λ_i or μ_i is $r\ell^2$, so we just need to precompute the powers α_i, α_i^2, …, $\alpha_i^{r\ell}$. With this precomputation, for each term we then do at most $(g+g(g+1)/2)+(r-1)$ multiplications. Since $r=2$ or $r=4$, this gives the complexity $O(\ell^{rg/2})$ appearing in Theorem 1.1.

4.4. **The case of level 2.** Here we assume that the embedding given by the theta functions of level 2 is projectively normal (in particular the abelian variety is simple), so that the even theta null coordinates are non zero.

We can of course still use Proposition 4.1 in this case, so we just need to explain how we can compute the points

$$n_1\tilde{e}_1+\dots n_g\tilde{e}_g\in K_A=A/\pm 1$$

starting from the points $\tilde{e}_1,\dots,\tilde{e}_g\in K_A$. In fact, since we can still do differential additions, the only difficulty is to compute the points $\tilde{e}_i+\tilde{e}_j$. By the discussion from Section 3, we can compute $\{\tilde{e}_i\pm\tilde{e}_j\}\subset K_A$, but we need to make compatible choices. Fix an element in each of the sets $\{\tilde{e}_1\pm\tilde{e}_i\}$. Then we choose the other elements in $\{\tilde{e}_i\pm\tilde{e}_j\}$ by doing "compatible additions", as described in [21, Section 3.2.1].

For pushing a point x via the isogeny, likewise we make a choice for the set $\{x\pm e_1\}$, and we make choice for the other sets $\{x\pm e_i\}$ compatible with the choice for $x\pm e_1$ and the choice $e_1\pm e_i$.

5. Application to genus 2 curves

In this section, we apply the preceding results in the case where the abelian variety is the Jacobian of an hyperelliptic curve $\mathcal{C}$ of genus 2. To compute the isogenous curve we procede as follows:

Algorithm 5.1. ***Input:*** *A genus 2 curve $\mathcal{C}$ over a field k, a maximal isotropic subgroup K of $\mathrm{Jac}(\mathcal{C})[\ell]$.*
Output: *A curve $\mathcal{C}'$ over k such that $\mathrm{Jac}(\mathcal{C}') = \mathrm{Jac}(\mathcal{C})/K$.*

- *Find a basis of K in Mumford's coordinates.*
- *Find a Rosenhain equation of the curve $\mathcal{C}$.*
- *Use Thomae's formulae to compute the 4th power of theta constants of level n of the corresponding abelian variety $A_{k''}$ (Section 5.1).*
- *Extract the roots to get the theta constants (Section 5.1).*
- *Send the basis of K in $A_{k''}$ (Section 5.3 and the appendix).*
- *Apply algorithms 4.3 and 4.5 to get the theta constants of the isogenous abelian variety $B_{k''}$.*
- *Recover a Rosenhain form of $\mathcal{C}'$ (Section 5.2).*
- *If needed, apply Mestre's algorithm to recover a rational equation of $\mathcal{C}'$.*

We want to compute an ℓ-isogeny between $\mathrm{Jac}(\mathcal{C})$ and $\mathrm{Jac}(\mathcal{C}')$ where the points are represented by their Mumford's polynomials. We compute the following commutative diagram where points on the abelian varieties A and B are given by theta functions of level n. Remember that for arithmetic reasons we use $n = 4$ or $n = 2$ if we work on the Kummer variety.

$$\begin{array}{ccc} A_{k''} & B_{k''} & \text{thetas of level } n \\ \simeq & \simeq & \\ \mathrm{Jac}_k(\mathcal{C}) & \mathrm{Jac}_k(\mathcal{C}') & \text{Mumford's coordinates} \end{array}$$

In Section 5.4, we insist on the rationality of the process. Finally, we look at the complexity of computing isogenies in Section 5.5 and give an exemple of computation.

These sections heavily use the following formulae which link the thetas of level 2 with the squares of the thetas of level $(2,2)$: for all $a, b \in \frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$,

$$4\Theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega)^2 = \sum_{\beta \in \frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2} (-1)^{4^t a\beta} \Theta\left[\begin{smallmatrix} 0 \\ b+\beta \end{smallmatrix}\right]\left(z, \frac{\Omega}{2}\right) \Theta\left[\begin{smallmatrix} 0 \\ \beta \end{smallmatrix}\right]\left(0, \frac{\Omega}{2}\right)$$

$$\Theta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right]\left(z, \frac{\Omega}{2}\right) \Theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]\left(0, \frac{\Omega}{2}\right) = \sum_{\alpha \in \frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2} \Theta\left[\begin{smallmatrix} \alpha \\ b \end{smallmatrix}\right](z,\Omega)^2$$

Note that the theta functions of level $(2,2)$ are evaluated at z and not at $2z$.

To have compact formulae we number the theta functions of level 4 as given in the appendix (we follow Dupont [8]). Moreover, for the theta constants, we omit the argument 0 and write Θ_i instead of $\Theta_i(0)$.

5.1. **Computing theta constants from the equation of the curve.** Let $\mathcal{C}$ be an hyperelliptic curve of genus 2 given by the equation $y^2 = f(x)$ over $\mathbb{C}$. Thomae's formulae [29, III.8] give relations between the roots of f and the fourth power of the theta constants of level $(2,2)$ with period matrix Ω associated to $\mathcal{C}$.

For instance, assumes that the curve is in Rosenhaim form

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

then the ordering $\{0,1,\lambda,\mu,\nu\}$ leads to the following relations:

$$\begin{array}{lcllcl}
\left(\frac{\Theta_4}{\Theta_0}\right)^4 & = & \frac{\mu}{\lambda\nu} & \left(\frac{\Theta_8}{\Theta_0}\right)^4 & = & \frac{\mu(\nu-1)(\lambda-\mu)\mu}{\nu(\mu-1)(\lambda-\nu)} \\
\left(\frac{\Theta_1}{\Theta_0}\right)^4 & = & \frac{\mu(\nu-1)(\lambda-1)}{\lambda\nu(\mu-1)} & \left(\frac{\Theta_2}{\Theta_0}\right)^4 & = & \frac{\mu(\lambda-1)(\nu-\mu)}{\lambda(\mu-1)(\nu-\lambda)}
\end{array}$$

We keep this choice for the rest of the paper. Note that another choice of ordering leads to an isomorphic variety (over $\mathbb{C}$). In previous work [13] the ordering $\{\nu,\mu,\lambda,1,0\}$ was used but this choice implies the use of $\sqrt{-1}$ which is not the case with our ordering.

To get the equations defining the abelian variety A, we need to know how to take the roots in Thomae's formulae. Of course this is easy if we are in a subfield of $\mathbb{C}$ since we can evaluate the theta constants. However, this cannot be done in finite fields.

Since we are only interested in finding an abelian variety $A_{k''}$ (given by theta constants of level n) isomorphic to the Jacobian of the curve, we can choose $A_{k''}$ up to isomorphism.

A matrix $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ in the group $\mathrm{Sp}(4,\mathbb{Z})$ acts on $\mathbb{C}^2 \times \mathcal{H}_2$ in the following way

$$\begin{array}{ccccc}
\mathbb{C}^2 \times \mathcal{H}_2 & \longrightarrow & \mathbb{C}^2 \times \mathcal{H}_2 & & \\
(z,\Omega) & \longmapsto & (\gamma.z, \gamma.\Omega) & = & \left({}^t\left(C\Omega+D\right)^{-1} z, \left(A\Omega+B\right)\left(C\Omega+D\right)^{-1}\right)
\end{array}$$

This action defines an isomorphism between the two tori:

$$\begin{array}{ccc}
\mathbb{C}^2/\left(\Omega\mathbb{Z}^2+\mathbb{Z}^2\right) & \simeq & \mathbb{C}^2/\left(\gamma.\Omega\mathbb{Z}^2+\mathbb{Z}^2\right) \\
z & \mapsto & \gamma.z
\end{array}$$

On the other hand, each isomorphism between two tori comes from a matrix γ in $\mathrm{Sp}(4,\mathbb{Z})$. The only matrix $\gamma \in \mathrm{Sp}(4,\mathbb{Z})$ such that $\gamma.\Omega = \Omega$ for all $\Omega \in \mathcal{H}_2$ are the matrices $\gamma = \pm \mathrm{Id}_4$. The matrix $-\mathrm{Id}_4$ acts on $\mathbb{C}^2/\left(\Omega\mathbb{Z}^2+\mathbb{Z}^2\right)$ by the automorphism $z \mapsto -z$ and the equation of A is invariant under this automorphism, thus we will identify γ with $-\gamma$.

We will need the following subgroups of $\mathrm{Sp}(4,\mathbb{Z})$:

$$\Gamma'(n) = \Gamma'(n,n) = \{\gamma \in \mathrm{Sp}(4,\mathbb{Z}),\ \gamma \equiv \pm\mathrm{Id}_4\ [n]\}$$

$$\Gamma'(n,2n) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma'(n),\ \mathrm{diag}\left({}^tAC\right) \equiv \mathrm{diag}\left({}^tBD\right) \equiv 0\ [2n] \right\}$$

Note that $\Gamma'(n)$ corresponds to the group of isomorphisms which fix the n-torsion of the torus modulo the automorphism $z \mapsto -z$. Let's study the action of these groups on the theta constants of level n for n even. Mumford [28] showed that for $\gamma \in \Gamma'(1,2)$ it is given by

$$\Theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](\gamma.z,\gamma.\Omega) = \Theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z,\Omega) C_\gamma \exp\left(\pi i^t \left(C\Omega+D\right)^{-1} Cz\right)$$

where C_γ is a complex number which depends only on γ and Ω. for characteristics (a,b) in $\frac{1}{n}\mathbb{Z}^4/\mathbb{Z}^4$ and for $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ in $\Gamma'(n)$ we put $z = \gamma^{-1}.(\Omega a + b)$ in the preceding equation to obtain

$$\frac{\Theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0,\gamma.\Omega)}{\Theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0,\gamma.\Omega)} = \frac{\Theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0,\Omega)}{\Theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0,\Omega)} \exp\left(\pi i^t a^t DBa - \pi i^t b^t ACb - 2\pi i^t a(A - \mathrm{Id})b\right)$$

In fact an element γ not in $\Gamma'(n)$ does not preserve the characteristics of the theta constants in the quotient. Thus $\Gamma'(n)$ is exactly the group of isomorphisms which fix the $2n$-th power of the theta constants of level (n,n) (modulo a constant), $\Gamma'(n,2n)$ the n-th power and $\Gamma'(n^2,2n^2)$ the theta constants of level (n,n).

The choice of the ordering of the roots of the hyperelliptic polynomial corresponds to the choice of a numbering of the two-torsion, thus of a fixed class in $\Gamma'(1)/\Gamma'(2)$. With the possible use of an element of $\Gamma'(2)/\Gamma'(2,4)$ we can take the square roots of the following quotients in an arbitrary way:

$$\left(\frac{\Theta_1}{\Theta_0}\right)^4, \quad \left(\frac{\Theta_2}{\Theta_0}\right)^4, \quad \left(\frac{\Theta_4}{\Theta_0}\right)^4, \quad \left(\frac{\Theta_8}{\Theta_0}\right)^4.$$

The other squares of theta constants of level $(2,2)$ are given by the formulae:

$$\begin{array}{rclcrcl} \Theta_6^2 &=& \frac{1}{\nu}\frac{\Theta_0^2\Theta_2^2}{\Theta_4^2} & & \Theta_{12}^2 &=& \frac{1}{\lambda}\frac{\Theta_0^2\Theta_8^2}{\Theta_4^2} \\ \Theta_3^2 &=& (\nu-1)\frac{\Theta_4^2\Theta_6^2}{\Theta_1^2} & & \Theta_9^2 &=& (\lambda-1)\frac{\Theta_4^2\Theta_{12}^2}{\Theta_1^2} \end{array}$$

$$\Theta_{15}^2 = \frac{\Theta_0^2\Theta_3^2 - \Theta_1^2\Theta_2^2}{\Theta_{12}^2}.$$

For each quotient $\Theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]^2/\Theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]^2$ with a,b in $(\frac{1}{2}\mathbb{Z}^2)/\mathbb{Z}^2$, there exists an element of $\Gamma'(2,4)/\Gamma'(4,8)$ witch changes its sign but leaves invariant the other quotients (Note that this works because some theta constants are zero). Therefore to get the variety A in level 4 we can take arbitrary square roots of each quotient.

5.2. **Computing the equation of the curve from theta constants.** From the squares of the theta constants of level $(2,2)$, the underlying hyperelliptic curve is given by the equation

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

with

$$\lambda = \frac{\Theta_0^2\Theta_8^2}{\Theta_4^2\Theta_{12}^2}, \qquad \mu = \frac{\Theta_8^2\Theta_2^2}{\Theta_{12}^2\Theta_6^2}, \qquad \nu = \frac{\Theta_2^2\Theta_0^2}{\Theta_6^2\Theta_4^2}.$$

5.3. **Maps between abelian varieties and Jacobians.** We need to link divisors in the Jacobian of the curve (given by their Mumford's coordinates) and points on the abelian variety given by theta functions of level n. The formulae are given in the appendix. They come from Mumford [29] and Van Wamelen [38].

Of course, it is not possible to compute v from the theta of level 2. In fact only its square is computable. This is coherent with the fact that level 2 corresponds to the Kummer variety.

For the level $n = 4$, we still have to find the value of $c_{1,2}\sqrt{a_2 - a_1}$ in the formulae of the appendix. With our numbering of the roots of the hyperelliptic polynomial, $\sqrt{a_2 - a_1} = \sqrt{1-0}$ can be chosen to be 1. The constant $c_{1,2}$ is just a sign and corresponds to the action of the automorphism $P \mapsto -P$ in the abelian variety.

Thus it can be chosen arbitrary. Over $\mathbb{C}$ the choice of this sign corresponds to the choice of the orientation of the paths used to compute the Abel-Jacobi map.

5.4. **Rationality considerations.** Although the process of computing isogenies can be made rational, our algorithms clearly use arithmetic in fields extension. The first extension comes from the fact that an abelian variety of level n associated to a given curve cannot be defined on the same field as the curve. If the base field is k, we will denote k'' the extension where the theta null point of level n lives. Then if P is a rational point on the Jacobian, its theta coordinates will live in k''. If the curve is defined over a finite field then the arithmetic must be performed in an extension field of degree at most 2 if $n = 2$ or 4 if $n = 4$. This requires to find quadratic non-residues.

In particular, if one is interested in computing all the isogenous curves, he must compute the possible kernels of the isogeny as a rational subgroup of $\mathrm{Jac}(\mathcal{C})$ and not as rational subgroup of A (where we can only look at k''-rational isogenies). Thus for computing chains of isogenies, one must always return to the curves in Weierstrass form for the isogenies to be rational.

The second extension comes from the fact that for the isogeny algorithm we work over the field of definition of the theta coordinates of the points of the kernel. If the points live in an extension k' of k, then by the above discussion, their theta coordinates will live in the composite extension of k' and k'' over k. Since the result of the isogeny computation of Section 4 give elements of k'', it should be possible to not take this extension by decomposing the right side member of (5) as elementary symmetric functions on the points of the kernel..

With our method, we compute the Rosenhain invariants of the isogenous curves. Hence, as remarked above, its equation may not be on the same base field as the original curve. To avoids this we can compute its absolute invariants which are elements of the base field since the isogenous curve is defined over the same field as the curve. With Mestre's algorithm [24], an equation over the base field can be found. It remains to find an isomorphism between the two equations and to push the points.

In the case where the two-torsion is rational on the first curve, the two-torsion will be rational on the isogenous curve (the degree ℓ of the isogeny being odd). Thus the isogenous curve admits an equation in Rosenhain form over the base field. In this case we don't need Mestre's algorithm since our algorithm returns the correct curve.

5.5. **Complexity.** Let $\mathcal{C}$ be an hyperelliptic curve of genus 2 over a field k. Assume that we are given a rational isotropic subgroup K of the ℓ-torsion defined by two generators in Mumford coordinates (possibly over an extension field). The cost of computing the abelian variety A of level n associated to $\mathcal{C}$ and of sending the two generators of K and their sum can be done in $O(1)$. Computing the abelian variety $B = A/K$ is $O(\ell^r)$ operations in the composite field k_0 of the field of definition k' of the geometric points of K and k'' (notations as in the Section 5.4). Finally the reconstruction of the isogenous curve is $O(1)$.

However, k'' is the field of definition of the theta null point of level n of A. Since the theta null point is rational when the $2n$-torsion is, the degree of this extension is bounded by a function of n. For instance, over a finite field it is bounded by $(2n)^{2g}$.

Since n (and g) are fixed, this means that computing B/K can be done in $O(\ell^r)$ operations in k'.

For sending a point between two Jacobians, the cost of the morphisms is also a $O(1)$ while the cost of pushing the point between A and B is $O(\ell^r)$ operations in k_0 (and thus in k').

Lastly, if $\mathcal{C}$ is defined over a finite field k and K is rational, then the field k' where the geometric points of K are defined lie in an extension of degree at most $\ell^2 - 1$ of k. This concludes the proof of Theorem 1.2. (We can even bound the extension degree by $\ell - 1$ when ℓ is splits completely in the endomorphism ring of the Jacobian).

5.6. **Implementations.** Together with Gaetan Bisson we have implemented the computation of ℓ-isogenies in a Magma package called AVIsogenies (it can be found at http://avisogenies.gforge.inria.fr/). To have an efficient implementation we designed some specific codes for genus 2 and level 2. In particular, it avoids taking some of the field extensions.

For instance, take the hyperelliptic curve:

$$y^2 = x^5 + 41691x^4 + 24583x^3 + 2509x^2 + 15574x$$

over the finite field $\mathbb{F}_{42179}$. The cardinality of the Jacobian is $2^{10}1321^2$ and there is one rational isotropic subgroup K of $\ell = 1321$ torsion. The isogenous curve with respect to K is

$$y^2 = 33266x^6 + 20155x^5 + 31203x^4 + 9732x^3 + 4204x^2 + 18026x + 29732$$

The computation took around two hours on a core 2 with 32 GB of RAM. This exemple was specifically chosen so that the theta null point of level 2 is rational over the base field, and also all the geometric points in the kernel. Thus we avoided some intermediate field extensions. Taking a field extension would increase the computation by a quadratic or linear factor (depending on whether asymptotically fast algorithms are used for the arithmetic).

Even if the morphisms are $O(1)$ in theory, we saw that in practice their computations are not negligible. This is especially the case when ℓ is small: most of the time is spend by converting points from Mumford's coordinates to theta coordinates.

6. Conclusion

In Section 4, we have explained how to compute isogenies between abelian varieties described by theta coordinates of level n. In fact, the algorithms from this section can be seen as a composition from the algorithms of [21], which describe the isogeny with theta functions of level n on the domain, and theta functions of level ℓn on the codomain, and an algorithm to convert from level ℓn theta functions to level n theta functions induced by Koizumi's addition formulae. The techniques developed in this paper also allow to convert from level n theta coordinates to level ℓn theta coordinates (provided that we know the level n coordinates of the points of ℓ-torsion), thus an easy adaptation of Algorithm 4.3 gives a method to convert between theta functions of different level. More details on this method can be found in [32, Section 7.8].

One drawback of Theorems 1.1 and 1.2 is that they apply only to maximal isotropic kernels. When we look at isogenies graphs in genus 2 for instance, we do not always recover the full isogenies graphs by only looking at (ℓ, ℓ)-isogenies.

It would be interesting to relax this condition of maximality, and in particular to obtain an algorithm to compute an isogeny with a cyclic kernel. The major difficulty of looking at isogenies whose kernel is not maximally isotropic is that the pullback of the polarisation by this isogeny is much harder to describe algebraically.

Appendix A. Explicit formulae for the conversion between Mumford and theta coordinates

A.1. **Numbering.**

$$\begin{aligned}
\Theta_0(z) &= \Theta\begin{bmatrix}(0\ 0)\\(0\ 0)\end{bmatrix}(z,\Omega), & \Theta_1(z) &= \Theta\begin{bmatrix}(0\ 0)\\(\frac12\ 0)\end{bmatrix}(z,\Omega),\\
\Theta_2(z) &= \Theta\begin{bmatrix}(0\ 0)\\(0\ \frac12)\end{bmatrix}(z,\Omega), & \Theta_3(z) &= \Theta\begin{bmatrix}(0\ 0)\\(\frac12\ \frac12)\end{bmatrix}(z,\Omega),\\
\Theta_4(z) &= \Theta\begin{bmatrix}(\frac12\ 0)\\(0\ 0)\end{bmatrix}(z,\Omega), & \Theta_5(z) &= \Theta\begin{bmatrix}(\frac12\ 0)\\(\frac12\ 0)\end{bmatrix}(z,\Omega),\\
\Theta_6(z) &= \Theta\begin{bmatrix}(\frac12\ 0)\\(0\ \frac12)\end{bmatrix}(z,\Omega), & \Theta_7(z) &= \Theta\begin{bmatrix}(\frac12\ 0)\\(\frac12\ \frac12)\end{bmatrix}(z,\Omega),\\
\Theta_8(z) &= \Theta\begin{bmatrix}(0\ \frac12)\\(0\ 0)\end{bmatrix}(z,\Omega), & \Theta_9(z) &= \Theta\begin{bmatrix}(0\ \frac12)\\(\frac12\ 0)\end{bmatrix}(z,\Omega),\\
\Theta_{10}(z) &= \Theta\begin{bmatrix}(0\ \frac12)\\(0\ \frac12)\end{bmatrix}(z,\Omega), & \Theta_{11}(z) &= \Theta\begin{bmatrix}(0\ \frac12)\\(\frac12\ \frac12)\end{bmatrix}(z,\Omega),\\
\Theta_{12}(z) &= \Theta\begin{bmatrix}(\frac12\ \frac12)\\(0\ 0)\end{bmatrix}(z,\Omega), & \Theta_{13}(z) &= \Theta\begin{bmatrix}(\frac12\ \frac12)\\(\frac12\ 0)\end{bmatrix}(z,\Omega),\\
\Theta_{14}(z) &= \Theta\begin{bmatrix}(\frac12\ \frac12)\\(0\ \frac12)\end{bmatrix}(z,\Omega), & \Theta_{15}(z) &= \Theta\begin{bmatrix}(\frac12\ \frac12)\\(\frac12\ \frac12)\end{bmatrix}(z,\Omega).
\end{aligned}$$

A.2. **Notations.** In this section we recall some notations of Van Wamelen [38] which we apply in the genus 2 case. Assume that the roots of f (which is of degree 5) are numbered: $\{a_1,\dots,a_5\}$. Let

$$\begin{aligned}
\eta_1 &= \left[\tfrac12,0;0,0\right] & \eta_2 &= \left[\tfrac12,0;\tfrac12,0\right] & \eta_3 &= \left[0,\tfrac12;\tfrac12,0\right]\\
\eta_4 &= \left[0,\tfrac12;\tfrac12,\tfrac12\right] & \eta_5 &= \left[0,0;\tfrac12,\tfrac12\right] & \eta_\infty &= \left[0,0;0,0\right]
\end{aligned}$$

For a subset S in $\{1,\dots,5,\infty\}$, we set

$$\eta_S = \sum_{i\in S}\eta_i$$

We define η'_S and η''_S to be the first and second part of η_S. This notation comes from the fact that the divisor $\sum_{i\in S}a_i - \#S(\infty)$ is mapped to $\Omega\eta'_S+\eta''_S$ by the Abel-Jacobi map.

All theta functions of level $(2,2)$ can be written as $\Theta\left[\eta_{UoA}\right]$ with $U=\{1,3,5\}$ and a subset A of $\{1,\dots,5\}$ of odd cardinality where o denote the symmetric difference of two sets. For each such subset, Van Wamelen defines (definition 3) the function $t_A(z)$ to be $t_A(z)=f_A\Theta\left[\eta_{UoA}\right](z)$ where f_A is a constant which is $f_A=\Theta\left[0\right]/\Theta\left[\eta_{UoA}\right]$ for the even functions (i.e. $\#A=3$) and for the others

$$\begin{aligned}
f_1 &= \tfrac{-1}{\sqrt{a_2-a_1}}\tfrac{\Theta_0\Theta_4\Theta_6\Theta_{12}}{\Theta_1\Theta_3\Theta_9\Theta_{15}} & f_2 &= \tfrac{-1}{\sqrt{a_2-a_1}}\tfrac{\Theta_4\Theta_6\Theta_{12}}{\Theta_2\Theta_8\Theta_{15}}\\
f_3 &= \tfrac{-1}{\sqrt{a_2-a_1}}\tfrac{\Theta_0\Theta_6}{\Theta_2\Theta_3} & f_4 &= \tfrac{1}{\sqrt{a_2-a_1}}\tfrac{\Theta_4}{\Theta_1}\\
f_5 &= \tfrac{-1}{\sqrt{a_2-a_1}}\tfrac{\Theta_0\Theta_{12}}{\Theta_8\Theta_9} & f_{\{1,2,3,4,5\}} = f_\emptyset &= \tfrac{-1}{\sqrt{a_2-a_1}^3}\tfrac{\Theta_4^2\Theta_6^2\Theta_{12}^2}{\Theta_1\Theta_2\Theta_3\Theta_8\Theta_9\Theta_{15}}
\end{aligned}$$

Note that we made a choice of the sign of the last six f_A. If A is not of even cardinality, we write t_A and f_A instead of t_{A^c} and f_{A^c} where A^c denotes the complement set of A in $\{1,\dots,5\}$. We have the following Theorem:

Theorem A.1. *Let $D = P_1 + P_2 - 2(\infty)$ be a non theta divisor which corresponds to a vector $z \in \mathbb{C}^2/(\Omega\mathbb{Z}^2 + \mathbb{Z}^2)$. Let (x_i, y_i) be the coordinates of the point P_i. Write (u, v) for the Mumford's polynomials of D. For $k \in \{1,\dots,5\}$, and l, m two distinct elements of $\{1,\dots,5\} \setminus \{k\}$ we have*

$$U(a_k) = \frac{t_k^2(z)}{t_\emptyset^2(z)}, \qquad V(a_k) = \frac{Y_{k,m} - Y_{k,l}}{a_l - a_m},$$

$$Y_{l,m} := \frac{y_1(x_2 - a_l)(x_2 - a_m) - y_2(x_1 - a_l)(x_1 - a_m)}{x_2 - x_1} = c_{1,2}\frac{t_l(z)t_m(z)t_{\{l,m\}}(z)}{t_\emptyset^3(z)}$$

where $c_{1,2}$ is just a sign ± 1.

This is Theorems 4, 5, 6 and 7 of Van Wamelen. By using a similar argument as in the proof of Theorem 6 for $Y_{l,m}Y_{l,k}$ instead of $Y_{l,m}^2$, we can compute the products $c_{l,m}c_{l,k}$ (where $c_{i,j}$ are the signs in Wamelen's theorems) in terms of theta constants. With our choice of constants f_A, we find that $c_{i,j} = c_{1,2}$. With (almost) the same proof as Van Wamelen we have

Theorem A.2. *With the previous notations and choices,*

$$Y := y_1y_2 = \prod_{l=1}^{5} \frac{t_l(z)}{t_\emptyset(z)}$$

Non generic divisors D can easily be recognized in Mumford's coordinates (u, v). Let z be the image of D by the Abel-Jacobi map. Let Θ be the set of all theta divisors in the Jacobian,

$$D \in \Theta \iff \deg(u) \leq 1 \iff t_\emptyset(z) = 0 \iff \Theta_{14}(z) = 0.$$

$$D \in \Theta + (a_k - (\infty)) \iff u(a_k) = 0 \iff t_k(z) = 0 \iff \Theta\left[\eta_{U\circ\{k\}}\right](z) = 0.$$

In particular, in genus 2, if the divisor is not of two torsion then not two odd theta functions are zero.

A.3. **From theta to Mumford.** Let $\mathcal{C}$ be the hyperelliptic curve $y^2 = f(x)$. Write a_i for the roots of f with a choice of an ordering. Assume that the divisor D in $\mathrm{Jac}(\mathcal{C}) \setminus \Theta$ is given by the mean of theta functions of level n with $n = 2$ or $n = 4$.

The following formulae allow to compute u, v by using Lagrange interpolation.

$$u(a_1) = (a_2 - a_1)^2 \frac{\Theta_0^2\Theta_2^2\Theta_8^2}{\Theta_4^2\Theta_6^2\Theta_{12}^2} \frac{\Theta_{10}(z)^2}{\Theta_{14}(z)^2}, \qquad u(a_2) = (a_2 - a_1)^2 \frac{\Theta_1^2\Theta_3^2\Theta_9^2}{\Theta_4^2\Theta_6^2\Theta_{12}^2} \frac{\Theta_{11}(z)^2}{\Theta_{14}(z)^2}.$$

$$v(a_1) = \frac{1}{a_3 - a_2}\left(Y_{1,2} - Y_{1,3}\right), \qquad v(a_2) = \frac{1}{a_3 - a_1}\left(Y_{1,2} - Y_{2,3}\right).$$

Applying the previous theorem, we have

$$\begin{aligned}
Y_{1,2} &= c_{1,2}\sqrt{a_2-a_1}^7\,\frac{\Theta_0^2\Theta_1^2\Theta_2^2\Theta_3^2\Theta_8^2\Theta_9^2}{\Theta_4^4\Theta_6^4\Theta_{12}^4}\,\frac{\Theta_{10}(z)\Theta_{11}(z)\Theta_{15}(z)}{\Theta_{14}(z)^3},\\
Y_{1,3} &= c_{1,2}\sqrt{a_2-a_1}^7\,\frac{\Theta_0^3\Theta_1^2\Theta_2^2\Theta_8^3\Theta_9^2\Theta_{15}^2}{\Theta_4^5\Theta_6^4\Theta_{12}^5}\,\frac{\Theta_3(z)\Theta_7(z)\Theta_{10}(z)}{\Theta_{14}(z)^3},\\
Y_{2,3} &= c_{1,2}\sqrt{a_2-a_1}^7\,\frac{\Theta_0^2\Theta_1^2\Theta_3^3\Theta_8^2\Theta_9^3\Theta_{15}^2}{\Theta_4^5\Theta_6^4\Theta_{12}^5}\,\frac{\Theta_2(z)\Theta_7(z)\Theta_{11}(z)}{\Theta_{14}(z)^3}.
\end{aligned}$$

The products of theta functions involved can be computed from the theta of level 4 by:

$$\begin{aligned}
4\Theta_{14}(z)^4 &= \Theta_0(2z)\Theta_0^3-\Theta_1(2z)\Theta_1^3-\Theta_2(2z)\Theta_2^3+\Theta_3(2z)\Theta_3^3+\Theta_4(2z)\Theta_4^3\\
&\quad -\Theta_6(2z)\Theta_6^3-\Theta_8(2z)\Theta_8^3+\Theta_9(2z)\Theta_9^3-\Theta_{12}(2z)\Theta_{12}^3-\Theta_{15}(2z)\Theta_{15}^3.
\end{aligned}$$

$$\begin{aligned}
4\Theta_{10}(z)^2\Theta_{14}(z)^2 &= \Theta_0(2z)\Theta_0\Theta_4^2+\Theta_4(2z)\Theta_4\Theta_0^2-\Theta_2(2z)\Theta_2\Theta_6^2\\
&\quad -\Theta_6(2z)\Theta_6\Theta_2^2-\Theta_8(2z)\Theta_8\Theta_{12}^2-\Theta_{12}(2z)\Theta_{12}\Theta_8^2,\\
4\Theta_{11}(z)^2\Theta_{14}(z)^2 &= \Theta_1(2z)\Theta_1\Theta_4^2+\Theta_4(2z)\Theta_4\Theta_1^2-\Theta_3(2z)\Theta_3\Theta_6^2\\
&\quad -\Theta_6(2z)\Theta_6\Theta_3^2-\Theta_9(2z)\Theta_9\Theta_{12}^2-\Theta_{12}(2z)\Theta_{12}\Theta_9^2.
\end{aligned}$$

$$\begin{aligned}
4\Theta_{10}(z)\Theta_{11}(z)\Theta_{14}(z)\Theta_{15}(z) &= \Theta_5(2z)\Theta_0\Theta_1\Theta_4-\Theta_7(2z)\Theta_2\Theta_3\Theta_6\\
&\quad -\Theta_{13}(2z)\Theta_8\Theta_9\Theta_{12},\\
4\Theta_4(z)\Theta_7(z)\Theta_{10}(z)\Theta_{14}(z) &= \Theta_5(2z)\Theta_1\Theta_8\Theta_{12}-\Theta_{11}(2z)\Theta_2\Theta_6\Theta_{15}\\
&\quad -\Theta_{13}(2z)\Theta_0\Theta_4\Theta_9,\\
4\Theta_2(z)\Theta_7(z)\Theta_{11}(z)\Theta_{14}(z) &= \Theta_5(2z)\Theta_0\Theta_9\Theta_{12}-\Theta_{10}(2z)\Theta_3\Theta_6\Theta_{15}\\
&\quad -\Theta_{13}(2z)\Theta_1\Theta_4\Theta_8.
\end{aligned}$$

From the theta functions of level 2 we can compute the $\Theta_i(z)^2$ and thus find the polynomial u. Since we have quotiented the abelian variety by $\{\pm 1\}$, we can't recover v but only its square. The formulae for $Y_{1,2}^2$, $Y_{1,3}^2$ and $Y_{2,3}^2$ involve only squares. It remains to compute the products $Y_{1,2}Y_{1,3}$, $Y_{1,2}Y_{2,3}$ and $Y_{1,3}Y_{2,3}$ and thus we need the following products of theta functions:

$$\begin{aligned}
\Theta_3(z)\Theta_7(z)\Theta_{11}(z)\Theta_{15}(z)\Theta_0\Theta_4\Theta_8\Theta_{12} &= -\Theta_0(z)^2\Theta_3(z)^2\Theta_0^2\Theta_3^2\\
&\quad +\Theta_3(z)^2\Theta_{15}(z)^2\Theta_0^2\Theta_{12}^2+\Theta_0(z)\Theta_1(z)\Theta_2(z)\Theta_3(z)\Theta_0\Theta_1\Theta_2\Theta_3,
\end{aligned}$$

$$\begin{aligned}
\Theta_2(z)\Theta_{10}(z)\Theta_{14}(z)\Theta_{15}(z)\Theta_1\Theta_4\Theta_9\Theta_{12} &= \Theta_1(z)^2\Theta_2(z)^2\Theta_1^2\Theta_2^2\\
&\quad +\Theta_2(z)^2\Theta_{15}(z)^2\Theta_1^2\Theta_{12}^2-\Theta_0(z)\Theta_1(z)\Theta_2(z)\Theta_3(z)\Theta_0\Theta_1\Theta_2\Theta_3,
\end{aligned}$$

$$\begin{aligned}
\Theta_2(z)\Theta_3(z)\Theta_{10}(z)\Theta_{11}(z)\Theta_0\Theta_1\Theta_8\Theta_9 &= \Theta_2(z)^2\Theta_3(z)^2\Theta_0^2\Theta_1^2\\
&\quad -\Theta_0(z)\Theta_1(z)\Theta_2(z)\Theta_3(z)\Theta_0\Theta_1\Theta_2\Theta_3.
\end{aligned}$$

If we write x,y,z,t for $\Theta_0(z),\Theta_1(z),\Theta_2(z),\Theta_3(z)$ and a,b,c,d for the corresponding theta constants then

$$\begin{aligned}
2E'abcd\,xyzt &= F(x^2t^2+y^2z^2)+G(x^2z^2+y^2t^2)+H(x^2y^2+z^2t^2)\\
&\quad -(x^4+y^4+z^4+t^4)
\end{aligned}$$

where

$$\begin{aligned} A' &= a^2+b^2+c^2+d^2, & B' &= a^2+b^2-c^2-d^2,\\ C' &= a^2-b^2+c^2-d^2, & D' &= a^2-b^2-c^2+d^2, \end{aligned}$$

$$E' = \frac{A'B'C'D'}{(a^2d^2-b^2c^2)(a^2c^2-b^2d^2)(a^2b^2-c^2d^2)},$$

$$\begin{aligned} F &= (a^4-b^4-c^4+d^4)/(a^2d^2-b^2c^2),\\ G &= (a^4-b^4+c^4-d^4)/(a^2c^2-b^2d^2),\\ H &= (a^4+b^4-c^4-d^4)/(a^2b^2-c^2d^2). \end{aligned}$$

A.4. **From Mumford to Theta.** Let $D = \sum_{i=1}^g P_i - gP_\infty$ be a divisor in $\mathrm{Jac}(\mathcal{C})$ corresponding to $z \in \mathbb{C}^2/(\Omega\mathbb{Z}^2+\mathbb{Z}^2)$. Assume that D is given by its Mumford's coordinates (u,v) (or u and v^2 if we work on the Kummer surface). As before, we assume here that the divisor is generic. Note that we work with projective coordinates so we only want the theta functions of level n up to a constant factor (which will be $1/\Theta_{14}(z)$ for $n=2$ and $1/\Theta_{14}(z)^4$ for $n=4$).

From v^2 it is possible to compute the squares of the $Y_{i,j}$ since the formulae defining $Y_{i,j}^2$ can be made algebraic in terms of the coefficient of u and v^2. By evaluating u at the root of f, we obtain formulae for all the $\Theta_i(z)^2/\Theta_{14}(z)^2$ with $0 \le i \le 15$. If we want the theta of level 2 we are done.

For level $n=4$, we can invert the previous formulae and use the Frobenius relations. A more natural way is to use the doubling formulae [13]:

$$4\Theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2z)\,\Theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\Theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]^2 = \sum_{\alpha,\beta\in\frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2} \exp\left(-4i\pi^t a\beta\right)\Theta\left[\begin{smallmatrix}a+\alpha\\b+\beta\end{smallmatrix}\right](z)^2\,\Theta\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right](z)^2$$

$$4\Theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2z)\,\Theta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right]\Theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\Theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]$$

$$= \sum_{\alpha,\beta\in\frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2} \exp\left(-4i\pi^t a\beta\right)\Theta\left[\begin{smallmatrix}a+\alpha\\b+\beta\end{smallmatrix}\right](z)\,\Theta\left[\begin{smallmatrix}a+\alpha\\\beta\end{smallmatrix}\right](z)\,\Theta\left[\begin{smallmatrix}\alpha\\b+\beta\end{smallmatrix}\right](z)\,\Theta\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right](z).$$

The first formula allows to recover the even theta functions. For the odd theta functions, we will use the second formula. The products on the right side can be expressed in terms of the constants f_A and the functions $Y_{l,m}$, Y and $u(a_i)$. Since we need to divide by some $u(a_i)$, we make the hypothesis that the divisor is not of 2-torsion.

For instance,

$$\begin{aligned}
\Theta_{14}(2z)\Theta_0\Theta_2\Theta_{12} &= \Theta_0(z)\Theta_2(z)\Theta_{12}(z)\Theta_{14}(z) - \Theta_5(z)\Theta_7(z)\Theta_9(z)\Theta_{11}(z)\\
&\quad +\Theta_4(z)\Theta_6(z)\Theta_8(z)\Theta_{10}(z) - \Theta_1(z)\Theta_3(z)\Theta_{13}(z)\Theta_{15}(z)\\
\Theta_{14}(2z)\Theta_0\Theta_2\Theta_{12} &= \frac{t_{2,4}(z)t_{2,3}(z)t_{3,4}(z)t_\emptyset(z)}{f_{2,4}f_{2,3}f_{3,4}f_\emptyset} + \frac{t_{1,5}(z)t_2(z)t_4(z)t_3(z)}{f_{1,5}f_2f_4f_3}\\
&\quad + \frac{t_{3,5}(z)t_{4,5}(z)t_{2,5}(z)t_1(z)}{f_{3,5}f_{4,5}f_{2,5}f_1} + \frac{t_{1,3}(z)t_{1,4}(z)t_{1,2}(z)t_5(z)}{f_{1,3}f_{1,4}f_{1,2}f_5},\\
\frac{\Theta_{14}(2z)\Theta_0\Theta_2\Theta_{12}}{t_\emptyset^4(z)} &= \frac{Y_{2,4}Y_{2,3}Y_{3,4}}{u(a_2)u(a_3)u(a_4)}\frac{1}{f_{2,4}f_{2,3}f_{3,4}f_\emptyset} + \frac{Y_{1,5}Y}{u(a_1)u(a_5)}\frac{1}{f_{1,5}f_2f_3f_4}\\
&\quad + \frac{Y_{2,5}Y_{3,5}Y_{4,5}Y}{u(a_2)u(a_3)u(a_4)u(a_5)^2}\frac{1}{f_{2,5}f_{3,5}f_{4,5}f_1}\\
&\quad + \frac{Y_{1,2}Y_{1,3}Y_{1,4}Y}{u(a_1)^2u(a_2)u(a_3)u(a_4)}\frac{1}{f_{1,2}f_{1,3}f_{1,4}f_5}.
\end{aligned}$$

We only worked in the generic case but the formulae can be extended to degenerate divisors: see for instance Gaudry [13] for level $n = 2$.

References

[1] A.O.L. Atkin. The number of points on an elliptic curve modulo a prime. *manuscript, Chicago IL*, 1988.

[2] C. Birkenhake and H. Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[3] G. Bisson and A.V. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *Journal of Number Theory*, 2009.

[4] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.

[5] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. *Journal of Cryptology*, 17(4):297–319, 2004.

[6] R. Bröker, D. Gruenewald, and K. Lauter. Explicit CM-theory in dimension 2, 10 2009.

[7] R. Bröker, K. Lauter, and A.V. Sutherland. Modular polynomials via isogeny volcanoes. *Preprint*, 2009.

[8] R. Dupont. *Moyenne arithmético-géométrique, suites de Borchardt et applications*. PhD thesis, École polytechnique, 2006.

[9] N.D. Elkies. Explicit isogenies. *manuscript, Boston MA*, 1992.

[10] A. Enge, P. Gaudry, and E. Thomé. An $L(1/3)$ discrete logarithm algorithm for low degree curves. *J. Cryptology*, 24(1):24–41, 2010.

[11] J.-C. Faugère, D. Lubicz, and Robert D. Computing modular correspondences for abelian varieties, 05 2009.

[12] M. Fouquet and F. Morain. Isogeny volcanoes and the SEA algorithm. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 276–291. Springer, Berlin, 2002.

[13] P. Gaudry. Fast genus 2 arithmetic based on theta functions. *Journal of Mathematical Cryptology*, 1(3):243–265, 2007.

[14] P. Gaudry. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. *Journal of Symbolic Computation*, 44(12):1690–1702, 2009.

[15] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security*, page 98. ACM, 2006.

[16] A. Joux. A one round protocol for tripartite Diffie–Hellman. *Journal of Cryptology*, 17(4):263–276, 2004.

[17] G.R. Kempf. Linear systems on abelian varieties. *American Journal of Mathematics*, 111(1):65–94, 1989.
[18] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.
[19] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California, 1996.
[20] S. Koizumi. Theta relations and projective normality of abelian varieties. *American Journal of Mathematics*, pages 865–889, 1976.
[21] D. Lubicz and Robert D. Computing isogenies between abelian varieties, May 2010.
[22] D. Lubicz and Robert D. Efficient pairing computation with theta functions. *Algorithmic Number Theory*, 6197, 07 2010. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings.
[23] A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. In *Proceedings of the twenty-third annual ACM symposium on Theory of computing*, page 89. ACM, 1991.
[24] J.-F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. In T. Mora and C. Traverso, editors, *Effective methods in algebraic geometry*, volume 94 of *Progr. Math.*, pages 313–334. Birkhäuser, 1991.
[25] D. Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1:287–354, 1966.
[26] D. Mumford. On the equations defining abelian varieties. II. *Invent. Math.*, 3:75–135, 1967.
[27] D. Mumford. On the equations defining abelian varieties. III. *Invent. Math.*, 3:215–244, 1967.
[28] D. Mumford. *Tata lectures on theta I*, volume 28 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1983. With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman.
[29] D. Mumford. *Tata lectures on theta II*, volume 43 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1984. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura.
[30] F. Richelot. Essai sur une méthode générale pour déterminer la valeur des intégrales ultra-elliptiques, fondée sur des transformations remarquables de ces transcendantes. *C. R. Acad. Sci. Paris*, 2:622–627, 1836.
[31] F. Richelot. De transformatione Integralium Abelianorum primiordinis commentation. *J. reine angew. Math.*, 16:221–341, 1837.
[32] D. Robert. *Theta functions and applications in cryptography*. PhD thesis, Université Henri-Poincarré, Nancy 1, France, July 2010.
[33] A. Sahai and B. Waters. Fuzzy identity-based encryption. *Advances in Cryptology–EUROCRYPT 2005*, pages 457–473, 2005.
[34] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of computation*, 44(170):483–494, 1985.
[35] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7(1):219–254, 1995.
[36] B. Smith. Isogenies and the discrete logarithm problem in jacobians of genus 3 hyperelliptic curves, 2 2009.
[37] A.V. Sutherland. Computing Hilbert class polynomials with the Chinese remainder theorem. *Mathematics of Computation*, 2009.
[38] P. Van Wamelen. Equations for the Jacobian of a hyperelliptic curve. *AMS*, 350(8):3083–3106, 08 1999.
[39] E. Verheul. Self-blindable credential certificates from the Weil pairing. *Advances in Cryptology—ASIACRYPT 2001*, pages 533–551, 2001.