Computing isogenies between Abelian Varieties

David Lubicz, Damien Robert

Computing Isogenies Between Abelian Varieties

David Lubicz[1,2], Damien Robert[3]

[1] CÉLAR,
BP 7419, F-35174 Bruz
[2] IRMAR, Universté de Rennes 1,
Campus de Beaulieu, F-35042 Rennes
[3] LORIA, Campus Scientifique, BP 239,
F-54506 Vandœuvre-lès-Nancy

Abstract

We describe an efficient algorithm for the computation of separable isogenies between abelian varieties represented in the coordinate system given by algebraic theta functions. Our algorithm decomposes in two principal steps. First, from the knowledge of a subgroup K isotropic for the Weil pairing of an abelian variety A, we explain how to compute the theta null point corresponding to the quotient abelian variety A/K. Second, from the knowledge of the theta null point of A/K, we give an algorithm to obtain a rational expression for the isogeny from A to A/K. The algorithm resulting as the combination of these two steps can be viewed as a higher dimensional analog of the well known algorithm of Vélu to compute isogenies between elliptic curves.

In order to improve the efficiency of our algorithms, we introduce a compressed representation that allows to encode a point of level 4ℓ of a g dimensional abelian variety using only $g(g+1)/2 \cdot 4^g$ coordinates. We also give formulas to compute the Weil and commutator pairings given input points in theta coordinates. All the algorithms presented in this paper work in general for any abelian variety defined over a field of odd characteristic.

Contents

List of Algorithms

List of Notations

Notation	**Description**	**Page List**
$Z(\overline{n})$	$\mathbb{Z}^g/n\mathbb{Z}^g$	8
$\mathscr{M}_{\overline{n}}$	The moduli space of theta null points of level n.	9
A_k	$(A_k, \mathscr{L}, \Theta_{A_k})$ is a polarized abelian variety with a theta structure of level ℓn.	8
B_k	$(B_k, \mathscr{L}_0, \Theta_{B_k})$ is an abelian variety ℓ-isogenous to A_k with a theta structure of level n.	10
ϑ_i	$(\vartheta_i)_{i\in Z(\overline{\ell n})}$ are the canonical projective coordinates on A_k given by the theta structure.	9
$\mathsf{0}_{A_k}$	The theta null $\mathsf{0}_{A_k} = \vartheta_i(\mathsf{0}_{A_k})_{i\in Z(\overline{\ell n})}$.	9
$\mathsf{0}_{B_k}$	The theta null $\mathsf{0}_{B_k} = \vartheta_i(\mathsf{0}_{B_k})_{i\in Z(\overline{n})}$.	10
$G(\mathscr{L})$	The Theta group of $(A_k, \mathscr{L})$	8
$K(\mathscr{L})$	$K(\mathscr{L}) = K_1(\mathscr{L}) \oplus K_2(\mathscr{L})$ is the decomposition of the kernel of the polarization $\mathscr{L}$ induced by the Theta structure Θ_A	8
$H(\delta)$	The Heisenberg group of type δ.	8
$s_{K(\mathscr{L})}$	The natural section $K(\mathscr{L}) \to G(\mathscr{L})$ induced by the Theta structure.	8
$\widetilde{\rho}_{\mathscr{L}}$	The affine action of $G(\mathscr{L})$ on $\widetilde{A}_k$.	11
$\widetilde{A}_k$	The affine cone of A_k.	11
$\widetilde{B}_k$	The affine cone of B_k.	11
$\widetilde{\vartheta}_i$	$(\widetilde{\vartheta}_i)_{i\in Z(\overline{\ell n})}$ are the affine coordinates on $\widetilde{A}_k$.	11
$\widetilde{\mathsf{0}}_{B_k}$	An affine lift of $\mathsf{0}_{B_k}$.	13
$\widetilde{\mathsf{0}}_{A_k}$	The affine lift of $\mathsf{0}_{A_k}$ such that $\widetilde{\pi}(\widetilde{\mathsf{0}}_{A_k}) = \widetilde{\mathsf{0}}_{B_k}$.	13
π	The ℓ-isogeny $\pi : A_k \to B_k$.	10
$\widetilde{\pi}$	$\widetilde{\pi}(\widetilde{\vartheta}_i(\widetilde{x})_{i\in Z(\overline{\ell n})}) = \widetilde{\vartheta}_i(\widetilde{x})_{i\in Z(\overline{n})}$ is the affine lift of π to $\widetilde{A}_k \to \widetilde{B}_k$.	11
$\widetilde{\pi}_i$	$\widetilde{\pi}_i = \widetilde{\pi} \circ (1, i, 0) = \widetilde{\vartheta}_{i+j}(\cdot)_{j\in Z(\overline{n})}$.	12
$\widetilde{P}_i$	$\widetilde{P}_i = (1, i, 0).\widetilde{\mathsf{0}}_{A_k} = (\vartheta_{i+j}(\widetilde{\mathsf{0}}_{A_k}))_{j\in Z(\overline{\ell n})}$.	13
$\widetilde{R}_i$	$\widetilde{R}_i = \widetilde{\pi}_i(\widetilde{\mathsf{0}}_{A_k}) = \widetilde{\pi}(\widetilde{P}_i)$.	13
$(e_1, \dots, e_g)$	A basis of $Z(\overline{\ell n})$	24
$(d_1, \dots, d_g)$	$d_i = n e_i$	24
$\mathscr{S}$	$\mathscr{S} = Z(\overline{\ell})$ (When $\ell \wedge n = 1$)	12
$\mathfrak{S}$	$\mathfrak{S} = \{d_1, d_2, \dots, d_g, d_1 + d_2, \dots d_1 + d_g, d_2 + d_3, \dots d_{g-1} + d_g\}$ (When $\ell \wedge n = 1$)	25
$e_{\mathscr{L}_0^\ell}$	The extended commutator pairing on $B_k[\ell]$	36
e_W	The Weil pairing.	37
$\langle\cdot,\cdot\rangle$	The canonical pairing on $Z(\overline{n}) \times \hat{Z}(\overline{n})$.	8

Glossary

Notation	**Description**	**Page List**
$\widetilde{B_k}'$	the affine cone of $(B_k, \mathscr{M}_0, \Theta_{B_k,\mathscr{M}_0})$ where $\mathscr{M}_0 = [\ell]^* \mathscr{L}_0$ and $\Theta_{B_k,\mathscr{M}_0}$ is a theta structure on $(B_k, \mathscr{M}_0)$ compatible with Θ_{B_k}.	31
$\widetilde{[\ell]}$	$\widetilde{[\ell]} : \widetilde{B_k}' \to \widetilde{B}_k$ is the morphism lifting $[\ell] : B_k \to B_k$.	31
`chain_add`	An addition chain	15
`chain_multadd`	A multiplication chain	18

1 Introduction

The general problem of computing separable isogenies between abelian varieties splits into different computational sub-problems depending on the expected input and output of the algorithm. These problems are:

- Given an abelian variety A_k over a field k and an abstract finite abelian group K compute all the abelian varieties B_k such that there exists an isogeny $A_k \rightarrow B_k$ whose kernel is isomorphic to K, and give rational expressions for the corresponding isogenies.
- Given an abelian variety A_k and a finite subgroup K of A_k, recover the quotient abelian variety $B_k = A_k/K$ as well a rational expression for an isogeny $A_k \rightarrow B_k$.
- Given two isogenous abelian varieties, A_k and B_k, compute a rational expression for an isogeny $A_k \rightarrow B_k$.

In the present paper, we are concerned with the first two problems. In the case that the abelian variety is an elliptic curve, efficient algorithms have been described that solve all the aforementioned problems [Ler]. In particular, an algorithm proposed by Vélu [Vél71] takes as input a finite subgourp G of cardinal ℓ of an elliptic curve E_k, and returns the equation of the quotient E_k/G at the cost of $O(\ell)$ additions in E_k. The algorithm of Vélu also gives a rational expression for the isogeny $E_k \rightarrow E_k/G$ in the coordinate system provided by the Weierstrass form of the elliptic curves.

For higher-dimensional abelian varieties much less is known. Richelot's formulas [Ric36, Ric37] can be used to compute $(2,2)$-isogenies between abelian varieties of dimension 2. The paper [Smi09] also introduces a method to compute certain isogenies of degree 8 between jacobian of curves of genus three. In this paper, we present an algorithm to compute $(\ell, \dots, \ell)$-isogenies between abelian varieties of dimension g represented in the coordinate system provided by algebraic theta functions for any $\ell \geqslant 2$ and $g \geqslant 1$ when the characteristic of k is odd and relatively prime to ℓ.

Let $n \in \mathbb{N}$ be such that $2|n$ and $n \geqslant 4$. Let $\overline{n} = (n, n, \dots, n) \in \mathbb{Z}^g$, and $Z(\overline{n}) = \mathbb{Z}^g/n\mathbb{Z}^g$. We denote by $\mathcal{M}_{\overline{n}}$ the modular space of marked abelian varieties $(A_k, \mathcal{L}, \Theta_{A_k})$ where $\mathcal{L}$ is a totally symmetric ample line bundle on A_k and Θ_{A_k} is a symmetric theta structure of type $Z(\overline{n})$ for $\mathcal{L}$ (see [Mum66, sec. 2]). In the following, we will also call a theta structure of type $Z(\overline{n})$ a theta structure of level n. The modular space $\mathcal{M}_{\overline{n}}$ is well-suited for computing modular correspondences since the algebraic systems which play the same role in this space as the classical modular polynomials have their coefficients in $\{1, -1\}$, and as a consequence are much more amenable to computations than their counterparts using the j-invariant in genus 1 or the Igusa invariants in genus 2 . In the article [FLR09], we have defined a modular correspondence:

$$\varphi : \mathcal{M}_{\overline{\ell n}} \rightarrow \mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}, (a_i)_{i \in Z(\overline{\ell n})} \mapsto ((a_i)_{i \in Z(\overline{n})}, (\sum_{j \in Z(\overline{\ell})} a_{i+nj})_{i \in Z(\overline{n})})$$

for $\ell \in \mathbb{N}^*$ prime to n, which can be seen as a generalization of the classical modular correspondence $X_0(\ell) \rightarrow X_0(1) \times X_0(1)$ for elliptic curves (see for instance [Koh03]). To explain it, let p_1 and p_2 be respectively the first and second projections $\mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}} \rightarrow \mathcal{M}_{\overline{n}}$, and let $\varphi_1 = p_1 \circ \varphi$, $\varphi_2 = p_2 \circ \varphi$. The map $\varphi_1 : \mathcal{M}_{\overline{\ell n}} \rightarrow \mathcal{M}_{\overline{n}}$ is such that $(x, \varphi_1(x))$ for $x \in \mathcal{M}_{\overline{\ell n}}(k)$ are modular points corresponding to ℓ-isogenous abelian varieties.

In fact, consider $(a_i)_{i \in Z(\overline{\ell n})} \in \varphi_1^{-1}((b_i)_{i \in Z(\overline{n})})$. The modular point $(a_i)_{i \in Z(\overline{\ell n})}$ defines a triple $(A_k, \mathscr{L}, \Theta_{A_k})$ and the classical isogeny theorem for algebraic theta functions [Mum66, th. 4] gives an explicit isogeny $\pi : A_k \to B_k$. We denote by $\hat{\pi} : B_k \to A_k$ the isogeny that makes the following diagram commutative:

$$\begin{tikzcd}
x \in A_k \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A_k \\
& y \in B_k \arrow[ur, "\hat{\pi}"'] &
\end{tikzcd}$$

The main result of this paper is:

Theorem 1.1:
Let B_k be a dimension g marked abelian variety. Let $(T_1, \dots, T_g) \subset B_k[\ell]$ be a basis of a maximal subgroup K of $B_k[\ell]$ isotropic for the Weil pairing. Let $\hat{\pi} : B_k \to B_k/K$ be the corresponding isogeny. One can compute the compressed coordinates of the modular point $(a_i)_{i \in Z(\overline{\ell n})}$ corresponding to $\hat{\pi}$ with $O(\log(\ell))$ addition chains in B_k and $O(1)$ ℓ^{th}-roots of unity extractions.

Once we have $(a_i)_{i \in Z(\overline{\ell n})}$, we can compute the compressed coordinates of the image of a point in B_k by $\hat{\pi}$ with $O(\log(\ell))$ addition chains in B_k. Taking the generic point of B_k, we obtain in particular a rational expression for the isogeny $\hat{\pi}$.

The precise meaning of addition chain and compressed coordinates will be made clear in the course of the paper. A proof of this theorem is given in Section 4.2 and Section 5.1. It should be remarked that this result constitute a higher dimensional analog of the classical Vélu's algorithm since by combining the two conclusions of the theorem, we obtain an efficient algorithm which takes as input an abelian variety B_k and a maximal subgroup K of $B_k[\ell]$ isotropic for the Weil pairing and computes a rational expression for the isogeny $B_k \to B_k/K$.

Note that the classical isogeny theorem for theta functions is not sufficient for our purpose of computing isogenies between abelian varieties. Although it is effective, the isogeny theorem can only be used to compute isogenies from a marked abelian variety of level ℓ to a marked abelian variety of level n where $\overline{n}$ divides $\overline{\ell}$, so it only provides us with a way to compute isogenies by "going down" in the level of the theta structure. At some point, we need a way to compute isogenies by "going up" the level and this is precisely what gives Theorem 1.1. We can then combine the two theorems: once we have computed an isogeny $\hat{\pi} : B_k \to A_k$, it is possible to compose $\hat{\pi}$ with an isogeny $\pi_2 : A_k \to C_k$ given by the isogeny theorem such that $\pi_2 \circ \hat{\pi}$ is an ℓ^2-isogeny (see [FLR09, Sec 3] or Section 2.2). In fact, let C_k be the abelian variety associated to the modular point $(c_i)_{i \in Z(\overline{n})} = \varphi_2\left((a_i)_{i \in Z(\overline{\ell n})}\right)$ then we have the following diagram

$$\begin{tikzcd}
B_k \arrow[dd, "{[\ell]}"'] \arrow[dr, "\hat{\pi}"] & & \\
& A_k \arrow[dl, "\pi"'] \arrow[dr, "\pi_2"] & \\
B_k & & C_k
\end{tikzcd}$$

The isogeny $\pi_2 \circ \hat{\pi}$ is then an ℓ^2 isogeny between B_k and C_k which are two marked abelian varieties with a theta structure of level n. Possible applications of our algorithm includes:

- The transfer the discrete logarithm from an abelian variety to another abelian variety where the discrete logarithm is easy to solve [Smi08]
- The computation of isogeny graphs to obtain a description the endomorphism ring of an abelian variety.
- The computation of Hilbert class polynomials.

We end up the introduction with some general remarks about the algorithms presented in this paper. The assumption that n is prime to ℓ is inessential. There is nonetheless one noticeable difference if we drop this hypothesis. Suppose that we are given $B_k[\ell]$. Since B_k is given by a theta structure of level n, we can recover $B_k[n]$ using the action of the theta group on the theta null point $(b_i)_{i \in Z(\overline{n})}$. If ℓ is prime to n, this gives us $B_k[\ell n]$, and we can use the first assertion of Theorem 1.1 to obtain a modular point of type $Z(\overline{\ell n})$. If ℓ is not prime to n, we have to compute $B_k[\ell n]$ directly.

Although we only consider the case of $(\ell, \ldots, \ell)$-isogeny, it is also possible to compute more general types of isogenies with our algorithm. With the notations of Section 2, let $\delta_0 = (\delta_1, \ldots, \delta_g)$ be a sequence of integers such that $2 | \delta_1$ and $\delta_i | \delta_{i+1}$, and let $(b_i)_{i \in Z(\delta_0)} \in \mathcal{M}_{\delta_0}$ be a modular point corresponding to an abelian variety B_k. Let $\delta' = (\ell_1, \ldots, \ell_g)$ (where $\ell_i | \ell_{i+1}$) and define $\delta = (\delta_1 \ell_1, \ldots, \delta_g \ell_g)$. Let $(a_i)_{i \in Z(\delta)} \in \mathcal{M}_\delta$ be such that $\varphi_1\left((a_i)_{i \in Z(\delta)}\right) = (b_i)_{i \in Z(\delta_0)}$ where φ_1 is the natural inclusion of $Z(\delta_0)$ into $Z(\delta)$. The theta null point $(a_i)_{i \in Z(\delta)}$ corresponds to an abelian variety A_k, such that there is a $(\ell_1, \cdots, \ell_g)$-isogeny $\pi : A_k \to B_k$, which can be computed by the isogeny theorem [Mum66, Th. 4] (see Section 2.2). The isogeny we compute in Step 2 is the contragredient isogeny $\hat{\pi} : B_k \to A_k$ of type $(\ell_g/\ell_1, \ell_g/\ell_2, \cdots, 1, \ell_g, \ell_g, \cdots, \ell_g)$. Using the modular correspondence φ_1 to go back to a modular point of type $Z(\delta_0)$ (see Section 1) gives an isogeny of type $(\ell_g/\ell_1, \ell_g/\ell_2, \cdots, 1, \ell_1 \ell_g, \ell_2 \ell_g, \cdots, \ell_g \ell_g)$. For the clarity of the exposition, we will stick to the case $\delta_0 = \overline{n}$ and $\delta = \overline{\ell n}$ and we leave to the reader the easy generalization.

For an actual implementation, we want to use the smallest n possible to get a compact representation of the points and a fast addition chain. In fact it is possible to tweak Theorem 1.1 to make it works with the case $n = 2$. This case is very important in practice: it allows a more compact representation of the points than for $n = 4$ (we gain a factor 2^g in space), a faster addition chain (see Section 4.1.1), but most importantly it reduces the most consuming part of our algorithm, the computation of the points of ℓ-torsion, since there are half as much such points on the Kummer variety associated to an abelian variety. For each algorithm that we use, we give an explanation on how to adapt it for the type $Z(\overline{2})$ case: see Section 3.2.1 and the end of Sections 4.2, 5.1, 5.3 and 6.2.

The paper is organized as follow. In Section 2, we recall the isogeny theorem and we study the relationship between isogenies and the action of the theta group. We recall the addition relations, which play a central role in this paper in Section 3. We then explain how to compute the isogeny associated to a modular point in Section 4. If the isogeny is given by theta functions of type $Z(4\ell)$, it requires $(4\ell)^g$ coordinates. We give a point compression algorithm in Section 4.1, showing how to express such an isogeny with only $g(g+1)/2 \cdot 4^g$ coordinates. In Section 5 we give a full generalization of Vélu's formulas that constructs an isogenous modular point with prescribed kernel. This algorithm is more efficient than the special Gröbner basis algorithm from [FLR09]. There is a strong connection between isogenies and pairings, and we use the above work to explain how one can compute the commutator pairing and how it relates to the usual Weil pairing in Section 6.

2 Modular correspondences and theta null points

In this section, we fix some notations that we use in the rest of the paper. In Section 2.1, we recall the definition of a theta structure and the projective embedding [Mum66, Sec. 1] deduced from it. In Section 2.2 we recall the isogeny theorem, which relate the theta functions of two isogenous abelian varieties with compatible theta structures. In Section 2.3 we study the connection between isogenies and the action of the theta group on the affine cone of the projective embedding given by the theta structure.

Let A_k be an abelian variety of dimension g over a perfect field k and denote by $K(A_k)$ its function field. An isogeny is a finite surjective map of abelian varieties $\pi : A_k \rightarrow B_k$ and is said to be separable if the function field $K(A_k)$ is a finite separable extension of $K(B_k)$. A separable isogeny is uniquely determined by its kernel, which is a finite subgroup of $A_k(\overline{k})$. In that case, the cardinality of the kernel is the degree of the isogeny. Since we will only consider isogenies of degree prime to the characteristic of k, we will only deal with separable isogenies. In the rest of this paper, by ℓ-isogeny for $\ell > 0$, we always mean a $(\ell, \cdots, \ell)$-isogeny where $(\ell, \cdots, \ell) \in \mathbb{N}^g$.

2.1 Theta structures

Let A_k be a g dimensional abelian variety over a perfect field k. Let $\mathscr{L}$ be an ample totally symmetric line bundle of degree d on A_k. We suppose moreover that d is prime to the characteristic of k. Denote by $K(\mathscr{L})$ the kernel of the isogeny $\varphi_{\mathscr{L}} : A_k \rightarrow \hat{A}_k$, defined on geometric points by $x \mapsto \tau_x^* \mathscr{L} \otimes \mathscr{L}^{-1}$ where τ_x is the translation by x. Let $\delta = (\delta_1, \ldots, \delta_g)$ be the sequence of integers satisfying $\delta_i | \delta_{i+1}$ such that, as group schemes $K(\mathscr{L}) \simeq \bigoplus_{i=1}^g (\mathbb{Z}/\delta_i \mathbb{Z})_k^2$. We say that δ is the type of $\mathscr{L}$. In the following we let $Z(\delta) = \bigoplus_{i=1}^g (\mathbb{Z}/\delta_i \mathbb{Z})_k$, $\hat{Z}(\delta)$ be the Cartier dual of $Z(\delta)$, and $K(\delta) = Z(\delta) \times \hat{Z}(\delta)$. If $x \in Z(\delta)$ and $\ell \in \hat{Z}(\delta)$, we denote $\langle x, \ell \rangle := \ell(x)$.

Let $G(\mathscr{L})$ and $\mathscr{H}(\delta)$ be respectively the theta group of $(A_k, \mathscr{L})$ and the Heisenberg group of type δ [Mum66, p. 294]. In this article, elements of $G(\mathscr{L})$ will be written as (x, ψ_x) with $x \in K(\mathscr{L})$ and $\psi_x : \mathscr{L} \rightarrow \tau_x^* \mathscr{L}$ is an isomorphism. We know that $G(\mathscr{L})$ and $\mathscr{H}(\delta)$ are central extensions of $K(\mathscr{L})$

and $K(\delta)$ by the multiplicative group $\mathbb{G}_{m,k}$. By definition, a theta structure Θ_{A_k} on $(A_k, \mathscr{L})$ is an isomorphism of central extensions from $\mathscr{H}(\delta)$ to $G(\mathscr{L})$. We denote by $e_{\mathscr{L}}$ the commutator pairing [Mum66, p. 203] on $K(\mathscr{L})$ and by e_δ the canonical pairing on $K(\delta) = Z(\delta) \times \hat{Z}(\delta)$. We recall that if (x_1, x_2) and (y_1, y_2) are in $K(\delta)$ we have $e_\delta((x_1,x_2),(y_1,y_2)) = \langle x_1, y_2\rangle / \langle y_1, x_2\rangle$. We remark that a theta structure Θ_{A_k} induces a symplectic isomorphism $\overline{\Theta}_{A_k}$ from $(K(\delta), e_\delta)$ to $(K(\mathscr{L}), e_{\mathscr{L}})$. Let $K(\mathscr{L}) = K_1(\mathscr{L}) \times K_2(\mathscr{L})$ be the decomposition into maximal isotropic subspaces induced by $\overline{\Theta}_{A_k}$.

The section $K(\delta) \to \mathscr{H}(\delta)$ defined on geometric points by $(x,y) \mapsto (1,x,y)$ can be transported by the theta structure to obtain a natural section $s_{K(\mathscr{L})} : K(\mathscr{L}) \to G(\mathscr{L})$ of the projection $\varkappa : G(\mathscr{L}) \to K(\mathscr{L})$. We note $s_{K_1(\mathscr{L})}$ (resp. $s_{K_2(\mathscr{L})}$) the restriction of this section to $K_1(\mathscr{L})$ (resp. $K_2(\mathscr{L})$). Recall [Mum66, p. 291] that a level subgroup $\widetilde{K}$ of $G(\mathscr{L})$ is a subgroup such that $\widetilde{K}$ is isomorphic to its image by $\varkappa$.

Let $V = \Gamma(A_k, \mathscr{L})$. There is an action of the theta group $G(\mathscr{L})$ on V by $v \mapsto \psi_x^{-1}\tau_x^*(v)$ for $v \in V$ and $(x, \psi_x) \in G(\mathscr{L})$. This action can be transported via Θ_{A_k} to an action of $\mathscr{H}(\delta)$ on V. It can be shown that there is a unique (up to a scalar factor) basis $(\vartheta_i)_{i \in Z(\delta)}$ of V such that this action is given by:

$$(\alpha, i, j).\vartheta_h^{\Theta_{A_k}} = \alpha.\langle -i-h, j\rangle.\vartheta_{h+i}^{\Theta_{A_k}}. \tag{1}$$

If there is no ambiguity, in this paper, we will sometimes drop the superscript Θ_{A_k} in the notation $\vartheta_k^{\Theta_{A_k}}$.

This basis gives a projective embedding $\varphi_{\Theta_{A_k}} : A_k \to \mathbb{P}_k^{d-1}$ which is uniquely defined by the theta structure Θ_{A_k}. The point $(a_i)_{i \in Z(\delta)} = \varphi_{\Theta_{A_k}}(0_{A_k})$ is called the theta null point associated to the theta structure. Mumford proves [Mum66] that if $4|\delta$, $\varphi_{\Theta_{A_k}}(A_k)$ is the closed subvariety of $\mathbb{P}_k^{d-1}$ defined by the homogeneous ideal generated by the Riemann equations:

Theorem 2.1 (Riemann equations):
For all $x, y, u, v \in Z(2\delta)$ that are congruent modulo $Z(\delta)$, and all $\chi \in \hat{Z}(\overline{2})$, we have

$$\Big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{x+y+t}\vartheta_{x-y+t}\Big).\Big(\sum_{t \in Z(\overline{2})} \chi(t)a_{u+v+t}a_{u-v+t}\Big) = \\ = \Big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{x+u+t}\vartheta_{x-u+t}\Big).\Big(\sum_{t \in Z(\overline{2})} \chi(t)a_{y+v+t}a_{y-v+t}\Big). \tag{2}$$

The data of a triple $(A_k, \mathscr{L}, \Theta_{A_k})$ is called a marked abelian variety of type $Z(\delta)$. We denote by $\mathscr{M}_\delta$ the quasi-projective variety defined as the locus of all theta null points associated to marked abelian varieties of type $Z(\delta)$. We recall [Kem89, Th. 28] that if $n > 4$, then $\mathscr{M}_{\overline{n}}$ is an open subset in the projective variety described by the following equations in $\mathbb{P}(k(Z(\overline{n})))$:

$$\Big(\sum_{t \in Z(\overline{2})} \chi(t)a_{x+t}a_{x+t}\Big).\Big(\sum_{t \in Z(\overline{2})} \chi(t)a_{u+t}a_{u+t}\Big) = \\ \Big(\sum_{t \in Z(\overline{2})} \chi(t)a_{z-x+t}a_{z-y+t}\Big).\Big(\sum_{t \in Z(\overline{2})} \chi(t)a_{z-u+t}a_{z-v+t}\Big) \tag{3}$$

$$a_x = a_{-x}$$

for all $x, y, u, v, z \in Z(\overline{n})$, such that $x + y + u + v = 2z$ and all $\chi \in \hat{Z}(\overline{2})$.

2.2 Isogenies compatible with a theta structure

Let $(a_i)_{i \in Z(\delta)} \in \mathcal{M}_\delta$ be a theta null point associated to a triple $(A_k, \mathscr{L}, \Theta_{A_k})$. Let $\delta_0 \in \mathbb{Z}^g$ be such that $4|\delta_0|\delta$, and write $\delta = \delta_0 \cdot \delta'$. In the following we consider $Z(\delta_0)$ as a subgroup of $Z(\delta)$ via the map $\varphi : (x_i)_{i \in [1..g]} \in Z(\delta_0) \mapsto (\delta'_i x_i)_{i \in [1..g]} \in Z(\delta)$. From now on, when considering $Z(\delta_0) \subset Z(\delta)$, we always refer to this map. Let $K \subset K(\mathscr{L})$ be any isotropic subgroup for $e_{\mathscr{L}}$ such that we can write $K = K_1 \times K_2$ with $K_i \subset K_i(\mathscr{L})$.

Let $B_k = A_k/K$ and $\pi : A_k \to B_k$ be the associated isogeny. Since K is isotropic, $\widetilde{K} := s_{K(\mathscr{L})}(K)$ is a level subgroup, so by Grothendieck descent theory there exists a polarization $\mathscr{L}_0$ on B_k and an isomorphism $\mathscr{L} \simeq \pi_K^*(\mathscr{L}_0)$. The theta group $G(\mathscr{L}_0)$ is isomorphic to $\mathscr{Z}(\widetilde{K})/\widetilde{K}$ where $\mathscr{Z}(\widetilde{K})$ is the centralizer of $\widetilde{K}$ in $G(\mathscr{L})$ [Mum66, Prop. 2]. We say that a theta structure Θ_{B_k} on $(B_k, \mathscr{L}_0)$ is π-compatible with Θ_{A_k} if it respects this isomorphism. The isogeny theorem ([Mum66, Th. 4]) then gives a way to compute $(\pi^*(\vartheta_i^{\Theta_{B_k}}))_{i \in Z(\overline{n})}$ given $(\vartheta_i^{\Theta_{A_k}})_{i \in Z(\overline{\ell n})}$. Note $\overline{\Theta}_A^{-1}(K) = Z_1 \times Z_2$, we call $Z_1 \times Z_2$ the type of π. If $Z_1 = 0$ we say that π is of type 1, and if $Z_2 = 0$ that π is of type 2. We note $Z_1^\perp = \{x \in Z(\delta) \mid \langle x, Z_2 \rangle = 1\}$. Then there is a bijection between π-compatible theta structures on $(B_k, \mathscr{L}_0)$ and isomorphisms $\sigma : Z_1^\perp / Z_1 \to Z(\delta_0)$ (see [Mum66, Th 4]).

Since we are mainly interested with ℓ-isogenies, we now specialize to the case $\delta = \overline{\ell n}$, $\delta' = \overline{\ell}$ so that $\delta_0 = \overline{n}$. We take $K = A_k[\ell]_2$, we then have $Z_1 = 0$, $Z_2 = \hat{Z}(\overline{\ell}) \subset \hat{Z}(\overline{\ell n})$ so that $\pi : A_k \to B_k$ is an ℓ-isogeny of type 1. In this case we have $Z_1^\perp = Z(\overline{n}) \subset Z(\overline{\ell n})$, and we always consider the compatible theta structure on B_k corresponding to $\sigma = \mathrm{Id}$ [FLR09, Sec. 3]. We recall the following proposition [FLR09, Prop 4].

Proposition 2.2 (Isogeny theorem for compatible theta structures):
Let $(a_i)_{i \in Z(\overline{\ell n})}$ be a theta null point associated to a triple $(A_k, \mathscr{L}, \Theta_{A_k})$ and $(b_i)_{i \in Z(\overline{n})}$ a theta null point associated to $(B_k, \mathscr{L}_0, \Theta_{B_k})$. Let $\varphi : Z(\overline{n}) \to Z(\overline{\ell n})$ be the canonical embedding. Then $(b_i)_{i \in Z(\delta')} = \varphi_1(a_i)_{i \in Z(\delta')}$ if and only if there is an ℓ-isogeny π of type 1 such that Θ_{B_k} is π-compatible with Θ_{A_k}. In this case, let $(\vartheta_i^{\Theta_{A_k}})_{i \in Z(\overline{\ell n})}$ (resp. $(\vartheta_i^{\Theta_{B_k}})_{i \in Z(\overline{n})}$) be the canonical basis of $\mathscr{L}$ (resp. $\mathscr{L}_0$) associated to Θ_{A_k} (resp. Θ_{B_k}). There exists some $\omega \in \overline{k}^*$ such that for all $i \in Z(\overline{n})$

$$\pi_K^*(\vartheta_i^{\Theta_{A_k}}) = \omega \vartheta_{\varphi(i)}^{\Theta_{B_k}}. \tag{4}$$

It is easy to describe ℓ-isogenies of type 2 from Proposition 2.2. In fact, let $\mathfrak{I}_0$ be the automorphism of the Heisenberg group $\mathscr{H}(\overline{\ell n})$ that permutes $Z(\overline{\ell n})$ and $\hat{Z}(\overline{\ell n})$: $\mathfrak{I}_0(\alpha, x, y) = (\alpha, y, x)$. We define $\mathfrak{I}_{A_k} = \Theta_{A_k} \circ \mathfrak{I}_0 \circ \Theta_{A_k}^{-1}$, where $\mathfrak{I}_{A_k}$ is the automorphism of the Theta group of A_k that permutes $K_1(\mathscr{L})$ and $K_2(\mathscr{L})$. (There is a similar automorphism $\mathfrak{I}_{B_k}$ of the theta group of B_k; we will usually note these automorphisms $\mathfrak{I}$ since the theta group is clear from the context.) If π_2 is a compatible isogeny of type 2 between $(A_k, \mathscr{L}, \Theta_{A_k})$ and $(B_k, \mathscr{L}_0, \Theta_{B_k})$, then π_2 is a compatible isogeny of type 1 between

$(A_k, \mathscr{L}, \mathfrak{I}_{A_k} \circ \Theta_{A_k})$ and $(B_k, \mathscr{L}, \mathfrak{I}_B \circ \Theta_{B_k})$. Since the action of $\mathfrak{I}$ is given by [FLR09, Section 5]

$$\vartheta_i^{\mathfrak{I}_{A_k} \circ \Theta_{A_k}} = \sum_{j \in \hat{Z}(\overline{\ell n})} e(i,j) \vartheta_j^{\Theta_{A_k}}, \tag{5}$$

we see that we have for all $i \in Z(\overline{n})$

$$\pi^*(\vartheta_i^{\Theta_{B_k}}) = \sum_{j \in Z(\overline{\ell})} \vartheta_{i+nj}^{\Theta_{A_k}}. \tag{6}$$

Applying Equations (4) and (6) to $\widetilde{0}_{A_k}$ yields the formulas for the modular correspondence $\varphi : \mathscr{M}_{\overline{\ell n}} \to \mathscr{M}_{\overline{n}} \times \mathscr{M}_{\overline{n}}$ from Section 1.

2.3 The action of the theta group on the affine cone and isogenies

Let $\pi : (A_k, \mathscr{L}, \Theta_{A_k}) \to (B_k, \mathscr{L}_0, \Theta_{B_k})$ be an ℓ-isogeny of type 1 between compatible theta structures. The action by translation $\rho_{\mathscr{L}}$ from $K(\mathscr{L})$ on A_k descends to an action on B_k: if $x \in K(\mathscr{L})$, the induced action on B_k is simply the translation by $\pi(x)$. The situation is more interesting if we consider the action of $G(\mathscr{L})$. Since $G(\mathscr{L})$ is a central extension of $K(\mathscr{L})$ by $\mathbb{G}_{m,k}$ it is natural to let $G(\mathscr{L})$ act on a central extension of A_k by $\mathbb{G}_{m,k}$ More precisely, let $V = \Gamma(A_k, \mathscr{L})$ and let $p_{\mathbb{A}_k(V)} : \mathbb{A}_k(V) \to \mathbb{P}_k(V)$ be the canonical projection. Let $\widetilde{A}_k = p^{-1}_{\mathbb{A}_k(V)}(A_k)$ be the affine cone of A_k which is a central extension of A_k by $\mathbb{G}_{m,k}$ The action of $G(\mathscr{L})$ on V given by (1), induces an action $\widetilde{\rho}_{\mathscr{L}}$ on $\widetilde{A}_k$. This action is compatible with the action of $K(\mathscr{L})$ on A_k in the following way: if $\varkappa : G(\mathscr{L}) \to K(\mathscr{L})$ is the projection, $p_{\mathbb{A}_k(V)} \circ \widetilde{\rho}_{\mathscr{L}} = \rho_{\mathscr{L}} \circ \varkappa$. Similarly we note $\widetilde{B}_k$ the affine cone of B_k and $\widetilde{\rho}_{\mathscr{L}_0}$ the action of $G(\mathscr{L}_0)$ on $\widetilde{B}_k$.

We say that a coordinate system $(\widetilde{\vartheta}_i^{\Theta_{A_k}})_{i \in Z(\overline{\ell n})}$ on $\widetilde{A}_k$ lifts the projective system $(\vartheta_i^{\Theta_{A_k}})_{i \in Z(\overline{\ell n})}$ on A_k if for all $j \in Z(\overline{\ell n})$, on the principal open set defined by $\vartheta_j^{\Theta_{A_k}}$, we have $p^*_{\mathbb{A}_k(V)}(\vartheta_i^{\Theta_{A_k}} / \vartheta_j^{\Theta_{A_k}}) = \widetilde{\vartheta}_i^{\Theta_{A_k}} / \widetilde{\vartheta}_j^{\Theta_{A_k}}$. Obviously, such a coordinate system $(\widetilde{\vartheta}_i)_{i \in Z(\overline{\ell n})}$ is defined up to an action of $\mathbb{G}_{m,k}$ and we fix such a choice for the rest of the paper. In the same manner, we denote by $(\widetilde{\vartheta}_i^{\Theta_{B_k}})_{i \in Z(\overline{n})}$ a coordinate system on $\widetilde{B}_k$ that lifts the coordinate system $(\vartheta_i^{\Theta_{B_k}})_{i \in Z(\overline{n})}$. We will usually replace $(\widetilde{\vartheta}_i^{\Theta_{A_k}})_{i \in Z(\overline{\ell n})}$ (resp. $(\widetilde{\vartheta}_i^{\Theta_{B_k}})_{i \in Z(\overline{n})}$) by $(\widetilde{\vartheta}_i)_{i \in Z(\overline{\ell n})}$ (resp. $(\widetilde{\vartheta}_i)_{i \in Z(\overline{n})}$) when no confusion is possible.

Since $\mathscr{L}$ is symmetric, there is an action of the morphism $[-1]$ on V given by $f \in V \mapsto \Phi(\iota^* f)$ where $\iota : A \to A$ maps x to $-x$ and Φ is the normalized isomorphism $\iota^* \mathscr{L} \to \mathscr{L}$. This action extends to an action on $\widetilde{A}_k$ that we denote also by $[-1] : \widetilde{x} \in \widetilde{A}_k(\overline{k}) \mapsto -\widetilde{x}$. Now since $G(\mathscr{L})$ is a symmetric theta structure we have $[-1]^* \widetilde{\vartheta}_i = \widetilde{\vartheta}_{-i}$ [Mum66, p. 331] so if $\widetilde{x} = (\widetilde{x}_i)_{i \in Z(\overline{\ell n})}$ then $-\widetilde{x} = (\widetilde{x}_{-i})_{i \in Z(\overline{\ell n})}$.

Let $\widetilde{\pi} : \widetilde{A}_k \to \widetilde{B}_k$ be the morphism such that $\widetilde{\pi}^*(\widetilde{\vartheta}_i^{\Theta_{B_k}}) = \widetilde{\vartheta}_i^{\Theta_{A_k}}$ for $i \in Z(\overline{n})$. Note that $\widetilde{\pi}$ is just a lift to the affine cone of the isogeny $\pi : A_k \to B_k$, so that the following diagram commutes:

$$\begin{tikzcd}
\widetilde{A}_k \arrow[r, "p_{A_k}"] \arrow[d, "\widetilde{\pi}"] & A_k \arrow[d, "\pi"] \\
\widetilde{B}_k \arrow[r, "p_{B_k}"] & B_k
\end{tikzcd}$$

We call $\widetilde{\pi}$ the lift of π compatible with the choice of affine coordinates on $\widetilde{A}_k$ and $\widetilde{B}_k$.

We will now study the link between the action $\widetilde{\rho}_{\mathscr{L}}$ of $G(\mathscr{L})$ on $\widetilde{A}_k$ and the morphism $\widetilde{\pi}$. To simplify the notations, if $(\alpha, i, i) \in \mathscr{H}(\delta)$ and $\widetilde{x}$ is a geometric point of $\widetilde{A}_k$, we will note $(\alpha, i, j).\widetilde{x} := \widetilde{\rho}_{\mathscr{L}}(\Theta_{A_k}((\alpha, i, j))).\widetilde{x}$. Let $K_\pi = \overline{\Theta}_{A_k}(\hat{Z}(\overline{\ell}))$ be the kernel of the isogeny $\pi : A_k \to B_k$ and recall (see Section 2.2) that $G(\mathscr{L}_0) = \mathscr{Z}(\widetilde{K}_\pi)/\widetilde{K}_\pi$.

Proposition 2.3:
Let $g \in \mathscr{Z}(\widetilde{K}_\pi)$ and note $\overline{g}$ its image in $\mathscr{Z}(\widetilde{K}_\pi)/\widetilde{K}_\pi$. We have $\widetilde{\rho}_{\mathscr{L}_0}(\overline{g}) = \widetilde{\pi} \circ \widetilde{\rho}_{\mathscr{L}}(g)$.

Proof: This is an immediate consequence of the fact that the two theta structures Θ_{A_k} and Θ_{B_k} are π-compatible. ■

For $i \in \mathscr{H}(\overline{\ell n})$, we can define a mapping $\widetilde{\pi}_i : \widetilde{A}_k \to \widetilde{B}_k$ given on geometric points by $\widetilde{x} \mapsto \widetilde{\pi}(\widetilde{\rho}_{\mathscr{L}}(\Theta_{A_k}(i)).\widetilde{x})$. If $\Theta_{A_k}(i) \in \mathscr{Z}(\widetilde{K}_\pi)$, Proposition 2.3 shows that $\widetilde{\pi}_i = \widetilde{\rho}_{\mathscr{L}_0}(\overline{\Theta_{A_k}(i)}) \circ \widetilde{\pi}$, hence $\widetilde{\pi}_i$ can be recovered from $\widetilde{\pi}$ and the action $\widetilde{\rho}_{\mathscr{L}_0}$. Since $\mathscr{Z}(\widetilde{K}_\pi) \supset s_{K(\mathscr{L})}(K_2(\mathscr{L}))$, the interesting mappings to study are then $\widetilde{\pi}_i := \widetilde{\pi}_{(1,i,0)}$ for $i \in Z(\overline{\ell n})$. They are given on geometric points by

$$\widetilde{\pi}_i((\widetilde{\vartheta}_j(\widetilde{x}))_{j \in Z(\overline{\ell n})}) = (\widetilde{\vartheta}_{i+\ell.j}(\widetilde{x}))_{j \in Z(\overline{n})}.$$

Corollary 2.4:
Keeping the notations from above, we have

1. *Let $\mathscr{S}$ be a subset of $Z(\overline{\ell n})$, such that $\mathscr{S} + Z(\overline{n}) = Z(\overline{\ell n})$. Then $\widetilde{x} \in \widetilde{A}_k(\overline{k})$ is uniquely determined by $\{\widetilde{\pi}_i(\widetilde{x})\}_{i \in \mathscr{S}}$.*
2. *Let $\widetilde{y} \in \widetilde{A}_k(\overline{k})$ be such that $\widetilde{\pi}(\widetilde{y}) = \widetilde{\pi}(\widetilde{x})$. Then there exists $j \in \hat{Z}(\overline{\ell}) \subset \hat{Z}(\overline{\ell n})$ such that $\widetilde{y} = (1, 0, j).\widetilde{x}$ and*
$$\widetilde{\pi}_i(\widetilde{y}) = e_{\overline{\ell n}}(i, j)\widetilde{\pi}_i(\widetilde{x}).$$
In particular $\widetilde{\pi}_i(\widetilde{y})$ and $\widetilde{\pi}_i(\widetilde{x})$ differ by an ℓ^{th}-root of unity.

Proof:

1. Since $\widetilde{\pi}_i((\widetilde{\vartheta}_j(\widetilde{x}))_{j \in Z(\overline{\ell n})}) = (\widetilde{\vartheta}_{i+\ell.j}(\widetilde{x}))_{j \in Z(\overline{n})}$, from $\{\widetilde{\pi}_i(\widetilde{x})\}_{i \in \mathscr{S}}$ one can obtain the values $\left\{\widetilde{\vartheta}_j(\widetilde{x})\right\}_{j \in \mathscr{S}+Z(\overline{n})}$. If $\mathscr{S} + Z(\overline{n}) = Z(\overline{\ell n})$ this shows that we can recover $\widetilde{x} = (\widetilde{\vartheta}_j(\widetilde{x}))_{j \in Z(\overline{\ell n})}$.

2. If $\widetilde{\pi}(\widetilde{y}) = \widetilde{\pi}(\widetilde{x})$, then $p_{A_k}(\widetilde{y}) - p_{A_k}(\widetilde{x}) \in K_\pi$. So there exists $j \in \hat{Z}(\overline{\ell})$ and $\alpha \in \overline{k}^*$ such that $\widetilde{y} = (\alpha, 0, j).\widetilde{x}$. Hence $\widetilde{\vartheta}_i(\widetilde{y}) = \alpha e_{\overline{\ell n}}(i,j)\widetilde{\vartheta}_i(\widetilde{x})$. Since $\widetilde{\pi}(\widetilde{x}) = \widetilde{\pi}(\widetilde{y})$, $\alpha = 1$. Moreover, as $j \in \hat{Z}(\overline{\ell})$, $e_{\overline{\ell n}}(i+k, j) = e_{\overline{\ell n}}(i,j)$ if $k \in Z(\overline{n})$ so that $\widetilde{\pi}_i(\widetilde{x}) = e_{\overline{\ell n}}(i,j)\widetilde{\pi}_i(\widetilde{y})$. ■

Corollary 2.4 shows that $\widetilde{\rho}_{\mathscr{L}}$ descends to an action on $\widetilde{B}_k/\mu_k(\ell)$ where $\mu_k(\ell)$ is the group scheme of ℓ-roots of unity on k.

Example 2.5:

- If ℓ is prime to n, the canonical mappings $Z(\overline{n}) \to Z(\overline{\ell n})$ and $Z(\overline{\ell}) \to Z(\overline{\ell n})$ induce an isomorphism $Z(\overline{n}) \times Z(\overline{\ell}) \xrightarrow{\sim} Z(\overline{\ell n})$, and one can take $\mathscr{S} = Z(\overline{\ell})$ in Corollary 2.4.
- If ℓ is not prime to n, a possible choice for $\mathscr{S}$ is
$$\mathscr{S} = \{ \sum_{i \in [1..g]} \lambda_i e_i | \lambda_i \in [0..\ell-1] \}.$$

3 The addition relations

In this section we study the addition relations and introduce the notion of addition chain on the affine cone of an abelian variety. These addition chains will be a basic tool for the isogeny computation algorithm presented in Section 4 and Vélu's like formulas of Section 5.

In Section 3.1 we use the action of $G(\mathscr{L})$ on the affine cone and the canonical lift $s_{K(\mathscr{L})} : K(\mathscr{L}) \to G(\mathscr{L})$ to introduce some canonical affine lifts on the affine cone. In Section 3.2 we prove in the framework of Mumford's theory a particular presentation of the Riemann relations, and we deduce from them the addition relations. In Section 3.3 we use the results of Section 2.3 to study the properties of the addition chain.

3.1 The canonical lift of the action of $K(\mathscr{L})$ to the affine cone

For the rest of this article we suppose that we are given a modular point $(b_i)_{i \in Z(\overline{n})}$ corresponding to a triple $(B_k, \mathscr{L}_0, \Theta_{B_k})$. We choose a coordinate system $(\widetilde{\vartheta}_i^{\Theta_{B_k}})_{i \in Z(\overline{n})}$ on $\widetilde{B}_k$ and a $\widetilde{0}_{B_k} \in p_{B_k}^{-1}(0_{B_k})$. We remark that a choice of $\widetilde{0}_{B_k} \in p_{B_k}^{-1}(0_{B_k}) \subset \widetilde{B}_k$ is nothing but a choice of an evaluation isomorphism: $\varepsilon_0 : \mathscr{L}(0) \simeq k$. In this Section and Section 4 we also suppose that we are given a modular point $(a_i)_{i \in Z(\overline{\ell n})}$ corresponding to a triple $(A_k, \mathscr{L}, \Theta_{A_k})$ such that $\varphi_1((a_i)_{i \in Z(\overline{\ell n})}) = (b_i)_{i \in Z(\overline{n})}$ where $\varphi_1 : \mathscr{M}_{\overline{\ell n}} \to \mathscr{M}_{\overline{n}}$ is the modular correspondence introduced in Section 1. By Proposition 2.2 we then have an ℓ-isogeny π of type 1 between A_k and B_k. We choose a coordinate system $(\widetilde{\vartheta}_i^{\Theta_{A_k}})_{i \in Z(\overline{\ell n})}$ on $\widetilde{A}_k$ and we denote by $\widetilde{0}_{A_k}$ the unique point in $p_{A_k}^{-1}(0_{A_k})$ such that $\widetilde{0}_{B_k} = \widetilde{\pi}(\widetilde{0}_{A_k})$ where $\widetilde{\pi}$ is given by $\widetilde{\pi}^*(\widetilde{\vartheta}_i^{\Theta_{B_k}}) = \widetilde{\vartheta}_i^{\Theta_{A_k}}$ for $i \in Z(\overline{n})$.

We recall that the theta structure Θ_{A_k} define a section $s_{K(\mathscr{L})} : K(\mathscr{L}) \to G(\mathscr{L})$, so that the map $x \in K(\mathscr{L}) \mapsto s_{K(\mathscr{L})}(x).\widetilde{0}_{A_k} \in \widetilde{A}_k$ induces a section $K(\mathscr{L}) \to \widetilde{A}_k$ of the map $p_{A_k} : \widetilde{A}_k \to A_k$. (More generally this give a canonical section of the action by translation of $K(\mathscr{L})$ on A_k to an action on $\widetilde{A}_k$).

Thus, once we have chosen $\widetilde{0}_{A_k}$, we have a canonical way to fix an affine lift for any geometric point in $K(\mathscr{L})$. For $i \in Z(\overline{\ell n})$, let $\widetilde{P}_i = (1, i, 0).\widetilde{0}_{A_k}$, and for $j \in \hat{Z}(\overline{\ell n})$, let $\widetilde{Q}_j = (1, 0, j).\widetilde{0}_{A_k}$. We also put $\widetilde{R}_i = \widetilde{\pi}(\widetilde{P}_i) = \widetilde{\pi}_i(\widetilde{0}_{A_k})$, and $R_i = p_{B_k}(\widetilde{R}_i)$. We remark that $\{R_i\}_{i \in Z(\overline{\ell})}$ is the kernel $K_{\hat{\pi}}$ of $\hat{\pi}$ which explains the important role the points $\widetilde{R}_i$ will play in the rest of this paper.

3.2 The general Riemann relations

The Riemann relations (3) for $\mathscr{M}_{\overline{\ell n}}$ and the Riemann equations (2) for A_k are all particular case of more general Riemann relations, which we will use to get the addition relations on A_k. An analytic proof of (a partial fourier transform) of these relations can be found in [Igu72, Th.1 p. 137].

Theorem 3.1 (Generalized Riemann Relations):
Let $(A_k, \mathscr{L}, \Theta_{A_k}) \in \mathscr{M}_{\overline{n}}$ and we suppose that $2|n$. Let $x_1, y_1, u_1, v_1, z \in A_k(\overline{k})$ be such that $x_1 + y_1 + u_1 + v_1 = 2z$. Let $x_2 = z - x_1$, $y_2 = z - y_1$, $u_2 = z - u_1$ and $v_2 = z - v_1$. Then there exist $\widetilde{x}_1 \in p_{A_k}^{-1}(x_1)$, $\widetilde{y}_1 \in p_{A_k}^{-1}(y_1)$, $\widetilde{u}_1 \in p_{A_k}^{-1}(u_1)$, $\widetilde{v}_1 \in p_{A_k}^{-1}(v_1)$, $\widetilde{x}_2 \in p_{A_k}^{-1}(x_2)$, $\widetilde{y}_2 \in p_{A_k}^{-1}(y_2)$, $\widetilde{u}_2 \in p_{A_k}^{-1}(u_2)$, $\widetilde{v}_2 \in p_{A_k}^{-1}(v_2)$ that satisfy the following relations: for any $i, j, k, l, m \in Z(\overline{\ell n})$ such that $i + j + k + l = 2m$, let $i' = m - i$, $j' = m - j$, $k' = m - k$ and $l' = m - l$, then for all $\chi \in \hat{Z}(\overline{2})$, we have

$$\Big(\sum_{t \in Z(\overline{2})} \chi(t) \widetilde{\vartheta}_{i+t}(\widetilde{x}_1) \widetilde{\vartheta}_{j+t}(\widetilde{y}_1)\Big).\Big(\sum_{t \in Z(\overline{2})} \chi(t) \widetilde{\vartheta}_{k+t}(\widetilde{u}_1) \widetilde{\vartheta}_{l+t}(\widetilde{v}_1)\Big) =$$
$$\Big(\sum_{t \in Z(\overline{2})} \chi(t) \widetilde{\vartheta}_{i'+t}(\widetilde{x}_2) \widetilde{\vartheta}_{j'+t}(\widetilde{y}_2)\Big).\Big(\sum_{t \in Z(\overline{2})} \chi(t) \widetilde{\vartheta}_{k'+t}(\widetilde{u}_2) \widetilde{\vartheta}_{l'+t}(\widetilde{v}_2)\Big). \quad (7)$$

Proof: If $x = y = u = v = 0_A$, the preceding result gives the algebraic Riemann relations, a proof of which can be found in [Mum66, p. 333]. We just need to adapt the proof of Mumford for the general case.

Let p_1 and p_2 be the first and second projections from $A_k \times A_k$ to A_k. Let $\mathscr{M} = {p_1}^*(\mathscr{L}) \otimes {p_2}^*(\mathscr{L})$. The theta structure Θ_{A_k} induces a theta structure $\Theta_{A_k \times A_k}$ such that for $(i, j) \in Z(\overline{\ell n}) \times Z(\overline{\ell n})$ we have $\vartheta_{i,j}^{\Theta_{A \times A}} = \vartheta_i^{\Theta_{A_k}} \otimes \vartheta_j^{\Theta_{A_k}}$ (see [Mum66, Lem. 1 p. 323]). Consider the isogeny $\xi : A_k \times A_k \to A_k \times A_k, (x, y) \mapsto (x + y, x - y)$. We have $\xi^*(\mathscr{M}) = \mathscr{M}^2$. Since Θ_{A_k} is a symmetric theta structure Θ_{A_k}, there exists a theta structure $\Theta^{\mathscr{L}^2}$ on $\mathscr{L}^2$ such that $\Theta^{\mathscr{L}^2}$ and $\Theta^{\mathscr{L}}$ are compatible in the sense of Mumford [Mum66, p. 317]. The theta structure $\Theta^{\mathscr{L}^2}$ then induces a theta structure $\Theta^{\mathscr{M}^2}$ on $\mathscr{M}^2$. One can check that this theta structure is compatible with the isogeny ξ [Mum66, p. 325]. Applying the isogeny theorem (see [Mum66, p. 324]), we obtain that there exists $\lambda \in \overline{k}^*$ such that for all $i, j \in Z(\overline{\ell n})$:

$$\xi^*(\vartheta_i^{\mathscr{L}} \otimes \vartheta_j^{\mathscr{L}}) = \lambda \sum_{\substack{u,v \in Z(\overline{2ln}) \\ u+v=i \\ u-v=j}} (\vartheta_u^{\mathscr{L}^2} \otimes \vartheta_v^{\mathscr{L}^2}). \quad (8)$$

Considering this equation on the affine cone, we can always choose our affine lifts such that taking the evaluation at these lifts yield $\lambda = 1$. In the following we assume this is the case. Using equation (8) we compute for all $i,j \in Z(\overline{2\ell n})$ which are congruent modulo $Z(\overline{\ell n})$ and $\widetilde{x},\widetilde{y} \in A_k(\overline{k})$:

$$\begin{aligned}\sum_{t\in Z(\overline{2})} \chi(t)\widetilde{\vartheta}^{\mathscr{L}}_{i+j+t}(\widetilde{x+y})\widetilde{\vartheta}^{\mathscr{L}}_{i-j+t}(\widetilde{x-y}) &= \sum_{\substack{t\in Z(\overline{2})\\ u,v\in Z(\overline{2ln})\\ u+v=i+j+t\\ u-v=i-j+t}} \chi(t)\widetilde{\vartheta}^{\mathscr{L}^2}_{u}(\widetilde{x})\widetilde{\vartheta}^{\mathscr{L}^2}_{v}(\widetilde{y}) \\ &= \sum_{t_1,t_2\in Z(\overline{2})} \chi(t_1+t_2)\widetilde{\vartheta}^{\mathscr{L}^2}_{i+t_1}(\widetilde{x})\widetilde{\vartheta}^{\mathscr{L}^2}_{j+t_2}(\widetilde{y}) \\ &= \left(\sum_{t\in Z(\overline{2})} \chi(t)\widetilde{\vartheta}^{\mathscr{L}^2}_{i+t}(\widetilde{x})\right)\cdot\left(\sum_{t\in Z(\overline{2})} \chi(t)\widetilde{\vartheta}^{\mathscr{L}^2}_{j+t}(\widetilde{y})\right).\end{aligned} \tag{9}$$

So we have:

$$\begin{gathered}\Big(\sum_{t\in Z(\overline{2})} \chi(t)\widetilde{\vartheta}^{\mathscr{L}}_{i+j+t}(\widetilde{x+y})\widetilde{\vartheta}^{\mathscr{L}}_{i-j+t}(\widetilde{x-y})\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\widetilde{\vartheta}^{\mathscr{L}}_{k+l+t}(\widetilde{u+v})\widetilde{\vartheta}^{\mathscr{L}}_{k-l+t}(\widetilde{u-v})\Big) = \\ \Big(\sum_{t\in Z(\overline{2})} \chi(t)\widetilde{\vartheta}^{\mathscr{L}^2}_{\widetilde{i+t}}(\widetilde{x})\Big)\cdot\Big(\sum_{t\in Z(\overline{2})} \chi(t)\widetilde{\vartheta}^{\mathscr{L}^2}_{\widetilde{j+t}}(\widetilde{y})\Big)\cdot\Big(\sum_{t\in Z(\overline{2})} \chi(t)\widetilde{\vartheta}^{\mathscr{L}^2}_{\widetilde{k+t}}(\widetilde{u})\Big)\cdot\Big(\sum_{t\in Z(\overline{2})} \chi(t)\widetilde{\vartheta}^{\mathscr{L}^2}_{\widetilde{l+t}}(\widetilde{v})\Big) = \\ \Big(\sum_{t\in Z(\overline{2})} \chi(t)\widetilde{\vartheta}^{\mathscr{L}}_{i+l+t}(\widetilde{x+v})\widetilde{\vartheta}^{\mathscr{L}}_{i-l+t}(\widetilde{x-v})\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\widetilde{\vartheta}^{\mathscr{L}}_{k+j+t}(\widetilde{u+y})\widetilde{\vartheta}^{\mathscr{L}}_{k-j+t}(\widetilde{u-y})\Big).\end{gathered} \tag{10}$$

Now if we let $x = x_0 + y_0$, $y = x_0 - y_0$, $u = u_0 + v_0$ and $v = u_0 - v_0$, we have $x + y + u + v = 2(x_0 + u_0)$ so we can choose $z = x_0 + u_0$, so that $z - x = u_0 - y_0$, $z - y = u_0 + y_0$, $z - u = x_0 - v_0$, $z - v = x_0 + v_0$. By doing the same change of variable for i,j,k,l we see that the theorem is just a restatement of Equation (10). (see [Mum66, p. 334]). ■

From the generalized Riemann relations it is possible to derive addition relations.

Theorem 3.2 (Addition Formulas):
We suppose that $4|\ell n$. Let $x,y \in A_k(\overline{k})$ and suppose that we are given $\widetilde{x} \in p_{A_k}^{-1}(x)$, $\widetilde{y} \in p_{A_k}^{-1}(y)$, $\widetilde{x-y} \in p_{A_k}^{-1}(x-y)$, then there is a unique point $\widetilde{x+y} \in \widetilde{A}_k(\overline{k})$ such that for $i,j,k,l,m \in Z(\overline{\ell n})$ verifying $i+j+k+l = 2m$

$$\begin{aligned}\Big(\sum_{t\in Z(\overline{2})} \chi(t)\widetilde{\vartheta}_{i+t}(\widetilde{x+y})\widetilde{\vartheta}_{j+t}(\widetilde{x-y})\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\widetilde{\vartheta}_{k+t}(\widetilde{0}_{A_k})\widetilde{\vartheta}_{l+t}(\widetilde{0}_{A_k})\Big) = \\ \Big(\sum_{t\in Z(\overline{2})} \chi(t)\widetilde{\vartheta}_{-i'+t}(\widetilde{y})\widetilde{\vartheta}_{j'+t}(\widetilde{y})\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\widetilde{\vartheta}_{k'+t}(\widetilde{x})\widetilde{\vartheta}_{l'+t}(\widetilde{x})\Big),\end{aligned} \tag{11}$$

where i', j', k', l' are defined as in Theorem 3.1. We have $p_{A_k}(\widetilde{x+y}) = x + y$.

Thus the addition law on A_k extends to a pseudo addition law on $\widetilde{A}_k$; we call it an addition chain and we note $\widetilde{x+y} = \texttt{chain\_add}(\widetilde{x},\widetilde{y},\widetilde{x-y})$.

Proof: We apply the Riemann relations (7) to $x+y, x-y, 0_A, 0_A$. We have $2x=(x+y)+(x-y)+0_A+0_A$, $-y = x-(x+y)$, $y = x-(x-y)$, $x = x-0_A$, $x = x-0_A$ so Theorem 3.1 shows that there exist a point $\widetilde{x+y} \in \tilde{A}_k(\overline{k})$ satisfying the addition relations (1 1). (Remember that $(\vartheta_i(-y))_{i\in Z(\overline{\ell n})} = (\vartheta_{-i}(y))_{i \in Z(\overline{\ell n})}$, see Section 2.3.)

It remains to show that this point is unique. For this, it is enough to prove that for all $i,j,k,l,m \in Z(\overline{\ell n})$ such that $i+j+k+l=2m$ and all $\chi \in \hat{Z}(\overline{2})$ there exist $k',l',m' \in Z(\overline{\ell n})$ such that $i+j+k'+l'=2m'$ and $\sum_{t\in Z(\overline{2})} \tilde{\vartheta}_{k'+t}(\tilde{0}_{A_k})\tilde{\vartheta}_{l'+t}(\tilde{0}_{A_k}) \neq 0$. Then, by summing over the characters the first bracket of the left hand side of equation (11) we obtain the products $\tilde{\vartheta}_{i+t}(\widetilde{x+y})\tilde{\vartheta}_{j+t}(\widetilde{x-y})$ for $i,j \in Z(\overline{\ell n})$, from which we can recover the coordinates of the point $\widetilde{x+y}$.

Now, let $k_1, l_1 \in Z(\overline{2\ell n})$ be such that $k = k_1 + l_1$ and $l = k_1 - l_1$. Using formula (9), we get:

$$\sum_{t\in Z(\overline{2})} \chi(t)\tilde{\vartheta}^{\mathscr{L}}_{k_1+l_1}(\tilde{0}_{A_k})\tilde{\vartheta}^{\mathscr{L}}_{k_1-l_1}(\tilde{0}_{A_k}) = \left(\sum_{t\in Z(\overline{2})} \chi(t)\tilde{\vartheta}^{\mathscr{L}^2}_{k_1+l}(\tilde{0}_{A_k})\right)\cdot\left(\sum_{t\in Z(\overline{2})} \chi(t)\tilde{\vartheta}^{\mathscr{L}^2}_{l_1+t}(\tilde{0}_{A_k})\right) \quad (12)$$

Using [Mum66, p. 339 eq. (*)], we obtain that for all $\chi \in Z(\overline{2})$ there exists $k_1' \in k_1 + Z(\overline{\ell n})$ and $l_1' \in l_1 + Z(\overline{\ell n})$ such that:

$$\left(\sum_{t\in Z(\overline{2})} \chi(t)\tilde{\vartheta}^{\mathscr{L}^2}_{k_1+l}(\tilde{0}_{A_k})\right)\cdot\left(\sum_{t\in Z(\overline{2})} \chi(t)\tilde{\vartheta}^{\mathscr{L}^2}_{l_1+t}(\tilde{0}_{A_k})\right) \neq 0.$$

This complete the proof. ■

In order to obtain an efficient algorithm to compute addition chain, we first we reformulate the addition formulas (see [Mum66, p. 334]). Let $H = Z(\overline{\ell n}) \times \hat{Z}(\overline{2})$, and for $(i,\chi) \in H$ define

$$\tilde{u}_{i,\chi}(\tilde{x}) = \sum_{t\in Z(\overline{2})} \chi(t)\tilde{\vartheta}_{i+t}(\tilde{x}).$$

Then we have for all $i,j,k,l,m \in H$ such that $2m = i+j+k+l$

$$\begin{aligned}&\tilde{u}_i(\widetilde{x+y})\tilde{u}_j(\widetilde{x-y})\tilde{u}_k(\tilde{0}_{A_k})\tilde{u}_l(\tilde{0}_{A_k}) = \\ &\qquad \frac{1}{2^{2g}} \sum_{\xi\in H, 2\xi = \in Z(\overline{2})\times 0} (m_2+\xi_2)(2\xi_1)\tilde{u}_{i-m+\xi}(\tilde{y})\tilde{u}_{m-j+\xi}(\tilde{y})\tilde{u}_{m-k+\xi}(\tilde{x})\tilde{u}_{m-l+\xi}(\tilde{x}). \quad (13)\end{aligned}$$

It is easy to see that $(\tilde{\vartheta}_i(\tilde{x}))_{i\in Z(\overline{\ell n})}$, is determined by $(\tilde{u}_i(\tilde{x}))_{i\in H}$.

> **Algorithm 3.3 (Addition chain):**
> **Input** $\tilde{x}, \tilde{y}$ and $\widetilde{x-y}$ such that $p_{A_k}(\tilde{x}) - p_{A_k}(\tilde{y}) = p_{A_k}(\widetilde{x-y})$.
> **Output** $\widetilde{x+y} = \mathtt{chain\_add}(\tilde{x}, \tilde{y}, \widetilde{x-y})$.

➔ **For all** $i \in Z(\overline{\ell n})$, $\chi \in \hat{Z}(\overline{2})$ and $X \in \{\widetilde{x+y}, \widetilde{x}, \widetilde{y}, \widetilde{0}_{A_k}\}$ **compute**

$$\widetilde{u}_{i,\chi}(X) = \sum_{t \in Z(\overline{2})} \chi(t) \widetilde{\vartheta}_{i+t}(X).$$

➔ **For all** $i \in Z(\overline{\ell n})$, **choose** $j, k, l \in Z(\overline{\ell n})$ such that $i+j+k+l = 2m$, $\widetilde{u}_j(\widetilde{x-y}) \neq 0$, $\widetilde{u}_k(\widetilde{0}_{A_k}) \neq 0$, $\widetilde{u}_l(\widetilde{0}_{A_k}) \neq 0$ and **compute**

$$\widetilde{u}_i(\widetilde{x+y}) = \frac{1}{2^{2g} \widetilde{u}_j(\widetilde{x-y}) \widetilde{u}_k(\widetilde{0}_{A_k}) \widetilde{u}_l(\widetilde{0}_{A_k})} \sum_{\xi \in H, 2\xi = \in Z(\overline{2}) \times 0} (m_2 + \xi_2)(2\xi_1) \widetilde{u}_{i-m+\xi}(\widetilde{y}) \widetilde{u}_{m-j+\xi}(\widetilde{y}) \widetilde{u}_{m-k+\xi}(\widetilde{x}) \widetilde{u}_{m-l+\xi}(\widetilde{x}). \quad (14)$$

➔ **For all** $i \in Z(\overline{\ell n})$, **output**

$$\widetilde{\vartheta}_i(\widetilde{x+y}) = \frac{1}{2^g} \sum_{\xi \in \hat{Z}(\overline{2})} \widetilde{u}_{i,\chi}(\widetilde{x+y}).$$

Complexity Analysis 3.4:
As $\widetilde{u}_{i+t,\chi} = \chi(t)\widetilde{u}_{i,\chi}$ we only need to consider $(\ell n)^g$ coordinates and the linear transformation between $\widetilde{u}$ and $\widetilde{\vartheta}$ can be computed at the cost of $(2n\ell)^g$ additions in k. We also have $\widetilde{u}_{i,\chi}(-\widetilde{x}) = \widetilde{u}_{-i,\chi}(\widetilde{x})$.

Using the fact that for $t \in Z(\overline{2})$ the right hand terms of (14) corresponding to $\xi = (\xi_1 + t, \xi_2)$ and to $\xi = (\xi_1, \xi_2)$ are the same up to a sign, one can compute the left hand side of (14) with $4 \cdot 4^g$ multiplications and 4^g additions in k. In total one can compute an addition chain in $4.(4\ell n)^g$ multiplications, $(4\ell n)^g$ additions and $(\ell n)^g$ divisions in k. We remark that in order to compute several additions using the same point, there is no need to convert back to the $\widetilde{\vartheta}$ at each step so we only need to perform Step 2.

The addition chain formula is a basic step for all the algorithms to be presented in the sequel of this paper and we will use it as an unit of time for all our running time analysis. In some cases it is possible to greatly speed up this computation. See for instance [Gau07] which uses the duplication formula between theta functions to speed up the addition chain of level two. See also Section 4.1 where it is explained how to use isogenies to compute the addition chain for a general level by using only addition chains of level two, so that we can use the speed up of [Gau07] in general whatever the level of the theta structure is.

Remark 3.5:
The addition formulas can also be used to compute the usual addition law in A_k by choosing $j = 0$ in Equation (14) for every i.

The addition chain law on $\widetilde{A}_k$ induces a multiplication by a scalar law which reduces via p_{A_k} to the multiplication by a scalar deduced from the group law of A_k. Let $\widetilde{x}, \widetilde{y} \in \widetilde{A}_k$ and $\widetilde{x+y} \in p_{A_k}^{-1}(x+y)$, then we can compute $\widetilde{2x+y} := \texttt{chain\_add}(\widetilde{x+y}, \widetilde{x}, \widetilde{y})$. More generally there is a recursive algorithm to compute for every $m \geqslant 2$:

$$\widetilde{mx+y} := \texttt{chain\_add}(\widetilde{(m-1)x+y}, \widetilde{x}, \widetilde{(m-2)x+y})$$

We put $\texttt{chain\_multadd}(n,\widetilde{x+y},\widetilde{x},\widetilde{y}) := \widetilde{mx+y}$ and define

$$\texttt{chain\_mult}(m,\widetilde{x}) := \texttt{chain\_multadd}(m,\widetilde{x},\widetilde{x},\widetilde{0}_{A_k}).$$

We have $p_{A_k}(\texttt{chain\_mult}(m,\widetilde{x})) = m.p_{A_k}(\widetilde{x})$. We call chain_multadd a multiplication chain.

Algorithm 3.6 (Multiplication chain):
Input $m \in \mathbb{N}, \widetilde{x+y}, \widetilde{x}, \widetilde{y} \in \widetilde{A}_k$.
Output $\texttt{chain\_multadd}(m,\widetilde{x+y},\widetilde{x},\widetilde{y})$.

```
→ Compute the binary decomposition of $m := \sum_{i=0}^{I} b_i 2^i$. Set $m' := 0$, $\mathtt{xy}_0 := \widetilde{y}$, $\mathtt{xy}_{-1} := \texttt{chain\_add}(\widetilde{y},-\widetilde{x},\widetilde{x+y})$, $\mathtt{x}_0 := \widetilde{0}_{A_k}$ and $\mathtt{x}_1 := \widetilde{x}$.
→ For i in $[I..0]$ do
    If $b_i = 0$ then compute
        $\mathtt{x}_{2m'} := \texttt{chain\_add}(\mathtt{x}_{m'},\mathtt{x}_{m'},\mathtt{x}_0)$
        $\mathtt{x}_{2m'+1} := \texttt{chain\_add}(\mathtt{x}_{m'+1},\mathtt{x}_{m'},\mathtt{x}_1)$
        $\mathtt{xy}_{2m'} := \texttt{chain\_add}(\mathtt{xy}_{m'},\mathtt{x}_{m'},\mathtt{xy}_0)$
        $m' := 2m'.$
    Else compute
        $\mathtt{x}_{2m'+1} := \texttt{chain\_add}(\mathtt{x}_{m'+1},\mathtt{x}_{m'},\mathtt{x}_1)$
        $\mathtt{x}_{2m'+2} := \texttt{chain\_add}(\mathtt{x}_{m'+1},\mathtt{x}_{m'+1},\mathtt{x}_0)$
        $\mathtt{xy}_{2m'+1} := \texttt{chain\_add}(\mathtt{xy}_{m'},\mathtt{x}_{m'},\mathtt{xy}_{-1})$
        $m' := 2m'+1.$
→ Output $\mathtt{xy}_m$.
```

Correction and Complexity Analysis 3.7:
It is not completely trivial to see that $mx+y$ does not depend on the Lucas sequence used to compute it. We prove this in Corollary 3.13 where we show that multiplication chains are associative. In order to do as few division as possible, we use a Montgomery ladder [CFA⁺06, Alg. 9.5] for our Lucas sequence, hence the algorithm.

We see that a multiplication chain requires $O(\log(m))$ addition chains.

3.2.1 The case $n = 2$

Let $\mathscr{L}_0$ be a principal polarization associated to a symmetric irreductible divisor Θ. Then $\mathscr{L} = \mathscr{L}_0^2$ is of degree 2 and we have for all $i \in Z(\overline{2})$, $(-1)^*\vartheta_i = \vartheta_i$, where (-1) is the inverse automorphism on A_k. As a consequence, $\mathscr{L}$ gives an embedding of the Kummer variety $K_A = A_k/\pm 1$. Suppose that the even theta nulls for Θ are non zero. Then the embedding given by $\mathscr{L}$ in the projective space is an immersion. (See [Kem88, Cor. 5] and [Kem92, Th. 1] or [Koi76, Cor. 4.5.2].)

There is no properly defined addition law on K_A: from $\pm x \in K_A$ and $\pm y \in K_A$, we may compute $\pm x \pm y$ which gives two points on K_A. However, if we are also given $\pm(x-y) \in K_A$, then we can identify $\pm(x+y) \in \{\pm x \pm y\}$. Thus the addition chain law from Theorem 3.2 extends to a pseudo addition on the Kummer variety. With our hypothesis, by looking at the proof of Theorem 11 we see that we can use it to compute the pseudo addition law on the Kummer variety.

Let $x, y \in K_A$. To compute $\pm x \pm y$ without $\pm(x-y)$ we can proceed as follows: let $X = (X_i)_{i \in Z(\overline{2})}$, $Y = (Y_i)_{i \in Z(\overline{2})}$ be the two projections of the generic point on $K_A \times K_A$. Then the addition relations $X = \texttt{chain\_add}(x, y, Y)$ describe a system of degree 2 in $K_A \times K_A$, whose solutions are $(\pm(x+y), \pm(x-y))$ and $(\pm(x-y), \pm(x+y))$. From this system, it is easy to recover the points $\{\pm(x+y), \pm(x-y)\}$, but this involves a square root in k. (The preceding claims are proved in the preprint [LR10, Lemma 3].) We call this a normal addition, coming back to isogenies computations, it means that when working with $n = 2$, we have to avoid computing normal additions, since they require a square root and are much slower than addition chains.

Finally, to make our algorithms work with $n = 2$, we have to introduce the notion of compatible additions. Suppose that we are given $\pm x, \pm y, \pm z \in K_A$, together with $\pm(x+y)$, and $\pm(y+z)$. Using a normal addition we can compute $\{\pm(x+z), \pm(x-z)\}$; we want to find $\pm(x+z)$. If we apply the normal addition to $\pm x + y$ and $\pm x + z$ we find $\{\pm(2x+y+z), \pm(y-z)\}$ while the normal addition applied to $\pm x + y$ and $\pm x - z$ give $\{\pm(2x+y-z), \pm(y+z)\}$. This allows us to identify $\pm(x+z)$ if we suppose $2x \neq 0$, $2y \neq 0$, $2z \neq 0$, and $2(x+y+z) \neq 0$. We call this the compatible addition $\pm(x+z)$ with $\pm(x+y)$ and $\pm(y+z)$.

3.3 Theta group and addition relations

In this Section, we study the action of the theta group on the addition relations. We also show that addition relations are compatible with isogenies between two abelian varieties with compatible theta structures. By combining this we find the addition relations linking the coordinates of the points $\{\widetilde{R}_i\}_{i \in Z(\overline{\ell n})}$ on $\widetilde{B}_k$. By considering different modular point $(a_i)_{i \in Z(\overline{\ell n})} \in \varphi_1^{-1}((b_i)_{i \in Z(\overline{n})})$ and the associated isogenies $\pi : A_k \to B_k$, we can then understand the addition chains between any isotropic subgroup of $B_k[\ell]$ (see Section 1). In particular we exploit this to show that we can compute the chain multiplication by ℓ in $O(\log(\ell))$ addition chains.

Given the way the addition relations are set up as a consequence of the isogeny theorem, there should be no surprise that they are compatible with the action of the theta group. Still, some care must be taken, if we have $\widetilde{x}, \widetilde{y}, \widetilde{x+y}$ and $\widetilde{x-y} \in \widetilde{A}_k(\overline{k})$ such that

$$\widetilde{x+y} = \texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y}),$$

and we take $g_1, g_2 \in G(\mathscr{L})$, then by looking at the projections in A_k we certainly have

$$(g_1 \circ g_2).\widetilde{x+y} = \lambda \, \texttt{chain\_add}(g_1.\widetilde{x}, g_2.\widetilde{y}, (g_1 \circ g_2^{-1}).\widetilde{x-y})$$

where $\lambda \in k^\times$. However for trivial reasons, $\lambda \neq 1$ in general (See Lemma 3.10), so we have to work a bit to determine λ.

We begin with two easy lemmas.

Lemma 3.8:
Suppose that $\widetilde{x}_1, \widetilde{y}_1, \widetilde{u}_1, \widetilde{v}_1, \widetilde{x}_2, \widetilde{y}_2, \widetilde{u}_2, \widetilde{v}_2 \in \widetilde{A}_k(\overline{k})$ satisfy the general Riemann relations (7).

- *For every $g \in G(\mathscr{L})$, $g.\widetilde{x}_1, g.\widetilde{y}_1, g.\widetilde{u}_1, g.\widetilde{v}_1, g.\widetilde{x}_2, g.\widetilde{y}_2, g.\widetilde{u}_2, g.\widetilde{v}_2$ also satisfy the Riemann relations.*

- *For every ℓ-isogeny of type 1 $\pi : (A, \mathscr{L}, \Theta_{A_k}) \to (B, \mathscr{L}_0, \Theta_{B_k})$ such that Θ_{B_k} is π-compatible with Θ_{A_k}, then $\widetilde{\pi}(\widetilde{x}_1), \widetilde{\pi}(\widetilde{y}_1), \widetilde{\pi}(\widetilde{u}_1), \widetilde{\pi}(\widetilde{v}_1), \widetilde{\pi}(\widetilde{x}_2), \widetilde{\pi}(\widetilde{y}_2), \widetilde{\pi}(\widetilde{u}_2), \widetilde{\pi}(\widetilde{v}_2) \in \widetilde{B}_k$ also satisfy the Riemann relations.*

Proof: This is an immediate computation. ■

Lemma 3.9:
Let $(\alpha, i, j) \in \mathscr{H}(\overline{\ell n})$ and $\widetilde{x} \in \widetilde{A}_k$. Then we have $-(\alpha, i, j).\widetilde{x} = (\alpha, -i, -j).(-\widetilde{x})$, and $\widetilde{\pi}(-\widetilde{x}) = -\widetilde{\pi}(\widetilde{x})$.

In particular $-(\alpha, i, j).\widetilde{0}_{A_k} = (\alpha, -i, -j).\widetilde{0}_{A_k}$.

Proof: If $\widetilde{x} = (x_i)_{i \in Z(\overline{\ell n})}$, we recall that we have defined $-\widetilde{x} = (x_{-i})_{i \in Z(\overline{\ell n})}$. The fact than $-(\alpha, i, j).\widetilde{x} = (\alpha, -i, -j).(-\widetilde{x})$ is a direct consequence of the fact than the coordinates $(\widetilde{\vartheta}_i)_{i \in Z(\overline{\ell n})}$ of $\widetilde{x}$ are the theta functions associated to a symmetric theta structure. We can also check this with a direct computation: If $u \in Z(\overline{\ell n})$ we have by (1): $((\alpha, i, j).\widetilde{x})_u = \alpha\langle -u - i, j\rangle a_{u+i}$, $((\alpha, -i, -j).\widetilde{x})_{-u} = \alpha\langle u + i, -j\rangle \widetilde{x}_{-u-i} = a_{u+i} = x_u$. The rest of the lemma is trivial. ■

We now turn to the action of $\mathscr{H}(\overline{\ell n})$ on $\widetilde{A}_k$. Since $\mathscr{H}(\overline{\ell n})$ is generated by k^*, $Z(\overline{\ell n})$ and $\hat{Z}(\overline{\ell n})$ (where we embed $Z(\overline{\ell n})$ and $\hat{Z}(\overline{\ell n})$ in $\mathscr{H}(\overline{\ell n})$ with the usual sections), it is enough to study separately the action of these subgroup on the addition relation. The action of k^* is immediate:

Lemma 3.10:
For $\lambda_x, \lambda_y, \lambda_{x-y} \in \overline{k}^*$ and $\widetilde{x}, \widetilde{y} \in A_k(\overline{k})$, we have:

$$\texttt{chain\_add}(\lambda_x \widetilde{x}, \lambda_y \widetilde{y}, \lambda_{x-y} \widetilde{x-y}) = \frac{\lambda_x^2 \lambda_y^2}{\lambda_{x-y}} \texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y}), \tag{15}$$

$$\texttt{chain\_multadd}(n, \lambda_{x+y} \widetilde{x+y}, \lambda_x \widetilde{x}, \lambda_y \widetilde{y}) = \frac{\lambda_x^{n(n-1)} \lambda_{x+y}^n}{\lambda_y^{n-1}} \texttt{chain\_multadd}(n, \widetilde{x+y}, \widetilde{x}, \widetilde{y}), \tag{16}$$

$$\texttt{chain\_mult}(n, \lambda_x \widetilde{x}) = \lambda_x^{n^2} \texttt{chain\_mult}(n, \widetilde{x}). \tag{17}$$

Proof: Formula (15) is an immediate consequence of the addition formulas (11). The rest of the lemma follows by an easy recursion. ■

A more interesting result is the compatibility between the addition formulas and the action of $Z(\overline{\ell n})$ on $\widetilde{A}_k$:

Proposition 3.11 (Compatibility of the pseudo-addition law):
For $\widetilde{x}, \widetilde{y}, \widetilde{x-y} \in \widetilde{A}_k(k)$, and $i, j \in Z(\overline{\ell n})$, we have:

$$(1, i+j, 0).\texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y}) = \texttt{chain\_add}((1, i, 0).\widetilde{x}, (1, j, 0).\widetilde{y}, (1, i-j, 0).\widetilde{x-y}) \tag{18}$$

In particular if we set $\widetilde{P}_i = (1,i,0).\widetilde{0}_{A_k}$ *we have:*

$$\widetilde{P}_{i+j} = \texttt{chain\_add}(\widetilde{P}_i, \widetilde{P}_j, \widetilde{P}_{i-j})$$

Proof: Let $\widetilde{x+y} = \texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y})$. By Theorem 3.2, we have for every $a,b,c,d,e \in Z(\overline{\ell n})$ such that $a+b+c+d = 2e$:

$$\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{a+t}(\widetilde{x+y})\vartheta_{b+t}(\widetilde{x-y})\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{c+t}(\widetilde{0})\vartheta_{d+t}(\widetilde{0})\Big) = \\ \Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{-e+a+t}(\widetilde{y})\vartheta_{e-b+t}(\widetilde{y})\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{e-c+t}(\widetilde{x})\vartheta_{e-d+t}(\widetilde{x})\Big). \quad (19)$$

Applying (19) to $a' = a+i+j, b' = b+i-j, c' = c, d' = d, e' = e+i$, it comes:

$$\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{i+j+a+t}(\widetilde{x+y})\vartheta_{b+i-j+t}(\widetilde{x-y})\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{c+t}(\widetilde{0})\vartheta_{d+t}(\widetilde{0})\Big) = \\ \Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{-j-e+a+t}(\widetilde{y})\vartheta_{j+e-b}(\widetilde{y})\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{i+e-c+t}(\widetilde{x})\vartheta_{i+e-d+t}(\widetilde{x})\Big). \quad (20)$$

Thus $(1,i+j,0).\widetilde{x+y}, (1,i,0).\widetilde{x}, (1,j,0).\widetilde{y}$ and $(1,i-j,0).\widetilde{x-y}$ satisfy the additions relations.■

By applying $\widetilde{\pi}$, we obtain the following corollary:

Corollary 3.12:
For $\widetilde{x}, \widetilde{y}, \widetilde{x-y} \in \widetilde{A}_k$*, and* $i,j \in Z(\overline{\ell n})$*, we have:*

$$\widetilde{\pi}_{i+j}(\texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y})) = \texttt{chain\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{\pi}_j(\widetilde{y}), \widetilde{\pi}_{i-j}(\widetilde{x-y})).$$

Proof: Remember that by definition $\widetilde{\pi}_i(\widetilde{x}) = \widetilde{\pi}((1,i,0).\widetilde{x})$. The lemma is then a trivial consequence of Proposition 3.11 and Lemma 3.8. ■

We remark that by setting $\widetilde{x} = \widetilde{y} = \widetilde{0}_{A_k}$ in Corollary 3.12, we find

$$\widetilde{R}_{i+j} = \texttt{chain\_add}(\widetilde{R}_i, \widetilde{R}_j, \widetilde{R}_{i-j}).$$

By considering different isogenies $\pi : A_k \to B_k$, we can use Corollary 3.12 to study the associativity of chain additions:

Corollary 3.13:
Let $x \in B_k[\ell]$ *and* $y \in B_k$*. Choose any affine lifts* $\widetilde{x}$*,* $\widetilde{y}$ *and* $\widetilde{x+y}$ *of respectively* x*,* y *and* $x+y$*.*

1. *For all $n \in \mathbb{N}^*$, we put $\widetilde{nx} = \texttt{chain\_mult}(n, \widetilde{x})$ and $\widetilde{nx+y} = \texttt{chain\_multadd}(n, \widetilde{x+y}, \widetilde{x}, \widetilde{y})$. Then for all $n_1, n_2 \in \mathbb{N}^*$ such that $n_1 > n_2$, we have*

$$\widetilde{(n_1+n_2)x} = \texttt{chain\_add}(\widetilde{n_1x}, \widetilde{n_2x}, \widetilde{(n_1-n_2)x}), \tag{21}$$

$$\widetilde{(n_1+n_2)x+y} = \texttt{chain\_add}(\widetilde{n_1x+y}, \widetilde{n_2x}, \widetilde{(n_1-n_2)x+y}). \tag{22}$$

In particular, we see that $\widetilde{nx+y}$ and $\widetilde{nx}$ do not depend on the particular sequence of `chain_add` *used to compute them.*

2. *For all $n \in \mathbb{N}^*$, $-\widetilde{nx+y} = \texttt{chain\_add}(n, -(\widetilde{x+y}), -\widetilde{x}, -\widetilde{y})$*

Proof: First we prove assertion 1. Let $\hat{K}$ be a subgroup of $B_k[\ell]$ containing x which is maximal and isotropic for the Weil pairing. Consider the isogeny $\hat{\pi} : B_k \to D_k = B_k/\hat{K}$ and let $\pi : D_k \to B_k$ be the contragredient isogeny. We choose any theta structure on $(D_k, \pi^*\mathscr{L}_0)$ compatible with π. There exist $i, j \in Z(\overline{\ell})$ and $\lambda_i, \lambda_j \in \overline{k}^*$ such that $\widetilde{x} = \lambda_i \widetilde{\pi}_i(\widetilde{0}_{D_k})$ and $\widetilde{y} = \lambda_j \widetilde{\pi}_j(\widetilde{0}_{D_k})$. If $\lambda_i = \lambda_j = 1$, then the assertion 1. of Corollary 3.13 is a consequence of Corollary 3.12. But it is easy (see Lemma 3.10) to see that (21) is homogeneous in λ_i, hence the result.

Next we prove assertion 2. Once again, let $i \in Z(\overline{\ell})$ be such that $\widetilde{x} = \lambda_i \widetilde{\pi}\left((1, i, 0).\widetilde{0}_{D_k}\right)$, and let $\widetilde{y}'$ be any point in $\widetilde{\pi}^{-1}(\widetilde{y})$. By homogeneity we may suppose that $\lambda_i = 1$. By Corollary 3.12 and Proposition 3.11, we have $\widetilde{nx+y} = \widetilde{\pi}\left((1, n.i, 0).\widetilde{y}'\right)$. Now by Lemma 3.9, we have $-\widetilde{nx+y} = \widetilde{\pi}\left(-(1, n.i, 0).\widetilde{y}'\right) = \widetilde{\pi}\left((1, -n.i, 0).-\widetilde{y}'\right) = \texttt{chain\_add}(n, -(\widetilde{x+y}), -\widetilde{x}, -\widetilde{y})$. ■

The following remark concerning Corollary 3.12 is a useful fact to study the case ℓ not prime to n:

Remark 3.14:
Let $\widetilde{x} \in \widetilde{A}_k$, $i \in Z(\overline{\ell n})$ and let $\widetilde{y} = \widetilde{\pi}(\widetilde{x})$. Let $m \in \mathbb{Z}$ be such that $\ell | m$. By Proposition 3.11 and Corollary 3.12, we have

$$\widetilde{\pi}((1, mi, 0).\widetilde{x}) = \texttt{chain\_multadd}(m, \widetilde{\pi}_i(\widetilde{x}), \widetilde{R}_i, \widetilde{y}).$$

But if $\ell | m$, then $mi \in Z(\overline{n}) \subset Z(\overline{\ell n})$. By Proposition 2.3 we have $\widetilde{\pi}((1, mi, 0).\widetilde{x}) = (1, mi, 0).\widetilde{y}$, and $(1, mi, 0).\widetilde{y}$ can be computed with the formulas (1). Hence

$$(1, mi, 0).\widetilde{y} = \texttt{chain\_multadd}(m, \widetilde{\pi}_i(\widetilde{x}), \widetilde{R}_i, \widetilde{y}).$$

◇

In order to have a complete picture of the action of $\mathscr{H}(\overline{\ell n})$ on $\widetilde{A}_k$, we have yet to describe the action of $\hat{Z}(\overline{\ell n})$ on $\widetilde{A}_k$. In order to do so, we recall from Section 2.2 that $\mathfrak{I}$ is the automorphism of the Theta group that permutes K_1 and K_2. Since $s_{K_2(\mathscr{L})} = \mathfrak{I} \circ s_{K_1(\mathscr{L})} \circ \mathfrak{I}$, we just have to explain what is the action of of $\mathfrak{I}$ on the addition relations.

Proposition 3.15:
Suppose that $x, y, u, v, x', y', u', v' \in \widetilde{A}_k(\overline{k})$ satisfy the general Riemann equations (7). Then $\mathfrak{I}.x$, $\mathfrak{I}.y$, $\mathfrak{I}.u$, $\mathfrak{I}.v$, $\mathfrak{I}.x'$, $\mathfrak{I}.y'$, $\mathfrak{I}.u'$, $\mathfrak{I}.v'$ also satisfy (7).

Proof: If $x = (x_i)_{i \in Z(\overline{\ell n})}$ we recall (see (5)) that

$$\mathfrak{I}.x = (\sum_{j \in Z(\overline{\ell n})} e(i,j) x_j)_{i \in Z(\overline{\ell n})}$$

where $e = e_{\mathscr{L}}$ is the commutator pairing.

By hypothesis, we have for $i, j, k, l \in Z(\overline{\ell n})$ such that $i + j + k + l = 2m$:

$$(\sum_{t \in Z(\overline{2})} \widetilde{\vartheta}_{i+t}(x) \widetilde{\vartheta}_{j+t}(y)).(\sum_{t \in Z(\overline{2})} \widetilde{\vartheta}_{k+t}(u) \widetilde{\vartheta}_{l+t}(v)) = \\ (\sum_{t \in Z(\overline{2})} \widetilde{\vartheta}_{i'+t}(x') \widetilde{\vartheta}_{j'+t}(y')).(\sum_{t \in Z(\overline{2})} \widetilde{\vartheta}_{k'+t}(u') \widetilde{\vartheta}_{l'+t}(v')). \quad (23)$$

Let $A_{\chi,x,y,i,j} = (\sum_{t \in Z(\overline{2})} \chi(t) \widetilde{\vartheta}_{i+t}(x) \widetilde{\vartheta}_{j+t}(y))$. If $I, J, K, L \in Z(\overline{\ell n})$ are such that $I + J + K + L = 2M$, we have:

$$\begin{aligned} A_{\chi,\mathfrak{I}.x,\mathfrak{I}.y,I,J} &= \sum_{T \in Z(\overline{2})} \chi(T) (\sum_{i \in Z(\overline{\ell n})} e(I+T,i) \widetilde{\vartheta}_i(x)) (\sum_{j \in Z(\overline{\ell n})} e(J+T,j) \widetilde{\vartheta}_j(x)) \\ &= \sum_{T \in Z(\overline{2}), i,j \in Z(\overline{\ell n})} \chi(T) e(T, i+j) e(I,i) e(J,j) \widetilde{\vartheta}_i(x) \widetilde{\vartheta}_j(y) \end{aligned}$$

$$\begin{aligned} & A_{\chi,\mathfrak{I}.x,\mathfrak{I}.y,I,J} A_{\chi,\mathfrak{I}.u,\mathfrak{I}.v,K,L} = \\ & \sum_{\substack{T_1,T_2 \in Z(\overline{2}) \\ i,j,k,l \in Z(\overline{\ell n})}} \chi(T_1+T_2) e(T_1, i+j) e(T_2, k+l) e(I,i) e(J,j) e(K,k) e(L,l) \widetilde{\vartheta}_i(x) \widetilde{\vartheta}_j(y) \widetilde{\vartheta}_k(u) \widetilde{\vartheta}_l(v) \\ & \qquad = \sum_{i,j,k,l \in Z(\overline{\ell n})} e(I,i) e(J,j) e(K,k) e(L,l) \widetilde{\vartheta}_i(x) \widetilde{\vartheta}_j(y) \widetilde{\vartheta}_k(u) \widetilde{\vartheta}_l(v) \\ & \qquad\qquad (\sum_{T_1,T_2 \in Z(\overline{2})} \chi(T_1+T_2) e(T_1, i+j) e(T_2, k+l)) \end{aligned}$$

But

$$(\sum_{T_1,T_2 \in Z(\overline{2})} \chi(T_1+T_2) e(T_1, i+j) e(T_2, k+l)) = \begin{cases} 4^g & \text{if } e(\cdot, i+j) = e(\cdot, k+l) = \chi \\ 0 & \text{otherwise} \end{cases}$$

and $e(\cdot, i+j) = e(\cdot, k+l)$ (as characters on $Z(\overline{2})$) if and only if there exists $m \in Z(\overline{\ell n})$ such that $i + j + k + l = 2m$. Now since $I + J + K + L = 2M$ we have $e(I+J, \cdot) = e(K+L, \cdot)$ and as a consequence:

$$\lambda \sum_{t_1,t_2\in Z(\overline{2})} e(I,i+t_1)e(J,j+t_1)e(K,k+t_2)e(L,l+t_2)\widetilde{\vartheta}_{i+t_1}(x)\widetilde{\vartheta}_{j+t_1}(y)\widetilde{\vartheta}_{k+t_2}(u)\widetilde{\vartheta}_{l+t_2}(v)=$$
$$\lambda e(I,i)e(J,j)e(K,k)e(L,l) \sum_{t_1,t_2\in Z(\overline{2})} \widetilde{\vartheta}_{i+t_1}(x)\widetilde{\vartheta}_{j+t_1}(y)\widetilde{\vartheta}_{k+t_2}(u)\widetilde{\vartheta}_{l+t_2}(v)=$$
$$\lambda e(I,i)e(J,j)e(K,k)e(L,l) \sum_{t_1,t_2\in Z(\overline{2})} \widetilde{\vartheta}_{i'+t_1}(x')\widetilde{\vartheta}_{j'+t_1}(y')\widetilde{\vartheta}_{k'+t_2}(u')\widetilde{\vartheta}_{l'+t_2}(v)=$$
$$\lambda e(I',i')e(J',j')e(K',k')e(L',l') \sum_{t_1,t_2\in Z(\overline{2})} \widetilde{\vartheta}_{i'+t_1}(x')\widetilde{\vartheta}_{j'+t_1}(y')\widetilde{\vartheta}_{k'+t_2}(u')\widetilde{\vartheta}_{l'+t_2}(v)$$

where $\lambda = 4^g$ if $i+j+k+l=2m$ and $\lambda=0$ otherwise. By combining these relations we find that

$$A_{\chi,\mathfrak{I}.x,\mathfrak{I}.y,I,J}A_{\chi,\mathfrak{I}.u,\mathfrak{I}.v,K,L} = A_{\chi,\mathfrak{I}.x',\mathfrak{I}.y',I',J'}A_{\chi,\mathfrak{I}.u',\mathfrak{I}.v',K,L}.$$

which concludes the proof. ■

Corollary 3.16:
Let $\widetilde{x},\widetilde{y},\widetilde{x-y} \in \widetilde{A}_k(\overline{k})$, and let $i,j\in Z(\overline{\ell n})$, $k,l\in \hat{Z}(\overline{\ell n})$. Then we have:

$$\begin{aligned}(1,i+j,k+l).\,\texttt{chain\_add}(\widetilde{x},\widetilde{y},\widetilde{x-y})\\ = \texttt{chain\_add}((1,i,k).\widetilde{x},(1,j,l).\widetilde{y},(1,i-j,k-l).\widetilde{x-y}).\end{aligned} \tag{24}$$

Proof: By Propositions 3.11 and 3.15 we have

$$(1,0,k+l).\,\texttt{chain\_add}(\widetilde{x},\widetilde{y},\widetilde{x-y}) = \texttt{chain\_add}((1,0,k).\widetilde{x},(1,0,l).\widetilde{y},(1,0,k-l).\widetilde{x-y}) \tag{25}$$

Now since $(1,i,k)=(1,0,k)(1,i,0)$, we conclude by combining Equations (18) and (25). ■

Using Proposition 3.15, we can prove that the addition relations are compatible with any isogeny.

Corollary 3.17:
Suppose that $\widetilde{x}_1,\widetilde{y}_1,\widetilde{u}_1,\widetilde{v}_1,\widetilde{x}_2,\widetilde{y}_2,\widetilde{u}_2,\widetilde{v}_2 \in \widetilde{A}_k$ satisfy the Riemann relations (7). If $\pi:(A,\mathscr{L},\Theta_{A_k})\to(B,\mathscr{L}_0,\Theta_{B_k})$ is an isogeny such that Θ_{B_k} is π-compatible with Θ_{A_k}, then $\widetilde{\pi}(\widetilde{x}_1)$, $\widetilde{\pi}(\widetilde{y}_1)$, $\widetilde{\pi}(\widetilde{u}_1)$, $\widetilde{\pi}(\widetilde{v}_1)$, $\widetilde{\pi}(\widetilde{x}_2)$, $\widetilde{\pi}(\widetilde{y}_2)$, $\widetilde{\pi}(\widetilde{u}_2)$, $\widetilde{\pi}(\widetilde{v}_2)\in\widetilde{B}_k$ also satisfy the general Riemann Relations. In particular, for all $\widetilde{x},\widetilde{y},\widetilde{x-y}\in\widetilde{A}_k$, we have

$$\widetilde{\pi}(\texttt{chain\_add}(\widetilde{x},\widetilde{y},\widetilde{x-y}) = \texttt{chain\_add}(\widetilde{\pi}(\widetilde{x}),\widetilde{\pi}(\widetilde{y}),\widetilde{\pi}(\widetilde{x-y})).$$

Proof: It is easy to see that Lemma 3.8 is valid for any compatible isogenies of type 1 (it is not restricted to ℓ-isogenies). By Proposition 3.15, we can apply Lemma 3.8 also in the case of compatible isogenies of type 2, which concludes since every compatible isogeny is a composition of isogenies of type 1 or 2.■

4 Application of the addition relations to isogenies

In this Section we apply the results of Section 3 to the computation of isogenies (see Section 4.2). More precisely, we present an algorithm to compute the isogeny $\hat{\pi} : B_k \rightarrow A_k$ from the knowledge of the modular point $\widetilde{0}_{A_k}$. We give in Section 5 algorithms to compute $\widetilde{0}_{A_k}$ from the kernel of $\hat{\pi}$.

But first, we remark that since the embedding of A_k that we consider is given by a theta structure of level $\overline{\ell n}$, a point $\hat{\pi}(x)$ is given by $(\ell n)^g$ coordinates, which get impractical because of memory consumption when ℓ is big. In order to mitigate this problem, in Section 4.1, we give a point compression algorithm such that the number of coordinates of a compressed point does not depend on ℓ.

We recall that we have chosen in Section 3.1 $\widetilde{0}_{A_k} = (a_i)_{i \in Z(\overline{\ell n})}$ such that $\widetilde{\pi}(\widetilde{0}_{A_k}) = \widetilde{0}_{B_k}$, and that we have defined for $i \in Z(\overline{\ell n})$, $\widetilde{R}_i = (a_{i+j})_{j \in Z(\overline{n})} \in \widetilde{B}_k(\overline{k})$.

4.1 Point compression

Suppose that ℓ is prime to n. We know that $\widetilde{x} \in \widetilde{A}_k(\overline{k})$ can be recovered from $(\widetilde{\pi}_i(\widetilde{x}))_{i \in Z(\overline{\ell})}$, by $(\widetilde{x})_{ni+\ell j} = (\widetilde{\pi}_i(\widetilde{x}))_j$. If $(d_1, \cdots, d_g)$ is a basis of $Z(\overline{\ell})$, we can prove that $\widetilde{x}$ can be easily computed from just $(\widetilde{\pi}_{d_i}(\widetilde{x}))_{i \in [1..g]}$ and $(\widetilde{\pi}_{d_i + d_j}(\widetilde{x}))_{i,j \in [1..g]}$. If $(e_1, \cdots, e_g)$ is the canonical basis of $Z(\overline{\ell n})$, in the following, we take $(d_i = ne_i)_{i \in [1..g]}$ as a basis of $Z(\overline{\ell})$.

Proposition 4.1:
Let $\widetilde{x} \in \widetilde{A}_k(\overline{k})$ and $i, j \in Z(\overline{\ell n})$. We have

$$\widetilde{\pi}_{i+j}(\widetilde{x}) = \texttt{chain\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{R}_j, \widetilde{\pi}_{i-j}(\widetilde{x})).$$

Proof: We apply Corollary 3.12 with $\widetilde{y} = \widetilde{0}_{A_k}$, $\widetilde{x-y} = \widetilde{x}$, so that we have $\texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y}) = \widetilde{x}$. We obtain:

$$\widetilde{\pi}_{i+j}(\widetilde{x}) = \texttt{chain\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{\pi}_j(\widetilde{0}_{A_k}), \widetilde{\pi}_{i-j}(\widetilde{x})). \qquad \blacksquare$$

Definition 4.2:
Let $S \subset G$ be a subset of a finite abelian group G such that $0_G \in S$. We denote by S' the smallest subset of G (for the inclusion) such that $S' \supset S$ and $S' = S' \bigcup \{x + y | x \in S', y \in S', x - y \in S'\}$. We say that S is a chain basis of G if $S' = G$.

Example 4.3:
Let $G = Z(\ell)$. Let $(e_1, \cdots, e_g)$ be the canonical basis of G. If ℓ is odd, a chain basis of G is given by

$$S = \{0_G, e_i, e_i + e_j\}_{i,j \in [1..g], i<j}.$$

If ℓ is even, a chain basis of G is given by

$$S = \{0_G, e_{i_1}, e_{i_1} + e_{i_2}, \cdots, e_{i_1} + \cdots + e_{i_g}\}_{i_1, \cdots, i_g \in [1..g], i_1 < \cdots < i_g}.$$

In each case, the chain basis S is minimal, we call it the canonical chain basis $\mathfrak{S}(G)$ of G.

We recall that, in Example 2.5, we have defined $\mathscr{S} \subset Z(\overline{\ell n})$ such that $\mathscr{S} + Z(\overline{n}) = Z(\overline{\ell n})$. To $\mathscr{S}$ we associate a canonical chain basis $\mathfrak{S} \subset \mathscr{S}$ as follow: if ℓ is prime to n, then $\mathscr{S} = Z(\overline{\ell}) \subset Z(\overline{\ell n})$, and we define $\mathfrak{S} = \mathfrak{S}(Z(\overline{\ell})) = \{d_1, \cdots, d_g, d_1+d_g, \cdots, d_{g-1}+d_g\}$. Otherwise we take $\mathfrak{S} = \mathfrak{S}(Z(\overline{\ell n}))$.

Theorem 4.4 (Point compression):
Let $\widetilde{x} \in \widetilde{A}_k(k)$. The point $\widetilde{x}$ is uniquely determined by $\widetilde{0}_{A_k}$ and $\{\widetilde{\pi}_i(\widetilde{x})\}_{i\in\mathfrak{S}}$. Moreover, $\widetilde{0}_{A_k}$ is uniquely determined by $\{\widetilde{\pi}_i(\widetilde{0}_{A_k})\}_{i\in\mathfrak{S}} = \{\widetilde{R}_i\}_{i\in\mathfrak{S}}$.

Proof: By Proposition 3.11 we have $\widetilde{\pi}_{i+j}(\widetilde{x}) = \texttt{chain\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{\pi}_j(\widetilde{0}_{A_k}), \widetilde{\pi}_{i-j}(\widetilde{x}), \widetilde{0}_{B_k})$. So by induction, from $\{\widetilde{\pi}_i(x)\}_{i\in\mathfrak{S}}$ we can compute every $\{\widetilde{\pi}_i(x)\}_{i\in\mathfrak{S}'}$. Since $\mathfrak{S}' = \mathscr{S}$ (or contains $\mathscr{S}$ if n is not prime to ℓ), Corollary 2.4 shows that $\widetilde{x}$ is entirely determined by $\{\widetilde{\pi}_i(x)\}_{i\in\mathfrak{S}}$ and $\{\widetilde{\pi}_i(\widetilde{0}_{A_k})\}_{i\in\mathfrak{S}}$.

In particular, $\widetilde{0}_{A_k}$ is entirely determined by $\{\widetilde{\pi}_i(\widetilde{0}_{A_k})\}_{i\in\mathfrak{S}}$. But $\widetilde{\pi}_i(\widetilde{0}_{A_k}) = \widetilde{\pi}(\widetilde{P}_i)$ by Proposition 2.3 and we are done. ■

In the description of the algorithms, we suppose that ℓ is prime to n, so that $\mathscr{S} = Z(\overline{\ell}) \subset Z(\overline{\ell n})$.

Algorithm 4.5 (Point compression):
Input $\widetilde{x} = (\vartheta_i(\widetilde{x}))_{i\in Z(\overline{\ell n})} \in \widetilde{A}_k(\overline{k})$
Output The compressed coordinates $(\widetilde{\pi}_i(\widetilde{x}))_{i\in\mathfrak{S}}$.

```
➔ For each $i \in \mathfrak{S}$, output $(\widetilde{\pi}_i(\widetilde{x})) = (\widetilde{\vartheta}_{ni+\ell j}(\widetilde{x}))_{j\in Z(\overline{n})}$
```

Algorithm 4.6 (Point decompression):
Input The compressed coordinates $\widetilde{\pi}(\widetilde{x})_{i\in\mathfrak{S}}$ of $\widetilde{x}$.
Ouput $\widetilde{x} = (\widetilde{\vartheta}_i(\widetilde{x}))_{i\in Z(\overline{\ell n})} \in \widetilde{A}_k(\overline{k})$.

```
➔ (Step 1) Set $\mathscr{S}' := \mathfrak{S}$.
➔ (Step 2) While $\mathscr{S}' \neq \mathscr{S}$.
    • Choose $i, j \in \mathscr{S}'$ such that $i + j \in \mathscr{S} \setminus \mathscr{S}'$ and $i - j \in \mathscr{S}'$.
    • Compute $\widetilde{\pi}_{i+j}(\widetilde{x}) = \texttt{chain\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{R}_j, \widetilde{\pi}_{i-j}(\widetilde{x}))$.
    • $\mathscr{S}' := \mathscr{S}' \bigcup \{i + j\}$.
➔ (Step 3) For all $i \in Z(\overline{\ell n})$, write $i = ni_0 + \ell j$ and output $\widetilde{\vartheta}_i(x) = \left(\widetilde{\pi}_{i_0}(\widetilde{x})\right)_j$.
```

Correction and Complexity Analysis 4.7:
By using repeatedly the formula from Proposition 3.11:

$$\widetilde{\pi}_{i+j}(\widetilde{x}) = \texttt{chain\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{R}_j, \widetilde{\pi}_{i-j}(\widetilde{x}), \widetilde{0}_{B_k})$$

we can reconstitute every $\widetilde{\pi}_i(\widetilde{x})$ for $i \in Z(\overline{\ell})$ in Step 2 since $\mathfrak{S}$ is a chain basis of $Z(\overline{\ell})$. We can then trivially recover the coordinates of $\widetilde{x}$ in Step 3 since they are just a permutation of the coordinates of the $\{\widetilde{\pi}_i(\widetilde{x}), i \in Z(\overline{\ell})\}$

(see Section 2.4). To recover $\widetilde{x}$, we need to do $\#\mathscr{S} - \#\mathfrak{S} = O(\ell^g)$ chain additions. The compressed point $\{\widetilde{\pi}_i(\widetilde{x})\}_{i \in \mathfrak{S}}$ is given by $\#\mathfrak{S} \times n^g$ coordinates.

If $\ell n = 2n_0$ and n_0 is odd we see that we can store a point in $\widetilde{A}_k$ with $2^g(1+g(g+1)/2)$ coordinates (4^g if n_0 is even) rather than $(2n_0)^g$.

4.1.1 Addition chains with compressed coordinates

Let $\widetilde{x}, \widetilde{y}$ and $\widetilde{x-y} \in \widetilde{A}_k$. Suppose that we have the compressed coordinates $(\widetilde{\pi}_i(\widetilde{x}))_{i \in \mathfrak{S}}$, $(\widetilde{\pi}_i(\widetilde{y}))_{i \in \mathfrak{S}}$, $(\widetilde{\pi}_i(\widetilde{x-y}))_{i \in \mathfrak{S}}$. Then if $i \in \mathfrak{S}$ we have by Corollary 3.12

$$\widetilde{\pi}_i(\widetilde{x+y}) = \mathtt{chain\_add}(\widetilde{\pi}_i(\widetilde{x}), \widetilde{\pi}_0(\widetilde{y}), \widetilde{\pi}_i(\widetilde{x-y}),$$

hence we may recover the compressed coordinates of $\widetilde{x+y}$.

We can compare the running time of addition chain with the full coordinates representation (of level ℓn) and the compressed representation. By the formulas from Theorem 3.2, since $2|n$ and the formulas sum over points of 2-torsion, we see that we are doing $\#\mathscr{S}$ addition chains in B_k using representations of level n. The additions chains with the compressed representation are much faster than the addition chains with the full representation since we need to do only $\#\mathfrak{S}$ addition chains of level n. In particular, since we can compute the multiplication by m with chain additions, we see that the cost of a multiplication by m is $O(\#\mathfrak{S} \log(m))$ addition chains of level n (and a point decompression if we want to recover the full coordinates).

Since we can take $n = 2$, the additions formulas of level 2 allows us to compute addition chains of any level. In particular the speed up for these formulas given by [Gau07] can be used for all levels.

4.2 Computing the dual isogeny

We recall that we have the following diagram:

$$\begin{tikzcd}
x \in A_k(\overline{k}) \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A_k(\overline{k}) \\
& y \in B_k(\overline{k}) \arrow[ur, "\hat{\pi}"'] &
\end{tikzcd}$$

Let $\widetilde{y} \in p_{B_k}^{-1}(y)$ and let $\widetilde{x} \in \widetilde{A}_k(\overline{k})$ be such that $\widetilde{\pi}(\widetilde{x}) = \widetilde{y}$. Let $i \in Z(\overline{\ell})$. In this section, we describe an algorithm to compute $\widetilde{\pi}_i(\ell.\widetilde{x})$ efficiently from the knowledge of $\widetilde{y}$ and $\widetilde{0}_{A_k}$ (i.e. without using $\widetilde{x}$ which may be hard to compute). By using this algorithm for $i \in \{d_1, \cdots, d_g, d_1 + d_2, \cdots d_{g-1} + d_g\}$, we can then recover $\hat{\pi}(y) = p_{A_k}(\ell.\widetilde{x})$ (see Theorem 4.4), where $(d_i)_{i \in [1..g]}$ is the basis of $Z(\overline{\ell})$ defined in Section 4.1). We know that $\pi_i(x) = y + R_i$ where $x = p_{A_k}(\widetilde{x})$. For $i \in Z(\overline{\ell})$, we choose a point $\pi_i^a(x) \in p_A^{-1}(y + R_i)$ so that for each $i \in Z(\overline{\ell})$ there exists $\lambda_i \in \overline{k}^*$ such that $\widetilde{\pi}_i(\widetilde{x}) = \lambda_i \pi_i^a(x)$. If $\widetilde{x}'$ is another point in $\widetilde{\pi}^{-1}(\widetilde{y})$, then we have $\widetilde{\pi}_i(\widetilde{x}') = \lambda'_i \pi_i^a(x)$, with $\lambda'_i = \zeta \lambda_i$, ζ a ℓ^{th}-root of unity by Section 2.3. As a consequence, it is possible to recover λ_i only up to an ℓ^{th}-root of unity, but this information is sufficient to compute $\widetilde{\pi}_i(\ell.\widetilde{x})$:

Theorem 4.8:
Let $\widetilde{y} \in \widetilde{B}_k(\overline{k})$ and let $\widetilde{x} \in \widetilde{A}_k(\overline{k})$ be such that $\widetilde{\pi}(\widetilde{x}) = \widetilde{y}$. For all $i \in Z(\overline{\ell})$,

$$\widetilde{\pi}_i(\ell.\widetilde{x}) = \lambda_i^\ell \, \texttt{chain\_multadd}(\ell, \pi_i^a(x), \widetilde{y}, \widetilde{R}_i)),$$

where λ_i^ℓ is determined by:

$$\widetilde{y} = \lambda_i^\ell \, \texttt{chain\_multadd}(\ell, \pi_i^a(x), \widetilde{R}_i, \widetilde{y}).$$

Proof: By Proposition 3.11 and Lemma 3.10 we have:

$$\widetilde{\pi}_i(\ell.\widetilde{x}) = \texttt{chain\_multadd}(\ell, \widetilde{\pi}_i(\widetilde{x}), \widetilde{\pi}(\widetilde{x}), \widetilde{\pi}(\widetilde{P}_i)) = \lambda_i^\ell \, \texttt{chain\_multadd}(\ell, \pi_i^a(x), \widetilde{y}, R_i).$$

Now we only need to find the λ_i^ℓ for $i \in Z(\overline{\ell})$. But by Proposition 3.11 and an easy recursion, we have $\widetilde{x} = s_{K_1(\mathscr{L})}(i)^\ell.\widetilde{x}$ so that by Corollary 3.12 and Lemma 3.10

$$\widetilde{\pi}(\widetilde{x}) = \texttt{chain\_multadd}(\ell, \widetilde{\pi}_i(\widetilde{x}), R_i, \widetilde{y}) = \lambda_i^\ell.\texttt{chain\_multadd}(\ell, \pi_i^a(x), R_i, \widetilde{y}). \qquad \blacksquare$$

Remark 4.9:
We can use the preceding theorem recover the equations of the isogeny by taking for y the generic point of B_k. ♢

Algorithm 4.10 (The image of a point by the isogeny):

```
Input  $y \in B_k(\overline{k})$.
Output  The compressed coordinates of $\hat{\pi}(y) \in A_k(\overline{k})$.
  ➔ For each $i \in \mathfrak{S}$
      • (Step 1) Compute $y + R_i$ and choose an affine lift $y_i$ of $y + R_i$.
      • (Step 2) Compute $\texttt{ylR}_i := \texttt{chain\_multadd}(\ell, y_i, \widetilde{R}_i, y_0)$
        Let $\lambda_i$ be such that $y_0 = \lambda_i \texttt{ylR}_i$.
      • Output $\lambda_i \, \texttt{chain\_multadd}(\ell, y_i, y_0, \widetilde{R}_i))$.
```

Correction and Complexity Analysis 4.11:
Let $\widetilde{y} = y_0$, and $\widetilde{x} \in \widetilde{A}_k(\overline{k})$ be such that $\widetilde{\pi}(\widetilde{x}) = \widetilde{y}$, and let $\widetilde{z} = \ell\widetilde{x}$. Then $p_{A_k}(\widetilde{z}) = \hat{\pi}(y)$ and we note $\widetilde{z} = \hat{\pi}(\widetilde{y})$. In the Output, Theorem 4.8 show that we compute $\widetilde{\pi}_i(\hat{\pi}(\widetilde{y})) = \lambda_i^\ell \, \texttt{chain\_multadd}(\ell, y_i, y_0, \widetilde{R}_i))$ since λ_i^ℓ is given in Step 2 by $y_0 = \lambda_i^\ell \, \texttt{chain\_multadd}(\ell, y_i, \widetilde{R}_i, \widetilde{y})$.

We can easily recover $\hat{\pi}(y)$ from the $\widetilde{\pi}_i(\hat{\pi}(\widetilde{y}))$, $i \in Z(\overline{\ell})$, but we note that it is faster to compute the $\widetilde{\pi}_i(\hat{\pi}(\widetilde{y}))$ only for $i \in \mathfrak{S}$ (with the notations of Example 4.3 in the preceding section). and then use Algorithm 4.7 to obtain the full coordinates of $\hat{\pi}(y)$. This last step is unnecessary if we only need the compressed coordinates of $\hat{\pi}(y)$.

To compute $\widetilde{\pi}_i(\hat{\pi}(\widetilde{y}))$, we need to do two multiplication chains of length ℓ. We obtain the compressed coordinates of $\ell.x$ after $g(g+1)/2$ such operations. In total we can compute the compressed coordinates of a point in $O(\frac{1}{2}g(g+1)\log(\ell))$ additions in B_k (with $\frac{1}{2}g(g+1)n^g$ divisions in k) and the full coordinates in $O(\ell^g)$ additions in B_k.

The kernel of the isogeny We know that the kernel of the isogeny $\hat{\pi} : B_k \rightarrow A_k$ is the subgroup K generated by $\{R_{d_i}\}_{i\in[1..g]}$. For $y \in B_k[\ell]$, let $\widetilde{y} \in p_{B_k}^{-1}(y)$. Up to a projective factor, we may suppose that $\texttt{chain\_mult}(\ell, \widetilde{y}) = \widetilde{0}_{B_k}$. Then y is in K if and only if for all $i \in Z(\overline{\ell})$ we have $\widetilde{\pi}_i(\hat{\pi}(\widetilde{y})) = \widetilde{R}_i$. Let $\widetilde{y+R_i}$ be any affine point above $y+R_i$. Since y and R_i are points of ℓ-torsion, for all $i \in Z(\overline{\ell})$, there exist $\alpha_i, \beta_i \in \overline{k}^*$ such that $\texttt{chain\_multadd}(\ell, \widetilde{y+R_i}, \widetilde{y}, \widetilde{R}_i)) = \alpha_i \widetilde{R}_i$ and $\texttt{chain\_multadd}(\ell, \widetilde{y+R_i}, \widetilde{R}_i, \widetilde{y}) = \beta_i \widetilde{y}$. By Theorem 4.8, we know that $\widetilde{\pi}_i(\hat{\pi}(\widetilde{y})) = \frac{\alpha_i}{\beta_i}\widetilde{R}_i$. In particular $y \in K$ if and only if $\frac{\alpha_i}{\beta_i} = 1$ for all $i \in Z(\overline{\ell n})$. In fact, we will show in Section 6 that $\alpha_i/\beta_i = e_{\mathscr{L}_0^\ell}(y, R_i)$ where $e_{\mathscr{L}_0^\ell}$ is the commutator pairing on $\mathscr{L}_0^\ell$. This is coherent with the fact that y is in K if and only if $e_{\mathscr{L}_0^\ell}(y, R_i) = 1$ for $i \in \{d_1, \cdots, d_g\}$.

The case $(n,\ell) > 1$ In this case we have to take $\mathfrak{S} = \{e_1, \cdots, e_g, e_1+e_2, \cdots\}$. If $i \in \mathfrak{S}$, $\widetilde{R}_i$ is a point of ℓn-torsion and we have by Remark 3.14

$$(1, \ell i, 0).\widetilde{y} = \lambda_i^\ell\, \texttt{chain\_multadd}(\ell, \pi_i^a(x), \widetilde{R}_i, \widetilde{y}),$$

so that we can still recover λ_i^ℓ.

The case $n = 2$ The only difficult part here is the ordinary additions $y + R_i$, since the addition chains do not pose any problems with $n = 2$. In particular, we first choose one of the two points $\pm(x \pm R_{e_1})$, which requires a square root. Now, since we have $\widetilde{0}_{A_k}$ given by a theta structure of degree $\ell n > 2$, we have the coordinates of $R_{e_1} + R_i$ on B_k. This means that we can compute the compatible additions $x + R_i$ from $x + R_{e_1}$ and $R_{e_1} + R_i$.

5 The computation of a modular point

We recall that $(A_k, \mathscr{L}, \Theta_{A_k})$ and $(B_k, \mathscr{L}_0, \Theta_{B_k})$ are marked abelian varieties and we let $\pi : A_k \rightarrow B_k$ be an isogeny of type 1. In Section 5.1, we explain how to compute the theta null point $\widetilde{0}_{A_k}$ from the knowledge of the kernel of $\hat{\pi}$ the contragredient isogeny of π. This section introduces the notion of an excellent point of ℓ-torsion, which is an affine lift of a point of ℓ-torsion that satisfy Equation (29). We study this notion in Section 5.2, and use it in Section 5.3 in order to compute all (or just one) modular points.

5.1 An analog of Vélu's formulas

We have seen in Section 4.2 how to use the addition formula to compute the isogeny $\hat{\pi} : B_k \rightarrow A_k$. The theta null point $(a_i)_{i\in Z(\overline{\ell n})}$ corresponding to $(A_k, \mathscr{L}, \Theta_{A_k})$ is an input of this computation. In this section, we explain how to recover the theta null point $(a_i)_{i\in Z(\overline{\ell n})}$, given the kernel $\hat{K} = \{T_i\}_{i\in Z(\overline{\ell})}$ of $\hat{\pi}$, by using only the addition relations. By combining this result with the algorithm of Section 4.2, we obtain an analog of Vélu's formulas for higher dimensional abelian varieties since we are able to compute an isogeny from the data of its kernel just by using addition relations. As in the course of the algorithm we have to take ℓ^{th}-root in k, we suppose that k is algebraically closed. (If $k = \mathbb{F}_q$, with $\ell | q - 1$ so that the ℓ^{th}-root of unity are in k, we only have to work over an extension of degree ℓ of k).

Let $\{T_{d_1}, \cdots, T_{d_g}\}$ be a basis of $\hat{K}$. Let $(a_i)_{i \in Z(\overline{\ell n})}$ be the theta null point corresponding to any theta structure on A_k π-compatible with the theta structure of $(B_k, \mathscr{L}_0, \Theta_{B_k})$. We recall that to $\widetilde{\mathtt{0}}_{A_k} = (a_i)_{i \in Z(\overline{\ell n})}$, one can associate the points $(\widetilde{R}_i)_{i \in Z(\overline{\ell})} = \widetilde{\pi}_i(\widetilde{\mathtt{0}}_{A_k})$ and Corollary 2.4 shows that this correspondence is one on one. By [FLR09, Prop. 7], we recover all the theta null points of the π-compatible theta structures on A_k, by acting over $\widetilde{\mathtt{0}}_{A_k} = (\widetilde{R}_i)_{i \in Z(\overline{\ell})}$ by

$$(\widetilde{R}_i)_{i \in Z(\overline{\ell})} \mapsto (\widetilde{R}_{\psi_1(i)})_{i \in Z(\overline{\ell})}, \tag{26}$$

$$(\widetilde{R}_i)_{i \in Z(\overline{\ell})} \mapsto (e(\psi_2(i), i)\widetilde{R}_i)_{i \in Z(\overline{\ell})}, \tag{27}$$

where ψ_1 is an automorphism of $Z(\overline{\ell})$ and ψ_2 is a symmetric endomorphism of $Z(\overline{\ell})$. We remark that the results of Section 4.1 show that $\widetilde{\mathtt{0}}_{A_k}$ is completely determined by $\{\widetilde{R}_{d_i}, \widetilde{R}_{d_i + d_j}\}_{i,j \in [1..g]}$ where $d_1, \cdots, d_g$ is a basis of $Z(\overline{\ell})$.

Up to an action (26) we may suppose that $\widetilde{\mathtt{0}}_{A_k}$ is such that $\widetilde{\pi}_{d_i}(\widetilde{\mathtt{0}}_{A_k}) = T_{d_i}$. Let $i \in Z(\overline{\ell})$ and let $\widetilde{T}_i$ be any affine point above T_i, we have $\widetilde{R}_i = \lambda_i \widetilde{T}_i$. Write $\ell = 2\ell' + 1$, since $R_i = p_{B_k}(\widetilde{R}_i)$ is a point of ℓ-torsion, we have $(1, \ell' + 1, \mathtt{0}).\widetilde{R}_i = -(1, \ell', \mathtt{0}).\widetilde{R}_i$. By Proposition 3.11 and Lemma 3.10, we have

$$\begin{aligned} \mathtt{chain\_mult}(\ell' + 1, \widetilde{R}_i) &= -\,\mathtt{chain\_mult}(\ell', \widetilde{R}_i), \\ \lambda_i^{(\ell'+1)^2}\,\mathtt{chain\_mult}(\ell' + 1, \widetilde{T}_i) &= -\lambda_i^{\ell'^2}\,\mathtt{chain\_mult}(\ell', \widetilde{T}_i), \\ \lambda_i^{\ell}\,\mathtt{chain\_mult}(\ell' + 1, \widetilde{T}_i) &= -\,\mathtt{chain\_mult}(\ell', \widetilde{T}_i). \end{aligned} \tag{28}$$

Hence we may find λ_i up to an ℓ^{th}-root of unity. If we apply this method for $i \in \{d_1, \cdots, d_g, d_1 + d_2, \cdots, d_{g-1} + d_g\}$, we find $\widetilde{R}_i$ up to an ℓ^{th}-root of unity. But the action (27) shows that every such choice of $\widetilde{R}_i$ gives a valid theta null point $\widetilde{\mathtt{0}}_{A_k}$ via the correspondence of Corollary 2.4.

Algorithm 5.1 (Vélu's like formula):

```
Input  $T_{d_1}, \cdots T_{d_g}$ a basis of the kernel $\hat{K}$ of $\hat{\pi}$.
Output  The compressed coordinates of $\widetilde{\mathtt{0}}_{A_k}$, the theta null point of level $\ell n$ corresponding to $\hat{\pi}$.
  Let $\mathfrak{S} = \{d_1, \cdots, d_g, d_1 + d_2, \cdots d_{g-1} + d_g\}$.
    ➔ Let $\ell'$ such that $\ell = 2\ell' + 1$.
    ➔ For $i, j \in [1..g]$, compute the points $T_{d_i} + T_{d_j}$.
    ➔ For each $i \in \mathfrak{S}$,
        • Choose any affine lift $T'_i$ of $T_i$, and compute $(\beta^i_j)_{j \in Z(\overline{n})} := \mathtt{chain\_mult}(\ell', T'_i)$, and $(\gamma^i_j)_{j \in Z(\overline{n})} := \mathtt{chain\_mult}(\ell' + 1, T'_i)$.
        • Compute $\alpha_i$ such that $(\gamma^i_j)_{j \in Z(\overline{n})} = \alpha_i (\beta^i_{-j})_{j \in Z(\overline{n})}$.
        • Output $\widetilde{R}_i := (\alpha_i)^{\frac{1}{\ell}} \cdot T'_i$.
```

Correction and Complexity Analysis 5.2:
In the Output we compute $\widetilde{R}_i$, one of the ℓ affine lift of T_i such that: $\texttt{chain\_mult}(\ell'+1, \widetilde{R}_i) = -\texttt{chain\_mult}(\ell', \widetilde{R}_i)$. Then $\{\widetilde{R}_i\}_{i \in \mathfrak{S}}$ give the compressed coordinates of $\widetilde{0}_{A_k}$, we can then recover $\widetilde{0}_{A_k}$ by doing a point decompression (see Algorithm 4.7).

To find $\widetilde{R}_i$, we need to do two chain multiplications of length $\ell/2$, and then take an ℓ^{th}-root of unity. After $g(g+1)/2$ such operations, we obtain the compressed coordinates of a $\widetilde{0}_{A_k}$, and we may recover the full coordinates of the corresponding $\widetilde{0}_{A_k}$ using the point decompression algorithm 4.7. We remark that we only need the compressed coordinates of $\widetilde{0}_{A_k}$ to compute the compressed coordinates of $\hat{\pi}$. In total we need to compute $g(g+1)/2$ ℓ^{th}-roots of unity and $O(\frac{1}{2}g(g+1)\log(\ell))$ additions in B_k to recover the compressed coordinates of $\widetilde{0}_{A_k}$. We can then recover the full coordinates of $\widetilde{0}_{A_k}$ at the cost of $O(\ell^g)$ additions in B_k.

The case $(n, \ell) > 1$. In this case once again we have to recover $\widetilde{R}_i$ for $i \in \mathfrak{S} = \{e_1, \cdots, e_g, e_1 + e_2, \cdots, e_1 + e_g\}$. Suppose that we have $\{T_i\}_{i \in Z(\overline{\ell})}$, ℓ^g points of ℓn-torsion such that $\ell.T_i = (1, \ell i, 0).0_B$. If $i \in \mathfrak{S}$, we may suppose that $\widetilde{R}_i = \lambda_i \widetilde{T}_i$.

If $\ell = 2\ell' + 1$ is odd, we have:

$$\lambda_i^\ell \,\texttt{chain\_mult}(\ell'+1, \widetilde{T}_i) = -(1, \ell(n-1), 0).\,\texttt{chain\_mult}(\ell', \widetilde{T}_i)$$

so that once again we can find λ_i^ℓ.

The kernel of $\hat{\pi}$ is then $\hat{K} = \{nT_i\}_{i \in Z(\overline{\ell})}$. Even if $\hat{K}$ is isotropic, it may be $\{T_i\}_{i \in Z(\overline{\ell})}$ are not isotropic, so some care must be taken when we choose the $\{T_i\}_{i \in Z(\overline{\ell})}$.

If $\ell = 2\ell'$ is even, we have:

$$\lambda_i^{2\ell} \,\texttt{chain\_mult}(\ell'+1, \widetilde{T}_i) = -(1, \ell(n-1), 0).\,\texttt{chain\_mult}(\ell'-1, \widetilde{T}_i),$$

so that we can recover only $\lambda_i^{2\ell}$. But every choice still corresponds to a valid theta null point $(a_i)_{i \in Z(\overline{\ell n})}$, because when $2|\ell$, to the actions (26) and (27) we have to add the action given by the change of the maximal symmetric level structure [FLR09, Prop. 7].

The case $n = 2$ Once again, the only difficulty rests in the standard additions. Using standard additions, we may compute $R_{e_1} \pm R_{e_2}, \cdots, R_{e_1} \pm R_{e_g}$, making a choice each time. Then we can compute $R_{e_i} + R_{e_j}$ by doing an addition compatible with $R_{e_1} + R_{e_i}$ and $R_{e_1} + R_{e_j}$.

5.2 Theta group and ℓ-torsion

Let $\widetilde{x} \in \widetilde{B}_k(\overline{k})$ be such that $p_{B_k}(x)$ is a point of ℓ-torsion. We say that x is an excellent point of ℓ-torsion if $\widetilde{x}$ satisfy:

$$\texttt{chain\_mult}(\ell'+1, \widetilde{x}) = -\texttt{chain\_mult}(\ell', \widetilde{x}). \tag{29}$$

Remark 5.3:
If $\widetilde{x}$ is an excellent point of ℓ-torsion, then Lemma 3.10 shows it is also the case for $\lambda.\widetilde{x}$ for any λ an ℓ^{th}-root of unity. ♢

We have seen in the preceding section the importance of taking lifts that are excellent points of ℓ-torsion. The aim of this section is to use the results of Section 3.3 to show that the addition chain of excellent points of ℓ-torsion is again an excellent-point of ℓ-torsion. This result will be used in Section 5.3 to compute excellent affine lifts of $B_k[\ell]$ by taking as few ℓ^{th}-roots as possible.

Let $\mathscr{M}_0 = [\ell]^* \mathscr{L}_0$ on B_k. As $\mathscr{L}_0$ is symmetric, we have that $\mathscr{M}_0 \simeq \mathscr{L}_0^{\ell^2}$ [Mum70, p. 59] and $K(\mathscr{M}_0)$, the kernel of $\mathscr{M}_0$ is isomorphic to $K(\overline{\ell^2 n})$. Let $\Theta_{B_k,\mathscr{M}_0}$ be a theta structure on $(B_k, \mathscr{M}_0)$ $[\ell]$-compatible with the theta structure Θ_{B_k} on $(B_k, \mathscr{L}_0)$. As in Section 2.3, we can define the affine cone $\widetilde{B_k}'$ associated to the canonical sections of $\mathscr{M}_0$ defined by the theta structure $\Theta_{B_k,\mathscr{M}_0}$. We choose a system of affine coordinates on $\widetilde{B_k}'$ above the projective coordinates given by $\Theta_{B_k,\mathscr{M}_0}$, and we let $\widetilde{[\ell]} : \widetilde{B_k}' \to \widetilde{B}_k$ be the lift to the affine cone of $[\ell]$ compatible with these coordinates. Finally, we note $\widetilde{0}_{\widetilde{B_k}'} \in \widetilde{B_k}'$ the affine lift of the theta null point associated to $\Theta_{B_k,\mathscr{M}_0}$ such that $\widetilde{[\ell]}\widetilde{0}_{\widetilde{B_k}'} = \widetilde{0}_{B_k}$. Since $\mathscr{M}_0 \simeq \mathscr{L}_0^{\ell^2}$, the natural action of $G(\mathscr{M}_0)$ on $H^0(\mathscr{M}_0)$ gives via $\Theta_{B_k,\mathscr{M}_0}$ an action of $\mathscr{H}(\overline{\ell^2 n})$ on $H^0(\mathscr{M}_0)$.

Lemma 5.4:
Let $y \in B_k[\ell](\overline{k})$, $\widetilde{y} \in p_{B_k}^{-1}(y)$ and $\widetilde{x} \in \widetilde{[\ell]}^{-1}(\widetilde{y})$. Then there exists $(\alpha, ni, nj) \in k^\ell \times Z(\overline{\ell^2 n}) \times \hat{Z}(\overline{\ell^2 n})$ such that $\widetilde{x} = (\alpha, ni, nj).\widetilde{0}_{\widetilde{B_k}'}$. Moreover, $\widetilde{y}$ is an excellent point of ℓ-torsion if and only if $\alpha = \lambda_{i,j} \mu$ where μ is an ℓ^{th}-root of unity and $\lambda_{i,j} = \langle i, j \rangle^{\ell' n(\ell-1)}$.

(If $x' \in \widetilde{B_k}'(\overline{k})$, then $x' \in \widetilde{[\ell]}^{-1}(y)$ if and only if $x' = (1, \ell i', \ell j').x$ where $(i', j') \in Z(\overline{\ell^2 n}) \times \hat{Z}(\overline{\ell^2 n})$), so the class of α in $k^*/k^{*\ell}$ does not depend on $\widetilde{x}$ but only on $\widetilde{y}$).

Proof: Since $p_{\widetilde{B_k}'}(\widetilde{x}) \in B_k[\ell^2]$, there is an element $h \in \mathscr{H}(\overline{\ell^2 n})$ such that $\widetilde{x} = h.0_{\widetilde{B_k}'}$, with $h = (\alpha, ni, nj)$. By Remark 5.3, we only need to check that $(\lambda_{i,j}, ni, nj).0_{\widetilde{B_k}'}$ is an excellent point of ℓ-torsion. Let $m \in \mathbb{Z}$, and let $\widetilde{x}_m = \texttt{chain\_mult}(m, \widetilde{x})$, $\widetilde{y}_m = \texttt{chain\_mult}(m, \widetilde{y})$. By Corollary 24 we have $\widetilde{x}_m = (\lambda_{i,j}^{m^2}, m \cdot i, m \cdot j).0_{\widetilde{B_k}'}$, and by Corollary 3.17 $\widetilde{y}_m = \widetilde{[\ell]}(\lambda_{i,j}^{m^2}, m \cdot i, m \cdot j).0_{\widetilde{B_k}'}$. So by Lemma 3.9

$$\begin{aligned}\widetilde{y}_{\ell'} &= \widetilde{[\ell]}(\lambda_{i,j}^{\ell'^2}, \ell' \cdot i, \ell' \cdot j).0_{\widetilde{B_k}'} = \widetilde{[\ell]}(1, \ell n(\ell-1)i, \ell n(\ell-1)j)(\lambda_{i,j}^{\ell'^2}, \ell' i, \ell' j +).0_{\widetilde{B_k}'} \\ &= \langle \ell' i, \ell n(\ell-1)j \rangle \widetilde{[\ell]}(\lambda_{i,j}^{\ell'^2}, (\ell' + \ell n(\ell-1)) \cdot i, (\ell' + \ell n(\ell-1)) \cdot j).0_{\widetilde{B_k}'} \\ &= \lambda_{i,j}^{\ell} \widetilde{[\ell]}(\lambda_{i,j}^{(\ell'+1)^2} / \lambda_{i,j}^{\ell}, -(\ell'+1) \cdot i, -(\ell'+1) \cdot j).0_{\widetilde{B_k}'} \\ &= \widetilde{[\ell]}(-\widetilde{x}_{\ell'+1}) = -\widetilde{y}_{\ell'+1}.\end{aligned}$$

■

Proposition 5.5:
Let $\widetilde{y}_1, \widetilde{y}_2, \widetilde{y_1 - y_2} \in \widetilde{B}_k(\overline{k})$ be excellent points of ℓ-torsion. Then $\widetilde{y_1 + y_2} := \texttt{chain\_add}(\widetilde{y}_1, \widetilde{y}_2, \widetilde{y_1 - y_2})$ is an excellent point of ℓ-torsion.

Proof: Let $(\alpha_1, i_1, j_1) \in \mathscr{H}(\overline{\ell^2 n}), (\alpha_2, i_2, j_2) \in \mathscr{H}(\overline{\ell^2 n}), (\alpha_3, i_3, j_3) \in \mathscr{H}(\overline{\ell^2 n})$, be such that

$$\widetilde{[\ell]}(\alpha_1, i_1, j_1).0_{\widetilde{B_k}'} = \widetilde{y_1}, \quad \widetilde{[\ell]}(\alpha_2, i_2, j_2).0_{\widetilde{B_k}'} = \widetilde{y_2}, \quad \widetilde{[\ell]}(\alpha_3, i_3, j_3).0_{\widetilde{B_k}'} = \widetilde{y_1 - y_2}$$

By the Remark at the end of Lemma 5.4, we may suppose that $i_3 = i_1 - i_2$, $j_3 = j_1 - j_2$. Since $\widetilde{y_1}, \widetilde{y_2}$ and $\widetilde{y_1 - y_2}$ are excellent points of ℓ-torsion, by Remark 5.3 and Lemma 5.4 we may suppose that $\alpha_1 = \lambda_{i_1, j_1}$, $\alpha_2 = \lambda_{i_2, j_2}$ and $\alpha_3 = \lambda_{i_1 - i_2, j_1 - j_2}$.

By Corollary 24 and Lemma 3.10, we have

$$\widetilde{y_1 + y_2} = \frac{\lambda^2_{i_1, j_1} \lambda^2_{i_2, j_2}}{\lambda_{i_1 - i_2, j_1 - j_2}} (1, i_1 + i_2, j_1 + j_2).0_{\widetilde{B_k}'} = (\lambda_{i_1 + i_2, j_1 + j_2}, i_1 + i_2, j_1 + j_2).0_{\widetilde{B_k}'},$$

so $\widetilde{y_1 + y_2}$ is indeed an excellent point of ℓ-torsion by Lemma 5.4. ■

5.3 Improving the computation of a modular point

In [FLR09], to compute the modular points $\widetilde{0}_{A_k}$, the following algorithm is used: let $\widetilde{0}_{B_k} = (b_i)_{i \in Z(\overline{n})}$, consider the algebraic system S defined by the Riemann and symmetry relations (3) with $(a_i)_{i \in Z(\overline{\ell n})}$ considered as unknown and where we put $a_i = b_i$ for $i \in Z(\overline{n})$. The algebraic system S define a 0-dimensional algebraic variety which contains the set of modular points $\widetilde{0}_{A_k}$. We then present algorithm to compute efficiently a Gröbner basis of the system S.

In this section, in order to improve the algorithm of [FLR09], we explain how, using the "Vélu's"-like formulas of Section 5.1, it is possible to recover all the modular points $\widetilde{0}_{A_k}$ solution of the system S from the knowledge of the ℓ-torsion of B_k. We then discuss different methods to compute the ℓ-torsion in B_k.

Algorithm 5.6 (Computing all modular points):
Input $T_1, \cdots, T_{2g}$ a basis of the ℓ-torsion of B_k.
Output All ℓ-isogenies.

We only give an outline of the algorithm, since we give a detailed description in Example 5.7. We suppose that we know how to compute $e_{\mathscr{L}_0^\ell}$ on $B_k[\ell]$. We will explain how to do this in the next section.

- Compute any affine excellent ℓ-torsion lifts $\widetilde{T_1}, \cdots, \widetilde{T_{2g}}, \widetilde{T_1 + T_2}, \cdots, \widetilde{T_{g-1} + T_g}$, and then use addition chains to compute affine lifts $\widetilde{T}$ for every point $T \in B_k[\ell]$. By Proposition 5.5 $\widetilde{T}$ is an excellent point of ℓ-torsion.
- For every isotropic subgroup $K \subset B_k[\ell]$, take the corresponding lifts and use them to reconstitute the corresponding theta null point $\widetilde{0}_{A_k}$ (see Section 5.1).

Example 5.7:
Suppose that $\{T_1, \ldots, T_{2g}\}$ is a symplectic basis of $B_k[\ell]$. (A symplectic basis is easy to obtain from a basis of the ℓ-torsion, we just need to compute the discrete logarithms of some of the pairings between the points, where the pairings can be computed with Algorithm 6.5).

Let $\Theta_{B_k,\mathscr{M}_0}$ be any theta structure of level $\ell^2 n$ on B_k compatible with Θ_{B_k}, and $\widetilde{0}'_{B_k}$ be the corresponding theta null point (see Section 5.2). We may suppose (see Section 5.1) that

$$\begin{aligned}
\widetilde{T}_1 &= \widetilde{[\ell]}(1,(n,0,\cdots,0),0).\widetilde{0}'_{B_k}\\
\widetilde{T}_2 &= \widetilde{[\ell]}(1,(0,n,\cdots,0),0).\widetilde{0}'_{B_k},\dots\\
\widetilde{T_{g+1}} &= \widetilde{[\ell]}(1,0,(n,0,\cdots,0)).\widetilde{0}'_{B_k}\\
\widetilde{T_{g+2}} &= \widetilde{[\ell]}(1,0,(0,n,\cdots,0)).\widetilde{0}'_{B_k},\dots\\
\widetilde{T_1+T_{g+2}} &= \widetilde{[\ell]}(1,(n,0,\cdots,0),(0,n,0,\cdots,0)).\widetilde{0}'_{B_k},\dots
\end{aligned}$$

Then by Corollary 24, using Algorithm 5.6, we compute the following affine lifts of the ℓ-torsion:

$$\{\widetilde{[\ell]}(1,in,jn).\widetilde{0}'_{B_k} : i,j \in \{0,1,\cdots,\ell-1\}^g \subset Z(\ell^2 n)\}. \tag{30}$$

Now if $K \subset B_k[\ell]$ is an isotropic group, in the reconstruction algorithm 5.1 we need to compute points of the form $\widetilde{[\ell]}(1,in,jn).\widetilde{0}'_{B_k}$ for $i,j \in Z(\ell^2 n)$. But we have

$$\begin{aligned}
\widetilde{[\ell]}(1,in,jn).\widetilde{0}'_{B_k} &= \widetilde{[\ell]}\zeta^{\ell\beta n\cdot(i-\ell\alpha)n}(1,\ell\alpha n,\ell\beta n).(1,(i-\ell\alpha)n,(j-\ell\beta)n).\widetilde{0}'_{B_k}\\
&= \widetilde{[\ell]}\zeta^{\ell\beta n\cdot(i-\ell\alpha)n}(1,(i-\ell\alpha)n,(j-\ell\beta)n).\widetilde{0}'_{B_k},
\end{aligned}$$

where $\alpha,\beta \in Z(\ell^2 n)$, and ζ is a $(\ell^2 n)^{th}$-root of unity. As a consequence, we can always go back to a point computed in (30) up to an ℓ^{th}-root of unity.

We give a detailed example with $g=1$, $\ell=3$, $n=4$. Let B_k be an elliptic curve, with a theta structure Θ_{B_k} of level n. Let T_1, T_2 be a basis of $B_k[\ell]$, and choose excellent affine lifts $\widetilde{T}_1, \widetilde{T}_2, \widetilde{T_1+T_2}$. Let $\Theta_{B_k,\mathscr{M}_0}$ be any theta structure of level $\ell^2 n$ compatible with Θ_{B_k}, and $\widetilde{0}'_{B_k}$ be the corresponding theta null point (see Section 5.2). We take $\Theta_{B_k,\mathscr{M}_0}$ such that $\widetilde{T}_1 = \widetilde{[\ell]}(1,n,0).\widetilde{0}'_{B_k}$, $\widetilde{T}_2 = \widetilde{[\ell]}(1,0,n).\widetilde{0}'_{B_k}$, and $\widetilde{T_1+T_2} = \widetilde{[\ell]}(1,n,n).\widetilde{0}'_{B_k}$.

We have seen in (30) that in the Algorithm 5.6 we compute the points: $\widetilde{[\ell]}(1,in,jn).\widetilde{0}'_{B_k}$ for $i,j \in 0,1,\cdots,\ell-1 \subset \mathbb{Z}/\ell^2 n\mathbb{Z}$.

Now let $T = \widetilde{[\ell]}(1,n,2n).\widetilde{0}'_{B_k}$, $K =< p_{B_k}(T) >$ is an isotropic subgroup of $B_k[\ell]$. Let $A_k = B_k/K$, choose a compatible theta structure Θ_{A_k} on A, and let $\widetilde{0}_{A_k}$ be the associated theta null point.

As usual, we define $\widetilde{R}_i = \widetilde{\pi}_i(\widetilde{0}_{A_k})$ if $i \in \mathbb{Z}/\ell Z \subset \mathbb{Z}/\ell n\mathbb{Z}$, and we may suppose (Section 5.1) that Θ_{A_k} is such that $R_1 = T$. More explicitly, if $n=4$ we have (Remember that we always choose $\widetilde{0}_{A_k}$

such that $\widetilde{\pi}(\widetilde{\mathtt{0}}_{A_k}) = \widetilde{\mathtt{0}}_{B_k}$):

$$\begin{gathered}
\widetilde{\mathtt{0}}_{A_k} = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}) \\
\widetilde{\pi}(x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}) = (x_0, x_3, x_6, x_9) \\
\widetilde{R}_0 = (a_0, a_3, a_6, a_9) = \widetilde{\mathtt{0}}_{B_k} \\
\widetilde{R}_1 = (a_4, a_7, a_{10}, a_1) \\
\widetilde{R}_2 = (a_8, a_{11}, a_2, a_5)
\end{gathered}$$

Now by Theorem 4.4 we know that $\widetilde{\mathtt{0}}_{A_k}$ is entirely determined by $\widetilde{R}_1$ (and $\widetilde{\mathtt{0}}_{B_k}$), in fact we have: $\widetilde{R}_2 = \texttt{chain\_add}(R_1, R_1, \widetilde{\mathtt{0}}_{B_k})$. By Corollary 24, we have

$$\widetilde{R}_2 = \widetilde{[\ell]}(1, 2n, 4n).\widetilde{\mathtt{0}}'_{B_k} = \widetilde{[\ell]}\zeta^{2n \cdot 3n}(1, 0, 3n).(1, 2n, n).\widetilde{\mathtt{0}}'_{B_k} = \zeta^{2n \cdot 3n}\widetilde{[\ell]}(1, 2n, n).\widetilde{\mathtt{0}}'_{B_k},$$

where ζ is a $(\ell^2 n)^{th}$-root of unity.

This shows that in the reconstruction step, we have to multiply the point $\widetilde{[\ell]}(1, 2n, n).\widetilde{\mathtt{0}}'_{B_k}$ which we have already computed by the ℓ-root of unity $\zeta^{2n \cdot \ell n}$.

Complexity Analysis 5.8:
To compute an affine lift $\widetilde{T}_i$, we have to compute an ℓ^{th}-root of unity (and do some addition chains but we can reuse the results for the next step). Once we have computed the $\ell(2\ell+1)^{th}$-root, we compute the whole (affine lifts of) ℓ-torsion by using $O(\ell^{2g})$ addition chains. We can now compute the pairings $e(T_i, T_j)$ with just one division since we have already computed the necessary addition chain (see Section 6). From these pairings we can compute a symplectic basis of $B_k[\ell]$. This requires to compute the discrete logarithm of the pairings and can be done in $O(\ell)$ time. Using this basis, we can enumerate every isotropic subgroup $K \subset B_k[\ell]$, and reconstruct the corresponding theta null point with $O(\ell^g)$ multiplications by an ℓ^{th}-root of unity.

The case $(n, \ell > 1)$ In this case, the only difference is that we have to compute $B_k[\ell n]$ rather than $B_k[\ell]$, and when T_i is a point of ℓn-torsion, we compute an affine lift $\widetilde{T}_i$ such that:

$$\texttt{chain\_mult}(\ell' + 1, \widetilde{T}_i) = -(1, \ell(n-1), 0).\,\texttt{chain\_mult}(\ell', \widetilde{T}_i).$$

The case $n = 2$: This works as in Section 5.1, once we have computed the $\widetilde{T_{e_1} + T_{e_i}}$, we have to take compatible additions to compute the $\widetilde{T_{e_i} + T_{e_j}}$.

Computing the points of ℓ-torsion in B_k: By applying the addition relations of Section 3.2 on the generic point of B_k, we obtain an algebraic system of equations of degree ℓ^{2g} in n^g unknown defining $B_k[\ell]$. We can compute the solutions of this system by using the general purpose Gröbner basis computation algorithm.

In general we prefer to work with Kummer surfaces (so with $n = 2$), since it cuts the degree of the system by two. In genus 2, Gaudry and Schost [GS08] have an algorithm to compute the ℓ-torsion on the Kummer surface using resultants rather than a general purpose Gröbner basis algorithm. The points are given in Mumford coordinates, but we can use the results of Wamelen [Wam99] to have them in theta coordinates. This algorithm is in $\widetilde{O}(\ell^6)$ (where we use the notation $\widetilde{O}$ to mean we forget about the log factors). The computation of the excellent affine points of ℓ-torsion from Algorithm 5.6 is in $\widetilde{O}(\ell^4)$, and each of the $O(\ell^3)$ isogeny requires $O(\ell^2)$ multiplication by an ℓ^{th}-root of unity. In total we see that we can compute all (ℓ,ℓ)-isogenies in $\widetilde{O}(\ell^6)$ in genus 2.

Isogenies graph: A possible application of the algorithms presented in this paper is the computation of isogenies graphs. In fact, the Vélu like algorithm of Section 5.1 allows to compute a theta null point $\widetilde{0}_{A_k}$ for a theta structure on A_k of level ℓn from a point corresponding to a theta structure of level n. We can then use the modular correspondence described in Section 2.2, taking an isogeny, to obtain a theta null point $\widetilde{0}_{C_k}$ corresponding to an abelian variety C_k with a marking of level n. With this method, it is possible to compute ℓ^2-isogenies graphs.

In this manner, when we compute a sequence of ℓ^2-isogenies it is possible to benefit from the computation of the intermediate step $\widetilde{0}_{A_k}$: since $\widetilde{0}_{A_k}$ is a theta null point of level ℓn, we can recover from it all points in $A_k[\ell]$. Denote by $\pi_2 : A_k \rightarrow C_k$ the isogeny defined by the modular correspondence. Then $K_2 := \pi_2(A_k[\ell])$ gives half the ℓ-torsion of C_k (to get an explicit description of K_2, just apply $\mathfrak{I}$ to the results of Section 2.3). Since K_2 is the kernel of the contragredient isogeny of π_2, we have a way to compute isogeny graph of ℓ^2-isogenies where the composition of two such isogenies give an ℓ^4-isogeny and not, for instance if $g = 2$, a $(1,\ell^2,\ell^2,\ell^4)$-isogeny (it is enough to consider the isotropic subgroups of $C_k[\ell]$ that intersect K_2 trivially).

The knowledge of K_2 can also be used to speed up the computation of $C_k[\ell]$. In the following section, we describe an algorithm to compute the Weil pairing e_W on $C_k[\ell]$. Let $(G_1,\cdots,G_g)$ be a basis of K_2, and consider the system of degree ℓ^{g+1} given by the ideal of ℓ-torsion and the relations $e(G_i,\cdot) = 1$ (which have a rational expression) for $i \in [2..g]$. Let H_1 be a point solution of this algebraic system different from $< G_1 >$ (which can be tested be verifying that $e_W(G_1,H_1) \neq 1$). We can now construct the system of degree ℓ^g given by the ideal of ℓ-torsion and the relations $e_W(G_i,\cdot) = 1$ for $i \neq 2$ and $e_W(H_1,\cdot) = 1$; and look for a solution H_2 such that $e(G_2,H_2) \neq 1$. Continuing this process, we obtain an algorithm to construct a basis $G_1,\cdots,G_g,H_1,\cdots,H_g of C_k[\ell]$ by solving a system of degree ℓ^{g+1}, then of degree ℓ^g, ..., then of degree ℓ^2. This is faster than solving the ideal of ℓ-torsion which is a system of degree ℓ^{2g}.

6 Pairing computations

In this section, we explain how to use the addition chains introduced in Section 3.2 in order to compute the commutator pairings on abelian varieties. We recall the definition of the commutator pairing and its link with the Weil pairing in Section 6.1.

6.1 Weil pairing and commutator pairing

Since $B_k[\ell] \subset K(\mathscr{L}_0)^\ell$ the commutator pairing $e_{\mathscr{L}_0^\ell}$ gives a non degenerate pairing on $B_k[\ell]$ (if n is prime to ℓ), we call $e_{\mathscr{L}_0^\ell}$ the extended commutator pairing on $B_k[\ell]$. We can give another interpretation of this pairing, more suitable for computation: let $\mathscr{M}_0 = [\ell]^*\mathscr{L}_0$ on B_k. We know that

$K(\mathscr{M}_0)$ is isomorphic to $K(\overline{\ell^2 n})$ (see Section 5.2). As $\mathscr{M}_0$ descends to $\mathscr{L}_0$ via the isogeny $[\ell]$, the commutator pairing $e_{\mathscr{M}_0}$ induced by the polarization $\mathscr{M}_0$ is trivial on $B_k[\ell]$. For $x_1, x_2 \in B_k[\ell]$, let $x'_1, x'_2 \in B_k[\ell^2]$ be such that $\ell . x'_i = x_i$ for $i = 1, 2$. The extended commutator pairing is then $e_{\mathscr{L}_0^\ell}(x_1, x_2) = e_{\mathscr{M}_0}(x'_1, x_2) = e_{\mathscr{M}_0}(x_1, x'_2) = e_{\mathscr{M}_0}(x'_1, x'_2)^\ell$. Indeed by [Mum70, p. 228] we have $e_{\mathscr{M}_0}(x'_1, x_2) = e_{\mathscr{L}_0^\ell}(\ell x'_1, x_2) = e_{\mathscr{L}_0^\ell}(x_1, x_2)$.

The isogeny $\varphi_{\mathscr{L}_0} : B_k \to \hat{B}_k$ has kernel $B_k[n]$ and by composing $\varphi_{\mathscr{L}_0}$ on the right side of $e_{\mathscr{L}_0^\ell}$, we obtain a perfect pairing $e'_W : B_k[\ell] \times \hat{B}_k[\ell] \to \mu_\ell$ where μ_ℓ is the subgroup of ℓ^{th}-roots of unity of $\overline{k}$.

The following proposition is well known

Proposition 6.1:
The pairing e'_W is the Weil pairing e_W.

Proof: A proof can be found in [Mum70, p. 228]. We give here a quick proof using the definition of $e_{\mathscr{L}_0^\ell}$ given in term of the polarization $\mathscr{M}_0$ since it will be instructive for our algorithm in Section 6.2.

For $y \in \hat{B}_k[\ell]$, we denote by Λ_y the degree-0 line bundle on B_k associated to y. A possible definition of the Weil pairing e_W is as follows: Let $(x, y) \in B_k[\ell] \times \hat{B}_k[\ell]$. Let $\mathscr{O}_{B_k}$ be the structural sheaf of B_k, and as $y \in \hat{B}_k[\ell]$ there is an isomorphism $\psi'_y : [\ell]^* \Lambda_y \simeq \mathscr{O}_{B_k}$. As a consequence, Λ_y is obtained as the quotient of the trivial bundle $B_k \times \mathbb{A}^1_k$ over B_k by an action g of $B_k[\ell]$ on $B_k \times \mathbb{A}^1_k$ given by $g_x(t, \alpha) = (t + x, \chi(x).\alpha)$ where $(t, \alpha) \in (B_k \times \mathbb{A}^1_k)(\overline{k})$, $x \in B_k[\ell]$ and χ is a character of $B_k[\ell]$. By definition [Mum70], we have $e_W(x, y) = \chi(x)$.

We can reformulate this definition as follow: we choose an isomorphism $\mathscr{O}_{B_k}(0) \simeq k$ from which we deduce via ψ'_y (resp. $\tau_x^* \psi'_y$) an isomorphism $\psi_0 : [\ell]^* \Lambda_y(0) \simeq k$ (resp. $\psi_1 : \tau_x^* [\ell]^* \Lambda_y(0) \simeq k$). There exists a unique isomorphism $\psi_x : [\ell]^* \Lambda_y \to \tau_x^* [\ell]^* \Lambda_y$ compatible on the 0 fiber with ψ_0 and ψ_1, i.e. we have that $\psi_1 \circ \psi_x \circ \psi_0^{-1}$ is the identity of k. Then, the following diagram commutes up to a multiplication by $e_W(x, y)$:

$$\begin{tikzcd}
{[\ell]^* \Lambda_y} \arrow[r, "\psi'_y"] \arrow[d, "\psi_x"] & \mathscr{O}_{B_k} \arrow[d, equal, "e_W(x,y)"] \\
\tau_x^* [\ell]^* \Lambda_y \arrow[r, "\tau_x^* \psi'_y"] & \tau_x^* \mathscr{O}_{B_k}
\end{tikzcd}$$

The polarization $\mathscr{L}_0$ gives the natural isogeny $\varphi_{\mathscr{L}_0}$, defined on geometric points by

$$\begin{aligned} \varphi_{\mathscr{L}_0}(\overline{k}) : B_k(\overline{k}) &\to \hat{B}_k(\overline{k}) \\ y &\mapsto \Lambda_y = \mathscr{L}_0 \otimes (\tau_y^* \mathscr{L}_0)^{-1}. \end{aligned}$$

As a consequence, for $y \in \hat{B}_k[\ell]$ there exists $y_0 \in B_k(\overline{k})$ such that $\Lambda_y = \mathscr{L}_0 \otimes (\tau_{y_0}^* \mathscr{L}_0)^{-1}$. Let $y' \in B_k[\ell^2]$ be such that $\ell . y' = y_0$. As $[\ell]^* \mathscr{L}_0 = \mathscr{M}_0$, we have $[\ell]^* \Lambda_y = [\ell]^* (\mathscr{L}_0 \otimes (\tau_{y_0}^* \mathscr{L}_0)^{-1}) =$

$\mathscr{M}_0 \otimes (\tau^*_{y'}\mathscr{M}_0)^{-1}$. We remark that the isomorphism $\psi'_y : [\ell]^*\Lambda_y = \mathscr{M}_0 \otimes (\tau^*_{y'}\mathscr{M}_0)^{-1} \to \mathscr{O}_{B_k}$ gives by tensoring on the right by $\tau^*_{y'}\mathscr{M}_0$ an isomorphism $\psi_{y'} : \mathscr{M}_0 \to \tau^*_{y'}\mathscr{M}_0$. Thus, the following diagram is commutative up to a multiplication by $e_W(x,y)$:

$$\begin{tikzcd}
\mathscr{M}_0 \arrow[r, "\psi_{y'}"] \arrow[d, "\psi_x"] & \tau^*_{y'}\mathscr{M}_0 \arrow[d, "\tau^*_{y'}\psi_x"] \\
\tau^*_x\mathscr{M}_0 \arrow[r, "\tau^*_x\psi_{y'}"] & \tau^*_{x+y'}\mathscr{M}_0
\end{tikzcd}$$

$\blacksquare$

But this is exactly the definition of $e'_W(x,y)$ thus we have $e'_W(x,y) = e_W(x,y)$.

6.2 Commutator pairing and addition chains

In this paragraph, we explain how to compute the Weil pairing using addition chains. All known algorithms to compute efficiently the Weil pairing on an abelian variety B_k are based on a Miller loop [Mil04] which can be used only in the case that B_k is a jacobian. We choose a theta structure $\Theta_{B_k,\mathscr{M}_0}$ for $\mathscr{M}_0$ compatible with Θ_{B_k} and we let $\widetilde{0}_{\widetilde{B_k}'}$ be an affine lift of the theta null point corresponding to Θ_{B_k} as in Section 5.2. Let $x, y \in B_k[\ell]$, and $x', y' \in B_k[\ell^2]$ be such that $\ell.x' = y$ and $\ell.y' = y$. There exist $(\alpha_1, \alpha_2), (\beta_1, \beta_2) \in Z(\overline{\ell^2 n}) \times \hat{Z}(\overline{\ell^2 n})$ such that $(1, \alpha_1, \alpha_2).\widetilde{0}_{\widetilde{B_k}'}$ is an affine lift of x' and $(1, \beta_1, \beta_2).\widetilde{0}_{\widetilde{B_k}'}$ is an affine lift of y'. We note $x'_i = \overline{\Theta}_{B_k,\mathscr{M}_0}(\alpha_i)$ and $y'_i = \overline{\Theta}_{B_k,\mathscr{M}_0}(\beta_i)$ for $i = 1,2$, we have $x' = x'_1 + x'_2$ and $y' = y'_1 + y'_2$ is the decomposition of x' and y' in the decomposition $K(\mathscr{M}_0) = K_1(\mathscr{M}_0) \times K_2(\mathscr{M}_0)$ into isotropic subspaces induced by the theta structure $\Theta_{B_k,\mathscr{M}_0}$.

Lemma 6.2:
Let $i \in Z(\ell^2 n)$ and put

$$s(1) = \frac{((1,\alpha_1,0).(1,\beta_1,0).\widetilde{\vartheta}_i)(\widetilde{0}_{\widetilde{B_k}'})}{((1,\alpha_1,0).\widetilde{\vartheta}_i)(\widetilde{0}_{\widetilde{B_k}'})} . \frac{\widetilde{\vartheta}_i(\widetilde{0}_{\widetilde{B_k}'})}{((1,\beta_1,0).\widetilde{\vartheta}_i)(\widetilde{0}_{\widetilde{B_k}'})}.$$

For all $k \in \mathbb{N}$, we have

$$s(k) = \frac{((1,k.\alpha_1,0).(1,\beta_1,0).\widetilde{\vartheta}_i)(\widetilde{0}_{\widetilde{B_k}'})}{((1,k.\alpha_1,0).\widetilde{\vartheta}_i)(\widetilde{0}_{\widetilde{B_k}'})} . \frac{\widetilde{\vartheta}_i(\widetilde{0}_{\widetilde{B_k}'})}{((1,\beta_1,0).\widetilde{\vartheta}_i)(\widetilde{0}_{\widetilde{B_k}'})} = s(1)^k. \tag{31}$$

Proof: Consider the degree-0 line bundle $\Lambda = \tau^*_{y'_1}\mathscr{M}_0 \otimes \mathscr{M}_0^{-1}$. We remark that as $y'_1 \in K(\mathscr{M}_0)$, Λ is isomorphic to the trivial line bundle on B_k. Let K be the subgroup of $K_1(\mathscr{M}_0)$ generated by x'_1 and let C_k be the quotient of B_k by K. The line bundle Λ descends to a line bundle Λ' over C_k. As Λ' has degree 0, it is the quotient of $B_k \times \mathbb{A}^1_k$ by an action of the form $g'_x(t,\alpha) = (t+x, \chi_0(x).\alpha)$, where $(t,\alpha) \in B_k \times \mathbb{A}^1_x$, $x \in K$, and χ_0 is a character of K.

As $\widetilde{\vartheta} \in H^0(\mathscr{M}_0)$, we remark that $f = ((1,\beta_1,0).\widetilde{\vartheta})/(\widetilde{\vartheta})$ is a section of Λ'. Thus, we have $s(k) = f(k.x'_1)/f(0_{B_k}) = \chi_0(k)$ and $s(k) = s(1)^k$. ■

Remark 6.3:
We remark that in the preceding lemma, α_1 and β_1 play the same role and as a consequence can be permuted. ♢

We keep the notation of the beginning of this paragraph to state the

Proposition 6.4:
We put:

$$L = \frac{((1,\ell.\alpha_1+\beta_1,\ell.\alpha_2+\beta_2)\widetilde{\vartheta})(\widetilde{0}_{B_k})}{((1,\beta_1,\beta_2)\widetilde{\vartheta})(\widetilde{0}_{B_k})} . \frac{\widetilde{\vartheta}(\widetilde{0}_{B_k})}{((1,\ell.\alpha_1,\ell.\alpha_2)\widetilde{\vartheta})(\widetilde{0}_{B_k})}.$$

$$R = \frac{((1,\alpha_1+\ell.\beta_1,\alpha_2+\ell.\beta_2)\widetilde{\vartheta})(\widetilde{0}_{B_k})}{((1,\alpha_1,\alpha_2)\widetilde{\vartheta})(\widetilde{0}_{B_k})} . \frac{\widetilde{\vartheta}(\widetilde{0}_{B_k})}{((1,\ell.\beta_1,\ell.\beta_2)\widetilde{\vartheta})(\widetilde{0}_{B_k})}.$$

We have :

$$e_{\mathscr{L}_0^\ell}(x,y) = L^{-1}.R. \tag{32}$$

Proof: First, we compute L. We have:

$$\begin{aligned}(1,\ell.\alpha_1+\beta_1,\ell.\alpha_2+\beta_2)\widetilde{\vartheta} &= \langle \ell.\alpha_1+\beta_1, -\ell.\alpha_2-\beta_2\rangle(1,\ell.\alpha+\beta_1,0)(1,0,\ell.\alpha_2+\beta_2)\widetilde{\vartheta} \\ &= \langle \ell.\alpha_1+\beta_1-i, -\ell.\alpha_2-\beta_2\rangle(1,\ell.\alpha_1+\beta_1,0)\widetilde{\vartheta}.\end{aligned}$$

In the same way, we have:

$$(1,\beta_1,\beta_2)\widetilde{\vartheta} = \langle \beta_1, -\beta_2 - i\rangle(1,\beta_1,0)\widetilde{\vartheta},$$
$$(1,\ell.\alpha_1,\ell.\alpha_2)\widetilde{\vartheta} = \langle \ell.\alpha_1, -\ell.\alpha_2 - i\rangle(1,\ell.\alpha_1,0)\widetilde{\vartheta}.$$

Taking the product, we obtain that

$$L = \langle \ell.\alpha_1, -\beta_2\rangle.L',$$

with

$$L' = \frac{((1,\beta_1,0).(1,\ell.\alpha_1,0)\widetilde{\vartheta})(\widetilde{0}_{B_k})}{(1,\beta_1,0)\widetilde{\vartheta}(\widetilde{0}_{B_k})} \frac{\widetilde{\vartheta}(\widetilde{0}_{B_k})}{(1,\ell.\alpha_1,0)\widetilde{\vartheta}(\widetilde{0}_{B_k})}.$$

In the same manner, we have:

$$R = \langle \ell.\beta_1, -\alpha_2\rangle.R',$$

with

$$R' = \frac{((1,\alpha_1,0).(1,\ell.\beta_1,0)\widetilde{\vartheta})(\widetilde{0}_{B_k})}{(1,\alpha_1,0)\widetilde{\vartheta}(\widetilde{0}_{B_k})} \frac{\widetilde{\vartheta}(\widetilde{0}_{B_k})}{(1,\ell.\beta_1,0)\widetilde{\vartheta}(\widetilde{0}_{B_k})}.$$

Using lemma 6.2 and the fact that $(1,\alpha_1,0)$ commutes with $(1,\beta_1,0)$ we get that $L' = R'$. Therefore,

$$L^{-1}.R = \frac{\langle \ell.\alpha_2, \beta_1 \rangle}{\langle \ell.\alpha_1, \beta_2 \rangle} = e_{\mathscr{L}_0^\ell}(x,y). \qquad \blacksquare$$

The preceding proposition gives us an algorithm to compute the pairing:

Algorithm 6.5 (Pairing computation):
Input $P, Q \in B_k[\ell]$
Output $e_{\mathscr{L}_0^\ell}(P,Q)$

Let $P, Q \in B_k[\ell]$, and choose any affine lift $\widetilde{P}$, $\widetilde{Q}$ and $\widetilde{P+Q}$, we can compute the following via addition chains:

$$\begin{array}{ccccc}
\widetilde{0}_{B_k} & \widetilde{P} & 2\widetilde{P} & \dots & \ell\widetilde{P} = \lambda_P^0 \widetilde{0}_{B_k} \\
\widetilde{Q} & \widetilde{P+Q} & 2\widetilde{P}+\widetilde{Q} & \dots & \ell\widetilde{P}+\widetilde{Q} = \lambda_P^1 \widetilde{Q} \\
2\widetilde{Q} & \widetilde{P}+2\widetilde{Q} & & & \\
\dots & \dots & & & \\
\ell\widetilde{Q} = \lambda_Q^0 \widetilde{0}_{B_k} & \widetilde{P}+\ell\widetilde{Q} = \lambda_Q^1 P & & &
\end{array}$$

- ➔ Namely we compute:

$$\ell\widetilde{P} := \texttt{chain\_mult}(\ell, \widetilde{P}) \quad \ell\widetilde{Q} := \texttt{chain\_mult}(\ell, \widetilde{Q})$$
$$\ell\widetilde{P}+\widetilde{Q} := \texttt{chain\_multadd}(\ell, \widetilde{P+Q}, \widetilde{P}, \widetilde{Q}) \quad \widetilde{P}+\ell\widetilde{Q} := \texttt{chain\_multadd}(\ell, \widetilde{P+Q}, \widetilde{Q}, \widetilde{P}).$$

- ➔ Then we have:

$$e_{\mathscr{L}_0^\ell}(P,Q) = \frac{\lambda_P^1 \lambda_Q^0}{\lambda_Q^1 \lambda_P^0} \tag{33}$$

Proof: Assume that $\widetilde{P}$, $\widetilde{Q}$ and $\widetilde{P+Q}$ are such that $\widetilde{P} = \widetilde{[\ell]}(1,\alpha_1,\beta_1)\widetilde{0}'_{B_k}$, $\widetilde{Q} = \widetilde{[\ell]}(1,\alpha_2,\beta_2)\widetilde{0}'_{B_k}$, and $\widetilde{P+Q} = \widetilde{[\ell]}(1,\alpha_1+\alpha_2,\beta_1+\beta_2)\widetilde{0}'_{B_k}$. Then by Corollary 24, we find that $\lambda_P^0 = \frac{\widetilde{\vartheta}(\widetilde{0}_{B_k})}{((1,\ell.\alpha_1,\ell.\alpha_2)\widetilde{\vartheta})(\widetilde{0}_{B_k})} = 1$ and that $\lambda_P^1 = \frac{((1,\ell.\alpha_1+\beta_1,\ell.\alpha_2+\beta_2)\widetilde{\vartheta})(\widetilde{0}_{B_k})}{((1,\beta_1,\beta_2)\widetilde{\vartheta})(0)}$, so that by Proposition 6.4, we have:

$$e_{\mathscr{L}_0^\ell}(P,Q) = \frac{\lambda_P^1 \lambda_Q^0}{\lambda_Q^1 \lambda_P^0}$$

Now by Lemma 3.10, it is easy to see that (33) is homogeneous and does not depend on the affine lifts $\widetilde{P}$, $\widetilde{Q}$ and $\widetilde{P+Q}$, which concludes the proof. ∎

Complexity Analysis 6.6:
By using a Montgomery ladder, we see that we can compute $e_{\mathscr{L}_0^\ell}(P,Q)$ with four fast addition chains of length ℓ, hence we need $O(\log(\ell))$ additions. It should be noted that we can reuse a lot of computation between the addition chains $P, 2P, 4P, \ldots$ and $P+Q, 2P+Q, 4P+Q, \ldots$ since we always add the same point at the same time between the two chains.

The case $n=2$ Let $\pm P, \pm Q \in K_B$, then we have $e_{\mathscr{L}_0^\ell}(\pm P, \pm Q) = \{e_{\mathscr{L}_0^\ell}(P,Q), e_{\mathscr{L}_0^\ell}(P,Q)^{-1}\}$. Thus the pairing on the Kummer variety is a bilinear pairing $K_B \times K_B \to k^{*,\pm}$ where $k^{*,\pm} = k^*/\{x = 1/x\}$. We represent a class $\overline{x} \in k^{*,\pm}$ by $x + 1/x \in k$, and we define the symmetric pairing $e_s'(\pm P, \pm Q) = e_{\mathscr{L}_0^\ell}(P,Q) + e_{\mathscr{L}_0^\ell}(P,-Q)$. We can use the addition relations to compute $P \pm Q$ and then use Algorithm 6.5 to compute $e_{\mathscr{L}_0^\ell}(P,Q)$, $e_{\mathscr{L}_0^\ell}(P,-Q)$.

7 Conclusion

We have described an algorithm that give a modular point from an isotropic kernel, and another one that can compute the isogeny associated to a modular point. By combining these two algorithms, we can compute any isogeny between abelian varieties. However, the level of the modular space that we use depend on the degree of the isogeny. Still, we can go back to a modular point of level n by using the modular correspondence introduced in [FLR09]. This mean that we can compute isogeny graphs if we restrict to ℓ^2-isogenies. We have also introduced a point compression algorithm, that allows to drastically reduce the number of coordinates of a projective embedding of level 4ℓ. This new representation can be useful when one has to work with such a projective embedding, rather than the usual one of level 4 (for instance if one need a quick access to the translation by a point of ℓ-torsion).

References

[CFA+06] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[FLR09] Jean-Charles Faugère, David Lubicz, and Damien Robert. Computing modular correspondences for abelian varieties, October 2009.

[Gau07] P. Gaudry. Fast genus 2 arithmetic based on Theta functions. *Journal of Mathematical Cryptology*, 1(3):243–265, 2007.

[GS08] P. Gaudry and E. Schost. Hyperelliptic curve point counting record: 254 bit jacobian, 06 2008. Available at http://webloria.loria.fr/ gaudry/record127/.

[Igu72] Jun-ichi Igusa. *Theta functions*. Springer-Verlag, New York, 1972. Die Grundlehren der mathematischen Wissenschaften, Band 194.

[Kem88] G.R. Kempf. Multiplication over abelian varieties. *American Journal of Mathematics*, 110(4):765–773, 1988.

[Kem89] George R. Kempf. Linear systems on abelian varieties. *Amer. J. Math.*, 111(1):65–94, 1989.

[Kem92] G.R. Kempf. Equations of Kümmer Varieties. *American Journal of Mathematics*, 114(1):229–232, 1992.

[Koh03] David R. Kohel. The AGM-$X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting. In *Advances in cryptology—ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Comput. Sci.*, pages 124–136. Springer, Berlin, 2003.

[Koi76] S. Koizumi. Theta relations and projective normality of abelian varieties. *American Journal of Mathematics*, pages 865–889, 1976.

[Ler] R. Lercier. Algorithmique des courbes elliptiques dans les corps finis. These, LIX–CNRS, juin 1997.

[LR10] D. Lubicz and D. Robert. Efficient Pairing Computation With Theta Functions. *Preprint*, 2010.

[Mil04] Victor S. Miller. The weil pairing, and its efficient calculation. *J. Cryptology*, 17(4):235–261, 2004.

[Mum66] D. Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1:287–354, 1966.

[Mum70] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[Ric36] 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.

[Ric37] F. Richelot. De transformatione Integralium Abelianorum primiordinis commentation. *J. reine angew. Math.*, 16:221–341, 1837.

[Smi08] Benjamin Smith. Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves. Smart, Nigel (ed.), Advances in cryptology – EUROCRYPT 2008. 27th annual international conference on the theory and applications of cryptographic techniques, Istanbul, Turkey, April 13–17, 2008. Proceedings. Berlin: Springer. Lecture Notes in Computer Science 4965, 163-180 (2008)., 2008.

[Smi09] Benjamin Smith. Isogenies and the discrete logarithm problem in jacobians of genus 3 hyperelliptic curves, February 2009.

[Vél71] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

[Wam99] P. Wamelen. Equations for the Jacobian of a hyperelliptic curve. *AMS*, 350(8):3083–3106, August 1999.