D. Lubicz and D. Robert *Res. Number Theory* (2023) 9:7
https://doi.org/10.1007/s40993-022-00407-9

Research in Number Theory

RESEARCH

Fast change of level and applications to isogenies

David Lubicz[1*] and Damien Robert[2]

*Correspondence:
david.lubicz@univ-rennes1.fr;
http://perso.univ-rennes1.fr/david.lubicz
[1]IRMAR, Universté de Rennes, 1 Campus de Beaulieu, 35042 Rennes, France
Full list of author information is available at the end of the article
This work was supported by the ANR project CIAO

Abstract

Let $(A, \mathscr{L}, \Theta_n)$ be a dimension g abelian variety together with a level n theta structure over a field k of odd characteristic. We thus denote by $(\theta_i^{\Theta_{\mathscr{L}}})_{(\mathbb{Z}/n\mathbb{Z})^g} \in \Gamma(A, \mathscr{L})$ the associated standard basis. For a positive integer ℓ relatively prime to n and the characteristic of k, we study change of level algorithms which allow one to compute level ℓn theta functions $(\theta_i^{\Theta_{\mathscr{L}^\ell}}(x))_{i\in(\mathbb{Z}/\ell n\mathbb{Z})^g}$ from the knowledge of level n theta functions $(\theta_i^{\Theta_{\mathscr{L}}}(x))_{(\mathbb{Z}/n\mathbb{Z})^g}$ or vice versa. The classical duplication formulas are an example of change of level algorithm to go from level n to level $2n$. The main result of this paper states that there exists an algorithm to go from level n to level ℓn in $O(n^g\ell^{2g})$ operations in k. We derive an algorithm to compute an isogeny $f : A \to B$ from the knowledge of $(A, \mathscr{L}, \Theta_n)$ and $K \subset A[\ell]$ isotropic for the Weil pairing which computes $f(x)$ for $x \in A(k)$ in $O((n\ell)^g)$ operations in k. We remark that this isogeny computation algorithm is of quasi-linear complexity in the size of K.

Keywords: Isogenies, Abelian varieties, Computational algebraic geometry

Mathematics Subject Classification: 14K02, 14Q15

1 Introduction

1.1 Fast change of level

Let $A = \mathbb{C}^g/\Lambda$ be a dimension g complex abelian variety. An analytic projective embedding of A can be defined provided that we have enough analytic functions on quasi-periodic $\mathbb{C}^g$ with respect to Λ. Let $n \in \mathbb{N}$; if $\Lambda = \mathbb{Z}^g + \Omega\mathbb{Z}^g$ where $\Omega \in \mathfrak{H}_g(\mathbb{C})$ is a Siegel period matrix, we define following [18, Chap. II, §1, Def. 1.2] the Λ-quasi-periodic functions of level n as the vector space R^n_Ω over $\mathbb{C}$ of analytic functions f on $\mathbb{C}^g$ such that

$$f(z+\lambda) = f(z), \quad f(z+\Omega\lambda) = \exp(-\pi i n^t\lambda\Omega\lambda - 2\pi i n^t z\lambda)f(z), \tag{1}$$

for all $z \in \mathbb{C}^g$, $\lambda \in \mathbb{Z}^g$. Let $Z(\overline{n}) = (\mathbb{Z}/n\mathbb{Z})^g$. It can be shown that the dimension of R^n_Ω is n^g, and a standard basis of it is provided by the classical theta functions with characteristics $\theta\begin{bmatrix}0\\ b/n\end{bmatrix}(z, \Omega/n)$ for $b \in Z(\overline{n})$.

Now, if ℓ and n are two positive integers, by a change of the level algorithm, we mean an algorithm to compute the elements of the standard basis of R^n_Ω from the knowledge of the standard basis of $R^{\ell n}_\Omega$ (going down in level) and the other way around (going up in level).

The vector spaces R^n_Ω can be interpreted as the space of sections $\Gamma(A, \mathscr{L}_0^n)$ where $\mathscr{L}_0$ is a principal line bundle on A. The standard basis of $\Gamma(A, \mathscr{L}_0^n)$ given by the theta functions is determined by the canonical (symmetric) theta structure (see Definition 2.6) associated to Ω. This point of view generalizes for an abelian variety over any field k. Let $(A, \mathscr{L})$ be a dimension g abelian variety over a field k together with an ample line bundle $\mathscr{L}$ such that $\mathscr{L} = \mathscr{L}_0^n$ with $\mathscr{L}_0$ as a principal line bundle. Then a theta structure $\Theta_{\mathscr{L}}$ determines a standard basis which we denote by $(\theta_i^{\Theta_{\mathscr{L}}})_{i\in Z(\overline{n})} \in \Gamma(A, \mathscr{L})$. If $\mathscr{L}$ is very ample (e.g. $n \geq 3$ by a theorem of Lefschetz), $\Theta_{\mathscr{L}}$ defines a unique projective embedding $A \to \mathbb{P}^{Z(\overline{n})}$ given on points by $x \mapsto (\theta_i^{\Theta_{\mathscr{L}}}(x))$. The projective point $(\theta_i^{\Theta_{\mathscr{L}}}(0_A))_{i\in Z(\overline{n})}$ is called the theta null point of $(A, \mathscr{L}, \Theta_n)$.

In the literature, change of level algorithms often take the form of a formula giving an expression of $(\theta_i^{\Theta_{\mathscr{L}^\ell}}(x))_{i\in Z(\overline{\ell n})}$ as a function of $(\theta_i^{\Theta_{\mathscr{L}}}(x))_{i\in Z(\overline{n})}$ or vice versa. Change-of-level formulas are central in the theory of theta functions. In fact, multiplication formulas [16, p. 330] from which one can immediately deduce Riemann formulas can be seen as a formula to go from level n to level $2n$. Using Koizumi formulas [11], the authors of [4] deduce a formula to go down from level ℓn to level n. In this paper, we are interested in the computational efficiency of change-of-level algorithms measured as the number of field operations required to obtain the result. In this regard, we prove the following two theorems. The first theorem, proved in Theorem 4.4, is for going from level n up to level ℓn:

Theorem 1.1 *Let n, ℓ be relatively prime integers with n even. Let $(A, \mathscr{L}, \Theta_{\mathscr{L}})$ be a dimension g abelian variety together with a level n symmetric theta structure defined over k.*

Assume that k is of characteristic zero or prime to ℓn.

We have the following:

- *Given a basis of $A[\ell]$ and the corresponding symplectic decomposition for the Weil pairing $A[\ell] = A_1[\ell] \oplus A_2[\ell]$, there is a canonical symmetric theta structure $\Theta_{\mathscr{L}^\ell}$ of level ℓn on $(A, \mathscr{L}^\ell)$.*
- *Let x be a point of A, such that from the knowledge of $(\theta_i^{\Theta_{\mathscr{L}}}(x))_{i\in Z(\overline{n})}$ defined over $k(x)$, one can compute $(\theta_i^{\Theta_{\mathscr{L}^\ell}}(x))_{i\in Z(\overline{\ell n})}$ with $O(n^g \ell^{2g})$ operations in $k(x)$.*

In particular, we can compute the theta null point of level ℓn in $O(n^g \ell^{2g})$ operations in k.

We also have a change-of-level algorithm to go from level ℓn down to level n.

Corollary 1.2 *Let n be an even integer and ℓ an integer relatively prime to n. Let $(A, \mathscr{L}^\ell, \Theta_{\mathscr{L}^\ell})$ be a dimension g abelian variety together with a level ℓn symmetric theta structure. We suppose that k, the field of definition of $(A, \mathscr{L}, \Theta_{\mathscr{L}^\ell})$, is of characteristic zero or prime to ℓn.*

We have the following:

- *$\Theta_{\mathscr{L}^\ell}$ induces a unique symmetric theta structure of level n for $(A, \mathscr{L})$;*
- *Let x be a point of A defined over $k(x)$ given by $(\theta_i^{\Theta_{\mathscr{L}^\ell}}(x))_{i\in Z(\overline{\ell n})}$. One can compute $(\theta_i^{\Theta_{\mathscr{L}}}(\ell x))_{i\in Z(\overline{n})}$ in $O(n^g \ell^g)$ operations in $k(x)$.*

In particular, one can compute the theta null point of level n from the knowledge of the theta null point of level ℓn in $O(n^g \ell^g)$ operations in k.

To obtain this result, proved in Theorem 5.1, the idea is to first use Theorem 1.1 to go from level $n\ell$ to level $n\ell^2$, and then descend along the isogeny $[\ell]$ using Mumford's isogeny theorem [16, Sect. 1, Theorem 4] to land in level n (see also Example 2.17). Note that if $\ell = m^2$, we can descend along $[m]$ directly, which only costs $O((nm)^g)$ field operations to compute $(\theta_i^{\Theta_{\mathscr{L}}}(mx))_{i\in Z(\overline{n})}$, hence $O((nm)^g)$ field operations to compute $(\theta_i^{\Theta_{\mathscr{L}}}(\ell x))_{i\in Z(\overline{n})}$.

In [4], the authors used Koizumi's formulas, given by an integral matrix F such that ${}^tFF = \ell \mathrm{Id}_r$, to descend levels. These take $O(\ell^{gr/2})$ field operations, where $r = 1$ if ℓ is a square, $r = 2$ if ℓ is a sum of two squares, and $r = 4$ otherwise. This dependence on r of the complexity of Koizumi's formulas comes from the size of the kernel of $F : A^r \to A^r$ which is ℓ^{gr}. As a consequence, Theorem 1.2 achieves a better complexity than Koizumi's formulas in the case in which ℓ is not a sum of two squares.

As an application, we can improve the complexity of the isogeny computation algorithms [4,14]. Let $f : A \to B$ be an isogeny with kernel $K \subset A[\ell]$ isotropic for the Weil pairing. In order to compute f, starting from $(A, \mathscr{L}, \Theta_{\mathscr{L}})$, an abelian variety together with a level n symmetric theta structure, we have to equip B with a level n symmetric theta structure and compute the isogeny in the coordinates provides by these theta structures. There are two strategies:

- ascend to level ℓn on A using Theorem 1.1 and then use Mumford's theorem to compute the isogeny from A with a theta structure of level ℓn to B with a theta structure of level n; and
- use the contragradient isogeny $\hat{f} : B \to A$ to endow B with a level ℓn theta structure by inverting Mumford's isogeny theorem using [13] (see also Sect. 4.1) and use Theorem 1.2 to descend from level ℓn on B to level n.

Both strategies give a quasi-linear time isogeny algorithm:

Theorem 1.3 *Let $(A, \mathscr{L}, \Theta_{\mathscr{L}})$ be an abelian variety together with a level n symmetric theta structure over k, n even.*

Let ℓ be an odd integer prime to n, and we suppose that ℓn is prime to the characteristic of k, or that k is of characteristic zero. Let $K \subset A[\ell]$ be a totally isotropic subgroup for the Weil pairing defined over k, and let $f : A \to B = A/K$ be an isogeny.

Then f induces a line bundle $\mathscr{M}$ together with $\Theta_{\mathscr{M}}$ a level n symmetric theta structure for $(B, \mathscr{M})$. Moreover, for a point x of A with field of definition $k(x)$ and given by $(\theta_i^{\Theta_{\mathscr{L}}}(x))_{i\in Z(\overline{n})}$ and suitable equations for K, we can compute $(\theta_i^{\Theta_{\mathscr{M}}}(f(x)))_{i\in Z(\overline{n})}$ in time $O((n\ell)^g)$ operations in $k(x)$.

Here, we say that K is totally isotropic whenever there exists a symplectic decomposition $A[\ell] = K \oplus K'$; in particular, K is then maximal isotropic. (The converse is not true; for instance, $A[\ell]$ is maximal isotropic in $A[\ell^2]$ for the Weil pairing e_{ℓ^2}, but is not totally isotropic.) In Remark 4.8, we explain the tweaks to make for the algorithms above when ℓ is no longer prime to n. This algorithm improves the isogeny algorithms of [4,13]: these followed the second approach with the slower descent of level algorithm from Koizumi's formula. Compared to Theorem 1.1, in Theorem 1.3, we only have to compute the action of the level subgroup $\tilde{K}$ above K rather than the full ℓn theta structure, which explains the resulting complexity. We refer to Corollary 4.6 for the proof, and we give examples of

isogeny computations in genus 1 and 2 in Examples 4.9 and 4.10. A similar approach is used in [5] but is limited to isogenies between Jacobians.

In Sect. 6, we outline how to extend these algorithms when the abelian variety A has real multiplication. For descending levels and computing cyclic isogenies, Koizumi's formula was extended to this case in [6]. But a drawback of this approach is that the isogeny F given by Koizumi's formula does not preserve the product theta structure, and hence required a very costly disentangling which makes the algorithm almost impractical. This drawback does not exist with the new approach. We stress however that our new approach has not yet been implemented for cyclic isogenies, so we leave the practical complexity for future work. There are still many hurdles to overcome: see Remark 6.6.

We note that apart from isogeny computations, being able to change level allows us to give the equivalent of Thomae formula for theta functions of higher level. These could also be used to compute modular forms (expressed as polynomials of theta functions of suitable levels), but, unfortunately, our method only gives the projective theta constants, not the affine (modular) ones. So for now, we can only apply our results to modular functions. See Sect. 1.3 for more details.

1.2 Outline

For simplicity, we work over the base field $\mathbb{C}$. Since our resulting algorithms are given by polynomial equations, by standard lifting and rigidity arguments, they apply over an algebraically closed field of characteristic p too as long as everything is étale, that is, as long as p is prime to ℓn. Indeed, the moduli stack of abelian varieties with a symmetric level ℓn structure is smooth over $\mathbb{Z}[\frac{1}{\ell n}]$, so we can lift them to characteristic zero (this works even for non-ordinary abelian varieties). Alternatively, it is not hard to use Mumford's algebraic theory [16] to give direct proofs; we refer to [21, Sect. 2.10] for this. Concerning the field of definition in Theorem 1.3, we explain in Remark 4.7 how to adapt the methods of [14] to compute the isogeny f using computations in the field of definition of K.

In Sect. 2, we review the theory of theta functions. Let A be an abelian variety and H a polarisation of A. We define the "universal theta group" $\mathfrak{G}(H)$ associated to H, and the theta group $G(\mathscr{L})$ (a subgroup of $\mathfrak{G}(H)$)) associated to a line bundle $\mathscr{L}$ whose polarisation is H. The group $\mathfrak{G}(H)$ acts on analytic functions, and this gives an action of $G(\mathscr{L})$ on sections of $\mathscr{L}$. The group $\mathfrak{G}(H)$ may be seen as the theta group of all isogenous abelian varieties with polarisation given by H glued together. In Proposition 2.11, we give a simple recipe to recover the basis of theta functions from just one section u of $\mathscr{L}$ and the action of $G(\mathscr{L})$. As an application, we recover Mumford's isogeny theorem and explain how to compute theta functions of isogenous abelian varieties in Proposition 2.15.

In Sect. 3, we explain how we may compute the action of a larger group G' than $G(\mathscr{L})$ on sections of $\mathscr{L}$, namely, $G' = \{g \in \mathfrak{G}(H) \mid g^\ell \in G(\mathscr{L})\}$. A caveat is that sections are no longer sent to sections. So algebraically, the action involves some non-canonical choices.

In Sect. 4.1, as an application, we show how to use this extended action to go up in level along an isogeny, i.e., given an isogeny $f : A' \to A$, recover the theta basis for $f^*\mathscr{L}$. Then in Sect. 4.2, given a decomposition $\ell = \sum a_i^2$, we construct a section u of $\mathscr{L}^\ell$ from sections of $\mathscr{L}$, and we use the action of G' determined previously on these sections to compute the action of $\mathfrak{G}(\ell H)$ on u, and hence of $G(\mathscr{L}^\ell)$ on u. Here, the action does give sections, so the choices we made earlier all give the same final result. Applying Proposition 2.11

then gives our basis of theta functions of level ℓn on A. The full algorithm is described in Theorem 4.4 and its application to isogenies in Corollary 4.6.

In Sect. 5, we explain how to descend in level. Finally, in Sect. 6, we outline how to extend our algorithms to the case of real multiplication.

1.3 Open problem

A drawback of Proposition 2.11 for constructing theta functions is that it only works projectively; i.e., our basis of theta functions is defined up to a constant. But theta constants are also modular forms (of weight 1/2), so given a period matrix Ω, there is a canonical affine basis of the theta function (the basis $\theta\left[\begin{smallmatrix}0\\ i/n\end{smallmatrix}\right](z, \Omega/n)$). Algebraically, to a basis of differential forms $w_1, \ldots, w_g$ on A, corresponds a canonical theta constant (up to a sign) depending only on $w_1 \wedge \cdots \wedge w_g$. Keeping this basis when going up, or pushing it forward through an isogeny, this also defines canonical theta coordinates of level ℓn. We leave as an open problem working out exactly how to get the correct coordinates as modular forms. In other words, how to determine the unknown constant C appearing in Theorem 4.4, Corollary 4.6 and Theorem 5.1. For the older isogeny algorithm of [4,13], getting this correct constant was done in [10], which was used to compute modular forms.

As mentioned in the Introduction, the importance of this problem lies in the following: by [9], every modular form of a certain level N is integral over a suitable ring of theta constants. Hence, being able to evaluate theta constants of arbitrary level would allow one to evaluate algebraically modular forms of any level (provided we are able to express its minimal polynomial over the theta constants and then select the correct root). Unfortunately, as long as we are not able to get the correct constant, we can only use the results of this paper to evaluate modular functions of level N, and not modular forms.

2 Constructing theta functions

In order to fix the notations, we briefly review complex abelian varieties and theta functions and refer to [1,18,19] for more details. Our presentation follows closely that of [1, Chap. 6] with slight changes in the definition of theta structure and symmetric theta structure for the sake of simplicity. Let $A = V/\Lambda$ be a complex abelian variety, where $V = \mathbb{C}^g$, and Λ is a $\mathbb{Z}$ lattice in V of rank $2g$. We denote by $\pi : V \to A$ the canonical projection.

2.1 Line bundles

Projective coordinates on A are given by analytic functions $u : V \to \mathbb{C}$ which are periodic with respect to Λ up to some automorphic factors: $u(z + \lambda) = a_{\mathscr{L}}(z, \lambda)^{-1}u(z)$ for $z \in V$, $\lambda \in \Lambda$. The factors $a_{\mathscr{L}}(z, \lambda)$ verify the cocycle condition $a_{\mathscr{L}}(z, \lambda_1+\lambda_2) = a_{\mathscr{L}}(z, \lambda_1)a_{\mathscr{L}}(z+\lambda_1, \lambda_2)$, $z \in V$, $\lambda_1, \lambda_2 \in \Lambda$. Equivalently, the automorphic factor $a_{\mathscr{L}}$ defines a line bundle $\mathscr{L}$ on A as the quotient of the trivial line bundle on $V \times \mathbb{C}$ over V by the action of Λ given by $\lambda.(v, t) \mapsto (v + \lambda, a_{\mathscr{L}}(z, \lambda)t)$.

The possible automorphic factors are classified by the Appel–Humbert theorem. Up to changing the automorphic factor by a suitable coboundary (this simply changes the corresponding line bundle by an isomorphism), we have $a_{\mathscr{L}}(z, \lambda) = \chi_{\mathscr{L}}(\lambda)e^{\pi/2H_{\mathscr{L}}(\lambda,\lambda)}e^{\pi H_{\mathscr{L}}(z,\lambda)}$, where $H_{\mathscr{L}}$ is an Hermitian form on V associated to $\mathscr{L}$. The Hermitian form $H_{\mathscr{L}}$ is such that if $E_{\mathscr{L}} = \Im H_{\mathscr{L}}$ (where $\Im$ stands for the imaginary part), $E_{\mathscr{L}}(\Lambda, \Lambda) \subset \mathbb{Z}$, and $\chi_{\mathscr{L}}$ is a

semi-character for $H_{\mathscr{L}}$ [1, Theorem 2.2.3]. We recall that a semi-character for $H_{\mathscr{L}}$ is a map $\chi : \Lambda \to \mathbb{C}_1$, satisfying $\chi(\lambda+\lambda') = \chi(\lambda)\chi(\lambda')e^{i\pi E_{\mathscr{L}}(\lambda,\lambda')}$ for all $\lambda, \lambda' \in \Lambda$.

One can recover $H_{\mathscr{L}}$ from $E_{\mathscr{L}}$, so we will call either a Riemann form of $\mathscr{L}$. The Riemann form of $\mathscr{L}$ characterises its algebraic equivalence class. The map $\mathscr{L} \mapsto (\chi_{\mathscr{L}}, H_{\mathscr{L}})$ is a bijective correspondence between isomorphism classes of line bundles and their associated semi-characters and Riemann forms.

The algebraic equivalence class $H_{\mathscr{L}}$ of a line bundle $\mathscr{L}$ is called a polarisation on A. The data of the polarisation associated to $\mathscr{L}$ is equivalent to that of the morphism $\phi_{\mathscr{L}} : A \to \widehat{A}_k, x \mapsto \tau_x^*\mathscr{L}.\mathscr{L}^{-1}$ whose analytic form is $z \mapsto H_{\mathscr{L}}(z,\cdot)$. We recall that $\mathscr{L}$ is ample if and only if either $\phi_{\mathscr{L}}$ is an isogeny or $H_{\mathscr{L}}$ is definite positive. The symplectic form $E_{\mathscr{L}}$ allows one to define the Weil pairing on $K(\mathscr{L})$ by $e_{\mathscr{L}}(\bar{x}_1,\bar{x}_2) = e^{-2\pi i E_{\mathscr{L}}(x_1,x_2)}$, where $\bar{x}_i = x_i \mod \Lambda$ for $i = 1, 2$. We denote by $K(\mathscr{L}) = \mathscr{L}\phi_{\mathscr{L}}$ the kernel of the polarisation, so we have $K(\mathscr{L}) \simeq \Lambda(\mathscr{L})/\Lambda$, where $\Lambda(\mathscr{L}) = \Lambda^{\perp_{e_{\mathscr{L}}}}$ is the $e_{\mathscr{L}}$ orthogonal of Λ. We say that $\mathscr{L}$ is of type n if $E_{\mathscr{L}}$ is of type n on Λ, in which case $K(\mathscr{L}) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$; equivalently, $\mathscr{L} = \mathscr{L}_0^n$ is the nth power of a principal line bundle (associated to the Hermitian form $H_{\mathscr{L}_0} = H_{\mathscr{L}}/n$).

Assume that we have a symplectic decomposition $\Lambda = \Lambda_1 \oplus \Lambda_2$ of Λ for a Riemann form $E_{\mathscr{L}}$. We will denote such a decomposition by $\sigma = (\sigma_1, \sigma_2)$ where σ_i is the projector onto Λ_i. Using σ, we can define a canonical semi-character by $\chi(\lambda) = e^{\pi i E(\sigma_1(\lambda),\sigma_2(\lambda))}$ [1, Lemma 3.1.1], which by Appel–Humbert theorem gives a canonical symmetric line bundle $\mathscr{L}^\sigma$, often denoted herein by $\mathscr{L}$ for simplicity.

Remark 2.1 For reasons explained in Sect. 3, we will mostly consider the case when the level n is even. In this case, all the symplectic decompositions σ of Λ give $\chi_{\mathscr{L}^\sigma} = 1$; hence, the line bundle associated by the Appel–Humber theorem to the canonical semi-character does not depend on the choice of a symplectic decomposition of Λ. This means that $\mathscr{L}$ is the unique (totally) symmetric line bundle in the algebraic class given by H, i.e. the unique line bundle in this algebraic equivalence class such that $\mathscr{L} = \mathscr{L}_0^n$ with $\mathscr{L}_0$ principal symmetric.

2.2 The theta group

In this section, we introduce the theta group and study two important properties of that group that we will use, namely

- the structure of extensions of V by $\mathbb{C}^*$ and the existence of sections above V; and
- the action of the theta group on sections of $\mathscr{L}$.

Following [1, Chap. 6], we denote by $\mathfrak{G}(\mathscr{L}) = \{[\alpha, w] \mid \alpha \in \mathbb{C}^*, w \in V\}$ the group with composition law $[\alpha_1, w_1].[\alpha_2, w_2] = [\alpha_1\alpha_2 e^{\pi H_{\mathscr{L}}(w_2,w_1)}, w_1 + w_2]$. We can interpret $\mathfrak{G}(\mathscr{L})$ as the automorphism group of the trivial line bundle $\pi^*\mathscr{L} \simeq V \times \mathbb{C}$ above translations on V. Note that $\mathfrak{G}(\mathscr{L})$ only depends on $H_{\mathscr{L}}$, so we may also use the notation $\mathfrak{G}(H_{\mathscr{L}})$ (or $\mathfrak{G}(H)$ if H is a general Riemann form).

The group $\mathfrak{G}(\mathscr{L})$ is non-commutative. If $z_1, z_2 \in V$, $g_1 = [\alpha_1, z_1]$ and $g_2 = [\alpha_2, z_2]$ two elements of $\mathfrak{G}(\mathscr{L})$ above z_1 and z_2, we also recover the Weil pairing $e_{\mathscr{L}}$ as the commutator pairing: $g_1g_2g_1^{-1}g_2^{-1} = [e^{-2i\pi E_{\mathscr{L}}(z_1,z_2)}, 0]$. It is clear that $\mathfrak{G}(\mathscr{L})$ is a central extension of V by $\mathbb{C}^*$. In order to study its sections above V, we need the following definition:

Definition 2.2 Let H be a Riemann form on V. Let $\sigma : V = V_1 \oplus V_2$ be a symplectic decomposition of V for E. Let Λ be a lattice of V, so we say that Λ is compatible with σ if $\Lambda = \Lambda \cap V_1 \oplus \Lambda \cap V_2$. We note that Λ is compatible with σ if and only if $\Lambda^\perp$ is.

A symplectic decomposition σ on Λ induces a symplectic decomposition $\sigma \otimes \mathbb{R} : V \to V_1 \oplus V_2$ on V which is compatible with Λ. This allows one to extend $a_{\mathscr{L}^\sigma}$ to all of $V \times V$ via $a_{\mathscr{L}^\sigma}(v, \lambda) = e^{\pi i E(\sigma_1(\lambda), \sigma_2(\lambda))} e^{\pi/2 H(\lambda,\lambda)} e^{\pi H(v,\lambda)}$, for all $(v, \lambda) \in V \times V$. This extension does not satisfy the cocycle condition and thus is not an automorphy factor.

Lemma 2.3 *Let H be a Riemann form on V. Let $\sigma : V = V_1 \oplus V_2$ be a symplectic decomposition of V for $E = \Im H$. Let Λ' be a lattice in V compatible with σ.*

Then Λ' is isotropic for E (i.e. $E(\Lambda', \Lambda') \subset \mathbb{Z}$) if and only if $a_{\mathscr{L}^\sigma}$ satisfies the cocycle condition on $V \times \Lambda'$, if and only if there is a group section $s_{\Lambda'} : \Lambda' \to \mathfrak{G}(\mathscr{L})$.

In this case, the map

$$s_\sigma : \Lambda' \to \mathfrak{G}(\mathscr{L})$$
$$s_\sigma(\lambda) = [a_{\mathscr{L}^\sigma}(0, \lambda), \lambda] = [e^{\pi i E_{\mathscr{L}}(\sigma_1(\lambda), \sigma_2(\lambda))} e^{\pi/2 H_{\mathscr{L}}(\lambda,\lambda)}, \lambda].$$

is an explicit group section.

Proof Writing the cocycle condition for $a_{\mathscr{L}^\sigma}$ or $V \times \Lambda'$, it is easy to see that it is equivalent to Λ' being isotropic for E. If there is a group section $\Lambda' \to \mathfrak{G}(\mathscr{L})$, then the commutator interpretation of the Weil pairing shows that Λ' has to be isotropic, since $s(\Lambda')$ is commutative.

Finally, if Λ' is isotropic, it remains to check that s_σ is a group section. We have seen that $a_{\mathscr{L}^\sigma}$ verifies the cocycle condition. We then have $[a_{\mathscr{L}^\sigma}(0, \lambda + \lambda'), \lambda + \lambda'] = [a_{\mathscr{L}^\sigma}(0, \lambda') a_{\mathscr{L}^\sigma}(\lambda', \lambda), \lambda + \lambda'] = [a_{\mathscr{L}^\sigma}(0, \lambda) a_{\mathscr{L}^\sigma}(0, \lambda') a_{\mathscr{L}^\sigma}(\lambda', \lambda) / a_{\mathscr{L}^\sigma}(0, \lambda), \lambda + \lambda'] = [a_{\mathscr{L}^\sigma}(0, \lambda), \lambda][a_{\mathscr{L}^\sigma}(0, \lambda'), \lambda']$. □

The group $\mathfrak{G}(\mathscr{L})$ acts on analytic functions u in V via $[\hat{I}\pm, w] \circ (\mathrm{Id} \times u) = (\mathrm{Id} \times [\hat{I}\pm, w] \cdot u) \circ t_{-w}$, where $t_{-w}(z) = z - w$; namely, we have

$$[\alpha, w] \cdot u(z) = \alpha e^{\pi H_{\mathscr{L}}(z-w,w)} u(z - w). \tag{2}$$

Let $\sigma : V = V_1 \oplus V_2$ be a symplectic decomposition of V and suppose that Λ is compatible with σ. By Lemma 2.3, we have a group section $s_\sigma : \Lambda \to \mathfrak{G}(\mathscr{L})$. We may extend it to a *set section* on the whole of V via $s_\sigma(v) = [a_{\mathscr{L}^\sigma}(0, v), v]$.

We have the following:

Lemma 2.4 *[1, Theorem 6.1.3] The automorphism group $G(\mathscr{L})$ of $\mathscr{L}$ is equal to $G(\mathscr{L}) = Z(s(\Lambda))/s(\Lambda)$, where $Z(s(\Lambda))$ denotes the commutator of $s(\Lambda)$ in $\mathfrak{G}(H_{\mathscr{L}})$. The action of Equation 2 induces an action of $G(\mathscr{L})$ on $\Gamma(A, \mathscr{L})$.*

Explicitly, for $\lambda \in \Lambda(\mathscr{L})$ and $u \in \Gamma(A, \mathscr{L})$, we have

$$s_\sigma(\lambda) \cdot u(z) = a_{\mathscr{L}}(z - \lambda, \lambda) u(z - \lambda). \tag{3}$$

Proof As $\mathscr{L}$ is the quotient of the trivial bundle over V by the action of $s_\sigma(\Lambda)$, it is clear that $s_\sigma(\Lambda)$ acts trivially on $\Gamma(A, \mathscr{L})$ (in fact, by definition, $\Gamma(A, \mathscr{L})$ are exactly the analytic functions on V fixed by this subgroup). In particular, the action (2) restricted to elements of $Z(s(\Lambda))$ sends sections of $\mathscr{L}$ to other sections, and hence induces an action of $G(\mathscr{L})$ on $\Gamma(A, \mathscr{L})$. Equation 3 is a simple computation. □

2.3 Theta structures

In this section, we introduce the notion of theta structure. Let $(A = V/\Lambda, \mathscr{L})$ be a polarised abelian variety. Let σ be a symplectic decomposition of V, and we suppose that Λ is compatible with σ and that $\mathscr{L} = \mathscr{L}^\sigma$. Note that by taking the quotient of $\Lambda(\mathscr{L})$ by Λ, σ induces a decomposition $K(\mathscr{L}) = K_1(\mathscr{L}) \oplus K_2(\mathscr{L})$ for $e_{\mathscr{L}}$. Let Λ' be such that $\Lambda \subset \Lambda' \subset \Lambda(\mathscr{L})$ and let $K = \Lambda'/\Lambda$. Then Λ' is compatible with σ if and only if the symplectic decomposition of $K(\mathscr{L})$ above induces a symplectic decomposition of K for the Weil pairing $e_{\mathscr{L}}: K = K_1 \oplus K_2$ with $K_i = K_i(\mathscr{L}) \cap K$.

Given such a compatible Λ', using Lemmas 2.3 and 2.4, $s_\sigma(\Lambda')$ induces a canonical section $\tilde{K}$ of K into $G(\mathscr{L})$. Applying this to $\Lambda' = \Lambda_1(\mathscr{L}) \oplus \Lambda_2$ and to $\Lambda' = \Lambda_1 \oplus \Lambda_2(\mathscr{L})$, we get canonical sections s_1 and s_2 of $K_1(\mathscr{L})$ and $K_2(\mathscr{L})$ (or more generally of any isotropic $K = K_1 \oplus K_2 \subset K_1(\mathscr{L}) \oplus K_2(\mathscr{L})$) into $G(\mathscr{L})$. We stress that these canonical sections depend on a choice of the symplectic decomposition σ of V; a choice of a symplectic decomposition of $K(\mathscr{L})$ is not sufficient to determine the sections s_i. We have proved the following:

Proposition 2.5 *Let $(A = V/\Lambda, \mathscr{L})$ be an abelian variety together with an ample line bundle. A choice of σ, a symplectic decomposition of Λ for $E_{\mathscr{L}}$, determines a symplectic decomposition $K(\mathscr{L}) = K_1(\mathscr{L}) \oplus K_2(\mathscr{L})$ and sections $s_i : K_i(\mathscr{L}) \to G(\mathscr{L})$.*

This motivates the following definition, slightly adapted from that of [16] and [1, Chap. 6.6]:

Definition 2.6 Let $(A = V/\Lambda, \mathscr{L})$ be an abelian variety of dimension g together with an ample line bundle. Let $K(\mathscr{L})$ be the kernel of the polarisation defined by $\mathscr{L}$. A theta structure $\Theta_{\mathscr{L}}$ for $(A, \mathscr{L})$ is the data of

- $K(\mathscr{L}) = K_1(\mathscr{L}) \oplus K_2(\mathscr{L})$, a symplectic decomposition of $K(\mathscr{L})$ for $e_{\mathscr{L}}$; and
- for $i = 1, 2$, sections $s_i^{\Theta_{\mathscr{L}}} : K_i(\mathscr{L}) \to G(\mathscr{L})$.

Via $s_i^{\Theta_{\mathscr{L}}}$ for $i = 1, 2$, we thus get an action of $K_i(\mathscr{L})$ on $\Gamma(A, \mathscr{L})$. For $i = 1, 2$, if $P \in K_i(\mathscr{L})$, we will denote by $P \cdot u$ the action $s_i^{\Theta_{\mathscr{L}}}(P) \cdot u$ of $s_i^{\Theta_{\mathscr{L}}}(P) \in G(\mathscr{L})$ on u.

In the following, if $\sigma : \Lambda = \Lambda_1 \oplus \Lambda_2$ is a symplectic decomposition of Λ, we denote by $\Theta_{\mathscr{L}}^\sigma$ the associated canonical theta structure following Proposition 2.5. We say that $\Theta_{\mathscr{L}}$ is symmetric if there exists a symplectic decomposition $\sigma : \Lambda = \Lambda_1 \oplus \Lambda_2$ such that $\mathscr{L} = \mathscr{L}^\sigma$ and $\Theta_{\mathscr{L}} = \Theta_{\mathscr{L}}^\sigma$.

Remark 2.7 We briefly explain the link between our definition of a symmetric theta structure and the usual one of [16] or [1, Chap. 6.9]. Let δ_{-1} be the group automorphism of $\mathfrak{G}(\mathscr{L})$ defined by $\delta_{-1}([\hat{I}\pm, w]) = [\hat{I}\pm, -w]$. Following [16], we say that an element g of $\mathfrak{G}(\mathscr{L})$ is symmetric if $\hat{I}'_{-1} g = g^{-1}$. One can check that the sections $s_i^{\Theta_{\mathscr{L}}}$ for $i = 1, 2$ deduced from the symplectic decomposition σ have value in symmetric elements of $\mathfrak{G}(\mathscr{L})$, and hence symmetric elements of $G(\mathscr{L})$. So a symmetric theta structure following Definition 2.6 is symmetric in the sense of [16].

Changing the symplectic decomposition of Λ will thus only change our sections by a sign on each element. Furthermore, symplectic decompositions σ of Λ give the same symmetric theta structure on $G(\mathscr{L})$ whenever they induce the same symplectic decomposition on $K(\mathscr{L}^2) \simeq \frac{1}{2}\Lambda(\mathscr{L})/\Lambda$. Finally, if $\lambda \in \Lambda'$ is of odd order modulo Λ, then $s_\sigma(\lambda)$

is *uniquely* defined as the unique symmetric lift of order ℓ, and hence does not depend on σ.

Definition 2.8 Let $(A = V/\Lambda, \mathscr{L}, \Theta_{\mathscr{L}})$ be an abelian variety with a symmetric theta structure on $\mathscr{L}$. We say that a symmetric theta structure $\Theta_{\mathscr{L}^\ell}$ on $\mathscr{L}^\ell$ is compatible with $\Theta_{\mathscr{L}}$ if there exists a symplectic decomposition σ of Λ such that $\Theta_{\mathscr{L}} = \Theta^\sigma_{\mathscr{L}}$ and $\Theta_{\mathscr{L}^\ell} = \Theta^\sigma_{\mathscr{L}^\ell}$.

The importance of theta structures lies in part in the following result (see [16, Sect. 1, Theorem 2]):

Theorem 2.9 (Maschke–Mumford) *The vector space $\Gamma(A, \mathscr{L})$ is the unique projective irreducible representation of $G(\mathscr{L})$.*

Corollary 2.10 *Suppose we have chosen a theta structure $\Theta_{\mathscr{L}}$ for $(A, \mathscr{L})$. There is a unique basis $(\theta_i^{\Theta_{\mathscr{L}}})_{i\in K_2(\mathscr{L})}$ (up to a common projective factor μ) of sections of $\mathscr{L}$ such that $\theta_0^{\Theta_{\mathscr{L}}}$ is invariant under the action of $s_1^{\Theta_{\mathscr{L}}}(K_1(\mathscr{L}))$, and if $i \in K_2(\mathscr{L})$, $\theta_i^{\Theta_{\mathscr{L}}} = s_2^{\Theta_{\mathscr{L}}}(i)\cdot\theta_0^{\Theta_{\mathscr{L}}}$. This basis is called the basis of theta functions of level n if $\mathscr{L}$ is of type n.*

The action of $s_i^{\Theta_{\mathscr{L}}}(K_i(\mathscr{L}))$ for $i = 1, 2$ on this basis is given by $j_1\cdot\theta_i^{\Theta_{\mathscr{L}}} = e_{\mathscr{L}}(j_1, i)\theta_i$ if $j_1 \in K_1(\mathscr{L})$, and $j_2\cdot\theta_i^{\Theta_{\mathscr{L}}} = \theta_{i+j_2}^{\Theta_{\mathscr{L}}}$ if $j_2 \in K_2(\mathscr{L})$.

Proof Since $\Gamma(A, \mathscr{L})$ is irreducible, it is isomorphic to the unique irreducible Heisenberg representation of $G(\mathscr{L})$ as described in [16, p. 297], from which we deduce the existence of the basis $(\theta_i^{\Theta_{\mathscr{L}}})$. The computation of the action of $s_i(K_i(\mathscr{L}))$ for $i = 1, 2$ on the family $(\theta_j^{\Theta_{\mathscr{L}}})_{j\in K_2(\mathscr{L})}$ is immediate from its definition. □

We thus immediately get the following recipe to construct the basis of theta functions of level n associated to a theta structure $\Theta_{\mathscr{L}}$:

Proposition 2.11 *Let $\Theta_{\mathscr{L}}$ be a theta structure for $(A, \mathscr{L})$. Let u be any section of $\Gamma(A, \mathscr{L})$ such that if $u = \sum\lambda_i\theta_i^{\Theta_{\mathscr{L}}}$, $\lambda_0 \neq 0$. Then, up to a constant, we have $\theta_0^{\Theta_{\mathscr{L}}} = \sum_{j\in K_1(\mathscr{L})} s_1^{\Theta_{\mathscr{L}}}(j)\cdot u$, and for $i \in K_2(\mathscr{L})$, $\theta_i^{\Theta_{\mathscr{L}}} = s_2(i)\cdot\theta_0^{\Theta_{\mathscr{L}}}$.*

We remark that using Mumford's algebraic theory of theta functions, the above proposition is valid for any theta structure of level n prime to the characteristic of the base field.

Remark 2.12 If u is such that $\lambda_0 = 0$, we can still reconstruct our theta basis as follows: assume that $\lambda_i \neq 0$. Then, since $\Gamma(A, \mathscr{L})$ decomposes into a sum of one-dimensional eigenspaces for the action of $G(\mathscr{L})$: $\Gamma(A, \mathscr{L}) = \oplus_{\chi\in K_1(\mathscr{L})^\vee}\Gamma(A, \mathscr{L})^\chi$, and $\theta_i^{\Theta_{\mathscr{L}}}$ is a generator of $\Gamma(A, \mathscr{L})^\chi$ for the character $\chi = e_{\mathscr{L}}(i, \cdot)$, we recover $\theta_i^{\Theta_{\mathscr{L}}}$ as the trace of u under $K_1(\mathscr{L})$ twisted by this character: $\theta_i^{\Theta_{\mathscr{L}}} = \sum_{j\in K_1(\mathscr{L})} e_{\mathscr{L}}(i, j)s(j)\cdot u = \sum_{j\in K_1(\mathscr{L})} s(i+j)\cdot u$ (alternatively, one could take the trace applied to $s(-i)\cdot u$). Then $\theta_{i'}^{\Theta_{\mathscr{L}}} = s(i-i')\cdot\theta_i^{\Theta_{\mathscr{L}}}$.

Example 2.13 Let $\sigma : \Lambda = \Lambda_1 \oplus \Lambda_2$ be a symplectic decomposition and let $(\theta_i^{\Theta^\sigma_{\mathscr{L}}})_{i\in K_2(\mathscr{L})}$ be the associated basis of theta functions. Then, permuting this decomposition $\sigma' : \Lambda = \Lambda_2 \oplus \Lambda_1$ gives another basis $(\theta_i^{\Theta^{\sigma'}_{\mathscr{L}}})$, indexed by $i \in K_1(\mathscr{L})$.

Applying Proposition 2.11, we get that (up to a constant) $\theta_0^{\Theta^{\sigma'}_{\mathscr{L}}} = \sum_{j\in K_2(\mathscr{L})}\theta_j^{\Theta^\sigma_{\mathscr{L}}}$, and if $i \in K_1(\mathscr{L})$, $\theta_i^{\Theta^{\sigma'}_{\mathscr{L}}} = i\cdot\theta_0^{\Theta^{\sigma'}_{\mathscr{L}}} = \sum_{j\in K_2(\mathscr{L})} e_{\mathscr{L}}(i, j)\theta_j^{\Theta^\sigma_{\mathscr{L}}}$.

2.4 Theta groups and isogenies

Let $A = V_A/\Lambda_A, B = V_B/\Lambda_B$ be dimension g abelian varieties. Let $f : A \to B$ be an isogeny and let $F : V_A \to V_B$ be the analytic representation of f. Let $\mathcal{M}$ be a line bundle on B with polarisation $H_{\mathcal{M}}$, then $\mathscr{L} = f^*\mathcal{M}$ has associated polarisation $H_{\mathscr{L}} = F^*H_{\mathcal{M}}$. We have a map $F : \mathfrak{G}(\mathscr{L}) \to \mathfrak{G}(\mathcal{M}), [\alpha, w] \mapsto [\alpha, F(w)]$, which is compatible with the action on sections: if u is an analytic function on V_B, then

$$[\alpha, w] \cdot F^*u = F^*([\alpha, F(w)] \cdot u). \tag{4}$$

Fix $\sigma = (\sigma_1, \sigma_2)$ as a symplectic decomposition of Λ_A with respect to $H_{\mathscr{L}}$ and let $K(\mathscr{L}) = K_1(\mathscr{L}) \oplus K_2(\mathscr{L})$ be the symplectic decomposition of $K(\mathscr{L})$ deduced from σ. Assume that $\Lambda' = F^{-1}(\hat{I} >_B) \subset \Lambda(\mathscr{L})$ is compatible with σ. This means that there exists a symplectic decomposition of $K = \mathscr{L}f, K = K_1 \oplus K_2$ such that $K_i = K \cap K_i(\mathscr{L})$. Then pushing σ through F, we obtain a symplectic decomposition of Λ_B that we denote by $F_*(\sigma \otimes \mathbb{R})_{|\Lambda_B} = F_*(\sigma \otimes \mathbb{R}_{|\Lambda'})$. Concretely, $F_*(\sigma_i \otimes \mathbb{R}) = F \circ (\sigma_i \otimes \mathbb{R}) \circ F^{-1}$. If $\mathcal{M}$ is the line bundle corresponding to the canonical automorphic factor $a_{\mathcal{M}}$ associated to $F_*(\sigma \otimes \mathbb{R})$, and $\mathscr{L}$ is the line bundle corresponding to σ, then we check that $a_{\mathcal{M}}(F(\nu), F(\lambda)) = a_{\mathscr{L}}(\nu, \lambda)$, and hence $f^*\mathcal{M} = \mathscr{L}$. Using Lemma 2.3, we have sections $s_{\Lambda_A}, s_{\Lambda_B}$ and $s_{\Lambda'}$, respectively, on Λ_A, Λ_B and Λ' which verify $s_{\Lambda'}(\hat{I} \gg') = s_{\Lambda_B}(F(\hat{I} \gg'))$. Taking the quotient modulo $s_{\Lambda'}(\Lambda_A)$, we get a canonical section $\bar{s} : K \to G(\mathscr{L})$. Since $G(\mathcal{M}) = Z(s_{\Lambda_B}(\Lambda_B))/s_{\Lambda_B}(\Lambda_B)$, we get that $G(\mathcal{M}) \simeq Z(s(K))/s(K)$.

Definition 2.14 Let $(A = V_A/\Lambda_A, \mathscr{L}, \Theta_{\mathscr{L}})$ and $(B = V_B/\Lambda_B, \mathcal{M}, \Theta_{\mathcal{M}})$ be abelian varieties together with symmetric theta structures, and let $f : A \to B$ be an isogeny with analytic representation F. We say that $\Theta_{\mathscr{L}}$ and $\Theta_{\mathcal{M}}$ are compatible (along F) if there exists symplectic decompositions σ_A and σ_B such that $F_*(\sigma_A \otimes \mathbb{R}) = \sigma_B \otimes \mathbb{R}$ and $H_{\mathscr{L}} = F^*H_{\mathcal{M}}$, $\mathscr{L} = \mathscr{L}^{\sigma_A}, \mathcal{M} = \mathcal{M}^{\sigma_B}, \Theta_{\mathscr{L}} = \Theta_{\mathscr{L}}^{\sigma_A}, \Theta_{\mathcal{M}} = \Theta_{\mathcal{M}}^{\sigma_B}$.

Using Proposition 2.11, we get the following proposition which immediately provides an algorithm to construct theta coordinates on $(B, \mathcal{M})$, provided that we have a section $u \in \Gamma(A, \mathscr{L})$ on which we know the action of $G(\mathscr{L})$:

Proposition 2.15 *Let σ be a symplectic decomposition of Λ from which we deduce a decomposition of $K(\mathscr{L}) = K_1(\mathscr{L}) \oplus K_2(\mathscr{L})$. Let K be a finite subgroup of A isotropic for the Weil pairing and compatible with σ, that is, $K = K_1 \oplus K_2$ where $K_i = K \cap K_i(\mathscr{L})$ for $i = 1, 2$. Let $f : (A, \mathscr{L}) \to (B = A/K, \mathcal{M})$ be the corresponding isogeny with analytic representation F and such that $f^*\mathcal{M} = \mathscr{L}$. Given the symmetric theta structure $\Theta_{\mathscr{L}} = \Theta_{\mathscr{L}}^{\sigma}$ on $\mathscr{L}$, there is a unique compatible symmetric theta structure $\Theta_{\mathcal{M}}$ on $\mathcal{M}$: in other words, $\Theta_{\mathcal{M}}$ only depends on $\Theta_{\mathscr{L}}$ and not on the decomposition σ used to define $\Theta_{\mathscr{L}}$.*

Let u be a non-trivial section of $\Gamma(A, \mathscr{L})$. Up to a constant, we have $F^*\theta_0^{\Theta_{\mathcal{M}}^{\sigma}} = \sum_{j \in K_1^{\perp e_{\mathscr{L}}} \oplus K_2} s(j) \cdot u$ (assuming this trace is non-zero), and for $i \in K_2^{\perp e_{\mathscr{L}}}$, $F^*\theta_{f(i)}^{\Theta_{\mathcal{M}}^{\sigma}} = s(i) \cdot \theta_0^{\Theta_{\mathcal{M}}^{\sigma}}$.

Proof From the discussion above, $\mathcal{M}$ is the quotient of $\mathscr{L}$ by the action defined by the section $\tilde{K} \subset G(\mathscr{L})$ of $K = K_1 \oplus K_2$ given by $\tilde{K} = s_1(K_1)s_2(K_2)$ (since K is isotropic, these two subgroups commute, so their product defines a lift).

Using [16, Sect. 1, Proposition 2], we have $K(\mathcal{M}) \simeq K_1^{\perp e_{\mathscr{L}}}/K_1 \oplus K_2^{\perp e_{\mathscr{L}}}/K_2$. For $i = 1, 2$, let $K_i(\mathcal{M}) = K_i^{\perp e_{\mathscr{L}}}/K_i$ and let $s_i^{\Theta_{\mathscr{L}}^{\sigma}} : K_i(\mathcal{M}) \to G(\mathscr{L})$ (resp. $s_i^{\Theta_{\mathcal{M}}^{\sigma}} : K_i(\mathcal{M}) \to G(\mathcal{M})$)

be the sections defining the theta structure $\Theta^\sigma_{\mathscr{L}}$ (resp. $\Theta^\sigma_{\mathcal{M}}$). Then we have $s_i^{\Theta^\sigma_{\mathcal{M}}}(P) = F(s_i^{\Theta^\sigma_{\mathscr{L}}}(P'))$ for $P' \in K_i^{\perp e_{\mathscr{L}}}$ such that $P = f(P')$. This shows that $\Theta^\sigma_{\mathcal{M}}$ is unique. Taking a trace of u under $\tilde{K}$, we get a section of $\mathcal{M}$ since $\Gamma(B, \mathcal{M}) = \Gamma(A, \mathscr{L})^{s(K)}$. We can then apply Proposition 2.11 to this trace to obtain the result. □

If the trace of u under $K_1^{\perp e_{\mathscr{L}}} \oplus K_2$ is zero, then since u is non-trivial and $\Gamma(A, \mathscr{L})$ is irreducible, there always exists an element in $g \in G(\mathscr{L})$ such that the trace of $g \cdot u$ will be non-zero. It is only in this case that we need the full action of $G(\mathscr{L})$. In general, we only need to be able to compute the action of $Z(s(K))$ to recover $\Theta_{\mathcal{M}}$.

Remark 2.16 As an aside of the preceding proof, if $\#K$ is odd, then by Remark 2.7, $\tilde{K}$, and hence $\mathcal{M}$, does not depend on σ.

Example 2.17 Applying Proposition 2.15 to $u = \theta_0^{\Theta_{\mathscr{L}}}$, we recover Mumford's isogeny theorem (compare with [1, Theorem 6.8.2]):

for $i \in K_2^{\perp e_{\mathscr{L}}}$, $F^*\theta^{\Theta_{\mathcal{M}}}_{f(i)} = \sum_{j \in K_2} \theta^{\Theta_{\mathscr{L}}}_{i+j}$.

Indeed, by definition $K_1(\mathscr{L})$ acts trivially on $\theta_0^{\Theta_{\mathscr{L}}}$, and if $j \in K_2(\mathscr{L})$, $j \cdot \theta_0^{\Theta_{\mathscr{L}}} = \theta_j^{\Theta_{\mathscr{L}}}$. So we have equality up to a constant C not depending on i. But by Example 2.18, in this case, this constant C is equal to 1.

Example 2.18 Given $\sigma : \Lambda = \Lambda_1 \oplus \Lambda_2$ is a symplectic decomposition of Λ, up to an automorphism of $V = \mathbb{C}^g$, we can assume that $\Lambda_2 = \mathbb{Z}^g$. Then $\Lambda_1 = \Omega\mathbb{Z}^g$ where Ω is a $g \times g$ matrix with complex coefficients called a period matrix of A. The data of a period matrix is equivalent to the data of Λ, a principal Riemann form H_0 with matrix representation $\Im(\Omega^{-1})$ on V and a symplectic decomposition of $\Lambda = \Omega\mathbb{Z}^g \oplus \mathbb{Z}^g$ for H_0. Let $H = nH_0$ and $\mathscr{L}$ be the line bundle associated to the symplectic decomposition given by Ω in the algebraic class defined by H.

Recall the definition of the analytic theta functions with the following characteristics:

$$\theta \begin{bmatrix} a \\ b \end{bmatrix}(z, \Omega) = \sum_{n \in \mathbb{Z}^g} e^{\pi i^t (n+a)\Omega(n+a) + 2\pi i^t (n+a)(z+b)}, \text{ for } a, b \in \mathbb{Q}^g.$$

We have $K_2(\mathscr{L}) = \frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g \simeq (\mathbb{Z}/n\mathbb{Z})^g$. Under this isomorphism, the classical basis of level n theta functions is given by $\theta_i(z, \Omega) = \theta \begin{bmatrix} 0 \\ i/n \end{bmatrix}(z, \Omega/n)$ (see [18, Chap. II, Proposition 1.3]). These functions are automorphic with respect to the classical factor of automorphy from Eq. 1 rather than the canonical one from Sect. 2.1. These two automorphic factors differ by a coboundary, and by using this coboundary one can translate the above theory to classical theta functions.

Mumford's isogeny theorem from Example 2.17 applied to the isogeny $A = \mathbb{C}^g/(\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g) \to B = \mathbb{C}^g/(\frac{\Omega}{\ell}\mathbb{Z}^g \oplus \mathbb{Z}^g)$ becomes the following tautological equation between classical theta functions of level ℓn on A and classical theta functions of level n on B: for $b \in \mathbb{Z}^g$:

$$\theta \begin{bmatrix} 0 \\ b/n \end{bmatrix}(z, \frac{\Omega/\ell}{n}) = \theta \begin{bmatrix} 0 \\ \ell b/\ell n \end{bmatrix}(z, \Omega/\ell n).$$

3 Affine lifts and Riemann relations

Let $(A, \mathscr{L}, \Theta_{\mathscr{L}})$ be an abelian variety together with a line bundle and a symmetric theta structure of even level n. We have seen that $\Theta_{\mathscr{L}}$ defines an embedding $\iota_{\Theta_{\mathscr{L}}} : A \to \mathbb{P}^{K_2(\mathscr{L})}$, $P \mapsto (\theta_i^{\Theta_{\mathscr{L}}}(P))_{i \in K_2(\mathscr{L})}$. In this section, we gather some useful definitions and results from [12, 14] to obtain the main ingredients of our algorithms.

Definition 3.1 We call any preimage $\tilde{P} \in \mathbb{A}^{K_2(\mathscr{L})}$ of P for the canonical projection $\mathbb{A}^{K_2(\mathscr{L})} \to \mathbb{P}^{K_2(\mathscr{L})}$ an affine lift. If $\tilde{P}$ is an affine lift of P and $i \in K_2(\mathscr{L})$, we denote by $(\tilde{P})_i$ or $\theta_i(\tilde{P})$ the i^{th} coordinate of $\tilde{P}$, so $\tilde{P} = (\theta_i(\tilde{P}))_{i\in K_2(\mathscr{L})}$.

Let $* : \mathbb{C}^* \times \mathbb{A}^{K_2(\mathscr{L})} \to \mathbb{A}^{K_2(\mathscr{L})}$ be the action $\big(\lambda, \tilde{P}\big) \mapsto \big(\lambda(\tilde{P})_i\big)_{i\in K_2(\mathscr{L})}$.

If P is a point of $A = V/\Lambda$, we denote by $z_P \in V$ any element whose equivalence class modulo Λ is P. The element z_P defines an *analytic* affine lift $\tilde{P} = (\theta_i^{\Theta_{\mathscr{L}}}(z_P))_{i\in K_2(\mathscr{L})}$ of P. The action of $\mathfrak{G}(\mathscr{L})$ on analytic functions extends to vectors of analytic functions by acting coordinate by coordinate, which induces an action of $G(\mathscr{L})$ on vectors of sections of $\mathscr{L}$, and thus an action of $G(\mathscr{L})$ on $\tilde{P}$.

We can construct the affine translation by points $z_P \in V$ on theta functions explicitly via the use of Riemann relations. In this section, in order to ease the notations, we omit the theta structure symbol when we name theta functions: for $i \in K_2(\mathscr{L})$, $\theta_i = \theta_i^{\Theta_{\mathscr{L}}}$.

Definition 3.2 If $\mathcal{V}$ is a commutative group, we say that the elements $v_1, v_2, v_3, v_4; w_1, w_2, w_3, w_4$ are in Riemann position whenever there exists $u \in \mathcal{V}$ such that $w_i = v_i + u$ and $v_1 + v_2 + v_3 + v_4 = -2u$.

Theorem 3.3 (Riemann's relations) *Let $z_1, z_2, z_3, z_4; z_1', z_2', z_3', z_4' \in V$ and $i_1, i_2, i_3, i_4; i_1', i_2', i_3', i_4' \in K_2(\mathscr{L})$ be in Riemann position. Let $T = K_2(\mathscr{L})[2] \simeq (\mathbb{Z}/2\mathbb{Z})^g$. Then for any character χ on T, we have*

$$\left(\sum_{t\in T} \chi(t)\theta_{i_1+t}(z_1)\theta_{i_2+t}(z_2)\right)\left(\sum_{t\in T} \chi(t)\theta_{i_3+t}(z_3)\theta_{i_4+t}(z_4)\right)$$
$$= \left(\sum_{t\in T} \chi(t)\theta_{i_1'+t}(z_1')\theta_{i_2'+t}(z_2')\right)\left(\sum_{t\in T} \chi(t)\theta_{i_3'+t}(z_3')\theta_{i_4'+t}(z_4')\right).$$

We can use Riemann's relations as follows. Let $z_i, z_i' \in V$ for $i = 1, \ldots, 4$ be in Riemann position. Assume that we know the affine points $\tilde{P}_i = (\theta_j(z_i))_{j\in K_2(\mathscr{L})}$ for $i = 2, 3, 4$, and $\tilde{P}_i' = (\theta_j(z_i'))_{j\in K_2(\mathscr{L})}$ for $i = 1, \ldots, 4$. We can recover $\tilde{P}_1 = (\theta_j(z_1))_{j\in K_2(\mathscr{L})}$, i.e. the affine theta coordinates of z_1, by first computing the projective theta coordinates of P_1 using the addition on A, taking an arbitrary affine lift $\tilde{P}_1$ and computing the projective factor λ_1 such that $\lambda_1 * \tilde{P}_1, \tilde{P}_2, \ldots$ satisfy Riemann's relations (so we only need to use one such relation).

Of course, in practice, the arithmetic on A itself is usually derived from Riemann's relations. We just present a few examples, and we refer to [15] for more details. In particular, when $n = 2$, we need to assume that the even theta null points are non-zero, which means by a result of Koizumi–Mumford–Kempf that the line bundle $\mathscr{L}$ is projectively normal.

Example 3.4 Let r be an integer. Given the affine theta coordinates of $0, z_1, z_2, \ldots, z_r \in V$ $\widetilde{0}_A = (\theta_u(0))_{u\in K_2(\mathscr{L})}$, $\tilde{P}_i = (\theta_u(z_i))_{u\in K_2(\mathscr{L})}$ and also of each $z_i + z_j$, $i \neq j$, $\tilde{P}_{ij} = (\theta_u(z_i + z_j))_{u\in K_2(\mathscr{L})}$, we can recover the affine theta coordinates of $m_1z_1 + m_2z_2 + \cdots + m_rz_r$ using Riemann relations. We denote the resulting affine lift by mult_add$(m_1, \ldots, m_r, \tilde{P}_i, \tilde{P}_{ij}, \widetilde{0}_A)$.

As a particular case, we can compute the affine theta coordinates of $\ell z_1 + z_2$ given the affine theta coordinates of 0, z_1, z_2 and $z_1 - z_2$ (via an easy change of variable), and so of ℓz_1 given the affine theta coordinates of 0 and z_1. We denote these by diff_mult$(\ell, \tilde{P}_1, \tilde{P}_2, P_1 \tilde{-} P_2, \widetilde{0}_A)$ and mult$(\ell, \tilde{P}_1, \widetilde{0}_A)$, respectively. These can be computed in $O(\log \ell)$ field operations using a double and add algorithm.

Another particular case is the computation of the affine theta coordinates of $z_1 + z_2 + z_3$ given that $z_1, z_2, z_3, z_1 + z_2, z_1 + z_3, z_2 + z_3$. With the notations above, we call this threeway_add($\tilde{P}_1, \tilde{P}_2, \tilde{P}_3, \tilde{P}_{23}, \tilde{P}_{13}, \tilde{P}_{12}, \widetilde{0}_A$). Then, conversely, mult_add can be constructed from threeway_add and diff_mult.

Finally, recall that $\theta_i(z_P) = \theta_{-i}(z_P)$, so we define $(-\tilde{P})_i = \tilde{P}_{-i}$.

We want to compute the action of suitable affine lifts given by $z_P \in V$ of the points of ℓ torsion $P \in A[\ell]$. Let $\sigma : \Lambda = \Lambda_1 \oplus \Lambda_2$ be a symplectic decomposition. Then the lattice $\Lambda'' = \ell\Lambda_1 \oplus \frac{1}{\ell}\Lambda_2$ is isotropic for $E_{\mathscr{L}}$; hence, by Lemma 2.3, we get a group section $s_{\Lambda''} : \Lambda'' \to \mathfrak{G}(\mathscr{L})$. We will compute the action of elements of $s_{\Lambda''}(\Lambda''_2)$ on the theta basis of level n, $(\theta_i^{\Theta^\sigma_{\mathscr{L}}})_{i\in K_2(\mathscr{L})}$. Since the $\theta_i^{\Theta^\sigma_{\mathscr{L}}}$ are invariants by $s_{\Lambda''}(\Lambda)$, the action of $\lambda'' \in \Lambda''_2$ only depends on its class modulo Λ_2, so only depends on the ℓ torsion point $P \in \Lambda''_2/\Lambda_2 \simeq K_2(\mathscr{L}^\ell)[\ell]$. In the following, we denote this action by $\bar{s}_{\Lambda''} : K_2(\mathscr{L}^\ell)[\ell] \to Aut(\Gamma(A, \mathscr{L}))$. A similar method will apply for the action of (the lifts of) the points in $K_1(\mathscr{L}^\ell)[\ell]$, for instance, using Example 2.13.

By Equation 2, the action by $\bar{s}_{\Lambda''}(P)$ for $P \in K_2(\mathscr{L}^\ell)[\ell]$ is given by the translation by ℓ torsion points, corrected by some scalar factor, and hence it is natural to use Riemann relations to compute it. In fact, Riemann relations are compatible with these corrective factors:

Lemma 3.5 *Assume that $z_1, z_2, z_3, z_4; z'_1, z'_2, z'_3, z'_4$ in V are in Riemann position, and moreover that $P_1, P_2, P_3, P_4; P'_1, P'_2, P'_3, P'_4$ in $K_2(\mathscr{L}^\ell)[\ell]$ are in Riemann position. Then the points $\bar{s}_{\Lambda''}(P_i) \cdot \theta_j^{\Theta^\sigma_{\mathscr{L}}}(z_i)$ satisfy Riemann's relations.*

Proof If $z_1, z_2, z_3, z_4; z'_1, z'_2, z'_3, z'_4$ are in Riemann position, and $g_1 = [a_1, \nu_1], g_2 = [a_2, \nu_2]$, …in $\mathfrak{G}(\mathscr{L})$ too (by which we mean the ν_i are in Riemann position and $\Pi a_i = \Pi a'_i$), then since the $(\theta_j^{\Theta^\sigma_{\mathscr{L}}}(z_i))_{j\in K_2(\mathscr{L})}$ satisfy Riemann relations by Theorem 3.3, we check by an easy (but a bit lengthy) computation that the $(g_i \cdot \theta_j^{\Theta^\sigma_{\mathscr{L}}}(z_i))_{j\in K_2(\mathscr{L})}$ also satisfy Riemann relations. We apply this to $g_i = s_{\Lambda''}(z_{P_i})$, $g'_i = s_{\Lambda''}(z_{P'_i})$, where $z_{P_i}, z_{P'_i} \in V$ are such that $z_{P_i} = P_i \mod \Lambda_2$ and $z_{P'_i} = P'_i \mod \Lambda_2$. □

This leads us to the following definition:

Definition 3.6 If K is a subgroup of $K(\mathscr{L}^\ell)$ isotropic for the Weil pairing, we say that $\tilde{K} = \{\tilde{P}\}_{P\in K}$ is an excellent lift of K if the points in $\tilde{K}$ satisfy all Riemann relations from Theorem 3.3 that involve only points in $\tilde{K}$.

We specify what this definition means for a point and its multiples computed by the help of Riemann equations.

Definition 3.7 Let P be a point of ℓ torsion with ℓ odd and prime to n. Write $\ell = 2\ell' + 1$. We say that an affine lift $\tilde{P}$ is an excellent point of ℓ torsion if $\text{mult}(\ell' + 1, \tilde{P}, \widetilde{0}_A) = -\text{mult}(\ell', \tilde{P}, \widetilde{0}_A)$.

It is easy to check that if $\tilde{P}$ is an excellent point of ℓ torsion, then $\mu * \tilde{P}$ is also if and only if $\mu^\ell = 1$. It is clear moreover, since mult is computed with Riemann equations, that if $\tilde{K}$ is an excellent lift of K, all $\tilde{P} \in \tilde{K}$ are excellent points of ℓ torsion. Furthermore, given $\tilde{K}$, if $P_1, \ldots, P_g$ is a basis of K, we only need to be given $\tilde{P}_i$ and $\tilde{P}_{ij}$, the lifts above P_i and $P_i + P_j$, respectively, to recover the others via mult_add.

In fact, this subset of the Riemann relations involving points of K is enough to construct an excellent lift of K, and even recover the section of K in $G(\mathscr{L})$ provided by $\bar{s}_{\Lambda''}$. Before stating the theorem, we give a word of warning: the section $s_{\Lambda''}$ does not extend to the whole of Λ; for instance, changing λ'' by an element of Λ_1 (modulo $\ell\Lambda_1$) will change $s_{\Lambda''}(\lambda'')$. In particular, changing the symplectic decomposition σ of Λ will change this $s_{\Lambda''}$, even if it does not change the induced symplectic decomposition on $A[\ell]$. This will be exploited in the following theorem where in order to keep track of the dependence of the sections $s_{\Lambda''}$ and the induced action $\bar{s}_{\Lambda''}$ with respect to the symplectic decomposition σ, we will denote them respectively by $s_{\Lambda'',\sigma}$ and $\bar{s}_{\Lambda'',\sigma}$.

Theorem 3.8 *Let $(A, \mathscr{L}, \Theta^{\sigma}_{\mathscr{L}})$ be an abelian variety together with a symmetric theta structure of level even defined by a symplectic decomposition σ. Let $K = K_2(\mathscr{L}^{\ell})[\ell]$ and let $P_1, \dots, P_g$ be a basis of K. Fix once and for all an affine lift $\widetilde{0}_A$ of 0_A. Choose $\tilde{P}_i$ and $\tilde{P}_{ij}$ as excellent lifts of P_i and $P_i + P_j$ (for $i \neq j$), respectively. We can then use* mult_add *to compute an affine lift $\tilde{P}$ above any point P in K. Then $\tilde{K} = \{\tilde{P}\}_{P\in K}$ is an excellent lift of K. Furthermore, up to changing the symplectic decomposition σ of Λ (more precisely, up to changing Λ_2 only), for all $P \in K$ and $\tilde{P}$ is exactly $\bar{s}_{\Lambda'',\sigma}(P).\widetilde{0}_A$.*

Proof A slightly less refined version is proved in [14, Theorem 3.4.] using the functional equation of theta functions. Using the theory from Sect. 2, we can give a self-contained proof.

First, given an excellent lift $\tilde{K}$, then multiplying every element of $\tilde{K}$ by a projective factor μ_0 still yields an excellent lift, so we may renormalise things such that $\widetilde{0}_A = (\theta_i^{\Theta^{\sigma}_{\mathscr{L}}}(0))_{i\in K_2(\mathscr{L})}$. Of course, $\tilde{K} = \{\bar{s}_{\Lambda'',\sigma}(P).\widetilde{0}_A\}_{P\in K}$ is an excellent lift of K by Lemma 3.5 applied to the elements $0, 0, 0, 0; 0, 0, 0, 0 \in V$ in Riemann position.

Conversely, we construct $\tilde{K}$ as in the theorem and for all $P \in K$ and σ a decomposition of Λ we let $\tilde{P}^{\sigma} = \bar{s}_{\Lambda'',\sigma}(P)$. Then we have $\tilde{P} = \mu_P * \tilde{P}^{\sigma}$, for μ_P an ℓth root of unity. It is enough to prove that we can always change the symplectic decomposition σ of Λ to σ' so that $\tilde{P}_i^{\sigma} = \mu_i * \tilde{P}_i^{\sigma'}$ and $\tilde{P}_{ij}^{\sigma} = \mu_{ij} * \tilde{P}_{ij}^{\sigma'}$ where μ_i and μ_{ij} are arbitrary ℓth roots of unity. We can then choose μ_i, μ_{ij} such that, after this change of decomposition, we have $\tilde{P}_i = \tilde{P}_i^{\sigma'}$, $\tilde{P}_{ij} = \tilde{P}_{ij}^{\sigma'}$, and hence $\tilde{P} = \tilde{P}^{\sigma'}$ for all $P \in K$.

First, note that by Remark 2.1, as the level of $\Theta_{\mathscr{L}}$ is even, changing the symplectic decomposition does not change the line bundle $\mathscr{L}$ associated to this decomposition. Now, given $(e_1, \dots, e_g, f_1, \dots, f_g)$ a symplectic basis of Λ with respect to σ, and fixing $i \in \{1, \dots, g\}$, we change the decomposition such that the new basis is given by $f_i' = f_i + 2k_i n\ell e_i$ (the other ones unchanged) for $k_i \in \{0, \dots, \ell - 1\}$. We let σ' be the new symplectic decomposition. The new symplectic basis still gives the same symplectic decomposition of $A[2n]$, and hence we have $\theta_i^{\Theta^{\sigma}_{\mathscr{L}}} = \theta_i^{\Theta^{\sigma'}_{\mathscr{L}}}$ for all $i \in K_2(\mathscr{L})$ by Remark 2.7. Using the definition of the sections $s_{\Lambda'',\sigma}$ and $s_{\Lambda'',\sigma'}$ of Lemma 2.3, we compute $s_{\Lambda'',\sigma'}(\frac{f_i'}{\ell}) = e^{-2\Pi i E_{\mathscr{L}}(\frac{f_i}{\ell}, k_i n e_i)} s_{\Lambda'',\sigma}(\frac{f_i}{\ell}) s_{\Lambda'',\sigma}(2k_i n e_i)$. Since n is prime to ℓ, and $s_{\Lambda'',\sigma}(2k_i n e_i)$ acts trivially on $\widetilde{0}_A$, we have $s_{\Lambda'',\sigma'}(\frac{f_i'}{\ell}) \cdot \widetilde{0}_A = \zeta^{k_i} * s_{\Lambda'',\sigma}(\frac{f_i}{\ell}) \cdot \widetilde{0}_A$ for $\zeta = e^{2\pi i z/\ell}$ a primary ℓth root of unity. In other words, by choosing $k_i \neq 0$ and $k_j = 0$ for $j \neq i$, we can adjust $\tilde{P}_i^{\sigma'}$ without touching the others (except the $\tilde{P}_{ij}^{\sigma'}$, $j \neq i$). Likewise, fixing $i \neq j$, taking a new decomposition such that $f_i' = f_i + 2k_{ij} n\ell e_j, f_j' = f_j + 2k_{ij} n\ell e_i$ will change only $\tilde{P}_{ij}^{\sigma'}$ by $\zeta^{2k_{ij}}$; hence we may change it by an arbitrary ℓth root of unity without affecting any others. □

Remark 3.9 We give an algebraic interpretation of our choice of affine lifts, which will be useful for Sect. 4.1. Let $\Lambda' = \ell\Lambda_1 \oplus \Lambda_2$; this lattice defines an abelian variety $A' = V/\Lambda'$, and the projection modulo $\Lambda \supset \Lambda'$ gives an isogeny $f : A' \to A$. The contragredient isogeny $\tilde{f} : A \to A'$ is given analytically by $z \mapsto \ell z$; its kernel is $K = K_2(\mathscr{L}^\ell)[\ell] \simeq \frac{1}{\ell}\Lambda_2/\Lambda$. We have $(\Lambda')^\perp = \Lambda_1 \oplus \frac{1}{\ell}\Lambda_2$; so if $\mathscr{L}' = f^*\mathscr{L}$, our lattice $\Lambda'' = \ell\Lambda_1 \oplus \frac{1}{\ell}\Lambda_2$ is exactly equal to $\Lambda'_1 \oplus \Lambda'(\mathscr{L}')_2$.

Now, $\frac{1}{\ell}\Lambda_2/\Lambda_2 \simeq K_2(\mathscr{L}')$ can be interpreted as a symplectic complement to the kernel $K' \simeq \Lambda_1/\ell\Lambda_1 = \tilde{f}(A[\ell]) \subset A'[\ell]$ of f. In other words, $\frac{1}{\ell}\Lambda_2$ modulo Λ determines the kernel of $\tilde{f}$, but for our action, we need to look at modulo Λ' where it further determines a symplectic complement of $\mathscr{L}f$.

If K is an isotropic subgroup of $A[\ell]$ and we fix an excellent lift $\tilde{K}$ of K, we may extend the definition by saying that $x \tilde{+} K = \{x \widetilde{+} P \mid P \in K\}$ is an excellent lift of x with respect to $\tilde{K}$ and $\tilde{x}$ if these points respect all Riemann relations involving only points of $\tilde{K}$ and of $x \tilde{+} K$.

Definition 3.10 With the notations of Definition 3.7, let $\tilde{P}$ be an excellent lift of an ℓ torsion point $P \in A[\ell]$. Let $x \in A$ and fix an affine lift $\tilde{x}$. We say that $x \widetilde{+} P$ is an excellent lift with respect to $\tilde{P}$ and $\tilde{x}$ if the affine point $x \tilde{+} \ell P$ computed via diff_multadd is equal to $\tilde{x}$.

If $x \widetilde{+} P$ is an excellent lift of $x + P$, then the other ones are given by $\mu * x \widetilde{+} P$ with $\mu^\ell = 1$. By the following Theorem, we may construct an excellent lift $x \tilde{+} K$ of x with respect to $\tilde{K}$ by first constructing excellent lifts $x \tilde{+} P_i$ for P_i a basis of K, and then obtaining all other points by multiway additions.

Theorem 3.11 *With the notations of Theorem 3.8, fix an excellent lift $\tilde{K}$ of K. Let x be a point in A which is not in $A[\ell]$, and $z \in V$ be such that $x = z \mod \Lambda$. Fix an affine lift $\tilde{x}$ of x, fix excellent lifts $x \tilde{+} P_i$ for $(P_i)_{i=1,\dots,g}$ a basis of K, and compute the other affine lifts $x \widetilde{+} P$ for $P \in K$ via* mult_add.

Then we may always change z by another representative modulo Λ (more precisely, by an element $z + \lambda$ with $\lambda \in \Lambda_1$), such that there exists a constant μ that satisfies $x \widetilde{+} P = \mu * (P \cdot (\theta_i^{\Theta^\sigma_{\mathscr{L}}}(z))_{i \in K_2(\mathscr{L})})$ for all $P \in K$. In other words, we recover (up to the constant μ that only depends on the choice of $\tilde{x}$) exactly the action of K on $(\theta_i^{\Theta^\sigma_{\mathscr{L}}}(z))$.

Proof First, if $\tilde{x} = (\theta_i^{\Theta^\sigma_{\mathscr{L}}}(z))_{i \in K_2(\mathscr{L})}$ and $x \widetilde{+} P = P \cdot \tilde{x}$ for $P \in K$, then the points $x \widetilde{+} P$ form an excellent lift of x with respect to $\tilde{x}$ and $\tilde{K}$ by Lemma 3.5 applied to the elements $z, z, 0, 0; 0, 0, z, z \in V$ in Riemann position.

As in the proof of Theorem 3.8, in general, we have for $i = 1, \dots, g$, $x \tilde{+} P_i = \mu_i * (P_i \cdot \theta_j^{\Theta^\sigma_{\mathscr{L}}}(z))_{j \in K_2(\mathscr{L})}$ for μ_i an ℓth root of unity. So it is enough to show that we can find $\lambda \in \Lambda$ such that for all $i = 1, \dots, g$, $(P_i \cdot \theta_j^{\Theta^\sigma_{\mathscr{L}}}(z))_{j \in K_2(\mathscr{L})} = \mu\mu_i^{-1} * (P_i \cdot \theta_j^{\Theta^\sigma_{\mathscr{L}}}(z+\lambda))_{j \in K_2(\mathscr{L})}$ where μ is a constant independent of i.

For this, denote the canonical projection by $\pi : V \to A$.

The pairing $e_{\mathscr{L}}$ being perfect, we know that for $i = 1, \dots, g$, there exists $\lambda_i \in \Lambda_1$ such that $e_{\mathscr{L}}(\pi(\lambda_i), P_i) = \mu_i^{-1}$, and $e_{\mathscr{L}}(\pi(\lambda_i), P_j) = 1$ for $j \neq i$. Set $\lambda = \sum_{i=1}^g \lambda_i$ and $z' = z + \lambda$. It is clear that $z' = x \mod \Lambda$. Moreover, using Equation (3), we compute for $i = 1, \dots, g$ and $j \in K_2(\mathscr{L})$:

$$\bar{s}_{\Lambda''}(\pi(-\lambda))\left(\bar{s}_{\Lambda''}(P_i)\cdot\theta_j^{\Theta^\sigma_{\mathscr{L}}}\right)(z) = a_{\mathscr{L}}(z+\lambda,\lambda)\left(\bar{s}_{\Lambda''}(P_i)\cdot\theta_j^{\Theta^\sigma_{\mathscr{L}}}\right)(z'). \tag{5}$$

Since we have $\bar{s}_{\Lambda''}(\pi(-\lambda))\bar{s}_{\Lambda''}(P_i) = e_{\mathscr{L}}(\pi(-\lambda),P_i)\bar{s}_{\Lambda''}(P_i)s_{\Lambda''}(\pi(-\lambda)) = \mu_i s_{\Lambda''}(P_i)$ $\bar{s}_{\Lambda''}(\pi(-\lambda))$, and since $\theta_j^{\Theta^\sigma_{\mathscr{L}}}(z)$ is invariant under $\bar{s}_{\Lambda''}(\pi(-\lambda))$, we also have

$$\bar{s}_{\Lambda''}(\pi(-\lambda))\left(s_{\Lambda''}(P_i)\cdot\theta_j^{\Theta^\sigma_{\mathscr{L}}}\right)(z) = \mu_i(\bar{s}_{\Lambda''}(P_i)\cdot\theta_j^{\Theta^\sigma_{\mathscr{L}}}(z)). \tag{6}$$

From (5) and (6), we get for all $i = 1,\dots,g$:

$$a_{\mathscr{L}}(z+\lambda,\lambda)\mu_i^{-1} * (P_i\cdot\theta_j^{\Theta^\sigma_{\mathscr{L}}}(z'))_{j\in K_2(\mathscr{L})} = (P_i\cdot\theta_j^{\Theta^\sigma_{\mathscr{L}}}(z))_{j\in K_2(\mathscr{L})}. \tag{7}$$

Using (5) with $P_i = 0$, we also have $a_{\mathscr{L}}(z+\lambda,\lambda) * (\theta_j^{\Theta^\sigma_{\mathscr{L}}}(z'))_{j\in K_2(\mathscr{L})} = (\theta_j^{\Theta^\sigma_{\mathscr{L}}}(z))_{j\in K_2(\mathscr{L})}$. On the other hand, multiplying $\tilde{x}$ by a factor μ changes $x\widetilde{+}P$ by the same factor μ too. So if we renormalise $\tilde{x}$ such that it corresponds exactly to $(\theta_j^{\Theta^\sigma_{\mathscr{L}}}(z'))_{j\in K_2(\mathscr{L})}$, then our updated $x\tilde{+}P_i$ are exactly equal to $(\bar{s}_{\Lambda''}(P_i)\cdot\theta_j^{\Theta^\sigma_{\mathscr{L}}}(z'))_{j\in K_2(\mathscr{L})}$, with no constants involved. □

Remark 3.12 If the field of definition is not algebraically closed, and if P is a point of ℓ torsion, taking an excellent lift $\tilde{P}$ of P involves computing a ℓth root μ_P, which may live in an extension of our base field. In practice, we never need μ_P: all our algorithms will be independent of the choices made to compute excellent lifts, and hence will only involve the value μ_P^ℓ, which is rational. The same holds to compute an excellent lift $x\widetilde{+}P$.

Algorithm 1: Algorithm to compute an excellent lift of a point.

input :

- The theta null point $\widetilde{0}_A$ of $(A,\mathscr{L},\Theta_{\mathscr{L}})$ an abelian variety with a symmetric level n theta structure;
- A point P in K and a lift $\tilde{x}$ of a point x in A

output: Excellent lifts $\tilde{P}$ of P and $x\widetilde{+}P$ of $x+P$ with respect to $\tilde{P}$

1 Fix $\tilde{P}_1$ and $x\widetilde{+}P_1$ arbitrary lifts of P and $x+P$;
2 Write $\ell = 2\ell'+1$ and determine λ such that $\mathrm{mult}(\ell'+1,\lambda*\tilde{P}_1,\widetilde{0}_A) = -\mathrm{mult}(\ell',\lambda*\tilde{P}_1,\widetilde{0}_A)$;
3 Set $\tilde{P} = \lambda*\tilde{P}_1$;
4 Determine μ such that $\mathrm{diff\_mult}(\ell,\mu*x\widetilde{+}P_1,\tilde{P},\tilde{x},\widetilde{0}_A) = \tilde{x}$;
5 Set $x\widetilde{+}P = \mu*x\widetilde{+}P_1$;
6 **return** $\tilde{P}, x\widetilde{+}P$;

Algorithm 2: Algorithm to compute an excellent lift of the kernel

input :

- The theta null point $\widetilde{0}_A$ of $(A,\mathscr{L},\Theta_{\mathscr{L}})$ an abelian variety with a symmetric level n theta structure;
- A kernel K and a lift $\tilde{x}$ of a point x in A.

output: Excellent lifts $\tilde{K}$ of K and $x\tilde{+}K$ of $x+K$ with respect to $\tilde{K}$

1 Fix a basis $(P_1,\dots,P_g)$ of K ;
2 Compute excellent lifts $\tilde{P}_i, P_i\tilde{+}P_j, x\tilde{+}P_i$ for $i\neq j\in\{1,\dots,g\}$ using Algorithm 1 ;
3 Use mult_add to compute the other lifts $\tilde{K}$ and $x\tilde{+}K$;

4 Ascending level

In this section, our goal is twofold:

1. compute the theta functions of level $n\ell$, i.e. the theta functions of $G(\mathscr{L}^\ell)$;
2. compute the theta functions of level n on $B = A/K$ where K is totally isotropic.

Of course, if we know how to do (1), we can apply Mumford's isogeny theorem to get (2).

From Propositions 2.11 and 2.15, we see that we need to

1. Construct a section u of $\mathscr{L}^\ell$;
2. Make explicit the action of $G(\mathscr{L}^\ell)$ on this u.

Since we will construct u from theta functions of level n, where the action of $G(\mathscr{L})$ is explicit, we only need to understand the action of (the sections) of $K_1(\mathscr{L}^\ell)[\ell]$ and $K_2(\mathscr{L}^\ell)[\ell]$. These are given by (symmetric) elements of order ℓ in $G(\mathscr{L}^\ell)$. If $g \in G(\mathscr{L}^\ell)$ is such an element and is represented by $[\alpha, z_P] \in \mathfrak{G}(\mathscr{L}^\ell)$, the action on u from Equation 2 shows that we need to be able to compute the translation $u(z - z_P)$. Here, z_P will be an affine point of ℓ torsion, i.e. a point in V such that $P = z_P \mod \Lambda$ is a point of ℓ torsion. The multiplicative factor $\alpha e^{\pi \ell H(z-z_P, z_P)}$ can be seen as a corrective factor such that $[\alpha, z_P]$ is of order ℓ in $G(\mathscr{L}^\ell)$. In fact, if we use the classical factor of automorphy instead, this action is exactly the action by translation whenever $z_P \in \frac{1}{\ell}\mathbb{Z}^g$.

4.1 Ascending level along an isogeny

As a warm-up, given an isogeny $f : A' = V/\Lambda' \to A = V/\Lambda$ such that its kernel K' is a maximal isotropic subgroup of $A'[\ell]$, we explain how to compute theta coordinates on A' from the knowledge of theta coordinates on A. This was already explained in [13], but Proposition 2.11 allows us to give a shorter proof.

We suppose that A is endowed with a polarisation given by a Riemann form H_A of type n, and we choose a symplectic decomposition $\sigma : V = V_1 \oplus V_2$ with respect to H_A such that Λ is compatible with σ following Definition 2.2. We have seen in Sect. 2.1 that σ defines a canonical line bundle $\mathscr{L}$ on A and a symmetric theta structure $\Theta^\sigma_{\mathscr{L}}$ by Proposition 2.5. Let F be the analytic representation of f; then $\sigma' : V = F^{-1}(V_1) \oplus F^{-1}(V_2)$ is a symplectic decomposition of V for $F^*(H_A)$, and Λ' is compatible with σ'. Thus, the decomposition σ' defines a line bundle $\mathscr{L}'$ on A' such that $\mathscr{L}' = f^*(\mathscr{L})$ and a symmetric theta structure $\Theta^{\sigma'}_{\mathscr{L}'}$.

In order to compute the canonical basis defined by $\Theta^{\sigma'}_{\mathscr{L}'}$, we need to obtain a section of $\mathscr{L}'$ and to explain how $G(\mathscr{L}')$ acts on it. We consider u a section of $\mathscr{L}$, and $u' = f^*u = u \circ f$. By the compatibility of the action (see Equation (4)), if $g' = [\alpha', w'] \in G(\mathscr{L}')$ is such that $f(w') \in K(\mathscr{L})$, then the action of g' on u' is given by the action of $F(g')$ on u. For instance, if $u = \theta_0 \in \Gamma(A, \mathscr{L})$, then for $i \in A'_1[n]$ acts trivially on $i \cdot u' = u'$, while the action of $i \in A'_2[n]$ is given by $i \cdot u' = F^*\theta_{f(i)}$.

It remains to explain how $A'[\ell]$ acts on u'. Take a decomposition $A'[\ell] = A'_1[\ell] \oplus A'_2[\ell]$ with $K' = \mathscr{L}f = A'_1[\ell]$, then $A'_1[\ell]$ acts trivially on u' since $u' = f^*(u)$. Thus, we only need to compute the action of $P \in A'_2[\ell]$. Changing if necessary the symplectic decomposition σ of Λ, we may assume that $\Lambda' = \ell\Lambda_1 \oplus \Lambda_2$, $F = \mathrm{Id}$. Then this action is exactly the action of the points in $\frac{1}{\ell}\Lambda_2/\Lambda_2$ that we computed in Sect. 3 (see Remark 3.9).

Note that we may always change the symplectic decomposition of Λ and Λ' in order to make them compatible, without changing the theta structure of level n on A (resp. ℓn on A') if the following algebraic conditions are satisfied (see Remark 2.7): let $A'[2\ell n] = A'_1[2\ell n] \oplus A'_2[2\ell n]$ be the symplectic decomposition inducing the theta structure of level ℓn on A'. Then we require that $\mathscr{L}f = 2nA'_1[2\ell n]$, and that the decomposition $A[2n] = f(A'_1[2\ell n]) \oplus f(\ell A'_2[2\ell n])$ induces the theta structure of level n on A.

When ℓ is prime to n, this amounts simply to saying that the decomposition of $A'[2n]$ is sent to the decomposition of $A[2n]$ via f. In particular, $A'_i[n]$ is fixed and $A'_1[\ell] = K' = \mathscr{L}f$ is fixed, so the only choice left is on the symplectic complement $A'_2[\ell]$ of K'.

From the proofs of Theorems 3.8 and 3.11 and Remark 3.9, we immediately get

Theorem 4.1 *Let $(A, \mathscr{L}, \Theta_{\mathscr{L}})$ be an abelian variety together with a level n symmetric theta structure. Let K be a maximal isotropic kernel of $A[\ell]$, ℓ prime to n, let $A' = A/K$, and let $f : A' \to A$ be the contragredient isogeny. Let $\mathscr{L}' = f^*\mathscr{L}$. Let $x \in A$ and fix a lift $\tilde{x}$. Fix an excellent lift $\tilde{K}$ of K, and $x \tilde{+} K$ of x, as in Theorems 3.8 and 3.11. Then*

1. *There exists a symmetric theta structure $\Theta_{\mathscr{L}'}$ on $(A', \mathscr{L}')$ such that, up to a constant, for $i \in K_2(\mathscr{L}')$, if $i = i_1 + i_2$ with $i_1 \in K_2(\mathscr{L}')[n]$ and $i_2 \in K_2(\mathscr{L}')[\ell]$, $\theta_i^{\Theta_{\mathscr{L}'}}(0) = \theta_{f(i)}^{\Theta_{\mathscr{L}}}(f(\tilde{i}_2))$. Furthermore, all $\ell^{g(g+1)/2}$ theta constants given by such (compatible) theta structures arise from a choice of an excellent lift of K.*
2. *If x' is the point such that, up to a constant depending only on x, $\theta_{i_1+i_2}^{\Theta_{\mathscr{L}'}}(x') = \theta_{i_1}^{\Theta_{\mathscr{L}}}(x + \tilde{f}(i_2))$, then x' is a preimage of x by f, and all ℓ^g preimages of x arise from a different choice of excellent lift $x \tilde{+} K$.*

Remark 4.2 Note that since the constant in Example 2.17 is 1, we can determine the implicit constants in the above theorem explicitly. Namely, if the chosen affine lift $\widetilde{0}_{A_k}$ corresponds to the affine theta null point $\theta_i^{\mathscr{L}}(0)$ up to a projective factor α, that is, $\widetilde{0}_{A_k} = \alpha \cdot \theta_i^{\mathscr{L}}(0)$, then in Theorem 4.1, we get $\theta_{f(i)}^{\Theta_{\mathscr{L}}}(f(\tilde{i}_2)) = \alpha\theta_i^{\Theta_{\mathscr{L}'}}(0)$. Likewise, if the choice of affine lift $\tilde{x}$ satisfies $\tilde{x} = \mu \cdot \theta_i^{\mathscr{L}}(z)$ for a representative z of $x = z \mod \Lambda$, then if $z' = F^{-1}(z)$, $\theta_{i_1+i_2}^{\Theta_{\mathscr{L}'}}(z') = \alpha\mu\theta_{i_1}^{\Theta_{\mathscr{L}}}(x + \tilde{f}(i_2))$.

4.2 Ascending level on the same variety

We assume we are given an abelian variety $(A = V/\Lambda, \mathscr{L}, \Theta_{\mathscr{L}})$ with a symmetric theta structure of even level n defined by a symplectic decomposition $\sigma : \Lambda = \Lambda \oplus \Lambda_2$. We want to construct the symmetric theta structure of level ℓn on $(A, \mathscr{L}^\ell)$ provided by σ following Proposition 2.5. For simplicity we assume that ℓ is prime to n. We will apply the tools of Sect. 2.

Let $a_i \in \mathbb{N}$ for $i = 1, \ldots, r$ be such that $\ell = \sum_{i=1}^r a_i^2$. Let $u_i \in \Gamma(A, \mathscr{L})$ for $i = 1, \ldots, r$; then, as $\mathscr{L}$ is symmetric, $u_i \circ [a_i]$ (where $[a_i] : A \to A$ is the isogeny defined on points by $P \mapsto a_i P$) is a section of $\mathscr{L}^{a_i^2}$, and hence $u = \prod u_i$ is a section of $\mathscr{L}^{\sum a_i^2} = \mathscr{L}^\ell$. We want to make explicit the action of $G(\mathscr{L}^\ell)$ on u; we can then apply Proposition 2.11 to recover the theta basis of level ℓn on $\mathscr{L}^\ell$. There is a morphism $E_\ell : \mathfrak{G}(\mathscr{L}) \to \mathfrak{G}(\mathscr{L}^\ell)$, $[\hat{I}\pm, w] \mapsto [\hat{I}\pm^\ell, w]$. As Λ is isotropic for $E_{\mathscr{L}}$ and $E_{\mathscr{L}^\ell}$ and is compatible with σ, Lemma 2.3 gives sections $s_{\Lambda,\mathscr{L}} : \Lambda \to \mathfrak{G}(\mathscr{L})$ and $s_{\Lambda,\mathscr{L}^\ell} : \Lambda \to \mathfrak{G}(\mathscr{L}^\ell)$. One can verify that E_ℓ is compatible with $s_{\Lambda,\mathscr{L}}$ and $s_{\Lambda,\mathscr{L}^\ell}$ in the following way: $E_\ell(s_{\Lambda,\mathscr{L}}(\lambda)) = s_{\Lambda,\mathscr{L}^\ell}(\lambda)$ for all $\lambda \in \Lambda$.

We check that the action of $\mathfrak{G}(\mathscr{L}^\ell)$ is compatible with products of sections, and combining with the compatibility of the action with isogenies (see Sect. 2.4), we get

Lemma 4.3 *Let $\Lambda' = \frac{1}{\ell}\Lambda_1 \oplus \Lambda_2$, or $\Lambda' = \Lambda_1 \oplus \frac{1}{\ell}\Lambda_2$.*

For $m \in \mathbb{N}^*$, we denote by $s_{\Lambda',\mathscr{L}^m} : \Lambda' \to \mathfrak{G}(\mathscr{L}^m)$ the set section defined by $s_{\Lambda',\mathscr{L}^m}(\lambda) = [a_{\mathscr{L}^m}(0,\lambda),\lambda]$. For $\lambda \in \Lambda'$, we have

$$s_{\Lambda',\mathscr{L}^\ell}(\lambda)\cdot\prod u_i(a_i z) = \prod s_{\Lambda',\mathscr{L}^{a_i^2}}(\lambda)\cdot u_i(a_i z) = \prod a_i^*\left(s_{\Lambda',\mathscr{L}}(a_i\lambda)\cdot u_i(z)\right).$$

Proof We use compatibility of the action with the product, followed by the compatibility of the action by the isogeny $[a_i]$ (see Equation 4), whose analytic representation is exactly $z \mapsto a_i z$.

One caveat here is that while $s_{\Lambda',\mathscr{L}^\ell}$ defines a section of Λ' into $G(\mathscr{L}^\ell)$ which does not depend on the symplectic decomposition of $A[\ell]$ (because ℓ is odd), $s_{\Lambda',\mathscr{L}}$ is only a group section on Λ, and the value of $s_{\Lambda',\mathscr{L}}(\lambda)$ depends crucially on the full symplectic decomposition of Λ. Indeed, we saw in Theorem 3.8 that we had several possible choices.

But when taking the product, these choices cancel out. We can verify this: if $s_{\Lambda',\mathscr{L}}(\lambda) = [\hat{I}\pm, w]$, another choice amounts to multiplying the first coordinate $\hat{I}\pm$ by an ℓth root of unity ζ, and translating the second coordinate by an element of Λ. Then we can check that this changes $s_{\Lambda',\mathscr{L}}(a_i\lambda)$ by a factor $\zeta^{a_i^2}$ on its first coordinate; hence, the final product of the actions is changed by $\zeta^{\sum a_i^2} = \zeta^\ell = 1$. □

Let $(A,\mathscr{L},\Theta_{\mathscr{L}})$ be an abelian variety together with a level n symmetric theta structure. Then Lemma 4.3 gives us a way to compute the actions of $s_{\Lambda',\mathscr{L}^\ell}$. Namely, if $P \in A[\ell]$ is such that $P = \lambda \mod \Lambda$ for $\lambda \in \Lambda'$ and $z \in V$ is such that $x = z \mod \Lambda$ for $x \in A$, inducing excellent lifts $\tilde{P}$ and $\widetilde{x+P}$, we get that $a_i^* s_{\Lambda',\mathscr{L}}(a_i\lambda)\cdot\theta_j^{\Theta_{\mathscr{L}}} = a_i^*(x \tilde{+} a_i P)_j = (a_i x \tilde{+} a_i P)_j = (a_i(\widetilde{x+P}))_j$. Here, one needs to be careful that we are working with affine theta coordinates, so the point $a_i(x \tilde{+} P) = a_i(\widetilde{x+P})$ has to be computed as an affine point, using Riemann relations (or as usual, using the projective arithmetic on A and determining the correct projective factor through Riemann relations).

Applying Proposition 2.11 to $u_i = \theta_0^{\Theta_{\mathscr{L}}}$ (we leave to the reader the obvious generalisation to $u_i = \theta_{j_i}^{\Theta_{\mathscr{L}}}$), we get

Theorem 4.4 *Let $(A,\mathscr{L},\Theta_{\mathscr{L}})$ be an abelian variety together with a level n symmetric theta structure. Assume that ℓ is prime to n, and let $A[\ell] = A_1[\ell]\oplus A_2[\ell]$ be a symplectic decomposition. There is a unique symmetric level ℓn theta structure $\Theta_{\mathscr{L}^\ell}$ compatible with $\Theta_{\mathscr{L}}$ following Definition 2.8 and this decomposition. Write $\ell = \sum_{i=1}^r a_i^2$ with $a_i \in \mathbb{N}$. Fix excellent lifts $\tilde{A_i}[\ell]$ of the maximal isotropic subgroups $A_i[\ell]$. For $x \in A$, fix an affine lift $\tilde{x}$, excellent lifts $\widetilde{x+P}$ with respect to $\tilde{x}$ and $\tilde{P}$ for $P \in A_1[\ell]$, and then excellent lifts $x+\tilde{P}+Q$ with respect to $\widetilde{x+P}$ and $\tilde{Q}$ for $Q \in A_2[\ell]$. Compute $a_i(x+\tilde{P}+Q)$ using* mult.

Let $z \in V$ be such that $x = z \mod \Lambda$, and let μ be such that $\theta_i^{\Theta_{\mathscr{L}}}(z) = \mu\tilde{x}$. We have, up to a constant C depending only on the choice of $\widetilde{0}_{A_k}$, the following:

$$\theta_0^{\Theta_{\mathscr{L}^\ell}}(z) = C\mu^\ell \sum_{\tilde{P}\in\tilde{A_1}[\ell]}\prod_{i=1}^r (a_i(\widetilde{x+P}))_0,$$

and if $i \in A_2[\ell]$, writing $J = Q + j$ with $Q \in A_2[\ell]$ and $j \in A_2[n]$,

$$\theta_J^{\Theta_{\mathscr{L}^\ell}}(z) = C\mu^\ell \sum_{\tilde{P}\in\tilde{A_1}[\ell]}\prod_{i=1}^r (a_i(x+\tilde{P}+Q))_{a_i j}.$$

Proof The unicity of $\Theta_{\mathscr{L}^\ell}$ comes from Remark 2.7 and the fact that ℓ is odd and prime to n: for $i = 1, 2$, the section $s_i^{\Theta_{\mathscr{L}^\ell}}$ (see Definition 2.6) above $A_i[n]$ is given by $E_\ell \circ s_i^{\Theta_{\mathscr{L}}}$, and above $A_i[\ell]$ as the unique symmetric group in $G(\mathscr{L}^\ell)$ (the unicity is because ℓ is odd).

By Theorem 3.8, up to changing the lattice decomposition of Λ (twice, once for Λ_2, then for Λ_1), we can assume that we have correct lifts of $A_1[\ell]$ and $A_2[\ell]$. Let $z \in V$ be such that $x = z \mod \Lambda$, by Theorem 3.11, upon changing z first by an element of Λ_1 and then by an element of Λ_2 we may assume that there exists μ such that $(\theta_i^{\Theta_{\mathscr{L}}}(z)) = \mu * \tilde{x}$, and $P \cdot (\theta_i^{\Theta_{\mathscr{L}}}(z)) = \mu * (x \widetilde{+} P)$ and $Q \cdot P \cdot (\theta_i^{\Theta_{\mathscr{L}}}(z)) = \mu * (x + \tilde{P} + Q)$. Other analytic lifts are given by $z+\lambda$ for $\lambda \in \Lambda$. If $(\theta_i^{\Theta_{\mathscr{L}}}(z+\lambda)) = \mu * (\theta_i^{\mathscr{L}}(z))$, then $(\theta_i^{\Theta_{\mathscr{L}^\ell}}(z+\lambda)) = \mu^\ell * (\theta_i^{\Theta_{\mathscr{L}^\ell}}(z))$; hence, the LHS is homogeneous of degree ℓ with respect to μ. Since $a_i(\mu\tilde{x}) = \mu^{a_i^2} a_i \tilde{x}$, the RHS is also homogeneous of degree ℓ with respect to μ. Hence, we may suppose that $\mu = 1$, whence the result follows by Lemma 4.3. □

From the theorem, we immediately deduce the Algorithm 3 to go up in level. Going through the trace and taking into account that the scalar multiplications by the a_i cost $O(\log \ell)$, we thus get a complexity of $O(n^g \ell^g \log \ell)$ for Theorem 1.1. We can gain a factor $\log \ell$ as follow: rather than generating all the points $\tilde{P}$ from a basis $\tilde{P}_1, \ldots, \tilde{P}_g$ of $A_1[\ell]$, we first embed this basis (and the sums $P_i \tilde{+} P_j$) into A^r via $P \mapsto (a_i \cdot P)$, and then we compute the differential additions on these embeddings directly. This allows one to only compute the scalar multiplications on $O(g^2)$ points rather than $O(\ell^g)$. We thus obtain the complexity result of Theorem 1.1.

Remark 4.5 The order matters here; if we normalise $x + \tilde{P} + Q$ with respect to $x \tilde{+} Q$ and $\tilde{P}$ instead, we would change its value by a factor μ such that $\mu^\ell = e_{\mathscr{L}^\ell}(P, Q)$, since $e_{\mathscr{L}^\ell}$ is the commutator pairing on $G(\mathscr{L}^\ell)$. A similar idea was used in [12] to compute the pairing of P and Q.

Algorithm 3: Algorithm to go up from level n to level ℓn.

input :

- The theta null point $\widetilde{0}_A$ of $(A = V/\Lambda, \mathscr{L}, \Theta_{\mathscr{L}})$ an abelian variety with a symmetric level n theta structure;
- for ℓ a positive odd integer, a symplectic decomposition $A[\ell] = A_1[\ell] \oplus A_2[\ell]$ given by the theta coordinates of its basis;
- a decomposition $\ell = \sum_{i=1}^r a_i^2$;
- $x \in A$, given by its level n theta-coordinates $(\theta_i^{\Theta_{\mathscr{L}}}(x))_{i \in K_2(\mathscr{L})}$;
- $J \in K_2(\mathscr{L}^\ell)$.

output: the level ℓn theta coordinate of index J of $x \in A$: $\theta_J^{\Theta_{\mathscr{L}^\ell}}(x)$.

1 Using Algorithm 2, compute excellent lifts $\tilde{x}$ and $x \widetilde{+} P$ for $P \in A_1[\ell]$;
2 Write $J = Q + j$ for $j \in A_2[n]$ and $Q \in A_2[\ell]$;
3 Chose any affine lift $\tilde{Q}$ of Q;
4 Using Algorithm 2, compute excellent lifts $x + \tilde{P} + Q$ with respect to $x \widetilde{+} P$ and $\tilde{Q}$ for all $P \in A_1[\ell]$;
5 **return** $\sum_{\tilde{P} \in A_1[\ell]} \prod_{i=1}^r \mathrm{mult}(a_i, x + \tilde{P} + Q, \widetilde{0}_A)_{a_i j}$;

As a corollary, applying Mumford's isogeny theorem (or using Proposition 2.15 directly) we get

Corollary 4.6 *Let $(A, \mathscr{L}, \Theta_{\mathscr{L}})$ be an abelian variety together with a symmetric level n theta structure. Let ℓ be prime to n and write $\ell = \sum_{i=1}^{r} a_i$ for $a_i \in \mathbb{N}$. Let $K \subset A[\ell]$ be a maximal totally isotropic subgroup and $f : A \to B = A/K$ be the isogeny. Since ℓ is odd, there is a unique symmetric level subgroup $\tilde{K}$ of K in $G(\mathscr{L}^{\ell})$, which induces via f a descent $\mathcal{M}$ of $\mathscr{L}^{\ell}$ on B. Furthermore, by Proposition 2.15, $\Theta_{\mathscr{L}}$ induces a unique symmetric level n theta structure $\Theta_{\mathcal{M}}$ on B. Let $x \in A$ fix an affine lift $\tilde{x}$, excellent lifts $\tilde{K}$ of K, and $x \tilde{+} K$ of x with respect to $\tilde{x}$ and $\tilde{K}$. Let $z \in V$ be such that $x = z \mod \Lambda$ and let μ be such that $\theta_i(z) = \mu(\tilde{x})_i$. Then identifying $K_2(\mathscr{L})$ with $K_2(\mathcal{M})$ via f, we have for $j \in K_2(\mathscr{L})$*

$$\theta^{\Theta_{\mathcal{M}}}_{f(j)}(f(z)) = C\mu^{\ell} \sum_{P \in \tilde{x}} \prod_{i=1}^{r} (a_i(x \widetilde{+} P))_{a_i j}. \tag{8}$$

Here, the constant C is the same as in Theorem 4.4 (so depends only on the choice of $\widetilde{0}_{A_k}$), because the constant involved in Mumford's isogeny theorem from Example 2.17 is equal to 1.

Algorithm 4: Algorithm to compute an ℓ^g isogeny.

input :

- The theta null point $\widetilde{0}_A$ of $(A, \mathscr{L}, \Theta_{\mathscr{L}})$ an abelian variety with a symmetric level n theta structure;
- ℓ a positive odd integer and a decomposition $\ell = \sum_{i=1}^{r} a_i^2$;
- $K \subset A[\ell]$ a rank g isotropic subgroup of A defining an isogeny $f : A \to B$, described by the theta coordinates of a basis;
- $x \in A$, given by its projective level n coordinates $(\theta_i^{\Theta_{\mathscr{L}}}(x))_{i \in K_2(\mathscr{L})}$.

output: the projective coordinates of $f(x) \in A$: $(\theta_i^{\Theta_{\mathcal{M}}}(f(x))_{i \in K_2(\mathcal{M})}$.

1 Using Algorithm 2, compute excellent lifts $\tilde{x}$ and $\tilde{K}$;
2 **for** $j \in K_2(\mathcal{M})$ **do**
3 Let $j_0 \in K_2(\mathscr{L})$ be such that $j = f(j_0)$;
4 Let $\theta_j^{\Theta_{\mathcal{M}}}(f(x)) = \sum_{\tilde{P} \in \tilde{K}} \prod_{i=1}^{r} \mathrm{mult}(a_i, x \widetilde{+} P, \widetilde{0}_A)_{a_i j}$;
5 **end**
6 **return** $(\theta_j^{\Theta_{\mathcal{M}}}(f(x)))_{j \in K_2(\mathcal{M})}$;

Remark 4.7 From the proof of Lemma 4.3, we do not need to take excellent lifts of K and $x + K$ globally. We just need excellent lifts $\tilde{P}$ and $x \widetilde{+} P$ individually for any $P \in K$. Indeed, the different choices cancel out in the product inside Equation 8.

When given a basis $P_1, \ldots, P_g$ of K, it is actually faster to compute excellent lifts of P_i, $P_i + P_j$, $x + P_i$ and $x + P_i + P_j$ and compute the rest using differential additions to get a global lift of K, rather than normalising each point individually.

However, if we have equations for the kernel K, rather than computing $x \widetilde{+} P$ for each $P \in K$, we can compute it for a formal point of K (i.e. work over the étale algebra defining Spec$K$), and then compute the product $\prod_{i=1}^{r} (a_i(x \widetilde{+} P))_i$ formally modulo the equations. If we have a univariate parametrisation of K, the trace across K is then given by a resultant, using the same method as in [14].

Remark 4.8 We now explain how to relax the assumption that ℓ odd is prime to n. Fix a symplectic decomposition of Λ giving our theta null point of level n on A. This induces a canonical symplectic decomposition of $A[\ell n]$. Algebraically, our (symmetric) theta structure of level n (resp. ℓn) is completely determined by the corresponding symplectic decomposition of $A[2n]$ (resp. $A[2n\ell]$), and the theta structures are compatible in the sense of Definition 2.8 if $\ell A_i[2\ell n] = A_i[2n]$.

If ℓ is odd, we only need to fix a symplectic decomposition of $A[n\ell]$ such that $\ell A_i[\ell n] = A[n]$. If P is a point of ℓn torsion, and $\tilde{x}$ an affine point given by the level n theta coordinate, we may extend the strategy of Sect. 3 to compute $s(P)\cdot\tilde{x}$ as follows: $g := s(P)^\ell$ is an element of $G(\mathscr{L})$, whence we know its action on $\tilde{x}$ explicitly. So we may extend the definition of an excellent lift $\tilde{P}$ and $x \widetilde{+} P$ by requiring in this case that if $\ell = 2\ell' + 1$, $(\ell'+1)\tilde{P} = g\cdot\ell'(-\tilde{P})$, and $x \tilde{+} \ell P = g\cdot\tilde{x}$. These define these lifts up to an ℓth root of unity as before.

From Corollary 4.6, we get Algorithm 4 to compute an isogeny between abelian varieties. In practice, an abelian variety together with a symmetric level n theta structure defined over k is determined by its theta null point which is a projective point in $\mathbb{P}_k^{n^g-1}$ defined over k. The theta null point can be obtained through Thomae-like formulas [3] if A is the Jacobian of a curve. In general, theta null points are described using the equations of (a closure of) the moduli space of abelian variety together with a level n theta structure as defined in [17].

Note that in order to use the results of this paper, we need n to be even. Moreover, as the ambient space in which A is embedded has dimension $n^g - 1$, and we look for compact representation of the objects for time and memory efficiency, we want n to be as small as possible. So in practice, we use $n = 2$ or $n = 4$. As all the level 2 theta functions are even, they do not provide an embedding of A but rather of its associated Kummer variety $K = A/(-1)$. Although K is not an algebraic group, its set of points still enjoy a pseudo-group law and pairings which makes it useful for computations and some applications in cryptography [7,8,15], and it is straightforward to adapt our algorithms to this case.

The examples have been computed using the MAGMA library [2]. They also could be done with the Sage reimplementation of AVIsogenies [22].

Example 4.9 Let $\mathbb{F}$ be the finite field of size 1511, and E the elliptic curve $y^2 = x^3 + 1211x + 600$ over $\mathbb{F}$. Let P be the 7 torsion point $(858\eta^2 + 1045\eta + 830 : 386\eta^2 + 1245\eta + 811 : 1)$ in the extension field of degree 3 where $\eta^3 + 2\eta + 1500 = 0$. We compute a level 4 theta null point of E using Thomae's formula (as implemented in [2]): it lives in an extension of degree 6 of $\mathbb{F}$, and convert P to theta coordinates. Let K be the kernel generated by P; we check that it is rational over $\mathbb{F}$. We compute an excellent lift $\tilde{K}$ of K by computing an excellent lift $\tilde{P}$ from P and then using differential addition to recover the other multiples. We now apply Corollary 4.6 to the decomposition $7 = 1 + 1 + \cdots + 1$, namely,

$$\theta_j^{E/K}(0) = \sum_{P\in\tilde{K}} \theta_j(\tilde{P})_j^\ell. \tag{9}$$

We get the following level 4 theta null point: $(853\nu^5 + 1372\nu^4 + 424\nu^3 + 743\nu^2 + 430\nu + 865, 440\nu^5 + 9\nu^4 + 663\nu^3 + 128\nu^2 + 170\nu + 280, 1042\nu^5 + 298\nu^4 + 853\nu^3 + 311\nu^2 + 632\nu + 107, 440\nu^5 + 9\nu^4 + 663\nu^3 + 128\nu^2 + 170\nu + 280)$ where $\nu^6 + \nu^4 + 106\nu^3 + 1278\nu^2 + 1032\nu + 11 = 0$.

We now convert back the theta null point of E/K to an equation of E/K (by computing its Legendre invariant). This gives a curve defined over an extension of degree 6 but whose j invariant is $j(E/K) = 491$; hence, E/K descends to $\mathbb{F}$ as expected. Comparing with Vélu's formula, we recover the same elliptic curve.

Example 4.10 Let C be the hyperelliptic curve of genus 2 given by the equation $y^2 = t^{254}x^6 + t^{223}x^5 + t^{255}x^4 + t^{318}x^3 + t^{668}x^2 + t^{543}x + t^{538}$ defined over the finite field $\mathbb{F}$ with 3^6 elements where $t^6 + 2t^4 + t^2 + 2t + 2 = 0$. There is a unique rational totally isotropic (for the Weil pairing) subgroup K in $\mathrm{Jac}(C)[7]$. We compute (using [2]) the theta null point of $\mathrm{Jac}(C)$ and convert two generators P, Q of K into theta coordinates. These points P and Q live in an extension of degree 4 of $\mathbb{F}$. We then normalise them to form excellent affine lifts $\tilde{P}, \tilde{Q}$, along with $P \tilde{+} Q$. From these lifts we can compute an excellent lift $\tilde{K}$ of K using differential additions and then compute the isogenous theta null point using a trace like in Equation 9. We compute the Rosenhain invariants associated to this theta null point and recover the isogenous curve: $y^2 = t^{293}x^6 + x^5 + t^{225}x^4 + t^{189}x^3 + t^{87}x^2 + t^{424}x + t^{289}$. We check that these two curves have the same zeta function, and hence are indeed isogenous.

5 Descending level

We now want to explain how to do the reverse of Sect. 4, namely, given theta functions for a (symmetric) theta structure of level ℓn on $\mathscr{L}^\ell$, compute the theta functions for the unique induced one of level n on $\mathscr{L}$ (recall that we assume n even).

To apply our algorithm of Proposition 2.11, we first need to construct a section $\nu \in \Gamma(A, \mathscr{L})$, and then explain how the theta group $G(\mathscr{L})$ acts on it. Unfortunately, we cannot build an element of $\Gamma(A, \mathscr{L})$ from those of $\Gamma(A, \mathscr{L}^\ell)$. However, we can try to build an element of $\Gamma(A, \mathscr{L}^{\ell^2})$ of the form $u = \nu \circ [\ell]$. In fact, if we know how (the lift of $A[\ell]$ acts in $G(\mathscr{L}^{\ell^2})$, we only need any $u \in \Gamma(A, \mathscr{L}^{\ell^2})$, and take the trace u' of u under $A[\ell]$ to get a section of the form $\nu \circ [\ell]$. More precisely, we can use Proposition 2.15 applied to the isogeny $[\ell]$ to construct the theta functions of level n on $\mathscr{L}$.

But we can use Sect. 4.2 to go from level $n\ell$ to level $n\ell^2$. In particular, if $\ell = \sum a_i^2$ and u_i are in $\Gamma(A, \mathscr{L}^\ell)$, then $u = \prod u_i(a_i x) \in \Gamma(A, \mathscr{L}^{\ell^2})$. While we cannot directly apply the results of this section since ℓ is not prime to $n\ell$ (but see Remark 4.8), to apply Proposition 2.15, we only need to compute the action of (the lift of) the points in $A[\ell]$ and in $A[n]$ on u. In our current case, this is actually easier than in Proposition 2.15, since we already have a theta structure of level ℓn, we already have the action of these points on the u_i, and hence (by compatibility with product and isogenies) on u.

Theorem 5.1 *Let $(A = V/\Lambda, \mathscr{L}^\ell, \Theta_{\mathscr{L}^\ell})$ be an abelian variety with a symmetric theta structure of level $n\ell$, with n even and ℓ prime to n, and let $\Theta_{\mathscr{L}}$ be the unique structure on $\mathscr{L}$ compatible with $\Theta_{\mathscr{L}^\ell}$ (Definition 2.8). Let $A[\ell n] = A_1[\ell n] \oplus A_2[\ell n]$ be the corresponding symplectic decomposition. Write $\ell = \sum_{i=1}^r a_i^2$. Let $x \in A$ and fix an arbitrary affine lift $\tilde{x}$; let $z \in V$ be such that $z \mod \Lambda = x$ and let μ be such that $\theta_i^{\Theta_{\mathscr{L}}}(z) = \mu \tilde{x}_i$.*

Then, up to a constant C depending only on the choice of $\widetilde{0}_{A_k}$, for $j \in A_2[n]$,

$$\theta_{\ell j}^{\Theta_{\mathscr{L}}}(\ell z) = C\mu^\ell \sum_{t \in A_2[\ell]} \prod_{i=1}^r (a_i \tilde{x})_{a_i(j+t)},$$

where $a_i\tilde{x}$ is computed via mult.

Proof Let $\Lambda' = \frac{1}{\ell}\Lambda$. By Lemma 2.3, there are group sections $s_{\Lambda',\mathscr{L}^\ell} : \Lambda' \to \mathfrak{G}(\mathscr{L}^\ell)$ and $s_{\Lambda,\mathscr{L}} : \Lambda \to \mathfrak{G}(\mathscr{L})$. Consider the group morphism $H_\ell : \mathfrak{G}(\mathscr{L}^\ell) \to \mathfrak{G}(\mathscr{L})$, $[\alpha, v] \mapsto [\alpha^\ell, \ell v]$, then H_ℓ is compatible with the sections $s_{\Lambda',\mathscr{L}^\ell}$ and $s_{\Lambda,\mathscr{L}}$: $H_\ell(s_{\Lambda',\mathscr{L}^\ell}(\lambda)) = s_{\Lambda,\mathscr{L}}(\ell\lambda)$. Thus, if $\Theta_{\mathscr{L}}$ is compatible with $\Theta_{\mathscr{L}^\ell}$, for $i = 1, 2$, the sections $s_i^{\Theta_{\mathscr{L}}} : A_i[n] \to G(\mathscr{L})$ defining the theta structure $\Theta_{\mathscr{L}}$ are completely determined by $s_i^{\Theta_{\mathscr{L}}}(P) = s_i^{\Theta_{\mathscr{L}^\ell}}(P')$ for any point $P' \in A_i[n\ell]$ with $P = \ell P'$. This proves the unicity of $\Theta_{\mathscr{L}}$.

As in Theorem 4.4, both the LHS and RHS are homogeneous of degree ℓ with respect to μ, so we may renormalise $\tilde{x}$ such that $\mu = 1$. Then we apply Proposition 2.15 combined with Lemma 4.3 and the results of Sect. 4. We remark that since $\theta_0^{\Theta_{\mathscr{L}^\ell}}$ is invariant by $A_1[\ell n]$, we only need to sum through $t \in A_2[\ell]$. □

Remark 5.2 We can use Theorem 5.1 to get an isogeny algorithm as follows: let $f : A \to B$ be the isogeny. Then we have a contragredient isogeny $\tilde{f} : B \to A$, and given $x \in A$, we can use the results of Sect. 4.1 to compute the theta coordinates of level ℓn of a preimage $y = \tilde{f}^{-1}(x)$ on B. Then, applying Theorem 5.1, we get the theta coordinates of level n of ℓy, which by definition of the contragredient isogeny is exactly $f(x)$. We let the reader check that this recovers exactly Corollary 4.6.

We constructed our descent algorithm by first using Theorem 4.4 to go up in level $n\ell^2$ and then descending to level n via Mumford's isogeny theorem applied to the isogeny $[\ell]$. Conversely, we could recover the ascending algorithm from Theorem 5.1 by first using Sect. 4.1 applied to $[\ell]$ to compute the coordinates of level $\ell^2 n$ of a point y such that $\ell y = x$, and then apply Theorem 5.1 to get the coordinates of level ℓn of x.

Remark 5.3 Another way of descending level used in [4] is to consider Koizumi's formula. Koizumi uses an isogeny $F : A^r \to A^r$, where F is an integer matrix such that ${}^tFF = \ell \mathrm{Id}_r$. In particular, the first column of F is given by $(a_1, \ldots, a_r)$ such that $\ell = \sum a_i^2$.

We can reinterpret our method as a tweak on this idea: we only use the first column of F to map A into A^r via $P \mapsto (a_i P)$; this is a generalised Segre mapping S. The important point is that since $S^*(\mathscr{L}^\ell)^{*,r} = (\mathscr{L}^\ell)^{\sum a_i^2} = \mathscr{L}^{\ell^2}$, $S(A[\ell])$ is isotropic in $(A^r, (\mathscr{L}^\ell)^{*,r})$; so we can apply Mumford's isogeny theorem to the kernel $S(A[\ell])$. This recovers the formula of Theorem 5.1.

6 The case of real multiplication

When our abelian variety A has real multiplication by an order O of rank g, then given a principal polarisation H_0, we can consider polarisations of the form βH_0 where β is a totally positive real element.

Recall that if $A = V/\Lambda$, V is canonically isomorphic to the tangent space of A at 0. This fixes an embedding ϕ of O into $\mathrm{End}(V)$. We fix a compatible isomorphism $v : O \otimes_Z \mathbb{C} \simeq \mathbb{C}^g \to V$.

Given a theta structure of level n on A (with polarisation $H = nH_0$), we want to compute a theta structure of level βn (with polarisation βH, where $\beta H(z_1, z_2) = H(\beta z_1, z_2) = H(z_1, \beta z_2)$). We also want to compute β isogenies: $f : (A, \mathscr{L}) \to (B, \mathcal{M})$, i.e. such that if F is the analytic representation of F and H_A, H_B is the associated polarisations: $f^* H_B = \beta H_A$. We denote by $\mathscr{L}^\beta$ the line bundle with polarisation βH induced by this decomposition.

Here, we need to assume that our theta structure is compatible with the real multiplication, i.e. is induced by a symplectic decomposition of Λ: $\Lambda = \Lambda_1 \oplus \Lambda_2$, such that Λ_i is

stable under the action of O given by $\beta.\lambda \mapsto \nu(\beta)\lambda$ for $\beta \in O$ and $\lambda \in \Lambda$. We call this an RM-symplectic decomposition. Then, for instance, if $\Lambda' = \Lambda_1/\beta \oplus \Lambda_2$ and $B = V/\Lambda'$, $F : z \mapsto z$ induces a β isogeny $(A, \mathscr{L}) \to (B, \mathcal{M})$, where $\mathcal{M}$ is the line bundle on B with polarisation $H_B = H_A$ induced by the symplectic decomposition of Λ'.

We generalise Sect. 4.2 as follows: fix a decomposition $\beta = \sum \beta_i$ where each $\beta_i \in O$ is totally positive. For each β_i, fix a (compatible) β_i isogeny $f_i : (A, \mathscr{L}) \to (B_i, \mathcal{M}_i)$ with analytic representation F_i. Let u_i be a section of $\mathcal{M}_i$; then $u = \prod u_i \circ f_i$ is a section of $\mathscr{L}$.

Example 6.1 If α_i is an endomorphism of A, it can be considered as an $\overline{\alpha}_i\alpha_i$ isogeny, where $\overline{\alpha}$ denotes the Rosati involution under our fixed principal polarisation. Then, if $\beta = \sum \overline{\alpha}_i\alpha_i$, we can use $f_i = \alpha_i$, i.e. endomorphisms rather than isogenies. The decomposition $\ell = \sum a_i^2$ from Sect. 4 is a special case of this where, furthermore, the α_i are integers.

A direct generalisation of Lemma 4.3 yields the following:

Lemma 6.2 *Fix an RM-symplectic decomposition $\Lambda = \Lambda_1 \oplus \Lambda_2$, and let $\Lambda' = \frac{1}{\beta}\Lambda_1 \oplus \Lambda_2$, or $\Lambda' = \Lambda_1 \oplus \frac{1}{\beta}\Lambda_2$. For $\beta \in O$, we denote by $s_{\Lambda',\mathscr{L}^\beta} : \Lambda' \to \mathfrak{G}(\mathscr{L}^\beta)$ the set section defined by $s_{\Lambda',\mathscr{L}^\beta}(\lambda) = [a_{\mathscr{L}^\beta}(0,\lambda),\lambda]$. For $\lambda \in \Lambda'$, such that we have*

$$s_{\Lambda',\mathscr{L}^\beta}(\lambda).\prod u_i(F_i(z)) = \prod s_{\Lambda',\mathscr{L}^{\beta_i}}(\lambda)u_i(F_i(z)) = \prod F_i^*\left(s_{\Lambda',\mathscr{L}}(F_i(\lambda)) \cdot u_i(z)\right).$$

To apply this Lemma 6.2, we need to assume that we know not only how to compute the isogenies f_i but also their analytic representations F_i. More precisely, given the (affine) theta coordinates of level n of z: $\tilde{x} = (\theta_j^{\mathscr{L}}(z))_{j\in K_2(\mathscr{L})}$, the algorithm should output the (affine) theta coordinates of $F_i(z)$: $F_i(\tilde{x}) = (\theta_j^{\mathcal{M}_i}(F_i(z)))_{j\in K_2(\mathcal{M}_i)}$. We also need compatibility with the action: given $\lambda \in \Lambda_1 \otimes_{\mathbb{Z}} \mathbb{Q}$ or in $\Lambda_2 \otimes_{\mathbb{Z}} \mathbb{Q}$, the coordinates $\tilde{x}$ of z and the coordinates of $s(\lambda)\cdot\tilde{x} = s(\lambda)\cdot(\theta_j^{\mathscr{L}}(z))_{j\in K_2(\mathscr{L})}$, the algorithm should output $F_i(s(\lambda)\cdot(\theta_j^{\mathscr{L}}(z))_{j\in K_2(\mathscr{L})}) = \left(s(F_i(\lambda))\cdot(\theta_j^{\mathcal{M}_i})_{j\in K_2(\mathcal{M}_i)}\right)(F_i(z))$ (if the former equation is satisfied, the latter is already automatically satisfied for $\lambda \in F_i^{-1}(\Lambda_{B,i})$).

We also need to explain how to adapt Theorems 3.8 and 3.11 to obtain an excellent lift of $K = A_1[\beta]$ when β is of odd norm. Let $P_1, \ldots, P_g$ be a basis of K such that P_i is of order m_i and $\#K = \prod m_i$. Take an excellent lift of each P_i with respect to the order m_i, that is, if $m_i = 2m_i' + 1$, $(m_i'+1)\tilde{P}_i = -m_i'\tilde{P}_i$, and compute the other lifts using mult_add. This gives an excellent lift $\tilde{K}$ of K. A similar method gives an excellent lift $x \tilde{+} K$ of a point $x \in A$.

Then we have the following generalisations of Theorem 4.4, Corollary 4.6 and Theorem 5.1:

Theorem 6.3 *Let $(A, \mathscr{L}, \Theta_{\mathscr{L}})$ be an abelian variety together with a level n symmetric theta structure. Assume that β is of norm prime to n and let $A[\beta] = A_1[\beta] \oplus A_2[\beta]$ be a symplectic decomposition. This induces a unique symmetric theta structure $\Theta_{\mathscr{L}^\beta}$ on $\mathscr{L}^\beta$ compatible with $\Theta_{\mathscr{L}}$.*

Let $\beta = \sum \beta_i$ and assume we can compute affine β_i isogenies $F_i : (A, \mathscr{L}) \to (B, \mathcal{M}_i)$ where F_i is the analytic representation of the isogeny f_i. Fix excellent lifts $A_i\tilde{[}\beta]$ of the maximal isotropic subgroups $A_i[\beta]$. For $x \in A$, fix an affine lift $\tilde{x}$, excellent lifts $x \widetilde{+} P$ with respect to $\tilde{x}$ for $P \in A_1[\beta]$ induced by $A_1\tilde{[}\beta]$, and then excellent lifts $x + \tilde{P} + Q$ with respect to $x \widetilde{+} P$ for $Q \in A_2[\beta]$. For this theta structure on $\mathscr{L}^\beta$, we have (up to a constant depending

on $\widetilde{0}_{A_k}$ *and* $\tilde{x}$ *only) the following:*

$$\theta_0^{\Theta_{\mathscr{L}^\beta}}(x) = \sum_{\tilde{P}\in A_1\tilde{[}\beta]} \prod \theta_0^{\Theta_{\mathcal{M}_i}}(F_i(x \widetilde{+} P)),$$

and if $J \in A_2[n\beta]$*, writing* $J = Q + j$ *with* $Q \in A_2[\beta]$ *and* $j \in A_2[n]$*,*

$$\theta_J^{\Theta_{\mathscr{L}^\beta}}(x) = \sum_{\tilde{P}\in\tilde{K}_1} \prod \theta_{f_i(j)}^{\Theta_{\mathcal{M}_i}}(F_i(x + \tilde{P} + Q)).$$

Proof By Lemma 6.2, $s_{\Lambda',\mathscr{L}^\beta}(\lambda).\prod \theta_0^{\Theta_{\mathcal{M}_i}}(F_i(z)) = \prod F_i^*\left(s_{\Lambda',\mathscr{L}}(F_i(\lambda))\cdot\theta_0^{\Theta_{\mathcal{M}_i}}(z)\right)$. By assumption, we know how to compute the analytic representation F_i of the isogenies in a manner compatible with the action: if $J = Q + j$ as in the theorem, $F_i^*\left(s_{\Lambda',\mathscr{L}}(F_i(J)).\theta_0^{\Theta_{\mathcal{M}_i}}(z)\right) = \theta_{f_i(j)}(F_j(s_{\Lambda',\mathscr{L}}(Q)\cdot\theta_j^{\Theta_{\mathscr{L}}}(z)))$, and the RHS is equal to $\theta_{f_i(j)}(F_j(z \tilde{+} Q))$. □

Corollary 6.4 *Let* $(A, \mathscr{L}, \Theta_{\mathscr{L}})$ *be an abelian variety together with a level* n *symmetric theta structure. Let* $K \subset A[\beta]$ *be a maximal totally isotropic subgroup and* $f : A \to B = A/K$ *be the isogeny. Assume that* β *is of norm prime to* n*, then there is a unique symmetric level subgroup* $\tilde{K}$ *of* K *in* $G(\mathscr{L}^\beta)$*, which induces via* f *a descent* $\mathcal{M}$ *of* $\mathscr{L}^\beta$ *on* B*. Furthermore, there is a unique level* n *theta structure on* B*,* $\Theta_{\mathcal{M}}$*, compatible with* $\Theta_{\mathscr{L}}$ *(see Definition 2.8).*

Let $\beta = \sum \beta_i$ *and assume we can compute affine* β_i *isogenies* $F_i : (A, \mathscr{L}) \to (B, \mathcal{M}_i)$*. Let* $x \in A$*. Fix an affine lift* $\tilde{x}$*, excellent lifts* $\tilde{K}$ *of* K*, and* $x \tilde{+} K$ *of* x *with respect to* $\tilde{x}$ *and* $\tilde{K}$*. Then identifying* $K_2(\mathscr{L})$ *with* $K_2(\mathcal{M})$ *via* f*, we have (up to a constant depending only on* $\widetilde{0}_{A_k}$ *and* $\tilde{x}$*)*

$$\theta_{f(j)}^{\Theta_{\mathcal{M}}}(f(x)) = \sum_{P\in\tilde{K}} \prod (F_i(x \widetilde{+} P))_{f_i(j)}. \tag{10}$$

Theorem 6.5 *Let* $(A, \mathscr{L}^\beta, \Theta_{\mathscr{L}^\beta})$ *be an abelian variety with a symmetric theta structure of level* $n\beta$*, with* n *even and* β *of norm prime to* n *and let* $\Theta_{\mathscr{L}}$ *be the unique structure on* $\mathscr{L}$ *compatible with* $\Theta_{\mathscr{L}^\beta}$ *(Definition 2.8). Let* $A[\beta n] = A_1[\beta n] \oplus A_2[\beta n]$ *be the corresponding symplectic decomposition. Write* $\beta = \sum_{i=1}^r \beta_i$ *and assume that we can compute affine* β_i *isogenies* $F_i : (A, \mathscr{L}^\beta) \to (B, \mathcal{M}_i)$*, where* F_i *is the analytic representation of* f_i*. Let* $x \in A$ *and fix an arbitrary affine lift* $\tilde{x}$*.*

Then, up to a constant depending only on $\widetilde{0}_{A_k}$ *and* $\tilde{x}$*, for* $j \in A_2[\beta n]$*,*

$$\theta_{\beta j}^{\Theta_{\mathscr{L}}}(\beta z) = \sum_{t\in A_2[\beta]} \prod_{i=1}^r F_i(\tilde{x})_{f_i(j+t)}.$$

Remark 6.6 It should be possible to adapt Lemma 6.2 to show that by computing commutator pairings in the spirit of [12], we may tweak the algorithm of Corollary 6.4 to not only compute the isogeny f but also its analytic representation F in a way compatible with the action. This would open up a recursive approach to compute β isogenies.

Most of the difficulty resides in bootstrapping the algorithm. In Sect. 4.2, we simply had to compute the multiplication by $[a_i]$, whose affine form (easily checked to be compatible with the action) is given by $\tilde{x} \mapsto \mathrm{mult}(a_i, \tilde{x})$. When $k = \mathbb{F}_q$ is a finite field, we may use the Frobenius π_q to compute more general endomorphisms. We then need to find a decomposition $\beta = \sum \alpha_i\overline{\alpha}_i$ of endomorphisms (possibly with denominators). This is

the approach followed in [6]. Alternatively, when $g = 2$, the real multiplication field is a quadratic real field $\mathbb{Q}(\sqrt{d})$, and the endomorphism $\sqrt{d}$ is a d isogeny which can be computed "affinely" using Corollary 4.6 or [4,14]; see [20] for this case.

In summary, the methods of this Sect. 6 provide a general framework, but fully handling real multiplication, in particular bootstrapping cyclic isogenies, remains a difficult topic. We leave the details to future work.

Data availability Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Author details
[1]IRMAR, Universté de Rennes, 1 Campus de Beaulieu, 35042 Rennes, France, [2]INRIA Bordeaux-Sud-Ouest, 200 avenue de la Vieille Tour, 33405 Talence Cedex, France.

Received: 17 September 2022 Accepted: 23 September 2022 Published online: 12 December 2022

References

1. Birkenhake, C., Lange, H.: Complex Abelian Varieties, 2nd edn, vol. 302. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer, Berlin (2004)
2. Bisson, G., Cosset, R., Robert, D.: "AVIsogenies". Magma package devoted to the computation of isogenies between abelian varieties (2010). https://www.math.ubordeaux.fr/~damienrobert/avisogenies. Free software (LGPLv2+), registered to APP (reference IDDN.FR.001.440011.000.R.P.2010.000.10000). Latest version 0.6, released on 2012-11-28
3. Cosset, R.: Application des fonctions thêta á la cryptographie sur courbes hyperelliptiques. PhD thesis (2011)
4. Cosset, R., Robert, D.: An algorithm for computing ($\updownarrow, \updownarrow$)-isogenies in polynomial time on Jacobians of hyperelliptic curves of genus 2. In: Mathematics of Computation 84.294, pp. 1953–1975 (2015). https://doi.org/10.1090/S0025-5718-2014-02899-8. http://www.normalesup.org/~robert/pro/publications/articles/niveau.pdf. HAL: hal-00578991, eprint: 2011/143
5. Couveignes, J.M., Ezome, T.: Computing functions on Jacobians and their quotients. LMS J. Comput. Math. **18**(1), 555–577 (2014) arXiv:1409.0481
6. Dudeanu, A., Jetchev, D., Robert, D., Vuille, M.: Cyclic isogenies for abelian varieties with real multiplication (2017). arXiv:1710.05147v2
7. Gaudry, P.: Fast genus 2 arithmetic based on Theta functions. J. Math. Cryptol. **1**(3), 243–265 (2007)
8. Gaudry, P., Lubicz, D.: The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines. Finite Fields Appl. **15**(2), 246–260 (2009). https://doi.org/10.1016/j.ffa.2008.12.006
9. Igusa, J.: On the graded ring of theta-constants (II). Am. J. Math. **88**(1), 221–236 (1966)
10. Kirschmer, M., Narbonne, F., Ritzenthaler, C., Robert, D.: Spanning the isogeny class of a power of an elliptic curve. Accepted for publication at Math. Comput. (2020). http://www.normalesup.org/~robert/pro/publications/articles/algebraic/_obstruction.pdf
11. Koizumi, S.: Theta relations and projective normality of abelian varieties. Am. J. Math. **98**, 865–889 (1976)
12. Lubicz, D., Robert, D.: Efficient pairing computation with theta functions. In: Hanrot, G., Morain, F., Thomé, E. (eds.) 9th International Symposium, vol. 6197. Lecture Notes in Computer Sciences, Nancy, France, ANTS-IX, 19–23 July 2010, Proceedings. Springer, Berlin (2010). https://doi.org/10.1007/978-3-642-14518-6_21. http://www.normalesup.org/robert/pro/publications/articles/pairings.pdf Slides: 2010-07-ANTS-Nancy.pdf (30 min, International Algorithmic Number Theory Symposium (ANTS-IX), July 2010, Nancy). HAL: hal-00528944
13. Lubicz, D., Robert, D.: Computing isogenies between abelian varieties. Compos. Math. **148**(5), 1483–1515 (2012). https://doi.org/10.1112/S0010437X12000243. arXiv: 1001.2016 [math.AG]. http://www.normalesup.org/~robert/pro/publications/articles/isogenies.pdf hal-00446062
14. Lubicz, D., Robert, D.: Computing separable isogenies in quasi-optimal time. LMS J. Comput. Math. **18**, 198–216 (2015). https://doi.org/10.1112/S146115701400045X. arXiv: 1402.3628. http://www.normalesup.org/~robert/pro/publications/articles/rational.pdf hal-00954895
15. Lubicz, D., Robert, D.: Arithmetic on Abelian and Kummer Varieties. Finite Fields Appl. **39**, 130–158 (2016). https://doi.org/10.1016/j.ffa.2016.01.009. http://www.normalesup.org/robert/pro/publications/articles/arithmetic.pdf. HAL: hal-01057467, eprint: 2014/493
16. Mumford, D.: On the equations defining abelian varieties. I. Invent. Math. **1**, 287–354 (1966)
17. Mumford, D.: On the equations defining abelian varieties. III. Invent. Math. **3**, 215–244 (1967)
18. Mumford, D.: Tata Lectures on Theta I, vol. 28. Progress in Mathematics. With the assistance of Musili, C., Nori, M., Previato, E., Stillman, M. Birkhäuser, Boston (1983)
19. Mumford, D.: Tata Lectures on Theta II, vol. 43. Progress in Mathematics. Jacobian Theta Functions and Differential Equations. With the Collaboration of Musili, C., Nori, M., Previato, E., Stillman, M., Umemura, H. Birkhäuser, Boston (1984)
20. Robert, D.: Isogenies between abelian varieties. In: ANR Peace Conference Effective Moduli Spaces and Applications to Cryptography. Rennes (2014). http://www.normalesup.org/~robert/pro/publications/notes/2014-06-Rennes-Moduli.pdf

21. Robert, D.: Efficient algorithms for abelian varieties and their moduli spaces. PhD thesis, Université Bordeaux, June 2021. http://www.normalesup.org/~robert/pro/publications/academic/hdr.pdf Slides: 2021-06-HDR-Bordeaux.pdf (1h, Bordeaux)
22. Somoza, A.: thetAV. Sage package devoted to the computation with abelian varieties with theta functions (2021). http://www.github.com

Publisher's Note