Computing modular correspondences for abelian varieties

Jean-Charles Faugère, David Lubicz, Damien Robert

Computing modular correspondences for abelian varieties

Jean-Charles Faugère[1], David Lubicz[2,3], Damien Robert[4]

[1] INRIA, Centre Paris-Rocquencourt, SALSA Project
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
UFR Ingénierie 919, LIP6 Passy Kennedy, Boite courrier 169,
4, place Jussieu, F-75252 Paris Cedex 05
[2] CÉLAR, BP 7419, F-35174 Bruz
[3] IRMAR, Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes
[4] LORIA, CACAO Project
Campus Scientifique
BP 239
54506 Vandoeuvre-lès-Nancy Cedex

Abstract. In this paper, we describe an algorithm to compute modular correspondences in the coordinate system provided by the theta null points of abelian varieties together with a theta structure. As an application, this algorithm can be used to speed up the initialisation phase of a point counting algorithm [CL09]. The main part of the algorithm is the resolution of an algebraic system for which we have designed a specialized Gröbner basis algorithm. Our algorithm takes advantage of the structure of the algebraic system in order to speed up the resolution. We remark that this special structure comes from the action of the automorphisms of the theta group on the solutions of the system which has a nice geometric interpretation. In particular we were able count the solutions of the system and to identify which one correspond to valid theta null points.
Keywords: *Abelian varieties, Theta functions, Isogenies, Modular correspondences.*

1 Introduction

The aim of this paper is to compute a higher-dimensional analog of the classical modular polynomials $\Phi_\ell(X,Y)$. We recall that $\Phi_\ell(X,Y)$ is a polynomial with integer coefficients. Moreover, if j is the j-invariant associated to an elliptic curve E_k over a field k then the roots of $\Phi_\ell(j,X)$ correspond to the j-invariants of elliptic curves that are ℓ-isogeneous to E_k. These modular polynomials have important algorithmic applications. For instance, Atkin and Elkies (see [Elk98]) take advantage of the modular parametrisation of ℓ-torsion subgroups of an elliptic curve to improve the original point counting algorithm of Schoof [Sch95].

In [Sat00], Satoh introduced an algorithm to count the number of rational points of an elliptic curve E_k defined over a finite field k of small characteristic

p that relies on the computation of the canonical lift of the j-invariant of E_k. Here again it is possible to improve the original lifting algorithm of Satoh [VPV01,LL06] by solving over the p-adics the equation given by the modular polynomial $\Phi_p(X, Y)$.

This last algorithm has been improved by Kohel in [Koh03] using the notion of *modular correspondence*. For N a strictly positive integer, the modular curve $X_0(N)$ parametrizes the set of isomorphism classes of elliptic curves together with an N-torsion subgroup. For instance, the curve $X_0(1)$ is just the line of j-invariants. Let p be prime to N. A map $X_0(pN) \to X_0(N) \times X_0(N)$ is a modular correspondence if the image of each point represented by a pair (E, G), where G is a subgroup of order pN of E, is a couple $((E_1, G_1), (E_2, G_2))$ with $E_1 = E$ and G_1 is the unique subgroup of index p of G, and $E_2 = E/H$ where H is the unique subgroup of order p of G. In the case that the curve $X_0(N)$ has genus zero, the correspondence can be expressed as a binary equation $\Phi(X, Y) = 0$ in $X_0(N) \times X_0(N)$ cutting out a curve isomorphic to $X_0(pN)$ inside the product. For instance, if one considers the correspondence $X_0(\ell) \to X_0(1) \times X_0(1)$ for ℓ a prime number then the polynomial defining its image in the product is the modular polynomial $\Phi_\ell(X, Y)$.

In this paper, we are interested in the computation of an analog of modular correspondences for higher dimensional abelian varieties over a field k. We suppose that the characteristic of k is different from 2 and that it is possible to represent the elements of k and compute efficiently the addition and multiplication laws of k: this is the case for instance for finite fields of characteristic different from 2. We use a model of moduli space which is amenable to computations. We fix an integer $g > 0$ for the rest of the paper. In the following if n is a positive integer, $\overline{n}$ denotes the element $(n, \ldots, n) \in \mathbb{N}^g$. We consider the set of triples of the form $(A_k, \mathscr{L}, \Theta^B_{\overline{n}})$ where A_k is a g dimensional abelian variety equipped with a symmetric ample line bundle $\mathscr{L}$ and a symmetric theta structure $\Theta^B_{\overline{n}}$ of type $\overline{n}$. Such a triple is called an abelian variety with an $\overline{n}$-marking. To a triple $(A_k, \mathscr{L}, \Theta^B_{\overline{n}})$, one can associate following [Mum66] its theta null point (see Section 2). The locus of theta null points corresponding to the set of abelian varieties with an $\overline{n}$-marking is a quasi-projective variety $\mathcal{M}_{\overline{n}}$. Moreover, it is proved in [Mum67a] that if $8|n$ then $\mathcal{M}_{\overline{n}}$ is a classifying space for abelian varieties with an $\overline{n}$-marking. We would like to compute an analog of modular correspondences in $\mathcal{M}_{\overline{n}}$.

For this, let $(A_k, \mathscr{L}, \Theta^A_{\overline{\ell n}})$ be an abelian variety with a $(\overline{\ell n})$-marking. We suppose that ℓ and n are relatively prime. From the theta structure $\Theta^A_{\overline{\ell n}}$, we deduce a decomposition of the kernel of the polarization $K(\mathscr{L}) = K_1(\mathscr{L}) \times K_2(\mathscr{L})$ into maximal isotropic subspaces for the commutator pairing associated to $\mathscr{L}$. Let $K(\mathscr{L})[\ell] = K_1(\mathscr{L})[\ell] \times K_2(\mathscr{L})[\ell]$ be the induced decomposition of the ℓ-torsion part of $K(\mathscr{L})$. Let B_k be the quotient of A_k by $K_2(\mathscr{L})[\ell]$ and C_k be the quotient of A_k by $K_1(\mathscr{L})[\ell]$. In this paper, we show that the theta structure of type $\overline{\ell n}$ of A_k induces in a natural manner theta structures of type $\overline{n}$ on B_k and C_k. As a consequence, we obtain a modular correspondence, $\Phi_\ell : \mathcal{M}_{\overline{\ell n}} \to \mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}$. In the projective coordinate system provided by theta constants, we give a system

of equations for the image of $\mathcal{M}_{\overline{\ell n}}$ in the product $\mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}$ as well as an efficient algorithm to compute, given the theta null point $(b_u)_{u \in Z(\overline{n})}$ of B_k with a theta structure of type $\overline{n}$, all the theta null points $(c_u)_{u \in Z(\overline{n})}$ of C_k with a theta structure of type $\overline{n}$ such that $((b_u)_{u \in Z(\overline{n})}, (c_u)_{u \in Z(\overline{n})})$ is in the image of Φ_ℓ. It should be remarked that in genus 1 our notion of modular correspondence does not coincide with the definition of [Koh03] which gives a parametrisation of ℓ-isogenies while with our definition with obtain a parametrisation of ℓ^2-isogenies. Still in the case of genus 1, our modular correspondence can be used in the aforementioned applications.

This paper is organized as follows. In Section 2 we recall some basic definitions and properties relating to algebraic theta functions. In Section 3, we define formally the modular correspondence, and then in Section 4 we give explicit equations for the computation of this correspondence. In particular, given the theta null an abelian variety B_k with an $\overline{n}$-marking, we define a polynomial system (the equations of the image of $\mathcal{M}_{\overline{\ell n}}$), of which the solutions give theta null points of varities isogenous to B_k. In Section 5, we describe the geometry of these solutions. The last section is devoted to the description of a fast algorithm compute the solutions.

2 Some notations and basic facts

In this section, we fix some notations for the rest of the paper and recall well known results on abelian varieties and theta structures.

Let A_k be a g-dimensional abelian variety over a field k. Let $\mathscr{L}$ be a degree-d ample symmetric line bundle on A_k. From here, we suppose that d is prime to the characteristic of k. Denote by $K(\mathscr{L})$ the group given by the geometric points in the kernel of the polarization corresponding to $\mathscr{L}$ and by $G(\mathscr{L})$ the theta group (see [Mum66, p. 289]) associated to $\mathscr{L}$. For x a geometric point of A_k, we denote by τ_x the translation by x map on A_k. The theta group $G(\mathscr{L})$ (see the definition of [Mum66, p. 289]) is by definition the group (representable by a group scheme by [Mum84, prop. 1]) given by the set of pairs (x, ψ), where x is a point of $K(\mathscr{L})$ and ψ is an isomorphism of line bundles $\psi : \mathscr{L} \to \tau_x^* \mathscr{L}$, together with the composition law $(x, \psi) \circ (y, \varphi) = (x + y, \tau_y^* \psi \circ \varphi)$. Let $\delta = (\delta_1, \ldots, \delta_g)$ be a finite sequence of integers such that $\delta_i | \delta_{i+1}$. We consider the finite group $Z(\delta) = (\mathbb{Z}/\delta_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/\delta_g\mathbb{Z})$ with elementary divisors given by δ. For a well chosen unique δ, the finite group $K(\delta) = Z(\delta) \times \hat{Z}(\delta)$ (where $\hat{Z}(\delta)$ is the Cartier dual of $Z(\delta)$) is isomorphic to $K(\mathscr{L})$ (see [Mum70a, p. 132]). We note $\mathbb{G}_{m,k}$ the group $\overline{k}^*$. The Heisenberg group of type δ is the group $\mathcal{H}(\delta) = \mathbb{G}_{m,k} \times Z(\delta) \times \hat{Z}(\delta)$ together with the group law defined on points by $(\alpha, x_1, x_2).(\beta, y_1, y_2) = (\alpha.\beta.y_2(x_1), x_1 + y_1, x_2 + y_2)$. We recall (see [Mum66, cor. of Th. 1, p. 294]) that a theta structure Θ_δ of type δ is an isomorphism of central

extensions from $\mathcal{H}(\delta)$ to $G(\mathscr{L})$ fitting in the following diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_{m,k} & \longrightarrow & \mathcal{H}(\delta) & \longrightarrow & K(\delta) & \longrightarrow & 0\ , \\ & & \| & & \downarrow{\scriptstyle \Theta_\delta} & & \downarrow{\scriptstyle \overline{\Theta}_\delta} & & \\ 0 & \longrightarrow & \mathbb{G}_{m,k} & \longrightarrow & G(\mathscr{L}) & \xrightarrow{\kappa} & K(\mathscr{L}) & \longrightarrow & 0 \end{array} \tag{1}$$

where κ is the natural projection.

We note that Θ_δ induces an isomorphism, denoted $\overline{\Theta}_\delta$ in the preceding diagram, from $K(\delta)$ into $K(\mathscr{L})$ and as a consequence a decomposition $K(\mathscr{L}) = K_1(\mathscr{L}) \times K_2(\mathscr{L})$ where $K_2(\mathscr{L})$ is the Cartier dual of $K_1(\mathscr{L})$. As it will be explained shortly, the data of a triple $(A_k, \mathscr{L}, \Theta_\delta)$ defines a basis of global sections of $\mathscr{L}$ that we denote $(\vartheta_i)_{i\in Z(\delta)}$ and as a consequence an morphism of A_k into $\mathbb{P}_k^{d-1}$ where $d = \prod_{i=1}^g \delta_i$ is the degree of $\mathscr{L}$. We recall the construction of this basis. We recall ([Mum66, p. 291]) that a level subgroup $\tilde{K}$ of $G(\mathscr{L})$ is a subgroup such that $\tilde{K}$ is isomorphic to its image by κ in $K(\mathscr{L})$ where κ is defined in (1). We define the maximal level subgroups $\tilde{K}_1$ over $K_1(\mathscr{L})$ and $\tilde{K}_2$ over $K_2(\mathscr{L})$ as the image by Θ_δ of the subgroups $(1, x, 0)_{x\in Z(\delta)}$ and $(1, 0, y)_{y\in \hat{Z}(\delta)}$ of $\mathcal{H}(\delta)$. Let A_k^0 be the quotient of A_k by $K_2(\mathscr{L})$ and $\pi : A_k \to A_k^0$ be the natural projection. By the descent theory of Grothendieck (see [Mum66, p. 290]), the data of $\tilde{K}_2$ is equivalent to the data of a couple $(\mathscr{L}_0, \lambda)$ where $\mathscr{L}_0$ is a degree-one ample line bundle on A_k^0 and λ is an isomorphism $\lambda : \pi^*(\mathscr{L}_0) \to \mathscr{L}$. Let s_0 be the unique global section of $\mathscr{L}_0$ up to a constant factor and let $s = \lambda(\pi^*(s_0))$. We have the following proposition which is an immediate consequence of [Mum66, th. 2 p. 297] and Step I of [Mum66]:

Proposition 1: *For all $i \in Z(\delta)$, let $(x_i, \psi_i) = \Theta_\delta((1, i, 0))$. We set $\vartheta_i^{\Theta_\delta} = (\tau_{-x_i}^* \psi_i(s))$. The elements $(\vartheta_i^{\Theta_\delta})_{i\in Z(\delta)}$ form a basis of the global sections of $\mathscr{L}$ which is uniquely determined, up to a multiplication by a factor independent of i, by the data of Θ_δ.*

If no ambiguity is possible, we let $\vartheta_i^{\Theta_\delta} = \vartheta_i$ for $i \in Z(\delta)$.

The image of the zero point 0 of A_k by the projective embeding defined by Θ_δ, which has homogeneous coordinates $(\vartheta_i(0))_{i\in Z(\delta)}$, is by definition the *theta null point* associated to $(A_k, \mathscr{L}, \Theta_\delta)$. If Θ_δ is symmetric [Mum66, p. 308 and p. 317], we say that $(A_k, \mathscr{L}, \Theta_\delta)$ is an abelian variety with a δ-marking. The locus of the theta null points associated to abelian varieties with a δ-marking is a quasi-projective variety denoted $\mathcal{M}_\delta$.

Let $(A_k, \mathscr{L}, \Theta_\delta)$ be an abelian variety with a δ-marking. We recall that the natural action of $G(\mathscr{L})$ on the global sections of $\mathscr{L}$ is given by $(x, \psi).f = \tau_{-x}^* \psi(f)$ for $f \in \Gamma(\mathscr{L})$ and $(x, \psi) \in G(\mathscr{L})$. There is an action of $\mathcal{H}(\delta)$ on the global sections of $\mathscr{L}$. After an immediate computation using the group law of $\mathcal{H}(\delta)$ and the definition of $(\vartheta_i)_{i\in Z(\delta)}$ given by Proposition 1, on obtains the following expression for this action:

$$(\alpha, i, j).\vartheta_m = \alpha e_\delta(m + i, -j)\vartheta_{m+i}, \tag{2}$$

for $(\alpha, i, j) \in \mathcal{H}(\delta)$ and e_δ the commutator pairing on $K(\delta)$. By construction, this action is compatible via Θ_δ with the natural action of $G(\mathscr{L})$ on $(\vartheta_i)_{i\in Z(\delta)}$. Using (2), one can compute the coordinates in the projective system given by the $(\vartheta_i)_{i\in Z(\delta)}$ of any point of $K(\mathscr{L})$ from the theta null point associated to $(A_k, \mathscr{L}, \Theta_\delta)$. Indeed, let $(x, \psi) \in G(\mathscr{L})$ be any lift of $x \in K(\mathscr{L})$ and let $(\alpha, i, j) = \Theta_\delta^{-1}((x, \psi))$ then the coordinates of x in the projective system given by the $(\vartheta_i)_{i\in Z(\delta)}$ are $((\alpha, i, j).\vartheta_m)(0))_{m\in Z(\delta)}$.

For $\delta = (\delta_1, \ldots, \delta_g) \in \mathbb{N}^g$ and $\delta' = (\delta'_1, \ldots, \delta'_g) \in \mathbb{N}^g$, we write $\delta|\delta'$ if for $i = 1, \ldots, g$, we have $\delta_i|\delta'_i$. If $n \in \mathbb{N}$, then $n|\delta$ means that $n|\delta_i$ for all i. If $\delta|\delta'$, then we have the usual embedding

$$i : Z(\delta) \to Z(\delta'), (x_i)_{i\in\{1,\ldots,g\}} \mapsto (\delta'_i/\delta_i.x_i). \tag{3}$$

A basic ingredient of our algorithm is given by the Riemann relations which are algebraic relations satisfied by the theta null values if $2|\delta$.

Theorem 2 (Mumdord [Mum66] p. 333): *Denote by $\hat{Z}(\overline{2})$ the dual group of $Z(\overline{2})$. Let $(a_i)_{i\in Z(\delta)}$ be the theta null point associated to an abelian variety with a δ-marking $(A_k, \mathscr{L}, \Theta_\delta)$ where $2|\delta$ and δ is not divisible by the characteristic of k. For all $x, y, u, v \in Z(2\delta)$ that are congruent modulo $2Z(2\delta)$, and all $\chi \in \hat{Z}(\overline{2})$, we have*

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

Here we embed $Z(\overline{2})$ into $Z(\delta)$ and $Z(\delta)$ into $Z(2\delta)$ using (3).

Remark 3: It is moreover proved in [Mum66, Cor. p. 349] that if $4|\delta$ the image of A_k by the projective morphism defined by Θ_δ is the closed subvariety of $\mathbb{P}_k^{d-1}$ defined by the homogeneous ideal generated by the relations of Theorem 2. (This result can be sharpened, see [Kem89, Section 8]).

A consequence of Theorem 2 is the fact that if $4|\delta$, from the knowledge of a valid theta null point $(a_i)_{i\in Z(\delta)}$, one can recover a couple $(A_k, \mathscr{L})$ which it comes from. In fact, the abelian variety A_k is defined by the homogeneous equations of Theorem 2. Moreover, from the knowledge of the projective embedding of A_k, one recover immediately $\mathscr{L}$ by pulling back the sheaf $\mathcal{O}(1)$ of the projective space.

An immediate consequence of the preceding theorem is the

Theorem 4: *Let $(a_i)_{i\in Z(\delta)}$ be the theta null point associated to an abelian variety with a δ-marking $(A_k, \mathscr{L}, \Theta_\delta)$ where $2|\delta$. For all $x, y, u, v \in Z(2\delta)$ that are congruent modulo $2Z(2\delta)$, and all $\chi \in \hat{Z}(\overline{2})$, we have*

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

As Θ_δ is symmetric, the theta constants also satisfy the additional symmetry relations $a_i = a_{-i}$, $i \in Z(\delta)$.

Theorem 4 gives equations satisfied by the theta null points of abelian varieties together with a δ-marking. Let $\overline{\mathcal{M}}_\delta$ be the projective variety over k defined by the relations from Theorem 4. Mumford proved in [Mum67a, p. 83] the following

Theorem 5: *Suppose that* $8|\delta$. *Then*

1. *$\mathcal{M}_\delta$ is a classifying space for abelian varieties with a δ-marking: to a theta null point corresponds a unique triple $(A_k, \mathscr{L}, \Theta_\delta)$.*
2. *$\mathcal{M}_\delta$ is an open subset of $\overline{\mathcal{M}}_\delta$.*

A geometric point P of $\overline{\mathcal{M}}_\delta$ is called a theta constant. If a theta constant P is in $\mathcal{M}_\delta$ we say that P is a valid theta null point, otherwise we say that P is a degenerate theta null point.

Remark 6: As the results of Section 5 show, $\overline{\mathcal{M}}_\delta$ may not be a projective closure of $\mathcal{M}_\delta$. Nonetheless, every degenerate theta null point can be obtained from a valid theta null point by a "degenerate" group action (see the discussion after Proposition 18), hence the terminology.

3 Theta null points and isogenies

Let k be a field. Let ℓ and n be relatively prime integers and suppose that n is divisible by 2 and that $n\ell$ is prime to the characteristic of k. Let $(A_k, \mathscr{L}, \Theta^A_{\overline{\ell n}})$ be a g-dimensional abelian variety together with an $(\overline{\ell n})$-marking. We recall from just above Proposition 1 that the theta structure $\Theta^A_{\overline{\ell n}}$ induces a decomposition of the kernel of the polarization

$$K(\mathscr{L}) = K_1(\mathscr{L}) \times K_2(\mathscr{L}) \tag{4}$$

into maximal isotropic subgroups for the commutator pairing associated to $\mathscr{L}$. Let K be either $K_1(\mathscr{L})[\ell]$ or $K_2(\mathscr{L})[\ell]$. There are two possible choices for K, one contained in $K_1(\mathscr{L})$, the other one in $K_2(\mathscr{L})$. In the next subsection, we explain that a choice of K determines a certain abelian variety together with an $\overline{n}$-marking. The main results of this section are Corollary 8 and Proposition 9, which explain how its theta null point is related to A.

3.1 The isogenies defined by K

Let X_k be the quotient of A_k by K and let $\pi : A_k \to X_k$ be the natural projection. Let $\kappa : G(\mathscr{L}) \to K(\mathscr{L})$ be the natural projection. As K is a subgroup of $K(\mathscr{L})$, we can consider the subgroup G of $G(\mathscr{L})$ defined as $G = \kappa^{-1}(K)$. Let $\tilde{K}$ be the level subgroup of $G(\mathscr{L})$ defined as the intersection of G with the image of $(1, x, y)_{(x,y)\in Z(\overline{\ell n})\times \hat{Z}(\overline{\ell n})} \subset \mathcal{H}(\overline{\ell n})$ by $\Theta^A_{\overline{\ell n}}$. By the descent theory of Grothendieck,

we know that the data of $\tilde{K}$ is equivalent to the data of a line bundle $\mathscr{X}$ on X_k and an isomorphism $\lambda : \pi^*(\mathscr{X}) \to \mathscr{L}$.

Now, we explain that the $(\overline{\ell n})$-marking on A_k induces an $\overline{n}$-marking on X_k. Let $G^*(\mathscr{L})$ be the centralizer of $\tilde{K}$ in $G(\mathscr{L})$. Applying [Mum66, Proposition 2 p. 291], we obtain an isomorphism

$$G^*(\mathscr{L})/\tilde{K} \simeq G(\mathscr{X}) \tag{5}$$

and as a consequence a natural projection $q : G^*(\mathscr{L}) \to G(\mathscr{X})$.

As $\mathcal{H}(\overline{n})$ is generated by the subgroups $\mathbb{G}_m \times 0 \times 0$, $1_{\mathbb{G}_m} \times Z(\overline{n}) \times 0_{\hat{Z}(\overline{n})}$ and $1_{\mathbb{G}_m} \times 0_{Z(\overline{n})} \times \hat{Z}(\overline{n})$, in order to define a theta structure $\Theta^B_{\overline{n}} : \mathcal{H}(\overline{n}) \to G(\mathscr{X})$, it is enough to give morphisms $1_{\mathbb{G}_m} \times Z(\overline{n}) \times 0_{\hat{Z}(\overline{n})} \to G(\mathscr{X})$ and $1_{\mathbb{G}_m} \times 0_{Z(\overline{n})} \times \hat{Z}(\overline{n}) \to G(\mathscr{X})$ such that the resulting $\Theta^B_{\overline{n}}$ is an isomorphism. Let $Z^*(\overline{\ell n})$, $\hat{Z}^*(\overline{\ell n})$, K_1^* and K_2^* be such that

$$1_{\mathbb{G}_m} \times Z^*(\overline{\ell n}) \times 0_{\hat{Z}(\overline{\ell n})} = {\Theta^A_{\overline{\ell n}}}^{-1}(G^*(\mathscr{L})) \cap (1_{\mathbb{G}_m} \times Z(\overline{\ell n}) \times 0_{\hat{Z}(\overline{\ell n})}),$$

$$1_{\mathbb{G}_m} \times 0_{Z(\overline{\ell n})} \times \hat{Z}^*(\overline{\ell n}) = {\Theta^A_{\overline{\ell n}}}^{-1}(G^*(\mathscr{L})) \cap (1_{\mathbb{G}_m} \times 0_{Z(\overline{\ell n})} \times \hat{Z}(\overline{\ell n})),$$

$$1_{\mathbb{G}_m} \times K_1^* \times 0_{\hat{Z}(\overline{\ell n})} = {\Theta^A_{\overline{\ell n}}}^{-1}(\tilde{K}) \cap (1_{\mathbb{G}_m} \times Z(\overline{\ell n}) \times 0_{\hat{Z}(\overline{\ell n})}),$$

$$1_{\mathbb{G}_m} \times 0_{Z(\overline{\ell n})} \times K_2^* = {\Theta^A_{\overline{\ell n}}}^{-1}(\tilde{K}) \cap (1_{\mathbb{G}_m} \times 0_{Z(\overline{\ell n})} \times \hat{Z}(\overline{\ell n})).$$

There are natural isomorphisms $Z^*(\overline{\ell n})/K_1^* \simeq Z(\overline{n})$ and $\hat{Z}^*(\overline{\ell n})/K_2^* \simeq \hat{Z}(\overline{n})$ from which we deduce projections $p_1 : Z^*(\overline{\ell n}) \to Z(\overline{n})$ and $p_2 : \hat{Z}^*(\overline{\ell n}) \to \hat{Z}(\overline{n})$ (compare with the diagram of [Mum67a, p. 303]).

We define $\Theta^B_{\overline{n}}$ as the unique theta structure for $\mathscr{X}$ such that the following diagrams are commutative

$$\begin{array}{ccc} (1,x,0)_{x \in Z^*(\overline{\ell n})} & \xrightarrow{\Theta^A_{\overline{\ell n}}} & G^*(\mathscr{L}) \\ \downarrow{\scriptstyle \tilde{p}_1} & & \downarrow{\scriptstyle q} \\ (1,x,0)_{x \in Z(\overline{n})} & \xrightarrow{\Theta^B_{\overline{n}}} & G(\mathscr{X}) \end{array}, \tag{6}$$

$$\begin{array}{ccc} (1,0,y)_{y \in \hat{Z}^*(\overline{\ell n})} & \xrightarrow{\Theta^A_{\overline{\ell n}}} & G^*(\mathscr{L}) \\ \downarrow{\scriptstyle \tilde{p}_2} & & \downarrow{\scriptstyle q} \\ (1,0,y)_{y \in \hat{Z}(\overline{n})} & \xrightarrow{\Theta^B_{\overline{n}}} & G(\mathscr{X}) \end{array}, \tag{7}$$

where $\tilde{p}_1$ is induced by p_1 and $\tilde{p}_2$ is induced by p_2. Using the fact that $\Theta^A_{\overline{\ell n}}$ is symmetric, it is easy to see that $\Theta^B_{\overline{n}}$ is also symmetric.

We say that the theta structures $\Theta^A_{\overline{\ell n}}$ and $\Theta^B_{\overline{n}}$ are π-compatible (or compatible) if the diagrams (6) and (7) commute.

Let K_1 and K_2 be the maximal ℓ-torsion subgroups of respectively $K_1(\mathscr{L})$ and $K_2(\mathscr{L})$. By taking $K = K_2$ and $K = K_1$ in the preceding construction, we obtain respectively $(B_k, \mathscr{L}_0, \Theta^B_{\overline{n}})$ and $(C_k, \mathscr{L}_1, \Theta^C_{\overline{n}})$ two abelian varieties with an $\overline{n}$-marking. As a consequence, we have a well defined modular correspondence

$$\Phi_\ell : \mathcal{M}_{\overline{\ell n}} \to \mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}. \tag{8}$$

Let $\pi : A_k \to B_k$ and $\pi' : A_k \to C_k$ be the isogenies from the construction. Let $[\ell]$ be the isogeny of multiplication by ℓ on B_k and let $\hat{\pi} : B_k \to A_k$ be the isogeny such that $[\ell] = \pi \circ \hat{\pi}$. From the symmetry of $\mathscr{L}$ we deduce that $\mathscr{L}_0$ is symmetric and by applying the formula of [Mum66, p. 289], we have $[\ell]^* \mathscr{L}_0 = \mathscr{L}_0^{\ell^2}$. Denote by $K_{\pi'}$ the kernel of π'. Then $\pi(K_{\pi'}) = \pi(A_k[\ell])$ so this subgroup of B_k is exactly the kernel of $\hat{\pi}$:

$$\begin{array}{ccccc} B_k & & \xrightarrow{\hat{\pi}} & & \\ \downarrow{\scriptstyle [\ell]} & & & A_k & \\ & \swarrow{\scriptstyle \pi} & & & \searrow{\scriptstyle \pi'} \\ B_k & & & & C_k \end{array} \tag{9}$$

3.2 The theta null points defined by K

The following two propositions explain the relation between the theta null point of $(A_k, \mathscr{L}, \Theta^A_{\overline{\ell n}})$ and the theta null points of $(B_k, \mathscr{L}_0, \Theta^B_{\overline{n}})$ and $(C_k, \mathscr{L}_1, \Theta^C_{\overline{n}})$. Keeping the notations of the previous paragraph, we have

Proposition 7: *Let $(A_k, \mathscr{L}, \Theta^A_{\overline{\ell n}})$, $(B_k, \mathscr{L}_0, \Theta^B_{\overline{n}})$ and $\pi : A_k \to B_k$ be defined as above. There exists a constant factor $\omega \in \overline{k}$ such that for all $i \in Z(\overline{n})$, we have*

$$\pi^*(\vartheta_i^{\Theta^B_{\overline{n}}}) = \omega \vartheta_i^{\Theta^A_{\overline{\ell n}}}. \tag{10}$$

In this identity, $Z(\overline{n})$ is identified with a subgroup of $Z(\overline{\ell n})$ via the map $x \mapsto \ell x$.

Proof: The theta structure $\Theta^A_{\overline{\ell n}}$ (resp. $\Theta^B_{\overline{n}}$) induces a decomposition of the kernel of the polarization $K(\mathscr{L}) = K_1(\mathscr{L}) \times K_2(\mathscr{L})$ (resp. $K(\mathscr{L}_0) = K_1(\mathscr{L}_0) \times K_2(\mathscr{L}_0)$). Denote by K_2 the kernel of π. We have that K_2 is a subgroup of $K(\mathscr{L})$ contained in $K_2(\mathscr{L})$.

The hypotheses of [Mum66, Th. 4] are verified by construction of $\Theta^B_{\overline{n}}$ and Equation (10) is an immediate application of this theorem. ∎

As an immediate consequence of the preceding proposition, we have

Corollary 8: *Let $(A_k, \mathscr{L}, \Theta^A_{\overline{\ell n}})$ and $(B_k, \mathscr{L}_0, \Theta^B_{\overline{n}})$ be defined as above. Let $(a_u)_{u \in Z(\overline{\ell n})}$ and $(b_u)_{u \in Z(\overline{n})}$ be theta null points respectively associated to $(A_k, \mathscr{L}, \Theta^A_{\overline{\ell n}})$ and $(B_k, \mathscr{L}_0, \Theta^B_{\overline{n}})$. Considering $Z(\overline{n})$ as a subgroup of $Z(\overline{\ell n})$ via the map $x \mapsto \ell x$, there exists a constant factor $\omega \in \overline{k}$ such that for all $u \in Z(\overline{n})$, $b_u = \omega a_u$.*

Proposition 9: *Let* $(A_k, \mathscr{L}, \Theta^A_{\overline{\ell n}})$ *and* $(C_k, \mathscr{L}_0, \Theta^B_{\overline{n}})$ *be defined as above. Let* $(a_u)_{u\in Z(\overline{\ell n})}$ *and* $(c_u)_{u\in Z(\overline{n})}$ *be the theta null points respectively associated to* $(A_k, \mathscr{L}, \Theta^A_{\overline{\ell n}})$ *and* $(C_k, \mathscr{L}_1, \Theta^C_{\overline{n}})$. *We have for all* $u \in Z(\overline{n})$,

$$c_u = \sum_{t\in Z(\overline{\ell})} a_{u+t}, \tag{11}$$

where $Z(\overline{n})$ *and* $Z(\overline{\ell})$ *are considered as subgroups of* $Z(\overline{\ell n})$ *via the maps* $j \mapsto \ell j$ *and* $j \mapsto nj$.

Proof: The proof follows the same line as that of Proposition 7. The theta structure $\Theta^A_{\overline{\ell n}}$ (resp. $\Theta^C_{\overline{n}}$) induces a decomposition of the kernel of the polarization $K(\mathscr{L}) = K_1(\mathscr{L}) \times K_2(\mathscr{L})$ (resp. $K(\mathscr{L}_1) = K_1(\mathscr{L}_1) \times K_2(\mathscr{L}_1)$). Denote by K_1 the kernel of π'. We have that K_1 is a subgroup of $K_1(\mathscr{L})$ and we have an isomorphism:

$$\sigma' : K_1(\mathscr{L})/K_1 \to K_1(\mathscr{L}_1),$$

which translate via $\Theta^A_{\overline{\ell n}}$ and $\Theta^C_{\overline{n}}$ into the natural isomorphism

$$\sigma'_0 : Z(\overline{\ell n})/Z(\overline{\ell}) \to Z(\overline{n}).$$

The hypotheses of [Mum66, Th. 4] are then verified and Equation (11) is an immediate application of this theorem. ■

4 The image of the modular correspondence

In this section, we use the results of the previous section in order to give equations for the image of the modular correspondence Φ_ℓ given by (8). That is, for a given point x of $\mathcal{M}_{\overline{n}}$, we give equations for the set of points in $\mathcal{M}_{\overline{n}}$ that correspond to x via the map defined by $\Phi_\ell(\mathcal{M}_{\overline{\ell n}})$.

In order to make this precise, we let $(B_k, \mathscr{L}_0, \Theta^B_{\overline{n}})$ be an abelian variety together with an $\overline{n}$-marking and denote by $(b_u)_{u\in Z(\overline{n})}$ its associated theta null point. Unless specified, we shall assume that $4 \mid n$.

Denote by p_1 (resp. p_2) the first (resp. second) projection from $\mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}$ into $\mathcal{M}_{\overline{n}}$, and let $\pi_1 = p_1 \circ \Phi_\ell$, $\pi_2 = p_2 \circ \Phi_\ell$. We would like to compute the algebraic set $\pi_2(\pi_1^{-1}((b_u)_{u\in Z(\overline{n})}))$ which we call the *image of the modular correspondence*. We remark that this question is the analog in our situation of the computation of the solutions of the equation $\Phi_\ell(j, X)$ obtained by substituting in the modular polynomial Φ_ℓ a certain j-invariant $j \in \overline{k}$. The only difference is that our modular correspondence parametrizes ℓ^2-isogenies while the usual one deals with ℓ-isogenies.

Let $\mathbb{P}_k^{Z(\overline{\ell n})} = \mathrm{Proj}(k[x_u | u \in Z(\overline{\ell n})])$ be the ambient projective space of $\overline{\mathcal{M}}_{\overline{\ell n}}$, and let I be the homogeneous ideal defining $\overline{\mathcal{M}}_{\overline{\ell n}}$, which is spanned by the relations of Theorem 4, together with the symmetry relations. Let J be the image of I under the specialization map

$$k[x_u | u \in Z(\overline{\ell n})] \to k[x_u | u \in Z(\overline{\ell n}), nu \neq 0], \quad x_u \mapsto \begin{cases} b_u, & \text{if} \quad u \in Z(\overline{n}) \\ x_u, & \text{else} \end{cases}.$$

and let V_J be the affine variety defined by J.

Let $\tilde{\pi}_1^0 : \mathbb{P}_k^{Z(\overline{\ell n})} \to \mathbb{P}_k^{Z(\overline{n})}$ and $\tilde{\pi}_2^0 : \mathbb{P}_k^{Z(\overline{\ell n})} \to \mathbb{P}_k^{Z(\overline{n})}$ be the rational maps of the ambient projective spaces respectively defined on geometric points by $(a_u)_{u\in Z(\overline{\ell n})} \mapsto (a_u)_{u\in Z(\overline{n})}$ and $(a_u)_{u\in Z(\overline{\ell n})} \mapsto (\sum_{t\in Z(\overline{\ell})} a_{u+t})_{u\in Z(\overline{n})}$. Clearly, π_1 and π_2 are the restrictions of $\tilde{\pi}_1^0$ and $\tilde{\pi}_2^0$ to $\mathcal{M}_{\overline{\ell n}}$. The rational map $\tilde{\pi}_1^0$ (resp $\tilde{\pi}_2^0$) restricts to a rational map $\tilde{\pi}_1 : \overline{\mathcal{M}_{\overline{\ell n}}} \to \overline{\mathcal{M}_{\overline{n}}}$ (resp $\tilde{\pi}_2 : \overline{\mathcal{M}_{\overline{\ell n}}} \to \overline{\mathcal{M}_{\overline{n}}}$). By definition of J, we have $V_J = \tilde{\pi}_1^{-1}((b_u)_{u\in Z(\overline{n})})$.

Let $S = k[y_u, x_v | u \in Z(\overline{n}), v \in Z(\overline{\ell n})]$, we can consider J as a subset of S via the natural inclusion of $k[x_u | u \in Z(\overline{\ell n})]$ into S. Let $\mathcal{L}'$ be the ideal of S generated by J together with the elements $y_u - \sum_{t\in Z(\overline{\ell})} x_{u+t}$ and let $\mathcal{L} = \mathcal{L}' \cap k[y_u | u \in Z(\overline{n})]$. Let $V_{\mathcal{L}}$ be the subvariety of $\mathbb{A}^{Z(\overline{n})}$ defined by the ideal $\mathcal{L}$. By the definition of $\mathcal{L}$, $V_{\mathcal{L}}$ is the image by $\tilde{\pi}_2$ of the fiber V_J, so that $V_{\mathcal{L}} = \tilde{\pi}_2(\tilde{\pi}_1^{-1}((b_u)_{u\in Z(\overline{n})}))$.

Proposition 10: *Keeping the notations from above, we suppose that* $4 \mid n$ *and let* $(b_u)_{u\in Z(\overline{n})}$ *be the geometric point of* $\mathcal{M}_{\overline{n}}$ *corresponding to* $(B_k, \mathscr{L}_0, \Theta_{\overline{n}}^B)$*. The algebraic variety* $V_{\mathcal{L}}^0 = \pi_2(\pi_1^{-1}(b_u)_{u\in Z(\overline{n})})$ *has dimension* 0 *and is isomorphic to a subvariety of* $V_{\mathcal{L}}$*.*

Proof: From the preceding discussion the only thing left to prove is that $V_{\mathcal{L}}^0$ has dimension 0. But this follows from the fact that the algebraic variety V_J has dimension 0 [CL09, Th. 2.7] which generalize easily to the case where n is not a power of 2. ■

From an algorithmic point of view, with our method the hard part of the computation of the modular correspondence is the computation of $V_J^0 = \pi_1^{-1}((b_u)_{u\in Z(\overline{n})})$, the set of points in V_J that are valid theta null points. From now on, we consider only V_J^0, since computing $V_{\mathcal{L}}^0$ from it is trivial by Proposition 9.

We proceed in two steps. First we compute the solutions in V_J using a specialized Gröbner basis algorithm (Section 6.3) and then we detect the valid theta null points using the results of Section 5 (see Theorem 23). But first we recall the moduli interpretation of V_J^0 given by Section 3:

Proposition 11: *We suppose that* $4 \mid n$*, then* V_J^0 *is the locus of theta null points* $(a_u)_{u\in Z(\overline{\ell n})}$ *in* $\mathcal{M}_{\overline{\ell n}}$ *such that if* $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ *is the corresponding variety with an* $(\overline{\ell n})$*-marking then* $\Theta_{\overline{\ell n}}^A$ *is compatible with the theta structure* $\Theta_{\overline{n}}^B$ *of* B_k*.*

Proof: Let $(a_u)_{u\in Z(\overline{\ell n})}$ be a geometric point of V_J^0. Let $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ be a corresponding variety with $(\overline{\ell n})$-marking. If we apply the construction of Section 3, we get an abelian variety $(B'_k, \mathscr{L}'_0, \Theta'_{\overline{n}})$ with an $\overline{n}$-marking and an isogeny $\pi : A_k \to B'_k$ such that $\Theta_{\overline{\ell n}}^A$ is compatible with $\Theta'_{\overline{n}}$. By definition of J, Corollary 8 shows that the theta null point of B' is $(b_u)_{u\in Z(\overline{n})}$. As $4 \mid n$, the paragraph directly below Theorem 2 shows that $(B'_k, \mathscr{L}'_0) \simeq (B_k, \mathscr{L}_0)$. By [Mum67b, p. 82] we then have that the triples $(B'_k, \mathscr{L}'_0, \Theta'_{\overline{n}})$ and $(B_k, \mathscr{L}_0, \Theta_{\overline{n}})$ are isomorphic, so that $\Theta_{\overline{\ell n}}^A$ is compatible with $\Theta_{\overline{n}}^B$. ■

5 The solutions of the system

Let B_k and V_J be as in the previous section. This section is devoted to the study of the geometric points of V_J. Our aim is twofold. First we need a way to identify degenerate theta null points in V_J, and then we would like to know when two geometric points in V_J correspond to isomorphic varieties.

If $(a_u)_{u\in Z(\overline{\ell n})}$ is a valid theta null point in V_J, let $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ be the corresponding abelian variety with an $(\overline{\ell n})$-marking and denote by $\pi : A_k \to B_k$ the isogeny defined in Section 3. We denote by $G((a_u)_{u\in Z(\overline{\ell n})})$ the subgroup $\pi(A_k[\ell])$ of B_k which is isomorphic to $Z(\overline{\ell})$. From the knowledge of $(a_u)_{u\in Z(\overline{\ell n})}$, one can recover the coordinates of the points $G((a_u)_{u\in Z(\overline{\ell n})})$. We study the image of the map G in Section 5.1, and study its fiber in Section 5.3. For this, we introduce an action of the automorphisms of the theta group $\mathcal{H}(\delta)$ on the modular space $\mathcal{M}_{\overline{\ell n}}$ in Section 5.2. In particular, we explain when two valid points give isomorphic varieties in Proposition 20. In Section 5.4 we extend the map $(a_u)_{u\in Z(\overline{\ell n})} \mapsto G((a_u)_{u\in Z(\overline{\ell n})})$ to non valid theta null point in V_J. The main result of this section is Theorem 23 which states that a geometric point of V_J is valid if and only if the associated subgroup is isomorphic to $Z(\overline{\ell})$. We then show how to obtain all degenerate points at the end of Section 5.4. In Section 5.5 we illustrate the previous results with some examples.

5.1 A group associated to valid theta null points of V_J

Suppose that $(a_v)_{v\in Z(\overline{\ell n})}$ is a valid theta null point in V_J^0. Let $(A_k, \mathscr{L}, \Theta^A_{\overline{\ell n}})$ be the corresponding abelian variety with an $(\overline{\ell n})$-marking and denote by $\pi : A_k \to B_k$ the isogeny defined in Section 3. We recall that the kernel of π is K_2, where $A[\ell] = K_1 \times K_2$ is the symplectic decomposition introduced in Section 3.1. Then $\pi(K_1)$ is the kernel of the contragredient isogeny $\hat{\pi} : B_k \to A_k$. We denote this kernel by $G((a_u)_{u\in Z(\overline{\ell n})})$. More explicitly, we can consider A_k as a closed subvariety of $\mathbb{P}_k^{Z(\overline{\ell n})}$ via the embedding provided by $\Theta^A_{\overline{\ell n}}$. Using the action (2) of the theta group on $(a_v)_{v\in Z(\overline{\ell n})}$, one sees that for $i \in Z(\overline{\ell})$, the point with homogeneous coordinates $(a_{v+ni})_{v\in Z(\overline{\ell n})}$ corresponds via $\overline{\Theta}^A_{\overline{\ell n}}$ to the point $\overline{\Theta}^A_{\overline{\ell n}}(i)$ of the ℓ-torsion subgroup K_1 of $A_k(\overline{k})$ (with the notations of Section 3). By definition of the isogeny π, we then have $G((a_u)_{u\in Z(\overline{\ell n})}) = \pi(K_1) = \{P_i, i \in Z(\overline{\ell})\}$, where $P_i = (a_{ni+\ell j})_{j\in Z(\overline{n})}$. We want to determine the set of such groups $G((a_u)_{u\in Z(\overline{\ell n})})$ as $(a_u)_{u\in Z(\overline{\ell n})}$ goes through the geometric points of V_J^0.

For this, let $\mathscr{M}_0 = [\ell]^*\mathscr{L}_0$ on B_k. As $\mathscr{L}_0$ is symmetric, we have that $\mathscr{M}_0 \simeq \mathscr{L}_0^{\ell^2}$ and as a consequence $K(\mathscr{M}_0)$, the kernel of $\mathscr{M}_0$ is isomorphic over $\overline{k}$ to $Z(\overline{\ell^2 n})$. The polarisation $\mathscr{M}_0$ induces a commutator pairing $e_{\mathscr{M}_0}$ on $K(\mathscr{M}_0)$ and as $\mathscr{M}_0$ descends to $\mathscr{L}_0$ via the isogeny $[\ell]$, we know that $e_{\mathscr{M}_0}$ is trivial on $B_k[\ell]$. For $x_1, x_2 \in B_k[\ell]$, let $x_1', x_2' \in B_k[\ell^2]$ be such that $\ell.x_i' = x_i$ for $i = 1, 2$. We remark that x_1' and x_2' are defined up to an element of $B_k[\ell]$. As a consequence, $e_{\mathscr{M}_0}(x_1', x_2) = e_{\mathscr{M}_0}(x_1, x_2')$, does not depend on the choice of x_1' and x_2' and

if we put $e_W(x_1, x_2) = e_{\mathscr{M}_0}(x_1', x_2)$, we obtain a well defined bilinear map $e_W : B_k[\ell] \times B_k[\ell] \to \overline{k}$. As $e_{\mathscr{M}_0}$ is a perfect pairing, for any $x_1' \in B_k[\ell^2]$ there exits $x_2' \in B_k[\ell^2]$ such that $e_{\mathscr{M}_0}(x_1', x_2')$ is a primitive ℓ^2th root of unity. As a consequence, for any $x_1 \in B_k[\ell]$ there exists $x_2 \in B_k[\ell]$ such that $e_W(x_1, x_2)$ is a primitive ℓ^{th} root of unity and e_W is also a perfect pairing. By [Mum70b, p. 228], the pairing e_W is the restriction of the commutator pairing $e_{\mathscr{L}_0^\ell}$ on $B_k[\ell] \times B_k[\ell]$. We then have:

Theorem 12: *Let G be a subgroup of $B_k[\ell]$. Then the following are equivalent:*

1. *there exists a geometric point $(a_u)_{u \in Z(\overline{\ell n})}$ of V_J^0 corresponding to a valid theta null point such that G equals $G((a_u)_{u \in Z(\overline{\ell n})})$;*
2. *G is an isotropic subgroup for the pairing e_W isomorphic to $Z(\overline{\ell})$.*

Proof: Let $(a_u)_{u \in Z(\overline{\ell n})}$ be a geometric point of V_J corresponding to a valid theta null point. We know that $(a_u)_{u \in Z(\overline{\ell n})}$ is the theta null point of a triple $(A_k, \mathscr{L}, \Theta^A_{\overline{\ell n}})$. The theta structure $\Theta^A_{\overline{\ell n}}$ induces a decomposition $K(\mathscr{L}) = K_1(\mathscr{L}) \times K_2(\mathscr{L})$ into isotropic subgroups for the commutator pairing $e_{\mathscr{L}}$. As the isogeny π is such that $\pi^*(\vartheta_i^{\Theta^B_{\overline{n}}}) = \vartheta_i^{\Theta^A_{\overline{\ell n}}}$ for all $i \in Z(\overline{n})$ (and identifying $i \in Z(\overline{n})$ with $\ell i \in Z(\overline{\ell n})$), we know that $G((a_u)_{u \in Z(\overline{\ell n})}) = \pi(K_1(\mathscr{L}))$. We denote by $\hat{\pi} : B_k \to A_k$ the isogeny such that $\pi \circ \hat{\pi} = [\ell]$ as in the diagram (9). For any $x_1, x_2 \in G((a_u)_{u \in Z(\overline{\ell n})})$, there exists $\overline{x}_1, \overline{x}_2 \in K_1(\mathscr{L})[\ell]$ such that $x_i = \pi(\overline{x}_i)$, $i = 1, 2$. Let $x_1' \in B_k[\ell^2]$ be such that $\ell . x_1' = x_1$. We have $e_W(x_1, x_2) = e_{\mathscr{M}_0}(x_1', x_2) = e_{\mathscr{L}}(\hat{\pi}(x_1'), \hat{\pi}(x_2))$. But $\hat{\pi}(x_2) = \hat{\pi} \circ \pi(\overline{x}_2) = [\ell](\overline{x}_2) = 0$. As a consequence, we have $e_W(x_1, x_2) = 0$.

Now, we prove the opposite direction. Let G be an ℓ-torsion subgroup of $B_k[\ell]$ isomorphic to $Z(\overline{\ell})$ which is isotropic for the pairing e_W and $\hat{G}$ be the dual group of G for the pairing e_W. As e_W is a perfect pairing, $\hat{G}$ is also a maximal rank g ℓ-torsion subgroup of $B_k[\ell]$. We want to show that G is of the form $G(x)$ with x a geometric point of V_J where J is defined by the triple $(B_k, \mathscr{L}_0, \Theta^B_{\overline{n}})$. For this, we consider the isogeny $\hat{\pi} : B_k \to A_k$ with kernel the subgroup G of B_k. As G is contained in $B_k[\ell]$, G is an isotropic subgroup of $(B_k, \mathscr{M}_0)$, and $\mathscr{M}_0$ descends via $\hat{\pi}$ to a polarization $\mathscr{L}$ on A_k. Let $\pi : A_k \to B_k$ be the isogeny with kernel $\hat{\pi}(\hat{G})$. By the commutativity of the following diagram,

$$\begin{array}{ccc} (B_k, \mathscr{M}_0) & & \\ & \searrow^{\hat{\pi}} & \\ \downarrow{\scriptstyle [\ell]} & & (A_k, \mathscr{L}) \\ & \swarrow_{\pi} & \\ (B_k, \mathscr{L}_0) & & \end{array} \quad , \tag{12}$$

$\mathscr{L}$ descends via π to $\mathscr{L}_0$.

The theta structure $\Theta^B_{\overline{n}}$ induces a decomposition $K(\mathscr{L}_0) = K_1(\mathscr{L}_0) \times K_2(\mathscr{L}_0)$. Let $x_i = \hat{\pi}(x'_i)$ with $x'_i \in \hat{G}$ and $i = 1, 2$. Let $y'_1 \in B_k[\ell^2]$ be such that $\ell.y'_1 = x'_1$. We have by hypothesis $1 = e_W(x'_1, x'_2) = e_{\mathscr{M}_0}(y'_1, x'_2)$ and as a consequence $1 = e_{\mathscr{M}_0}(x'_1, x'_2) = e_{\mathscr{L}}(x_1, x_2)$. Thus $\hat{\pi}(\hat{G})$ is isotropic for the pairing $e_{\mathscr{L}}$. As a consequence, we can chose a decomposition $K(\mathscr{L}) = K_1(\mathscr{L}) \times K_2(\mathscr{L})$ such that for $i = 1, 2$, $\pi(K_i(\mathscr{L})) = K_i(\mathscr{L}_0)$ and $K_2(\mathscr{L})[\ell] = \hat{\pi}(\hat{G})$. Take any theta structure $\Theta^A_{\overline{\ell n}}$ for $\mathscr{L}$ compatible with this decomposition. Let $(a_u)_{u \in Z(\overline{\ell n})}$ be the associated theta null point. By Corollary 8, $(a_u)_{u \in Z(\overline{\ell n})}$ is a geometric point of V_J. Moreover, we have $G((a_u)_{u \in Z(\overline{\ell n})}) = \pi(K_1(\mathscr{L})) = G$. ■

We want to study the structure of the fibres of a given subgroup G of $B_k[\ell]$, under the map $(a_u)_{u \in Z(\overline{\ell n})} \mapsto G((a_u)_{u \in Z(\overline{\ell n})})$ for $(a_u)_{u \in Z(\overline{\ell n})}$ a geometric point of V^0_J. For this we need to study how a theta null point varies with a change of theta structure.

5.2 The action of the theta group on V^0_J

We denote by $\mathrm{Aut}_{\mathbb{G}_\mathrm{m}} \mathcal{H}(\delta)$ the group of automorphisms ψ of $\mathcal{H}(\delta)$ inducing the identity on $\mathbb{G}_{m,k}$, i.e., the group of automorphisms ψ fitting in a diagram of the form

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_{m,k} & \longrightarrow & \mathcal{H}(\delta) & \longrightarrow & K(\delta) & \longrightarrow & 0\,. \\ & & \| & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \overline{\psi}} & & \\ 0 & \longrightarrow & \mathbb{G}_{m,k} & \longrightarrow & \mathcal{H}(\delta) & \longrightarrow & K(\delta) & \longrightarrow & 0 \end{array} \tag{13}$$

Obviously, the set of all theta structures for $\mathscr{L}$ is a principal homogeneous space for the group $\mathrm{Aut}_{\mathbb{G}_\mathrm{m}} \mathcal{H}(\delta)$ via the right action $\Theta_\delta.\psi = \Theta_\delta \circ \psi$ for $\psi \in \mathrm{Aut}_{\mathbb{G}_\mathrm{m}} \mathcal{H}(\delta)$ and Θ_δ a theta structure. So we can identify $\mathrm{Aut}_{\mathbb{G}_\mathrm{m}} \mathcal{H}(\delta)$ with the group of change of theta structures. If ψ is an automorphism fitting in diagram (13), it induces an automorphism $\overline{\psi}$ of $K(\delta)$. The commutativity of diagram (13) shows that $\overline{\psi}$ is symplectic with respect to the commutator pairing, i.e., we have for all $x_1, x_2 \in K(\delta)$, $e_\delta(\overline{\psi}(x_1), \overline{\psi}(x_2)) = e_\delta(x_1, x_2)$. Denote by $\mathrm{Sp}(K(\delta))$ the group of symplectic automorphisms of $K(\delta)$. In order to study the possible extensions of $\overline{\psi} \in \mathrm{Sp}(K(\delta))$ to an element of $\mathrm{Aut}_{\mathbb{G}_\mathrm{m}} \mathcal{H}(\delta)$ it is convenient to introduce the following definition:

Definition 13: *Let $\overline{\psi} \in \mathrm{Sp}(K(\delta))$. A $\overline{\psi}$-semi-character (or a semi-character if no confusion is possible) for the canonical pairing is a map $\chi_{\overline{\psi}} : K(\delta) \to \mathbb{G}_{m,k}$ such that for $(x_1, x_2), (x'_1, x'_2) \in K(\delta)$,*

$$\chi_{\overline{\psi}}((x_1 + x'_1, x_2 + x'_2)) = \chi_{\overline{\psi}}((x_1, x_2)).\chi_{\overline{\psi}}((x'_1, x'_2)).[\overline{\psi}(x'_1, x'_2)_2(\overline{\psi}(x_1, x_2)_1)], \tag{14}$$

where we write $\overline{\psi}(x_1, x_2) = (\overline{\psi}(x_1, x_2)_1, \overline{\psi}(x_1, x_2)_2)$ (resp. $\overline{\psi}(x'_1, x'_2) = (\overline{\psi}(x'_1, x'_2)_1, \overline{\psi}(x'_1, x'_2)_2)$ in the canonical decomposition of $K(\delta)$. A semi-character $\chi_{\overline{\psi}}$ is said to be symmetric if for all $(x_1, x_2) \in K(\delta)$, $\chi_{\overline{\psi}}(-(x_1, x_2)) = \chi_{\overline{\psi}}((x_1, x_2))$.

The preceding definition is motivated by the lemma:

Lemma 14: *Let $\psi \in \mathrm{Aut}_{\mathbb{G}_m} \mathcal{H}(\delta)$ and let $\overline{\psi}$ be the associated symplectic automorphism of $K(\delta)$. There exists a unique semi-character $\chi_{\overline{\psi}}$ such that for all $(\alpha, (x_1, x_2)) \in \mathcal{H}(\delta)$,*

$$\psi : (\alpha, (x_1, x_2)) \mapsto (\alpha \chi_{\overline{\psi}}((x_1, x_2)), \overline{\psi}((x_1, x_2))). \tag{15}$$

As a consequence, if $\overline{\psi} \in \mathrm{Sp}(K(\delta))$ there is a one on one correspondence between the set of extensions of $\overline{\psi}$ to $\mathrm{Aut}_{\mathbb{G}_m} \mathcal{H}(\delta)$ and the set of semi-characters.

Proof: Note that (15) uniquely defines a map $\chi_{\overline{\psi}}$ given ψ, and conversely, also uniquely defines a map ψ given $\overline{\psi}$ and $\chi_{\overline{\psi}}$. Moreover, by writing out the definitions, it follows that $\chi_{\overline{\psi}}$ is a semi-character if and only if ψ is a homomorphism. ■

Let $\overline{\psi} \in \mathrm{Sp}(K(\delta))$. If we want to show that $\overline{\psi}$ admits an extension to $\mathcal{H}(\delta)$, by the preceding lemma, it suffices to show that there exists a $\overline{\psi}$-semi-character.

Lemma 15: *Let $B = (v_\kappa, v_{\kappa+g})_{\kappa \in \{1,\dots,g\}}$ be a basis of $K(\delta)$. Let $\overline{\psi} \in \mathrm{Sp}(K(\delta))$. For $\kappa \in \{1, \dots, 2g\}$ let ℓ_κ be the order of v_κ in $K(\delta)$ and let t_κ be an ℓ_κ^{th}-root of unity. There exists a unique semi-character $\chi_{\overline{\psi}}$ such that $\chi_{\overline{\psi}}(v_\kappa) = t_\kappa$. Suppose that $2|\delta$, then this semi-character is symmetric if and only if for all $\kappa \in \{1, \dots, 2g\}$, $t_\kappa \in \{-1, 1\}$.*

Proof: By definition of a semi-character, there exists a function $\Phi : K(\delta) \times \mathbb{G}_{m,k} \times K(\delta) \times \mathbb{G}_{m,k} \to \mathbb{G}_{m,k}$ such that for every semi-character $\chi_{\overline{\psi}}$ and $x, y \in K(\delta)$ we have $\chi_{\overline{\psi}}(x + y) = \Phi(x, \chi_{\overline{\psi}}(x), y, \chi_{\overline{\psi}}(y))$. Recall that for $(u, v), (u', v') \in K(\delta)$, we have

$$e_\delta((u, v), (u', v')) = v'(u).v(u')^{-1}. \tag{16}$$

Using (15) and the fact that $\overline{\psi}$ is simplectic, we obtain that for $x, y \in K(\delta)$, $\Phi(x, \chi_{\overline{\psi}}(x), y, \chi_{\overline{\psi}}(y)) = \Phi(y, \chi_{\overline{\psi}}(y), x, \chi_{\overline{\psi}}(x))$. An easy computation shows that for $x, y, z \in K(\delta)$, $\Phi(x + y, \chi_{\overline{\psi}}(x + y), z, \chi_{\overline{\psi}}(z)) = \Phi(x, \chi_{\overline{\psi}}(x), y + z, \chi_{\overline{\psi}}(y + z))$. Moreover, we have $\chi_{\overline{\psi}}(0) = 1_{\mathbb{G}_{m,k}}$ and for $(u, v) \in K(\delta)$, $\chi_{\overline{\psi}}(-(u, v)) = \chi_{\overline{\psi}}((u, v))^{-1} \overline{\psi}(v)(\overline{\psi}(u))^{-1}$.

Let $\mathbb{Z}^B$ be the free commutative group over the basis B and denote by $\pi_0 : \mathbb{Z}^B \to K(\delta)$ the canonical projection. The preceding properties show that the map $B \to \mathbb{G}_{m,k}, v_\kappa \mapsto t_\kappa$ extends to a well defined semi-character $\tilde{\chi}_{\overline{\psi}} : \mathbb{Z}^B \to \mathbb{G}_{m,k}$ such that for $(u, v), (u', v') \in \mathbb{Z}^B$

$$\tilde{\chi}_{\overline{\psi}}((u + u', v + v')) = \tilde{\chi}_{\overline{\psi}}((u, v)).\tilde{\chi}_{\overline{\psi}}((u', v')).\overline{\psi}(\pi_0(v'))\overline{\psi}((\pi_0(u))).$$

In order to finish the proof, we just have to prove that $\tilde{\chi}$ induces a well defined map on $K(\delta)$. For this it is enough to prove that for all $x \in \ker \pi_0$, $\tilde{\chi}_{\overline{\psi}}(x) = 1$ and finaly we have to check that for all $i \in \{1, \dots, 2g\}$, $\tilde{\chi}_{\overline{\psi}}(\ell_i v_i) = 1$. But an easy recursion shows that for all $k \in \mathbb{N}$, $\tilde{\chi}_{\overline{\psi}}(k.v_i) = \tilde{\chi}_{\overline{\psi}}(v_i)^k$ and as a consequence, we

have that $\tilde{\chi}_{\overline{\psi}}(\ell_i.v_i) = 1$ if and only if $\tilde{\chi}_{\overline{\psi}}(v_i)$ is a ℓ_i^{th}-root of unity. This concludes the proof of the first claim of the lemma.

If $\chi_{\overline{\psi}}$ is symmetric then for all $i \in \{1, \ldots, 2g\}$, and for $k \in \{0, \ldots, \ell_i - 1\}$, we have $\chi_{\overline{\psi}}(k.v_i) = \chi_{\overline{\psi}}(v_i)^k = \chi_{\overline{\psi}}((\ell_i - k).v_i) = \chi_{\overline{\psi}}(v_i)^{\ell_i - k}$. As a consequence, we have for all $k \in \{0, \ldots, \ell_i - 1\}$, $\chi_{\overline{\psi}}(v_i)^{2k} = 1$ and in particular $\chi_{\overline{\psi}}(v_i)^2 = 1$. ■

If $\overline{\psi} \in \mathrm{Sp}(K(\delta))$ and $\chi_{\overline{\psi}}$ is a semi-character, in the following, we denote by $\sigma_{\chi_{\overline{\psi}}}(\overline{\psi})$ the associated automorphism of $\mathcal{H}(\delta)$. The kernel of the group morphism $\Psi : \mathrm{Aut}_{\mathbb{G}_\mathrm{m}} \mathcal{H}(\delta) \to \mathrm{Sp}(K(\delta)), \psi \mapsto \overline{\psi}$ consists of automorphisms that preserve a symplectic basis. Such automorphisms are determined by a choice of level subgroups $\tilde{K}_1$ and $\tilde{K}_2$ over the maximal isotropic subspaces $Z(\delta)$ and $\hat{Z}(\delta)$. As follows, this data defines a ψ by letting for all $x \in Z(\delta)$, $\psi((1, x, 0)) = (\alpha, x, 0)$ where $(\alpha, x, 0) \in \tilde{K}_1$ and for all $y \in \hat{Z}(\delta)$, $\psi((1, 0, y)) = (\alpha, 0, y)$ where $(\alpha, 0, y) \in \tilde{K}_2$. It is well known (see the proof of [BL04, Lem. 6.6.5 p. 162] which can easily be extended to the case of a general base field) that such choices are in bijection with elements $c \in K(\delta)$: we map $c \in K(\delta)$ to the automorphism of $\mathcal{H}(\delta)$ given by

$$(\alpha, x, y) \mapsto (\alpha e_\delta(c, (x, y)), x, y). \tag{17}$$

As a consequence, we get an exact sequence

$$0 \longrightarrow K(\delta) \longrightarrow \mathrm{Aut}_{\mathbb{G}_\mathrm{m}} \mathcal{H}(\delta) \xrightarrow{\Psi} \mathrm{Sp}(K(\delta)) \longrightarrow 0\ . \tag{18}$$

Suppose that Θ_δ is symmetric. An automorphism $\psi \in \mathrm{Aut}_{\mathbb{G}_\mathrm{m}} \mathcal{H}(\delta)$ is said to be symmetric if it commutes with the action $(\alpha, x, y) \mapsto (\alpha, -x, -y)$ on $\mathcal{H}(\delta)$. We denote by $\mathrm{Aut}_{\mathbb{G}_\mathrm{m},\mathrm{s}} \mathcal{H}(\delta)$ the group of symmetric automorphisms of $\mathcal{H}(\delta)$. Obviously, an automorphism $\psi \in \mathrm{Aut}_{\mathbb{G}_\mathrm{m}} \mathcal{H}(\delta)$ coming from $c \in K(\delta)$ is symmetric if and only if $c \in K(\delta)[2]$, the subgroup of 2-torsion of $K(\delta)$.

Now consider $(A_k, \mathscr{L}, \Theta_\delta)$ an abelian variety with a δ-marking and let $(\vartheta_i)_{i \in Z(\delta)}$ be the associated basis of global sections of $\mathscr{L}$. Note that if $\overline{\psi}$ is a symplectic automorphism of $K(\delta)$ and if $\chi_{\overline{\psi}}$ is a symmetric semi-character then $\psi = \sigma_{\chi_{\overline{\psi}}}(\overline{\psi})$ is symmetric. We suppose that this is the case in the following. Let $\overline{\psi}(\hat{Z}(\delta))) = Z^\psi \times \hat{Z}^\psi$, where $Z^\psi \subset Z(\delta)$ and $\hat{Z}^\psi \subset \hat{Z}(\delta)$. Denote by $(\tilde{\vartheta}_i)_{i \in Z(\delta)}$ the basis of global sections of $\mathscr{L}$ associated to $(A_k, \mathscr{L}, \Theta_\delta.\psi)$. In the following, we give an explicit formula to obtain $(\tilde{\vartheta}_i)_{i \in Z(\delta)}$ from the knowledge of $(\vartheta_i)_{i \in Z(\delta)}$.

Let $A_k^0 \simeq A_k / \overline{\Theta_\delta}(\overline{\psi}(\hat{Z}(\delta)))$ and $\pi : A_k \to A_k^0$ be the canonical map. The data of the maximal level subgroup $\Theta_\delta(\psi((1, 0, y)_{y \in \hat{Z}(\delta)}))$ is equivalent to the data of a line bundle $\mathscr{L}_0$ on A_k^0 and an isomorphism $\pi^*(\mathscr{L}_0) \to \mathscr{L}$. Let $\tilde{s}_0$ be the unique global section of $\mathscr{L}_0$. Let $Z^{\psi\perp} = \{x \in Z(\delta) | l(x) = 1, \quad \text{all} \quad l \in \hat{Z}^\psi\}$. As $\overline{\psi}$ is symplectic, it is clear that $Z^{\psi\perp} \supset Z^\psi$ and in fact $Z^{\psi\perp} = Z^\psi$ since $\mathscr{L}_0$ is a principal polarisation. We can then apply the isogeny theorem [Mum66, Sec. 1, Th. 4], with $\sigma : Z^{\psi\perp}/Z^\psi \to 0$ to obtain

$$\tilde{\vartheta_0} = \lambda \pi^*(\tilde{s_0}) = \sum_{i \in Z^\psi} \vartheta_i, \tag{19}$$

for $\lambda \in k^*$.

Now by definition we have

$$\tilde{\vartheta}_i = \psi((1,i,0)).\tilde{\vartheta}_0. \tag{20}$$

where the dot product is the action (2).

By evaluating at 0 the basis of global sections of $\mathscr{L}$ in (20), we get an explicit description of the action of $\mathrm{Sp}(K(\delta))$ on the geometric points of $\mathcal{M}_\delta$. Actually the obtained formulas give a valid action of $\mathrm{Sp}(K(\delta))$ on the geometric points of $\overline{\mathcal{M}_\delta}$.

5.3 The stabiliser of V_J^0

Now, let $(a_u)_{u\in Z(\overline{\ell n})}$ be a geometric point of V_J^0. As $\mathrm{Aut}_{\mathbb{G}_{\mathrm{m}},\mathrm{s}}\,\mathcal{H}(\overline{\ell n})$ acts on $\mathcal{M}_{\overline{\ell n}}$, we are interested in the subgroup $\mathfrak{H}$ of the elements of $\mathrm{Aut}_{\mathbb{G}_{\mathrm{m}},\mathrm{s}}\,\mathcal{H}(\overline{\ell n})$ that leave $(a_u)_{u\in Z(\overline{\ell n})}$ in V_J^0.

Definition 16: *Let $\psi \in \mathrm{Aut}_{\mathbb{G}_{\mathrm{m}},\mathrm{s}}\,\mathcal{H}(\overline{\ell n})$ and denote by $\Theta^{A\,\prime}_{\overline{\ell n}}$ the theta structure $\Theta^A_{\overline{\ell n}} \circ \psi$. Then we can define $Z^*(\overline{\ell n})'$, $\hat{Z}^*(\overline{\ell n})'$, $K_1^{*\prime}$, $K_2^{*\prime}$, $\tilde{p}_1'$, $\tilde{p}_2'$ for $\Theta^{A\,\prime}_{\overline{\ell n}}$ exactly as in the definition of $Z^*(\overline{\ell n})$,$\hat{Z}^*(\overline{\ell n})$, K_1^*, K_2^*, $\tilde{p}_1$, $\tilde{p}_2$ for $\Theta^A_{\overline{\ell n}}$ is Section 3.1. Then, we say that ψ is compatible with $\mathcal{H}(\overline{n})$ if the following diagrams commute:*

$$\begin{array}{ccc} (1,x,0)_{x\in Z^*(\overline{\ell n})'} & \xrightarrow{\psi} & (1,x,0)_{x\in Z^*(\overline{\ell n})} \\ \downarrow{\scriptstyle \tilde{p}_1'} & & \downarrow{\scriptstyle \tilde{p}_1} \\ (1,x,0)_{x\in Z(\overline{n})} & = & (1,x,0)_{x\in Z(\overline{n})} \end{array}, \tag{21}$$

$$\begin{array}{ccc} (1,0,y)_{y\in \hat{Z}^*(\overline{\ell n})'} & \xrightarrow{\psi} & (1,0,y)_{y\in \hat{Z}^*(\overline{\ell n})} \\ \downarrow{\scriptstyle \tilde{p}_2'} & & \downarrow{\scriptstyle \tilde{p}_2} \\ (1,0,y)_{y\in \hat{Z}(\overline{n})} & = & (1,0,y)_{y\in \hat{Z}(\overline{n})} \end{array}. \tag{22}$$

Lemma 17: *We have that $\mathfrak{H}$ is the subgroup of compatible symmetric automorphisms of $\mathcal{H}(\overline{\ell n})$. In particular it does not depend on $(a_u)_{u\in Z(\overline{\ell n})}$ so it is also a subgroup of $\mathrm{Aut}_{\mathbb{G}_{\mathrm{m}},\mathrm{s}}\,\mathcal{H}(\overline{\ell n})$ that leaves V_J^0 invariant.*

Proof: Let $(A,\mathscr{L},\Theta^A_{\overline{\ell n}})$ be a triple corresponding to the theta null point $(a_u)_{u\in Z(\overline{\ell n})}$. Let $\psi \in \mathrm{Aut}_{\mathbb{G}_{\mathrm{m}},\mathrm{s}}\,\mathcal{H}(\overline{\ell n})$, and $(a'_u)_{u\in Z(\overline{\ell n})} = \psi.(a_u)_{u\in Z(\overline{\ell n})}$. Proposition 11 shows that $(a'_u)_{u\in Z(\overline{\ell n})}$ is in V_J^0 if and only if the associated theta structure $\Theta^A_{\overline{\ell n}}.\psi$ is compatible with the theta structure $\Theta^B_{\overline{n}}$ of B. But this means exactly that ψ is compatible with $\mathcal{H}(\overline{n})$. ■

We can describe the action of $\mathfrak{H}$ more precisely:

Proposition 18: *The action of $\mathfrak{H}$ on V_J^0 is generated by the actions given by*

$$(a_u)_{u\in Z(\overline{\ell n})} \mapsto (a_{\psi_2(u)})_{u\in Z(\overline{\ell n})}, \tag{23}$$

for every automorphism ψ_2 of $Z(\overline{\ell n})$ fixing $Z(\overline{n})$ and

$$(a_u)_{u\in Z(\overline{\ell n})} \mapsto \left(e_{\overline{\ell n}}(\psi_1(u),u).a_u\right)_{u\in Z(\overline{\ell n})}, \tag{24}$$

for every symmetric morphism $\psi_1 : Z(\overline{\ell n}) \to \hat{Z}(\overline{\ell}) \subset \hat{Z}(\overline{\ell n})$ and where $e_{\overline{\ell n}}$ is the commutator pairing on $\mathcal{H}(\overline{\ell n})$.

Proof: Let $\psi \in \mathfrak{H}$ and denote by $\overline{\psi} \in \mathrm{Sp}(\mathcal{H}(\delta))$ the associated symplectic automorphism. With respect to a basis $(v_\kappa, \hat{v}_\kappa)_{\kappa\in\{1,\dots,g\}}$ of $Z(\overline{\ell n}) \times \hat{Z}(\overline{\ell n})$, $\overline{\psi}$ is represented by a matrix $M[A,B,C,D] = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_\delta^{2g}(\mathbb{Z})$. Since

$$K = \overline{\Theta}_{\overline{\ell n}}(\overline{\psi}(\hat{Z}(\overline{\ell}))) \subset \overline{\Theta}_{\overline{\ell n}}(\hat{Z}(\overline{\ell n})),$$

we have $B = 0$. So $D = {}^tA^{-1}$ and we see that $\overline{\psi}$ is in the subgroup of $\mathrm{Sp}(K(\overline{\ell n}))$ generated by the matrices:

1. $M[A,B,C,D]$ such that C=0 and $B = 0$. Then A is an automorphism and the compatibility condition implies that it must fix $Z(\overline{n})$. By Lemma 15, there exists an extension ψ' of $\overline{\psi}$ defined by the semi-character $\chi_{\overline{\psi}}$ such that $\chi_{\overline{\psi}}(v_\kappa) = 1$, $\chi_{\overline{\psi}}(\hat{v}_\kappa) = 1$ for $\kappa = 1,\dots,g$. It is easily seen that $\psi' \in \mathfrak{H}$ and using (19) and (20), we see that ψ' yields the action (23).
2. $M[A,B,C,D]$ such that $A = \mathrm{Id}$ and $B = 0$. Then ${}^tC = C$. For $x \in Z(\overline{\ell n})$, we can write $\overline{\psi}((x,0)) = (x, \psi_1(x))$. By looking at the conditions (6) and (7) we see that
$$\overline{\psi}((x,y)) - (x,y) \in \overline{\psi}(\hat{Z}(\overline{\ell})) \subset \hat{Z}(\overline{\ell}), \tag{25}$$
for all $(x,y) \in Z^*(\overline{\ell n}) \times \hat{Z}^*(\overline{\ell n})$. Using (25), we deduce that $\psi_1(x)$ is in $\hat{Z}(\overline{\ell})$. Again, by Lemma 15, there exists an extension ψ' of $\overline{\psi}$ defined by the semi-character $\chi_{\overline{\psi}}$ such that $\chi_{\overline{\psi}}(v_\kappa) = t_\kappa$ for $t_\kappa \in \mathbb{G}_{m,k}$. In order to have that $\psi' \in \mathfrak{H}$ we must choose t_κ such that $\ell(t_\kappa, v_\kappa, \psi_1(v_\kappa)) = (1, \ell v_\kappa, 0)$. For this we can take $t_\kappa = \psi_1(v_\kappa)(v_\kappa)^{1/2.(\ell-1)}$. In this case, we obtain the action (24) following (19) and (20). ∎

Because of the exact sequence from equation (18), we see that by composing ψ with a $\psi' \in \mathfrak{H}$ coming from the two preceding cases, we only have to study the case where ψ comes from a change of maximal level structure. Let $c \in K(\delta)$ defining the symplectic base change by (17). Then $c \in K(\delta)[2]$ since ψ is symmetric and from the compatibility conditions $c \in \overline{\psi}(\hat{Z}(\overline{\ell}))$. As ℓ is odd, we have $c = 0$.

Remark 19: The action (23) gives an automorphism of the $(P_i)_{i\in Z(\overline{\ell})}$ while the action (24) leaves the $(P_i)_{i\in Z(\overline{\ell})}$ invariant. In fact by taking a basis of $Z(\overline{\ell n})$, we see that if ζ is a $(\ell n)^{th}$-root of unity, the actions (24) are generated by

$$a_{(n_1,n_2,\dots,n_g)} \mapsto \zeta^{\sum_{i,j\in[1,g]} a_{i,j} n_i n_j} a_{(n_1,\dots,n_g)}$$

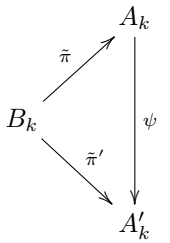
where $(a_{i,j})_{i,j\in[1,g]}$ is a symmetric matrix and $a_{i,j} \in \mathbb{Z}/n\mathbb{Z} \subset \mathbb{Z}/\ell n\mathbb{Z}$ (via $x \mapsto \ell x$) for $i, j \in [1, g]$. So each coefficient of one P_i is multiplied by the same ℓ^{th}-root of unity.

Our study of valid theta null points allows us to better understand the geometry of V_J^0. We know from Proposition 11 that geometric points $(a_u)_{u\in Z(\overline{\ell n})} \in V_J^0$ classifies the isogenies $\pi : A_k \to B_k$ between marked abelian varieties verifying the compatibility condition.

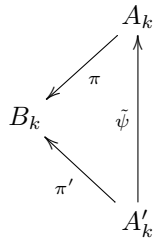
Taking the contragredient of π gives an isogeny from B_k to A_k with kernel $K = G((a_u))_{u\in Z(\overline{\ell n})})$. Thus, the theta null points on V_J^0 correspond to varieties $\overline{\ell}$-isogeneous to B_k. But we have seen in Proposition 18 that it may happen that different points of V_J^0 give the same kernel K and hence the same variety. We want to classify the points of V_J^0 corresponding to isomorphic varieties $\overline{\ell}$-isogeneous to B_k. In other words, we want to study the fiber of the map $(a_u)_{u\in Z(\overline{\ell n})} \mapsto G((a_u)_{u\in Z(\overline{\ell n})})$ defined in Section 5.1 for $(a_u)_{u\in Z(\overline{\ell n})}$ a valid theta null point.

Proposition 20: *Let K be a subgroup of $B_k[\ell]$ isomorphic to $Z(\overline{\ell})$ that is isotropic for the pairing e_W. Then $G^{-1}(\{K\})$ is a subset of the valid theta null points in V_J^0 that forms a principal homogeneous space under the action of $\mathfrak{H}$. In particular, the geometric points of $V_J^0/\mathfrak{H}$ are in bijection with the $\overline{\ell}$-isogenies from B_k (with isotropic kernel).*

Proof: Let $K = \{P_i, i \in Z(\overline{\ell})\}$ be such a maximal subgroup. Theorem 12 gives a geometric point $(a_u)_{u\in Z(\overline{\ell n})}$ of V_J^0 corresponding to a marked abelian variety $(A_k, \mathscr{L}_A, \Theta_A)$ (and an isogeny $\pi : A_k \to B_k$) such that $G((a_u)_{u\in Z(\overline{\ell n})}) = K$. Let $(a'_u)_{u\in Z(\overline{\ell n})}$ be another valid theta null point in V_J^0 in $G^{-1}(K)$, corresponding to a marked abelian variety $(A'_k, \mathscr{L}_{A'}, \Theta_{A'})$, and an associated isogeny $\pi : A_k \to B_k$. Since $A_k \xrightarrow{\sim} B_k/K \xrightarrow{\sim} A'_K$, there exists an isomorphism ψ making the following diagram commutative:



Taking the contragredient, we then obtain that this diagram commutes:



By definition of the associated isogenies π and π', we know that $\mathscr{L}_A = \pi^*(\mathscr{L}_B)$ and $\mathscr{L}_{A'} = \pi'^*(\mathscr{L}_B) = \tilde{\psi}^*(\mathscr{L}_A)$. So $\tilde{\psi}$ induces a morphism of the theta groups $G(\mathscr{L}_A)$ and $G(\mathscr{L}_{A'})$, and pulling back by the theta structures we get a symmetric automorphism $\tilde{\psi}$ of $\mathcal{H}(\overline{\ell n})$. Since the theta structures Θ_A and $\Theta_{A'}$ are compatible with Θ_B, $\tilde{\psi}$ is in $\mathfrak{H}$. This shows that $(a_u)_{u\in Z(\overline{\ell n})}$ and $(a'_u)_{u\in Z(\overline{\ell n})}$ are in the same orbit under $\mathfrak{H}$. ■

5.4 Classification of the valid and degenerate theta null points

In this section, we extend the map G from the set V_J^0 of valid theta null points so that the domain of the extended map is V_J. We start by making the structure of the solutions of the algebraic system defined by J explicit. For this let $\rho : Z(\overline{n}) \times Z(\overline{\ell}) \to Z(\overline{\ell n})$ be the group isomorphism given by $(x, y) \mapsto \ell x + ny$. Denote by $I_{\Theta_{\overline{n}}^B}$ the ideal of $k[y_u | u \in Z(\overline{n})]$ for the theta structure $\Theta_{\overline{n}}^B$ generated by the equations of Theorem 2 where we have substituted ϑ_u by y_u and a_u by b_u for $u \in Z(\overline{n})$. The homogeneous ideal $I_{\Theta_{\overline{n}}^B}$ defines a projective variety $V_{I_{\Theta_{\overline{n}}^B}}$, isomorphic to B_k.

Proposition 21: *We suppose that* $4 \mid n$. *Let* $(a_v)_{v\in Z(\overline{\ell n})}$ *be a geometric point of* V_J. *For any* $i \in Z(\overline{\ell})$ *such that* $(a_{\rho(j,i)})_{j\in Z(\overline{n})} \neq (0, \ldots, 0)$, *let* P_i *be the geometric point of* $\mathbb{P}_k^{Z(\overline{n})}$ *with homogeneous coordinates* $(a_{\rho(j,i)})_{j\in Z(\overline{n})}$. *We denote by* S *the set* $\{i, i \in Z(\overline{\ell}), P_i$ *is well defined*$\}$, *and let* $G((a_v)_{v\in Z(\overline{\ell n})}) = \{P_i, i \in S\}$. *Then* S *is a subgroup of* $Z(\overline{\ell})$, $G((a_v)_{v\in Z(\overline{\ell n})})$ *is an isotropic subgroup of* $B_k[\ell]$ *for* e_W, *and the map* $S \to G((a_v)_{v\in Z(\overline{\ell n})})$ *is a morphism of group.*

Proof: The fact that P_i for $i \in S$ is a point of ℓ-torsion comes from [CL09, Lem. 5.6] which can be easily adapted to the case n divisible by 4 and ℓ relatively prime to n.

The proof of the preceding proposition in [CL09] proves moreover that $\{P_i, i \in S\}$ is a subgroup of the group of ℓ-torsion points of $V_{I_{\Theta_{\overline{n}}^B}}$ (that we identify with B_k via $\Theta_{\overline{n}}^B$) and the map $i \in S \to P_i \in B[\ell]$ is a group morphism. The fact that this subgroup is isotropic comes easily from [LR10, Theorem 2]. ■

If $(a_v)_{v\in Z(\overline{\ell n})}$ is a general geometric point of V_J, it can happen that certain P_i are not well defined and as a consequence $(a_v)_{v\in Z(\overline{\ell n})}$ is not a valid theta null

point. But even if every P_i is well defined, $(a_v)_{v\in Z(\overline{\ell n})}$ need not be a valid theta null point, as we can see for instance in Example 25 of Section 5.5 below. We need a criterion to identify the solutions of J that correspond to valid theta null points. From the discussion of Section 5.1, we know that a necessary condition for a solution $(a_v)_{v\in Z(\overline{\ell n})}$ of J to be a valid theta null point is that $G((a_u)_{u\in Z(\overline{\ell n})})$ form a subgroup of rank g of $B_k[\ell]$. Theorem 23 below asserts that this necessary condition is indeed sufficient.

First we remark that there is an action of $\mathfrak{H}$ on V_J given by (23) and (24) which extends the previously defined action of $\mathfrak{H}$ on V_J^0. By Remark 19 (which can easily be extended to the case of degenerate theta null points) we know that if $(a_u)_{u\in Z(\overline{\ell n})}$ is a theta null point giving the associated group $\{P_i, i \in Z(\overline{\ell}), P_i \text{ well defined projective point}\}$, then the points $\psi.(a_u)_{u\in Z(\overline{\ell n})}$ where $\psi \in \mathfrak{H}$ give the same associated group. In fact the converse is true:

Lemma 22: *We suppose that $4 \mid n$. Let $(c_u)_{u\in Z(\overline{\ell n})}$ and $(d_u)_{u\in Z(\overline{\ell n})}$ be two geometric points of V_J giving the same associated group*

$$\{P_i, i \in Z(\overline{\ell}), P_i \text{ well defined projective point}\}.$$

Then there exists $\psi \in \mathfrak{H}$ such that $(d_u)_{u\in Z(\overline{\ell n})} = \psi.(c_u)_{u\in Z(\overline{\ell n})}$.

Proof: To ease the notation, we suppose here that $S = Z(\overline{\ell})$, because the lemma will only be applied for this case in Theorem 23. Let $P_i' = (a'_{\rho(j,i)})_{j\in Z(\overline{n})}$ for $i \in Z(\overline{\ell})$. First, up to an action of type (23), we can suppose that for all $i \in Z(\overline{\ell})$, we have $P_i^{(c_u)_{u\in Z(\overline{\ell n})}} = P_i^{(d_u)_{u\in Z(\overline{\ell n})}}$. Thus there exists $\lambda_i \in \overline{k}$ such that $(c_{\rho(j,i)})_{j\in Z(\overline{n})} = \lambda_i (d_{\rho(j,i)})_{j\in Z(\overline{n})}$. Since $(c_u)_{u\in Z(\overline{\ell n})}$ and $(d_u)_{u\in Z(\overline{\ell n})}$ are projective, we can assume that $\lambda_0 = 1$. It suffices to show that up to an action of type (24), for every $i \in Z(\overline{\ell})$ such that P_i is well defined, $\lambda_i = 1$. But first we show that for such points, we have $\lambda_i^\ell = 1$.

Let $i \in Z(\overline{\ell})$ be such that $(c_{\rho(j,i)})_{j\in Z(\overline{n})}$ is a well defined projective point. Let $x, y, u, v \in Z(2\overline{n})$ be congruent modulo $Z(\overline{n})$. We remark that for $\mu \in \{1, \dots, \ell\}$, $\rho'(x, \mu.i)$, $\rho'(y, i)$, $\rho'(u, 0)$, $\rho'(v, 0)$, where $\rho' : Z(2n) \times Z(\overline{\ell n}) \to Z(2\overline{\ell n})$ is the morphism defined in the same manner as ρ, are elements of $Z(2\overline{\ell n})$ congruent modulo $Z(\overline{\ell n})$. Applying Theorem 4, we obtain that

$$\begin{aligned}\Big(\sum_{t\in Z(\overline{2})} \chi(t) c_{\rho(x+y+t,(\mu+1).i)} c_{\rho(x-y+t,(\mu-1).i)}\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t) c_{\rho(u+v+t,0)} c_{\rho(u-v+t,0)}\Big) = \\ = \Big(\sum_{t\in Z(\overline{2})} \chi(t) c_{\rho(x+u+t,\mu.i)} c_{\rho(x-u+t,\mu.i)}\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t) c_{\rho(y+v+t,i)} c_{\rho(y-v+t,i)}\Big),\end{aligned} \tag{26}$$

for any $\chi \in \hat{Z}(\overline{2})$. We have a similar formula involving $(d_u)_{u\in Z(\overline{\ell n})}$. Using [Mum66, eq. (*) p. 339], we obtain as $4 \mid n$ that for every $x, y \in Z(2\overline{\ell n})$, we can choose

$u, u \in Z(2\overline{\ell n})$ such that $\sum_{t\in Z(\overline{2})} \chi(t) c_{\rho(u+v+t,0)} c_{\rho(u-v+t,0)} \neq 0$ (and the same is true of course if we replace c by d in the preceding inequality).

Using equation (26) for both $(c_u)_{u\in Z(\overline{\ell n})}$ and $(d_u)_{u\in Z(\overline{\ell n})}$, and an easy induction, we obtain that $\lambda_{\mu.i} = \lambda_i^{u_\mu}$ where (u_μ) is a sequence such that $u_0 = 0$, $u_1 = 1$ and $u_{\mu+1} + u_{\mu-1} = 2.u_\mu + 2$. The general term of this sequence is $u_\mu = \mu^2$. For $\mu = \ell$, we have

$$\lambda_i^{\ell^2} = \lambda_{\ell.i} = \lambda_0 = 1 \tag{27}$$

Now, by the symmetry relations, we have for $j \in Z(\overline{n})$, $c_{\rho(j,\mu.i)} = c_{\rho(-j,-\mu.i)}$. Applying this for $\mu = 1$ and $j = 0$, we obtain that $\lambda_i = \lambda_i^{(\ell-1)^2}$ which together with (27) gives

$$\lambda_i^{\ell} = 1 \tag{28}$$

which concludes the claim.

Let $(e_1, \ldots, e_g)$ be the canonical basis of $Z(\overline{\ell})$. Up to an action of type (24) we may assume that $\lambda_{e_i} = 1$ and $\lambda_{e_i+e_j} = 1$ for $i, j \in \{1, \ldots, g\}, j < i$. Now let $a, b \in Z(\overline{\ell})$ be such that $\lambda_a = 1$, $\lambda_b = 1$ and $\lambda_{a-b} = 1$. Then by Theorem 4 we have the relations:

$$\begin{aligned}\Big(\sum_{t\in Z(2)} \chi(t) c_{\rho(x+y+t,a+b)} c_{\rho(x-y+t,a-b)}\Big).\Big(\sum_{t\in Z(2)} \chi(t) c_{\rho(u+v+t,0)} c_{\rho(u-v+t,0)}\Big) = \\ = \Big(\sum_{t\in Z(2)} \chi(t) c_{\rho(x+u+t,-b)} c_{\rho(x-u+t,b)}\Big).\Big(\sum_{t\in Z(2)} \chi(t) c_{\rho(y+v+t,a)} c_{\rho(y-v+t,a)}\Big).\end{aligned} \tag{29}$$

Since by symmetry, $\lambda_{-b} = 1$, the relations (29) give that $\lambda_{a+b} = 1$. An easy induction shows that for any $i \in Z(\overline{\ell})$ we have $\lambda_i = 1$, which concludes the proof. ■

As an application of Lemma 22, we have:

Theorem 23: *Let $(B_k, \mathscr{L}_0, \Theta^B_{\overline{n}})$ be a marked abelian variety and let $(b_u)_{u\in Z(\overline{n})}$ be its associated theta null point. Let $(a_u)_{u\in Z(\overline{\ell n})}$ be a geometric point of V_J where V_J is the algebraic variety defined in Section 4. For any $i \in Z(\overline{\ell})$, let P_i be the geometric point, if well defined, of $\mathbb{P}_k^{Z(\overline{n})}$ with homogeneous coordinates $(a_{\rho(j,i)})_{j\in Z(\overline{n})}$. Denote by S the subset of $Z(\overline{\ell})$ of those elements i such that P_i is a well defined projective point.Then $G((a_u)_{u\in Z(\overline{\ell n})}) := \{P_i, i \in S\}$ is an ℓ-torsion subgroup of $B_k = V_{I_{\Theta^B_{\overline{n}}}}$ isomorphic to $Z(\overline{\ell})$ if and only if $(a_u)_{u\in Z(\overline{\ell n})}$ is a valid theta null point. In other words, $G((a_u)_{u\in Z(\overline{\ell n})})$ is isomorphic to $Z(\overline{\ell})$ if and only if there exists $(A_k, \mathscr{L}, \Theta^A_{\overline{\ell n}})$ an abelian variety together with an $(\overline{\ell n})$-marking with associated theta null point $(a_u)_{u\in Z(\overline{\ell n})}$.*

Proof: The if part of the statement follows from the discussion in Section 5.1.

For the only if part of the statement, by Proposition 21 the group $G((a_u)_{u\in Z(\overline{\ell n})})$ is isotropic, so by Theorem 12 there exists a valid theta null point $(a'_u)_{u\in Z(\overline{\ell n})}$

such that $G((a'_u)_{u\in Z(\overline{\ell n})}) = \{P_i, i \in Z(\overline{\ell})\}$. Since $(a_u)_{u\in Z(\overline{\ell n})}$ and $(a'_u)_{u\in Z(\overline{\ell n})}$ are geometric points of V_J, we can apply Lemma 22 to obtain $\psi \in \mathfrak{H}$ such that $(a_u)_{u\in Z(\overline{\ell n})} = \psi.((a'_u)_{u\in Z(\overline{\ell n})})$. This proves that $(a_u)_{u\in Z(\overline{\ell n})}$ is a valid theta null point.

The next proposition is another application of the techniques used to prove Lemma 22. This proposition is important for the algorithmic applications presented in this paper since it allows to bound the degree of the 0-dimensional variety V_J which is crucial in order to assess the running time of our algorithms.

Proposition 24: *If ℓ is prime to the characteristic of k and $8 \mid n$ then V_J is a geometrically reduced scheme.*

Proof: We recall that V_J is the affine variety defined by J where J is the image of the homogeneous ideal I defining $\overline{\mathcal{M}}_{\overline{\ell n}}$, under the specialization map

$$k[x_u|u \in Z(\overline{\ell n})] \to k[x_u|u \in Z(\overline{\ell n}), nu \neq 0], \quad x_u \mapsto \begin{cases} b_u\,, \text{ if } \quad u \in Z(\overline{n}) \\ x_u, \text{ else} \end{cases},$$

with $(b_u)_{u\in Z(\overline{n})}$ the theta null point associated to $(B_k, \mathscr{L}_0, \Theta^B_{\overline{n}})$.

By definition, V_J is a closed subvariety of the affine space $\mathbb{A}^{Z(\overline{\ell n})}$. For $i \in Z(\overline{\ell})$, denote by $\pi_i : \mathbb{A}^{Z(\overline{\ell n})} \to \mathbb{A}^{Z(\overline{n})}$ the projection induced by the inclusion $\varphi_i : k[x_u|u \in Z(\overline{n})] \to k[x_u|u \in Z(\overline{\ell n})]$, $x_u \mapsto x_{\rho(u,i)}$. In order to prove that V_J is a reduced scheme, we can suppose by doing a base change if necessary that $k = \overline{k}$ and it is enough to prove that for any connected subvariety x of V_J and all $\lambda \in Z(\overline{\ell})$, $\pi_\lambda(x)$ is a reduced subvariety of $\mathbb{A}^{Z(\overline{n})}$. We consider two cases.

If $\pi_\lambda(x)$ is not the point at the origin of $\mathbb{A}^{Z(\overline{n})}$ then it defines a projective point of $\mathbb{P}^{Z(\overline{n})}$ which is an ℓ-torsion point of $V_{I_{\Theta^B_{\overline{n}}}}$ by Proposition 21. We will show that $\pi_\lambda(x)$ is contained in the reduced line L_λ between the origin point of $\mathbb{A}^{Z(\overline{n})}$ and this point of ℓ-torsion. We identify L_λ with $\mathrm{Spec}(k[z])$ and we suppose that $x = \mathrm{Spec}(k[[t]]/(t^m))$ for $m \in \mathbb{N}^*$. Then the image of x in L_λ is defined by an element $\alpha_\lambda \in k[[t]]/(t^m)$. Now, we suppose that $m = 2$ so that we can write $\alpha_\lambda = \beta_\lambda(1 + t\xi_\lambda)$, with $\beta_\lambda, \xi_\lambda \in k$. Using equation (26) of the preceding lemma, we obtain that for all $\mu \geqslant 2$ integer, we have $\xi_{(\mu+1).\lambda} + \xi_{(\mu-1).\lambda} = 2\xi_{\mu.\lambda} + 2\xi_\lambda$. As $\xi_0 = 0$, since the theta null point $(b_u)_{u\in Z(\overline{n})}$ is reduced, we deduce immediately that for all $\mu \geqslant 2$, $\xi_{\mu.\lambda} = \xi_\lambda \mu^2$. Applying this for $\mu = \ell$ yields that $\xi_{\ell.\lambda} = \xi_\lambda \ell^2 = 0$ using again that $(b_u)_{u\in Z(\overline{n})}$ is reduced. As ℓ is prime to the characteristic of k, we get that for all $\lambda \in Z(\overline{\ell})$, $\xi_\lambda = 0$ and as a consequence, for $m = 2$ and all $\lambda \in Z(\overline{\ell})$, the image of x in L_λ is reduced. An easy induction on m based on the preceding reasoning then tells us that for all $\lambda \in Z(\overline{\ell})$, the image of x in L_λ is reduced.

We now treat the case when $\pi_\lambda(x)$ is the origin point of $\mathbb{A}^{Z(\overline{n})}$. Let $\mathfrak{P} = (x_u|u \in Z(\overline{n}))$ be the ideal of $k[x_u|u \in Z(\overline{n})]$ defining the reduced point at the origin of $\mathbb{A}^{Z(\overline{n})}$. Let $J_\lambda = J \cap \varphi_\lambda(k[x_u|u \in Z(\overline{n})])$ and denote by $J_{\lambda\mathfrak{P}}$ the local ring of J_λ in $\mathfrak{P}$. As J is a 0-dimensional ideal, we know that there exists m a positive integer such that $J_{\lambda\mathfrak{P}} \supset \mathfrak{P}^m$ in $k[x_u|u \in Z(\overline{n})]_{\mathfrak{P}}$. Let r_λ be the smallest

integer with this property. We want to show that $r_\lambda = 1$. In order to do so, we are going to use another formulation of the Riemann relations given by Theorem 2.

For this, we let $H(\overline{\ell n}) = Z(\overline{\ell n}) \times \hat{Z}(\overline{2})$ and $H(\overline{n}) = Z(\overline{n}) \times \hat{Z}(\overline{2})$. We denote by $\rho' : H(\overline{n}) \times Z(\overline{\ell}) \to H(\overline{\ell n})$ the natural isomorphism deduced from ρ. For all $v = (v', v'') \in H(\overline{\ell n})$, we let $y_v = \sum_{t \in Z(\overline{2})} v''(t) x_{v'+t}$. Let $a_1, a_2, a_3, a_4, \tau \in H(\overline{n})$ such that $2\tau = a_1 - a_2 - a_3 - a_4$. Set $\alpha_1 = \rho'(a_1, 2\lambda)$, $\alpha_2 = \rho'(a_2, 0)$, $\alpha_3 = \rho'(a_3, 0)$, $\alpha_4 = \rho'(a_4, 0)$ and $\tau_1 = \rho'(\tau, \lambda)$ so that we have $2\tau_1 = \alpha_1 - \alpha_2 - \alpha_3 - \alpha_4$. We write $\tau = (\tau', \tau'')$ and let $H(\overline{2}) = \{x \in H(\overline{\ell n}) | x \,\text{is}\, 2-\text{torsion modulo}\, Z(\overline{2}) \times \{0\}\}$. By applying [Mum67a, formula (C") p. 334], we have the following relation in J:

$$y_{\alpha_1} y_{\alpha_2} y_{\alpha_3} y_{\alpha_4} = \\ = \frac{1}{2^g} \sum_{t \in H(\overline{2})} (\tau'' + t'')(2t') y_{\alpha_1 - \tau_1 + t} y_{\alpha_2 + \tau_1 + t} y_{\alpha_3 + \tau_1 + t} y_{\alpha_4 + \tau_1 + t}, \quad (30)$$

where $t = (t', t'') \in H(\overline{2})$.

By definition, for $i = 2, 3, 4$, if we write $a_i = (a_i', a_i'')$, we have $y_{\alpha_i} = \sum_{t \in Z(\overline{2})} a_i''(t) b_{a_i'+t}$. As by hypothesis $(b_u)_{u \in Z(\overline{n})}$ is valid theta null points, by applying [Mum67a, formulas (*) p. 339], we obtain that for any $a_i = (a_i', a_i'') \in H(\overline{n})$ there exists $\beta_i' \in 2Z(\overline{n})$ such that $\sum_{t \in Z(\overline{2})} a_i''(t) b_{a_i'+\beta_i'+t} \neq 0$. As a consequence, for any choice of a_1, we can find a_2, a_3, a_4, and $\tau \in H(\overline{n})$ such that $2\tau = a_1 - a_2 - a_3 - a_4$ and for $i = 2, 3, 4$, $y_{\alpha_i} = \sum_{t \in Z(\overline{2})} a_i''(t) b_{a_i'+t} \neq 0$. (We can take for instance $a_1 = a_2 = a_3 = a_4$ so that $a_1 - a_2 - a_3 - a_4 \in 2H(\overline{n})$ and then if necessary add to a_2, a_3, a_4 elements of $2Z(\overline{n})$ in order to have $y_{(a_i,0)} \neq 0$.) As an immediate consequence, we obtain that $\pi_{2\lambda}(x)$ is also the origin point of $\mathbb{A}^{Z(\overline{n})}$.

Let r_λ' be the smallest integer such that $r_\lambda' \geqslant r_\lambda$ and $4 | r_\lambda'$. We remark that $\varphi_{2\lambda}(k[x_u | u \in Z(\overline{n})]) = k[y_{\rho'(v,2\lambda)} | v \in H(\overline{n})]$. Let M be a degree $r_\lambda'/4$ monomial in the variables $y_{\rho'(v,2\lambda)}$. If necessary, by multiplying M by a suitable non null constant, we see that M is equal to a product M' of $r_\lambda'/4$ polynomials given by the right hand of (30). These polynomials have degree 4 and are sums of products of monomials of the form $y_{\rho'(v,\lambda)}$ (using the symmetry relations). We deduce from this that $M' \in \mathfrak{P}^{r_\lambda}$ and as a consequence $M' \in J_\lambda$. But this means that $M \in J_{2\lambda}$ and as M can be any degree $r_\lambda'/4$ monomial in the variables $y_{\rho'(v,2\lambda)}$, we have proved that $J_{2\lambda\mathfrak{P}} \supset \mathfrak{P}^{r_\lambda'/4}$.

Let m be an integer such that $2^m \lambda = \lambda$ in $Z(\overline{\ell})$. Using the previous result and an easy induction, we see that if $r_\lambda > 1$ then $r_\lambda = r_{2^m\lambda} < r_\lambda$ which is a contradiction. ■

We conclude this section by a study of the degenerate theta null points. It is easy to see that $\mathfrak{H}$ leaves V_J invariant. Now, let ψ_2 be a endomorphism of $Z(\overline{\ell n})$ fixing $Z(\overline{n})$. Here we do not require ψ_2 to be an automorphism. We let ψ_2 act on V_J by

$$(a_u)_{u \in Z(\overline{\ell n})} \mapsto (a_{\psi_2(u)})_{u \in Z(\overline{\ell n})}$$

Since ψ_2 fixes $Z(\overline{n}) \subset Z(\overline{\ell n})$, it fixes the 2-torsion points in $Z(\overline{\ell n})$, and it is easy to see that $(a_{\psi_2(u)})_{u \in Z(\overline{\ell n})}$ satisfies the equations of Theorem 4 and the symmetry relations. As a consequence, the point $(a_{\psi_2(u)})_{u \in Z(\overline{\ell n})}$ is in $\overline{\mathcal{M}}_{\overline{\ell n}}$. Moreover, as ψ_2 fixes $Z(\overline{n})$, $(a_{\psi_2(u)})_{u \in Z(\overline{\ell n})}$ is a point in V_J, so if we denote by $\mathfrak{H}_1$ the monoid of endomorphisms of $Z(\overline{\ell n})$ fixing $Z(\overline{n})$, we have a well defined monoid action $\mathfrak{H}_1 \times V_J \to V_J$ extending the group action given by (23) and (24).

By acting on V_J with an endomorphism of $Z(\overline{\ell n})$ fixing $Z(\overline{n})$ which is not an automorphism, we obtain a point of V_J which is degenerate: it is a theta null point such that the associated points P_i from Proposition 21 are well defined but not distinct projective points (so they do not form a rank g ℓ-torsion subgroup of B_k).

There is another way to obtain degenerate theta null points in V_J. Take any geometric point $(a_u)_{u \in Z(\overline{\ell n})} \in V_J$, and a subgroup S of $Z(\overline{\ell})$ (in particular S is not empty). We define a new point $(a'_u)_{u \in Z(\overline{\ell n})}$ where

$$a'_{\rho(j,i)} = \begin{cases} a_{\rho(j,i)} & \text{if } i \in S, \\ 0 & \text{otherwise,} \end{cases}$$

and we recall that ρ has be defined at the begining of Section 5.1.

Since ℓ is odd, it is easily seen that $(a'_u)_{u \in Z(\overline{\ell n})}$ is in general a degenerate point in V_J: the P_i from Proposition 21 are not defined when $i \notin S$.

Now, we explain that combining the two methods described above, we obtain all the degenerate theta null points of V_J. For this, let $(a'_u)_{u \in Z(\overline{\ell n})}$ be a degenerate point of V_J. Let $S \subset Z(\overline{\ell})$ be the subgroup where the points of ℓ-torsion P'_i, $i \in S$ of Proposition 21 are well defined. The points P'_i form a subgroup S' of the ℓ-torsion points of B_k, and $f : S \to S', i \mapsto P'_i$ is a group morphism (which may not be an isomorphism, since as $(a'_u)_{u \in Z(\overline{\ell n})}$ is degenerate the P'_i are not necessarily distinct). Now, we extend S' into a subgroup T of $B_k[\ell]$ isomorphic to $Z(\overline{\ell})$, isotropic for e_W (this is possible by Proposition 21). We then extend f to a morphism $\tilde{f} : Z(\overline{\ell}) \to T$ by sending an element in $Z(\overline{\ell}) \backslash S$ to 0_B. We take an isomorphism h between $Z(\overline{\ell})$ and T. By Theorem 23 there exists a geometric point $(a_u)_{u \in Z(\overline{\ell n})} \in V_J^0$ such that the corresponding group morphism $i \in Z(\overline{\ell}) \mapsto P_i$ is h. Take ψ_2 to be the endomorphism of $Z(\overline{\ell n})$, that we identify to $Z(\overline{\ell}) \times Z(\overline{n})$ via ρ, which is the identity on $Z(\overline{n})$ and $h^{-1}\tilde{f}$ on $Z(\overline{\ell})$. Consider the point $(a_{\psi_2(u)})_{u \in Z(\overline{\ell n})}$ with the coefficients $\rho(j,i), i \notin S$ taken to be 0. Then it has exactly the same defined points P'_i as $(a'_u)_{u \in Z(\overline{\ell n})}$. Lemma 22 shows that it is the same point as $(a'_u)_{u \in Z(\overline{\ell n})}$ up to an action of the form given by Proposition (18).

We remark that the degenerate points in V_J are exactly the points where the action of $\mathfrak{H}$ is not free: if $(a_u)_{u \in Z(\overline{\ell n})}$ is a degenerate point such that the corresponding P_i are not all well defined, then there is an action of the form (24) giving the same point. If the P_i are well defined but do not form a maximal subgroup, then this time there is an action of the form (23) giving the same point.

5.5 Applications and examples

Together with the study of degenerate theta null points, it is now possible to count the points in V_J. In this section, we suppose that ℓ is prime. For instance, take $g = 1$, $n = 4$ and $\ell = 3$. Let E be an elliptic curve, and $(b_u)_{u\in(\mathbb{Z}/n\mathbb{Z})}$ be a level 4 theta null point on E. There are $4 = \#\mathbb{P}^1(\mathbb{F}_3)$ classes of 3-isogenies from E, and $6 = 3 \times \varphi(3)$ solutions in V_J for each class. The actions (23) are given by $(a_u)_{u\in(\mathbb{Z}/\ell n\mathbb{Z})} \mapsto (a_{x.u})_{u\in\mathbb{Z}/\ell n\mathbb{Z}}$ where $x \in \mathbb{Z}/\ell n\mathbb{Z}$ is invertible and congruent to 1 mod n. There are $\varphi(\ell)$ such actions. The actions (24) are given by $(a_u)_{u\in\mathbb{Z}/\ell n\mathbb{Z}} \mapsto (\zeta^{c.u^2} a_u)_{u\in\mathbb{Z}/\ell n\mathbb{Z}}$ where ζ is a ℓ^{th}-root of unity and $c \in \mathbb{Z}/\ell\mathbb{Z}$.

If $g = 2$ and $n = 4$, it is easy to compute the number of valid theta null points in V_J. First, we remark that the number of isogeny classes of degree ℓ^2 of a given dimension 2 abelian variety B_k is parametrised by the points of a Grassmanian $Gr(2, 4)(\mathbb{F}_\ell)$ which are isotropic (see Theorem 12): there are $(\ell^2 + 1)(\ell + 1)$ such points.

Next, the number of actions of the form (23) is parametrised by the number of invertible matrices of dimension 2 with coefficients in $\mathbb{F}_\ell$ with is given by $(\ell^2 - 1).(\ell^2 - \ell)$. The number of actions of the form (24) is ℓ^3 (the number of symmetric matrices of dimension 2). As a consequence, the number of valid theta null points in V_J is

$$\ell^{10} - \ell^8 - \ell^6 + \ell^4.$$

We remark that this number is $O(\ell^{10})$. For $g = 2$, $\ell = 3$, we have 51840 valid theta null points in V_J.

For a general g and ℓ, we assess the order of the number of valid theta null point which are solution of V_J. The number of isotropic points of a Grassmanian $Gr(g, 2.g)(\mathbb{F}_\ell)$ is $O(\ell^{g(g+1)/2})$. The number of actions of the form (23) is $O(\ell^{g^2})$ and the number of actions of the form (24) is $O(\ell^{g(g+1)/2})$. We deduce that the number of valid theta null point in V_J is bounded by

$$O(\ell^{2.g^2+g}). \tag{31}$$

Example 25: In the case of genus 1 and small ℓ it is possible to list all the geometric points of V_J. We take $\ell = 3$ and let E be the elliptic curve given by an affine equation $y^2 = x^3 + 11.x + 47$ over $\mathbb{F}_{79}$. A corresponding theta null point of level 4 for E is $(1 : 1 : 12 : 1)$. The four subgroups of 3-torsion of $E \simeq V_{I_{\Theta_{\overline{4}}}}$ are

$$\begin{aligned}
K_1 &= \{(1 : 1 : 12 : 1), (37 : 54 : 46 : 1), (8 : 60 : 74 : 1)\}\\
K_2 &= \{(1 : 1 : 12 : 1), (67 : 10 : 68 : 1), (62 : 8 : 70 : 1)\}\\
K_3 &= \{(1 : 1 : 12 : 1), (42 : 5 : 15 : 1), (40 : 16 : 3 : 1)\}\\
K_4 &= \{(1 : 1 : 12 : 1), (72 : 56 : 31 : 1), (69 : 24 : 33 : 1)\}
\end{aligned}$$

All geometric points of V_J are defined over $\mathbb{F}_{79}(\upsilon)$ where υ is a root of the irreducible polynomial $X^3 + 9.X + 76$. For each of the four subgroups K_i, there are 6 geometric points of V_J giving the curve E/K_i. We give a point in each class (the other points can be obtained via the actions (23) and (24)):

$Q_1 = (16\upsilon^2 + 19\upsilon + 17 : 1 : 46 : 16\upsilon^2 + 19\upsilon + 17 : 37 : 54 : 34\upsilon^2 + 70\upsilon + 46 : 54 : 37 : 16\upsilon^2 + 19\upsilon + 17 : 46 : 1)$ corresponds to K_1.

$Q_2 = (64\upsilon^2 + 67\upsilon + 68 : 1 : 68 : 64\upsilon^2 + 67\upsilon + 68 : 67 : 10 : 57\upsilon^2 + 14\upsilon + 26 : 10 : 67 : 64\upsilon^2 + 67\upsilon + 68 : 68 : 1)$ corresponds to K_2.

$Q_3 = (8\upsilon^2 + 49\upsilon + 48 : 1 : 3 : 8\upsilon^2 + 49\upsilon + 48 : 40 : 16 : 17\upsilon^2 + 35\upsilon + 23 : 16 : 40 : 8\upsilon^2 + 49\upsilon + 48 : 3 : 1)$ corresponds to K_3.

$Q_4 = (32\upsilon^2 + 73\upsilon + 34 : 1 : 33 : 32\upsilon^2 + 73\upsilon + 34 : 69 : 24 : 68\upsilon^2 + 7\upsilon + 13 : 24 : 69 : 32\upsilon^2 + 73\upsilon + 34 : 33 : 1)$ corresponds to K_4.

We also have the following degenerate points in V_J: if we take $x = 9$ in the action (23), the image of the class of any Q_i is $\mathcal{C} = \{(55 : 1 : 12 : 55 : 1 : 1 : 28 : 1 : 1 : 55 : 12 : 1), (1 : 1 : 12 : 1 : 1 : 1 : 12 : 1 : 1 : 1 : 12 : 1), (23 : 1 : 12 : 23 : 1 : 1 : 39 : 1 : 1 : 23 : 12 : 1)\}$. For this class, the corresponding ℓ-torsion subgroup (the points P_i of Proposition 21) is $\{(1 : 1 : 12 : 1), (1 : 1 : 12 : 1), (1 : 1 : 12 : 1)\}$ which has rank 0. On $\mathcal{C}$ the action (23) is trivial, so there are only 3 points in this degenerate class, coming from the action (24). The last degenerate point is $(1 : 0 : 0 : 1 : 0 : 0 : 12 : 0 : 0 : 1 : 0 : 0)$, alone in its class.

Let ν be the 2-adic valuation of n. We conclude this section with some remarks concerning the case $\nu = 1$ and the case where the characteristic of k is equal to ℓ. First, for computational reasons, for instance in order to limit the number of variables when computing the points of V_J, we would like to have ν as small as possible. All the results of Section 5 are valid under the hypothesis that $\nu \geqslant 2$ (except Proposition 24 which is only proved for $\nu \geqslant 3$)) and that the characteristic of k is different from ℓ. In the case $\nu = 1$, we can not even prove that V_J is a zero dimensional variety. Nonetheless we have made extensive computations which support the idea that even in the case $\nu = 1$, in general, V_J is a zero dimensional variety whose degree is the same $O()$ with respect to the parameter ℓ as in the case $\nu = 2$.

We remark that the definition of V_J at the begining of Section 4 is valid even if we do not suppose that ℓ is prime to the characteristic of the base field k. Moreover, the proof that V_J is a 0-dimensional scheme is still correct without the hypothesis that ℓ is prime to the characteristic of k. In this case V_J is not anymore reduced and the computation of the number of solutions of V_J are not valid. Nonetheless, from our computations, we see the degree of the variety V_J is of the same order with respect to the parameter ℓ as in the case where the characteristic of k is different from ℓ.

In the following section, we give an algorithm to find the solutions of V_J. We explain why this algorithm is efficient in the case $\nu \geqslant 2$ and when the characteristic of k is different from ℓ. If $\nu = 1$ or if the characteristic of k is equalto ℓ, we will make the hypothesis that V_J is a zero dimensional variety whose degree is given by formula (31). Under this hypothesis, we can also give heuristics explaining the efficiency our algorithm.

6 An efficient algorithm

We would like to use the formulas of Section 4 to compute the image of the modular correspondence Φ_ℓ as described in the introduction of this paper for some positive integer ℓ. As said before, the main algorithmic difficulty is to solve a polynomial system defined from the equations of Theorem 4. The aim of this section is to give an algorithm to solve efficiently this system. We have made an implementation of our algorithm and used it to test the hypothesis described at the end of Section 5.

Let $n = 2^\nu$ and we suppose in this section that ℓ is an odd prime. In this section, k is a finite field. We let $(B_k, \mathscr{L}_0, \Theta^B_{\overline{n}})$ be a dimension-g abelian variety together with an $\overline{n}$-marking and we denote by $(b_u)_{u\in Z(\overline{n})}$ its associated theta null point. Let J be the image of the homogeneous ideal defining $\overline{\mathcal{M}_{\overline{\ell n}}}$ given by the equation of Theorem 2, under the specialization map

$$k[x_u | u \in Z(\overline{\ell n})] \to k[x_u | u \in Z(\overline{\ell n}), nu \neq 0], \quad x_u \mapsto \begin{cases} b_u\,, \text{ if } \quad u \in Z(\overline{n}) \\ x_u, \text{ else} \end{cases}.$$

We denote by V_J the 0-dimensional affine variety (hypothetically 0-dimensional if $\nu = 1$) defined by the ideal J. Let $\rho : Z(\overline{n}) \times Z(\overline{\ell}) \to Z(\overline{\ell n})$ be the group isomorphism given by $(x, y) \mapsto \ell x + ny$

6.1 Motivation

In order to find the points of the variety V_J a first idea is to use an efficient Gröbner basis computation algorithm [BW93] such as F_4 [Fau99]. We have carried out computations in the case $g = 2$, $\nu = 1$ and $\ell = 3$ with respect to a total degree order (the DRL [AL94,CLO92] or grevlex order) using the computer algebra system Magma [BCP97] implementation of F_4. From our computation, we conclude that

- even for a small coefficient field ($k = \mathbb{F}_{3^{10}}$), it takes 20 hours of computations using Magma on a powerful computer with 16 GB of RAM to obtain a Gröbner basis of J.
- as expected from the computations of Section 5, the number of solutions in the algebraic closure $\overline{k}$ of k is big: 30853 solutions in characteristic 3 (we note that this is consistent with the number of solutions discussed after Proposition 20 when $g = 2$, $\nu = 2$ and $\ell = 3$ since it is smaller than 51840).
- to fully solve the system (that is to say, find explicitly all the solutions in $\overline{k}$) we need to compute a second Gröbner basis with respect to a lexicographical order.

This last operation can be done using the FGLM [FGLM93] algorithm. In our case it is equivalent to computing the characteristic polynomial of a 30853×30853 matrix. This computation did not finish using Magma for the base field $k = \mathbb{F}_{3^{10}}$. So we see that even for $g = 2$, $\nu = 1$ and $\ell = 3$ the computation of the points of V_J is painful using a generic algorithm. In this section, we give an algorithm

to solve the algebraic system defined by J for small ℓ over a big coefficient field efficiently. As an application of our method, we can mention the initialisation phase of a point counting algorithm [CL09]. Because this last point counting algorithm is efficient for curves defined over a field of small characteristic p (equal to ℓ), but has a bad behavior with respect to p, in this part, we are mainly interested by the complexity of the algorithms in the size of k.

The main idea of our algorithm is to use explicitly the symmetry inside the problem deduced from the action of the theta group: we compute a Gröbner basis not for the whole ideal J but rather a Gröbner basis of a well chosen projection $J \cap k[x_{\rho(v,\lambda)} | v \in Z(\overline{n})]$ for $\lambda \in Z(\overline{\ell})$. With our strategy, the same problem ($k = \mathbb{F}_{3^{10}}$) can be solved in seconds and far bigger problems ($k = \mathbb{F}_{3^{1500}}$) can be solved in less than 1 hour (see Section 6.6 for experimental results).

6.2 Intuitions behind the algorithm

Our method is a combination of existing algorithms and the results of Section 5. As explained before we need to take advantage of the structure of the polynomial system (symmetries) to speedup the computations. Solving efficiently polynomial systems with symmetries is a difficult open issue. In this paper, we propose an ad hoc algorithm which is somewhat similar to the algorithm given in [**?**] for bilinear systems. The two important parameters to estimate the complexity of computing Gröbner bases of 0-dimensional ideals are the total number of solutions and the maximal degree of the polynomials occurring in the computations (this is also known as the degree of regularity of the ideal). We first recall the bounds in the case of bilinear systems, then we go back to the equations of Theorem 4.

We first give an example to motivate our strategy. In the following we denote by T the set $[x_1, \ldots, x_s]$ of variables and we make the hypothesis that we can split the set of variables into two *non-empty* subsets $T = X \cup Y$. Suppose that we are given an ideal $J \subset k[T]$ generated by quadratic polynomials $[f_1, \ldots, f_m]$ such that for $i = 1, \ldots, m$, f_i is a polynomial in $k[T]$ which is also bilinear; that is to say f_i is linear with respect to each set of variables X and Y. When $m = s$ and under some regularity assumption (see theorem 6 in [**?**]) it can be proved that a Gröbner basis with respect to a total degree ordering of the ideal $K = J \cap k[Y]$ is composed of polynomials of degree less than $1 + \min(\#X, \#Y)$. In other words the ideal K can be generated by polynomials of degree as low as $1 + \min(\#X, \#Y)$. On the other hand, if we consider an ideal $I \subset k[T]$ generated by quadratic polynomials $[h_1, \ldots, h_s]$, it is well known that a Gröbner basis of I contains polynomials of degree $1 + s = 1 + \#X + \#Y$ (Macaulay bound) when the sequence $h_1, \ldots, h_s$ is regular. In summary, for an ideal J generated by bilinear systems and a well chosen set of variables X and Y the ideal $J \cap k[Y]$ can be generated by polynomials of degree less than expected (more precisely of degree less than the maximal degree of the polynomials of a Gröbner basis of an ideal generated by generic polynomials of the same degree). Moreover, the total number of solutions counted with multiplicities of I is 2^s as given by the Bézout bound whereas in the case of the ideal J generated by bilinear polynomials this number drops to $\binom{s}{\#Y} \ll 2^s$ when $s \to \infty$. Thus, we observe that when $\#Y$ is

constant then the number of solutions is polynomial in s and a Gröbner basis for any monomial ordering can be computed in polynomial time.

Now we go back to the equation of Theorem 4: even if the equations are not bilinear we will apply a similar strategy. We chose $j \in Z(\overline{\ell})$ and we split the set variables into two sets: $Y = [x_{\rho(u,j)} | u \in Z(\overline{n})]$ and $X = T \backslash Y$. For fixed g and ν the cardinality of Y is also fixed. Moreover, we know by Proposition 21 that the solutions of the system $J \cap k[Y]$ can be either the origin point of $\mathbb{A}^{Z(\overline{n})}$ or represent a ℓ-torsion point of $V_{I_{\Theta_{\overline{n}}^B}}$. In this last case, by Lemma 22 we know that there are ℓ solutions of J corresponding to the same projective point. Denote by D the number of solutions of $J \cap k[Y]$ counted with multiplicities. As there are ℓ^{2g} ℓ-torsion points in $V_{I_{\Theta_{\overline{n}}^B}}$, we have $D \leqslant \ell^{2g+1} + 1$. Hence, following [**?**], we compute a Gröbner basis of the ideal J generated by polynomials of Theorem 4 for a special elimination ordering with respect to the two blocks of variables X and Y: when comparing two monomials m and m' we first try to establish if $\deg_X(m) < \deg_X(m')$ or $\deg_X(m) > \deg_X(m')$ where $\deg_X$ designates the total degree with respect to the first block of variables X. The intuition is that we hope to eliminate more quickly the variables from the first block X and so to compute a Gröbner basis of $K = J \cap k[Y]$. Contrarily to the case of bilinear systems we cannot prove any bound on the degree of regularity of the ideal J but we have made extensive computations which show that in general our algorithm is much more efficient than a general purpose Gröbner basis algorithm.

It is easy to detect if the system has no solution since in that case any Gröbner basis of K contains the constant polynomial 1. Now, if we assume that a solution exists, then by Proposition 21 there exists a subgroup G of rank at least 1 of the ℓ-torsion group of $V_{I_{\Theta_{\overline{n}}^B}}$ such that all the points of G are defined over k. As the solutions of $J \cap k[Y]$ are points of $V_{I_{\Theta_{\overline{n}}^B}}[\ell]$, we conclude that for some $r \geqslant \ell$ we have:

$$\sqrt{J} = P_1 \cap \cdots \cap P_r \text{ where } P_i \text{ is a prime ideal and } \deg(P_i) = 1.$$

Hence as soon as we obtain a Gröbner basis of K, we compute a prime decomposition of the ideal K (so that we need to factorize univariate polynomials). When the characteristic of k is precisely equal to ℓ, the ideals J and K are not reduced; in that case we can take advantage of this fact to obtain a faster algorithm: as soon as we obtain a Gröbner basis of K we compute a Gröbner basis of $\sqrt{K}$ (this can be done efficiently using gcd operations) before computing a decomposition into primes.

6.3 General strategy

In the following, J is the ideal generated by polynomials given in Theorem 4; we give a general strategy for computing at least one solution of the corresponding system (that is to say one point in V_J). All the steps of our algorithm are standard with the exception of step 1 and step 4.

Step 1 For any non-zero $j \in Z(\bar{\ell})$, let $Y = [x_{\rho(u,j)} | u \in Z(\overline{n})]$. Using a dedicated algorithm given in Section 6.4, we compute a truncated Gröbner basis for an elimination order and a modified graduation. This allows us to obtain an ideal K_1 (which is zero-dimensional as a $k[Y]$-ideal). In general K_1 is not equal to K. The output of the algorithm is a sequence of polynomials $[p_1, \ldots, p_\kappa]$ in $k[Y]$ such that K_1 is generated by $(p_1, \ldots, p_\kappa)$.

Step 2 Compute a Gröbner basis G_{DRL} of K_1 for a total degree order (DRL or grevlex). This can be done with any efficient algorithm for computing Gröbner basis, for instance F_4.

Step 3 Compute a Gröbner basis G_{Lex} of K_1 for a lexicographical order. This can be done by using the FGLM algorithm [**?**] to change the monomial order of G_{DRL}.

Step 4 Using the method of Section 6.4, compute a decomposition into primes of the following ideal:

$$\sqrt{K_1} = P_1 \cap \cdots \cap P_r$$

We assume that $\deg(P_i) = 1$ (if it is not the case we replace k by some finite extension of k a minimal polynomial of which is easy to obtain since each P_i is described by a lexicographical Gröbner basis, so we can compute explicitly the splitting field of each univariate polynomials occurring in each Gröbner bases).

Step 5 For i from 1 to r, we repeat the following Steps a,b,c for the ideal $(P_i) + J$:

(a) Compute a Gröbner basis G_i of $(P_i) + J$ for a total degree order (DRL).

(b) Change the monomial order to obtain G'_i a lexicographical Gröbner basis of $(P_i) + J$.

(c) Compute a decomposition into primes: $\sqrt{P_i + J} = P_{j_{i-1}+1} \cap \cdots P_{j_i}$ (by convention $j_0 = r$).

Since we have $\sqrt{J} = \sqrt{K_1 \cap J} = \sqrt{P_1 \cap J} \cap \cdots \cap \sqrt{P_r \cap J}$ and since the decomposition of each component $\sqrt{P_i \cap J}$ is done by step 5 of the previous algorithm, we obtain a decomposition of the ideal I:

$$\sqrt{J} = P_{r+1} \cap \cdots \cap P_{j_r}.$$

Remark 26: We can use Theorem 23 in order to recognize a valid theta null point given a geometric point P of V_J. Once we have obtained a point P of V_J corresponding to a valid theta null point, by Proposition 20 we can easily recover all the solutions of V_J corresponding to the same isotropic subgroup K of B_k using the action given by Proposition 18.

6.4 Description of the algorithm

In this section, we give a detailed explanation of the Step 1 and Step 4 of the algorithm described in Section 6.3.

Step 1: elimination algorithm

The normal strategy for computing Gröbner bases (Buchberger, F_4, F_5) consists in considering first the pairs with the minimal total degree among the list of critical pairs (see [CLO92,Bec93], for instance).

In the following, to select critical pairs, we consider only the total degree with respect to the first set of variables X. More precisely:

Definition 27: *Partial degree of critical pair $p = (f, g)$:*

$$\deg_X(p) = \textit{total degree of } \operatorname{lcm}\left(\underset{<}{\mathrm{LT}}(f), \underset{<}{\mathrm{LT}}(g)\right) \textit{ in the polynomial ring } R[X] \textit{ where } R = k[Y].$$

Moreover, we stop the computation of the Gröbner basis as soon as we find a zero dimensional system in $k[Y]$.

To this end, we will use the following well known algorithmic criterion to determine when a variety in $\overline{k}^n$ contains only a finite number of points:

Proposition 28: *Let K be an ideal in $k[x_{\kappa+1}, \ldots, x_s]$. Let $V = V_K$ be an affine variety in $\overline{k}^{s-\kappa}$ and fix a monomial ordering in $k[x_{\kappa+1}, \ldots, x_s]$. Then the following statements are equivalent:*

1. *V is a finite set.*
2. *Let G be a Gröbner basis for K. Then $\left\langle \sqrt{\mathrm{LT}_<(g)} \mid g \in G \right\rangle = \langle x_{\kappa+1}, \ldots, x_s \rangle$ where*
$$\sqrt{x_{\kappa+1}^{\alpha_{\kappa+1}} \cdots x_s^{\alpha_s}} = x_{\kappa+1}^{\min(1,\alpha_{\kappa+1})} \cdots x_s^{\min(1,\alpha_s)}$$

Algorithm 29: Algorithm F_4 (main loop – modified version)

Input: $\begin{cases} F \text{ a finite subset of } k[x_1, \ldots, x_s] \\ < \text{ a monomial admissible order} \\ X = [x_1, \ldots, x_\kappa] \text{ and } Y = [x_{\kappa+1}, \ldots, x_s] \end{cases}$
Output: a finite subset of $k[x_1, \ldots, x_s]$.
$G := F$ and $P := \left\{\mathrm{CritPair}(f, g) \mid (f, g) \in G^2 \text{ with } f \neq g\right\}$
while $P \neq \varnothing$ and $\dim(G \cap k[Y]) \neq 0$ **do**
  $d := \min\{\deg_X(p) \mid p \in P\}$ minimal partial degree of critical pairs
  extract from P, P_d the list of critical pairs of degree d
  $R :=$MATRIX_REDUCTION$(\mathrm{Left}(P_d) \cup \mathrm{Right}(P_d), G)$
  for $h \in R$ **do**
    $P := P \cup \{\mathrm{CritPair}(h, g) \mid g \in G\}$
    $G := G \cup \{h\}$
return G

Step 4: decomposition into primes

The known general purpose algorithms to compute a primary decomposition of an ideal are inefficient in our case. To speed up the computation, we proceed as follow:

Step 1 The basis G_{Lex} always contains a univariate polynomial $g(x_s)$. We can factorize this polynomial. As we will see in the experimental section this is the most consuming part of the whole algorithm. We obtain

$$g(x_s) = f_1(x_s)^{\alpha_1} \cdots f_l(x_s)^{\alpha_l}.$$

Step 2 For all factors i from 1 to l we apply the lextriangular algorithm [Laz92] to obtain efficiently a decomposition into triangular sets of $J_1 + \langle f_i(x_s)\rangle$.
We can describe the algorithm beginning by the special case of two variables $[x_{s-1}, x_s]$ (this enough in our case since we assume that $k = \overline{k}$ as we will see later). The general shape of a Gröbner basis with respect to a lexicographical ordering is as follows [Laz85, Theorem 1]:

$$G_{\text{Lex}} = \begin{cases} g(x_s) \\ h_1(x_{s-1}, x_s) = g_1(x_s)\left(x_{s-1}^{k_1} + \cdots\right) \\ h_2(x_{s-1}, x_s) = g_2(x_s)\left(x_{s-1}^{k_2} + \cdots\right) \\ \cdots \\ h_s(x_{s-1}, x_s) = x_{s-1}^{k_s} + \cdots \\ \text{polynomials in variables } x_1, \ldots, x_s \end{cases} \tag{32}$$

with $k_1 < k_2 < \cdots < k_s$ and $g_{s-1}(x_s) \mid \cdots \mid g_2(x_s) \mid g_1(x_s)$. Hence we can obtain easily some factors of $g(x_s)$:

$$\begin{aligned} g(x_s) &= \left(\frac{g(x_s)}{g_1(x_s)}\right) g_1(x_s) \\ &= \left(\frac{g(x_s)}{g_1(x_s)}\right)\left(\frac{g_1(x_s)}{g_2(x_s)}\right) g_2(x_s) \\ &= \cdots \end{aligned}$$

Step 3 For any factor $f_i(x_s)$ of $g(x_s) = f_1(x_s)^{\alpha_1} \cdots f_l(x_s)^{\alpha_l}$, it is enough to find the first element $h_j(x_{s-1}, x_s)$ of the Gröbner basis such that

$$\gcd(f_i(x_s), g_j(x_s)) \neq 0.$$

By doing a finite extension of $k' \subset k$ if necessary, we can suppose that each factor is linear $f_i(x_s) = x_s - \beta_i$ so that we search for the first j such that $g_j(\beta_i) \neq 0$: then we obtain a new polynomial in one variable $h_j(x_{s-1}, \beta_i)$ that can be factorized. Hence we can iterate the algorithm for all the other variables $x_{s-2}, \ldots, x_1$.

6.5 First experiments and optimizations

In this section, we give running times for an implementation of the strategy that we have presented in Section 6.2. We also explain some important optimizations.

The main motivation of the examples presented is this section, is to illustrate that the initialisation phase of the point counting algorithm described in [CL09] can be made efficient enough to be negligible in the overall running time of the algorithm. For this, we take $g = 2$ and $n = 2$ and we work over a field k of characteristic 3 or 5. We construct a theta null point of level 2 corresponding to an abelian variety B_k of dimension 2. In order to obtain a theta null point of level 2, we can proceed in the following way:

- first compute a theta null point $(b'_u)_{u\in Z(\overline{4})}$ of level 4 by picking up at random a geometric point of the affine variety defined by the equations of Theorem 4 ;
- then obtain the level 2 theta null point $(b_u)_{u\in Z(\overline{2})}$ by letting $b_u = b'_{2u}$ for all $u \in Z(\overline{2})$.

We explain how to pick up at random an element of $\overline{\mathcal{M}}_{\overline{n}}$. Start with a generic point $(x_u)_{u\in Z(\overline{n})}$, we chose randomly $\dim \overline{\mathcal{M}}_{\overline{n}}$ elements of k that we use in order to specialise $\dim \overline{\mathcal{M}}_{\overline{n}}$ coordinates of $(x_u)_{u\in Z(\overline{n})}$. Then we recover the other coordinates of $(x_u)_{u\in Z(\overline{n})}$ using the zero dimensional algebraic system provided by the equations of Theorem 4 where we have substituted a_u by x_u for all $u \in Z(\overline{n})$ (if we have to chose between different roots we pick up one at random). We repeat this process until we find a point defined over k.

We construct the modular correspondence of level ℓ where ℓ is the characteristic of k. Any valid solution of the modular correspondence will corresponds to the theta null point of level 2ℓ of an abelian variety isogeneous to B_k. We can then use the algorithm of [CL09] to count the number of points of B_k.

First experiments As explained in 6.1 if we try to compute directly a Gröbner basis of the ideal generated by the equations, even when k is very small ($k = \mathbb{F}_{3^{10}}$ for instance), it takes 20 hours of computations on a computer with 16 GB of RAM just to compute a DRL Gröbner basis. Moreover, in characteristic 3, there is a huge number of solutions: 30853. This implies that there is no hope to solve efficiently the corresponding problem directly.

Keeping the notations of the beginning of Section 6, we apply the method described in 6.3 to find the solutions of J. We let $\nu = 1$, $\ell = 3$ and $g = 2$ so that $Z(\overline{\ell n}) = (\mathbb{Z}/6\mathbb{Z})^2$. Let $T = [x_u | u \in Z(\overline{\ell n})]$. For $j \in Z(\overline{\ell})$, we define $Y = [x_{\rho(u,j)} | u \in Z(\overline{n})]$. Taking $j = \rho(0, 1)$ and in the following, for $u = (i, j) \in Z(\overline{\ell n})$, we let $x_u = x_{ij}$. With these notations, we take $Y = [x_{31}, x_{32}, x_{02}, x_{01}]$ and $X = T\backslash Y$ the set of all other variables. Then we consider J embedded in the polynomial ring $k[T]$ where k is $\mathbb{F}_{3^{k'}}$ or $\mathbb{F}_{5^{k'}}$. In that case $J \cap k[x_{31}, x_{32}, x_{02}, x_{01}] = J \cap k[Y]$ is an ideal of degree 160 (to be compared with 30853 the degree of the whole ideal J). When $k = \mathbb{F}_{5^{k'}}$ (resp. $k = \mathbb{F}_{3^{k'}}$) the polynomial $g(x_s)$ obtained in section 6.4 is a square-free polynomial of degree 124 (resp. a non square-free polynomial of degree 70). We report in the following table some experiments using the algorithm of section 6.3 implemented in Magma and in C (see section 6.6 for a full description of the experimental framework). First we consider only very small example:

Algo 6.3	Step 1	Step 2 + Step 3	Step 4	Step 5
$k = \mathbb{F}_{5^{10}}$	0.35 sec	0.25 sec	3.25 sec	8.86 sec
$k = \mathbb{F}_{5^{20}}$	0.35 sec	1.14 sec	28.44 sec	48.94 sec

While the theoretical complexity is linear in the size of k it is clear from the example that, in practice, the behavior of the magma implementation is not linear in $\log(k)$ as one might expect from an optimal implementation. Moreover, when we increase the size of k, step 5 becomes the most consuming part of our algorithm. Hence, even if the new algorithm is efficient enough to solve the problem for a small base field k, the problems become intractable when $\#k > 5^{100}$. In the next paragraph we propose several optimizations to overcome this limitation.

Optimizations The idea is to apply the algorithm of section 6.3 *recursively* to perform Step 5: we split again the remaining variables into two parts: $X = X' \cup Y' = X' \cup [x_{42}, x_{21}, x_{51}, x_{12}]$ as in the Step 1 of the algorithm but choosing another j.

Algo 6.3	Original Step 5	Recursive Step 5
$k = \mathbb{F}_{5^{10}}$	8.86 sec	0.8 sec
$k = \mathbb{F}_{5^{20}}$	48.94 sec	4.1 sec
$k = \mathbb{F}_{5^{40}}$		9.78 sec

When $k = \mathbb{F}_{3^{k'}}$ we obtain in step 3 of Algorithm 6.3 the following lexicographical Gröbner basis:

$$\begin{cases} g\left(x_{01}\right) \text{ of degree } 70 \\ h_1\left(x_{02}, x_{01}\right) = g_1\left(x_{01}\right)\left(x_{02}^2 + \cdots\right) \text{ and } g_1 \text{ of degree } 39 \\ h_2\left(x_{02}, x_{0,1}\right) = x_{02}^3 + \cdots \\ \cdots \text{ polynomials in variables } x_{31}, x_{32}, x_{02}, x_{01} \end{cases}$$

and thus we can split $g\left(x_{01}\right)$ into two factors:

$$\begin{aligned} g_1\left(x_{01}\right) &= \left(x_{01} + \alpha_1\right)^3 \left(x_{01} + \alpha_2\right)^9 \cdots \left(x_{01} + \alpha_4\right)^9 \\ \frac{g\left(x_{01}\right)}{g_1\left(x_{01}\right)} &= x_{01} \left(x_{01} + \beta_1\right)^3 \left(x_{01} + \beta_2\right)^9 \cdots \left(x_{01} + \beta_3\right)^9 \end{aligned}$$

Hence the polynomial $g_1\left(x_{01}\right)$ can be efficiently factorized when k is big.

6.6 Experimental results

Programming language and workstation
The experimental results have been obtained with several Xeon bi-processor 3.2 GHz, with 16 GB of RAM. The instances of our problem have been generated using the Magma software. We used the Magma version 2.14 for our computations. The F_5 [Fau02] algorithm has been implemented in language C in the FGb software [**?**] and we used this implementation for computing the first Gröbner basis. All the

other computations are performed under Magma including factorizing some univariate polynomials and computing Gröbner basis using the F_4 algorithm.

Table Notation

The following notations are used in the tables of Fig.1 and Fig.2 below:

- k is the ground field, $k' \supset k$ is the field extension (as explained in step 4 on page 30, we sometimes have to consider an extension k' of k). The practical behavior of our algorithm is strongly depending on the size of k'; hence, since k is fixed, the practical depends strongly on the degree of the field extension $[k' : k]$. In order to obtain consistent data in the following tables we keep only the case $[k' : k] = 2$.
- T is the total CPU time (in seconds) for the whole algorithm.
- T_{Gen} is the time for generating the Riemann equations and computing a valid level 2 theta null point (Magma).
- T_{Grob} is the sum of the Gröbner bases computations (FGb and Magma).
- T_{Fact} is the sum of the Factorization steps (Magma).
- T_1 is the total time of the algorithm excluding generating the equations: $T_1 = T - T_{\text{Gen}}$.

$\sharp k$	$\sharp k$'	T_{Gen}	T_{Grob}	T_{Fact}	T_1	T
5^{50}	5^{100}	1.9	2.7	9.3	12	14
5^{70}	5^{140}	3.4	3.3	16.0	19	23
5^{100}	5^{200}	19.5	15.9	116.7	133	152
5^{150}	5^{300}	27.9	16.8	159.7	177	205
5^{200}	5^{400}	141.3	57.3	401.0	459	600
5^{250}	5^{500}	178.4	62.1	651.8	715	893
5^{300}	5^{600}	227.8	86.7	935.3	1023	1251
5^{350}	5^{700}	674.8	108.5	1306.1	1416	2091
5^{400}	5^{800}	764.1	100.5	2411.3	2513	3277
5^{450}	5^{900}	1144.0	165.3	2451.3	2619	3763
5^{500}	5^{1000}	1070.1	185.4	2990.0	3177	4247
5^{600}	5^{1200}	1979.5	273.5	4888.6	5164	7144
5^{700}	5^{1400}	3278.0	422.5	6872.2	7297	10575

Fig 1: Algorithm $\ell = 3$, characteristic of k is 5.

$\#k$	$\#k$'	T_{Gen}	T_{Grob}	T_{Fact}	T_1	T
3^{80}	3^{160}	3.6	2.0	0.4	3	7
3^{80}	3^{160}	3.6	2.0	0.2	3	6
3^{200}	3^{400}	29.0	11.1	6.9	20	49
3^{600}	3^{1200}	239.2	36.2	44.5	88	327
3^{800}	3^{1600}	403.7	50.6	89.6	150	554
3^{1000}	3^{2000}	591.8	61.8	151.0	225	816
3^{1500}	3^{3000}	2122.0	137.7	474.5	666	2788
3^{3000}	3^{6000}	11219.9	396.3	3229.6	3704	14923

Fig 2: Algorithm $\ell = 3$, characteristic of k is 3.

Interpretation of the results

– In characteristic 3, the hardest part is the generation of the equations and the computation of a valid level 2 theta null point: $T_{\mathrm{Gen}} \approx T$. In characteristic, 5 we have $T \approx 3\,T_{\mathrm{Gen}}$.
– The most consuming part in the algorithm described in 6.3 is the univariate factorization. Moreover due to the implementation in Magma T_{Fact} is not really linear in the size of k.
– The algorithm is much more efficient in characteristic 3 since:
  • All the solutions occur with some multiplicity, hence we have to deal with not square-free polynomials. As a consequence, the degree of the univariate polynomials can be decreased by taking the square-free part of the polynomials.
  • The corresponding Gröbner bases are in not in shape-position: as explain in section 6.4 we can split the univariate polynomial by taking a gcd.
– The algorithm is very efficient since we can completely find the solutions of the ideal J for sizes of the base field $k = 3^{1500}$ or $k = 5^{700}$ which are interesting for point counting application.

References

[AL94] W. Adams and P. Loustaunau. *An introduction to Gröbner bases*, volume 3 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1994.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma Algebra System I: The User Language. *J. Symbolic Comp.*, 24(3):235–265, 1997.

[Bec93] Becker T. and Weispfenning V. *Groebner Bases, a Computationnal Approach to Commutative Algebra*. Graduate Texts in Mathematics. Springer-Verlag, 1993.

[BL04] C. Birkenhake and H. Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundament al Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[BW93] T. Becker and V. Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993. A computational approach to commutative algebra, In cooperation with Heinz Kredel.

[CL09] R. Carls and D. Lubicz. A p-adic quasi-quadratic time point counting algorithm. *Int. Math. Res. Not. IMRN*, (4):698–735, 2009.

[CLO92] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties and Algorithms*. Springer Verlag, New York, 1992.

[Elk98] N. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 21–76. Amer. Math. Soc., Providence, RI, 1998.

[Fau99] J. C. Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *J. Pure Appl. Algebra*, 139(1-3):61–88, 1999. Effective methods in algebraic geometry (Saint-Malo, 1998).

[Fau02] J. C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 75–83 (electronic), New York, 2002. ACM.

[FGLM93] J. C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symbolic Comput.*, 16(4):329–344, 1993.

[Kem89] G.R. Kempf. Linear systems on abelian varieties. *American Journal of Mathematics*, 111(1):65–94, 1989.

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

[Laz85] D. Lazard. Ideal Bases and Primary Primary Decomposition:Case of Two Variables. *JSC*, 1(3):261–270, September 1985.

[Laz92] D. Lazard. Solving zero-dimensional algebraic systems. *JSC*, 13(2):117–132, February 1992.

[LL06] R. Lercier and D. Lubicz. A quasi quadratic time algorithm for hyperelliptic curve point counting. *Ramanujan J.*, 12(3):399–423, 2006.

[LR10] D. Lubicz and D. Robert. Efficient pairing computation with theta functions, 2010. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings.

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

[Mum67a] D. Mumford. On the equations defining abelian varieties. II. *Invent. Math.*, 3:75–135, 1967.

[Mum67b] D. Mumford. On the equations defining abelian varieties. II. *Invent. Math.*, 3:75–135, 1967.

[Mum70a] D. Mumford. *Abelian varieties.* Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[Mum70b] D. Mumford. *Abelian varieties.* Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[Mum84] D. Mumford. *Tata lectures on theta II*, volume 43 of *Progress in Mathematics.* Birkhäuser Boston Inc., Boston, MA, 1984. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura.

[Sat00] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000.

[Sch95] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théorie des nombres de Bordeaux*, 7(1):219–254, 1995.

[VPV01] F. Vercauteren, B. Preneel, and J. Vandewalle. A memory efficient version of Satoh's algorithm. In *Advances in cryptology—EUROCRYPT 2001 (Innsbruck)*, volume 2045 of *Lecture Notes in Comput. Sci.*, pages 1–13. Springer, Berlin, 2001.