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, Universté de Rennes 1, Campus de Beaulieu, F-35042 Rennes
[4] LORIA, CACAO Project
Campus Scientifique
BP 239
54506 Vandoeuvre-lès-Nancy Cedex

Abstract. The aim of this paper is to give a higher dimensional equivalent of the classical modular polynomials $\Phi_\ell(X,Y)$. 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 the curves which are ℓ-isogeneous to E_k. Denote by $X_0(N)$ the modular curve which parametrizes the set of elliptic curves together with a N-torsion subgroup. It is possible to interpret $\Phi_\ell(X,Y)$ as an equation cutting out the image of a certain modular correspondence $X_0(\ell) \to X_0(1) \times X_0(1)$ in the product $X_0(1) \times X_0(1)$. Let g be a positive integer and $\overline{n} \in \mathbb{N}^g$. We are interested in the moduli space that we denote by $\mathcal{M}_{\overline{n}}$ of abelian varieties of dimension g over a field k together with an ample symmetric line bundle $\mathscr{L}$ and a symmetric theta structure of type $\overline{n}$. If ℓ is a prime and let $\overline{\ell} = (\ell,\ldots,\ell)$, there exists a modular correspondence $\mathcal{M}_{\overline{\ell n}} \to \mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}$. We give a system of algebraic equations defining the image of this modular correspondence. We describe an algorithm to solve this system of algebraic equations which is much more efficient than a general purpose Gröbner basis algorithm. As an application, we explain how this algorithm can be used to speed up the initialisation phase of a point counting algorithm.
Keywords: *Abelian varieties, Theta functions, Isogenies, Modular correspondences.*

1 Introduction

The aim of this paper is to give a higher dimensional equivalent of the classical modular polynomials $\Phi_\ell(X,Y)$. We recall that $\Phi_\ell(X,Y)$ is a polynomial with integer coefficients and that 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 which 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 has 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 which rely 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 an equations given by the modular polynomial $\Phi_p(X,Y)$.

This last algorithm has been improved by Kohel in [Koh03] using the notion of oriented modular correspondence. For $N \in \mathbb{N}^*$, the modular curve $X_0(N)$ parametrizes the set of isomorphism classes of elliptic curves together with a N-torsion subgroup. For instance, the curve $X_0(1)$ is just the line of j-invariants. Let p be prime to N. A rational map of curves $X_0(pN) \to X_0(N) \times X_0(N)$ is an oriented 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 consider the oriented 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 oriented modular correspondences for higher dimensional abelian varieties over a field k. We use a moduli space which is different from the one of [Koh03]. We fix an integer $g > 0$ for the rest of the paper. In the following if n is an integer, $\overline{n}$ denotes the element $(n,\ldots,n) \in \mathbb{Z}^g$. We consider the set of triples of the form $(A_k, \mathscr{L}, \Theta_{\overline{n}})$ where A_k is a g dimensional abelian variety equipped with a symmetric ample line bundle $\mathscr{L}$ and a symmetric theta structure $\Theta_{\overline{n}}$ of type $\overline{n}$. Such a triple is called an abelian variety with a $\overline{n}$-marking. To a triple $(A_k, \mathscr{L}, \Theta_{\overline{n}})$, one can associate following [Mum66] its theta null point. The locus of theta null points corresponding to the set of abelian varieties with a $\overline{n}$-marking is a quasi-projective variety $\mathcal{M}_{\overline{n}}$. Moreover, it is proved in [Mum67] that if $8|n$ then $\mathcal{M}_{\overline{n}}$ is a classifying space for abelian varieties with a $\overline{n}$-marking. We would like to compute oriented modular correspondences in $\mathcal{M}_{\overline{n}}$.

For this, let $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ be an abelian variety with a $(\overline{\ell n})$-marking. We suppose that ℓ and n are relatively prime. From the theta structure $\Theta_{\overline{\ell n}}$, 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, $\mathcal{M}_{\overline{\ell n}} \to \mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}$. 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 solve this system.

This paper is organized as follows. In Section 2 we recall some basic definitions and properties about 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, we define a polynomial system (the equations of the image of $\mathcal{M}_{\overline{\ell n}}$), which solutions give theta null points of isogeneous varieties. 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 or that A_k is ordinary. Denote by $K(\mathscr{L})$ the kernel of the polarization $\mathscr{L}$ and by $G(\mathscr{L})$ the theta group (see [Mum66]) associated to $\mathscr{L}$. The theta group $G(\mathscr{L})$ is by definition the set of pairs (x, ψ) where x is a geometric 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 $\delta = (d_1, \dots, d_g)$ be a finite sequence of integers such that $d_i | d_{i+1}$, we consider the finite group scheme $Z(\delta) = (\mathbb{Z}/d_1\mathbb{Z})_k \times_k \dots \times_k (\mathbb{Z}/d_g\mathbb{Z})_k$ with elementary divisors given by δ. For a well chosen unique δ, the finite group scheme $K(\delta) = Z(\delta) \times \hat{Z}(\delta)$ (where $\hat{Z}(\delta)$ is the Cartier dual of $Z(\delta)$) is isomorphic to $K(\mathscr{L})$ (see [Mum70]). The Heisenberg group of type δ is the scheme $\mathcal{H}(\delta) = \mathbb{G}_{m,k} \times Z(\delta) \times \hat{Z}(\delta)$ together with the group law defined on geometric 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 [Mum66] that a theta structure Θ_δ of type δ is an isomorphism of central extension from $\mathcal{H}(\delta)$ to $G(\mathscr{L})$ fitting in the following diagram:

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{G}_{m,k} \arrow[r] \arrow[d, equal] & \mathcal{H}(\delta) \arrow[r] \arrow[d, "\Theta_\delta"] & K(\delta) \arrow[r] \arrow[d, "\overline{\Theta}_\delta"] & 0 \\ 0 \arrow[r] & \mathbb{G}_{m,k} \arrow[r] & G(\mathscr{L}) \arrow[r, "\kappa"] & K(\mathscr{L}) \arrow[r] & 0 \end{tikzcd} \qquad (1)$$

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 $K_1(\mathscr{L})$. 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 $d = \prod_{i=1}^g d_i$ is the degree of $\mathscr{L}$. We briefly recall the construction of this basis. We recall [Mum66, pp.

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, 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 (see [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 morphism provided 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, pp. 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 $(\vartheta_i)_{i \in Z(\delta)}$ given by:

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

for $(\alpha, i, j) \in \mathcal{H}(\delta)$ and e_δ the commutator pairing on $K(\delta)$, which 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 $(\theta_i)_{i \in Z(\delta)}$ of any point of $K(\mathscr{L})$ from the data of the theta null point associated to $(A_k, \mathscr{L}, \Theta_\delta)$.

Let $\delta = (\delta_1, \ldots, \delta_g) \in \mathbb{N}^g$ and $\delta' = (\delta'_1, \ldots, \delta'_g) \in \mathbb{N}^g$, $\delta|\delta'$ means that for $i = 1, \ldots, g$, $\delta_i|\delta'_i$. If $n \in \mathbb{N}$, $n|\delta$ means that $(n, \ldots, n) \in \mathbb{N}^g|\delta$. If $\delta|\delta'$ 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 $4|\delta$.

Theorem 1. *Denote by $\hat{Z}(\overline{2})$ the dual group of $Z(\overline{2})$. Let $(a_i)_{i \in Z(\delta)}$ be the theta null points associated to an abelian variety with a δ-marking $(A_k, \mathscr{L}, \Theta_\delta)$ where $2|\delta$. For all $x, y, u, v \in Z(2\delta)$ which are congruent modulo $Z(\overline{2})$, 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).

It is moreover proved in [Mum66] 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 1.

A consequence of Theorem 1 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 $(A_k, \mathscr{L})$ from which it comes from. In fact, the abelian variety A_k is defined by the homogeneous equations of Theorem 1. 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 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 $2|\delta$. For all $x, y, u, v \in Z(2\delta)$ which are congruent modulo $Z(\delta)$, 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 $a_i = a_{-i}$, $i \in Z(\delta)$.

The Theorem 2 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 symmetry relations together with the relations from theorem 2. Mumford proved in [Mum67] the following

Theorem 3. *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 1. 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 7), hence the notation.

3 Theta null points and isogenies

In this section, we are interested in the following situation. Let ℓ and n be relatively prime integers and suppose that n is divisible by 2. Let $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ be a g-dimensional abelian variety together with a $(\overline{\ell n})$-marking. We recall that the theta structure $\Theta_{\overline{\ell n}}$ 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 a maximal isotropic ℓ-torsion subgroup of $K(\mathscr{L})$ compatible with the decomposition (4). 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 paragraph, we explain that a choice of K determines a certain abelian variety together with a $\overline{n}$-marking. The main results of this Section are Corollary 1 and Proposition 3 which explain how to compute the theta null points associated to the abelian variety together with a $\overline{n}$-marking defined by a choice of 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 deduced from the diagram (1). 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 $\Theta_{\overline{\ell n}}$. 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 a $\overline{n}$-marking on X_k. Let $G^*(\mathscr{L})$ be the centralizer of $\tilde{K}$ in $G(\mathscr{L})$. Applying [Mum66, Proposition 2 pp. 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 $1_{\mathbb{G}_m} \times Z(\overline{n}) \times 0_{\hat{Z}(\overline{n})}$ and $1_{\mathbb{G}_m} \times 0_{Z(\overline{n})} \times \hat{Z}(\overline{n})$, in order to define a theta structure $\Theta_{\overline{n}} : \mathcal{H}(\overline{n}) \to G(\mathscr{X})$, 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 $1_{\mathbb{G}_m} \times 0_{Z(\overline{n})} \times \hat{Z}(\overline{n}) \to G(\mathscr{X})$. Let $Z^*(\overline{\ell n})$ be such that $1_{\mathbb{G}_m} \times Z^*(\overline{\ell n}) \times 0_{\hat{Z}(\overline{\ell n})} = \Theta_{\overline{\ell n}}^{-1}(G^*(\mathscr{L})) \cap Z(\overline{\ell n})$ and let $\hat{Z}^*(\overline{\ell n})$ be such that $1_{\mathbb{G}_m} \times 0_{Z(\overline{\ell n})} \times \hat{Z}^*(\overline{\ell n}) = \Theta_{\overline{\ell n}}^{-1}(G^*(\mathscr{L})) \cap \hat{Z}(\overline{\ell n})$.

As $\hat{Z}^*(\overline{\ell n})$ is in the orthogonal of $\overline{\Theta}_{\overline{\ell n}}^{-1}(K)$ for the commutator pairing, we have $\hat{Z}^*(\overline{\ell n}) = \hat{Z}(\overline{\ell n})$ or $\hat{Z}^*(\overline{\ell n}) = \hat{Z}(\overline{n})$ depending on the choice of $\tilde{K}$. In any case, there exists a natural projection $p : \hat{Z}^*(\overline{\ell n}) \to \hat{Z}(\overline{n})$. In the same way, $Z^*(\overline{\ell n}) = Z(\overline{\ell n})$ or $Z^*(\overline{\ell n}) = Z(\overline{n})$ and there is a natural injection $i : Z(\overline{n}) \to Z^*(\overline{\ell n})$.

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

$$\begin{tikzcd}
(1,0,y)_{y\in\hat{Z}^*(\overline{\ell n})} \arrow[r, "\Theta_{\overline{\ell n}}"] \arrow[d, "\tilde{p}"] & G^*(\mathscr{L}) \arrow[d, "q"] \\
(1,0,y)_{y\in\hat{Z}(\overline{n})} \arrow[r, "\Theta_{\overline{n}}"] & G(\mathscr{X})
\end{tikzcd} \tag{6}$$

$$\begin{tikzcd}
(1,x,0)_{y\in Z^*(\overline{\ell n})} \arrow[r, "\Theta_{\overline{\ell n}}"] & G^*(\mathscr{L}) \arrow[d, "q"] \\
(1,x,0)_{y\in Z(\overline{n})} \arrow[r, "\Theta_{\overline{n}}"] \arrow[u, "\tilde{i}"] & G(\mathscr{X})
\end{tikzcd} \tag{7}$$

where $\tilde{i}$ is deduced from i and $\tilde{p}$ is deduced from p. Using the fact that $\Theta_{\overline{\ell n}}$ is symmetric, it is easy to see that $\Theta_{\overline{n}}$ is also symmetric.

We say that the theta structures $\Theta_{\overline{\ell n}}$ and $\Theta_{\overline{n}}$ 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 $(B_k, \mathscr{L}_0, \Theta_{\overline{n}})$ and $(C_k, \mathscr{M}, \Theta'_{\overline{n}})$ two abelian varieties with a $\overline{n}$-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 deduced 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, pp. 289], we have $[\ell]^*\mathscr{L}_0 = \mathscr{L}_0^{\ell^2}$. The following diagram shows that C_k is obtain by quotienting B_k by a maximal isotropic subgroup of $(B_k, \mathscr{L}_0^{\ell^2})$ of order ℓ^{2g}.

$$\begin{tikzcd}
B_k \arrow[dd, "{[\ell]}"'] \arrow[dr, "\hat{\pi}"] & & \\
& A_k \arrow[dl, "\pi"] \arrow[dr, "\pi'"] & \\
B_k & & C_k
\end{tikzcd} \quad . \tag{9}$$

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

Proposition 2. *Let $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$, $(B_k, \mathscr{L}_0, \Theta_{\overline{n}})$ 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*

$\pi^*(\vartheta_i^{\Theta_{\overline{n}}}) = \omega \vartheta_i^{\Theta_{\overline{\ell n}}}$. *In this last relation,* $Z(\overline{n})$ *is identified as a subgroup of* $Z(\overline{\ell n})$ *via the map* $x \mapsto \ell x$.

Proof. This proposition is a particular case of the isogeny theorem [Mum66, Th. 4] but we give here a direct proof.

Let $\tilde{K}_A$ be the level subgroup of $G(\mathscr{L})$ defined by the image of $(1, 0, y)_{y \in \hat{Z}(\overline{\ell n})}$ by $\Theta_{\overline{\ell n}}$ and let K_A be the subgroup of A_k which is the image of $(0, y)_{y \in \hat{Z}(\overline{\ell n})}$ by $\overline{\Theta}_{\overline{\ell n}}$. Let D_k be the quotient of A_k by K_A and $\pi_A : A_k \to D_k$ the natural projection. The data of $\tilde{K}_A$ gives a couple $(\mathscr{L}_A, \lambda_A)$ where $\mathscr{L}_A$ is a degree one line bundle on D_k and λ_A is an isomorphism $\lambda_A : \pi_A^*(\mathscr{L}_A) \to \mathscr{L}$. We recall that $\tilde{K}$ be the level subgroup of $G(\mathscr{L})$ defined as the intersection of $G = \kappa^{-1}(K)$ 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 $\Theta_{\overline{\ell n}}$.

In the same manner, we can consider $\tilde{K}_B$ the level subgroup of $G(\mathscr{L}_0)$ defined by the image of $(1, 0, y)_{y \in \hat{Z}(\overline{n})}$ by $\Theta_{\overline{n}}$ and K_B the subgroup of B_k which is the image of $(0, y)_{y \in \hat{Z}(\overline{n})}$ by $\overline{\Theta}_{\overline{n}}$. By (6) $K_B = \pi(K_A)$ and by definition of π its kernel K is contained in K_A. We deduce that D_k is the quotient of B_k by K_B and $\pi_A = \pi_B \circ \pi$ where π_B is the natural projection $B_k \to D_k$. Because of (6) and the fact that $\hat{Z}^*(\overline{\ell n}) = \hat{Z}(\overline{\ell n})$, we have an isomorphism $\tilde{K}_B \simeq \tilde{K}_B / \tilde{K}$ and the data of $\tilde{K_B}$ gives a couple $(\mathscr{L}_B, \lambda_B)$ where λ_B is an isomorphism $\lambda_B : \pi_B^*(\mathscr{L}_B) \to \mathscr{L}_0$ and we have $\mathscr{L}_B = \mathscr{L}_A$ and $\lambda_A \circ \pi_A^* = \lambda \circ \pi^* \circ \lambda_B \circ \pi_B^*$.

If s_0 is the unique global section of $\mathscr{L}_A$ up to multiplication by a constant factor, we have $\lambda_A(\pi_A^*(s_0)) = \lambda(\pi^*(\lambda_B(\pi_B^*(s_0))))$. By definition, $\vartheta_0^{\Theta_{\overline{n}}} = \lambda_B(\pi_B^*(s_0))$ and $\vartheta_0^{\Theta_{\overline{\ell n}}} = \lambda_A(\pi_A^*(s_0))$. As a consequence, there exists $\omega \in \overline{k}$ such that we have that $\pi^*(\vartheta_0^{\Theta_{\overline{n}}}) = \omega \vartheta_0^{\Theta_{\overline{\ell n}}}$.

Let $s = \vartheta_0^{\Theta_{\overline{\ell n}}}$ and $s' = \vartheta_0^{\Theta_{\overline{n}}}$. We set for all $i \in Z(\overline{\ell n})$, $(x_i, \psi_i) = \Theta_{\overline{\ell n}}((1, i, 0))$ and for all $i \in Z(n)$, $(x_i', \psi_i') = \Theta_{\overline{n}}((1, i, 0))$. Then $\pi^*(\vartheta_i^{\Theta_{\overline{n}}}) = \pi^*(\psi_i' \tau_{-x_i'}^*(s')) = \psi_i \tau_{-x_i}^* \pi^*(s')$ by the commutativity of (7). But we already know that $\pi^*(s') = \omega s$ and $\psi_i \tau_{-x_i}^*(\omega s) = \omega \vartheta_i^{\Theta_{\overline{\ell n}}}$. This concludes the proof.

As an immediate consequence of the preceding proposition, we have

Corollary 1. *Let* $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ *and* $(B_k, \mathscr{L}_0, \Theta_{\overline{n}})$ *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* $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ *and* $(B_k, \mathscr{L}_0, \Theta_{\overline{n}})$. *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 3. *Let* $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ *and* $(C_k, \mathscr{L}_0, \Theta_{\overline{n}})$ *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* $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ *and* $(C_k, \mathscr{L}_0, \Theta_{\overline{n}})$. *We have for all* $u \in Z(\overline{n})$,

$$c_u = \sum_{t \in Z(\overline{\ell})} a_{u+t}, \tag{10}$$

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 theta structure $\Theta_{\overline{\ell n}}$ (resp. $\Theta'_{\overline{n}}$) induces a decomposition of the kernel of the polarization $K(\mathscr{L}) = K_1(\mathscr{L}) \times K_2(\mathscr{L})$ (resp. $K(\mathscr{M}) = K_1(\mathscr{M}) \times K_2(\mathscr{M})$). Denote by K' the kernel of π'. We have that K' is a subvariety of $K_1(\mathscr{L})$ and we have an isomorphism:

$$\sigma : K_1(\mathscr{L})/K' \to K_1(\mathscr{M}).$$

The hypothesis of [Mum66, Th. 4] are then verified and Equation (10) 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.

We let $(B_k, \mathscr{L}_0, \Theta_{\overline{n}})$ be an abelian variety together with a $\overline{n}$-marking and denote by $(b_u)_{u\in Z(\overline{n})}$ its associated theta null point. Let ν be the 2-adic valuation of n. Unless specified, we shall assume that $\nu \geqslant 3$. Let $\mathscr{C}$ be the reduced subvariety of $\mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}$ which is the image of $\Phi_\ell(\mathcal{M}_{\overline{\ell n}})$ in $\mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}$ given on geometric points by $\pi : (a_u)_{u\in Z(\overline{\ell n})} \mapsto ((a_u)_{u\in Z(\overline{n})}, (\sum_{t\in Z(\overline{\ell})} a_{u+t})_{u\in Z(\overline{n})})$.

Denote by p_1 (resp. p_2) the restriction to $\mathscr{C}$ of the first (resp. second) projection from $\mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}$ into $\mathcal{M}_{\overline{n}}$, and let $\pi_1 = p_1 \circ \pi$, $\pi_2 = p_2 \circ \pi$. We would like to compute the algebraic set $\pi_2(\pi_1^{-1}((b_u)_{u\in Z(\overline{n})}))$. We remark that this question is the analog in our situation to the computation of the solutions of the equation $\Phi_\ell(j, X)$ defined from the modular polynomial and $j \in \overline{k}$ a certain j-invariant.

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 2, 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 morphisms 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 morphism $\tilde{\pi}_1^0$ (resp $\tilde{\pi}_2^0$) restricts to a morphism $\tilde{\pi}_1 : \overline{\mathcal{M}}_{\overline{\ell n}} \to \overline{\mathcal{M}}_{\overline{n}}$ (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 $\mathcal{L} = \mathcal{L}' \cap k[y_u | u \in Z(\overline{n})]$. 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 4. *Keeping the notations from above, let* $(b_u)_{u\in Z(\overline{n})}$ *be the geometric point of* $\mathcal{M}_{\overline{n}}$ *corresponding to* $(B_k, \mathscr{L}_0, \Theta_{\overline{n}})$ *. The algebraic variety* $V^0_{\mathcal{L}} = \pi_2(\pi_1^{-1}(b_u)_{u\in Z(\overline{n})})$ *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 $V^0_{\mathcal{L}}$ has dimension 0. But this follows from the fact that the algebraic variety V_J has dimension 0 [CL08].

From an algorithmic point of view, the hard part of this modular correspondence is the computation of $V^0_J = \pi_1^{-1}((b_u)_{u\in Z(\overline{n})})$, the set of points in V_J that are valid theta null points. 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 the next section (see Theorem 4). But at first we recall the geometric nature of V^0_J given by Section 3:

Proposition 5. V^0_J *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 a* $(\overline{\ell n})$*-marking then* $\Theta_{\overline{\ell n}}$ *is compatible with the theta structure* $\Theta_{\overline{n}}$ *of* B_k*.*

Proof. Let $(a_u)_{u\in Z(\overline{\ell n})}$ be a geometric point of V^0_J. 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 a $\overline{n}$-marking and an isogeny $\pi : A_k \to B'_k$ such that $\Theta_{\overline{\ell n}}$ is compatible with $\Theta'_{\overline{n}}$. By definition of J, Corollary 1 shows that the theta null point of B' is $(b_u)_{u\in Z(\overline{n})}$. As $\nu \geqslant 2$, by Proposition 1 this means that $B' \simeq B$. Since $\nu \geqslant 3$, we even know by Theorem 3 that the triples $(B'_k, \mathscr{L}'_0, \Theta'_{\overline{n}})$ and $(B_k, \mathscr{L}_0, \Theta_{\overline{n}})$ are isomorphic, so that $\Theta_{\overline{\ell n}}$ is compatible with $\Theta_{\overline{n}}$.

We say that the isogeny from Section 3 $A_k \to B_k$ is the $\overline{\ell}$-isogeny associated to the $(\overline{\ell n})$-marking of A_k.

5 The solutions of the system

This section is devoted to the study of the geometric points of V_J. Our aim is twofolds. 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, let $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ be the corresponding abelian variety with a $(\overline{\ell n})$-marking and denote by $\pi : A_k \to B_k$ the isogeny defined in Section 3. From the knowledge of $(a_u)_{u\in Z(\overline{\ell n})}$, one can recover the coordinates the points of a maximal ℓ-torsion subgroup of B_k of rank g. Actually, even if $(a_u)_{u\in Z(\overline{\ell n})}$ is not a valid theta null point it is possible to associate to $(a_u)_{u\in Z(\overline{\ell n})}$ a set of ℓ-torsion points $P_i \in B_k$. The main result of this section is Theorem 4 which states that a geometric point of V_J is non degenerate if and only if the corresponding P_i form a maximal subgroup of rank g of the ℓ-torsion points of B_k. To prove this Theorem, we introduce an action from the automorphisms of the theta group to the modular space $\mathcal{M}_{\overline{\ell n}}$. Using Theorem 4 and this action, we make explicit the structure of V_J: we explain when two valid points give isomorphic varieties in Proposition 9, and how to obtain every degenerate points in the discussion following Proposition 7.

We start by making explicit the structure of the solutions of the algebraic system defined by J. 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 $I_{\Theta_{\overline{n}}}$ the ideal of $k[y_u | u \in Z(\overline{n})]$ for the theta structure $\Theta_{\overline{n}}$ generated by the equations of Theorem 1. The homogeneous ideal $I_{\Theta_{\overline{n}}}$ defines a projective variety $V_{I_{\Theta_{\overline{n}}}}$, isomorphic to B_k.

We have the following proposition [CL08]:

Proposition 6. *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 $(a_{\rho(j,i)})_{j \in Z(\overline{n})} \neq (0, \dots, 0)$, let P_i be the geometric point, of $\mathbb{P}_k^{Z(\overline{n})}$ with homogeneous coordinates $(a_{\rho(j,i)})_{j \in Z(\overline{n})}$. Then for all $i \in Z(\overline{\ell})$ such that P_i is well defined, P_i is a ℓ-torsion point of $V_{I_{\Theta_{\overline{n}}}}$.*

The proof of the preceding proposition in [CL08] proves moreover that if we denote by S the subset of $Z(\overline{\ell})$ such that P_i is well defined for all $i \in S$, then S is a subgroup of $Z(\overline{\ell})$, the set $\{P_i, i \in S\}$ is a subgroup of the group of ℓ-torsion points of $V_{I_{\Theta_{\overline{n}}}}$ and the application $i \in S \to P_i \in B[\ell]$ is a group morphism.

Suppose that $(a_v)_{v \in Z(\overline{\ell n})}$ is a valid theta null point. Let $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ be the corresponding abelian variety with a $(\overline{\ell n})$-marking and denote by $\pi : A_k \to B_k$ the isogeny defined in Section 3. We can consider A_k as a closed subvariety of $\mathbb{P}_k^{Z(\overline{\ell n})}$ via the morphism provided by $\Theta_{\overline{\ell n}}$. 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 points with homogeneous coordinates $(a_{v+ni})_{v \in Z(\overline{\ell n})}$ form the isotropic (for the commutator pairing) ℓ-torsion subgroup K_1 of A_k (with the notations of Section 3). By definition of the isogeny π, we have $\pi((a_{v+ni})_{v \in Z(\overline{\ell n})}) = P_i$ and as a consequence $\pi(K_1) = \{P_i, i \in Z(\overline{\ell})\}$. We see that if $(a_v)_{v \in Z(\overline{\ell n})}$ is a valid theta null point then the $(P_i)_{i \in Z(\overline{\ell})}$ are well defined projective points which form a maximal subgroup of rank g of $B_k[\ell]$. Moreover, since the kernel of π is K_2, $\pi(K_1) = \{P_i, i \in Z(\overline{\ell})\}$ is the kernel of the dual isogeny $\hat{\pi} : B_k \to A_k$.

If $(a_v)_{v \in Z(\overline{\ell n})}$ is a general solution, it can happen that certain of the 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 are well defined, $(a_v)_{v \in Z(\overline{\ell n})}$ need not be a valid theta null point. We need a criterion to identify the solutions of J which correspond to valid theta null points. From the discussion of the preceding paragraph, 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 $(P_i)_{i \in Z(\overline{\ell})}$ are all valid projective points which form a subgroup of rank g if $B_k[\ell]$. The Theorem 4 asserts that this necessary condition is indeed sufficient. In order to prove this theorem, we have to study how a theta null point vary together with a change of the theta structure.

We denote by $\operatorname{Aut}\mathcal{H}(\delta)$ the group of automorphisms ψ of $\mathcal{H}(\delta)$ inducing the identity on $\mathbb{G}_{m,k}$:

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{G}_{m,k} \arrow[r] \arrow[d, equal] & \mathcal{H}(\delta) \arrow[r] \arrow[d, "\psi"] & K(\delta) \arrow[r] \arrow[d, "\overline{\psi}"] & 0 . \\ 0 \arrow[r] & \mathbb{G}_{m,k} \arrow[r] & \mathcal{H}(\delta) \arrow[r] & K(\delta) \arrow[r] & 0 \end{tikzcd}$$

Obviously, the set of all theta structures for $\mathscr{L}$ is a principal homogeneous space for the group $\operatorname{Aut}\mathcal{H}(\delta)$ via the right action $\Theta_\delta.\psi = \Theta_\delta \circ \psi$ for $\psi \in \operatorname{Aut}\mathcal{H}(\delta)$ and Θ_δ a theta structure. So we can identify $\operatorname{Aut}\mathcal{H}(\delta)$ with the group of automorphisms of theta structures. If ψ is such an automorphism, it induces an automorphism $\overline{\psi}$ of $K(\delta)$. The preceding diagram shows that $\overline{\psi}$ is symplectic with respect to the commutator pairing. Denote by $Sp(K(\delta))$ the group of symplectic automorphisms of $K(\delta)$. In order to study the possible extensions of $\overline{\psi} \in Sp(K(\delta))$ to an automorphism of $\mathcal{H}(\delta)$ it is enough to introduce the following definition:

Definition 1. *Let $\overline{\psi} \in Sp(K(\delta))$. A semi-character for the canonical pairing is a map $\chi_{\overline{\psi}} : K(\delta) \to \mathbb{G}_{m,k}$ such that for $(u, v), (u', v') \in K(\delta)$,*

$$\chi_{\overline{\psi}}((u+u', v+v')) = \chi_{\overline{\psi}}((u,v)).\chi_{\overline{\psi}}((u',v')).\overline{\psi}(u',v')_2(\overline{\psi}(u,v)_1).v'(u)^{-1}, \quad (11)$$

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

The preceding definition is motivated by the lemma:

Lemma 1. *Let $\psi \in \operatorname{Aut}\mathcal{H}(\delta)$ et let $\overline{\psi}$ be the associated symplectic automorphism of $K(\delta)$. There exists a unique semi-character $\chi_{\overline{\psi}}$ such that for all $(\alpha, u, v) \in \mathcal{H}(\delta)$,*

$$\psi : (\alpha, (u,v)) \mapsto (\alpha\chi_{\overline{\psi}}((u,v)), \overline{\psi}((u,v)). \quad (12)$$

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 $\operatorname{Aut}\mathcal{H}(\delta)$ and the set of semi-characters.

Proof. By verifying that ψ given by (11) is a group morphism, we obtain that $\chi_{\overline{\psi}}$ is a semi-character. Moreover, it is clear that a semi-character defines by formula (12) a unique extension to $\mathcal{H}(\delta)$ of $\overline{\psi}$.

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 semi-character.

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

Proof. The proof of this lemma is a matter of a simple verification that we leave to the reader.

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 morphism $\Psi : \mathrm{Aut}\,\mathcal{H}(\delta) \to Sp(K(\delta)), \psi \mapsto \overline{\psi}$ is given by automorphisms preserving a symplectic basis and are determined by a choice of level subgroups $\tilde{K}_1$ and $\tilde{K}_2$ over maximal isotropic subspaces K_1 and K_2. It is well known [BL04, pp. 162] 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

$$(\alpha, x, y) \mapsto (\alpha e_\delta(c, x + y), x, y). \tag{13}$$

As a consequence, we get an exact sequence

$$0 \longrightarrow K(\delta) \xrightarrow{\nu} \mathrm{Aut}\,\mathcal{H}(\delta) \longrightarrow Sp(K(\delta)) \longrightarrow 0\ . \tag{14}$$

Suppose that Θ_δ is symmetric, an automorphism $\psi \in \mathrm{Aut}\,\mathcal{H}(\delta)$ is said to be symmetric if it commutes with the symmetric action $(\alpha, x, y) \mapsto (\alpha, -x, -y)$ on $\mathcal{H}(\delta)$. We denote by $\mathrm{Aut_s}\,\mathcal{H}(\delta)$ the group of symmetric automorphisms of $\mathcal{H}(\delta)$. Obviously, an automorphism $\psi \in \mathrm{Aut}\,\mathcal{H}(\delta)$ 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 isomorphism 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 $\mathscr{L}_0$, we can apply the isogeny theorem [Mum66, Th. 4] to obtain

$$\tilde{\vartheta}_0 = \lambda\pi^*(\tilde{s_0}) = \sum_{i\in Z^\psi} \vartheta_i, \tag{15}$$

for $\lambda \in k^*$.

Now by definition we have

$$\tilde{\vartheta}_i = \psi((1, i, 0)).\tilde{\vartheta}_0. \tag{16}$$

where the dot product is the action (2).

By evaluating at 0 the basis of global sections of $\mathscr{L}$ in (16), we get an explicit description of the action of $Sp(K(\delta))$ on the geometric points of $\mathcal{M}_\delta$. Actually the obtained formulas give a valid action of $Sp(K(\delta))$ on the geometric points of $\overline{\mathcal{M}}_\delta$.

Now, let $(a_u)_{u \in Z(\overline{\ell n})}$ be a geometric point of V_J^0. As $\operatorname{Aut_s} \mathcal{H}(\overline{\ell n})$ acts on $\mathcal{M}_{\overline{\ell n}}$, we are interested in the subgroup $\mathfrak{H}$ of $\operatorname{Aut_s} \mathcal{H}(\overline{\ell n})$ that leaves $(a_u)_{u \in Z(\overline{\ell n})}$ in V_J^0.

Lemma 3. *Let $\psi \in \operatorname{Aut_s} \mathcal{H}(\overline{\ell n})$. We say that ψ is compatible with $\mathcal{H}(\overline{n})$ if it commutes with the morphisms $\tilde{p}$ and $\tilde{i}$ from (6) and (7). Then $\mathfrak{H}$ 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 the subgroup of $\operatorname{Aut_s} \mathcal{H}(\overline{\ell n})$ that leaves V_J^0 invariant.*

Proof. Let $(A, \mathscr{L}, \Theta_{\overline{\ell n}})$ be a triple corresponding to the theta null point $(a_u)_{u \in Z(\overline{\ell n})}$. Let $\psi \in \operatorname{Aut_s} \mathcal{H}(\overline{\ell n})$, and $(a'_u)_{u \in Z(\overline{\ell n})} = \psi.(a_u)_{u \in Z(\overline{\ell n})}$. The Proposition 5 shows that $(a'_u)_{u \in Z(\overline{\ell n})}$ is in V_J^0 if and only if the associated theta structure $\Theta_{\overline{\ell n}}.\psi$ is compatible with the theta structure $\Theta_{\overline{n}}$ of B. But this means exactly that ψ is compatible with $\mathcal{H}(\overline{n})$.

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

Proposition 7. *The action of $\mathfrak{H}$ on V_J^0 is generated by the actions given by*

$$(a_u)_{u \in Z(\overline{\ell n})} \mapsto (a_{\psi_2(u)})_{u \in Z(\overline{\ell n})}, \tag{17}$$

where ψ_2 is an automorphism of $Z(\overline{\ell n})$ fixing $Z(\overline{n})$ and

$$(a_u)_{u \in Z(\overline{\ell n})} \mapsto \big(e_{\overline{\ell n}}(\psi_1(u), u).a_u\big)_{u \in Z(\overline{\ell n})}, \tag{18}$$

where ψ_1 is a "symmetric" morphism $Z(\overline{\ell n}) \to \hat{Z}(\overline{\ell}) \subset \hat{Z}(\overline{\ell n})$ and $e_{\overline{\ell n}}$ is the commutator pairing on $\mathcal{H}(\overline{\ell n})$.

Proof. Let $\psi \in \mathfrak{H}$ and denote by $\overline{\psi} \in \operatorname{Sp}(\mathcal{H}(\delta))$ the associated symplectic automorphism. In 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 $M[A,B,C,D] = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SP_\delta^{2g}(\mathbb{Z})$. 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 $D = {}^t A^{-1}$ and we see that $\overline{\psi}$ is in the subgroup of $\operatorname{Sp}(K(\overline{\ell n}))$ generated by the matrices:

1. $M[A,B,C,D]$ such that $C{=}0$. Then A is an automorphism and the compatibility condition implies that it must fix $Z(\overline{n})$. By Lemma 2, 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 easely seen that $\psi' \in \mathfrak{H}$ and using (15) and (16), we see that ψ' yields the action (17).
2. $M[A,B,C,D]$ such that $A = \mathrm{Id}$. Then ${}^t C = C$. 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

$$\overline{\psi}((x,y)) - (x,y) \in \overline{\psi}(\hat{Z}(\overline{\ell})) \subset \hat{Z}(\overline{\ell}), \tag{19}$$

for all $(x, y) \in Z^*(\overline{\ell n}) \times \hat{Z}^*(\overline{\ell n})$. Using (19), we deduce that $\psi_1(x)$ is in $\hat{Z}(\overline{\ell})$. Again, by Lemma 2, 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 (18) following (15) and (16).

Because of the exact sequence from equation (14), 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 (13). 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 2. The action (17) gives an automorphism of the $(P_i)_{i \in Z(\overline{\ell})}$ while the action (18) 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 (18) are generated by

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

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.

From the preceding remark, we see that $\mathfrak{H}$ leaves V_J invariant. Now, let ψ_2 be a morphism of $Z(\overline{\ell n})$ fixing $Z(\overline{n})$. Here we do not require ψ_2 to be an isomorphism. 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 2 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 we have a well defined action extending that of the form (17).

By acting on V_J with a morphism of $Z(\overline{\ell n})$ fixing $Z(\overline{n})$ which is not an isomorphism, 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 6 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

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

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 6 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 6 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 embed S' into a maximal subgroup T of rank g of $B_k[\ell]$, and extend f to a morphism $\tilde{f} : Z(\overline{\ell}) \to T$ (for instance if $i \notin Z(\overline{\ell})$ then send i to the neutral point P'_0). We take an isomorphism h between $Z(\overline{\ell})$ and T. Theorem 4 that we prove later on shows that 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. Now take ψ_2 to be the morphism of $Z(\overline{\ell n}) = Z(\overline{\ell}) \times Z(\overline{n})$ 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 $(a'_u)_{u\in Z(\overline{\ell n})}$. The next lemma shows that it is the same point as $(a'_u)_{u\in Z(\overline{\ell n})}$ up to an action of the form (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 (18) 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 (17) giving the same point.

By Remark 2 we know that if $(a_u)_{u\in Z(\overline{\ell n})}$ is a theta null point giving the associated group $\{P_i, i \in Z(\overline{\ell})\}$, 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 4. *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 $\{P_i, i \in Z(\overline{\ell})\}$. Then there exist $\psi \in \mathfrak{H}$ such that $(d_u)_{u\in Z(\overline{\ell n})} = \psi.(c_u)_{u\in Z(\overline{\ell n})}$.*

Proof. First, up to an action of type (17), 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 exist $\lambda_i \in \overline{k}$ 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 $\lambda_0 = 1$. We will show that up to an action of type (18), 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 $x, y, u, v \in Z(2\overline{n})$ which are congruent modulo $Z(\overline{n})$, we remark that for $\mu \in \{1, \ldots, \ell\}$, $\rho(x, \mu.i)$, $\rho(y, i)$, $\rho(u, 0)$, $\rho(v, 0)$ are elements of $Z(2\overline{\ell n})$ congruent modulo $Z(\overline{\ell n})$. Calling Theorem 2, we obtain that

$$\Big(\sum_{t\in Z(2)} \chi(t) c_{\rho(x+y+t,(\mu+1).i)} c_{\rho(x-y+t,(\mu-1).i)}\Big).\Big(\sum_{t\in Z(2)} \chi(t) c_{\rho(u+v+t,0)} c_{\rho(u-v+t,0)}\Big) = \\ = \Big(\sum_{t\in Z(2)} \chi(t) c_{\rho(x+u+t,\mu.i)} c_{\rho(x-u+t,\mu.i)}\Big).\Big(\sum_{t\in Z(2)} \chi(t) c_{\rho(y+v+t,i)} c_{\rho(y-v+t,i)}\Big), \tag{20}$$

for any $\chi \in \hat{Z}(2)$.

We have a similar formula involving $(d_u)_{u\in Z(\overline{\ell n})}$. Using equation (20) and an easy recurrence, 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

$$\lambda_i^{\ell^2} = \lambda_{\ell.i} = \lambda_0 = 1 \tag{21}$$

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 (21) gives

$$\lambda_i^{\ell} = 1 \tag{22}$$

which concludes the claim.

Let $(e_1, \dots, e_g)$ be the canonical basis of $Z(\bar{\ell})$. Up to an action of type (18) we may assume that $\lambda_{e_i} = 1$ and $\lambda_{e_i+e_j} = 1$ for $i, j \in \{1, \dots, g\}, j < i$. Now let $a, b \in Z(\bar{\ell})$ be such that $\lambda_a = 1$, $\lambda_b = 1$ and $\lambda_{a-b} = 1$. Then by Theorem 2 we have the relations:

$$\Big(\sum_{t\in Z(2)} \chi(t) c_{\rho(x+y+t,a+b)} c_{\rho(x-y+t,a-b)}\Big).\Big(\sum_{t\in Z(2)} \chi(t) c_{\rho(u+v+t,0)} c_{\rho(u-v+t,0)}\Big) = \\ = \Big(\sum_{t\in Z(2)} \chi(t) c_{\rho(x+u+t,-b)} c_{\rho(x-u+t,b)}\Big).\Big(\sum_{t\in Z(2)} \chi(t) c_{\rho(y+v+t,a)} c_{\rho(y-v+t,a)}\Big). \tag{23}$$

Since by symmetry, $\lambda_{-b} = 1$, the relations (23) give that $\lambda_{a+b} = 1$. An easy recurrence shows that for any $i \in Z(\bar{\ell})$ we have $\lambda_i = 1$, which concludes the proof.

As a first application of this lemma, we have:

Proposition 8. *If ℓ is prime to the characteristic of k and $\nu \geqslant 2$ then V_J is a 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 $(B_k, \mathscr{L}_0, \Theta_{\overline{n}})$.

By definition, V_J is a closed subvariety of the affine space $\mathbb{A}^{Z(\overline{\ell n})}$. For $\lambda \in Z(\overline{\ell})$, denote by $\pi_\lambda : \mathbb{A}^{Z(\overline{\ell n})} \to \mathbb{A}^{Z(\overline{n})}$ the projection deduced from the inclusion $\varphi_\lambda : k[x_u | u \in Z(\overline{n})] \to k[x_u | u \in Z(\overline{\ell n})]$, $x_u \mapsto x_{\rho(u,\lambda)}$. In order to prove that V_J is a reduced scheme it is enough to prove that for any x geometric point of V_J and all $\lambda \in Z(\overline{\ell})$, $\pi_\lambda(x)$ is a reduced point of $\mathbb{A}^{Z(\overline{n})}$. We consider two cases.

If $\pi_\lambda(x)$ is not the point at origin of $\mathbb{A}^{Z(\overline{n})}$ then it defines a projective point of $\mathbb{P}^{Z(\overline{\ell})}$ which is a ℓ-torsion point of $V_{I_{\Theta_{\overline{n}}}}$ by Proposition 6. As a consequence, $\pi_\lambda(x)$ is contained in the reduced line L between the origin point of $\mathbb{A}^{Z(\overline{n})}$ and $\pi_\lambda(x)$. By the preceding lemma, the intersection of V_J with L is contained in a variety isomorphic to $\mathrm{Spec}(k[x]/(x^\ell - 1))$ where $x^\ell - 1$ is a separated polynomial as ℓ is prime to the characteristic of k. We deduce that x is a reduced point of $\mathbb{A}^{Z(\overline{n})}$.

If $\pi_\lambda(x)$ is the origin point of $\mathbb{A}^{Z(\overline{n})}$, it is enough to prove that $\pi_\lambda(x)$ is reduced in the case that $\nu = 2$. In fact, the set of equations generating J in the case $\nu \geqslant 2$ contains the set of equations generating J in the case $\nu = 2$. We suppose now that $\nu = 2$. 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 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 exist 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 1.

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 $H(\overline{2}) = \{x \in H(\overline{\ell n}) | x \,\mathrm{is}\, 2-\mathrm{torsion\ modulo}\, Z(\overline{2}) \times \{0\}\}$. By applying [Mum67, formula (C”) p. 334], we have the following relation in J:

$$
\begin{aligned}
&y_{\alpha_1} y_{\alpha_2} y_{\alpha_3} y_{\alpha_4} = \\
&\qquad = \frac{1}{2^g} \sum_{t \in H(\overline{2})} (\tau'' + t'')(2t') y_{\alpha_1 - \tau_1 + t} y_{\alpha_2 + \tau_1 + t} y_{\alpha_3 + \tau_1 + t} y_{\alpha_4 + \tau_1 + t},
\end{aligned} \tag{24}
$$

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 [Mum67, 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 (24). 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 recurrence, we see that if $r_\lambda > 1$ then $r_\lambda = r_{2^m\lambda} < r_\lambda$ which is a contradiction.

As a second application of Lemma 4, we have:

Theorem 4. *Let $(a_u)_{u\in Z(\overline{\ell n})}$ be a geometric point of V_J. 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 $Z(\overline{\ell})$ such that P_i is a well defined projective point for all $i \in S$. If $K = \{P_i, i \in S\}$ is a maximal ℓ-torsion subgroup of $V_{I_{\Theta_{\overline{n}}}}$ of rank g then $(a_u)_{u\in Z(\overline{\ell n})}$ is a well defined theta null point. In other words there exists $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ an abelian variety together with a $(\overline{\ell n})$-marking with associated theta null point $(a_u)_{u\in Z(\overline{\ell n})}$.*

Proof. Let A_k be the quotient of $B_k \simeq V_{I_{\Theta_{\overline{n}}}}$ by K and let $\pi : B_k \to A_k$ be the canonical isogeny. As K is a subgroup of $B_k[\ell]$, there exists an isogeny $\hat{\pi} : A_k \to B_k$ such that $[\ell] = \hat{\pi} \circ \pi$. Let $\mathscr{L} = \hat{\pi}^*(\mathscr{L}_0)$. We are going to show that there exists a certain theta structure $\Theta_{\overline{\ell n}}$ such that the theta null point associated to $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ is $(a_u)_{u\in Z(\overline{\ell n})}$.

Let $K(\mathscr{L}_0) = K_1(\mathscr{L}_0) \times K_2(\mathscr{L}_0)$ be the decomposition into isotropic subspaces for the commutator pairing induced by the theta structure $\Theta_{\overline{n}}$. Denote by $\hat{K}$ the kernel of $\hat{\pi}$. As $\mathscr{L} = \hat{\pi}^*(\mathscr{L}_0)$, we know that $\hat{K}$ is an isotropic subgroup of $K(\mathscr{L})$ for the commutator pairing. Moreover, by construction it is contained in the ℓ-torsion subgroup of A and by hypothesis has rank g. We choose a decomposition as isotropic subspaces $K(\mathscr{L}) = K_1(\mathscr{L}) \times K_2(\mathscr{L})$ such that $\hat{K}$ is contained in $K_2(\mathscr{L})$ and for $i = 1, 2$, $\pi(K_i(\mathscr{L})[n]) = K_i(\mathscr{L}_0)$.

Denote by $\kappa : G(\mathscr{L}) \to K(\mathscr{L})$ the natural projection. By the descent theory of Grothendieck, there exists a unique level subgroup $\tilde{K}_\ell$ of $G(\mathscr{L})$ contained in $\kappa^{-1}(\hat{K})$ such that the quotient of $(A_k, \mathscr{L})$ by the action defined by $\tilde{K}_\ell$ gives $(B_k, \mathscr{L}_0)$. Let $G^*(\mathscr{L})$ be the centralizer of $\tilde{K}_\ell$ in $G(\mathscr{L})$. By [Mum66, Prop. 2 pp. 291], we have an isomorphism

$$i : G^*(\mathscr{L})/\tilde{K}_\ell \simeq G(\mathscr{L}_0).$$

Let $G(\mathscr{L})[n] = \kappa^{-1}(K(\mathscr{L})[n])$. We remark that

1. $G(\mathscr{L})[n]$ is contained in $G^*(\mathscr{L})$,
2. $\kappa(G(\mathscr{L})[n] \cap \tilde{K}_\ell)$ is the zero subgroup of A_k.

Let $\tilde{K}_0$ be the level subgroup of $G(\mathscr{L}_0)$ defined as the image by $\Theta_{\overline{n}}$ of the subgroup $(1,0,y)_{y \in \hat{Z}(\overline{n})}$ of $\mathcal{H}(\overline{n})$. An immediate consequence of 1. and 2. is that there exists a unique level subgroup $\tilde{K}_n$ of $G(\mathscr{L})$ such that $i(\tilde{K}_n) = \tilde{K}_0$.

Denote by $\tilde{K}_2$ the level subgroup of $G(\mathscr{L})$ whose restriction over $K(\mathscr{L})[n]$ and $K(\mathscr{L})[\ell]$ is respectively given by $\tilde{K}_n$ and $\tilde{K}_\ell$. By construction, we have

$$i(\tilde{K}_2) = \tilde{K}_0. \tag{25}$$

Choose any theta structure $\Theta_{\overline{\ell n}} : \mathcal{H}(\overline{\ell n}) \to G(\mathscr{L})$ such that the image by $\Theta_{\overline{\ell n}}$ of the subgroup $(1,0,y)_{y \in \hat{Z}(\overline{\ell n})}$ is exactly $\tilde{K}_2$. Because of (25) and construction of Proposition 1, we have $\vartheta_0^{\Theta_{\overline{\ell n}}} = \hat{\pi}^*(\vartheta_0^{\Theta_{\overline{n}}})$.

We suppose moreover that $\Theta_{\overline{\ell n}}$ is such that for all $x \in Z(\overline{n})$, $i(\Theta_{\overline{\ell n}}(1,x,0)) = \Theta_{\overline{n}}(1,x,0)$, where we consider $Z(\overline{n})$ as a subgroup of $Z(\overline{\ell n})$ via the map $x \mapsto \ell x$. We remark that by construction, $\Theta_{\overline{\ell n}}$ and $\Theta_{\overline{n}}$ verify the conditions (6) and (7) and as a consequence are $\hat{\pi}$-compatible. As a consequence of Corollary 1, we have that for all $i \in Z(\overline{n})$, $\vartheta_i^{\Theta_{\overline{\ell n}}} = \hat{\pi}^*(\vartheta_i^{\Theta_{\overline{n}}})$.

Let $(a'_u)_{u \in Z(\overline{\ell n})}$ be the theta null point associated to $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$. For $i \in Z(\overline{n})$, denote by Q_i the geometric point of $\mathbb{P}_k^{Z(\overline{n})}$ with homogeneous coordinates $(a'_{\rho(j,i)})_{j \in Z(\overline{n})}$.

We know that the projective coordinates of a maximal isotropic ℓ-torsion subgroup of A_k is obtained by the action of the theta group on $(a'_u)_{u \in Z(\overline{\ell n})}$ by translation. Denote by K' the ℓ-torsion subgroup of A_k given by the points with projective coordinates $(a'_{v+i})_{v \in Z(\overline{\ell n})}$. By construction, K' is the dual of $\hat{K}$ for the commutator pairing which implies that A_k is exactly the quotient of B_k by $\hat{\pi}(K')$. As a consequence, we have $\hat{\pi}(K') = K$.

The applications $Z(\overline{\ell}) \to B_k[\ell]$, $j \mapsto P_j$ is a group morphism (see for instance the proof of [CL08, Lemma 5.6]), as well as the application $Z(\overline{\ell}) \to B_k[\ell]$, $j \mapsto \hat{\pi}(Q_j)$. By changing the theta structure $\Theta_{\overline{\ell n}}$, we can suppose that for all $j \in Z(\overline{\ell})$, $\hat{\pi}(Q_j) = P_j$. As a consequence, for $j \in Z(\overline{\ell})$ there exists $\lambda_j \in \overline{k}$ such that for $i \in Z(\overline{n})$, $a_{\rho(j,i)} = \lambda_j a'_{\rho(j,i)}$. We know moreover that $(a_u)_{u \in Z(\overline{\ell n})}$ and $(a'_u)_{u \in Z(\overline{\ell n})}$ are geometric points of V_J. Applying Lemma 4 we are done.

If $(a_u)_{u \in Z(\overline{\ell n})}$ is a geometric point of V_J, we denote by $G((a_u)_{u \in Z(\overline{\ell n})})$ the subgroup of $B_k[\ell]$ generated by the valid projective points $(a_{\rho(j,i)})_{j \in Z(\overline{n})}$ for $i \in Z(\overline{\ell})$ of $V_{I_{\Theta_{\overline{n}}}} = B_k$. The preceding theorem tells us that whenever a solution $(a_u)_{u \in Z(\overline{\ell n})}$ of J is such that $G((a_u)_{u \in Z(\overline{\ell n})})$ is a maximal ℓ-torsion subgroup of $B_k[\ell]$ then it is a valid theta null point, that is, it corresponds to a certain $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$. It would be desirable to be able to determine which maximal rank g subgroups of $B_k[\ell]$ can arise as a $G(x)$ where x is a geometric point of V_J representing a valid theta null point.

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 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 $\mathscr{M}_0$ descend 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 application $e_W : B_k[\ell] \times B_k[\ell] \to \overline{k}$. 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.

Theorem 5. *A maximal ℓ-torsion subgroup of B_k of rank g is of the form $G(x)$ where x is a geometric point of V_J corresponding to a valid theta null point if and only if $G(x)$ is an isotropic subgroup for the pairing e_W.*

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 $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$. The theta structure $\Theta_{\overline{\ell n}}$ 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 $\pi^*(\vartheta_i^{\Theta_{\overline{n}}}) = \vartheta_i^{\Theta_{\overline{\ell n}}}$ 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 a maximal rank g ℓ-torsion subgroup of $B_k[\ell]$ 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 $(B_k, \mathscr{L}_0, \Theta_{\overline{n}})$. 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 $\mathscr{M}_0$ descend 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,

$$\begin{tikzcd}
(B_k, \mathscr{M}_0) \arrow[dd, "{[\ell]}"] \arrow[dr, "\hat{\pi}"] & \\
& (A_k, \mathscr{L}) \arrow[dl, "\pi"] \\
(B_k, \mathscr{L}_0) &
\end{tikzcd} , \tag{26}$$

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

The theta structure $\Theta_{\overline{n}}$ 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 $\Theta_{\overline{\ell n}}$ for $\mathscr{L}$ compatible with this decomposition. Let $(a_u)_{u \in Z(\overline{\ell n})}$ be the associated theta null point. By Corollary 1, $(a_u)_{u \in Z(\overline{\ell n})}$ is a geometric point of V_J. Moreover, we have $G((a_u)_{u \in Z(\overline{\ell n})}) = \pi(K_1(\mathscr{L})) = G$.

Our study of valid theta null points allows us to better understand the geometry of V_J^0. We know from Proposition 5 that V_J^0 classifies the isogenies $\pi : A_k \to B_k$ between marked abelian varieties verifying the compatibility condition.

Taking the dual of π gives an isogeny from B_k to A_k with kernel $K = \pi(K_1) = \{P_1, \ldots, P_n\}$. Thus the theta null points on V_J^0 correspond to varieties $\overline{\ell}$-isogeneous to B_k. But we have seen in Proposition 7 that it may happen that different points of V_J^0 give the same kernel K and hence the same isogeneous variety. We want to classify the points of V_J^0 corresponding to isomorphic varieties $\overline{\ell}$-isogeneous to B_k.

To do that, let K be a maximal isotropic subgroup of rank g of the points of ℓ-torsion of B_k. We are interested in the class $\mathfrak{T}_K$ of isogenies of kernel K. More precisely, if π is an isogeny from B_k to A_k with kernel K, then $\mathfrak{T}_K$ is the class of isogenies $\pi' : B_k \to A'_k$ such that there exists an isomorphism $\psi : A_k \to A'_k$ that makes the following diagram commutative:

$$\begin{tikzcd} & & & A_k \arrow[dd, "\psi"] \\ 0 \arrow[r] & K \arrow[r] & B_k \arrow[ur, "\pi"] \arrow[dr, "\pi'"'] & \\ & & & A'_k \end{tikzcd}$$

Proposition 9. *Let K be a maximal subgroup of rank g of the points of ℓ-torsion of B_k which is isotropic for the pairing e_W. There is a point $(a_u)_{u \in Z(\overline{\ell n})} \in V_J^0$ such that the corresponding dual isogeny $\pi : B_k \to A_k$ is in $\mathfrak{T}_K$. Every other point in V_J^0 giving the class $\mathfrak{T}_K$ is obtained by the action of $\mathfrak{H}$ on $(a_u)_{u \in Z(\overline{\ell n})}$. In particular, the geometric points of $V_J^0/\mathfrak{H}$ are in bijection with the $\overline{\ell}^g$-isogenies of B.*

Proof. Let $K = \{P_i, i \in Z(\overline{\ell})\}$ be such a maximal subgroup. Theorem 4 gives a geometric point $(a_u)_{u \in Z(\overline{\ell n})}$ of V_J^0 corresponding to a marked abelian variety $(A_k, \mathscr{L}_A, \Theta_A)$ such that the associated isogeny $\tilde{\pi} : A_k \to B_k$ sends $K_1(\mathscr{L}_A)$ to K. Hence, the unique isogeny $\pi : B_k \to A_k$ such that $\tilde{\pi} \circ \pi = [\ell]$, is in $\mathfrak{T}_K$. If $(a'_u)_{u \in Z(\overline{\ell n})}$ is another valid theta null point in V_J^0, corresponding to a marked abelian variety $(A', \mathscr{L}_{A'}, \Theta_{A'})$ such that the dual of the associated isogeny gives the same class as π, then we have the following diagram:

$$\begin{tikzcd}
 & A_k \arrow[dl, "\tilde{\pi}"'] \\
B_k & \\
 & A'_k \arrow[ul, "\tilde{\pi}'"] \arrow[uu, "\tilde{\psi}"']
\end{tikzcd}$$

By definition of the associated isogenies $\tilde{\pi}$ and $\tilde{\pi}'$, we know that $\mathscr{L}_A = \tilde{\pi}^*(\mathscr{L}_B)$ and $\mathscr{L}_{A'} = \tilde{\pi}'^*(\mathscr{L}_B) = \tilde{\psi}^*(\mathscr{L}_A)$. 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 $\mathfrak{H}$.

Together with the study of degenerate theta null points, it is now possible to count the points in V_J. 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 (17) 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 (18) 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 $g = 2$, it is easy to compute the number of valid theta null point 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 5): there are $(\ell^2+1)(\ell+1)$ such points.

Next, the number of actions of the form (17) 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 (18) is ℓ^3 (the number of symmetric matrices of dimension 2). As a consequence, the number of valid theta null point in V_J is

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

We remark that this number is a $O(\ell^{11})$. 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 a $O(\ell^{g(g+1)/2})$. The number of action of the form (17) is a $O(\ell^{g^2})$ and the number of action of the form is a $O(\ell^{g(g+1)/2})$. We deduce that the number of valid theta null point in V_J is bounded by

$$O(\ell^{2.g^2+g}). \tag{27}$$

Example 1. In the case of genus 1 and small ℓ it is possible to list all the solutions 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 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 (17) and (18)):

$Q_1 = (16\upsilon^2 + 19\upsilon + 17 : 1 : 46 : 16\upsilon^2 + 19\upsilon + 17 : 37 : 54 : 34\upsilon^2 + 70\upsilon + 46 : 54 : 37 : 16\upsilon^2 + 19\upsilon + 17 : 46 : 1)$ 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 (17), 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 6) is $\{(1 : 1 : 12 : 1), (1 : 1 : 12 : 1), (1 : 1 : 12 : 1)\}$ which has rank 0. On $\mathcal{C}$ the action (17) is trivial, so there are only 3 points in this degenerate class, coming from the action (18). The last degenerate point is $(1 : 0 : 0 : 1 : 0 : 0 : 12 : 0 : 0 : 1 : 0 : 0)$, alone in its class.

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 $\nu \geqslant 2$ 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 back the idea that even in the case $\nu = 1$, in general, V_J is a zero dimensional variety whose degree is of the same order with respect to the parameter ℓ as in the case $\nu = 2$.

In the case that the characteristic of the base field k is equal to ℓ and $\nu \geqslant 2$, the proof that V_J is a 0-dimensional scheme is still valid. 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 that in this case 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 can prove that this algorithm is efficient in the case $\nu \geqslant 2$ and when the characteristic of k is different from ℓ. In the case that $\nu = 1$ or when the characteristic of k is equal to ℓ we will make the hypothesis that V_J is a zero dimensional variety whose degree is given by formula (27). Under these hypothesis, we can also prove that our algorithm is efficient.

6 An efficient algorithm

We would like to use the formulas of Section 4 to compute the image of the modular correspondence Φ_ℓ for some positive integer ℓ. We have seen that the main algorithmic difficulty is to solve the polynomial system defined by the equations of Theorem 1 together with the symmetry relations. 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 heuristics described at the end of Section 5.

Let $n = 2^\nu$. In this section, k is a finite field. We let $(B_k, \mathscr{L}_0, \Theta_{\overline{n}})$ be a dimension g abelian variety together with a $\overline{n}$-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 1, 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 (heuristically 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 could 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 Go of RAM;
- 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 coherent with the number of solutions discussed after Proposition 9 when $g = 2$, $\nu = 2$ and $\ell = 3$).

– 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 compute 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 efficiently the algebraic system defined by J for small ℓ over a big coefficient field. As an application of our method, we can mention the initialisation phase of a point counting algorithm [CL08].

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 Assumptions

Our method is a combination of existing algorithms. We first describe in full generality the assumptions upon which our algorithm is faster than a general purpose Gröbner basis algorithm. Then, using the results of Section 5, we explain that these assumptions hold for J in the case that $\nu \geqslant 2$ and that the characteristic of k is not ℓ. If $\nu = 1$ or if the characteristic of k is equal to ℓ, we can not prove the assumptions but we have made extensive computations which show that in general our algorithm is much more efficient than a general purpose Gröbner basis algorithm.

Let T be a set $[x_1, \ldots, x_s]$ of variables, we assume that $J \subset k[T]$ is a zero dimensional ideal generated by the polynomials $[f_1, \ldots, f_m]$ where for $i = 1, \ldots, m$, f_i is a polynomial in $k[T]$. We make the hypothesis that we can split the set of variables into two subsets $T = X \cup Y$ such that the ideal $K = J \cap k[Y]$ contains low degree polynomials.

In order to make precise what we mean by low degree polynomials, we denote by I_{gen} an ideal generated by the polynomials $[g_1, \ldots, g_m]$ where for $i = 1, \ldots, m$, g_i is a general polynomial of total degree $\deg(f_i)$. We define for any ideal I of $k[T]$:

$$D_Y(I) = \min\{deg(g) \mid 0 \neq g \in I \cap k[Y]\}.$$

Our assumption that $J \cap k[Y]$ contains low degree polynomials means that

$$D_Y(J) \ll D_Y(I_{gen}). \tag{H1-1}$$

The previous assumption implies that our algorithm will perform much faster with the particular ideal J than it would do for a general ideal I_{gen}.

We must also ensure that it is more efficient to compute a Gröbner basis for $J \cap k[Y]$ instead of a Gröbner basis for J. If we suppose that a Gröbner basis computation for a total degree order has the same complexity for J and I_{gen}, we have to check that $D_Y(J) \ll D_T(I_{gen})$. It is well known that, generically, a lower bound for $D_T(I_{gen})$ is given by the Macaulay bound which is given by $D_T(I_{gen}) = 1 + \sum_{i=1}^{m}(\deg(f_i) - 1)$ if $m \leqslant s$. We can now state explicitly the second part of our first assumption:

$$D_Y(J) \ll \sum_{i=1}^{m} \deg(f_i). \tag{H1-2}$$

Our second assumption is that J can be decomposed into many prime ideals. There exists a positive integer $r \gg 1$ such that

$$\sqrt{J} = P_1 \cap \cdots \cap P_r \text{ and } P_i \text{ is a prime ideal.} \tag{H2}$$

We recall that for a homogeneous ideal we define the Hilbert function $\mathrm{HF}_I(d) = \dim(k[T]/I)_d$ and the degree of the ideal I, $\deg(I)$, is given by the Hilbert series $\sum\limits_{i=0}^{\infty} \mathrm{HF}_I(d)\, z^i = \frac{M(z)}{(1-z)^{\dim(I)}}$ and $\deg(I) = M(1) \neq 0$. With this, we can state the third (optional) assumption

$$\deg\left(\sqrt{I}\right) \ll \deg\left(I\right). \tag{H3}$$

We discuss the validity of hypothesis (H1-1), (H1-2), (H2) and (H3) in the case that J is defined as in the introduction of the present section. First, we remark that $D_Y(I_{gen})$ can be easily computed: let $M(s,d)$ be the number of monomials of degree less or equal to d in s variables. The total number of solutions counted with multiplicities of I_{gen} is given by the Bézout bound: $D = \Pi_{i=1}^{m} \deg(f_i)$. Hence, we have

$$D_Y(I_{gen}) = \min_d \left\{M(h,d) > D\right\}, \tag{28}$$

where h is the cardinal of Y and $M(h,d) = \binom{h+d}{d}$. By considering $M(h,d)$ as a polynomial in the unknown d, we obtain that for a given h, $D_Y(I_{gen})$ is the biggest real root of the polynomial:

$$\frac{1}{h!}\prod_{i=1}^{h}(x+i) = D.$$

As a consequence, we have

$$D_Y(I_{gen}) \sim_{D\to\infty} (h!D)^{\frac{1}{h}}. \tag{29}$$

We know moreover that $\overline{\mathcal{M}}_{\overline{\ell n}}$ has dimension $1/2.g.(g+1)$ and is embedded via the relations given in Theorem 1 in the projective space of dimension $(n\ell)^g - 1$. We deduce that J contains at least $(n\ell)^g - 1/2.g.(g+1)$ algebraically independent polynomials. As the equations of Theorem 1 have degree 4, a lower bound for D is $4^{(n\ell)^g-1/2.g.(g+1)-1}$.

On the other side, if we chose for $j \in Z(\overline{\ell})$, $Y = [x_{\rho(u,j)} | u \in Z(\overline{n})]$, we know by Proposition 6 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 $V_{I_{\Theta_{\overline{n}}}}$. In this last case, by Lemma 4 we know that there is ℓ solutions of J corresponding to the same projective points. Denote by D' the number of solutions of $J \cap k[Y]$ counted with multiplicities. We have $D' \leqslant \ell^{2g+1} + 1$ and using the heuristic evaluation of $D_Y(J)$ given by (28), we obtain

$$D_Y(J) \sim_{D\to\infty} (h!D')^{\frac{1}{h}}. \tag{30}$$

For a fixed g and ν the cardinal of Y are fixed. Using (29) and (30), we see that hypothesis (H1-1) is verified for ℓ big enough.

Next, $1 + \sum_{i=1}^{m}(\deg(f_i) - 1) = 3.(n\ell)^g$. On the other side, $(h!D')^{\frac{1}{h}}$ with $D' \leqslant \ell^{2g+1} + 1$ and $h = n^g$. As $n \geqslant 2$, we have, using the Stirling approximation formula, that $(h!D')^{\frac{1}{h}} = O(\ell)$ and hypothesis (H1-2) is verified as soon as $g \geqslant 2$ and ℓ big enough.

Since we want to find at least one solution of J defined over k, we can assume that such a solution exists. By Proposition 6, this implies that there exists a subgroup G of rank at least 1 of the ℓ-torsion group of $V_{I_{\Theta_{\overline{n}}}}$ such that all the points of G are defined over k. As the solutions of $J \cap k[Y]$ are points of $V_{I_{\Theta_{\overline{n}}}}[\ell]$, we conclude that for $r \geqslant \ell$ we have:

$$\sqrt{J} = P_1 \cap \cdots \cap P_r \text{ and } P_i \text{ is a prime ideal,}$$

and hypothesis (H2) is verified.

In general, we know from Proposition 8 that the hypothesis (H3) is not verified since J is a reduced ideal. Nonetheless, in the case that the characteristic of k is equal to ℓ, the scheme defined by J is not reduced and we use (H3) in order to speed up the computations.

6.3 General strategy

In the following, we give a general strategy for computing the solutions of the algebraic system defined by J. All the steps of our algorithm are standard with the exception of step 1 and step 4. In step 1, we try to use as much as possible the assumptions (H1-1) and (H1-2) and step 4 is based upon the assumptions (H2),(H3).

Step 1 Using a specific 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 zero dimensional ideal J_1 contained in J. In general J_1 is not equal to J. The output of the algorithm is a sequence of polynomials $[p_1, \ldots, p_\kappa]$ in $k[Y]$ such that J_1 is generated by $(p_1, \ldots, p_\kappa)$.

Step 2 Compute a Gröbner basis G_{DRL} of J_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 J_1 for a lexicographical order. This can be done by using the FGLM algorithm to change the monomial order of G_{DRL}.

Step 4 Compute a decomposition into primes of the following ideal:

$$\sqrt{J_1} = P_1 \cap \cdots \cap P_r$$

We assume that $\deg(P_i) = 1$ (if it is not the case we replace k by some algebraic extension of k).

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

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

(b) Change the monomial order to obtain G_i' a lexicographical Gröbner basis of $(P_i) + I$.

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

Since we have $\sqrt{I} = \sqrt{J_1 \cap I} = \sqrt{P_1 \cap I} \cap \cdots \cap \sqrt{P_r \cap I}$ and since the decomposition of each component $\sqrt{P_i \cap I}$ is done by step 5 of the previous algorithm, we obtain a decomposition of the ideal I:

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

Remark 3. Once we have obtained a point P of V_J corresponding to a valid theta null point, we can recover all the solutions of V_J corresponding to valid theta null points using the action given by Proposition 7.

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 2. *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 $k[Y]$. Consequently we obtain an new version of the F_4 algorithm:

Algorithm 6 *Algorithm F_4 (modified version)*

$$\textit{Input:} \begin{cases} F \text{ a finite subset of } k[x_1,\dots,x_s] \\ < \text{ a monomial admissible order} \\ X = [x_1,\dots,x_\kappa] \text{ and } Y = [x_{\kappa+1},\dots,x_s] \end{cases}$$

Output: *a finite subset of $k[x_1,\dots,x_s]$.*
$G := F$ *and* $P := \left\{\mathrm{CritPair}(f,g) \mid (f,g) \in G^2 \text{ with } f \neq g\right\}$
while $P \neq \varnothing$ *and* $\dim(G \cap k\,[Y]) > 0$ ***do***
  $d := \min\left\{\deg_X(p) \mid p \in P\right\}$ *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 following the three steps:

Step 1 The basis G_{Lex} always contains a univariate polynomial $g(x_s)$. We can factorize this polynomial. We will see that 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). By a theorem of Lazard [Laz85, Theorem 1], the general shape of G_{Lex} the lexicographical order Gröbner basis is as follows:

$$\begin{cases} g\,(x_s) \\ h_1\,(x_{s-1},x_s) = g_1\,(x_s)\left(x_{s-1}^{k_1} + \cdots\right) \\ h_2\,(x_{s-1},x_s) = g_2\,(x_s)\left(x_{s-1}^{k_2} + \cdots\right) \\ \cdots \\ h_s\,(x_{s-1},x_s) = x_{s-1}^{k_s} + \cdots \\ \text{polynomials in variables } x_1,\dots,x_s \end{cases} \tag{31}$$

with $k_1 < k_2 < \cdots < k_s$ and $g_1\,(x_s) \mid g_2\,(x_s) \mid \cdots$. Hence we can obtain for free some factors of $g(x_s)$:

Step 3

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

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

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

In our case $k = \overline{k}$ and 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 $x_{s-2}, \dots, x_1$.

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 show that the initialisation phase of the point counting algorithm described in [CL08] 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 A_k of dimension 2. 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 A_k. We can then use the algorithm of [CL08] to count the number of points of A_k.

First experiments As explained in 6.1 if we can 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 10 hours of computations on a powerful computer with 16 Go of RAM just to compute a DRL Gröbner basis. Moreover, in characteristic 3, there is a huge number of solutions: 30853. This imply 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 $X = T - Y$ 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 first 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	3.24+0.01=3.25 sec	8.0+0.77+0.01+0.08=8.86 sec
$k = \mathbb{F}_{5^{20}}$	0.35 sec	1.14 sec	28.4+0.04=28.44 sec	39.3+9.1+0.05+0.49=48.94 sec

Even if the theoretical complexity is linear in the size of k it is clear that, in practice, the behavior of the algorithm is not linear in $\log(k)$. 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 *recursively* the algorithm of section 6.3 to perform the step 5: we split again the first of variable into two parts: $X = X' \cup Y' = X' \cup [x_{42}, x_{21}, x_{51}, x_{12}]$.

Algo 6.3	Original Step 5	Recursive Step 5
$k = \mathbb{F}_{5^{10}}$	8.0+0.77+0.01+0.08=8.86 sec	0.05+0.41+0.33+0.01=0.8 sec
$k = \mathbb{F}_{5^{20}}$	39.3+9.1+0.05+0.49=48.94 sec	0.12+1.53+2.44+0.01+0.02=4.1 sec
$k = \mathbb{F}_{5^{40}}$		0.13+2.46+7.16+0.01+0.01=9.78 sec

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

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

and thus we can split $g_1(x_{01})$ into two factors:

$$g_1(x_{01}) = (x_{01} + \alpha_1)^3 \, (x_{01} + \alpha_2)^9 \cdots (x_{01} + \alpha_4)^9$$
$$\frac{g(x_{01})}{g_1(x_{01})} = x_{01} \, (x_{01} + \beta_1)^3 \, (x_{01} + \beta_2)^9 \cdots (x_{01} + \beta_3)^9$$

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

6.6 Experimental results

Programming language – 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 have been implemented in C language in the FGb software and we used this implementation for computing the first Gröbner base. All the other computations are performed under Magma including factorizing some univariate polynomials and computing Gröbner bases 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. 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: $T_1 = T - T_{\mathrm{Gen}}$.

k	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: $T_{\text{Gen}} \approx T$. In characteristic, 5 we have $T \approx 3\, T_{\text{Gen}}$.
- The most consuming part in 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 non-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.

7 Conclusion

In this paper, we have described 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 [CL08]. The main part of the algorithm is the resolution of an algebraic system for which we have designed a specific 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.

References

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

[BCP97] Wieb Bosma, John Cannon, and Catherine 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] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundament al Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[BW93] Thomas Becker and Volker 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.

[CL08] D. Carls, R. and Lubicz. A p-adic quasi-quadratic time and quadratic space point counting algorithm. 2008. preprint.

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

[Elk98] Noam D. 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] Jean-Charles Faugére. 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] Jean-Charles 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.

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

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

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

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

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

[Mum67] D. Mumford. On the equations defining abelian varieties. II. *Invent. Math.*, 3:75–135, 1967.

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

[Sat00] Takakazu 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] Frederik Vercauteren, Bart Preneel, and Joos 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.