Linear representation of endomorphisms of Kummer varieties

David Lubicz, Damien Robert

LINEAR REPRESENTATION OF ENDOMORPHISMS OF KUMMER VARIETIES

DAVID LUBICZ AND DAMIEN ROBERT

Abstract. Let K_A be a Kummer variety defined as the quotient of an Abelian variety A by the automorphism (-1) of A. Let $T_0^*(A)$ be the co-tangent space at the point 0 of A. Let $\mathrm{End}(A)$ be the additive group of endomorphisms of A. There is a well defined map $\rho : \mathrm{End}(A) \to \mathrm{Aut}(T_0^*(A))$, $f \mapsto (df)_0^*$, where $(df)_0^*$ is the differential of f in 0 acting on $T_0^*(A)$. The data of $\overline{f} \in \mathrm{End}(K_A)$ which comes from $f \in \mathrm{End}(A)$, determines $\rho(f)$ up to a sign. The aim of this paper is to describe an efficient algorithm to recover $\rho(f)$ up to a sign from the knowledge of $\overline{f}$. Our algorithm is based on a study of the tangent cone of a Kummer variety in its singular 0 point. We give an application to Mestre's point counting algorithm.

1. Introduction

1.1. **Characteristic polynomial of the Frobenius.** One of the motivations of this paper is to improve point counting on abelian varieties based on canonical lifts. A point counting algorithm takes as input an Abelian variety $\overline{A}$ defined over a finite field $\mathbb{F}_q$ where $q = p^r$ and outputs the cardinality of $\overline{A}(\mathbb{F}_q)$, and even the full characteristic polynomial of the Frobenius morphism.

These family of point counting algorithms using canonical lifts were pioneered by Satoh [Sat00] for elliptic curves, and Mestre's algorithm [Mes01; Rit03] (and its generalisations) extend this to abelian varieties.

An algorithm of this family proceeds in two steps and works under the generic hypothesis that $\overline{A}$ is ordinary. First, it uses p-modular equations (for suitable modular invariants) to compute a canonical lift A of $\overline{A}$ over $\mathbb{Q}_q$ the degree r unramified extension of $\mathbb{Q}_p$. Satoh uses modular polynomials in terms of the j-invariant of elliptic curves. This has been extended to abelian surfaces in [MR20; MR21] by using modular polynomials in terms of the Igusa invariants. Mestre uses the duplication formula between theta constants, which is given by a generalization of the Arithmetic–Geometric Mean (AGM) sequence in higher dimension (so works when $p = 2$), and extensions [CL07; CKL06; CL09; FLR11] use p-multiplication formula between theta constants.

The second step is to compute the action of the q^{th}-Frobenius morphism (or its dual the q^{th}-Verschiebung) on $T_0^*(A)$ the co-tangent space in 0 of A. Modular invariants cannot recover this action, so this step needs an explicit p-modular correspondance (parametrizing normalised isogenies) between modular forms of some weight ρ. We will call this an affine modular correspondance. By definition of a modular form, this allows to recover the determinant of the action of the Verschiebung to the power ρ. This determinant is exactly the product of the invertible eigenvalues of the Frobenius.

Satoh computes this affine modular correspondance directly by lifting the kernel of the Verschiebung, using Vélu's formulae [Vél71] to compute the equation $E' : y^2 = x^3 + a'x + b'$ of the normalised isogenous elliptic curve, and then using the fact that the coefficients a' and b' of E' are modular forms of weight 4 and 6 respectively to recover the action of the Frobenius to the square. This gives the value t^2 of the trace, from which it is easy to recover t by using Hasse's formula. Mestre's algorithm using duplication formulas and its extensions using p-multiplication formulas relate the theta constants directly hence already give an affine modular correspondance (of weight 1/2 from which it is easy to construct modular relations between modular forms of weight 1). Of course it is easy from this affine modular correspondance to give relations between quotients θ_i/θ_0 of theta constants, i.e. relations between modular functions, which is what was used in the lifting step. For abelian surfaces, in [MR20] the authors use the same approach as Satoh's, namely they lift the kernel and then use [CR15] to compute the theta constants of the normalised isogeny.

A problem of this approach using modular forms of weight ρ is that it only allows to recover $\prod_{i=1}^{g} \lambda_i^\rho$ where λ_i are the invertible eigenvalues of the Frobenius. When $g = 1$ this is not a problem: given λ^ρ, then as mentioned above Hasse's formula allows to take the correct root λ, from which the trace is recovered as $t = \lambda + q/\lambda$. In higher dimension, Mestre explains in [Mes02a] how to recover in most cases the characteristic polynomial of the Frobenius morphism. But his method is painful from an algorithmic point of view: it involves raising the level of p-adic precision needed for the computation of a canonical lift above the level prescribed by Weil bounds and then to use a LLL algorithm on a lattice of dimension $2^g - 1$. Moreover, Mestre gives examples of Abelian varieties of dimension $g \geqslant 4$ for which the determinant of the Verschiebung does not characterises its isogeny class: as a consequence it is not even possible to recover the characteristic polynomial of the Frobenius morphism from this data only.

In this article, we make the trivial but crucial remark that this ambiguity can be avoided if instead of modular forms we compute the equation of the isogeny induced by the Verschiebung directly so that we can compute its action on the differentials (or by duality its action on the tangent space at 0), to recover not only the determinant, but the full matrix M of the Verschiebung (up to conjugation). It is then straightforward to recover the characteristic polynomial of the Frobenius as the characteristic polynomial of the matrix $M + qM^{-1}$. Strangely it seems that this obvious idea was not considered in the literature, although it raises no difficulty: Satoh already lifts the kernel, and Vélu's formula give the equations of the isogeny along with the equations of the normalised isogenous elliptic curve. Mestre uses the duplication formula between theta constants $\theta_i(0, \tau)$, but it is well known that this duplication formula extends to a duplication formula between theta functions $\theta_i(z, \tau)$ which give an explicit equation for the 2-isogeny. The extensions of Mestre algorithm [CKL06; CL09; FLR11] to characteristic $p > 2$ uses a p-multiplication formula between theta constants of level $2p$ (or $4p$), which readily extends to a p-multiplication formula between theta functions. The isogeny algorithm [CR15] used by [MR20] also gives the equations for the isogeny, not only the theta constants of the normalised isogenous abelian variety.

We refer to section 4 for more details, and give examples in dimension $g = 1, 2$ in Section 5.

1.2. **The tangent cone of the Kummer variety.** A technical difficulty that arises when implementing the strategy above, is that using level 2 theta functions as in Mestre's original algorithm only give an embedding of the Kummer variety $K_A = A/\pm 1$ rather than of A itself (if the polarisation is absolutely simple). A solution would be to switch to theta functions of level $n > 2$, but this would increase the complexity of finding a canonical lift (which would be described using $n^g - 1$ coordinates rather than $2^g - 1$).

So a natural question that we tackle in this article is the following: given an isogeny $f : A \to B$ which is expressed in terms of the Kummer varieties $\overline{f} : K_A \to K_B$. Can we recover the action of df on the tangent space of A and B at 0 from the action of $\overline{f}$ on the tangent cone of K_A and K_B at 0?

Before describing our main results, we explain why this question is interesting for its own sake. In many algorithmic applications Kummer varieties are more amenable to computation than Abelian varieties. For instance, using theta functions, one can embed Kummer varieties inside the projective space of dimension $2^g - 1$ whereas Abelian varieties need at least $3^g - 1$ parameters (generically). Moreover, $4^g - 1$ parameters are required in order to have Riemann equations and all that arise from them such as efficient representation and arithmetic [LR16]. This is why there is a series of papers dealing with all sorts of computations with Kummer varieties: arithmetic, pairings, isogenies [LR15b; LR15a; CR15]. Computing $\rho(f)$ from the knowledge of an isogeny $\overline{f} \in \mathrm{End}(K_A)$ can be viewed as a continuation of this approach by enlarging our computational toolbox. Of course, in doing so, we want to do it significantly more efficiently than recovering $f \in \mathrm{End}(A)$ (which in the case of theta coordinates, involves manipulating an ambient space of at least $3^g - 1$ parameters) and then computing $(df)_0^*$. Our algorithm works at the conditions that we have a description of a Zariski neighbourhood of $0 \in K_A(k)$ as a closed sub-variety of an affine space $\mathbb{A}^m$ given by explicit polynomial equations. Such models are known for Kummer varieties of dimension less than 3 [CF+96]. In general, the Kummer variety can be defined by equations of degree 3 and 4 [Kem92].

A first idea, if we are given a rational point[1] P on A which is not of 2-torsion, since K_A is smooth at P, then the action of $df : T_P(A) \to T_{f(P)}B$ can be recovered directly on the Kummer variety. But, unlike 0_A which is always rational, such a point may not exist, and we would like not to take an extension of the base field to find such a point. Since the Kummer variety is singular at 0, we need to replace tangent spaces by tangent cones.

We now fix the notations we are going to use for the rest of the paper. We let A be a dimension g abelian variety over a field k of characteristic $\mathrm{char}(k)$, and denote by K_A its associated Kummer variety (by which we mean the quotient of A by the automorphism -1 acting on it). We denote by 0 the neutral point of A. Let $\mathrm{End}(A)$ be the additive group of endomorphisms of A. For x any point of a variety X, we denote by $T^*_x(X)$ its co-tangent space in x. The map $\rho : \mathrm{End}(A) \to \mathrm{Aut}(T^*_0(A))$, $f \mapsto (df)^*_0$, where $(df)_0$ is the differential in 0 map of f. Apart from point counting, this differential has many theoretical and algorithmic applications [Shi98; Sat00]. It is clear that any $f \in \mathrm{End}(A)$ induces on the quotient a map $\overline{f} : K_A \to K_A$. Any such $\overline{f}$ is called an endomorphism of K_A and we denote by $\mathrm{End}(K_A)$ the monoid of endomorphism of K_A.

An endomorphism $\overline{f} \in \mathrm{End}(K_A)$ determines up to a sign an endomorphism $\pm f : A \to A$ and then up to a sign a linear automorphism $\pm(df)^*_0 : T^*_0(A) \to T^*_0(A)$. In this paper, we describe how to compute efficiently $\pm(df)^*_0$ from the knowledge of $\overline{f}$. In fact our algorithm easily generalizes to isogenies $f : A \to B$ rather than only endomorphisms.

As explained above, the problem we face in recovering the linear representation of $\mathrm{End}(K_A)$ is that the 0-point of K_A is singular. As a consequence, the co-tangent space in 0 of K_A, $T^*_0(K_A)$, has dimension higher than that of g and it is not evident how to recover a g-dimensional linear action from an higher dimensional action on $T^*_0(K_A)$.

Let $R^g = k[x_1, \ldots, x_g]$, recall that $\mathrm{Sym}^2(R^g)$ is nothing but $\frac{k[u_{ij}|i,j\in\{1,\ldots,g\},i\leqslant j]}{(u_{ij}u_{kl}-u_{ik}u_{jl})}$ where $(u_{ij}u_{kl}-u_{ik}u_{jl})$ is the ideal generated by the elements $u_{ij}u_{kl} - u_{ik}u_{jl}$. Let $Q^g = \mathrm{Spec}(\mathrm{Sym}^2(R^g))$. The variety Q^g is easily seen to be the quotient of $\mathbb{A}^g = \mathrm{Spec}(R^g)$ by the action of ± 1 on it. Considering this, the following proposition should not be surprising:

Proposition 1.1. *Let A be a dimension g variety over a field k of characteristic different from 2, and let K_A be its Kummer variety. Let $T^c_0(K_A)$ be its tangent cone at the point $0 \in K_A(k)$. Then $T^c_0(K_A)$ is isomorphic as an algebraic variety to*

$$Q^g = \mathrm{Spec}(\mathrm{Sym}^2(k[x_1, \ldots, x_g])).$$

The proposition is a general structure theorem for the tangent cone at the point 0 of a Kummer variety. It implies in particular that the dimension of the cotangent space in 0 of K_A is $g(g+1)/2$. Its interest for the purpose of this paper is that it describes a coordinate system where one can read the linear action of an isogeny.

To explain this, denote by $\mathrm{Aut}(\mathbb{A}^g)$ (resp. by $\mathrm{Aut}(Q^g)$) the group of automorphisms of $\mathbb{A}^g$ (resp. of Q^g) preserving the origin. Every automorphism f of $\mathbb{A}^g$ preserving the origin is linear, so that f commutes with the action of -1 and induces an automorphism $\overline{f}$ of Q^g. Denote by τ the map given by $f \mapsto \overline{f}$.

The following theorem tells that an element of $\mathrm{Aut}(Q^g)$ determines an elements of $\mathrm{Aut}(\mathbb{A}^g)$ up to a sign.

Theorem 1.2. *There is an exact sequence:*

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\varepsilon} \mathrm{Aut}(\mathbb{A}^g) \xrightarrow{\tau} \mathrm{Aut}(Q^g) \longrightarrow 0$$

where $\varepsilon : \mathbb{Z}/2\mathbb{Z} \to \{-1, 1\}$, is given by $x \mapsto (-1)^x$. Moreover, the computation of the inverse image of τ in the canonical coordinate system of Q^g can be done via one square root computation in k and $O(1)$ field operations.

[1] In the cryptographic setting, such a point will of course be given as part of the public key cryptosystem.

Now let $\overline{f} \in \mathrm{End}(K_A)$ be an isogeny that we suppose given explicitly. By differentiating the expression of $\overline{f}$ we easily deduce $(d\overline{f})_0^* : T_0^*(K_A) \to T_0^*(K_A)$ from which we deduce a map of algebraic varieties $(d\overline{f})_0 : T_0^c(K_A) \to T_0^c(K_A)$. In the following commutative diagram:

$$\begin{array}{ccc} T_0^c(K_A) & \xrightarrow{(d\overline{f})_0} & T_0^c(K_A) \\ \lambda \uparrow & & \uparrow \lambda \\ Q^g & \xrightarrow{\delta} & Q^g \end{array}$$

we know, by Theorem 1.2 that from the knowledge of δ, we can efficiently recover the linear action $(df)_0^* : T_0^*(A) \to T_0^*(A)$ up to a sign where f is a lift of $\overline{f}$ to A. In order to compute δ, as $(d\overline{f})_0$ is known, the preceding diagram shows that it is sufficient to be able to compute quickly:

- the tangent cones $T_0^c(K_A)$;
- the isomorphism λ.

These two algorithms are explained in Section 3.

One last algorithmic difficulty lies in that the isomorphism from Proposition 1.1 is defined over the field of definition k of our model of the Abelian variety A. But we are algorithmically given a model of K_A, which may have a smaller field of definition k_0. Since we really want to work over the field k_0 rather than k, we twist the isomorphism of Proposition 1.1 by g quadratic characters (see Example 3.2).

Before going further, we describe the organisation of the paper. In Section 1.3, we give some notations and basic facts which will be used in the rest of the paper. Section 2 is devoted to the study of the tangent cone at 0 of Kummer varieties. In section 3, we describe the algorithms to compute the linear representation of the group of endomorphisms of a Kummer variety. As mentioned above, we give an application of our algorithms to improve Mestre's point counting algorithm in section 4.

1.3. **Notations and basic facts.** Let k be a perfect field, we denote by $\overline{k}$ its algebraic closure. If $\mathscr{A}$ is a k-algebra, we denote by $\mathrm{Spec}(\mathscr{A})$ the associated algebraic variety over k. In this paper, we only consider integral algebraic varieties. If X is an integral algebraic variety over k, we denote by $\mathscr{O}_X$ its structural sheaf. If x is a point of X, the stalk $\mathscr{O}_{X,x}$ of $\mathscr{O}_X$ in x is a local ring. Let $\mathfrak{M}$ be the maximal ideal of $\mathscr{O}_{X,x}$ and let $k' = \mathscr{O}_{X,x}/\mathfrak{M}$ be the residue field in x. We denote by $T_x^*(X)$ the co-tangent space of X in x that is the k' vector space $\mathfrak{M}/\mathfrak{M}^2$. The point x is regular if $\dim_{k'} T_x^*(X) = g$ and singular otherwise, in which case, $\dim_{k'} T_x^*(X) > g$. We denote by $T_x(X))$ the affine algebraic variety over k': $\mathrm{Spec}(\mathrm{Sym}(\mathfrak{M}/\mathfrak{M}^2))$, where $\mathrm{Sym}(\mathfrak{M}/\mathfrak{M}^2)$ is the symmetric algebra of $\mathfrak{M}/\mathfrak{M}^2$. Concretely, let $\mathfrak{M}$ (resp. k') be the maximal ideal (resp. the residual field) of $\mathscr{O}_{X,x}$, then $\mathrm{Sym}(\mathfrak{M}/\mathfrak{M}^2) = k'[x_1, \ldots, x_g]$ where $x_1, \ldots x_g$ are a k' basis of $\mathfrak{M}/\mathfrak{M}^2$ (i.e. are uniformisers).

If $f : X \to Y$ is a map of algebraic varieties and x a point of X then $(df)_x^* : T_{f(x)}^*(Y) \to T_x^*(X)$ is the derivative of f in x. It induces a map of algebraic varieties $(df)_x : T_x(X)) \to T_{f(x)}(Y)$ that we also call the derivative of f in x.

If X is an Abelian variety over k, we denote by K_X, or by K when no confusion is possible, its associated Kummer variety that is the quotient of X by the automorphism -1. We denote by 0 the origin point of X as well as its projection on K_X.

If R is a local ring over k with maximal ideal $\mathfrak{M}$, we denote by

$$\mathrm{Gr}_{\mathfrak{M}} R = \oplus_{i \in \mathbb{N}} \mathfrak{M}^i/\mathfrak{M}^{i+1},$$

its associated graduated ring, where by convention $\mathfrak{M}^0 = R$. For all $i \in \mathbb{N}$, let $\mathrm{Gr}_{\mathfrak{M}}^i R = \mathfrak{M}^i/\mathfrak{M}^{i+1}$. When no confusion is possible we will often replace $\mathrm{Gr}_{\mathfrak{M}}$ by Gr.

Example 1.3. If R is regular of dimension g then $\mathrm{Gr}_{\mathfrak{M}} R = k'[x_1, \ldots, x_g]$ is the polynomial ring over $k' = R/\mathfrak{M}$ in the g variables $x_1, \ldots, x_g$.

Definition 1.4. Let X be an integral variety over k and x a point of X. Let $\mathscr{O}_{X,x}$ be the local ring of X in x and denote by $\mathfrak{M}$ the maximal ideal of $\mathscr{O}_{X,x}$. The tangent cone of X in x that we

denote by $T_x^c(X)$ is by definition $\mathrm{Spec}(\mathrm{Gr}_{\mathfrak{M}}(\mathscr{O}_{X,x}))$. It is naturally embedded in $T_x(X)$, via the map $\mathrm{Sym}(\mathfrak{M}/\mathfrak{M}^2) \to \mathrm{Gr}_{\mathfrak{M}}(\mathscr{O}_{X,x})$.

We recall the basic properties of tangent cones that we use in the following and refer the reader to [CLO92] for a more in-depth coverage of the subject. First, if X is an algebraic variety of pure dimension $\dim X$ then $\dim X = \dim T_x^c(X)$ for all x point of X. If x is a regular point then $T_x^c(X) = T_x(X)$.

Moreover, if $f : A \to B$ is a map of algebraic varieties and x a point of A then $(df)_x : T_x(A) \to T_x(B)$ induces a map $(df)_x : T_x^c(A) \to T_{f(x)}^c(B)$ which is functorial.

2. Tangent cone at 0 of Kummer varieties

This section is devoted to the study of tangent cone of Kummer varieties K_A in 0 the 0-point of K_A. We prove that the tangent cone is isomorphic to a certain simple model. We use this isomorphism to deduce interesting algorithmic consequences for the computation of the tangent cone of a Kummer variety.

Let X be an Abelian variety over k. As the set of 2-torsion points of X are left invariant by -1, these points project to double points on K_X. In particular, $0 \in K_X(k)$ is singular and $\dim T_0^*(K_X) > g$. We would like to have a structure theorem for $T_0^c(K_X)$. First, we prove:

Lemma 2.1. *Let k be a field of characteristic different from 2. Let R be a regular local ring of dimension g which is a k-algebra. Denote by $\mathfrak{M}$ its unique maximal ideal. Let σ be an automorphism of R. As $\sigma(\mathfrak{M}) \subset \mathfrak{M}$, σ acts on $\mathrm{Gr}_{\mathfrak{M}}R$. We also denote by σ this action. We suppose that σ :*

- *acts as the identity on $k' = R/\mathfrak{M}$;*
- *acts like -1 on the co-tangent k'-vector space $\mathfrak{M}/\mathfrak{M}^2$.*

Then R^σ is a local ring with maximal ideal $\mathfrak{M}^\sigma$ and there is an isomorphism of graduated rings

$$\mathrm{Gr}_{\mathfrak{M}^\sigma}(R^\sigma) \simeq (\mathrm{Gr}_{\mathfrak{M}}R)^\sigma, \tag{1}$$

where R^σ (resp. $(\mathrm{Gr}_{\mathfrak{M}}R)^\sigma$) is the sub-ring of invariants of R (resp. $\mathrm{Gr}_{\mathfrak{M}}R$) for the action of σ.

Proof. Let $x \in R^\sigma \backslash \mathfrak{M}^\sigma$. As $\mathfrak{M}$ is a maximal ideal of R, there exists $m \in \mathfrak{M}$ and $u \in R$ such that $m + ux = 1$ so that $1/2(m + m^\sigma) + 1/2(u + u^\sigma)x = 1$. This shows that $R^\sigma/\mathfrak{M}^\sigma$ is a field so that $\mathfrak{M}^\sigma$ is a maximal ideal of R^σ. If $\mathfrak{M}_0$ is a maximal ideal of R^σ then $\mathfrak{M}_0 R$ is a proper ideal of R. Thus $\mathfrak{M}_0 \subset \mathfrak{M}$ since R is local so that $\mathfrak{M}_0 \subset \mathfrak{M}^\sigma$. So R^σ is a local ring with maximal ideal $\mathfrak{M}^\sigma$.

Note that, as σ acts by -1 on $\mathfrak{M}/\mathfrak{M}^2$, we have that $(\mathrm{Gr}^n_{\mathfrak{M}}R)^\sigma = \mathrm{Gr}^n_{\mathfrak{M}}R$ for n even and $(\mathrm{Gr}^n_{\mathfrak{M}}R)^\sigma = 0$ for n odd. Since $\mathfrak{M}^\sigma \subset \mathfrak{M}$ and $\mathfrak{M}^\sigma/\mathfrak{M}^2 \subset (\mathfrak{M}/\mathfrak{M}^2)^\sigma = \{0\}$, $\mathfrak{M}^\sigma \subset \mathfrak{M}^2$. Moreover $\mathfrak{M}^2 \cap R^\sigma$ is a strict ideal of R^σ which contains $\mathfrak{M}^\sigma$. Thus $\mathfrak{M}^\sigma = \mathfrak{M}^2 \cap R^\sigma$. From this, we deduce that

$$(\mathfrak{M}^\sigma)^n \subset \mathfrak{M}^{2n} \cap R^\sigma, \tag{2}$$

for all $n \in \mathbb{N}$.

For all $n \in \mathbb{N}$, the inclusion $(\mathfrak{M}^\sigma)^n \to (\mathfrak{M})^{2n}$ induces a map $(\mathfrak{M}^\sigma)^n/(\mathfrak{M}^\sigma)^{n+1} \to \mathfrak{M}^{2n}/\mathfrak{M}^{2n+1}$ and so a map $\mathrm{Gr}_{\mathfrak{M}^\sigma}(R^\sigma) \to \mathrm{Gr}_{\mathfrak{M}}R$. This last map factors through $\mu^* : \mathrm{Gr}_{\mathfrak{M}^\sigma}(R^\sigma) \to (\mathrm{Gr}_{\mathfrak{M}}R)^\sigma$. We are going to prove that μ^* is an isomorphism that we seek.

We prove that μ^* is surjective. It suffices to prove that $\overline{y} \in (\mathrm{Gr}^{2d}_{\mathfrak{M}}R)^\sigma$, represented by $y \in \mathfrak{M}^{2d}$, has a pre-image. Write $y = y_1 \dots y_d$ for $y_i \in \mathfrak{M}^2$, let $y_i' = 1/2(y_i + y_i^\sigma)$ for $i = 1, \dots, d$ and $y' = y_1' \dots y_d'$. We note that $y_i' = y_i \mod \mathfrak{M}^3$ so that $y' \in (\mathfrak{M}^\sigma)^d$ and $y = y' \mod \mathfrak{M}^{2d+1}$. Thus y' is a representative of the pre-image of $\overline{y}$.

Next, we prove that μ^* is injective. Let $\overline{x} \in \mathrm{Gr}_{\mathfrak{M}^\sigma}(R^\sigma)$ such that $\mu^*(\overline{x}) = 0$. We can suppose that $\overline{x} \in \mathrm{Gr}^d_{\mathfrak{M}^\sigma}(R^\sigma)$. Let $x \in (\mathfrak{M}^\sigma)^d$ be a representative of $\overline{x}$. As $\mu^*(x) = 0$, $x \in \mathfrak{M}^{2d+1}$ and we have to prove that $x = 0$ that is $\mathfrak{M}^{2d+1} \cap (\mathfrak{M}^\sigma)^d \subset (\mathfrak{M}^\sigma)^{d+1}$. But as $(\mathrm{Gr}^{2d+1}_{\mathfrak{M}}R)^\sigma = 0$, we have $\mathfrak{M}^{2d+1} \cap (\mathfrak{M}^\sigma)^d = \mathfrak{M}^{2d+2} \cap (\mathfrak{M}^\sigma)^d$. So to prove that μ^* is injective, it is enough to prove that for all $n > 0$ integer,

$$\mathfrak{M}^{2n} \cap R^\sigma \subset (\mathfrak{M}^\sigma)^n. \tag{3}$$

If we can prove that for all $n > 0$

$$\mathfrak{M}^{2n} \cap R^\sigma \subset (\mathfrak{M}^\sigma)^n + (\mathfrak{M}^{2(n+1)} \cap R^\sigma). \tag{4}$$

then for $m \geqslant n$, we have:

$$\mathfrak{M}^{2m} \cap R^\sigma \subset (\mathfrak{M}^\sigma)^n + (\mathfrak{M}^{2(m+1)} \cap R^\sigma),$$

and by an easy induction, we obtain that for all $m \geqslant n$:

$$\mathfrak{M}^{2n} \cap R^\sigma \subset (\mathfrak{M}^\sigma)^n + (\mathfrak{M}^{2(m+1)} \cap R^\sigma).$$

As $\cap_{i\in\mathbb{N}}\mathfrak{M}^i = \{0\}$, we have proved (3). So in order to finish the proof, it is enough to obtain (4).

For this, let $x \in \mathfrak{M}^{2n} \cap R^\sigma$, there exists $a_1, \ldots, a_n \in \mathfrak{M}^2$ such that $x = a_1 \ldots a_n$. Using the surjectivity of μ^*, we know that there exists $a_{\sigma,i} \in \mathfrak{M}^\sigma$ for $i = 1, \ldots, n$ such that $a_i = a_{\sigma,i} + \varepsilon_i$ with $\varepsilon_i \in \mathfrak{M}^3$. Let $\theta = a_1 \ldots a_n - a_{\sigma,1} \ldots a_{\sigma,n}$. Clearly, $\theta \in \mathfrak{M}^{2n+1} \cap R^\sigma$. Using the fact that $(\mathrm{Gr}_{\mathfrak{M}}^{2n+1} R)^\sigma = 0$, we have that actually $\theta \in \mathfrak{M}^{2n+2}$ and we are done. □

The following easy lemma complement the preceding lemma.

Lemma 2.2. *Keeping the hypothesis of the preceding lemma, we have an isomorphism:*

$$\mathrm{Gr}_{\mathfrak{M}}(R)^\sigma \simeq \mathrm{Sym}^2(k'[x_1, \ldots, x_g]). \tag{5}$$

Proof. As R is a regular local ring of dimension g, $\mathrm{Gr}_{\mathfrak{M}}(R) \simeq k'[x_1, \ldots, x_g]$. By hypothesis, σ acts by on $\mathrm{Gr}_{\mathfrak{M}}(R)$ by leaving k' fixed and $\sigma(x_i) = -x_i$ for $i = 1, \ldots, g$. As a consequence, $\mathrm{Gr}_{\mathfrak{M}}(R)^\sigma = k'[x_i x_j | i, j \in \{1, \ldots, g\}]$. □

Definition 2.3. Let $(R, \mathfrak{M})$ and $(R', \mathfrak{M}')$ be local rings. We say that a morphism $\lambda : \mathrm{Spec}(\mathrm{Gr}_{\mathfrak{M}'}(R')) \to \mathrm{Spec}(\mathrm{Gr}_{\mathfrak{M}}(R))$ is homogeneous if $\lambda^* : \mathrm{Gr}_{\mathfrak{M}}(R) \to \mathrm{Gr}_{\mathfrak{M}'}(R')$ is a morphism of graduated rings.

Proposition 2.4. *Let K be a dimension g Kummer variety over k and let $T_0^c(K_A)$ be its tangent cone at the point $0 \in K_A(k)$. Then there is a homogeneous isomorphism of algebraic varieties:*

$$\lambda : Q^g = \mathrm{Spec}(\mathrm{Sym}^2(k[x_1, \ldots, x_g])) \to T_0^c(K_A).$$

.

Remark 2.5. In the notation, we omit the field of definition of Q^g since it will be always clear by the context.

Proof. By definition K_A is the quotient of an Abelian variety A by the automorphism (-1) of A. The local ring $\mathscr{O}_{A,0}$ in 0 of A with maximal ideal $\mathfrak{M}$ is regular. The action of the automorphism $(-1)^*$ on $\mathscr{O}_{A,0}$ verifies the hypothesis of lemma 2.1 and $\mathscr{O}_{A,0}^{(-1)} = \mathscr{O}_{K_A,0}$ is the local ring in 0 of K_A. We thus have an isomorphism $\lambda^* : \mathrm{Gr}_{\mathfrak{M}^{(-1)}}(\mathscr{O}_{K_A,0}) \to (\mathrm{Gr}_{\mathfrak{M}}\mathscr{O}_{A,0})^{(-1)}$ and $\mathrm{Gr}_{\mathfrak{M}}(\mathscr{O}_{A,0}))^{(-1)} \simeq \mathrm{Sym}^2(k[x_1, \ldots, x_g])$ by Lemma 2.2. Whence the existence of λ. □

Remark 2.6. We deduce from Proposition 2.4 that the co-tangent space in 0 of a Kummer variety has dimension $g(g+1)/2$. An immediate consequence is that a Kummer variety of dimension g can not be embedded as a closed sub-variety in an ambient space of dimension less than $g(g+1)/2$.

Remark 2.7. Using the standard theory of quotients by a finite group, we can recover Proposition 2.4 as follow. Let $G = \mathbb{Z}/2\mathbb{Z}$ acts on A. Then since A is projective, the quotient $K_A = A/G$ exists, and furthermore the quotient commutes with flat base change. This is a special case of the Keel-Mori theorem [KM97] (see also [Ryd13] for a nice overview). In fact, the existence of a quotient for a finite locally free group acting on a projective scheme is already given in [Gro57, III. Théorème 5.3] (in the greater generality of an action by a groupoid, see also [GD+70, V. Théorème 4.1] for the proofs), and the construction clearly shows that the quotient is uniform (that is stable by flat base change). Furthermore the quotient is geometric in the sense of [MFK94, Theorem 1.1]. See also [GM07, Theorem 4.16] for another proof (in the case of an action by a group).

Now let P be a point of K_A. Its completion $\widehat{O}_{K_{A,P}}$ is flat and quasi compact over $O_{K_{A,P}}$. Since $\pi : A \to K_A$ is finite, the pullback of $\mathrm{Spec}\,\widehat{K}_{A,P}$ is given by $\coprod_{Q\in A,\pi(Q)=P} \mathrm{Spec}\,\widehat{A}_Q$. By uniformity, we then have that $\widehat{O}_{K_{A,P}} = \prod_{Q\in A,\pi(Q)=P} \widehat{O}_{A_Q}^G$.

So if $P \in K_A$ is not a point of 2-torsion, there are two points Q_1 and Q_2 above it. The action of G permutes Q_1 and Q_2, so $\widehat{O}_{K_{A,P}} = \widehat{O}_{A_{Q_1}}\widehat{O}_{A_{Q_2}} \simeq k[[x_1, \ldots, x_g]$. If $P \in K_A$ is a point of two torsion,

Q above P, then since the action of G on the tangent space at Q is given by $x \mapsto -x$, we get that $\widehat{O}^G_{A_Q} \simeq k[[x,y]]/\pm 1 \simeq \mathrm{Sym}^2 k[[x_1,\dots,x_g] \simeq k[[x_i x_j]]$.

Since the tangent cone is also the graduate ring of the completion, we deduce immediately Proposition 2.4. In our case the action is sufficiently simple that we preferred to give an elementary proof of this Proposition.

Proposition 2.8. *The variety $Q^g = \mathrm{Spec}(\mathrm{Sym}^2(k[x_1,\dots,x_g]))$ is birationally equivalent to $\mathbb{A}^g$. By Proposition 2.4 so is $T_0^c(A)$.*

Proof. It suffices to prove that the function field $K(Q^g)$ of Q^g is isomorphic to $k(y_1,\dots,y_g)$. Fix an isomorphism $\mathrm{Sym}^2(k[x_1,\dots,x_g]) \simeq \frac{k[u_{ij}|i,j\in\{1,\dots,g\},i\leqslant j]}{(u_{ij}u_{kl}-u_{ik}u_{jl})}$. Then $K(Q)$ is the field of fractions of $\frac{k[u_{ij}|i,j\in\{1,\dots,g\},i\leqslant j]}{(u_{ij}u_{kl}-u_{ik}u_{jl})}$. The elements u_{1i} for $i=1,\dots,g$ of $K(Q)$ are algebraically independent since from any non trivial algebraic relations between u_{1i} we deduce a non trivial algebraic relation between the y_i of $k[y_1,\dots,y_g]$ via the morphism of k-algebra $\frac{k[u_{ij}|i,j\in\{1,\dots,g\},i\leqslant j]}{(u_{ij}u_{kl}-u_{ik}u_{jl})} \to k[y_1,\dots,y_g]$, $u_{ij}\mapsto y_i y_j$. . Thus we can define a morphism of function fields $\zeta^* : K \to k(y_1,\dots,y_g)$ by $u_{1i}\mapsto y_i$ for $i=1,\dots,g$. It is clear that ζ^* is onto. Since for all $1\leqslant k\leqslant l\leqslant g$, $u_{kl}=u_{1k}u_{1l}/u_{11}$, ζ^* has an inverse and we are done. □

In general the description of an isomorphism between algebraic varieties can involve high degree polynomials and computing it may be difficult. It turns out that the isomorphism of Proposition 2.4 is linear. This is the content of the following proposition and corollary:

Lemma 2.9. *Let R and R' be regular local rings of dimension g with respective maximal ideals $\mathfrak{M}$ and $\mathfrak{M}'$. We suppose that $\mathrm{Gr}_{\mathfrak{M}}R$ and $\mathrm{Gr}_{\mathfrak{M}'}R'$ are isomorphic graded rings and let $\lambda^* : \mathrm{Gr}_{\mathfrak{M}}R \to \mathrm{Gr}_{\mathfrak{M}'}R'$ be an isomorphism of graded rings. Then λ^* induces a linear morphism $\lambda_1^* : \mathfrak{M}/\mathfrak{M}^2 \to \mathfrak{M}'/\mathfrak{M}'^2$. If moreover, R' is generated as a ring by $\mathfrak{M}'/\mathfrak{M}'^2$ then λ^* is uniquely determined by λ_1^*.*

Proof. This is immediate. □

Corollary 2.10. *Every homogeneous isomorphism $\lambda : Q^g \to T_0^c(K_A)$ is linear which means that there exists a linear morphism $\mu : \mathbb{A}(T_0^*(K_A)) \to \mathbb{A}^{g(g+1)/2}$ such that we have the diagram:*

$$\begin{array}{ccc} Q^g & \xrightarrow{\lambda} & T_0^c(K_A) \\ \downarrow & & \downarrow \\ \mathbb{A}^{g(g+1)/2} & \xrightarrow{\mu} & \mathbb{A}(T_0^*(K_A)) \end{array}$$

where the vertical arrows are the canonical immersions.

Proof. This is an immediate consequence of the preceding Lemma. □

Denote by $\mathrm{Aut}(\mathbb{A}^g)$ the group of automorphisms of $\mathbb{A}^g$ preserving the origin. Let $\mathrm{Aut}(Q^g)$ be the group of homogeneous (see Definition 2.3) automorphisms of Q^g. In order to compute an isomorphism between $T_0^c(K_A)$ and Q^g, it will be useful to have a description of $\mathrm{Aut}(Q^g)$ since this group acts on the right on the set of isomorphisms between $T_0^c(K_A)$ and Q^g. First, we remark that

Lemma 2.11. *The variety Q^g is the quotient of $\mathbb{A}^g$ by the action of ± 1 on it.*

Proof. Let $\pi : Q^g \to \mathbb{A}^g$ be the map given on coordinate ring by the injection $\pi^* : \mathrm{Sym}^2(k[x_1,\dots,x_g]) \simeq \frac{k[u_{ij}|i,j\in\{1,\dots,g\},i\leqslant j]}{(u_{ij}u_{kl}-u_{ik}u_{jl})} \to k[x_i|i\in\{1,\dots,g\}]$, $u_i\mapsto x_i^2$, $v_{ij}\mapsto x_i x_j$. It is clear that the image of π^* is the sub-ring of invariants of $k[x_i|i\in\{1,\dots,g\}]$ by the action of -1 whence the lemma. □

We denote by $\pi : \mathbb{A}^g \to Q^g$ the canonical projection. Every automorphism f of $\mathbb{A}^g$ preserving the origin is linear, so that f commutes with the action of -1 and induces an automorphism $\overline{f}$ of Q^g such that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{A}^g & \xrightarrow{f} & \mathbb{A}^g \\ \pi \downarrow & & \downarrow \pi \\ Q^g & \xrightarrow{\overline{f}} & Q^g \end{array}$$

Denote by τ the map given by $f \mapsto \overline{f}$.

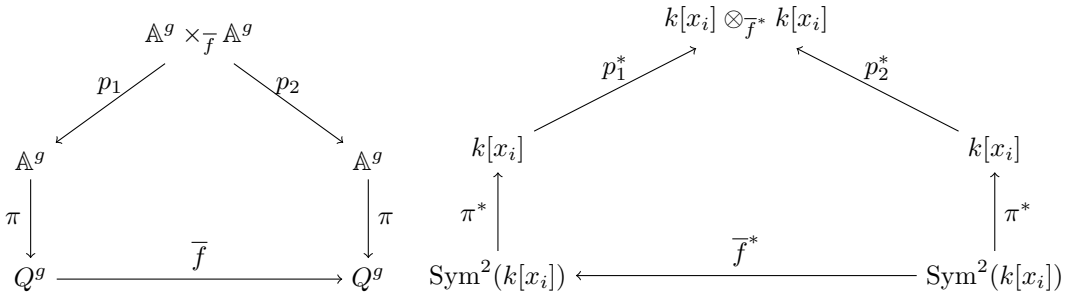
Theorem 2.12. *There is an exact sequence:*

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{A}^g) \xrightarrow{\tau} \mathrm{Aut}(Q^g) \to 0, \tag{6}$$

where $\mathbb{Z}/2\mathbb{Z}$ is sent to the ± 1 subgroup of $\mathrm{Aut}(\mathbb{A}^g)$.

Proof. Let $f \in \mathrm{Aut}(\mathbb{A}^g)$ be such that $\overline{f} = \tau(f) = 1$. Let $R = \frac{k[u_{ij}|i,j\in\{1,\dots,g\},i\leqslant j]}{(u_{ij}u_{kl}-u_{ik}u_{jl})}$, we fix the isomorphism $R \simeq \mathrm{Sym}^2(k[x_1,\dots,x_g])$, $u_{ij} \mapsto x_ix_j$. As $\overline{f}^*(u_{ii}) = u_{ii}$, $f^*(x_i) = \pm x_i$. Suppose, for instance, that $f^*(x_1) = x_1$, then for $j \in \{2,\dots,g\}$, as $\overline{f}^*(u_{1j}) = u_{1j}$, $f^*(x_j) = x_j$. The case $f^*(x_1) = -x_1$ is similar so that we have proved that $\ker(\tau) \simeq \mathbb{Z}/2\mathbb{Z}$.

It only remains to prove that τ is onto. For this let $\overline{f} \in \mathrm{Aut}(Q^g)$ and consider the followings dual diagrams:



In these diagrams, $\mathbb{A}^g \times_{\overline{f}} \mathbb{A}^g$ is the fiber product of $\mathbb{A}^g$ by $\mathbb{A}^g$ over $\overline{f}$. We condider $k[x_1,\dots,x_g]$ as a R-module via the inclusion $\pi^* : R \to k[x_1,\dots,x_g]$, $u_{ij} \mapsto x_ix_j$. As $\overline{f}^*$ is an automorphism of $\mathrm{Sym}^2(k[x_1,\dots,x_g])$, the tensor product $k[x_i] \otimes_{\overline{f}^*} k[x_i]$ is the coordinate ring of $\mathbb{A}^g \times_{\overline{f}} \mathbb{A}^g$. We consider $k[x_i] \times_R k[x_i]$ as a skew-right-module in the following sense: for all $x \in k|x_i] \times_R k[x_i]$ and $\lambda \in R$, we put $\lambda x = x\overline{f}^*(\lambda)$. It is then clear that the map $k[x_i] \otimes_R k[x_i] \to k[x_i] \otimes_{\overline{f}} k[x_i], x \otimes y \mapsto x \otimes y$ is an isomorphism so that $\mathbb{A}^g \times_{\overline{f}} \mathbb{A}^g$ is isomorphic to $\mathbb{A}^g \times_{Q^g} \mathbb{A}^g$. But as $\pi : \mathbb{A}^g \to Q^g$ is a degree two étale covering, $\mathbb{A}^g \times_{Q^g} \mathbb{A}^g \simeq \sqcup_{i=1,2}\mathbb{A}^g$. By considering the restriction of p_1 on one of the two components of $\sqcup_{i=1,2}\mathbb{A}^g \xrightarrow{p_1} \mathbb{A}^g$, p_1 admits a section that we denote by p_1^{-1}. Let $f = p_2 \circ p_1^{-1}$, it clear by construction that $\tau(f) = \overline{f}$. □

We can give a useful matrix interpretation of the preceding theorem. For this, we fix coordinate systems with the isomorphisms $\mathbb{A}^g \simeq \mathrm{Spec}(k[x_i])$ and $Q^g \simeq \mathrm{Spec}(\frac{k[u_{ij}|i,j\in\{1,\dots,g\},i\leqslant j]}{(u_{ij}u_{kl}-u_{ik}u_{jl})})$ and $\pi^*(u_{ij}) = x_ix_j$ for $i,j \in \{1,\dots,g\}$, $i \leqslant j$. Then to $f \in \mathrm{Aut}(\mathbb{A}^g)$, we can associate the matrix $M_{f^*} = (\alpha_{ij}) \in \mathrm{GL}(g,k)$ such that $f^*(x_i) = \sum_{j=1}^g \alpha_{ij}x_j$. In the same way, by choosing a bijection $\nu : \{1,\dots,g(g+1)/2\} \to \{(i,j), 1 \leqslant i \leqslant j \leqslant g\}$, to $\overline{f} \in \mathrm{Aut}(Q^g)$, we can associate the matrix $M_{\overline{f}^*} = (\gamma_{ij}) \in \mathrm{GL}(g(g+1)/2,k)$ such that $f^*(u_{\nu(i)}) = \sum_{j=1}^{g(g+1)/2} \alpha_{ij}u_{\nu(j)}$.

We have $M_{\overline{f}^*} = \mathrm{Sym}^2(M_{f^*})$ because

$$\overline{f}^*(u_{ij}) = f^*(x_ix_j) = (\sum_{k=1}^g \alpha_{ik}x_k)(\sum_{l=1}^g \alpha_{jl}x_l) = \sum_{k,l=1,\dots,g,k\leqslant l}^g (\alpha_{ik}\alpha_{jl} + \alpha_{jk}\alpha_{il})u_{kl}.$$

In order to describe the image of the map $M_{f^*} \mapsto \mathrm{Sym}^2(M_{f^*})$, consider the quadratic forms:

$$Q_{ijkl} = u_{ij}u_{kl} - u_{ik}u_{jl},$$

for $i,j,k,l = 1,\dots,g, i < j < k < l$. We have an action of $\mathrm{GL}(g(g+1)/2,k)$ on $k[u_{ij}|i,j \in \{1,\dots,g\}, i \leqslant j]$ by setting for $(\alpha_{kl}) \in \mathrm{GL}(g(g+1)/2,k)$, $(\alpha_{kl})(u_{ij}) = \sum_{m=1}^{g(g+1)/2} \alpha_{\nu^{-1}((i,j)),m} u_{\nu(m)}$. We denote by $SO(Q^g)$ (resp. $O(Q^g)$) the subgroup of $\mathrm{SL}(g(g+1)/2,k)$ (resp. of $\mathrm{GL}(g(g+1)/2,k)$ which leaves invariant the vector space generated by the quadratic forms Q_{ijkl}.

We have isomorphisms $d_0 : \mathrm{GL}(g,k) \simeq SL(g,k) \rtimes k^*$ and $d_1 : O(Q^g) \simeq SO(Q^g) \rtimes k^*$ and the following commutative diagram:

$$\begin{array}{ccc} \mathrm{GL}(g,k) & \xrightarrow{\varphi} & O(Q^g) \\ \Big\downarrow{\scriptstyle d_0} & & \Big\downarrow{\scriptstyle d_1} \\ SL(g,k) \rtimes k^* & \xrightarrow{\varphi'} & SO(Q^g) \rtimes k^* \end{array}$$

where φ and φ' are defined by:

$$\varphi : M \mapsto \mathrm{Sym}^2(M), \varphi' : (M,\lambda) \mapsto (\mathrm{Sym}^2(M), \lambda^2). \tag{7}$$

Then Theorem (2.12) tells that φ is surjective and that φ' restricted to $SL(g,k)$ is surjective onto $SO(Q^g)$.

Example 2.13. In the case $g = 2$, there is one quadratic form $Q_{1122} = u_{11}u_{22} - u_{12}^2$. Its associated matrix in the basis (u_{11}, u_{22}, u_{12}) is:

$$M(Q_{1122}) = \frac{1}{2}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}.$$

If

$$\begin{pmatrix} x_1' \\ x_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x_1' \\ x_2' \end{pmatrix}$$

is a change of coordinates then:

$$\mathrm{Sym}^2\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} a^2 & b^2 & 2ab \\ c^2 & d^2 & 2cd \\ ac & bd & ad+bc \end{pmatrix}.$$

And Theorem (2.12) tells that the map:

$$\begin{aligned} SL(2,k)/\pm 1 &\to SO(Q^2) \\ \pm M &\mapsto \mathrm{Sym}^2(M) \end{aligned} \tag{8}$$

is a bijection.

Remark 2.14. It is clear that from the knowledge of $\mathrm{Sym}^2(M) \in SO(Q^g)$, one can recover $\pm M$ at the expense of a square root and $g^2 - 1$ divisions in k.

We consider the computation of the tangent cone of a Kummer variety. We suppose that a Zariski neighbourhood U of $0 \in K_A(k)$ is given as a closed sub-variety of $\mathbb{A}^m$, the affine space of dimension m, by an ideal $I(U)$ generated by $(h_i)_{i=1,\dots,\ell}$ with $h_i \in k[x_1,\dots,x_m]$. We suppose that via this embedding, the point $0 \in K_A(k)$ is sent to the point $0 \in \mathbb{A}^m(k)$. We would like to compute a model of the tangent cone. By that we mean computing a coordinate system of $T_0(K_A)$ and a embedding of $T_0^c(K_A)$ inside $T_0(K_A)$ by a set of algebraic equations.

For any $h \in k[x_1,\dots,x_m]$ we denote by $\min(h)$ the homogeneous component of smallest degree of h. Then we know [CLO92, Definition 2, p. 527] that the ideal $I(T_0^c(K_A))$ of $T_0^c(K_A)$ is generated by the set $\{\min(h)|h \in I(U)\}$. As for $\alpha, \beta \in k[x_1,\dots,x_m]$, we do not have in general that $\min(\alpha) + \min(\beta) = \min(\alpha+\beta)$, it is not true that $I(T_0^c(K_A))$ is generated by $(\min(h_i))_{i=1,\dots,\ell}$. It is shown in [CLO92, Proposition 4] that a set of generators of $I(T_0^c(K_A))$ can be recovered by computing a homogeneous

Groebner basis for a well chosen monomial order of the homogenized ideal of I. Such a computation may be very time consuming and the complexity of a Groebner basis computation is sometimes difficult to assess. In the case of the tangent cone of a Kummer variety, the following proposition, the proof of which relies on Proposition 2.4 shows that it can be obtained with a well controlled and limited amount of computations.

Proposition 2.15. *Let K_A be a Kummer variety. We suppose given a closed embedding $\zeta : U \to \mathbb{A}^m = \mathrm{Spec}(k[x_1,\dots,x_m])$ where U is a Zariski neighbourhood of $0 \in K_A(k)$. Let $I(U) = \{z \in k[x_1,\dots,x_m] | \zeta^*(z) = 0\}$, we suppose that the ideal I is generated by $(h_i)_{i=1,\dots,\ell}$ and that $\zeta(0) = 0 \in \mathbb{A}^m(k)$. Let I_1 be the ideal generated by the set $\{\min(h_i) | \deg(\min(h_i)) = 1, i = 1,\dots,\ell\}$. Let I_2 be the ideal generated by the set $\{\min(h), h \in I(U), \deg(\min(h)) = 2\}$. Then:*

- *the image of $(d\zeta)_0 : T_0(K_A)) \to \mathbb{A}^m$ (where $(d\zeta)_0$ is the derivative of ζ in 0, see Section 1) is the linear sub-space of $\mathbb{A}^m$ such that $(d\zeta)_0^*(I_1) = 0$;*
- *$\mathrm{Spec}(\frac{k[x_1,\dots,x_m]}{(I_1,I_2)})$ is $T_0^c(K_A)$ embedded in $T_0^*(K_A)$.*

Remark 2.16. The first claim of the proposition which describes $T_0(K_A)$ is general and makes no use of any particular property of the singular point of a Kummer variety.

Proof. For the first claim of the proposition, let $S_\varepsilon = \mathrm{Spec}(\overline{k}[\varepsilon]/\varepsilon^2])$ then $T_0(K_A)(\overline{k})$ is by definition the set of morphisms $S_\varepsilon \to K_A$ such that $\mathrm{Spec}(\overline{k}) \to S_\varepsilon \to K_A$ is the 0-point morphism (here $\mathrm{Spec}(\overline{k}) \to S_\varepsilon$ comes from the map $\overline{k}[\varepsilon]/\varepsilon^2 \to \overline{k}$ defined by $1 \mapsto 1$, $\varepsilon \mapsto 0$). This is in bijection with the set of $\overline{k}$-algebra morphisms $\kappa : \frac{\overline{k}[x_1,\dots,x_m]}{(h_1,\dots,h_\ell)} \to \overline{k}[\varepsilon]/\varepsilon^2$ such that $\kappa(x_i) = 0 \mod \varepsilon$. Such a $\overline{k}$-algebra morphism κ is given by $(\lambda_i) \in \overline{k}^m$ such that $\kappa(x_i) = \lambda_i\varepsilon$. By writing that $\kappa(h_i) = 0$, it is clear that the point $(\lambda_i) \in \overline{k}^m$ is in $T_0^*(K_A)(\overline{k})$ if and only if it satisfies the relations of I_1.

For the second claim of the proposition, we know from Corollary 2.10 that the isomorphism $\mu : T_0^c(K_A) \to Q^g$ is linear so that μ^* preserves the degree of rational functions. As a consequence, if we make the identification $Q^g = \mathrm{Spec}(\frac{k[u_{ij}|i,j\in\{1,\dots,g\},i\leqslant j]}{(u_{ij}u_{kl}-u_{ik}u_{jl})})$, the $\mu^*(u_{ij}u_{kl} - u_{ik}u_{jl})$ are contained in I_2. We know moreover that the $u_{ij}u_{kl} - u_{ik}u_{jl}$ is a complete set of relations for Q^g. Since μ^* is an isomorphism the $\mu^*(u_{ij}u_{kl} - u_{ik}u_{jl})$ generate the ideal of the tangent cone $T_0^c(K_A)$ embedded in $T_0(K_A)$. □

Remark 2.17. In the preceding proposition, up to a linear transformation of $\mathbb{A}^m$, we can suppose that I_1 is generated by $(x_{g(g+1)/2+1},\dots,x_m)$. In this case, the embedding $(d\zeta)_0 : T_0^*(K_A) = \mathrm{Spec}(k[x_1,\dots,x_{g(g+1)/2}]) \to \mathbb{A}^m = \mathrm{Spec}(k[x_1,\dots,x_m])$ is defined by $(d\zeta)_0^*(x_i) = 0$ if $i > g(g+1)/2$ and $(d\zeta)_0^*(x_i) = x_i$ otherwise. The tangent cone of $T_0^c(K_A)$ considered as a closed subset of $T_0(K_A) = \mathrm{Spec}(k[x_1,\dots,x_{g(g+1)/2}])$ is then just defined by the ideal $(d\zeta)_0^*(I_2)$.

From the Proposition 2.15 and Remark 2.17, we deduce the Algorithm 3 which computes equations for the tangent cone at 0 of a dimension g Kummer variety K_A over the field k. More precisely, Algorithm 3, takes as input a closed embedding $U \to \mathbb{A}^m$ where U is an open neighbourhood of $0 \in K_A(k)$ and outputs:

- A linear automorphism $\sigma : \mathbb{A}^m \to \mathbb{A}^m$ such that the image of the embedding $\sigma \circ (d\zeta)_0 : \mathbb{A}(T_0^*(K_A)) \to \mathbb{A}^m = \mathrm{Spec}(k[x_1,\dots,x_m])$ is the closed sub-variety given by $x_i = 0$ for $i > g(g+1)/2$ so that we can identify $T_0^*(K_A)$ with $\mathrm{Spec}(k[x_1,\dots,x_{g(g+1)/2}])$;
- G_{I_2} a set of generators of the ideal I_2 such that $T_0^c(K_A)$ is the closed sub-variety of $\mathbb{A}(T_0^*(K_A))$ given as $\mathrm{Spec}(k[x_1,\dots,x_{g(g+1)/2}]/I_2)$

In general, to compute degree m relations of the tangent cone, one need to compute the Macauley matrix of degree m induced by generators of the defining ideal $I(U)$ and compute the row echelon form. In our case, from the structure theorem, we know that once we have done the linear change of variable to work in a linear space of dimension $g(g+1)/2$, we can recover the degree 2 relations directly from the generators.

If the closed embedding is given by ℓ polynomials in $(h_i)_{i=1,\dots,\ell}, h_i \in k[x_1,\dots,x_m]$ then Algorithm 1 for the computation of the equation of the tangent cone needs to compute the Gaussian elimination of a matrix with $O(\ell)$ lines and $O(m)$ columns, (line 2 of Algorithm 1). This costs $O(\ell^2 m)$ operations in the base field. We remark that heuristically, in practice we may take $\ell = m + O(1)$. Afterwards, for

the substitution of x'_i, we may precompute all x_ix_j in terms of the x'_i for a total cost of $O(m^2g^4)$, and then the substitution of h_i costs $O(m^2)$ additions of a polynomials with $O(g^4)$ monomials (since we may truncate everything in degree 2). The total cost is $O(\ell m^2 g^4)$.

We may also compute an echelon form of the monomial coefficients of the elements in G_{I_2} in order to remove the linear relations between the equations. This involve the reduction of a matrix with ℓ lines and $g(g+1)/2$ columns, hence costs $O(\ell^2 g^2)$. We may then assume that G_{I_2} is given by $O(g^4)$ equations.

Proposition 2.18. *Suppose that $h_i = 0$, where $h_i \in k[x_1, \dots, x_m]$, for $i = 1, \dots, \ell$ are equations for K_A, a dimension g Kummer variety over k, in a neighbourhood of $0 \in K_A(k)$ in the ambient space $\mathbb{A}^m$. The complexity of Algorithm 1 to compute equations of $T_0^c(K_A)$ is $O(\ell m^2 g^4)$ operations in the base field.*

Algorithm 1: Algorithm to compute equations for the tangent cone at 0 of a Kummer variety.

input : The polynomials:

$$(h_i)_{i=1,\dots,\ell}, h_i \in k[x_1, \dots, x_m],$$

where $h_i = 0$ for $i = 1, \dots, \ell$ are equations for K_A, a dimension g Kummer variety over k, in a neighbourhood of $0 \in K_A(k)$ in the ambient space $\mathbb{A}^m$.

output :

- An invertible matrix Σ such that if $(x'_1, \dots, x'_m) = (x_1, \dots, x_m)\Sigma$ the ideal I_1 is generated by x'_i for $i > g(g+1)/2$;
- G_{I_2} a set of generators of the ideal I_2 such that $T_0^c(K_A) \simeq \mathrm{Spec}(\frac{k[x'_1,\dots,x'_{g(g+1)/2}]}{I_2})$.

Set $G_{I_1} = \{\min(h_i) | \deg(\min(h_i)) = 1, i = 1, \dots, \ell\}$;
Using a Gaussian elimination compute an invertible matrix Σ such that if $(x'_1, \dots, x'_m) = (x_1, \dots, x_m)\Sigma$, $\mathrm{Span}(x'_{g(g+1)/2+1}, \dots, x'_m) = \mathrm{Span}(G_{I_1})$;
for $i \leftarrow 1$ **to** ℓ **do**
    Compute h'_i such that $h'_i(x'_1, \dots, x'_m) = h_i(x_1, \dots, x_m)$;
    $w_i \leftarrow h'_i(x'_1, \dots, x'_{g(g+1)/2}, 0, \dots, 0)$ // $w_i \in k[x'_1, \dots, x'_{g(g+1)/2}]$
end
for $i \leftarrow 1$ **to** ℓ **do**
    if $\deg(\min(w_i)) = 2$ **then**
        Add $\min(w_i)$ to G_{I_2};
    end
end
return Σ, G_{I_2};

Example 2.19. Let k be a field of characteristic different from 2 and let K_A be a Kummer surface over k. Using level 2 theta coordinates, one can embed K_A into $\mathbb{P}^3$. This embedding is defined by a degree 4 homogeneous equation f [CF+96]. The 0 point of K_A inside $\mathbb{P}^3$ is given by homogeneous coordinates $(\theta_i(0_A)_{i=0,\dots,3})$. If $\theta_0(0_A) \neq 0$, an affine neighborhood of 0_A is given by the coordinates $(\theta_i/\theta_0 - \theta_i(0_A)/\theta_0(0_A))_{i=1,\dots,3}$. Plugging these coordinates into the equation f and taking the degree 2 part gives the equation of the tangent cone at 0_A. It lives inside the cotangent space which in this case is $\mathbb{P}^3$, so does not require any linear equation.

3. Linear representation of endomorphisms of Kummer varieties

Let $K_A = A/\pm 1$ be a Kummer variety over k. We say that $\overline{f} : K_A \to K_A$ is an endomorphism of K_A if there exists $f \in \mathrm{End}(A)$ such that the diagram:

$$\begin{array}{ccc} A & \xrightarrow{f} & A \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ K_A & \xrightarrow{\overline{f}} & K_A \end{array}$$

is commutative. We denote by $\mathrm{End}(K_A)$ the group of endomorphisms of K_A. Let $f \in \mathrm{End}(A)$, it induces an automorphism $(df)_0^* : T_0^*(A) \to T_0^*(A)$ so that we have a map $\rho : \mathrm{End}(A) \to \mathrm{Aut}(T_0(A))$. If moreover we chose a basis of $T_0^*(A)$, we obtain:

$$\rho_0 : \mathrm{End}(A) \to \mathrm{GL}(g,k). \tag{9}$$

Starting from $\overline{f} \in \mathrm{End}(K_A)$ we can lift it to $\{f, -f\} \subset \mathrm{End}(A)$ so that we have a map:

$$\overline{\rho}_0 : \mathrm{End}(K_A) \to \mathrm{GL}(g,k)/(\pm 1) \tag{10}$$

The aim of this section is to present an efficient method to compute $\overline{\rho}_0$. More precisely, for each $\overline{f} \in \mathrm{End}(K_A)$ we want to compute a matrix $M_{\overline{f}}$ which is in the same conjugacy class as $\overline{\rho}_0(f)$. By this, we mean that there exists $T \in \mathrm{GL}(g,k)$ such that:

$$M_{\overline{f}} = \pm T\rho(f)T^{-1}. \tag{11}$$

In particular, we obtain all the similarity invariants of $\rho_0(f)$ up to a sign.

Let $\overline{f} \in \mathrm{End}(K_A)$, the idea of how to compute $\rho_0(f)$ up to a sign is explained in Diagram (12).

$$\begin{array}{ccccc} & & T_0(A) & \xrightarrow{(df)_0} & T_0^*(A) & & \\ & \swarrow^{\gamma} & \downarrow{\scriptstyle\pi_0} & & \downarrow{\scriptstyle\pi_0} & \searrow^{\gamma} & \\ & & T_0^c(K_A) & \xrightarrow{(d\overline{f})_0} & T_0^c(K_A) & & \\ & & {\scriptstyle\lambda_0}\uparrow & & \uparrow{\scriptstyle\lambda_0} & & \\ & & Q^g & \xrightarrow{\mathrm{Sym}^2(\delta)} & Q^g & & \\ & & \uparrow{\scriptstyle\pi_1} & & \uparrow{\scriptstyle\pi_1} & & \\ & \searrow_{\gamma} & \mathbb{A}^g & \xrightarrow[\delta]{} & \mathbb{A}^g & \swarrow_{\gamma} & \end{array} \tag{12}$$

In this diagram $\pi_0 : T_0(A) \to T_0^c(K_A)$ and $\pi_1 : \mathbb{A}^g \to Q^g$ are the canonical projections. From the knowledge of $\overline{f}$, one can compute $(d\overline{f})_0$ and we would like to recover $\pm(df)_0$ up to conjugation. For this we chose an isomorphism $\gamma : T_0(A) \to \mathbb{A}^g$. Then $\delta = \gamma \circ (df)_0 \circ \gamma^{-1}$ and we want to recover δ. Proposition 2.4 ensure that there exists an isomorphism $\lambda : Q^g \to T_0^c(K)$. We are going to show that once we have chosen γ, there exists a unique isomorphism $\lambda_0 : Q^g \to T_0^c(K_A)$ which makes Diagram (12) commutative. As we know $(d\overline{f})_0$ we can recover $\mathrm{Sym}^2(\delta)$ as $\lambda_0^{-1} \circ (d\overline{f})_0 \circ \lambda_0$. From $\mathrm{Sym}^2(\delta)$ we recover easily $\pm\delta$ and we are done. We want to prove that there exists a (unique) λ_0 which makes Diagram (12) commutative and at the same time have an effective way to compute λ_0. For this, it is convenient look more in detail at the arithmetic of a group quotiented by (-1).

Let G be a general Abelian group and denote by K the quotient of G by the automorphism (-1). Let $\pi : G \to K$ be the canonical projection. In the following if $x \in G$, we denote by $\overline{x} \in K$ the element $\pi(x)$. In general, K is not anymore a group but still enjoys some arithmetic properties inherited from G. For instance, for all $\lambda \in \mathbb{N}$ and $\overline{x} \in K$, $\lambda\overline{x} \in K$ is well defined. In fact, $\overline{x}$ lift via π to $\{+x, -x\}$ and $\{\lambda x, -\lambda x\}$ is going via π to the same element in K that we denote by $\lambda\overline{x}$. In the same way, we have the following arithmetic operations in K [LR16]:

- Normal addition: from the knowledge of $\overline{x}, \overline{y} \in K$, compute the pair $\{\overline{x-y}, \overline{x+y}\}$. We denote it by $\mathrm{NormAdd}(\overline{x}, \overline{y})$.
- Differential addition: from the knowledge of $\overline{x}, \overline{y}, \overline{x-y} \in K$ compute $\overline{x+y}$. We denote it by $\mathrm{DiffAdd}(\overline{x}, \overline{y}, \overline{x-y})$.
- Three-way addition: from the knowledge of $\overline{x}, \overline{y}, \overline{z}, \overline{x+y}, \overline{y+z}$, compute $\overline{y+z}$. We denote it by $\mathrm{ThreeWayAdd}(\overline{x}, \overline{y}, \overline{z}, \overline{x+y}, \overline{x+y})$.

All this apply to $K_A(\overline{k})$ which is the quotient of $A(\overline{k})$ by the automorphism -1 acting on it, and to $T_0^c(K_A)(\overline{k}) = T_0(A)(\overline{k})/\pm 1$.

Definition 3.1. We denote by $\pi_1 : \mathbb{A}^g \to Q^g = \mathbb{A}^g/(\pm 1)$ the canonical projection. Let $\overline{x}_1, \dots, \overline{x}_g \in Q^g(\overline{k})$. We say that $\overline{x}_1, \dots, \overline{x}_g \in Q^g(\overline{k})$ are in general position if there exists $x_1, \dots, x_g \in \mathbb{A}^g(\overline{k})$ such that

- $\pi_1(x_i) = \overline{x}_i$ for $i = 1, \dots, g$;
- $x_1, \dots, x_g$ span the $\overline{k}$-vector space $\mathbb{A}^g(\overline{k})$.

Let $\overline{x}_1, \dots, \overline{x}_g \in Q^g(\overline{k})$ be points in general position. We define $(\overline{x}_{ij})_{1 \leqslant i \leqslant j \leqslant g} \in Q^g(\overline{k})$ in the following manner:

- for $j = 1, \dots, g$, $\overline{x}_{jj} = \overline{x}_j$;
- for $j = 2, \dots, g$, $\overline{x}_{1j}$ is an element in $\mathrm{NormAdd}(\overline{x}_1, \overline{x}_j)$ (recall that NormAdd returns of pair);
- for $1 \leqslant i \leqslant j \leqslant g$, $i \geqslant 2$, $\overline{x}_{ij}$ is defined as: $\mathrm{ThreeWayAdd}(\overline{x}_1, \overline{x}_i, \overline{x}_j, \overline{x}_{1i}, \overline{x}_{1j})$.

We say that $(\overline{x}_{ij})_{1 \leqslant i \leqslant j \leqslant g}$ is a compatible basis of $Q^g(\overline{k})$ associated to $\overline{x}_1, \dots, \overline{x}_g \in Q^g(\overline{k})$.

We extend these definitions for any $\overline{x}_1, \dots, \overline{x}_g \in T_0^c(K_A)(\overline{k})$ using an isomorphism $\lambda : Q^g \to T_0^c(K_A)$ given by Proposition 2.4.

Example 3.2. Let $Q^g = \mathrm{Spec}(\frac{k[u_{ij} | i,j \in \{1,\dots,g\}, i \leqslant j]}{(u_{ij}u_{kl} - u_{ik}u_{jl})})$ so that we have the coordinate system (u_{ij}) on Q^g. Let $\Lambda = (\lambda_1, \dots, \lambda_g) \in \overline{k}^g$. For $1 \leqslant k \leqslant l \leqslant g$, we define the points $P_{kl}(\Lambda) \in Q^g(\overline{k})$ as:

$$u_{ij}(P_{kl}) = \begin{cases} \lambda_i^2 \text{ if } i = j = k \text{ or if } i = j = l, \\ \lambda_i \lambda_j \text{ if } i = k \text{ and } j = l, \\ 0 \text{ otherwise,} \end{cases} \tag{13}$$

for $1 \leqslant i \leqslant j \leqslant g$. Let $\mathbb{A}^g = \mathrm{Spec}(k[x_1, \dots, x_g])$, for $1 \leqslant i \leqslant g$, we define the points $P_i(\Lambda) \in \mathbb{A}^g(\overline{k})$ such that

$$x_j(P_i) = \lambda_i \text{ if } i = j \text{ and } 0 \text{ otherwise.}$$

Then it is easily seen that for $1 \leqslant i \leqslant g$, $\pi_1(P_i) = P_{ii}$ and for $1 \leqslant i \leqslant j \leqslant g$, $\pi_1(P_i + P_j) = P_{ij}$. From this, we deduce that $(P_{kl}(\Lambda))$ form a compatible basis of $Q^g(\overline{k})$ that we call the Λ-standard compatible basis. If $\Lambda = (1, \dots, 1)$, we denote it by (P_{kl}) and call it the standard compatible basis of $Q^g(\overline{k})$.

Proposition 3.3. *Let $(x_i)_{i=1,\dots,g} \in \mathbb{A}^g(\overline{k})$. Define the $(\overline{x}_{ij})_{1 \leqslant i \leqslant j \leqslant g}$ a family of points of Q^g by:*

$$\begin{aligned} \pi_1(x_i) &= \overline{x}_{ii}, \quad \textit{for} \quad i = 1, \dots, g \\ \pi_1(x_i + x_j) &= \overline{x}_{ij}, \quad \textit{for} \quad 1 \leqslant i \leqslant j \leqslant g. \end{aligned} \tag{14}$$

Then $(\overline{x}_{ij})_{1 \leqslant i \leqslant j \leqslant g}$ is a compatible basis of Q^g if and only if $(x_i)_{=1,\dots,g}$ is a basis of $\mathbb{A}^g(\overline{k})$. Moreover $(x_i)_{i=1,\dots,g}$ and $(-x_i)_{i=1,\dots,g}$ are the only two basis of $\mathbb{A}^g(\overline{k})$ satisfying the relations (14).

Proof. The first claim is an immediate consequence of Definition 3.1.

Let $x_i' \in \mathbb{A}^g(\overline{k})$ be such that $\pi_1(x_i') = \overline{x}_i$. We chose $x_1 \in \{x_1', -x_1'\}$. For $j \geqslant 2$, we have $\mathrm{NormAdd}(\overline{x}_1, \overline{x}_i) \in \{\overline{x_1 + x_i'}, \overline{x_1 - x_i'}\}$ so the knowledge of $\overline{x}_{1i}$ corresponds to a choice of x_i in $\{x_i', -x_i'\}$. Hence the signs of x_i is completely determined from the choice of sign of x_1, and it is clear that replacing x_1 by $-x_1$ replaces all the x_i by $-x_i$. Once we have chosen the base $(x_i)_{i=1,\dots,g}$, it is clear from the definition of a compatible basis that it is a basis of $\mathbb{A}^g(\overline{k})$ and it satisfies all the relations (14). □

We have the following easy lemma:

Lemma 3.4. *Let $\overline{x}_1, \dots, \overline{x}_g \in Q^g(k)$ be points in general position. Let $(\overline{x}_{ij})_{1 \leqslant i \leqslant j \leqslant g}$ be the associated compatible basis following Definition 3.1. Denote by $k[\overline{x}_{ij}]$ the field of definition of $\overline{x}_{ij}$. Then :*

(1) *$k[\overline{x}_{ij}]$ is either k or a degree 2 extension of k;*
(2) *the field of definition of all the points in $(\overline{x}_{ij})$ is the compositum of the fields $k[\overline{x}_{1j}]$ for $j = 1, \dots, g$;*
(3) *suppose that for a $j = 2, \dots, g$, $k[\overline{x}_{1j}]$ is a degree 2 extension of k, let $\{\overline{x}_{1j}, \overline{x}'_{1j}\} = \mathrm{NormAdd}(\overline{x}_1, \overline{x}_j)$ then $\overline{x}_{1j}, \overline{x}'_{1j}$ are conjugates by the Galois action of the extension $k[\overline{x}_{1j}]$ over k.*

Proof. The first claim follows from the fact that π_1 has degree 2. The second is a consequence that $(\overline{x}_{ij})$ can be computed from the knowledge of $\overline{x}_{jj}$ for $j = 1, \dots, g$ and $\overline{x}_{1j}$ for $j = 2, \dots, g$ using ThreeWayAdd which is defined over k. The last claim is clear. □

Proposition 3.5. *Let $\overline{x}_{ij} \in Q^g(\overline{k})$ for $1 \leqslant i \leqslant j \leqslant g$ be a compatible basis of Q^g. Then $(\overline{x}_{ij})$ is a basis of the vector space of geometric points of $\mathbb{A}^{g(g+1)/2}$ in which Q^g is embedded. Moreover there exists a unique automorphism μ of Q^g which extends to the linear morphism $\mu' : \mathbb{A}^{g(g+1)/2} \to \mathbb{A}^{g(g+1)/2}$ defined by $\mu'(P_{ij}(\Lambda)) = \overline{x}_{ij}$ for $1 \leqslant i \leqslant j \leqslant g$ and $\Lambda \in \overline{k}^g$.*

Proof. The first claim follows immediately from the second and the fact that the standard compatible basis of Q^g defined in Example 3.2 is basis of the vector space $\mathbb{A}^{g(g+1)/2}(\overline{k})$.

By Proposition 3.3, $(\overline{x}_{ij})$ (resp. $(P_{ij}(\Lambda))$) lifts to a unique, basis $(x_i)_{i=1,\dots,g}$ (resp. $(Q_i)_{i=1,\dots,g}$) up to a sign of $\mathbb{A}^g(\overline{k})$. There exists a unique linear automorphism $\mu_0 \in \mathrm{Aut}(\mathbb{A}^g))$ such that $\mu_0(Q_i) = x_i$ for $i = 1, \dots, g$. This μ_0 is defined up to a sign by the choice of the basis $(x_i)_{i=1,\dots,g}$ and $(Q_i)_{i=1,\dots,g}$. So that μ_0 defines via π_1 a unique μ which makes the diagram commutative:

$$\begin{array}{ccc} \mathbb{A}^g & \xrightarrow{\mu_0} & \mathbb{A}^g \\ \pi_1 \downarrow & & \downarrow \pi_1 \\ Q^g & \xrightarrow{\mu} & Q^g \end{array}$$

By construction μ extends to the linear morphism $\mu' : \mathbb{A}^{g(g+1)/2} \to \mathbb{A}^{g(g+1)/2}$ defined by $\mu'(P_{ij}(\Lambda)) = \overline{x}_{ij}$ for $1 \leqslant i \leqslant j \leqslant g$. □

Corollary 3.6. *Let $(\overline{x}_{ij})_{1\leqslant i\leqslant j\leqslant g} \in T_0^c(K_A)(\overline{k})$ be a compatible basis of $T_0^c(K_A)$. Then $(\overline{x}_{ij})$ is a basis of the vector space $T_0(K_A)(\overline{k})$. Moreover there exists a unique isomorphism $\lambda : Q^g \to T_0^c(K_A)$ which extends to the linear morphism $\lambda' : \mathbb{A}^{g(g+1)/2} \to T_0(K_A)$ such that $\lambda'(P_{ij}(\Lambda)) = \overline{x}_{ij}$ for $1 \leqslant i \leqslant j \leqslant g$ and $\Lambda \in \overline{k}^g$.*

Proof. This is an immediate consequence of Proposition 3.5 and Proposition 2.4. □

Corollary 3.7. *Once we have chosen γ in Diagram (12), there is a unique $\lambda_0 : Q^g \to T_0^c(K_A)$ which makes the diagram commutative.*

Proof. Let $(x_i)_{i=1,\dots,g}$ be a basis of $T_0(A)(\overline{k})$. Then $(\gamma(x_i))_{i=1,\dots,g}$ is a basis of $\mathbb{A}^g(\overline{k})$. Using Proposition 3.3, we define a compatible basis $(\overline{x}_{ij})_{1\leqslant i\leqslant j\leqslant g} \in T_0^c(K_A)(\overline{k})$ (resp. $(\widetilde{P}_{ij})_{1\leqslant i\leqslant j\leqslant g} \in Q^g(\overline{k})$) from $(x_i)_{i=1,\dots,g}$ (resp. from $(\gamma(x_i))_{i=1,\dots,g}$). By Corollary 3.6 there is a unique $\lambda_0 : Q^g \to T_0^c(K_A)$ such that $\lambda_0(\widetilde{P}_{ij}) = \overline{x}_{ij}$ for $1 \leqslant i \leqslant j \leqslant g$. It is clear that this λ_0 makes the Diagram (12) commutative. □

We can use the notion of compatible basis to efficiently compute an isomorphism $\lambda : Q^g \to T_0^c(K_A)$ given by Proposition 2.4. We remark that from the knowledge of an isomorphism $\lambda : Q^g \to T_0^c(K_A)$, one can easily recover g points of $T_0^c(K_A)$. Actually, fix an isomorphism $Q^g = \mathrm{Spec}(\frac{k[u_{ij}|i,j\in\{1,\dots,g\},i\leqslant j]}{(u_{ij}u_{kl}-u_{ik}u_{jl})})$, the family of points $(P_i)_{i=1,\dots,g}$ such that $u_{jj}(P_i) = \delta_{ij}$ and $u_{jl}(P_i) = 0$ for $j \neq l$ are obviously in Q^g. We are going to show that, under some general computational hypothesis about K_A, reciprocally, if one is given g points of $T_0^c(K_A)$ in general position, there is an efficient algorithm to compute an isomorphism $\lambda : Q^g \to T_0^c(K_A)$.

We make the following algorithmic hypothesis:

Hypothesis 3.8. *There exists efficient algorithms to perform differential additions, normal additions and three-way additions with the representation of $K_A(\overline{k})$. By efficient algorithm, we mean algorithm with a running time at most quadratic in the size of the representation of an element of $K_A(\overline{k})$.*

This hypothesis is verified in the case that K_A is represented by level 2 theta functions [LR16]. But it should apply in general with any efficient representation of Kummer varieties. We explain that the arithmetic of $K_A(\overline{k})$ compatible with the projection $\pi_A : A \to K_A$ extends to an arithmetic of $T_0^c(K_A)(\overline{k})$ compatible with the projection $\pi_0 : T_0(A) \to T_0^c(K_A)$. Recall from proof of Proposition 2.15 that if $S_\varepsilon = \mathrm{Spec}(\overline{k}[\varepsilon]/\varepsilon^2])$ then $T_0(K_A)(\overline{k})$ is by definition the set of morphisms $S_\varepsilon \to K_A$ such that $\mathrm{Spec}(\overline{k}) \to S_\varepsilon \to K_A$ is the 0-point morphism. The arithmetic of K_A (normal addition, differential addition, three-way addition) acts on $K_A(S_\varepsilon)$ and thus on $T_0(K_A)(\overline{k})$ and it is clear that it respects the tangent cone inside $\mathbb{A}(T_0^*(K_A))$. For instance, if $\overline{x}, \overline{y}, \overline{x-y} \in T_0^c(K_A)(\overline{k})$ then $\mathrm{DiffAdd}(\overline{x}, \overline{y}, \overline{x-y}) \in T_0^c(K_A)(\overline{k})$. The functoriality of S_ε-points shows that everything is compatible with $\pi_A : A \to K_A$. From this discussion, we conclude that under Hypothesis 3.8, we have efficient algorithms to compute the arithmetic laws of $T_0^c(K_A)$.

We thus have a reduction of the computation of λ to the problem of finding g general points of $T_0^c(K_A)$. We keep the hypothesis of Proposition 2.15 then Algorithm 1 gives a coordinate system $(x'_1, \ldots, x'_{g(g+1)/2})$ for $T_0^*(K_A)$ as well as a set of degree 2 generators G_{I_2} for an ideal I_2 such that $T_0^c(K_A)$ is the closed sub-variety of $T_0(K_A) = \mathrm{Spec}(k[x'_1, \ldots, x'_{g(g+1)/2}])$ defined by the ideal I_2.

By Proposition 2.8, $T_0^c(A)$ is birationally equivalent to $\mathbb{A}^g$. Up to a random linear change of coordinate, we can suppose that $x'_1, \ldots, x'_g$ are algebraically independent and we have a birational isomorphism $T_0^c(A) \simeq \mathrm{Spec}(k[x'_1, \ldots, x'_g])$. We can choose a k-point P of $T_0^c(A)$ by setting $x'_i(P) = P_i \in k$. We specialize each element $w \in G_{I_2}$ by setting $x_i = x_i(P)$ for $i = 1, \ldots, g$. Then, as presented in Algorithm 2, we can recover the $x'_i(P)$ for $i > g$ at the expense of a Gaussian elimination in a matrix with $g(g+1)/2$ columns and $O(g^4)$ lines. This can be done in $O(g^8)$ operations.

Proposition 3.9. *The Algorithm 2 computes g general elements of $T_0^c(K_A)(k)$ in time $O(g^9)$ operations on the base field.*

Heuristically, taking a submatrix with $g(g+1)/2 + O(1)$ lines will have the same rank, so in practice the computation will be in $O(g^7)$.

Algorithm 2: Algorithm to chose a random elements in $T_0^c(K_A)(k)$.

input : G_{I_2} generators for the ideals I_2 defining $T_0^c(K_A)$ as a closed sub-variety of $\mathbb{A}^{g(g+1)/2} = \mathrm{Spec}(k[x'_1, \ldots, x'_{g(g+1)/2}])$.

output : $\overline{x} \in T_0^c(K_A)(k)$ a random element;

Choose at random $x'_i(\overline{x})$ in k for $i = 1, \ldots, g$;
for $w \in G_{I_2}$ **do**
  $w' \leftarrow w(x'_1(\overline{x}), \ldots, x'_g(\overline{x}), \ldots, x'_{g(g+1)/2})$;/* we specialize the variables $x'_1, \ldots, x'_g$ in $\overline{x}$ */
  Write $w' = \sum \mu_i M_i$ where M_i are monomials ordered following a monomial order ;
  Add the row vector $[\mu_i]$ is the matrix M whose columns are indexed by the M_i and μ_i is in the column corresponding to M_i ;
end
Let M_0 be the row-echelon form of M ;
The rows of M_0 corresponding to degree 1 monomials gives us $x'_i(\overline{x})$ for $i > g$;
return $\overline{x}$

We suppose that A is defined over k so that there exists an isomorphism $\gamma : T_0(A)) \to \mathbb{A}^g$ defined over k and the associated λ_0 via Diagramm (12) is also defined over k. We would like to be able to find efficiently a $\lambda : Q^g \to T_0^c(K_A)$ such as λ_0 which is defined over k. With Algorithm 2, we know how to find general elements $\overline{x}_1, \ldots, \overline{x}_g \in T_0^c(K_A)(k)$. Let $(\overline{x}_{ij})_{1 \leqslant i \leqslant j \leqslant g}$ be a compatible basis associated to $\overline{x}_1, \ldots, \overline{x}_g$ following Definition 3.1. If the $(\overline{x}_{ij})$ are points defined over k then it is clear that the morphism $\lambda : Q^g \to T_0^c(K_A)$ given by Corollary 3.6 (with $\Lambda = (1, \ldots, 1)$) is also defined over k. Unfortunately, in general $(\overline{x}_{ij})$ are not defined over k because each element of $\mathrm{NormAdd}(\overline{x}_1, \overline{x}_j)$ for $j = 2, \ldots, g$ is not in general defined over k but over a degree 2 extension of it. Still the following Proposition shows that it is

possible to ensure, by choosing carefully $\Lambda \in \overline{k}^g$ that $\lambda : Q^g \to T_0^c(K_A)$ associated by Corollary 3.6 to the compatible basis $(\overline{x}_{ij})$ and the Λ-standard compatible basis $(P_{ij}(\Lambda))$ (see Definition 3.1) is defined over k.

Proposition 3.10. *Let $\overline{x}_1^0, \dots, \overline{x}_g^0$ be g elements of $T_0^c(K_A)(k)$ is general position (see Definition 3.1), let $(\overline{x}_{ij}^0)_{1\leqslant i\leqslant j\leqslant g}$ be an associated compatible basis following Definition 3.1. For $1 \leqslant i \leqslant j \leqslant g$, denote by $k[\overline{x}_{ij}^0]$ the field of definition of $\overline{x}_{ij}^0$ which is either k or a degree 2 extension of it by Lemma 3.4. For $j = 2, \dots, g$, let $\lambda_j \in k[\overline{x}_{1j}^0]$ be 1 if $k[\overline{x}_{1j}^0] = k$ or such that $k[\lambda_j] = k[\overline{x}_{1j}^0]$ if $k[\overline{x}_{1j}^0] \neq k$. Let $\Lambda = (1, \lambda_2, \dots, \lambda_g)$, then the morphism $\lambda : Q^g \to T_0^c(K_A)$ associated by Corollary 3.6 to the Λ-standard compatible basis $(P_{ij}(\Lambda))$ and the compatible basis $(\overline{x}_{ij}^0)$ is defined over k.*

Proof. Let λ' be the unique linear morphism $\lambda' : \mathbb{A}^{g(g+1)/2} \to T_0(K_A)$ such that $\lambda'(P_{ij}(\Lambda)) = \overline{x}_{ij}^0$ for $1 \leqslant i \leqslant j \leqslant g$ as in Corollary 3.6. Note that for $2 \leqslant j \leqslant g$ there exists $P_{1j}^1(\Lambda) \in \mathbb{A}^{g(g+1)/2}(\overline{k})$ such that $\{P_{1j}^0(\Lambda), P_{1j}^1(\Lambda)\} = \mathrm{NormAdd}(P_{11}(\Lambda), P_{jj}(\Lambda))$ where we have set $P_{ij}^0(\Lambda) = P_{ij}(\Lambda)$ for all $1 \leqslant i \leqslant j \leqslant g$. In the same manner, there exists $\overline{x}_{1j}^1 \in \mathbb{A}(T_0^*(K_A))(\overline{k})$ such that $\{\overline{x}_{1j}^0, \overline{x}_{1j}^1\} = \mathrm{NormAdd}(\overline{x}_{11}, \overline{x}_{jj})$.

As λ' respects the quotient structure of Q^g and $T_0^c(K_A)$ respectively, $\lambda'(P_{1j}^1(\Lambda)) \in \mathrm{NormAdd}(\overline{x}_{11}, \overline{x}_{jj})$ and because λ' is injective we deduce that

$$\lambda'(P_{1j}^1(\Lambda)) = \overline{x}_{1j}^1 \tag{15}$$

Let k' be the field of definition of all the points in $(\overline{x}_{ij}^0)_{1\leqslant i\leqslant j\leqslant g}$. Then by Lemma 3.4, $k' = k(\lambda_2, \dots, \lambda_g)$ is the compositum of the fields $k[\overline{x}_{1j}^0]$ for $2 \leqslant j \leqslant g$. More precisely, there exists a smallest integer r and a map $\xi : \{1, \dots, r\} \to \{1, \dots, g\}$ such that $k' = k(\lambda_{\xi(1)}, \dots, \lambda_{\xi(r)})$. Then k' a finite Galois extension of k and $\mathrm{Gal}(k'/k)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$. Via this isomorphism, we can describe the action of $g \in (\mathbb{Z}/2\mathbb{Z})^r$ on k'. For this we denote by $g[j] \in \mathbb{Z}/2\mathbb{Z}$ the j^{th}-component of g and we have:

$$g(\lambda_{\xi(j)}) = (-1)^{g[j]}\lambda_{\xi(j)}. \tag{16}$$

Then it is clear that for $g \in \mathrm{Gal}(k'/k) = (\mathbb{Z}/2\mathbb{Z})^r$, g is uniquely determined by its action on $P_{1\xi(j)}^0$ (resp. $\overline{x}_{1\xi(j)}^0$) for $j = 1, \dots, r$ and we have:

$$g(P_{1\xi(j)}^0) = P_{1\xi(j)}^{g[j]} \text{ and } g(\overline{x}_{1\xi(j)}^0) = \overline{x}_{1\xi(j)}^{g[j]}. \tag{17}$$

From this and Equation (15), we deduce that for all $g \in \mathrm{Gal}(k'/k)$ and $2 \leqslant j \leqslant g$, $\lambda'(g(P_{1j}^0(\Lambda)) = g(\overline{x}_{1j}^0)$. Using the fact that $(\overline{x}_{ij}^0)$ can be computed from the knowledge of $\overline{x}_{jj}^0$ for $j = 1, \dots, g$ and $\overline{x}_{1j}^0$ for $j = 2, \dots, g$ using ThreeWayAdd which is defined over k, we obtain that for all $1 \leqslant i \leqslant j \leqslant g$:

$$\lambda'(g(P_{ij}(\Lambda)) = g(\overline{x}_{ij}^0). \tag{18}$$

so that λ' is defined over k. □

From Corollary 3.6, we deduce Algorithm 3 to compute an isomorphism $\lambda : Q^g \to T_0^c(K_A)$ from the knowledge of g points of $T_0^c(K_A)(k)$. Moreover, Proposition 3.10 tells that if A is defined over k the matrix M returned by Algorithm 3 has coefficients in k. From our algorithmic hypothesis, the arithmetic operations require in $O(g^2)$ elementary operations in k, so the complexity is dominated by the linear algebra and is in $O(g^6)$.

Proposition 3.11. *The complexity of Algorithm 3 to comptute the linear isomorphism $\lambda : Q^g \to T_0^c(K_A)$ is in $O(g^6)$.*

There is a still a missing piece in the description of our approach. It is due to the fact that we don't want to lift our computation to A since it would be too expansive from a computational point of view. Thus the morphism γ of Diagram (12), although we know it exists, is not given to us explicitly nor is the isomorphism $\lambda_0 : Q^g \to T_0^c(K_A)$ associated to γ via Diagram (12) and Corollary 3.7. The only thing that we are going to be able to compute is an isomorphism $\lambda : Q^g \to T_0^c(K_A)$ that we cannot explicitly relate to γ. Denote by $\mu : Q^g \to Q^g$ an automorphism such that $\lambda = \lambda_0 \circ \mu$. The situation is summarised in Diagram (20).

Algorithm 3: Algorithm to compute an isomorphism $\lambda : Q^g \to T_0^c(K_A)$.

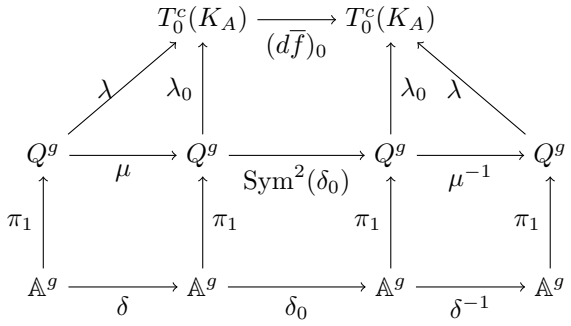
input : The elements $\overline{x}_{11}, \dots, \overline{x}_{gg} \in T_0^c(K_A)(k)$ with A an Abelian variety defined over the field k;
output : A matrix M representing the linear isomorphism $\lambda : Q^g \to T_0^c(K_A)$.

for $j \leftarrow 2$ **to** g **do**
  $\{\alpha_0, \alpha_1\} \leftarrow \mathrm{NormAdd}(\overline{x}_{11}, \overline{x}_{jj})$;
  $\overline{x}_{1j} \leftarrow \alpha_0$;
  Let $\lambda_i \in k[\alpha_0]$ the field of definition of α_0 be such that $k[\lambda_i] = k[\alpha_0]$;
end
for $i, j \leftarrow 2$ **to** g, $i \leqslant j$ **do**
  $\overline{x}_{ij} \leftarrow \mathrm{ThreeWayAdd}(\overline{x}_{11}, \overline{x}_{ii}, \overline{x}_{jj}, \overline{x}_{1i}, \overline{x}_{1j})$;
end
Let $\Lambda = (\lambda_1, \dots, \lambda_g)$;
Let $(P_{ij}(\Lambda))$ be the Λ-standard compatible basis of Q^g (see Example 3.2);
Compute the unique matrix $M \in \mathrm{GL}(k, g(g+1)/2)$ such that $MP_{ij}(\Lambda) = \overline{x}_{ij}$ in $T_0(K_A)(\overline{k})$;
return M.

We suppose that we know how to compute $(d\overline{f})_0$ and we want to obtain the conjugacy class of $\pm\delta_0$. By looking at Diagram (20), we see that

$$\lambda^{-1} \circ (d\overline{f})_0 \circ \lambda = \mu^{-1} \circ \mathrm{Sym}^2(\delta_0) \circ \mu. \tag{19}$$

But, by the surjectivity of τ in Theorem 2.12, there exists $\delta \in \mathrm{Aut}(\mathbb{A}^g)$ such that $\mu = \mathrm{Sym}^2(\delta)$. So $\mu^{-1} \circ \mathrm{Sym}^2(\delta_0) \circ \mu = \mathrm{Sym}^2(\delta^{-1} \circ \delta_0 \circ \delta)$ from which we obtain $\pm\delta^{-1} \circ \delta_0 \circ \delta$ which is exactly the conjugacy class of δ_0 up to a sign.



(20)

Putting all together the results of this section, we obtain Algorithm 4 to compute a matrix representing the conjugate class of $\rho(f)$ up to a sign from the knowledge of $\overline{f} \in \mathrm{End}(K_A)$.

We just have to explain how to compute $(d\overline{f})_0$ in this algorithm. If we identify $\mathbb{A}^m = \mathrm{Spec}(k[x_1, \dots, x_m])$, up to a linear change of coordinates, we can suppose that $(x_1, \dots, x_{g(g+1)/2})$ is a coordinate system of K_A in 0 (that is the class of functions $x_i - x_i(0) \in \mathscr{O}_{K_A,0}$ generate $T_0^*(K_A)$). For $j = 1, \dots, g(g+1)/2$, we define the points $P_{\varepsilon_j} \in K_A(k[\varepsilon]/\varepsilon^2)$ by setting $x_i(P_{\varepsilon_j}) = x_i(0) + \varepsilon$ if $i = j$ and $x_i(0)$ otherwise. These points form a basis of $T_0(K_A)(k)$ as a k-vector space.

Suppose that $\overline{f} \in \mathrm{End}(K_A)$ is given by functions $(f_i)_{i=1,\dots,m}$ defined in a neighbourhood of $0 \in K_A(k)$ such that for all $P \in K_A(\overline{k})$,

$$x_i(P) = f_i(x_1(P), \dots, x_m(P)).$$

Definition 3.12. For $i = 1, \dots, m$, we call the computation size of f_i and denote it by $S(f_i)$ the minimal number operation in a k-algebra $\mathscr{A}$ to evaluate $f_i(x_1, \dots, x_m)$ for $x_1, \dots, x_m \in \mathscr{A}$. The size of $(f_i)_{i=1,\dots,m}$ that we denote by $S((f_i))$ is $\sum_i S(f_i)$.

We write:

$$\lambda_i + \mu_{ij}\varepsilon = f_i(x_1(P_{\varepsilon_j}), \dots, x_m(P_{\varepsilon_j})), \tag{21}$$

for $\lambda_i \in k$. Then the matrix $(\mu_{ij}) \in \mathrm{GL}(k, g(g+1)/2)$ is the matrix of $(d\overline{f})_0$ in the coordinate system of $T_0^*(K_A)$ given by the (P_{ε_j}).

Proposition 3.13. *Let $\overline{f} \in \mathrm{End}(K_A)$ be given by functions $(f_i)_{i=1,\dots,m}$ defined in a neighbourhood of $0 \in K_A(k)$ such that for all $P \in K_A(\overline{k})$,*

$$x_i(P) = f_i(x_1(P), \dots, x_m(P)).$$

There exists an algorithm the complixity of which is $O(S((f_i)))$ to compute a matrix $(\mu_{ij}) \in \mathrm{GL}(k, g(g+1)/2)$ representing $(d\overline{f})_0$.

We now can use Algorithm 4 to recover the similitude class of $\pm df_0$. Gathering the complexity analysis of Proposition 2.18, Proposition 3.9, Proposition 3.11 and Proposition 3.13, we deduce:

Proposition 3.14. *The complexity of Algorithm 4 to compute the linear representation of $\mathrm{End}(K_A)$ is $O(\max(g^9, \ell m^2 g^4, S((f_i))))$ base field operations (heuristically $O(\max(g^7, \ell m^2 g^4, S((f_i))))$ base field operations).*

Algorithm 4: Algorithm to compute the linear representation of $\mathrm{End}(K_A)$.

input :

- Let K_A be a dimension g Kummer variety given by:
$$(h_i)_{i=1,\dots,\ell}, h_i \in k[x_1, \dots, x_m]$$
equations for K_A in a neighbourhood of $0 \in K_A(k)$;
- $f \in \mathrm{End}(K_A)$, given by functions $(f_i)_{i=1,\dots,m}$ such that for all $P \in K_A(\overline{k})$,
$$x_i(P) = f_i(x_1(P), \dots, x_m(P)).$$

output : A matrix $M \in \mathrm{GL}(k, g)$ a matrix representing the conjugation class of $\overline{\rho}(\overline{f})$.

1 Call Algorithm 1 to compute a coordinate system $(x'_1, \dots, x'_{g(g+1)/2})$ for $T_0^*(K_A)$ as well as G_{I_2} generators for the ideal I_2 such that $T_0^c(K_A)$ is isomorphic to $\mathrm{Spec}(k[x'_1, \dots, x'_{g(g+1)/2}]/I_2)$;
2 Call g times Algorithm 2 to obtain g elements $\overline{x}_1, \dots, \overline{x}_g \in T_0^c(K_A)(k)$;
3 Call Algorithm 3 to compute a Matrix $M_\lambda \in \mathrm{GL}(\overline{k}, g(g+1)/2)$ representing $\lambda : Q^g \to T_0^c(K_A)$;
4 Compute the matrix $M_{(d\overline{f})_0} = (\mu_{ij})$ where μ_{ij} is defined by Equation 21;
5 $M_{\mathrm{Sym}} \leftarrow M_\lambda^{-1}.M_{(d\overline{f})_0}.M_\lambda$;
6 Compute $M \in \mathrm{GL}(k, g)$ such that $M_{\mathrm{Sym}} = \mathrm{Sym}(M)$;
7 **return** M;

4. Applications to point counting algorithms in small characteristic

Strictly speaking, a point counting algorithm is an algorithm that takes as input a genus g curve $\overline{X}$ (resp. a dimension g Abelian variety $\overline{A}$) defined over a finite field $\mathbb{F}_q$ and outputs the cardinality of $\overline{X}(\mathbb{F}_q)$ (resp. $\overline{A}(\mathbb{F}_q)$). Most of the time, one expects that a point counting algorithm returns a slightly more general information which is $L(\overline{X}, t)$, the L-function of $\overline{X}$ that encodes the cardinality of $\overline{X}(k)$ for any k finite extension of $\mathbb{F}_q$.

The efficiency of a point counting algorithm is measured by its worst case running time as a function of the size of the input. Designing efficient point counting algorithms has applications in cryptography [CFA+06]. All known efficient point counting algorithms can be interpreted as the computation of the action of the Frobenius morphism on some Weil cohomology group $H_W^*(\overline{X})$. Actually, let $\chi_p(\overline{X}, t)$ be

the characteristic polynomial of the Frobenius morphism acting on $H^1_W(\overline{X})$ then the L-function of $\overline{X}$ is given by :

$$L(\overline{X},t)=\frac{t^g\chi_p(\overline{X},1/t)}{(1-t)(1-qt)}.$$

Note that if $\overline{A}$ is the jacobian of $\overline{X}$ then the cardinality of $\overline{A}(\mathbb{F}_q)$ is given by the residue in 1 of $L(\overline{X},t)$ that is $\chi_p(1)$.

One can distinguish several families of point counting algorithms with different algorithmic behavior according to what cohomological theory they are based on. Mestre's point counting algorithm belongs to the p-adic point counting algorithm family which has been introduced by a paper of Satoh [Sat00].

4.1. **Limitations of canonical lifts algorithms.** We briefly recall the principles of Mestre's algorithm which is a variation of Satoh's algorithm [Mes01; Mes02b] to explain our improvement. Let $\overline{X}$ be a genus g ordinary curve over $\mathbb{F}_q$ with $q=p^m$ and let $\overline{A}=J(\overline{X})$ be its jacobian variety which is a dimension g Abelian variety. Let $\mathbb{Z}_q$ be the degree m unramified extension of $\mathbb{Z}_p$. A lift of $\overline{A}$ over $\mathbb{Z}_q$ is an Abelian scheme over $\mathbb{Z}_q$ which reduces to $\overline{A}$ over $\mathbb{F}_q$. Among all the possible lifts of $\overline{A}$, there is only one up to isomorphism, that we denote by A, such that the reduction morphism induces an isomorphism $\mathrm{End}(A)\simeq\mathrm{End}(\overline{A})$. In particular, the q^{th}-Frobenius endomorphism of $\overline{A}$ lifts to an endomorphism of A that we denote by Σ. Its contragredient morphism is the q^{th}-Verschiebung V. Let $\chi_1(X,t)$ be the characteristic polynomial of the q^{th}-Verschiebung acting on the space $H^0(A,\Omega)$ of global differential forms of A. As $\overline{X}$ is ordinary, there are g Eigenvalues $\pi_1,\ldots,\pi_g$ of the q^{th}-Frobenius morphism acting on $H^1_W(\overline{X})$ which are units modulo p [Del69]. Then the roots of $\chi_1(\overline{X},t)$ are $\pi_1,\ldots,\pi_g$ so that $\chi_p(\overline{X},t)=t^g\chi_1(\overline{X},q/t)\chi_1(\overline{X},t)$. The computation of the action of V on $H^0(A,\Omega)$ is difficult because, when q is big, V is a high degree isogeny. Using a classical trick [Ked01], we can replace it by the computation of the action of the of the p^{th}-Verschiebung and then take the norm of the resulting matrix. The p-adic precision of the computations is chosen big enough according to Weil conjectures to be able to recover $\chi_p(\overline{X},t)$. To sum up, Mestre and Satoh's algorithms can be decomposed in two main steps:

- The computation of the canonical lift A of the jacobian of $\overline{X}$;
- The computation of the action of the p^{th}-Verschiebung morphism acting on the global differential forms of A.

We detail this second step, because this is where our improvement lies. In order to fix the notations, we need a more precise description of canonical lift algorithms. They take as input an ordinary projective algebraic curve $\overline{X}$ of genus g (resp. the theta null point of a dimension g Abelian variety $\overline{A}$) over $\mathbb{F}_q$ where $q=p^m$ and returns $\chi_p(\overline{X},t)$ the characteristic polynomial of the Frobenius morphism. Denote by $\overline{\sigma}:\mathbb{F}_q\to\mathbb{F}_q$, $x\mapsto x^p$ the p^{th}-Frobenius morphism. Let $\overline{A}=\overline{A}_0$ be the jacobian of $\overline{X}$.

For $i=0,\ldots,m$, let $\overline{A}_i=\overline{A}\times_{\mathbb{F}_q}\overline{\sigma}^i(\mathbb{F}_q)$. Note that $\overline{A}=\overline{A}_0=\overline{A}_m$. Denote by $\overline{\sigma}_i:\overline{A}_i\to\overline{A}_{i+1}$ the p^{th}-Frobenius morphism and by $\overline{V}_i:\overline{A}_{i+1}\to\overline{A}_i$ the p^{th}-Verschiebung morphism: by definition $\overline{V}_i$ is the contragredient morphism of σ_i that is we have $\overline{V}_i\circ\overline{\sigma}_i=p$. We let $\overline{\Sigma}=\overline{\sigma}_{m-1}\circ\ldots\circ\overline{\sigma}_0\in\mathrm{End}(\overline{A}_0)$ be the q^{th}-Frobenius endomorphism of A_0 and $\overline{V}\in\mathrm{End}(A_0)$ be the contragredient endomorphism of $\overline{\sigma}$. Let A be a canonical lift of $\overline{A}$. For $i=0,\ldots,m$, let $A_i=A\times_{\mathbb{Z}_q}\sigma^i(\mathbb{Z}_q)$, we remark that A_i is a canonical lift of $\overline{A}_i$. For $i=0,\ldots,m$, denote by $\sigma_i:A_i\to A_{i+1}$ (resp. $V_i:A_{i+1}\to A_i$) a lift of $\overline{\sigma}_i$ (resp. of $\overline{V}_i$) and let $\Sigma=\sigma_{m-1}\circ\ldots\circ\sigma_0\in\mathrm{End}(A_0)$ be a lift of $\overline{\Sigma}$. Denote by $V\in\mathrm{End}(A_0)$ the contragredient morphism of Σ, so that we have $V\circ\Sigma=q$. We also let $\sigma:\mathbb{Z}_q\to\mathbb{Z}_q$ be the Frobenius morphism of $\mathbb{Z}_q$ which is the unique automorphism of $\mathbb{Z}_q$ which reduces to $\overline{\sigma}$ modulo p. We have the following diagram where the vertical arrows are reduction mod p:

$$\begin{array}{ccccccc}
A_0 & \underset{V_0}{\overset{\sigma_0}{\rightleftarrows}} & A_1 & \ldots & A_i & \underset{V_i}{\overset{\sigma_i}{\rightleftarrows}} & A_{i+1} \quad \ldots \quad A_{m-1} \underset{V_{m-1}}{\overset{\sigma_{m-1}}{\rightleftarrows}} A_m = A_0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \qquad\qquad\quad \downarrow \qquad\quad \downarrow \\
\overline{A}_0 & \underset{\overline{V}_0}{\overset{\overline{\sigma}_0}{\rightleftarrows}} & \overline{A}_1 & \ldots & \overline{A}_i & \underset{\overline{V}_i}{\overset{\overline{\sigma}_i}{\rightleftarrows}} & \overline{A}_{i+1} \quad \ldots \quad \overline{A}_{m-1} \underset{\overline{V}_{m-1}}{\overset{\overline{\sigma}_{m-1}}{\rightleftarrows}} \overline{A}_m = \overline{A}_0
\end{array}$$

Let $w_{A_0} = (w_1^0, \dots, w_g^0)$ be a basis of $T_0^*(A_0)$ as a $\mathbb{Q}_q$ vector space. Let σ be the unique automorphism of $\mathbb{Q}_q$ which reduce to $\overline{\sigma}$ modulo p, we can transport w_{A_0} by acting on its field of definition by σ. For this, for $i = 1, \dots, r-1$, let $w_{A_0}^{\sigma^i} = w_{A_0} \times_{\sigma^i} \mathbb{Q}_q$ be a basis of $T_0^*(A_0 \times_{\sigma^i} \mathbb{Q}_q)$. Remark that $A_0 \times_{\sigma^i} Q_q$ is isomorphic to A_i so that $w_{A_0}^{\sigma^i}$ defines a basis w_{A_i} of $T_0^*(A_i)$. Denote by M_i the matrix of $(dV_{i+1})_0^* : T_0^*(A_{i+1}) \to T_0^*(A_i)$ expressed in the basis $w_{A_{i+1}}$ and w_{A_i}. It is easy to see that for $i = 1, \dots, r-1$, $M_i = M_0^{\sigma^i}$ and that $\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(M_0)$ is the matrix of the Frobenius morphism acting on $T_0^*(A_0)$.

If $\mathfrak{g}$ is a scalar modular form of weight ρ, the algebraic interpretation of $\mathfrak{g}$ (in the sense of Katz) shows that $\mathfrak{g}(A_i^\sigma, w_{A_i}^\sigma) = \det^\rho(M_i)\mathfrak{g}(A_{i+1}, w_{A_{i+1}})$. The quotient of these two modular forms allows us to recover $\det^\rho(M_i)$ and then $\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(\det(M_0)) = \prod_{i=1}^g \lambda_i^\rho$ where λ_i are the invertible eigenvalues of the Frobenius.

For instance, Mestre's algorithmuse theta coordinates to represent Abelian varieties over $\mathbb{Q}_q$. In particular, for the second step, it relies on the transformation formula of theta functions [BL04] to build a scalar modular form of weight $\rho = 1$ and thus to recover the product $\pi_1 \dots \pi_g$. This is one of the main limitations of the higher genus version of Mestre's algorithm: it does not recover each of the $\pi_1, \dots, \pi_g$. Mestre has proposed in [Mes02b] an algorithm to recover $\pi_1, \dots, \pi_g$ from the knowledge of the product $\pi_1 \dots \pi_g$. This algorithm consists in computing a degree $2^g - 1$ symmetric polynomial P_{sym} with coefficients in $\mathbb{Z}$, a roots of which is $\pi_1 \dots \pi_g$ using LLL algorithm. From the knowledge of this polynomial it is then easy to recover $\pi_1, \dots, \pi_g$. The complexity of this algorithm is $\widetilde{O}(m^4\beta)$ where $m = O(2^g)$ is the dimension of the lattice and β the precision used by [NS16]. Indeed in order to use the LLL algorithm, it is necessary to increase the p-adic precision of the computation far beyond what it prescribed by the Weil conjectures [LL06, § 5.4]. Moreover starting from genus 4, Mestre has shown in [Mes02b] that, in general, the product $\pi_1 \dots \pi_g$ does not characterize the isogeny class of $J(\overline{X})$ so that there is no way to recover the individual $\pi_1, \dots, \pi_g$ from it. The improvement that we propose is more efficient and easier to implement. For instance it does not rely on an efficient implementation of the LLL algorithm which is tricky and needs a quick floating point arithmetic. Moreover, it always allows to recover the characteristic polynomial of the Frobenius morphism even if $g \geqslant 4$.

4.2. **The improvement.** As explained in the introduction, our improvement in the second step of the algorithm is that whenever we have the equations of the isogeny induced by the lift of the small Verschiebung V_0, we can compute its action on the basis of differentials w_{A_0}, $\sigma^{-1}w_{A_0}$ to recover the matrix M_{m-1} (up to conjugation). Taking the norm then gives the action M of V on w_{A_0}.

We detail this step for Mestre's algorithm which uses theta function, but a similar method would work for other models. The original version of Mestre's algorithm is for curves defined over a characteristic 2 field. It has been generalized for field of any (small) characteristic [CKL06; CL08] and improved from an algorithmic point of view in [LL06] to achieve a complexity of $\widetilde{O}(n)$ over the field $\mathbb{F}_{p^n}$. We detail our improvement to this more general version of Mestre's algorithm.

We recall briefly, and refer the reader to [Mum66] for a more in-depth presentation of the algebraic theory of theta functions, that if $(B, \mathscr{L}_B)$ is a dimension g Abelian variety together with a principal polarization then for $\ell \geqslant 2$ an integer, a level ℓ theta structure for $(B, \mathscr{L}^\ell)$, that we denote by Θ_B^ℓ in the following, determines a basis $(\theta_i^{\Theta_B^\ell})_{i \in (\mathbb{Z}/\ell\mathbb{Z})^g}$ of $H^0(B, \mathscr{L}_B^\ell)$. For all ℓ positive integer, we let $Z(\bar{\ell}) = (\mathbb{Z}/\ell\mathbb{Z})^g$ and in order to ease the notations we write $(\theta_i)_{i \in Z(\bar{\ell})}$ instead of $(\theta_i^{\Theta_B^\ell})_{i \in Z(\bar{\ell})}$ when no confusion is possible. We will also have to evaluate these sections only in the case that the base field of B is a characteristic 0 field k_0. In this case, by embedding k_0 into $\mathbb{C}$, following [Mum83], we can identify $(\theta_i^{\Theta_B^\ell})_{i \in Z(\bar{\ell})}$ with the theta functions $(\theta \left[\begin{smallmatrix} 0 \\ i/\ell \end{smallmatrix}\right](z, \Omega/\ell))_{i \in Z(\bar{\ell})}$. Here Ω is a representative of a class of $\mathbb{H}_g/\Gamma(\ell, 2\ell)$ where $\mathbb{H}_g$ is the dimension g the Siegel upper half space and $\Gamma(\ell, 2\ell)$ is a Igusa subgroup of the symplectic group acting on $\mathbb{H}_g$ [Rit03]. This allows us to consider the sections $\theta_i^{\Theta_B^\ell}$ as functions on $\mathbb{C}^g$ by taking care of the fact that this imply that we have chosen an embedding of k_0 into $\mathbb{C}$ and a particular Ω in a conjugation class. Let $\Lambda_\Omega = \mathbb{Z}^g + \Omega\mathbb{Z}^g$ and let $A_{\Lambda_\Omega} = \mathbb{C}^g/\Lambda_\Omega$ then A is an Abelian variety analytically isomorphic to B over $\mathbb{C}$.

The projective point with homogeneous coordinates $(\theta_i^{\Theta_B^\ell}(0))_{i\in(\mathbb{Z}/\ell\mathbb{Z})^g}$ is the theta null point associated to $(B, \mathscr{L}_B^\ell, \Theta_B^\ell)$. Its data is equivalent to the data of $(B, \mathscr{L}_B^\ell, \Theta_B^\ell)$: in particular they have the same field of definition. With these settings, we can give a more thorough description of the improved version of Mestre's algorithm in 4 main steps:

(1) Using Thomae-Formulas (if $\overline{X}$ is a hyperelliptic curve) or a generalization for it, compute the theta null point of $(\overline{A}_0, \mathscr{L}^2_{\overline{A}_0}, \Theta^2_{\overline{A}_0})$ where $\overline{A} = \overline{A}_0$ is the jacobian of $\overline{X}$, $\mathscr{L}_{\overline{A}_0}$ a degree 1 symmetric ample line bundle on $\overline{A}_0$ and $\Theta^2_{\overline{A}_0}$ is a level 2 theta structure for $\mathscr{L}^2_{\overline{A}_0}$.
(2) Using a Newton lift with a modular equation, compute (a p-adic approximation of) the theta null point of $(A_0, \mathscr{L}^2_{A_0}, \Theta^2_{A_0})$ an Abelian scheme together with a level 2 theta structure which reduces modulo p to $(\overline{A}_0, \mathscr{L}^2_{\overline{A}_0}, \Theta^2_{\overline{A}_0})$. Here $A_0 = A$ is an Abelian scheme over $\mathbb{Z}_q$ which is a canonical lift of $\overline{A}$.
(3) Compute $\overline{K}_{m-1}$ the kernel of $\overline{V}_{m-1}$. and lift it to K_{m-1} the kernel of V_{m-1} as the only unramified lift.
(4) Compute the isogeny V_{m-1} from the kernel K_{m-1}, the matrix M_{m-1} of $(dV_{m-1})^*$ in the basis $\sigma^{-1}w_{A_0}$, w_{A_0}, and then via a norm a matrix of $(dV)_0 \in \mathrm{Aut}(T_0(A_0))$ where $T_0(A_0)$ is the co-tangent space in the 0 section of A_0.

For a comparison with Mestre's original version, where Steps (3) and (4) are replaced by the theta transformation formula, we refer the reader to [LL06].

Remark 4.1. Some remarks about this brief description of Mestre's algorithm:

- If the input of the algorithm is the theta null point of an Abelian variety with a theta structure over $\mathbb{F}_q$, $(\overline{A}, \mathscr{L}^2_{\overline{A}}, \Theta^2_{\overline{A}})$, we can skip step (1).
- In the papers [MR20; MR21] we use modular polynomials between theta constants of level 2, and then lift the kernels as indicated in the algorithm above.
- In the paper [CL08], step (2) is instead replaced by the computation of $(\overline{A}_0, \mathscr{L}^{2p}_{\overline{A}_0}, \Theta^{2p}_{\overline{A}_0})$ and then lifting it to $(A_0, \mathscr{L}^{2p}, \Theta^{2p}_{A_0})$. This can be seen as lifting both $\overline{A}_0$ and the kernel $\overline{K}_{m-1}$ simultaneously. More precisely, using the algorithms of [FLR11; LR12; CR15], we can recover $(A_0, \mathscr{L}^{2p}, \Theta^{2p}_{A_0})$ from $(A_1, \mathscr{L}^2, \Theta^2_{A_1})$ and $K_0 = \mathrm{Ker}\, V_0$ and conversely, in $O((2p)^g)$ base field operations.

  So from the theta null point of level $2p$ we can recover the kernel in level 2 and then apply [CR15] to compute the isogeny. But in fact once we are in level $2p$ we can also directly use Mumford's isogeny formula to compute the isogeny $V_{m-1} : A_0 \to A_{m-1}$. To compare the action on differentials we need to go from level $2p$ on A_0 to level 2, which can be done either by using the formula from [FLR11, § 3.2] (which descends to A_1) hence encode a p^2-isogeny, or using the descent formula from [CR15, § 4] (which descends to A_0).

A problem with step (4) is that for efficiency reason we want to work with theta functions of level 2. As all level 2 theta functions are even, they form a coordinate system for a projective embedding of the Kummer variety K_{A_0}. Hence we work over the Kummer variety rather than over A_0. In this case we cannot directly compute the tangent space T_0A_0, let alone the action of V_0 on it. We could use [LR16], to compute a level 4 theta null point for A_0 and then compute the action of V^* on $T_0(A_0)$ but we would end up with an algorithm less efficient than the original one since we would have to compute with $(4p)^g$ coordinates instead of the $(2p)^g$ coordinates of a level 2 embedding. But we have just explained in Section 3, how to recover $(dV)_0 : T_0(A_0) \to T_0(A_0)$ up to a sign from the knowledge of $(dV)_0 : T_0(K_{A_0}) \to T_0(K_{A_0})$. More precisely, we actually compute V_{m-1} then $d(V_{m-1})_0$ and recover the action of $(dV)_0$ by a norm computation. In the following, we detail the computation of V_{m-1} and how to recover the action of $(dV)_0$.

If $p > 2$, we can compute V_{m-1} with the isogeny computation algorithm [CR15]. Actually, from the preceding steps of the algorithm, we know $(\theta_i^{\Theta^2_{A_0}}(0))_{i\in Z(\overline{2})}$ and K_{m-1} the kernel of V_{m-1} which are exactly the inputs of algorithm [CR15].

If $p = 2$, the expression of $V_{m-1} : A_0 \to A_{m-1}$ is given by the duplication formula. With the convention taken for the numbering of ramification points in the computation of Thomae formula in Step (1) of the algorithm, we know by [Rit03] that there exists $\Omega \in \mathbb{H}_g$, such that $(\theta_i^{\Theta^2_{A_{m-1}}}(0))_{i\in Z(\overline{2})} = (\theta\left[\begin{smallmatrix}0\\ i/2\end{smallmatrix}\right](0,\Omega/2))_{i\in Z(\overline{2})}$ and $(\theta_i^{\Theta^2_{A_0}}(0))_{i\in Z(\overline{2})} = (\theta\left[\begin{smallmatrix}0\\ i/2\end{smallmatrix}\right](0,\Omega))_{i\in Z(\overline{2})}$. Said in a more informal way, we have the analytic isomorphisms $A_{\Lambda_\Omega} \simeq A_{m-1}$ and $A_{\Lambda_{2\Omega}} \simeq A_0$ and the isogeny $A_{\Lambda_\Omega} \to A_{\Lambda_{2\Omega}}$, $z \mapsto z$ reduces modulo p to the Frobenius morphism σ_{m-1}.

By setting $\theta_i(z) = \theta\left[\begin{smallmatrix}0\\ i/2\end{smallmatrix}\right](z,\Omega)$ and $\theta'_i(z) = \theta'\left[\begin{smallmatrix}0\\ i/2\end{smallmatrix}\right](z,\Omega/2)$ for $i \in Z(\overline{2})$, the usual duplication formula [Igu72, p. 139] gives for all $i, j \in Z(\overline{2})$, $z_1, z_2 \in \mathbb{C}^g$:

$$\theta_{i+j}(z_1+z_2)\theta_{i-j}(z_1-z_2) = \frac{1}{2^g}\sum_{\eta\in Z(\overline{2})}\theta'_{i+\eta}(z_1)\theta'_{j+\eta}(z_2). \tag{22}$$

By setting $z_1 = z_2 = 0$ in (22), for $g = 1$, we recover the usual arithmetic-geometric mean. For $\chi \in \hat{Z}(\overline{2})$, the dual group of $Z(\overline{2})$, using this formula, we compute

$$\begin{aligned}\sum_{\eta\in Z(\overline{2})}\chi(\eta)\theta_{i+j+\eta}(z_1+z_2)\theta_{i-j+\eta}(z_1-z_2) &= \frac{1}{2^g}\sum_{\eta_1,\eta_2\in Z(\overline{2})}\chi(\eta_1+\eta_2)\theta'_{i+\eta_1}(z_1)\theta'_{j+\eta_2}(z_2)\\ &= \frac{1}{2^g}\left(\sum_{\eta\in Z(\overline{2})}\chi(\eta)\theta'_{i+\eta}(z_1)\right)\left(\sum_{\eta\in Z(\overline{2})}\chi(\eta)\theta'_{j+\eta}(z_2)\right).\end{aligned} \tag{23}$$

By setting $z_2 = 0$ and $j = 0$ in (23), we obtain an expression of $V_{m-1} : A_{m-1} \to A_0$:

$$\sum_{\chi\in\hat{Z}(2)}\chi(i)\frac{\sum_{\eta\in Z(\overline{2})}\chi(\eta)\theta_{i+\eta}(z_1)^2}{\left(\sum_{\eta\in Z(\overline{2})}\chi(\eta)\theta'_\eta(0)\right)} = \theta'_i(z_1). \tag{24}$$

In order to use this expression, we only have to know the theta null points $(\theta'_i(0))_{i\in Z(\overline{2})}$. But from Step (2) of the algorithm, we know a theta null point of $(A_0, \mathscr{L}^2_{A_0}, \Theta^2_{A_0})$ which is $(\theta_i^{\Theta^2_{A_0}}(0))_{i\in Z(\overline{2})}$. This theta null point is defined over $\mathbb{Q}_q$ and we obtain a theta null point of $(A_j, \mathscr{L}^2_{A_j}, \Theta^2_{A_j})$ as $(\theta_i^{\Theta^2_{A_0}}(0))^{\sigma^j}_{i\in Z(\overline{2})}$.

We explain how to adapt Algorithm 4 for our purpose. By Proposition 2.4, there exists a morphism $\lambda_0 : Q^g \to T_0^c(K_{A_0})$, as A_0 is defined over $\mathbb{Q}_q$, by Proposition 3.10, we can compute such a λ_0 defined over $\mathbb{Q}_q$. The Algorithm 3 allows to compute such a λ_0 defined over $\mathbb{Q}_q$. We let $\lambda_i = \lambda_0^{\sigma^i} : Q^g \to T_0^c(K_{A_0})^{\sigma^i} \simeq T_0^c(K_{A_i})$ be the twist of λ_0 by σ^i.

We have the following diagram:

(25)

$$\begin{array}{ccccccc}
T_0^c(K_{A_0}) & \xleftarrow{(dV_0)_0} & T_0^c(K_{A_1}) & \dots & T_0^c(K_{A_i}) & \dots & T_0^c(K_{A_{m-1}}) \xleftarrow{(dV_{m-1})_0} T_0^c(K_{A_0}) \\
\uparrow{\scriptstyle \lambda_0} & & \uparrow{\scriptstyle \lambda_1} & & \uparrow{\scriptstyle \lambda_i} & & \uparrow{\scriptstyle \lambda_{m-1}} \quad \uparrow{\scriptstyle \lambda_0} \\
Q^g & \xleftarrow{\mathrm{Sym}^2(\delta_0)} & Q^g & \dots & Q^g & \dots & Q^g \xleftarrow{\mathrm{Sym}^2(\delta_{m-1})} Q^g \\
\uparrow{\scriptstyle \pi_1} & & \uparrow{\scriptstyle \pi_1} & & \uparrow{\scriptstyle \pi_1} & & \uparrow{\scriptstyle \pi_1} \quad \uparrow{\scriptstyle \pi_1} \\
\mathbb{A}^g & \xleftarrow{\delta_0} & \mathbb{A}^g & \dots & \mathbb{A}^g & \dots & \mathbb{A}^g \xleftarrow{\delta_{m-1}} \mathbb{A}^g
\end{array}$$

where $\pi_1 : \mathbb{A}^g \to Q^g$ are the canonical projections, $\mathrm{Sym}^2(\delta_i) : Q^g \to Q^g$ are the unique map which make the upper squares commutative. The fact that the maps $\mathrm{Sym}^2(\delta_i)$ are acutally of the form $\mathrm{Sym}^2(\delta_i)$ for $\delta_i : \mathbb{A}^g \to \mathbb{A}^g$ is a consequence of Theorem 1.2. Then the δ_i which makes the Diagram (25) commutative are defined up to a sign. We chose δ_0 and set $\delta_i = \delta_0^{\sigma^i}$. Then $\mathrm{Sym}^2(\delta_i) = \mathrm{Sym}^2(\delta_0)^{\sigma^i}$.

Algorithm 5: Algorithm to compute a representative up to a sign in the conjugacy class of the action of V on $T_0(A)$.

input :

- $(\theta_i^{\Theta^2_{A_0}}(0))_{i\in Z(\overline{2})}$ the level 2 theta null point of K_{A_0} a canonical lift over $\mathbb{Z}_q$ of $K_{\overline{A}_0}$ the Jacobian of a curve $\overline{X}$ defined over $\mathbb{F}_q$.

output : A matrix $M \in \mathrm{GL}(k, g)$ whose characteristic polynomial χ_1 verifies:

$$\chi_p(\overline{X}, t) = t^g \chi_1(q/t)\chi_1(t).$$

1 Using $(\theta_i^{\Theta^2_{A_0}}(0))_{i\in Z(\overline{2})}$ compute a complete set of equations $(h_i)_{i=1,\dots,\ell}$ verified by K_{A_0};
2 Call Algorithm 1 to compute a coordinate systems $(x'_1, \dots, x'_{g(g+1)/2})$ for $T_0^*(K_A)$ as well as G_{I_2} generators for the ideal I_2 such that $T_0^c(K_A)$ is isomorphic to $\mathrm{Spec}(k[x'_1, \dots, x'_{g(g+1)/2}]/I_2)$;
3 Call g times Algorithm 2 to obtain g elements $\overline{x}_1, \dots, \overline{x}_g \in T_0^c(K_A)(k)$;
4 Call Algorithm 3 to compute a Matrix $M_\lambda \in \mathrm{GL}(\overline{k}, g(g+1)/2)$ representing $\lambda : Q^g \to T_0^c(K_A)$;
5 Using Equation (24) compute an expression of V_{m-1};
6 Compute the matrix $M_{(dV_{m-1})_0} = (\mu_{ij})$ where μ_{ij} is defined by Equation (21);
7 $M_{\mathrm{Sym},0} \leftarrow M_\lambda . M_{(dV_{m-1})_0} . (M_\lambda^{-1})^\sigma$;
8 Compute $M_0 \in \mathrm{GL}(k, g)$ such that $M_{\mathrm{Sym},0} = \mathrm{Sym}(M_0)$;
9 Compute $M = \mathrm{N}_{\mathbb{Z}_q/\mathbb{Z}_p}(M_0)$;
10 **return** M;

Now, if we define δ and $\mathrm{Sym}^2(\delta)$ such that the following diagram is commutative:

$$\begin{array}{ccc} T_0^c(K_{A_0}) & \xleftarrow{(dV)_0} & T_0^c(K_{A_1}) \\ \uparrow{\scriptstyle \lambda_0} & & \uparrow{\scriptstyle \lambda_0} \\ Q^g & \xleftarrow{\mathrm{Sym}^2(\delta)} & Q^g \\ \uparrow{\scriptstyle \pi_1} & & \uparrow{\scriptstyle \pi_1} \\ \mathbb{A}^g & \xleftarrow{\delta} & \mathbb{A}^g \end{array} \tag{26}$$

then it is clear that:

$$\mathrm{Sym}^2(\delta) = \mathrm{Sym}^2(\delta_0) \circ \mathrm{Sym}^2(\delta_0)^\sigma \circ \dots \circ \mathrm{Sym}^2(\delta_0)^{\sigma^{m-1}} \tag{27}$$

$$\delta = \delta_0 \circ \delta_0^\sigma \circ \dots \circ \delta_0^{\sigma^{m-1}} \tag{28}$$

where

$$\mathrm{Sym}^2(\delta_0) = \lambda_0^{-1} \circ (dV_0)_0 \circ \lambda_0^\sigma. \tag{29}$$

From these formulas, we deduce immediately the Algorithm 5 to compute the Eigenvalues of the Verschiebung morphism V.

We recall that Algorithm 5 corresponds to the Step (4) of the description of Mestre's algorithm to compute the number of points of $\overline{X}$ a curve defined over $\mathbb{F}_q$ with $q = p^m$. We remark that if $p \neq 2$, Algorithm 5 involves no loss of p-adic precision. Actually, one can check easily that all the computations makes sense modulo p as long as the used models have good reduction: $T_0^c(K_A)$ and the morphism $\lambda : Q^g \to T_0^c(K_A)$ are well defined modulo p, so is the matrix $M_{(dV_{m-1})_0}$. In the case of $p = 2$, in the numerical example that we have treated (see next section), we found that the loss of precision was

small. We leave a full analysis of the loss of precision in this case, using the results of [CRV14], for a subsenquent work.

The level 2 theta functions provide with a embedding of a Kummer variety in the projective space of dimension 2^g-1. Moreover the p-adic precision needed for the computation is $m/2$. As a consequence the running time of an operation in $\mathbb{Z}_q$ is $O(m/2\log(p))$. Using Proposition 3.14, we deduce that the running time of Algorithm 5 is $O(\max(g^9,2^g)m/2\log(p))$.

5. Examples

In this section, we suppose given an ordinary genus g curve C defined over $\mathbb{F}_{2^m}$. Let $\overline{A}_0$ be jacobian of C which is an ordinary principally polarized Abelian variety of dimension g. Let A_0 be a canonical lift of $\overline{A}_0$ which is a Abelian scheme of $\mathbb{Z}_{2^m}$. We give a step by step execution of our algorithm when $g=1,2$.

5.1. **Genus 1.** A dimension 1 Kummer K_A variety is obtained as the quotient of an elliptic curve A by the automorphism (-1). It is easily seen that A is isomorphic to the projective line. The arithmetic in the theta representation of Kummer lines has been studied in [GL09].

The level 2 theta functions $(\theta_i^{A_0})_{i\in Z(\overline{2})}$ gives an isomorphism $K_{A_0}\to\mathbb{P}^1_{\mathbb{Z}_{2^m}}$ so that:

$$x_{A_0}=\frac{\theta_1^{A_0}}{\theta_0^{A^0}},$$

is a local parameter of K_{A_0} in 0 (for a general choice of A_0). We note that for $g=1$, K_A is smooth in 0. Keeping the notation of Diagram (25), we can define local parameters x_{A_i} in 0 for K_{A_i} by twisting x_{A_0} by σ^i. The duplication formula gives an expression of $V_{m-1}:A_0\to A_{m-1}$ at 0:

$$x_{A_{m-1}}=\frac{(A+B)x_{A_0}^2+B-A}{(B-A)x_{A_0}^2+A+B}, \tag{30}$$

where $A=\theta_0^{A_{m-1}}(0)+\theta_1^{A_{m-1}}(0)$ and $B=\theta_0^{A_{m-1}}(0)-\theta_0^{A_{m-1}}(0)$. Then, we have:

$$dx_{A_{m-1}}=dx_{A_0}\frac{4x_{A_0}AB}{((B-A)x_{A_0}^2+A+B)^2}. \tag{31}$$

In this case, as the tangent cone and the tangent space are equal, our method is trivial and we obtain the trace of the Frobenius morphism as $t+2^m/t$ where:

$$t=\sqrt{\mathrm{Norm}_{\mathbb{Q}_{2^n}/\mathbb{Q}_2}\left(\frac{4x_{A_0}(0)AB}{(B-A)x_{A_0}(0)^2+A+B)^2}\right)}. \tag{32}$$

5.2. **Genus 2.** Let $(A,\mathscr{L}^2,\Theta_A^2)$ be a Abelian surface together with a level 2 theta structure over the field k such that $\mathrm{char}(k)\neq 2$. When A is not a product of elliptic curves (with their principal polarisations), the embedding $i:K_A\to\mathbb{P}^{Z(2)}$ such that $i^*(O_{\mathbb{P}^{Z(2)}}(1))=\mathscr{L}^2$ is a closed immersion (see [BL04]). The level 2 theta functions satisfy a degree 4 homogeneous equation parametrized by the theta null point $(\theta_i^{\Theta_A^2}(0))_{i\in Z(\overline{2})}$ that we denote by $E((\theta_i^{\Theta_A^2}(0))_{i\in Z(\overline{2})})\in k[X_i,i\in Z(\overline{2})]$. This equation defines the image of i as a closed surface inside $\mathbb{P}^{Z(2)}$ [CF+96; GL09]. From the knowledge of $(\theta_i^{\Theta_A^2}(0))$ one can easily compute $E((\theta_i^{\Theta_A^2}(0))_{i\in Z(\overline{2})})$.

The tangent cone $T_0^c(K_A)$ is a dimension 2 closed subvariety of the dimension 3 tangent space $T_0(K_A)$. If necessary by doing a linear transformation on the basis of theta functions, we can suppose that $\theta_0^{\Theta_A^2}$ does not cancel in $0\in K_A(k)$. Then by doing the change of variables $x_0=1$, $x_i=X_i/X_0+\theta_i(0)/\theta_0(0)$ in $E((\theta_i^{\Theta_A^2}(0))_{i\in Z(\overline{2})})$ we obtain a new equation $E'((\theta_i^{\Theta_A^2}(0))_{i\in Z(\overline{2})})\in k[x_i,i\in Z(\overline{2})-0]$. An equation of $T_0^c(K_A)$ inside $T_0(K_A)$ is given by the degree 2 homogeneous component of $E'((\theta_i^{\Theta_A^2}(0))_{i\in Z(\overline{2})})$ that we denote by Q_{K_A}. We have $T_{K_A}^c=\mathrm{Spec}(k[x_1,x_2,x_3]/Q_{K_A})$.

Proposition 2.4 tells us that there exists a linear isomorphism:

$$\lambda^* : \frac{k[x_1,x_2,x_3]}{Q_A} \to \frac{k[u_{11},u_{22},u_{12}]}{u_{11}u_{22}-u_{12}^2}. \tag{33}$$

One can use Algorithm 3 to find λ^* but in genus 2, we give another point of view. For this, we consider Q_A as a quadratic form and we remark that it is the orthogonal sum of a hyperbolic plane and a definite one dimensional quadratic form. We can compute λ^* with the following steps:

(1) find an isotropic vector v for Q_{K_A} ;
(2) take any w such that $Q^s_{K_A}(v,w) \neq 0$ where $Q^s_{K_A}$ is the scalar product associated to Q_{K_A};
(3) find $\lambda \in k$ such that if we set $w' = w + \lambda v$, we have $Q_{K_A}(w') = 0$ and scale such that $Q^s_{K_A}(v,w') = 1$;
(4) compute an orthogonal vector z to the plane (v,w');
(5) we put $t = -1/2Q_{K_A}(z)$ so that we have an isomorphism

$$\lambda_1 : \frac{k[x_1,x_2,x_3]}{Q_{K_A}} \to \frac{k[u,v,w]}{uv-tw^2}.$$

We remark that all the computations in step (1) to (4) can be done over the base field k. But, in step (5), if t is not a square in k it is not possible to chose z such that $Q_{K_A}(z) = 1$. We define

$$\lambda_2 : \frac{k[u,v,w]}{yv-tw^2} \to \frac{k[u_{11},u_{22},u_{12}]}{u_{11}u_{22}-u_{12}^2},$$

such as $\lambda_2(u) = tu_{11}$, $\lambda_2(v) = u_{22}$, $\lambda_2(w) = u_{12}$ then $\lambda^* = \lambda_2 \circ \lambda_1$.

All the preceding steps are trivial except finding an isotropic vector for Q_{K_A} for which we give more details. In order to find an isotropic vector of $Q_{K_A}(x_1,x_2,x_3)$, we can specialize the variables x_2 and x_3 by computing $Q_{K_A}(x_1,t_2,t_3)$ with $t_2,t_3 \in k$. Then by Proposition 2.8, for a general choice of t_2,t_3, $Q_{K_A}(x_1,t_2,t_3)$ is a degree 2 equation with a solution in k.

5.3. **Example.** Let $\mathbb{F}_8 \simeq \frac{\mathbb{F}_2[u]}{x^3+x+1}$ and denote by $\mathbb{F}_8[x]$ the polynomial ring in the variable x over $\mathbb{F}_8$. Let:

$$\begin{aligned} h &= (x^2+x+1)a^3 + (x+1)a^2 + a + x + 1 \\ k &= xa^3 + (x+1)a^2 + a + x^2 + x + 1 \end{aligned} \tag{34}$$

Let H be the ordinary genus 2 hyperelliptic curve over $\mathbb{F}_{16}$ given by its equation:

$$y^2 + hy = hk \tag{35}$$

Let $\mathbb{Q}_8$ by the unramified extension of $\mathbb{Q}_2$ defined by $\frac{\mathbb{Q}_2[w]}{w^3+w+1}$. Using Thomae formulas, we can compute a level 2 theta null point for the jacobian of H :

$$\theta_{\overline{A}} = [\theta^{\overline{A}}_{00}(0), \theta^{\overline{A}}_{01}(0), \theta^{\overline{A}}_{10}(0), \theta^{\overline{A}}_{11}(0)] = \\ [1, 17+16w^2+O(2^5), 17+24w^2+O(2^5), 1+16w+8w^2+O(2^5)]$$

By computing a sequence of generalized AGM steps starting from $\theta_{\overline{A}}$, we obtain the theta null point of an Abelian variety which is an approximation to 2-adic precision 23 of the canonical lift of a 2^k-isogeneous for a certain k to canonical lift of the Jacobian of H:

$$\theta_{A_0} = [1, 1618241+2703936w+1893624w^2+O(2^{21}), 3154537+1708228w+260732w^2+O(2^{21}), \\ 4465257+856260w+981628w^2+O(2^{21})]$$

With one more step of generalized AGM, we compute the theta null point of A_1 which is 2-isogeneous to A_0:

$$\theta_{A_1} = [1, 1377889+1471112w+287912w^2+O(2^{21}), 306481+424180w+1198760w^2+O(2^{21}), \\ 2010417+686324w+1329832w^2+O(2^{21})]$$

For $i \in Z(\overline{2})$, let $x_i^{A_0} = \theta_i^{A_0}/\theta_0^{A_0}$ (resp. $x_i^{A_1} = \theta_i^{A_1}/\theta_0^{A_1}$) be a coordinate system in a neighbourhood of $0 \in A_0(k)$ (resp. $0 \in A_1(k)$). We use Equation (24) to express the isogeny $V_1 : A_0 \to A_1$ in the coordinate systems $(x_i^{A_j})$ for $j = 0, 1$ and compute the matrix of partial derivates in 0. We obtain:

$$\frac{\partial V_1^*(x_{01}^{A_1})}{\partial x_{01}^{A_0}}(0) = 11325 + 11501w + 12177w^2 + O(2^{14})$$

$$\frac{\partial V_1^*(x_{01}^{A_1})}{\partial x_{10}^{A_0}}(0) = 7980 + 2298w + 12300w^2 + O(2^{15})$$

$$\frac{\partial V_1^*(x_{01}^{A_1})}{\partial x_{11}^{A_0}}(0) = 24364 + 2298w + 12300w^2 + O(2^{15})$$

$$\frac{\partial V_1^*(x_{10}^{A_1})}{\partial x_{01}^{A_0}}(0) = 4178 + 2743/2w + 7815w^2 + O(2^{13})$$

$$\frac{\partial V_1^*(x_{10}^{A_1})}{\partial x_{10}^{A_0}}(0) = 6547 + 895/2w + 606w^2 + O(2^{13})$$

$$\frac{\partial V_1^*(x_{10}^{A_1})}{\partial x_{11}^{A_0}}(0) = 5842 + 11857/2w + 3933w^2 + O(2^{13})$$

$$\frac{\partial V_1^*(x_{11}^{A_1})}{\partial x_{01}^{A_0}}(0) = 4178 + 2743/2w + 7815w^2 + O(2^{13})$$

$$\frac{\partial V_1^*(x_{11}^{A_1})}{\partial x_{10}^{A_0}}(0) = 5842 + 11857/2w + 3933w^2 + O(2^{13})$$

$$\frac{\partial V_1^*(x_{11}^{A_1})}{\partial x_{11}^{A_0}}(0) = 6547 + 895/2w + 606w^2 + O(2^{13})$$

We denote by $M((dV_1)_0)$ the matrix $(\frac{\partial V_1^*(x_i^{A_1})}{\partial x_j^{A_0}})_{ij}$.

We have seen that the tangent cone $T_0^c(K_{A_0})$ is defined as a closed subvariety of $T_0(K_{A_0})$ by a unique quadratic form. In the basis (x_0, x_1, x_2) this quadratic form is given by the matrix $M_{Q_{K_{A_0}}}$ such that:

$$\begin{aligned}[[&75389 + 9245w + 105194w^2 + O(2^{17}), 82775 + 170179w + 39924w^2 + O(2^{18}),\\ &82775 + 137411w + 203764w^2 + O(2^{18})],\\ [&82775 + 170179w + 39924w^2 + O(2^{18}), 42077 + 112217w + 52286w^2 + O(2^{17}),\\ &23789 + 77601w + 69246w^2 + O(2^{18})],\\ [&82775 + 137411w + 203764w^2 + O(2^{18}), 23789 + 77601w + 69246w^2 + O(2^{18}),\\ &42077 + 46681w + 117822w^2 + O(2^{17})]]\end{aligned}$$

Then using the algorithm described in Paragraph 5.2, one can find a matrix M for the linear morphism

$$\lambda_1 : \frac{k[x_1, x_2, x_3]}{Q_A} \to \frac{\mathbb{Q}_{2^m}[u, v, w]}{uv - tw^2}.$$

with

$$t = 2894 + 38321/2w + 35959/2w^2 + 26927w^3 + O(2^{15}).$$

The matrix M is:

$$\begin{aligned}&[[1445/2+986w+892w^2+O(2^{10}), 503/2^3+1081/2^4w+267/2^2w^2+O(2^7), 15+29/2w+71/2^2w^2+O(2^5)],\\ &[83+845w+1289/2w^2+O(2^{10}), 1055/2^4+1773/2^4w+123w^2+O(2^7), 57/2+85/2^2w+83/2^2w^2+O(2^5)],\\ &[81/2+1513w+1821/2w^2+O(2^{11}), 877/2^4+199w+164w^2+O(2^8), 33/2+75/2^2w+10w^2+O(2^6)]]\end{aligned}$$

Denote by σ the 2^{th}-Frobenius automorphism acting on $\mathbb{Q}_8$. Following Algorithm 5, by computing:

$$\mathrm{N}_{\mathbb{Q}_8/\mathbb{Q}_2}(M^{-1}M((dV_1)_0)M^{\sigma}),$$

we obtain the action of the 8^{th}-Frobenius automorphism on the standard tangent cone of K_{A_0}. One must take care a little bit here that if the matrix of the Frobenius morphism acting of $T_0(A_0)$ is given by in the basis (x_0, x_1):

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{36}$$

as we are working with the basis (tx_1^2, x_2^2, x_1x_2) of $\mathrm{Sym}^2(k[x_1, x_2])$ the matrix that we obtain is:

$$\begin{pmatrix} a^2 & tb^2 & tab \\ c^2/t & d^2 & cd \\ ac/t & db & ad+bc \end{pmatrix} \tag{37}$$

which allows to recover the matrix (36) up to a sign. If ρ_1 and ρ_2 are the invertible root modulo 2 of the Frobenius polynomial of the Jacobian of H we obtain that $\rho_1 + \rho_2 = 0 \mod 64$ and $\rho_1\rho_2 = 7 \mod 64$. We deduce immediately that the Frobenius polynomial is:

$$x^4 + 7x^2 + 64.$$

References

[BL04] C. Birkenhake and H. Lange. *Complex abelian varieties*. Second. Vol. 302. Grundlehren der Mathematischen Wissenschaften [Fundament al Principles of Mathematical Sciences]. Berlin: Springer-Verlag, 2004, pp. xii+635. ISBN: 3-540-20488-1 (cit. on pp. 20, 24).

[CKL06] R. Carls, D. Kohel, and D. Lubicz. "Higher dimensional 3-adic CM construction". In: *preprint* (2006) (cit. on pp. 1, 2, 20).

[CL07] R. Carls and D. Lubicz. *Magma implementation of the genus 1 point counting algorithm*. Available at `http://www.mathematik.uni-ulm.de/ReineMath/mitarbeiter/carls/`. 2007 (cit. on p. 1).

[CL08] R. Carls and D. Lubicz. "A p-adic quasi-quadratic time and quadratic space point counting algorithm". In: *International Mathematics Research Notices* (2008) (cit. on pp. 20, 21).

[CL09] R. Carls and D. Lubicz. "A p-adic quasi-quadratic time point counting algorithm". In: *Int. Math. Res. Not. IMRN* 4 (2009), pp. 698–735. ISSN: 1073-7928 (cit. on pp. 1, 2).

[CRV14] X. Caruso, D. Roe, and T. Vaccon. "Tracking p-adic precision". In: *LMS J. Comput. Math.* 17.suppl. A (2014), pp. 274–294. DOI: 10.1112/S1461157014000357. URL: https://doi.org/10.1112/S1461157014000357 (cit. on p. 23).

[CF+96] J. W. S. Cassels, E. V. Flynn, et al. *Prolegomena to a middlebrow arithmetic of curves of genus 2*. Vol. 230. Cambridge University Press, 1996 (cit. on pp. 2, 11, 24).

[CFA+06] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, eds. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006, pp. xxxiv+808. ISBN: 978-1-58488-518-4; 1-58488-518-1 (cit. on p. 18).

[CR15] R. Cosset and D. Robert. "An algorithm for computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of hyperelliptic curves of genus 2". In: *Mathematics of Computation* 84.294 (Nov. 2015), pp. 1953–1975. DOI: 10.1090/S0025-5718-2014-02899-8. URL: http://www.normalesup.org/~robert/pro/publications/articles/niveau.pdf. HAL: hal-00578991, eprint: 2011/143. (Cit. on pp. 1, 2, 21).

[CLO92] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties and Algorithms*. Springer Verlag, New York, 1992 (cit. on p. 5).

[Del69] P. Deligne. "Variétés abéliennes ordinaires sur un corps fini". In: *Inventiones Mathematicae* 8.3 (1969), pp. 238–243 (cit. on p. 19).

[FLR11] J.-C. Faugère, D. Lubicz, and D. Robert. "Computing modular correspondences for abelian varieties". In: *Journal of Algebra* 343.1 (Oct. 2011), pp. 248–277. DOI: 10.1016/j.jalgebra.2011.06.031. arXiv: 0910.4668 [cs.SC]. URL: http://www.normalesup.org/~robert/pro/publications/articles/modular.pdf. HAL: hal-00426338. (Cit. on pp. 1, 2, 21).

[GL09] P. Gaudry and D. Lubicz. "The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines". In: *Finite Fields Appl.* 15.2 (2009), pp. 246–260. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2008.12.006. URL: https://doi.org/10.1016/j.ffa.2008.12.006 (cit. on p. 24).

[GM07] G. van der Geer and B. Moonen. "Abelian varieties". In: *Book in preparation* (2007), p. 71 (cit. on p. 6).

[Gro57] A. Grothendieck. *Fondements de la géométrie algébrique (FGA), Extraits du Séminaire Bourbaki.* 1957 (cit. on p. 6).

[GD+70] A. Grothendieck, M. Demazure, et al. "Schémas en groupes (SGA 3)". In: *Lecture notes in Math* 151 (1970), pp. 152–153 (cit. on p. 6).

[Igu72] J.-i. Igusa. *Theta functions.* Die Grundlehren der mathematischen Wissenschaften, Band 194. New York: Springer-Verlag, 1972, pp. x+232 (cit. on p. 22).

[Ked01] K. Kedlaya. "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology". In: *Preprint* (2001). arXiv: math/0105031 (cit. on p. 19).

[KM97] S. Keel and S. Mori. "Quotients by groupoids". In: *Annals of mathematics* 145.1 (1997), pp. 193–213 (cit. on p. 6).

[Kem92] G. Kempf. "Equations of Kümmer Varieties". In: *American Journal of Mathematics* 114.1 (1992), pp. 229–232 (cit. on p. 2).

[LL06] R. Lercier and D. Lubicz. "A quasi-quadratic time algorithm for hyperelliptic curve point counting". In: *Ramanujan J.* 12.3 (2006), pp. 399–423 (cit. on pp. 20, 21).

[LR12] D. Lubicz and D. Robert. "Computing isogenies between abelian varieties". In: *Compositio Mathematica* 148.5 (Sept. 2012), pp. 1483–1515. DOI: 10.1112/S0010437X12000243. arXiv: 1001.2016 [math.AG]. URL: http://www.normalesup.org/~robert/pro/publications/articles/isogenies.pdf. HAL: hal-00446062. (Cit. on p. 21).

[LR15a] D. Lubicz and D. Robert. "A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties". In: *Journal of Symbolic Computation* 67 (Mar. 2015), pp. 68–92. DOI: 10.1016/j.jsc.2014.08.001. URL: http://www.normalesup.org/~robert/pro/publications/articles/optimal.pdf. HAL: hal-00806923, eprint: 2013/192. (Cit. on p. 2).

[LR15b] D. Lubicz and D. Robert. "Computing separable isogenies in quasi-optimal time". In: *LMS Journal of Computation and Mathematics* 18 (1 Feb. 2015), pp. 198–216. DOI: 10.1112/S146115701400045X. arXiv: 1402.3628. URL: http://www.normalesup.org/~robert/pro/publications/articles/rational.pdf. HAL: hal-00954895. (Cit. on p. 2).

[LR16] D. Lubicz and D. Robert. "Arithmetic on Abelian and Kummer Varieties". In: *Finite Fields and Their Applications* 39 (May 2016), pp. 130–158. DOI: 10.1016/j.ffa.2016.01.009. URL: http://www.normalesup.org/~robert/pro/publications/articles/arithmetic.pdf. HAL: hal-01057467, eprint: 2014/493. (Cit. on pp. 2, 12, 15, 21).

[MR20] A. Maiga and D. Robert. "Computing the canonical lift of genus 2 curves in odd characteristic". Dec. 2020. URL: http://www.normalesup.org/~robert/pro/publications/articles/canonical_lift_g2.pdf. In preparation. (Cit. on pp. 1, 2, 21).

[MR21] A. Maiga and D. Robert. "Computing the 2-adic canonical lift of genus 2 curves". Accepted for publication at Proceedings of the 7th International Conference on Mathematics and Computing (ICMC 2021). Jan. 2021. URL: http://www.normalesup.org/~robert/pro/publications/articles/canonical_lift_g2_p2.pdf. HAL: hal-03119147. (Cit. on pp. 1, 21).

[Mes01] J.-F. Mestre. *Lettre à Gaudry et Harley.* 2001. URL: http://www.math.jussieu.fr/mestre (cit. on pp. 1, 19).

[Mes02a] J.-F. Mestre. *Notes of a talk given at the Cryptography Seminar Rennes*. 2002. URL: http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps (cit. on p. 2).

[Mes02b] J.-F. Mestre. *Notes of a talk given at the Cryptography Seminar Rennes*. Available at http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps. 2002 (cit. on pp. 19, 20).

[Mum66] D. Mumford. "On the equations defining abelian varieties. I". In: *Invent. Math.* 1 (1966), pp. 287–354 (cit. on p. 20).

[Mum83] D. Mumford. *Tata lectures on theta I*. Vol. 28. Progress in Mathematics. With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman. Boston, MA: Birkhäuser Boston Inc., 1983, pp. xiii+235. ISBN: 3-7643-3109-7 (cit. on p. 20).

[MFK94] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric invariant theory*. Vol. 34. Springer Science & Business Media, 1994 (cit. on p. 6).

[NS16] A. Neumaier and D. Stehlé. "Faster LLL-type reduction of lattice bases". In: *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*. 2016, pp. 373–380 (cit. on p. 20).

[Rit03] C. Ritzenthaler. "Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis". PhD thesis. Université Denis Diderot Paris VII, June 2003 (cit. on pp. 1, 20, 22).

[Ryd13] D. Rydh. "Existence and properties of geometric quotients". In: *Journal of Algebraic Geometry* 22.4 (May 13, 2013), pp. 629–669. ISSN: 1056-3911, 1534-7486. DOI: 10.1090/S1056-3911-2013-00615-3. arXiv: 0708.3333. URL: http://arxiv.org/abs/0708.3333 (visited on 07/02/2020) (cit. on p. 6).

[Sat00] T. Satoh. "The canonical lift of an ordinary elliptic curve over a finite field and its point counting". In: *J. Ramanujan Math. Soc.* 15.4 (2000), pp. 247–270 (cit. on pp. 1, 3, 19).

[Shi98] G. Shimura. *Abelian varieties with complex multiplication and modular functions*. Vol. 46. Princeton University Press, 1998 (cit. on p. 3).

[Vél71] J. Vélu. "Isogénies entre courbes elliptiques". In: *Compte Rendu Académie Sciences Paris Série A-B* 273 (1971), A238–A241 (cit. on p. 1).

IRMAR, Universté de Rennes 1, Campus de Beaulieu, F-35042 Rennes FRANCE
E-mail address: david.lubicz@univ-rennes1.fr
URL: http://perso.univ-rennes1.fr/david.lubicz/

INRIA Bordeaux–Sud-Ouest, 200 avenue de la Vieille Tour, 33405 Talence Cedex FRANCE
E-mail address: damien.robert@inria.fr
URL: http://www.normalesup.org/~robert/

Institut de Mathématiques de Bordeaux, 351 cours de la liberation, 33405 Talence cedex FRANCE